

T.C.  
SİNOP ÜNİVERSİTESİ  
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ  
SİYASET BİLİMİ VE KAMU YÖNETİMİ ANABİLİM DALI



TÜRKİYE’DE İÇ SAVUNMADA YAPAY ZEKANIN ETİK AÇIDAN  
DEĞERLENDİRİLMESİ

Fatih Kaan BOZER

YÜKSEK LİSANS TEZİ

DANIŞMAN

DOÇ. DR. ÖZGE ÖNKAN

SİNOP-2025

## TEZ KABUL

**FATİH KAAN BOZER** tarafından hazırlanan “**TÜRKİYE’DE İÇ SAVUNMADA YAPAY ZEKANIN ETİK AÇIDAN DEĞERLENDİRİLMESİ**” başlıklı bu çalışma, **08/10/2025** tarihinde yapılan savunma sınavı sonucunda başarılı bulunarak, jürimiz tarafından oybirliği ile **YÜKSEK LİSANS TEZİ** olarak kabul edilmiştir.

**Başkan**

Prof. Dr. Ali Rıza GÖKBUNAR  
İnönü Üniversitesi / Uygulamalı Bilimler Fakültesi

İmza

**Üye**

**(Danışman)**

Doç. Dr. Özge ÖNKAN  
Sinop Üniversitesi / Boyabat İ.İ.B.F.

İmza

**Üye**

Dr. Öğretim Üyesi Mehmet Samet ERDEM  
Sinop Üniversitesi / Boyabat İ.İ.B.F.

İmza

Enstitü Müdürü

Prof. Dr. Onur ŞAHİN

.....

## ETİK BEYANI

Tez Yazım Kurallarına uygun olarak hazırladığım bu tez çalışmasında; tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi, tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu, tez çalışmasında yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi, kullanılan verilerde herhangi bir değişiklik yapmadığımı, bu tezde sunduğum çalışmanın özgün olduğunu, bildirir, aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

Fatih Kaan BOZER

## ÖZET

### YÜKSEK LİSANS TEZİ

## TÜRKİYE’DE İÇ SAVUNMADA YAPAY ZEKANIN ETİK DEĞERLENDİRİLMESİ

FATİH KAAAN BOZER

SİNOP ÜNİVERSİTESİ

LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

SİYASET BİLİMİ VE KAMU YÖNETİMİ ANABİLİM DALI

DANIŞMAN: DOÇ.DR. ÖZGE ÖNKAN

Yapay zekâ (YZ) teknolojisinin hızlı gelişimi, küresel ölçekte güvenlik ve yönetim dinamiklerinde köklü dönüşümler yaratmaktadır. Bu tez, YZ’nin 21. yüzyılda ulusal güvenlik ve iç savunma stratejileri üzerindeki etkilerini etik yönetim odağında incelemektedir. Çalışmanın amacı, Türkiye’nin iç savunma alanında YZ tabanlı sistemleri nasıl entegre ettiğini ve bu süreçte ortaya çıkan fırsat ve riskleri sistematik biçimde değerlendirmektir. Bulgular, YZ’nin karar döngüsünde hız, kaynak tahsisinde verimlilik ve durumsal farkındalık artışı gibi önemli avantajlar sağladığını; buna karşılık yanlışlık, mahremiyet, ölçülülük ve hesap verebilirlik alanlarında etik riskler doğurduğunu göstermektedir. Araştırma, kanıt haritalaması ve karşılaştırmalı çerçeveleme yöntemleriyle yürütülmüştür. 2015–2025 dönemine ait resmî belgeler, hakemli yayınlar ve kurumsal raporlar üçleme yöntemiyle doğrulanarak analiz edilmiştir. İnceleme kapsamında otonom sistemler, biyometrik tanıma, gözetim ve video analitiği, öngörüşel analiz, karar destek sistemleri, siber savunma, veri yönetimi ve şeffaflık eksenleri ele alınmıştır. Türkiye’nin politika ve uygulamaları, Avrupa Birliği (AB), Ekonomik Kalkınma ve İş Birliği Örgütü (OECD), Birleşmiş Milletler (BM), Birleşmiş Milletler Eğitim, Bilim ve Kültür Örgütü (UNESCO) ve Elektrik ve Elektronik Mühendisleri Enstitüsü (IEEE) çerçeveleriyle; ayrıca Amerika Birleşik Devletleri (ABD), Çin, Hindistan, Güney Kore ve Japonya yaklaşımlarıyla karşılaştırılmıştır. Sonuç olarak Türkiye’nin uluslararası etik standartlarla yüksek uyum gösterdiği, ancak bağlayıcılık ve denetim alanlarında gelişime açık yönler bulunduğu belirlenmiştir. Tez, yüksek riskli kullanımlarda insan denetimi, izlenebilirlik, veri kartları ve bağımsız uygunluk denetimi gibi araçların kurumsal süreçlere entegrasyonunu önermektedir.

**Anahtar Kelimeler:** Yapay Zeka, Etik Yönetim, İç Güvenlik, Uluslararası Karşılaştırma, Politika Analizi

Ekim 2025, 147 Sayfa

## **ABSTRACT**

## **MSC THESIS**

# **ETHICAL EVALUATION OF ARTIFICIAL INTELLIGENCE IN DOMESTIC DEFENCE IN TURKEY**

**FATİH KAAAN BOZER**

**SİNOP UNIVERSITY**

**INSTITUTE OF POSTGRADUATE EDUCATION**

**DEPARTMENT OF POLITICAL SCIENCE AND PUBLIC ADMINISTRATION**

**SUPERVISOR: ASSOCIATE PROFESSOR ÖZGE ÖNKAN**

The rapid development of artificial intelligence (AI) technology has created profound transformations in global security and governance dynamics. This thesis examines the impact of AI on national security and internal defense strategies in the 21st century with a focus on ethical governance. The main objective is to systematically evaluate how Turkey integrates AI-based systems into its internal defense structure and to identify the emerging opportunities and risks in this process. The findings indicate that AI provides significant advantages such as speed in decision-making cycles, efficiency in resource allocation, and enhanced situational awareness, while also generating ethical risks in areas including bias, privacy, proportionality, and accountability. The research is based on evidence mapping and comparative framing methods, analyzing official documents, peer-reviewed publications, and institutional reports from the 2015–2025 period through triangulation. The findings are evaluated across dimensions such as autonomous systems, biometric identification, surveillance and video analytics, predictive analysis, decision-support systems, cyber defense, data governance, and transparency. Turkey's policies and practices are compared with the frameworks of the European Union (EU), the Organisation for Economic Co-operation and Development (OECD), the United Nations (UN), the United Nations Educational, Scientific and Cultural Organization (UNESCO), and the Institute of Electrical and Electronics Engineers (IEEE), as well as with the approaches of the United States (USA), China, India, South Korea, and Japan. The results show that Turkey demonstrates a high level of alignment with international ethical standards, yet has room for improvement in enforcement, oversight, and standardization. The thesis recommends integrating tools such as meaningful human control, traceability, data cards, data minimization, and independent conformity assessment into institutional processes, providing an evidence-based and ethically grounded governance framework.

**Keywords:** Artificial Intelligence, Ethical Governance, Internal Security, International Comparison, Policy Analysis

October 2025, 147 pages

## TEŞEKKÜR

Yüksek lisans eğitimim boyunca bana yol gösteren, desteğini hiçbir zaman esirgemeyen, bilgi birikimiyle bakış açımı zenginleştirerek her daim gelişime katkı sunan değerli danışmanım Doç. Dr. Özge ÖNKAN'a en içten teşekkürlerimi sunarım. Akademik yolculuğumun her aşamasında bilgi ve deneyimiyle bana ışık tutan, karşılaştığım zorluklar karşısında pes etmemem için beni sürekli motive eden, desteğini ve ilgisini hiçbir zaman esirgemeyen Dr. Öğr. Üyesi Mehmet Samet ERDEM'e yürekten teşekkür ederim.

Hayatımın her anında olduğu gibi bu zorlu süreçte de desteğini ve sevgisini benden esirgemeyen, her daim yanımda olan, sevincimi paylaşan ve düştüğümde beni ayağa kaldıran aileme minnettarım. Varlıkları, bu yolculuğun en güçlü dayanağı olmuştur.

Akademik serüvenime başlamamda beni motive eden, desteğini her zaman hissettiren dostum, arkadaşım ve abim Hakan GÜZÜN'e; ayrıca tez çalışmam süresince katkı sağlayan, destek olan ve yol gösteren herkese teşekkür eder, saygılarımı sunarım.

Fatih Kaan BOZER

## İÇİNDEKİLER

|                                                                |     |
|----------------------------------------------------------------|-----|
| TEZ KABUL.....                                                 | i   |
| ETİK BEYANI.....                                               | ii  |
| ÖZET .....                                                     | iii |
| ABSTRACT .....                                                 | iv  |
| TEŞEKKÜR.....                                                  | v   |
| İÇİNDEKİLER.....                                               | vi  |
| TABLolar DİZİNİ.....                                           | x   |
| SİMGELER VE KISALTMALAR DİZİNİ.....                            | xi  |
| 1. GİRİŞ.....                                                  | 1   |
| 2. YAPAY ZEKA SİSTEMİ .....                                    | 3   |
| 2.1 Yapay Zeka Tanımı ve Kavramı .....                         | 3   |
| 2.2 Yapay Zeka Tarihçesi.....                                  | 6   |
| 2.2.1 Hesaplama ve mantık temelleri .....                      | 7   |
| 2.2.1.1 Sembolik mantığın doğuşu .....                         | 8   |
| 2.2.1.2 Mekanik hesaplama cihazları .....                      | 8   |
| 2.2.1.3 İkili sayı sistemi.....                                | 8   |
| 2.2.1.4 Olasılık düşüncesi.....                                | 9   |
| 2.2.1.5 Mantık cebiri .....                                    | 9   |
| 2.2.1.6 Görsel mantık .....                                    | 9   |
| 2.2.2 Otomasyon ve programlanabilir makinelerin yükselişi..... | 9   |
| 2.2.2.1 Programlanabilir makinelerin öncüsü .....              | 10  |
| 2.2.2.2 Modern bilgisayarların kavramsal temeli .....          | 10  |
| 2.2.2.3 Genel amaçlı programlanabilir mimarinin doğuşu.....    | 10  |
| 2.2.2.4 İlk bilgisayar programcısı.....                        | 10  |
| 2.2.3 YZ biliminin doğuşu ve teorik yapıtaşları .....          | 11  |
| 2.2.3.1 Hesaplanabilirlik teorisi .....                        | 11  |
| 2.2.3.2 Yapay sinir ağının keşfi .....                         | 11  |
| 2.2.3.3 Siberetik ve geri besleme .....                        | 11  |
| 2.2.3.4 “Düşünen Makine” Kavramı .....                         | 12  |
| 2.2.3.5 Zeka sınavı: Turing Testi .....                        | 12  |
| 2.2.3.6 “Yapay Zeka” Teriminin ortaya çıkışı .....             | 12  |
| 2.2.3.7 Erken algoritmalar ve programlama dilleri .....        | 12  |
| 2.2.4 Öğrenen ve akıl yürüten sistemler .....                  | 13  |
| 2.2.4.1 Makine öğreniminin ilk adımları.....                   | 13  |

|                                                                                     |           |
|-------------------------------------------------------------------------------------|-----------|
| 2.2.4.2 Yapay sinir ağlarında gelişmeler .....                                      | 13        |
| 2.2.4.3 Mantıksal akıl yürütme ve uzman sistemler .....                             | 14        |
| 2.2.4.4 Olasılıksal akıl yürütme.....                                               | 14        |
| 2.2.4.5 Derin öğrenme atılımları .....                                              | 14        |
| 2.2.5 Otonom ve fiziksel robotlar .....                                             | 15        |
| 2.2.5.1 Uzaktan kumanda ve erken otomatlar .....                                    | 15        |
| 2.2.5.2 Endüstriyel ve mobil otomasyon.....                                         | 15        |
| 2.2.5.3 İnsansı ve sosyal robotlar .....                                            | 16        |
| 2.2.5.4 Sürücüsüz araçlar ve otonom sistemler .....                                 | 16        |
| 2.2.5.5 Ev robotları ve ticari yayılım.....                                         | 16        |
| 2.2.6 Doğal dil anlama ve insan etkileşimi .....                                    | 17        |
| 2.2.6.1 Erken sohbet programları .....                                              | 17        |
| 2.2.6.2 Gelişmiş dil işleme ve bilgi erişimi .....                                  | 17        |
| 2.2.6.3 Büyük dil modelleri (LLM).....                                              | 18        |
| 2.2.6.4 Diyalojsal YZ ve kitlelere ulaşım .....                                     | 18        |
| 2.2.6.5 Sesli asistanlar ve akıllı cihazlar .....                                   | 18        |
| 2.2.7 YZ'nin toplumsal yansımaları, etik tartışmalar ve “YZ Kışları” .....          | 19        |
| 2.2.7.1 Erken eleştirel yaklaşımlar .....                                           | 19        |
| 2.2.7.2 “YZ Kışları” ve Gerçekçi beklentiler .....                                  | 20        |
| 2.2.7.3 Teknolojik tekillik ve gelecek kaygıları .....                              | 20        |
| 2.2.7.4 Etik ve güvenli YZ gelişimi .....                                           | 20        |
| 2.3 YZ Sistemlerinin ve Uygulamalarının Amacı .....                                 | 21        |
| 2.4 YZ'nin Öğrenme Metotları.....                                                   | 22        |
| 2.4.1 Denetimli öğrenme .....                                                       | 22        |
| 2.4.2 Denetimsiz öğrenme.....                                                       | 23        |
| 2.4.3 Yarı-Denetimli öğrenme .....                                                  | 23        |
| 2.4.4 Pekiştirmeli öğrenme.....                                                     | 24        |
| 2.4.5 Derin öğrenme .....                                                           | 24        |
| 2.4.6 Transfer öğrenme.....                                                         | 25        |
| 2.5 Yapay Zekanın Önemi .....                                                       | 25        |
| <b>3. TÜRKİYE’DE YAPAY ZEKA VE İÇ GÜVENLİK ETKİLEŞİMİNİN DEĞERLENDİRİLMESİ.....</b> | <b>28</b> |
| 3.1 YZ ve İç Güvenlik .....                                                         | 28        |
| 3.2 YZ'nin İç Güvenlik Alanına Entegrasyonunun Tarihçesi .....                      | 30        |
| 3.2.1 Araştırma ekosisteminin doğuşu ve kurumsal temeller.....                      | 30        |



|                                                                                                          |    |
|----------------------------------------------------------------------------------------------------------|----|
| 3.2.2 Otonom sistemler ve operasyonel uygulamalar .....                                                  | 31 |
| 3.2.3 Biyometrik gözetim ve etik gerilimler .....                                                        | 31 |
| 3.2.4 Ulusal stratejiler ve jeopolitik rekabet.....                                                      | 32 |
| 3.2.5 Uluslararası normlar ve sorumlu YZ.....                                                            | 32 |
| 3.3 Seçilmiş Ülkelerin Güncel Yapay Zeka Politikaları.....                                               | 33 |
| 3.3.1 Amerika Birleşik Devletleri.....                                                                   | 33 |
| 3.3.2 Çin Halk Cumhuriyeti .....                                                                         | 34 |
| 3.3.3 Hindistan .....                                                                                    | 35 |
| 3.3.4 Güney Kore .....                                                                                   | 36 |
| 3.3.5 Japonya.....                                                                                       | 36 |
| 3.4 Seçilmiş Ülkelerin İç Güvenliğine Dair Geliştirdikleri Yapay Zeka Politikaları ve Uygulamaları ..... | 37 |
| 3.4.1 Amerika Birleşik Devletleri'nin YZ uygulamaları ve sistemleri .....                                | 37 |
| 3.4.1.1 ABD'nin sınır güvenliği için YZ uygulamaları.....                                                | 40 |
| 3.4.1.2 Siber savunma ve tehdit tespiti için YZ .....                                                    | 41 |
| 3.4.1.3 İç Güvenlik Analitiği ve Suç Tahmini YZ Sistemleri.....                                          | 42 |
| 3.4.2 Çin Halk Cumhuriyeti'nin YZ uygulamaları ve sistemleri .....                                       | 44 |
| 3.4.2.1 Çin'in otonom ve sürü insansız hava/deniz/kara araçları.....                                     | 46 |
| 3.4.2.2 YZ tabanlı istihbarat ve gözetleme sistemleri .....                                              | 47 |
| 3.4.2.3 Sınır güvenliği ve göçmen izleme sistemleri .....                                                | 48 |
| 3.4.2.4 Siber savunma ve tehdit tespiti.....                                                             | 49 |
| 3.4.2.5 İç güvenlik ve polis uygulamaları .....                                                          | 50 |
| 3.4.3 Hindistan YZ Uygulamaları ve Sistemleri .....                                                      | 51 |
| 3.4.3.1 İç Güvenlik ve Polislik Uygulamaları .....                                                       | 53 |
| 3.4.4 Güney Kore'nin YZ Sistem ve Uygulamaları .....                                                     | 55 |
| 3.4.4.1 İç güvenlik ve polislik uygulamaları .....                                                       | 58 |
| 3.4.5 Japonya'nın YZ uygulamaları ve sistemleri.....                                                     | 59 |
| 3.4.5.1 İç güvenlik ve polis uygulamaları .....                                                          | 61 |
| 3.5 Türkiye'nin Yapay Zeka Politikası .....                                                              | 63 |
| 3.5.1 Ulusal Yapay Zeka Stratejisi hedefleri ve temel ilkeleri .....                                     | 64 |
| 3.6 Türkiye'de Yapay Zeka Alanını Düzenleyen ve Destekleyen Çeşitli Yasal ve İdari Belgeler              |    |
| 65                                                                                                       |    |
| 3.6.1 2015-2018 Bilgi Toplumu Stratejisi ve Eylem Planı.....                                             | 65 |
| 3.6.2 6698 Sayılı Kişisel Verilerin Korunması Kanunu .....                                               | 66 |
| 3.6.3 On Birinci Kalkınma Planı .....                                                                    | 67 |
| 3.6.4 Dijital Dönüşüm Ofisi .....                                                                        | 68 |

|                                                                                                                     |            |
|---------------------------------------------------------------------------------------------------------------------|------------|
| 3.6.5 Ulusal Yapay Zeka Stratejisi Genelgesi .....                                                                  | 69         |
| 3.6.6 On İkinci Kalkınma Planı(OKP) .....                                                                           | 69         |
| 3.6.7 TBMM Yapay Zeka Kanun Teklifi ve Yapay Zeka Araştırma Komisyonu .....                                         | 71         |
| 3.6.8 183 Sayılı Cumhurbaşkanlığı Kararnamesi .....                                                                 | 72         |
| 3.7 Türkiye'nin İç Güvenlik Alanına Etki Eden Yapay Zeka Belgeleri ve Stratejileri .....                            | 72         |
| 3.7.1 Ulusal Siber Güvenlik Stratejisi .....                                                                        | 73         |
| 3.7.2 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2016-2019 .....                                               | 73         |
| 3.7.3 Türkiye Siber Güvenlik Kümelenmesi Projesi .....                                                              | 74         |
| 3.7.4 Siber Güvenlik Kurulu'nun kaldırılması ve kurumsal değişim .....                                              | 74         |
| 3.7.5 Ulusal Siber Güvenlik Stratejisi ve 2020-2023 Eylem Planı .....                                               | 75         |
| 3.7.6 Ulusal Siber Güvenlik Stratejisi ve 2024-2028 Eylem Planı .....                                               | 76         |
| 3.7.7 Siber Güvenlik Kanunu No. 7545 .....                                                                          | 76         |
| 3.8 Türkiye'nin İç Güvenlik Alanında Kullandığı YZ Sistemleri ve Uygulamaları .....                                 | 77         |
| 3.8.1 İç güvenlikte kullanılabilecek askeri YZ sistemleri .....                                                     | 77         |
| 3.8.2 İç güvenlikte iç işleri bakanlığına bağlı birimlerde kullanılan YZ uygulamaları .....                         | 79         |
| 3.8.2.1 YZ entegrasyonu ve kurumsal dönüşüm .....                                                                   | 79         |
| 3.8.2.2 Biyometrik tanıma sistemleri .....                                                                          | 80         |
| 3.8.2.3 Gözetim, video analitiği ve plaka tanıma sistemleri .....                                                   | 81         |
| 3.8.2.4 Öngörüye dayalı analitik ve siber savunma .....                                                             | 81         |
| 3.8.2.5 Çeşitlenen uygulama alanları .....                                                                          | 82         |
| <b>4. TÜRKİYE'NİN İÇ GÜVENLİĞİNDE YAPAY ZEKAYA İLİŞKİN ETİK SORUNLAR.....</b>                                       | <b>84</b>  |
| 4.1 Yapay Zeka Etiği .....                                                                                          | 84         |
| 4.2 Yapay Zeka Etiğinin Çerçevesi Uluslararası Kuruluşlar .....                                                     | 86         |
| 4.2.1 Avrupa Birliği .....                                                                                          | 86         |
| 4.2.2 Elektrik ve Elektronik Mühendisleri Enstitüsü .....                                                           | 87         |
| 4.2.3 Ekonomik İşbirliği ve Kalkınma Örgütü .....                                                                   | 88         |
| 4.2.4 UNESCO .....                                                                                                  | 89         |
| 4.2.5 Birleşmiş Milletler .....                                                                                     | 90         |
| 4.3 Türkiye ve Yapay Zeka Etiği .....                                                                               | 91         |
| 4.4 Türkiye'nin Ulusal Yapay Zeka Stratejisi Etik İlkeleri ile Uluslararası Etik Çerçevenin Karşılaştırılması ..... | 94         |
| 4.5 Seçilmiş Ülkeler ve Türkiye'nin Uluslararası Etik Belgelerle Karşılaştırılması .....                            | 101        |
| <b>5. SONUÇ .....</b>                                                                                               | <b>105</b> |
| <b>6. KAYNAKÇA .....</b>                                                                                            | <b>108</b> |
| <b>ÖZGEÇMİŞ .....</b>                                                                                               | <b>132</b> |

## TABLÖLAR DİZİNİ

|                                                                                                           |     |
|-----------------------------------------------------------------------------------------------------------|-----|
| Tablo 1.1 Yapay Zeka Tanımları.....                                                                       | 5   |
| Tablo 2.3.1. Yapay Zeka Etik Çerçevesini Oluşmasını Katkı Sağlayan Uluslararası Kurumlar<br>.....         | 95  |
| Tablo 3.3.2. Tablo Seçilmiş Ülkeler ve Türkiye'nin Uluslararası Etik Belgelerle<br>Karşılaştırılması..... | 101 |



## SİMGELER VE KISALTMALAR DİZİNİ

### Kısaltmalar

|                |                                                                                                                                           |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| <b>AAAI</b>    | : Yapay Zeka Geliştirme Derneği                                                                                                           |
| <b>ABD</b>     | : Amerika Birleşik Devletleri                                                                                                             |
| <b>AFIS</b>    | : Otomatik Parmak İzi Tanıma                                                                                                              |
| <b>AI</b>      | : Yapay Zeka                                                                                                                              |
| <b>AI Act</b>  | : Yapay Zeka Yasası                                                                                                                       |
| <b>AIMA</b>    | : Artificial Intelligence: A Modern Approach                                                                                              |
| <b>ALPR</b>    | : Otomatik Plaka Tanıma                                                                                                                   |
| <b>APFIS</b>   | : Gelişmiş Parmak ve Parmak İzi Tanıma Sistemi                                                                                            |
| <b>ARCYBER</b> | : Ordu Siber Komutanlığı (ABD)                                                                                                            |
| <b>ARPA</b>    | : Gelişmiş Araştırma Projeleri Ajansı                                                                                                     |
| <b>ASIMO</b>   | : Advanced Step in Innovative Mobility (Honda Firmasının Robotu)                                                                          |
| <b>ATS</b>     | : Otomatik Hedefleme Sistemi (ABD)                                                                                                        |
| <b>BAHA</b>    | : Bulut Altı (HAVELSAN Firmasının Keşif-Gözetleme Platformu)                                                                              |
| <b>BSF</b>     | : Sınır Güvenlik Gücü (Hindistan)                                                                                                         |
| <b>BTK</b>     | : Bilgi Teknolojileri ve İletişim Kurumu                                                                                                  |
| <b>C4I</b>     | : Komuta, Kontrol, Haberleşme, Bilgisayar ve İstihbarat                                                                                   |
| <b>CAC</b>     | : Siber Uzay İdaresi (Çin)                                                                                                                |
| <b>CAEIT</b>   | : Elektronik ve Bilgi Teknolojisi Akademisi(Çin)                                                                                          |
| <b>CAIR</b>    | : Yapay Zeka ve Robotik Merkezi (Hindistan)                                                                                               |
| <b>CBDDO</b>   | : Cumhurbaşkanlığı Dijital Dönüşüm Ofisi                                                                                                  |
| <b>CBP</b>     | : Gümrük ve Sınır Koruma (ABD)                                                                                                            |
| <b>CDAO</b>    | : Baş Dijital ve Yapay Zeka Ofisi (ABD)                                                                                                   |
| <b>CGC</b>     | : Cyber Grand Challenge (DARPA Tarafından Düzenlenen Tamamen Otomatik Çalışan Siber Savunma Sistemlerini Geliştirmeyi Hedefleyen Turnuva) |
| <b>CIBMS</b>   | : Kapsamlı Entegre Sınır Yönetim Sistemi                                                                                                  |
| <b>CoEAI</b>   | : Yapay Zeka Mükemmeliyet Merkezi                                                                                                         |
| <b>CETC</b>    | : China Electronics Tehnology Group Corporation (Çin'in Teknoloji Şirketi)                                                                |
| <b>CNMF</b>    | : Siber Ulusal Misyon Gücü (ABD)                                                                                                          |
| <b>CSIC</b>    | : China Shipbuilding Industry Corporation (Çin'in Teknoloji Şirketi)                                                                      |
| <b>DAIC</b>    | : Savunma Yapay Zeka Konseyi (Hindistan)                                                                                                  |
| <b>DAIPA</b>   | : Savunma Yapay Zeka Proje Ajansı (Hindistan)                                                                                             |

|                |                                                                                                                                                            |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>DARPA</b>   | : Gelişmiş Araştırma Projeleri Ajansı (ABD)                                                                                                                |
| <b>DEA</b>     | : Uyuşturucuyla Mücadele Dairesi (ABD)                                                                                                                     |
| <b>DMZ</b>     | : Askerden Arındırılmış Bölge (Güney Kore)                                                                                                                 |
| <b>DoD</b>     | : Savunma Bakanlığı (ABD)                                                                                                                                  |
| <b>DRDO</b>    | : Savunma Araştırma ve Geliştirme Organizasyonu (Hindistan)                                                                                                |
| <b>EAD</b>     | : Ethically Aligned Design (IEEE Tarafından Geliştirilmiş, Otonom ve Yapay Zeka Sistemlerinde Etik Değerleri Bütünsel Olarak Dikkate Alan Bir Rehber Seti) |
| <b>EGM</b>     | : Emniyet Genel Müdürlüğü (Türkiye)                                                                                                                        |
| <b>EIA</b>     | : Etik Etki Değerlendirmesi (UNESCO)                                                                                                                       |
| <b>ETRI</b>    | : Elektronik ve Telekomünikasyon Araştırma Enstitüsü (Güney Kore)                                                                                          |
| <b>FBI</b>     | : Federal Soruşturma Bürosu (ABD)                                                                                                                          |
| <b>FRT</b>     | : Yüz Tanıma Teknolojisi (Face Recognition Technology)                                                                                                     |
| <b>FRVT</b>    | : Yüz Tanıma Satıcısı Testi (ABD)                                                                                                                          |
| <b>G20</b>     | : Yirmi Ekonomi Grubu                                                                                                                                      |
| <b>GACC</b>    | : Çin Gümrükleri Genel İdaresi                                                                                                                             |
| <b>GAMER</b>   | : Güvenlik ve Acil Durumlar Koordinasyon Merkezi (Türkiye)                                                                                                 |
| <b>GPU</b>     | : Grafik İşlem Birimi                                                                                                                                      |
| <b>GPAI</b>    | : Küresel Yapay Zeka Ortaklığı                                                                                                                             |
| <b>GPT</b>     | : Üretken Metin Oluşturabilen Büyük Dil Modellerinin Genel Adı                                                                                             |
| <b>HLAB-AI</b> | : Yüksek Düzeyli Yapay Zeka Danışma Kurulu (BM)                                                                                                            |
| <b>HLEG</b>    | : Yüksek Düzeyli Yapay Zeka Uzman Grubu (Avrupa Komisyonu)                                                                                                 |
| <b>HPC</b>     | : Yüksek Başarımli Hesaplama                                                                                                                               |
| <b>IATA</b>    | : Uluslararası Hava Taşımacılığı Birliği                                                                                                                   |
| <b>ICT</b>     | : Bilgi ve İletişim Teknolojileri                                                                                                                          |
| <b>IEEE</b>    | : Elektrik ve Elektronik Mühendisleri Enstitüsü                                                                                                            |
| <b>İHA</b>     | : İnsansız Hava Aracı                                                                                                                                      |
| <b>ISO</b>     | : Uluslararası Standardizasyon Örgütü                                                                                                                      |
| <b>ITU</b>     | : Uluslararası Telekomünikasyon Birliği                                                                                                                    |
| <b>JADU</b>    | : Jandarma Akıllı Devriye Uygulaması (Türkiye)                                                                                                             |
| <b>JAIC</b>    | : Ortak Yapay Zeka Merkezi (ABD)                                                                                                                           |
| <b>KCG</b>     | : Kore Sahil Güvenlik                                                                                                                                      |
| <b>KGYS</b>    | : Kent Güvenlik Yönetim Sistemi (Türkiye)                                                                                                                  |
| <b>KNP</b>     | : Kore Ulusal Polis Teşkilatı                                                                                                                              |
| <b>KVKK</b>    | : Kişisel Verilerin Korunması Kanunu (Türkiye)                                                                                                             |
| <b>LAWS</b>    | : Ölümcül Otonom Silah Sistemleri                                                                                                                          |

|                |                                                                       |
|----------------|-----------------------------------------------------------------------|
| <b>Lisp</b>    | : Programlama Dili                                                    |
| <b>MCTE</b>    | : Askeri Telekomünikasyon Mühendisliği Koleji (Hindistan)             |
| <b>MHA</b>     | : İçişleri Bakanlığı (Hindistan)                                      |
| <b>MIT</b>     | : Massachusetts Teknoloji Enstitüsü                                   |
| <b>MND</b>     | : Milli Savunma Bakanlığı (Güney Kore)                                |
| <b>MOIS</b>    | : İçişleri ve Güvenlik Bakanlığı (Güney Kore)                         |
| <b>MOJ</b>     | : Adalet Bakanlığı (Güney Kore)                                       |
| <b>MPS</b>     | : Kamu Güvenliği Bakanlığı (Çin)                                      |
| <b>MSIT</b>    | : Bilim ve Bilgi Teknolojileri Bakanlığı (Güney Kore)                 |
| <b>MSS</b>     | : Devlet Güvenlik Bakanlığı (Çin)                                     |
| <b>MTDP</b>    | : Orta Vadeli Savunma Programı (Japonya)                              |
| <b>MYCIN</b>   | : Uzman Sistem                                                        |
| <b>NATGRID</b> | : Ulusal İstihbarat Ağı (Hindistan)                                   |
| <b>NATO</b>    | : Kuzey Atlantik Antlaşması Örgütü                                    |
| <b>NDPG</b>    | : Ulusal Savunma Programı Yönergeleri (Japonya)                       |
| <b>NGAIDP</b>  | : Yeni Nesil Yapay Zeka Gelişim Planı (Çin)                           |
| <b>NGI</b>     | : Yeni Nesil Kimlik Belirleme (FBI)                                   |
| <b>NIS</b>     | : Ulusal İstihbarat Servisi (Güney Kore)                              |
| <b>NIST</b>    | : Ulusal Standartlar ve Teknoloji Enstitüsü (ABD)                     |
| <b>NLP</b>     | : Doğal Dil İşleme                                                    |
| <b>NORINCO</b> | : China North Industries Group Corporation (Çin'in Teknoloji Şirketi) |
| <b>NSA</b>     | : Ulusal Güvenlik Ajansı (ABD)                                        |
| <b>NSAI</b>    | : Yapay Zeka için Ulusal Strateji (Hindistan)                         |
| <b>NSCAI</b>   | : Yapay Zeka Ulusal Güvenlik Komisyonu (ABD)                          |
| <b>NSM</b>     | : Ulusal Güvenlik Memorandumu (ABD)                                   |
| <b>NUDT</b>    | : Ulusal Savunma Bilim-Teknoloji Üniversitesi (Çin)                   |
| <b>OECD</b>    | : Ekonomik İşbirliği ve Kalkınma Örgütü                               |
| <b>OKP</b>     | : On İkinci Kalkınma Planı (Türkiye)                                  |
| <b>OMB</b>     | : Yönetim ve Bütçe Ofisi (ABD)                                        |
| <b>OPTES</b>   | : Biyometrik Veri Yönetim Sisteminin Parçası                          |
| <b>PCFIR</b>   | : Dördüncü Sanayi Devrimi Başkanlık Komitesi (Güney Kore)             |
| <b>PÖ</b>      | : Pekiştirmeli Öğrenme                                                |
| <b>PLA</b>     | : Halk Kurtuluş Ordusu (Çin)                                          |
| <b>RAM</b>     | : Hazırlık Ölçüm Metodolojisi (UNESCO)                                |
| <b>REAIM</b>   | : İlk Küresel Askeri Alanda Sorumlu Yapay Zeka Zirvesi                |

|                  |                                                                                  |
|------------------|----------------------------------------------------------------------------------|
| <b>R.U.R.</b>    | : Rossum's Universal Robots                                                      |
| <b>SBB</b>       | : Strateji ve Bütçe Başkanlığı (Türkiye)                                         |
| <b>SDF</b>       | : Öz Savunma Kuvvetleri (Japonya)                                                |
| <b>SEAD/DEAD</b> | : Düşman Hava Savunmalarının Bastırılması / İmhası                               |
| <b>SGK</b>       | : Sahil Güvenlik Komutanlığı (Türkiye)                                           |
| <b>SKA</b>       | : Sürdürülebilir Kalkınma Amaçları (BM)                                          |
| <b>SNARC</b>     | : Yapay Sinir Ağı Modeli                                                         |
| <b>SOME</b>      | : Siber Olaylara Müdahale Ekipleri (Türkiye)                                     |
| <b>SSB</b>       | : Savunma Sanayii Başkanlığı (Türkiye)                                           |
| <b>STB</b>       | : Sanayi ve Teknoloji Bakanlığı (Türkiye)                                        |
| <b>STM</b>       | : Türkiye Merkezli Sivil ve Askeri Alanlarda Faaliyet Gösteren Teknoloji Şirketi |
| <b>TBMM</b>      | : Türkiye Büyük Millet Meclisi                                                   |
| <b>TİHA</b>      | : Taktiksel İnsansız Hava Aracı                                                  |
| <b>TSK</b>       | : Türk Silahlı Kuvvetleri                                                        |
| <b>UAB</b>       | : Ulaştırma ve Altyapı Bakanlığı (Türkiye)                                       |
| <b>UCAV</b>      | : İnsansız Hava Taarruz Uçağı                                                    |
| <b>UDHB</b>      | : Ulaştırma, Denizcilik ve Haberleşme Bakanlığı (Türkiye)                        |
| <b>UN</b>        | : Birleşmiş Milletler                                                            |
| <b>UNESCO</b>    | : Birleşmiş Milletler Eğitim, Bilim ve Kültür Örgütü                             |
| <b>USOM</b>      | : Ulusal Siber Olaylara Müdahale Merkezi (Türkiye)                               |
| <b>UYZS</b>      | : Ulusal Yapay Zeka Stratejisi (Türkiye)                                         |
| <b>VR/AR</b>     | : Sanal Gerçeklik – Artırılmış Gerçeklik                                         |
| <b>YETEN</b>     | : Yetkinlik Tabanlı Ekosistem Yönetimi                                           |
| <b>YDÖ</b>       | : Yarı-Denetimli Öğrenme                                                         |
| <b>YZ</b>        | : Yapay Zekâ                                                                     |

## 1. GİRİŞ

Yapay zekâ (YZ) güncel literatürde genel amaçlı bir teknoloji olarak ele alınır. Kavramsal temellerden güncel uygulamalara uzanan gelişim, toplumsal yaşamı, ekonomiyi ve kamu hizmetlerini dönüştürür. Güvenlik alanında da benzer bir etki görülür. YZ sistemleri algılama, çıkarım ve karar süreçlerini hızlandırır. Ölçeklenebilirlik artar. Buna karşılık güvenlik gereksinimleri ile hak-odaklı yönetim beklentileri arasında bir gerilim doğar. Bu tez, söz konusu gerilimi kavramsal arka plan ve tarihsel gelişim çizgisi üzerinden ele alır.

Türkiye, YZ'yi iç güvenlik ve kamu düzeni uygulamalarına kademeli biçimde entegre etmektedir. Bu süreç, YZ'nin uluslararası ölçekte stratejik bir kapasiteye dönüşmesi ile paraleldir. Entegrasyon karar desteğini güçlendirir ve operasyonel etkinliği artırır. Bununla birlikte yanlışlık, mahremiyet, ölçülülük ve hesap verebilirlik başlıklarında etik ve hukuki riskler ortaya çıkar. Çalışma, bu fırsat ve riskleri sistematik olarak inceler ve bulguları politika-uygulama önerileriyle birleştirir.

Tezin amacı, Türkiye'nin iç güvenlik pratiğinde YZ kullanımını etik yönetim perspektifiyle değerlendirmektir. Bu kapsamda Türkiye'nin YZ tabanlı çözümleri nasıl entegre ettiği, entegrasyonun sağladığı faydalar ve ürettiği riskler analiz edilmiştir. Riskler yanlışlık, mahremiyet, ölçülülük ve hesap verebilirlik başlıkları altında sınıflandırılmıştır. Türkiye'deki ilke ve uygulamalar, Avrupa Birliği (AB), Ekonomik İşbirliği ve Kalkınma Teşkilatı (OECD), Birleşmiş Milletler Eğitim, Bilim ve Kültür Örgütü (UNESCO), Elektrik ve Elektronik Mühendisleri Enstitüsü (IEEE) ve Birleşmiş Milletler (BM) gibi uluslararası normatif çerçeveler ile Amerika Birleşik Devletleri (ABD), Çin, Hindistan, Japonya ve Güney Kore'nin politika yaklaşımlarıyla karşılaştırılmıştır. Analiz 2015–2025 dönemi resmî belgeleri, hakemli yayınları ve güvenilir kurum raporlarını temel alır. Yöntem, kanıt haritalaması ve karşılaştırmalı çerçevelemedir. İnceleme altı tematik eksen üzerinde yürütülür: otonom sistemler, biyometri ve kimlik doğrulama, büyük ölçekli gözetim ve video analitiği, öngörüselsel analitik ve karar destek, siber savunma, veri yönetimi ve şeffaflık.

Çalışmanın katkısı birden fazla düzeydedir. Türkiye bağlamında etik yönetim açısından güçlü uyum noktalarını ve geliştirilmesi gereken alanları birlikte gösteren karşılaştırmalı bir değerlendirme çerçevesi sunar. Yüksek riskli kullanım alanlarında anlamlı insan denetimi, izlenebilirlik ve bağımsız denetim gereksinimlerini erken aşamada tanımlar. Veri egemenliğinin KVKK ile uyumlu mahremiyet ilkeleriyle birlikte işletilmesi için tasarımdan itibaren



mahremiyet yaklaşımını somutlaştırır. Çalışma ayrıca çok paydaşlı yönetim ve disiplinler arası insan kaynağı geliştirme gereksinimini politika önerileriyle somutlaştırır.

Tezin yapısı giriş ve kaynakça bölümü hariç dört bölümden oluşmaktadır. Birinci bölüm YZ'nin kavramsal temellerini, tarihçesini ve öğrenme paradigmalarını ele alır. İkinci bölüm Türkiye'de YZ-iç güvenlik etkileşiminin tarihsel ve kurumsal boyutunu inceler ve strateji-mevzuat çerçevesini analiz eder. Üçüncü bölüm YZ etiği çerçevelerini sunar ve UYZS ilkeleriyle karşılaştırır. Dördüncü bölüm bulguları özetler ve politika yapıcılar ile uygulayıcılar için uygulanabilir öneriler geliştirir.



## 2. YAPAY ZEKA SİSTEMİ

YZ'nin kavramsal temelleri, insan merkezli ve rasyonel-ideal tip yaklaşımlar doğrultusunda açıklanmaktadır. Turing'in "taklit oyunu" yaklaşımı ve 1956'da gerçekleştirilen Dartmouth Konferansı, YZ'nin kurumsal temelleri olarak değerlendirilmektedir. Literatürde yaygın biçimde kullanılan Russell ve Norvig'in iki eksenli sınıflandırma çerçevesi bu değerlendirmeye yön vermektedir.

YZ alanının tarihsel gelişimi yedi tematik eksen üzerinden sistematik biçimde ele alınmaktadır. Bu eksenler; sembolik kökenler, programlanabilir makineler ve sibernetik, öğrenme ve çıkarım süreçleri, robotik ve otonomi, doğal dil etkileşimi, toplumsal ve etik yansımalar ile "YZ kışları" başlıklarını kapsamaktadır.

Çağdaş YZ'nin yöntemsel temelini oluşturan başlıca öğrenme paradigmaları tanımlanmaktadır. Denetimli, denetimsiz, yarı denetimli, pekiştirmeli, derin ve transfer öğrenme yaklaşımları arasındaki temel metodolojik farklılıklar karşılaştırılmaktadır. Bu karşılaştırma, alanın kuramsal çeşitliliğini ve yöntemsel gelişim çizgisini görünür kılmayı amaçlamaktadır.

Son olarak, YZ'nin devlet politikaları ve kurumsal stratejiler bağlamında neden kritik bir genel amaçlı teknoloji olarak değerlendirildiği tartışılmaktadır. Bu tartışma, güvenlik ve rekabet dinamikleri ile hak odaklı yönetim gereklilikleri arasındaki dengeyi irdelemekte ve tez kapsamında kullanılacak kavramsal çerçevenin temelini oluşturmaktadır.

### 2.1 Yapay Zeka Tanımı ve Kavramı

YZ kavramının çözümlenmesi, yalnızca teknik bir terimin tanımlanmasıyla sınırlı değildir. Bu kavramın, insan zihninin işleyişine ilişkin tarihsel varsayımlarla, kültürel hayal gücüyle ve teknoloji-toplum etkileşimleriyle birlikte ele alınması gerekmektedir. Günümüzde tanımlayıcı sınırların görece muğlak olduğu görülmektedir. Bunun başlıca nedenleri, hızlı inovasyon döngülerinin uygulama alanlarını genişletmesi ve The Matrix gibi distopik anlatıların "kontrolü ele geçiren makineler" imgesini yayarak toplumsal kaygıları beslemesidir (Bostrom, 2017: 8). Bu popüler korkular, YZ'nin insanlığı köleleştirebileceği ya da bir "süper zekâ"nın insan otoritesini aşabileceği yönündeki senaryoları gündeme taşıyarak kavramsal netliği gölgeleyebilmektedir. Dolayısıyla YZ'nin olası evrimini tutarlı biçimde değerlendirmek için disiplinler arası bir yaklaşımın benimsenmesi uygun görülmektedir.

YZ'nin kavramsal temeli, iki anahtar sözcüğün sözlüksel çözümlemesine dayanmaktadır. Türk Dil Kurumu "yapay"ı, doğadaki örneklerine benzer biçimde insan eliyle üretilmiş varlıklar

olarak; “zekâ”yı ise akıl yürütme, öğrenme ve yargılama gibi bilişsel yeteneklerin bütünü olarak tanımlamaktadır. Bu iki tanım birleştirildiğinde YZ, “insana benzer biçimde algılama, öğrenme ve karar verme” yetenekleri gösteren makine sistemleri olarak nitelendirilmektedir (TDK, 2025). Nitekim Özcan, teknolojik ilerlemenin, neredeyse her nesnenin “sentetik ikizini” üretebilir hale gelmesiyle “yapay” nitelemesinin giderek yaygınlaştığını belirtir (Özcan ve Sütçü, 2023: 5).

YZ’nin düşünsel ve kurumsal temelleri, “insan gibi düşünebilen makineler” fikrinin felsefi bir meydan okumaya dönüşmesiyle atılmıştır. Alan Turing’in “Computing Machinery and Intelligence” başlıklı makalesi, “Makineler düşünebilir mi?” sorusunu ortaya koymuş; önerdiği “taklit oyunu” (daha sonra “Turing Testi” olarak anılmıştır), bir makinenin yazılı diyalog yoluyla insan sorgulayıcıyı yanıltacak ölçüde inandırıcı yanıtlar verip veremeyeceğini ölçmeyi amaçlamıştır (Turing, 1950). Söz konusu ölçüt; doğal dilde tutarlı yanıt üretme, alan bilgisini işlevsel kullanma, mantıksal çıkarım yapma ve yeni deneyimlerden öğrenerek davranışı uyarlama olmak üzere dört yeteneğin aynı sistemde birleşmesini gerektirmektedir (Oppy ve Dowe, 2003). Bugüne kadar bu testi tutarlı bir şekilde geçtiği genel kabul gören bir sistemin henüz geliştirilmemiş olması, insan-benzeri zekanın karmaşıklığına işaret etmektedir (Landymore, 2025).

Turing’in ortaya koyduğu çerçeve, 1955’te John McCarthy, Marvin Minsky, Nathaniel Rochester ve Claude Shannon tarafından kaleme alınan “Dartmouth Summer Research Project on Artificial Intelligence” önerisine doğrudan zemin hazırlamıştır. Bu öneri, “insan zekasının tüm yönlerinin bir makine tarafından simüle edilebileceği” varsayımına dayanmaktadır (McCarthy vd., 1955). Temmuz–Ağustos 1956’da gerçekleştirilen Dartmouth Konferansı ise YZ teriminin akademik literatüre resmen giriş yaptığı dönüm noktası olarak kabul edilmektedir. Konferansta “insan zekâsını taklit eden makineler” fikri ayrıntılı biçimde tartışılmış ve “artificial intelligence” adlandırması teyit edilmiştir (Dartmouth, 2006). Böylece YZ araştırmaları, deneysel bilişsellikten mühendislik uygulamalarına geçebilmek için ilk kurumsal çatısını kazanmıştır.

Bunu izleyen dönemde Persson, “Yapay zekâ nedir?” sorusuna verilen yanıtların anlamsal tartışmalara saplanabildiğini belirterek alanın daha işlevsel biçimde sınırlandırılmasını önermiştir. Persson’a göre YZ, “insan etkinliklerinde rastlanan ve ‘zekice’ sayılabilecek davranışları sergileyen makinelerin tasarımı”dır (Persson, 1964: 88). Bu çerçeve, erken YZ literatüründe insanı taklit eden sistem tasarımı ana odak olarak konumlandırmış ve daha sonra “dar YZ” yaklaşımının çekirdeğini beslemiştir.

Stuart Russell ve Peter Norvig'in Artificial Intelligence: A Modern Approach (AIMA) adlı eseri, alanın kapsamlı ders kitaplarından biri olarak kabul edilmektedir. Yazarlar YZ'yi çift eksenli bir matrisle kavramsallaştırmaktadır: “insan benzerliği ↔ rasyonel ideallik” ve “düşünme süreçleri ↔ davranış çıktıları”. Bu yapı, literatürde yinelenen sekiz tanımı dört ana kümeye indirgemekte ve kavramsal alanı düzenlemektedir (Russell ve Norvig, 2016: 2-3).

Tablo 1.1 Yapay Zeka Tanımları

| <b>Düşünme Davranış</b> | <b>İnsana Yakın</b>                                                   | <b>Rasyonel Ölçüt</b>                                                  |
|-------------------------|-----------------------------------------------------------------------|------------------------------------------------------------------------|
| <b>Düşünmek</b>         | 1. Thinking Humanly (Bellman 1978; Haugeland 1985)                    | 3. Thinking Rationally (Charniak ve McDermott 1985; Winston 1992)      |
| <b>Davranmak</b>        | 2. Acting Humanly – Turing Testi (Kurzweil 1990; Rich ve Knight 1991) | 4. Acting Rationally – Rasyonel ajan (Nilsson 1998; Poole et al. 1998) |

(Kaynak: Russel ve Norvig (2016)'dan örnek alınmıştır)

YZ'nin iki eksenli çerçevesi, projelerin “İnsan ne yapıyor?” sorusundan mı yoksa “İdeal karar ne olurdu?” sorusundan mı hareketle tasarlandığını hızlıca saptamaya yardımcı olmaktadır. Bu çerçevede dört yaklaşım öne çıkmaktadır:

- **İnsanca Düşünme (Thinking Humanly):** Bu gelenek, bilgisayar programlarının insan zihninin gerçek işleyişini yakalamasını hedeflemektedir. Bellman, YZ'yi “insan düşünmesini gerektiren etkinliklerin mekanikleştirilmesi” olarak tanımlar (1978, akt. Russell ve Norvig, 2016: 2). Haugeland, “tam anlamıyla zihne sahip makineler” vurgusuyla ölçütü yükseltir (1985, akt. Russell ve Norvig, 2016: 2). İçgözlem, davranışsal deneyler ve beyin görüntüleme gibi ampirik yöntemler, bilişsel bilim ile YZ'yi buluşturur (Russell ve Norvig, 2016: 4).
- **İnsanca Davranmak (Acting Humanly):** Turing'in “taklit oyunu” (1950), bir sorgucunun yazılı diyalog sırasında makineyi insandan ayırt edememesine dayanan Turing Testi ile YZ'ye işlevsel bir ölçüt getirmiştir. Testi geçebilecek bir sistemin; doğal dil işleme, bilgi temsili, otomatik akıl yürütme, makine öğrenmesi, bilgisayarlı görü ve robotik olmak üzere altı beceriyi entegre etmesi beklenir (Russell ve Norvig, 2016: 3-4). Bu çerçeve, YZ'yi yalnızca simgesel akıl yürütmeye

ya da istatistiksel öğrenmeye indirgemeyen geniş bir yetkinlik seti öngörür. Kurzweil, YZ'yi “insanlar tarafından gerçekleştirildiğinde zekâ gerektiren işlevleri yerine getiren makineler yaratma sanatı” olarak tanımlar (1990, akt. Russell ve Norvig, 2016: 2). Rich ve Knight, odağı “şu anda insanların daha iyi yaptığı işleri bilgisayarların nasıl yapabileceği” sorusuna indirger (1991, akt. Russell ve Norvig, 2016: 2).

- **Rasyonel Düşünme (Thinking Rationally):** Aristoteles’in kıyas mantığından 19. yüzyıl sembolik mantığına uzanan çizgi, “doğru sonuçlara götüren akıl yürütme şemaları” geliştirmeyi amaçlar (Russell ve Norvig, 2016: 4). Charniak ve McDermott ile Winston, bu yaklaşımı “algılamak, akıl yürütmek ve eyleme geçmek için gerekli hesaplamaların çalışılması” biçiminde özetler (1985,1992, akt. Russell ve Norvig, 2016: 2). Mantıksal YZ, bilgiyi kesin kurallarla ifade ederek sonuç çıkarmaya yönelir; ancak belirsizlik ve hesaplama karmaşıklığı önemli güçlükler oluşturur. Buna karşın, otomatik teorem ispatı ve bilgi tabanlı sistemler gibi alanlarda değeri sürmektedir.
- **Rasyonel Davranmak (Acting Rationally):** AIMA rasyonel ajanı, “sahip olduğu bilgiye dayanarak her durumda en iyi sonucu üretecek eylemi seçen sistem” olarak tanımlar (Russell ve Norvig, 2016: 4). Nilsson bunu “yapay varlıklardaki zeki davranışın çalışılması” olarak; Poole ve arkadaşları ise “hesaplamalı zekâ: zeki ajan tasarımının incelenmesi” olarak genişletir (1998, 1998, akt. Russell ve Norvig, 2016: 2).

Sonuç olarak, iki eksenli yaklaşım (insana benzerlik ↔ rasyonel ideallik; düşünme süreçleri ↔ davranış çıktıları) YZ projelerinin hangi düşünme biçimine dayandığını ve hangi yetkinlikleri geliştirmeyi hedeflediğini açık biçimde göstermektedir. Bu yapı, araştırmacıların yöntem seçimini ve değerlendirme ölçütlerini daha tutarlı biçimde belirlemesine olanak tanımakta, böylece YZ'nin kuramsal temelleri ile uygulama alanları arasında sistematik bir bağ kurmaktadır.

## 2.2 Yapay Zeka Tarihçesi

YZ tarihçesi, insanlığın bilgi işleme, mantık ve hesaplama alanlarındaki birikimini bütüncül biçimde yansıtan bir gelişim çizgisi olarak değerlendirilmektedir. Bu gelişim süreci, sembolik mantık ve ikili sistem gibi temel kavramların ortaya çıkışından günümüzdeki gelişmiş YZ sistemlerinin oluşumuna kadar uzanmaktadır.

Tarihsel ilerleyişi daha açık biçimde ortaya koymak ve neden–sonuç ilişkilerini görünür kılmak amacıyla bu çalışma, YZ’nin gelişimini yedi tematik başlık altında incelemektedir. Çalışmanın temel amacı, YZ’nin düşünsel temellerden toplumsal ve etik boyutlara kadar uzanan gelişim hattını “fikir → makine → kuram → öğrenme → bedenlenme → dil/etkileşim → toplum/etik” eksenini boyunca bütüncül bir bakışla sunmaktır.

İncelenen YZ tarihçesi yedi ana temada ele alınmaktadır:

- Hesaplama Düşüncesinin Temelleri: Bilgi işleme ve mantıksal akıl yürütmeye dayalı ilk fikirlerin gelişimi.
- Programlanabilir Makinelerin Gelişimi: Mekanik sistemlerden programlanabilir yapılara uzanan teknolojik dönüşüm.
- YZ’nin Bilim Olarak Kurumsallaşması: Zekanın matematiksel olarak modellenmesi ve disiplinin bilimsel kimlik kazanması.
- Kural Yazımından Öğrenmeye Geçiş: Sistemlerin önceden tanımlı kurallar yerine veriden örüntü çıkarma yeteneği kazanması.
- Fiziksel Dünyada Bedenlenme: Zekânın yalnızca soyut bir süreç değil, fiziksel sistemlerle bütünleşen bir işlev hâline gelmesi.
- Dil ve Etkileşim Boyutu: İnsan-makine iletişiminin gelişmesi ve doğal dilin hesaplamalı biçimde işlenmesi.
- Toplumsal ve Etik Yansımalar: YZ’nin toplumsal yaşam, güven, sorumluluk ve etik değerlere etkisinin tartışılması.

Her bir tema, dönemin genel eğilimlerini, temsil niteliği taşıyan örnekleri ve alanın yönünü belirleyen temel kırılma noktalarını kapsamaktadır. Amaç, tarihsel gelişimi yalnızca kronolojik olarak sıralamak değil, bu gelişmelerin ardındaki düşünsel mantığı, teknolojik ilerlemeleri ve toplumsal yansımaları bütüncül bir çerçevede değerlendirmektir.

### 2.2.1 Hesaplama ve mantık temelleri

Bu başlıkta, YZ’nin düşünsel temelini oluşturan sembolik mantık, hesaplama ilkeleri ve matematiksel biçimselleştirme çabalarını kapsamaktadır. İkili sayı sisteminden mantık cebirine uzanan gelişim çizgisi, insan aklının kurallara dayalı bir dile aktarılabilmesi düşüncesini somutlaştırmış ve bilgisayar mimarilerinin kavramsal altyapısını oluşturmuştur. Bu süreçle birlikte “düşünme”nin temsil edilebilir ve işletilebilir bir süreç olduğu anlayışı yerleşmiştir.

### 2.2.1.1 Sembolik mantığın doğuşu

YZ'nin entelektüel temelleri, insan düşüncesini semboller aracılığıyla temsil etme çabalarına dayanmaktadır. Bu alandaki ilk sistematik girişim, Ramon Llull'un *Ars Generalis Ultima* (1308) adlı eserinde görülür. Llull, kavramları sınıflandırma ve bunlar arasındaki ilişkileri simgesel biçimde ifade etme amacıyla bir "kombinasyon mantığı" geliştirmiştir (Artlab EPFL, 2018). Bu yaklaşım, bilgi temsiline yönelik en erken mekanikleşme denemelerinden biri olarak kabul edilmektedir.

Bu çizgiyi daha ileriye taşıyan isim, Gottfried Wilhelm Leibniz olmuştur. Leibniz, *Dissertatio De Arte Combinatoria* (1666) adlı çalışmasında düşüncelerin sembolik biçimlerle temsil edilip yeni anlam kombinasyonları üretilebileceğini öne sürmüştür (UCLA, 2016: 3-7). Bu yaklaşımın, algoritmik düşüncenin felsefi temellerine katkı sunduğu ve yapay zekânın biçimsel temsil anlayışının erken bir örneğini ortaya koyduğu görülmektedir.

### 2.2.1.2 Mekanik hesaplama cihazları

Sembolik düşünceden mekanik hesaplama geçiş, insan zihninin işlemlerini fiziksel sistemlere aktarma yönünde önemli bir aşamayı temsil eder. Wilhelm Schickard'ın 1623'te geliştirdiği mekanik hesap makinesi, otomatik toplama ve çarpma yapabilmesiyle bilgisayar öncesi dönemin ilk adımlarından biri olmuştur (Prinz, 2023).

Bu dönemde Blaise Pascal tarafından geliştirilen Pascaline (1642), toplama ve çıkarma işlemlerini otomatikleştiren ilk ticari hesap makinesi olarak dikkat çeker. Pascal'ın bu buluşu, mekanik işlemlerin yaygınlaşmasını sağlamış ve hesaplamanın insan zihninden bağımsız olarak yürütülebileceği düşüncesini güçlendirmiştir (Akbulut, 2012; Britannica, 2022).

Benzer biçimde Leibniz, *Stepped Reckoner* (1673) adını verdiği makinesiyle çarpma ve bölme işlemlerini mekanikleştirerek karmaşık hesaplamaların otomatik biçimde yürütülmesini mümkün kılmıştır (Haverford, t.y.). Bu gelişmeler, modern bilgisayar mimarilerinin temellerini atan erken dönemin önemli kilometre taşlarıdır.

### 2.2.1.3 İkili sayı sistemi

Modern hesaplamanın matematiksel temeli, Leibniz'in *Explication de l'Arithmétique Binaire* (1703) adlı çalışmasıyla atılmıştır. Leibniz, doğadaki karşıtlık ilkesinden yola çıkarak tüm sayısal işlemlerin yalnızca "0" ve "1" değerleriyle temsil edilebileceğini göstermiştir. Bu yaklaşım, dijital devre tasarımının ve çağdaş bilgisayarların temelini oluşturmuş, YZ'nin mantıksal işlem gücüne dayanan yapısını mümkün kılmıştır (Bloch, 2019; Milestone, t.y.).

#### **2.2.1.4 Olasılık düşüncesi**

YZ'nin belirsizlik altında karar verme ve çıkarım yapma yeteneği, Thomas Bayes'in 1763 tarihli Essay towards solving a Problem in the Doctrine of Chances adlı çalışmasına dayanmaktadır. Bayes'in geliştirdiği teorem, olayların olasılıksal ilişkilerle açıklanabileceğini ortaya koyarak, belirsizlik içeren durumlarda akıl yürütmenin matematiksel biçimde modellenmesini sağlamıştır (Bayes ve Price, 1763/1997). Günümüzde olasılıksal modeller, makine öğrenmesi ve tahmine dayalı sistemlerin çekirdek bileşenini oluşturmaktadır.

#### **2.2.1.5 Mantık cebiri**

YZ'nin sembolik işleme kabiliyeti, George Boole'un An Investigation of the Laws of Thought (1854) adlı eseriyle kavramsal bütünlüğe ulaşmıştır. Boole, düşünme sürecini “doğru” ve “yanlış” değerleri üzerinden formelleştirerek mantıksal işlemleri cebirsel bir yapıya dönüştürmüştür. Bu sistem, günümüz bilgisayarlarında kullanılan AND, OR ve NOT devrelerinin doğrudan öncülüdür (Boole, 2005: 27-28). Mantık cebiri, bilgi işlemeyi kurallı bir biçime sokarak YZ'nin sembolik temsil gücünün temelini oluşturmuştur.

#### **2.2.1.6 Görsel mantık**

Bilginin soyut düzlemde görsel temsile taşınması, çıkarım süreçlerinin anlaşılmasını kolaylaştırmıştır. John Venn tarafından 1880 yılında geliştirilen “Venn Diyagramları”, küme ilişkilerini görselleştirerek mantıksal önermeler arasındaki bağlantıları sezgisel biçimde açıklamayı mümkün kılmıştır (Jain, 2024; Venn, 1880). Bu yaklaşım, bilgi temsiline görsel bir boyut kazandırmış ve günümüzde dahi YZ eğitiminde kavramsal ilişkilerin öğretiminde kullanılmaya devam etmektedir.

### **2.2.2 Otomasyon ve programlanabilir makinelerin yükselişi**

Bu başlıkta, mekanik otomatlardan program depolayabilen ve talimatları izleyerek işlem yapabilen cihazlara geçiş sürecini açıklamaktadır. Delikli kartlardan analitik makine tasarımına uzanan bu gelişim hattı, yazılım ve donanım arasındaki ayrımı görünür kılmış ve genel amaçlı hesaplama fikrinin temellerini atmıştır. Bu dönüşümle birlikte, düşünsel “fikir” fiziksel donanıma bürünmüş; hesaplama süreçleri tekrarlanabilir, ölçeklenebilir ve hata payı azaltılmış hale gelmiştir.



### **2.2.2.1 Programlanabilir makinelerin öncüsü**

Otomasyon fikrinin pratik biçimde uygulandığı ilk örneklerden biri, Joseph Marie Jacquard tarafından geliştirilen delikli kartlı dokuma tezgâhıdır. 1804 yılında üretilen bu tezgah, desen talimatlarını delikli kartlar aracılığıyla makineye ileterek dokuma işlemini insan müdahalesi olmadan gerçekleştirmiştir. Bu sistem, üretim sürecini standartlaştırmış ve “program depolama” fikrini ilk kez somut bir biçimde ortaya koymuştur (Britannica, 2024; Computerhistory, t.y.-a). Jacquard’ın tezgahı, yalnızca endüstriyel otomasyonu değil, daha sonra bilgisayar biliminde kullanılacak olan veri ve komutun ayrımı kavramını da öngörmüştür.

### **2.2.2.2 Modern bilgisayarların kavramsal temeli**

Mekanik hesaplamanın soyut bir düşünceden mühendislik düzeyine taşınması, Charles Babbage tarafından geliştirilen Fark Makinesi (1822) ile mümkün olmuştur. Bu makine, karmaşık polinom tablolarını hatasız biçimde hesaplamak üzere tasarlanmış ve otomatik hesaplama kavramını ilk kez işlevsel biçimde ortaya koymuştur (Marsh, 2022; Sciencemuseum, 2023). Babbage’ın tasarımı, hesaplamayı standartlaştırma ve insan hatasını azaltma çabasını somutlaştırarak modern bilgisayar düşüncesinin öncülü olmuştur. Bu dönemde mekanik bileşenlerle çalışan sistemler, soyut matematiksel işlemlerin fiziksel bir düzeneğe aktarılabilmesini göstermiştir.

### **2.2.2.3 Genel amaçlı programlanabilir mimarinin doğuşu**

Babbage, 1837’de geliştirdiği Analitik Makine tasarımıyla modern bilgisayarların kavramsal mimarisini öngörmüştür. Tasarımında yer alan bellek (store), işlem birimi (mill) ve kontrol mekanizmaları, günümüz merkezi işlem birimlerinin (CPU) işleyişini büyük ölçüde yansıtmaktadır. Babbage, delikli kartları veri ve talimat girişi için kullanarak yazılım ile donanım arasındaki işlevsel ayrımı ilk kez sistematik biçimde ortaya koymuştur (Marsh, 2022; Sciencemuseum, 2023). Bu yenilik, makinelerin yalnızca belirli görevleri değil, farklı talimat setlerini uygulayarak çok amaçlı işlevler yerine getirebileceğini göstermiştir.

### **2.2.2.4 İlk bilgisayar programcısı**

Babbage’ın çalışmalarına entelektüel katkı sağlayan Ada Lovelace, 1843 yılında Analitik Makine üzerine kaleme aldığı notlarda Bernoulli sayılarının hesaplanmasına yönelik bir algoritma geliştirmiştir. Bu çalışma, tarihteki ilk bilgisayar programı olarak kabul edilmektedir (Biography, 2021; Günel ve Bakırcı, 2021). Lovelace’in yaklaşımı, makinenin yalnızca sayısal işlemler değil, sembolik işlemler de gerçekleştirebileceğini öne sürerek yazılım kavramının

doğuşuna zemin hazırlamıştır. Onun katkısı, YZ'nin temelini oluşturan “soyut düşüncenin mekanik uygulanabilirliği” fikrinin erken bir ifadesi olarak değerlendirilmektedir.

### **2.2.3 YZ biliminin doğuşu ve teorik yapıtaşları**

Bu bölüm, “makine gerçekten düşünebilir mi?” sorusuna verilen erken dönem kuramsal yanıtları ele almaktadır. Hesaplanabilirlik, sibernetik ve sinirsel modeller, zekânın kurallara dayalı, ölçülebilir ve sınanabilir bir olgu olarak ele alınabileceğini göstermiştir. “Yapay zekâ” teriminin akademik literatüre girmesiyle birlikte alan, hedeflerini, yöntemlerini ve değerlendirme ölçütlerini tanımlayarak bağımsız bir araştırma disiplini hâline gelmiştir.

#### **2.2.3.1 Hesaplanabilirlik teorisi**

YZ'nin teorik zeminini oluşturan en önemli adımlardan biri, Alan Turing'in 1936 tarihli Turing Makinesi modelidir. Turing, “her hesap prosedürünün bir bant, bir okuma-yazma kafası ve sonlu kurallar dizisiyle temsil edilebileceğini” ileri sürerek algoritmaların evrensel bir modelini tanımlamıştır (Turing, 1937: 231-232). Bu yaklaşım, düşünmenin bir dizi işlem olarak modellenebileceği fikrini güçlendirmiş ve makinelerin karmaşık problemleri çözme kapasitesini kavramsallaştırmıştır.

#### **2.2.3.2 Yapay sinir ağının keşfi**

YZ'nin biyolojik esinli temelleri, 1940'lı yıllarda Warren McCulloch ve Walter Pitts tarafından geliştirilen sinirsel mantık modeliyle atılmıştır. Araştırmacılar, nöronların iki değerli mantık sistemiyle eşleştirilebileceğini ve bu yapıların, Turing makinesinin gerçekleştirdiği hesaplamaları simüle edebileceğini ortaya koymuştur(Mcculloch ve Pitts, 1943: 115-129).

Bu dönemde Donald Hebb, The Organization of Behavior (1949) adlı çalışmasında “birlikte ateşleyen nöronlar bağ kurar” ilkesini öne sürmüştür(Hebb, 2005). Hebb'in bu yaklaşımı, öğrenen yapay sinir ağlarının temelini oluşturmuş ve bağlantısal öğrenme fikrinin ortaya çıkmasına zemin hazırlamıştır.

#### **2.2.3.3 Sibernetik ve geri besleme**

YZ'nin gelişiminde önemli bir kuramsal katkı da Norbert Wiener'in Cybernetics (1948) adlı çalışmasıyla gelmiştir. Wiener, canlı ve makine sistemlerinde kontrol ve iletişim döngülerinin işleyişini açıklamış; geri besleme (feedback) mekanizmalarının, sistemlerin çevresine uyum sağlayabilmesi için temel bir rol oynadığını göstermiştir (Wiener, 2019). Bu yaklaşım, daha sonra pekiştirmeli öğrenme (reinforcement learning) yöntemlerinin kuramsal öncülü olarak değerlendirilmektedir.

#### **2.2.3.4 “Düşünen Makine” Kavramı**

YZ’nin toplumsal farkındalık kazanmasında Edmund Berkeley’in Giant Brains (1949) adlı eseri etkili olmuştur. Berkeley, bilgisayarların “machines that think” yani “düşünebilen makineler” olabileceği fikrini geniş kitlelere tanıtarak alanın popülerleşmesine katkı sağlamıştır (Berkeley, 2022; Özdemir, 2022: 631-632). Bu dönemde “düşünen makine” kavramı, yalnızca teknik bir olasılık değil, aynı zamanda insan–makine ilişkisini yeniden tanımlayan felsefi bir tartışma konusu hâline gelmiştir.

#### **2.2.3.5 Zeka sınavı: Turing Testi**

YZ’nin ölçülebilir bir olgu hâline gelmesini sağlayan en önemli önerilerden biri, Turing’in 1950 tarihli Computing Machinery and Intelligence makalesidir. Bu çalışmada Turing, “taklit oyunu” adı verilen bir deneyle bir makinenin insan benzeri zekâ sergileyip sergileyemeyeceğini ölçmeyi önermiştir (Turing, 1950). Bu test, davranış temelli bir zekâ ölçütü sunarak alanın deneysel araştırma yöntemlerine yön vermiştir.

#### **2.2.3.6 “Yapay Zeka” Teriminin ortaya çıkışı**

YZ’nin bağımsız bir bilim alanı olarak tanınması, 1955–1956 yılları arasında düzenlenen Dartmouth Yaz Araştırma Projesi ile gerçekleşmiştir. John McCarthy, Marvin Minsky, Nathaniel Rochester ve Claude Shannon tarafından yürütülen bu proje kapsamında “artificial intelligence” terimi ilk kez akademik düzeyde tanımlanmış ve YZ araştırmaları sistematik bir kimlik kazanmıştır (Dartmouth, 2006).

#### **2.2.3.7 Erken algoritmalar ve programlama dilleri**

1950’li yıllar, YZ’nin uygulamaya dönük ilk örneklerinin geliştirildiği dönem olmuştur. Marvin Minsky, 1951 yılında SNARC adlı vakum tüplü sinirsel ağı tasarlayarak öğrenme yeteneği sergileyen ilk mekanik sistemi ortaya koymuştur (Russell ve Norvig, 2016: 35). Arthur Samuel’in 1952’de geliştirdiği dama programı, deneyim yoluyla performansını artırabilen ilk “kendini öğrenen” yazılım olarak kabul edilmektedir (Wiederhold ve McCarthy, 1992: 2).

Bu dönemde Allen Newell ve Herbert Simon tarafından geliştirilen Logic Theorist (1955), matematik teoremlerini ispatlayabilen bir sistem olarak sembolik akıl yürütmenin gücünü göstermiştir (Kamer ve Ural, 2009: 20-21). Frank Rosenblatt’ın 1957 tarihli Perceptron modeli, örüntü tanıma kavramını geliştirerek derin öğrenmenin temellerini atmıştır (Kamer ve Ural, 2009: 32-33). John McCarthy’nin 1958’de geliştirdiği LISP programlama dili, sembolik hesaplama odaklanarak YZ araştırmalarının temel araçlarından biri hâline gelmiştir

(Mccarthy, 1996). Son olarak, Arthur Samuel'in 1959 tarihli Machine Learning makalesi, veriye dayalı kendini geliştiren sistemlerin kavramsal çerçevesini çizmiş ve "makine öğrenmesi" terimini literatüre kazandırmıştır (Wiederhold ve McCarthy, 1992: 8).

Bu dönemde şekillenen kuramsal yapı, hesaplanabilirlik teorisinden öğrenen programlara uzanan bir gelişim çizgisi ortaya koymuştur. Sibernetik, sinirsel ağ modelleri ve erken algoritmaların kesişimi, YZ'nin yalnızca teknik bir alan değil, bilişsel süreçleri anlamaya çalışan disiplinler arası bir bilim dalı olarak konumlanmasını sağlamıştır. Bu gelişmeler, modern YZ araştırmalarının kurumsal temelini oluşturmuş ve alanın sonraki on yıllarda hızla genişlemesine zemin hazırlamıştır.

#### **2.2.4 Öğrenen ve akıl yürüten sistemler**

Bu başlıkta da YZ araştırmalarında önceden tanımlı kurallara dayalı sistemlerden, veriden öğrenebilen modellere geçiş süreci açıklamaktadır. 1950'lerden itibaren geliştirilen makine öğrenimi, sinir ağları ve olasılıksal akıl yürütme yaklaşımları, YZ'nin bilgi işleme biçimini kökten değiştirmiştir. Bu gelişmeler, sistemlerin yalnızca verilen komutları uygulayan yapılar olmaktan çıkarak, deneyim yoluyla kendini geliştirebilen öğrenen yapılara dönüşmesini sağlamıştır.

##### **2.2.4.1 Makine öğreniminin ilk adımları**

Makine öğrenimi kavramı, 1950'li yılların başlarında yapılan öncü çalışmalarla temellenmiştir. Arthur Samuel, 1952 yılında kendi kendine öğrenebilen bir dama programı geliştirerek bilgisayarların deneyimden yararlanabileceğini göstermiştir. Samuel'in 1959 tarihli makalesinde "machine learning" terimini literatüre kazandırması, bu alanın kavramsal çerçevesinin oluşmasına katkı sağlamıştır. Bu çalışmalar, öğrenme süreçlerinin yalnızca programcı tarafından belirlenen kurallara bağlı kalmadan, veri üzerinden otomatik biçimde geliştirilebileceğini ortaya koymuştur.

##### **2.2.4.2 Yapay sinir ağlarında gelişmeler**

Yapay sinir ağları alanındaki ilerlemeler, insan beyninin öğrenme biçiminden esinlenen modellerin YZ araştırmalarında giderek daha fazla önem kazandığını göstermektedir. Daha önce değinilen Marvin Minsky'nin SNARC sistemi ve Frank Rosenblatt'ın Perceptron modeli, öğrenen makinelerin uygulanabilirliğini göstermiştir. Bu dönemin devamında, Bryson ve Ho tarafından geliştirilen Applied Optimal Control (1969) yaklaşımı, denetimli optimizasyon yöntemini tanımlamış ve daha sonra geliştirilen geri yayılım (backpropagation) algoritmasının

kuramsal temelini oluřturmuřtur. Bu geliřme, derin sinir aęlarının eęitilebilirlięini mmkn kılan dnm noktalarından biri olarak deęerlendirilmektedir (Dreyfus, 1990: 2).

#### **2.2.4.3 Mantıksal akıl yrtme ve uzman sistemler**

YZ'nin geliřiminde mantıksal akıl yrtme sistemleri, bilgiye dayalı karar verme srelerinin temelini oluřturmuřtur. Bu yaklařımın ilk rneklerinden biri, nceki blmde ele alınan Newell ve Simon'un Logic Theorist sistemidir. 1970'li yıllarda bu geleneęi srdren alıřmalar, insan uzmanlıęını belirli grev alanlarında taklit etmeyi amalayan “uzman sistemler” kavramını geliřtirmiřtir.

Bu dnemde ne ıkan rneklerden biri, MYCIN adlı sistemdir. 1972 yılında geliřtirilen bu kural tabanlı yapı, bakteriyel enfeksiyonların tanısında olasılıksal ıkarım tekniklerini kullanarak nerilerde bulunmuřtur (Copeland, t.y.; Uzun, 2020: 82). Bu sistem, karar destek srelerinde bilgi tabanlı ıkarımın etkinlięini gstererek YZ'nin saęlık alanındaki ilk uygulamalarına nclk etmiřtir.

#### **2.2.4.4 Olasılıksal akıl yrtme**

1980'li yıllara gelindięinde, YZ arařtırmalarında belirsizlik altında karar verme ve ıkarım yapma konuları nem kazanmaya bařlamıřtır. Judea Pearl, 1988 tarihli Probabilistic Reasoning in Intelligent Systems adlı alıřmasında Bayes aęlarını tanımlayarak olasılıksal akıl yrtmenin kuramsal temellerini geliřtirmiřtir (Cinicioęlu vd., 2015: 226). Bu yaklařım, bilgilerin kesin kurallara deęil, olasılıksal iliřkiler zerine inřa edildięi yeni bir model sunmuřtur. Bylece YZ sistemlerinin karmařık, eksik ya da belirsiz verilere raęmen makul sonular retebilmesi mmkn hle gelmiřtir.

#### **2.2.4.5 Derin ęrenme atılımları**

1980'lerin sonlarında sinir aęlarının derin katmanlarla geniřletilmesi, YZ'nin yeniden ivme kazanmasını saęlamıřtır. Yann LeCun, 1989 yılında el yazısı posta kodlarını tanıyabilen bir konvolsyonel sinir aęı (CNN) modeli geliřtirmiřtir (Lecun vd., 2023: 14). Bu alıřma, grsel verilerde rnt tanımanın bařarısını gstererek derin ęrenme alanındaki ilk nemli uygulamalardan biri olmuřtur.

Derin ęrenme yaklařımları, veriden doęrudan zellik ıkarımı yapabilen ok katmanlı yapılar sayesinde, insan mdahalesine daha az ihtiya duyan esnek modellerin geliřmesine olanak tanı mıřtır. Bu dnem, YZ'nin hem teorik hem de pratik olarak modern biimini kazandıęı bir dnřm srecini temsil etmektedir.

Bu gelişim çizgisi, YZ'nin kural tabanlı sistemlerden veri odaklı öğrenme sistemlerine evrilmesini göstermektedir. Makine öğrenimi, sinir ağları ve olasılıksal modellerin bütünleşmesiyle, YZ sistemleri artık yalnızca bilgi depolayan değil, aynı zamanda deneyimden öğrenen yapılar hâline gelmiştir. Bu dönüşüm, günümüz YZ uygulamalarında görülen özerklik, esneklik ve uyarlanabilirlik gibi temel özelliklerin altyapısını oluşturmuştur.

### **2.2.5 Otonom ve fiziksel robotlar**

Bu başlıkta, YZ araştırmalarında zekanın fiziksel dünyayla bütünleştiği aşamayı ele almaktadır. Bu bütünleşme, algı–planlama–eylem döngüsünün gerçek dünyada işlerlik kazanmasıyla ilgilidir. Endüstriyel robot kolları, mobil sistemler ve otonom araçlar, hesaplamayı fiziksel harekete dönüştürerek YZ'nin gözlemlenebilir çıktılar üretmesini sağlamaktadır. Bu süreçte, insanla paylaşılan ortamlarda güvenilirlik, emniyet ve etik ilkeler teknik gereksinimlere dönüşmüştür.

#### **2.2.5.1 Uzaktan kumanda ve erken otomatlar**

Otonom sistemlerin temeli, 19. yüzyılın sonlarında geliştirilen uzaktan kumanda mekanizmaları ve erken otomatlara dayanmaktadır. Nikola Tesla, 1898 yılında Madison Square Garden'daki gösterisinde “telautomat” adını verdiği radyo kontrollü botunu tanıtarak kablosuz kumanda fikrini ortaya koymuştur (Teslauniverse, 2023; K. M. Thompson, 2015). Leonardo Torres y Quevedo, 1914 yılında geliştirdiği satranç otomatında belirli mat pozisyonlarını otonom biçimde oynatarak oyun tabanlı karar algoritmalarının öncülerinden biri olmuştur (Quevedo, t.y.). Karel Čapek, 1921 tarihli R.U.R. adlı oyunuyla “robot” terimini popülerleştirmiş ve otomasyonun toplumsal-etik yönlerine dikkat çekmiştir (Britannica, 2025b). 1925'te Houdina Radio Control, New York'taki sürücüsüz otomobil gösterisiyle kent trafiğinde radyo kontrollü araç fikrinin uygulanabilirliğini kanıtlamıştır (Engelking, 2017; Özarpa vd., 2021: 3). Fritz Lang'ın Metropolis (1927) filmi sinemadaki ilk insansı robot örneğini sunarken, Makoto Nishimura'nın Gakutensoku (1928) adlı robotu insan benzeri mimikleriyle Asya'da insan–robot etkileşimine öncülük etmiştir (Frumer, 2020; Harbou ve Lang, 1927).

#### **2.2.5.2 Endüstriyel ve mobil otomasyon**

YZ'nin fiziksel dünyaya aktarımında 1960'lardan itibaren endüstriyel ve mobil otomasyon belirgin bir gelişim göstermiştir. Unimate, 1961 yılında General Motors üretim hattında kaynak ve taşıma görevleriyle kullanılan ilk endüstriyel robot olarak seri üretimde otomasyonun başlangıcını temsil etmiştir (Gasparetto ve Scalera, 2019). Shakey, 1966 yılında geliştirilen sensör-planlama bütünleşik mimarisiyle çevresini algılayarak bağımsız hareket edebilen ilk

“düşünen robot” olarak tanımlanmıştır (Computerhistory, t.y.-b). Stanford Cart, 1979’da Hans Moravec tarafından geliştirilen bilgisayar görüşü tabanlı yapısıyla engelleri aşabilen otonom hareket kabiliyeti sergilemiş ve otonom sürüş araştırmalarına yön vermiştir (Nilsson, 2009: 231). Bu dönem, YZ’nin hareket, algı ve planlama bileşenlerinin fiziksel sistemlerde birleşmeye başladığı dönüm noktasını oluşturmuştur.

### **2.2.5.3 İnsansı ve sosyal robotlar**

1980’lerden itibaren insansı ve sosyal robotlar, insan hareketlerini ve iletişim biçimlerini taklit edebilme yetenekleriyle YZ’nin yeni bir araştırma alanı hâline gelmiştir. WABOT-2, 1980 yılında nota okuyup müzik çalabilen ilk insansı robot olarak insan-robot koordinasyonuna dair erken bir örnek sunmuştur (Sugano ve Kato, 1987; Waseda, t.y.) Honda ASIMO, 2000 yılında yürüyüş stabilitesi, jest uyumu ve denge sistemleriyle insansı robotikte teknik bir dönüm noktası oluşturmuştur (Ng-Thow-Hing vd., 2008: 779-780). Aynı dönemde Cynthia Breazeal tarafından geliştirilen Kismet, duyguları tanıyan ve uygun yüz ifadeleriyle yanıt verebilen ilk robotlardan biri olmuş, sosyal YZ araştırmalarına ivme kazandırmıştır (Breazeal vd., 2001: 445). Bu gelişmeler, robotların yalnızca mekanik görevleri değil, aynı zamanda insana özgü sosyal etkileşim biçimlerini de simüle edebildiğini göstermektedir.

### **2.2.5.4 Sürücüsüz araçlar ve otonom sistemler**

Görsel algı ve kontrol mekanizmalarının birleşimi, sürücüsüz araç teknolojilerinin gelişiminde önemli bir aşama oluşturmuştur. Ernst Dickmanns, 1986’da geliştirdiği 4-D dinamik modelleme yöntemiyle modern otonom sürüş algoritmalarının temelini atmıştır (Dickmanns, 1997: 1577-1581). DARPA Grand Challenge, 2004 yılında düzenlenen yarışma ile akademi, savunma sanayii ve özel sektör arasında iş birliğini güçlendirmiştir. İlk denemede parkuru tamamlayan bir araç çıkmamasına rağmen yarışma, otonom sistem araştırmalarında uluslararası bir inovasyon ekosistemi oluşturmuştur (DARPA, 2014).

### **2.2.5.5 Ev robotları ve ticari yayılım**

2000’li yıllarda robot teknolojileri endüstriyel laboratuvarlardan gündelik yaşama taşınmıştır. iRobot Roomba, 2002 yılında piyasaya sürülen ilk geniş kullanıcı kitlesine ulaşan robot süpürge olarak kabul edilmiştir (İrobot, 2002). Bu gelişme, YZ’nin günlük yaşamın bir parçası hâline gelmesinin sembolü olmuştur. Ev robotları, YZ’nin yalnızca endüstriyel üretim ya da araştırma alanlarında değil, bireysel kullanımda da işlevsel hâle gelebileceğini göstermiştir.

Otonom ve fiziksel robotların gelişimi, YZ'nin yalnızca bilişsel süreçlerle sınırlı kalmadığını, aynı zamanda bedensel bir zekâ biçimi kazandığını göstermektedir. Bu süreç, hesaplamanın eyleme dönüştüğü bir dönüm noktasını temsil etmektedir. Robotik teknolojiler, üretimden ulaşım, sağlıktan ev yaşamına kadar geniş bir yelpazede uygulanabilir hâle gelmiş; böylece YZ'nin insan merkezli teknolojik ekosistemle etkileşimi daha görünür hâle gelmiştir.

## **2.2.6 Doğal dil anlama ve insan etkileşimi**

Bu bölüm, makinelerin insan diliyle kurduğu ilişkinin tarihsel gelişimini ve bu sürecin günümüz YZ sistemlerine etkisini ele almaktadır. Anahtar sözcük tabanlı ilk sohbet programlarından büyük dil modellerine (LLM) uzanan bu ilerleyiş, dili yalnızca bir “girdi” değil, aynı zamanda etkileşim ve bilgiye erişim aracı olarak konumlandırmıştır. Bu dönüşümle birlikte YZ, gündelik yaşamda daha görünür hale gelmiş; kullanım yaygınlaştıkça açıklanabilirlik, güven ve etik beklentiler de artmıştır.

### **2.2.6.1 Erken sohbet programları**

YZ'nin doğal dil alanındaki ilk uygulamaları, kullanıcılarla sınırlı düzeyde etkileşim kurabilen sohbet programları üzerinden şekillenmiştir.

Joseph Weizenbaum tarafından geliştirilen ELIZA (1966), anahtar sözcük eşlemesi ve şablon temelli yanıt üretimi yöntemiyle ilk diyalog deneyimlerinden birini sunmuş ve doğal dil işleme çalışmalarında önemli bir başlangıç noktası olmuştur (Weizenbaum, 1983: 1).

Daha sonraki yıllarda, Rollo Carpenter'ın Jabberwacky (1988) sistemi, kullanıcı etkileşimlerinden “öğrenerek” yanıt kalitesini geliştirmiştir (Xue vd., 2023: 4). Bu yaklaşım, dilin yalnızca tanıma değil, öğrenme sürecine de dâhil edilmesi açısından yenilikçi bir adım olarak görülmektedir.

1995 yılında Richard Wallace tarafından geliştirilen A.L.I.C.E., AIML dilini tanıtarak açık kaynak sohbetbot ekosistemini başlatmış ve Loebner Ödülleri aracılığıyla Turing Testi tartışmalarını yeniden gündeme taşımıştır (Wallace, 2009: 1-15).

### **2.2.6.2 Gelişmiş dil işleme ve bilgi erişimi**

YZ'nin bilgiye erişim kapasitesi, 2011 yılında IBM Watson'ın Jeopardy! yarışmasında elde ettiği başarıyla önemli bir görünürlük kazanmıştır. Watson'ın doğal dil işleme ve geniş veri tabanlarını eşzamanlı analiz etme becerisi, YZ'nin yalnızca metin yorumlayan değil, bağlamsal anlam kurabilen bir sistem haline geldiğini göstermiştir (Lenchner, 2014: 1).



Bu gelişme, dil anlama sistemlerinin yalnızca bilgi çekme değil, anlam çıkarımı yapabilme yönünde evrildiğine işaret etmektedir.

#### **2.2.6.3 Büyük dil modelleri (LLM)**

2020’li yıllar, dil modellemesinde ölçeklenebilir derin öğrenme yaklaşımlarının ön plana çıktığı bir dönemi temsil etmektedir. OpenAI tarafından geliştirilen GPT-3 (2020), 175 milyar parametresiyle few-shot öğrenme yeteneğini kullanarak çok sayıda doğal dil işleme görevinde insan benzeri çıktılar üretmiştir (Brown vd., 2020: 4-6).

Bunu takiben Google’ın PaLM modeli (2022), çok dilli ve yüksek kapasiteli yapısıyla karmaşık dil ilişkilerini daha isabetli biçimde kavrama potansiyeli göstermiştir (Chowdhery vd., 2022: 1-4).

Bu dönemde modellerin ölçeklenmesi, dilin istatistiksel örüntülerinin ötesinde anlamsal ilişkileri öğrenebilme kapasitesini artırmıştır.

#### **2.2.6.4 Diyalogsal YZ ve kitlelere ulaşım**

Doğal dil işleme sistemleri, 2020’lerin ortasından itibaren kullanıcıyla çift yönlü etkileşimi temel alan diyalogsal YZ biçiminde yaygınlaşmıştır. OpenAI ChatGPT (2022), doğal, bağlamsal ve akıcı sohbet yeteneğiyle kısa sürede geniş bir kullanıcı kitlesine ulaşmış; iki ay içinde 100 milyon kullanıcıya erişerek tarihteki en hızlı benimsenen teknolojilerden biri olmuştur (Hu, 2023). Aynı yıl DeepMind tarafından geliştirilen Gato, metin, görüntü ve oyun verilerini tek modelde bütünleştirerek çok görevli yapay zekâ sistemlerine yönelik yeni bir yönelim başlatmıştır (Deepmind, 2022).

Bu gelişmeler, YZ’nin yalnızca bilgiye erişim değil, öğrenme, çıkarım ve çok-modlu etkileşim alanlarında da insan benzeri kapasitelere yaklaşmakta olduğunu göstermektedir.

#### **2.2.6.5 Sesli asistanlar ve akıllı cihazlar**

Sesli asistanlar, YZ’nin gündelik yaşama yerleşmesinde önemli bir rol oynamıştır. Amazon Echo ve Alexa (2014), sesli komutlar aracılığıyla akıllı ev ekosistemine giriş yaparak kullanıcıyla doğrudan etkileşimi mümkün kılmıştır (Gao vd., 2018: 1). Bunu izleyen Apple HomePod (2017) ve Siri entegrasyonu, sesli etkileşimi oda akustiğiyle birleştirerek kullanıcı deneyimini daha doğal hale getirmiştir (Apple, 2017; Foxx, 2017).

Bu sistemler, YZ’nin fiziksel çevreyle etkileşimini somutlaştırarak insan-makine iletişimini gündelik pratiklerin parçası haline getirmiştir.

Doğal dil anlama ve insan-YZ etkileşimi, 1960’lardan günümüze kadar istikrarlı bir gelişim göstermiştir. ELIZA ile başlayan anahtar sözcük tabanlı yanıt üretiminden, günümüzün milyarlarca parametrelili büyük dil modellerine kadar uzanan süreç, dilin yapay zekâ sistemlerindeki rolünü kökten dönüştürmüştür.

Bu evrim, dili yalnızca komut-girdi aracı olmaktan çıkarıp, bilgiye erişim, öğrenme ve toplumsal etkileşim için merkezi bir bileşen haline getirmiştir.

Sonuç olarak, doğal dil işleme teknolojilerinin ilerleyişiyle birlikte, yapay zekânın insanla kurduğu ilişkinin gelecekte daha açıklanabilir, güvenilir ve etik temellere dayalı biçimde şekilleneceği öngörülmektedir.

### **2.2.7 YZ’nin toplumsal yansımaları, etik tartışmalar ve “YZ Kışları”**

Bu başlık, YZ teknolojilerinin teknik ilerlemesinin toplumsal meşruiyet, etik sorumluluk ve beklenti yönetimiyle nasıl karşılıklı etkileşim içinde geliştiğini incelemektedir. YZ tarihindeki “hype döngüleri” ve bu döngüleri izleyen “YZ kışları”, teknolojiye ilişkin toplumsal beklentilerin ve güven krizlerinin somut göstergeleri olarak değerlendirilmektedir. Bu durum, kanıt ile iddia arasındaki dengenin, açıklanabilirlik ve şeffaflığın sürdürülebilir ilerleme için temel koşullar olduğunu göstermektedir. Günümüzde teknik ilerlemenin yanı sıra, hak ve güvenlik dengesini birlikte yönetebilmek, YZ’nin etik gelişimi açısından temel bir gereklilik olarak öne çıkmaktadır.

#### **2.2.7.1 Erken eleştirel yaklaşımlar**

YZ’ye yönelik eleştirel düşüncenin temelleri, modern teknolojik dönemin öncesine uzanmaktadır. Jonathan Swift, *Gulliver’s Travels* (1726) adlı eserinde, Laputa adasında tasvir ettiği “yararsız icatlar” aracılığıyla teknolojik ilerlemenin toplumsal ve etik bedellerine dair ilk hicivlerden birini ortaya koymuştur (Swift, 2006).

Karel Čapek, *R.U.R.* (1921) adlı tiyatro eserinde “robot” terimini popülerleştirerek makine emeğinin insanlık üzerindeki potansiyel etkilerini tartışmaya açmıştır (Britannica, 2025b). Benzer biçimde, Fritz Lang’ın *Metropolis* (1927) filmi, insansı robot “Maria” figürü üzerinden sınıf çatışması, yabancılaşma ve otomasyon korkularını sinematik bir dille yansıtmıştır (Harbou ve Lang, 1927). Bu örnekler, teknolojik ilerlemenin yalnızca teknik değil, aynı zamanda kültürel ve etik sonuçlar doğurduğuna işaret etmektedir.

#### **2.2.7.2 “YZ Kışları” ve Gerçekçi beklentiler**

YZ tarihindeki “kış” dönemleri, teknolojinin abartılı beklentilerle yüklendiği dönemlerin ardından gelen durgunluk evrelerini tanımlamaktadır. İlk önemli örnek, 1973 yılında İngiliz Parlamentosu’na sunulan Lighthill Raporu’dur. Raporda, YZ araştırmalarının “abartılı vaatler” içerdiği öne sürülmüş ve bu eleştiriler kamu fonlarının kesilmesine yol açmıştır. Bu durum, literatürde “ilk YZ kışı” olarak anılmaktadır (Hendler, 2008: 2).

Benzer biçimde, 1984 yılında düzenlenen AAAI Paneli “The Dark Ages of AI”, aşırı iyimserliğin araştırma finansmanını olumsuz etkileyebileceğini vurgulamış; bu değerlendirme, 1980’lerin ortasında yaşanan ikinci YZ kışının entelektüel öncüsü olarak kabul edilmiştir (McDermott, 1985: 122-124).

Bu dönemler, beklentinin gerçekçi temellere oturtulmadığında, teknolojik ilerlemenin toplumsal güven ve kaynak sürekliliği açısından kırılma hale geldiğini göstermektedir.

#### **2.2.7.3 Teknolojik tekilik ve gelecek kaygıları**

YZ’nin geleceğine ilişkin tartışmalar, 1990’lı yıllardan itibaren “teknolojik tekilik” kavramı etrafında yoğunlaşmıştır. Vernor Vinge, 1993 tarihli “The Coming Technological Singularity” adlı makalesinde, teknolojik gelişmenin ivmelenerek insanüstü zekaya sahip varlıkların ortaya çıkmasına yol açabileceğini ileri sürmüştür. Vinge, bu olasılığın insanlık açısından öngörülemez ve kontrol edilmesi güç sonuçlar doğurabileceğini belirtmiştir (Vinge, 1993).

Bu görüş, YZ’nin yalnızca teknik değil, aynı zamanda varoluşsal ve etik bir mesele olarak değerlendirilmesi gerektiğini gündeme taşımış ve uzun vadeli güvenlik tartışmalarının önünü açmıştır.

#### **2.2.7.4 Etik ve güvenli YZ gelişimi**

YZ etiği alanındaki tartışmalar, teknolojinin insan davranışlarını nasıl etkilediğine ve bu etkileşimin sınırlarının nasıl çizileceğine odaklanmaktadır. Joseph Weizenbaum’un ELIZA (1966) deneyinde, kullanıcıların basit bir anahtar sözcük eşleştirme sistemini “empatik danışman” olarak algılaması, makinelere insani nitelikler atfetmenin doğurabileceği risklere dair erken bir uyarı olarak görülmüştür (Weizenbaum, 1983: 1).

Daha yakın dönemde, OpenAI’nin 2015 yılında kurulmasıyla “insanlığa faydalı, güvenli ve etik yapay genel zeka” geliştirme hedefi kurumsal bir çerçeveye oturtulmuştur (OpenAI, 2015). Bu gelişmeler, etik sorumluluk, insan denetimi ve toplumsal fayda ilkelerinin, YZ araştırmalarının sürdürülebilirliğinde belirleyici faktörler haline geldiğini göstermektedir.

YZ'nin tarihsel ilerleyişi, teknik kapasitenin ötesinde toplumsal, kültürel ve etik dinamiklerle şekillenmiştir. Erken dönem eleştirilerden YZ kışlarına, teknolojik tekillik tartışmalarından günümüz etik yönetim arayışlarına kadar uzanan bu süreç, YZ'nin yalnızca bilimsel değil, aynı zamanda insani bir mesele olduğunu ortaya koymaktadır. Dolayısıyla, gelecekte sürdürülebilir YZ gelişimi için teknik ilerlemenin hak, güvenlik ve etik sorumluluk ilkeleriyle dengeli biçimde yürütülmesi gerekmektedir.

### **2.3 YZ Sistemlerinin ve Uygulamalarının Amacı**

Bir önceki başlıklarda ele alınan tarihsel gelişimden hareketle, YZ araştırmalarının temel amacı, algılama, örüntü tanıma, akıl yürütme ve karar verme gibi karmaşık bilişsel süreçleri otomatikleştirerek, insanların yürüttüğü görevleri makineler aracılığıyla daha hızlı, tutarlı ve hatasız biçimde gerçekleştirmektir (Mehak vd., 2023: 20-30; Öztemel, 2020: 99-102).

Bu yönüyle YZ, bilgisayar tabanlı etmenlerin karmaşık sorunları insan benzeri, hatta bazı durumlarda insan performansını aşan bir düzeyde çözebilmesini hedeflemektedir. Böylece insan müdahalesi azaltılırken, başarı oranının artırılması amaçlanmaktadır (Suryawanshi ve Singh, 2024: 654).

Operasyonel düzeyde YZ sistemleri, emek yoğun veya yüksek risk içeren görevleri otonom algoritmalarla devrederek maliyet, hata ve süreyi azaltmayı öngörmektedir. Aynı zamanda, 7/24 kesintisiz hizmet sağlayarak üretkenliği ve güvenliği artırma potansiyeli taşımaktadır (Prorok, 2022: 77-86). Gerçek zamanlı büyük veri işleme kapasitesine sahip uyarlanabilir modeller, insan hız sınırlarının ötesine geçerek karar verme süreçlerini hızlandırmakta ve veriye dayalı içgörü üretimini yeni bir ölçeğe taşımaktadır (Mehak vd., 2023: 20-30).

Bilimsel açıdan bakıldığında, YZ araştırmalarının amacı; insan, hayvan ve yapay etmenlerde zeki davranışı mümkün kılan ilkeleri ortaya koymak ve bu ilkelerden hareketle bilgi temsili, muhakeme ve insan-bilgisayar etkileşimini kolaylaştıran sistemler geliştirmektir. Mühendislik düzeyinde ise bu anlayış, insan ve makinenin tamamlayıcı güçlerini birleştirerek karar kalitesini ve üretkenliği artıran “akıllı ajan” sistemlerinin tasarımına yön vermektedir (Tecuci, 2012: 168-169).

Kamusal alanda YZ, “akıllı hükümet” vizyonunun merkezinde yer almakta ve karar destek mekanizmaları aracılığıyla şeffaflığı, birlikte çalışabilirliği ve yolsuzlukla mücadeleyi güçlendirmektedir. Ayrıca çevresel değişimlerin izlenmesi, afetlere hızlı müdahale edilmesi ve vatandaşlara kişiselleştirilmiş hizmetlerin sunulması gibi işlevleri ölçeklenebilir biçimde desteklemektedir (Valle-Cruz ve Sandoval-Almazan, 2018, ss. 1-2).

Bununla birlikte, dijital dönüşümün itici gücü olarak YZ'nin sanayi, hizmet ve kamu sektörlerinde verimliliği artırarak toplumsal refahı genişletebileceği öngörülmektedir (Öztemel, 2020: 99-102).

Sonuç olarak, YZ'nin temel amacı kuramsal düzeyde zekâ olgusunu anlamak, pratik düzeyde ise bu kavrayışı bilgiye dayalı, uyarlanabilir ve karmaşık problemlere çözüm üretebilen sistemlere dönüştürmektir. Bu dönüşüm sayesinde endüstriyel süreçlerin verimliliği artmakta, toplumsal yaşam kolaylaşmakta ve karar verme süreçleri daha sağlam bir bilgi temeli üzerine inşa edilmektedir.

## **2.4 YZ'nin Öğrenme Metotları**

YZ alanında yaşanan hızlı ilerlemenin temelinde, farklı öğrenme yöntemlerinin geliştirilmesi ve uygulanması bulunmaktadır. Çalışmamızın bu başlığında, günümüz YZ sistemlerinin temelini oluşturan denetimli öğrenme, denetimsiz öğrenme, yarı denetimli öğrenme, pekiştirmeli öğrenme, derin öğrenme ve transfer öğrenme gibi başlıca metodolojiler tanıtılmakta; her bir yaklaşımın genel işleyişi, uygulama alanları ve sunduğu avantajlar açıklanmaktadır.

Bu öğrenme yöntemleri, karmaşık veri yapılarını anlamlandırma, karar süreçlerini optimize etme ve önceki deneyimlerden edinilen bilgileri yeni görevlerde kullanma açısından kritik bir öneme sahiptir. Söz konusu yaklaşımların incelenmesi, yalnızca YZ sistemlerinin performansını artırmakla kalmamakta; aynı zamanda alanın gelecekteki yönelimlerinin belirlenmesine de katkı sağlamaktadır.

### **2.4.1 Denetimli öğrenme**

Denetimli öğrenme, makine öğrenmesinin temel yöntemlerinden biridir ve etiketli veri kümeleri üzerinde çalışmaktadır. Bu yöntemde, her veri örneği hem giriş özniteliklerini ( $x_1, x_2, \dots, x_n$ ) hem de bu girdilere karşılık gelen doğru etiketi ( $y$ ) içerir (Turan ve Polat, 2024: 93). Model, eğitim sürecinde bu etiketli örneklerden öğrenir ve ardından daha önce görmediği veriler üzerindeki etiketleri tahmin ederek performansını değerlendirir (Özkul ve Aydın, 2015: 38). Bu süreç, modelin genelleme yeteneğini güçlendirir ve sistemin yeni örneklerde güvenilir tahminler üretebilmesini sağlar. Denetimli öğrenme, sınıflandırma ve regresyon gibi farklı görevlerde kullanılmaktadır (Alasu ve Talu, 2024: 1137).

Sonuç olarak, denetimli öğrenme, etiketli veriden öğrenilen kalıplar aracılığıyla bilinmeyen örneklerle yönelik yüksek doğrulukta öngörüler yapmayı amaçlamakta ve hem akademik

arařtırmalarda hem de endüstriyel uygulamalarda temel bir yöntem olarak önemini korumaktadır.

#### **2.4.2 Denetimsiz öğrenme**

Denetimsiz öğrenme, önceden tanımlı bir çıktı veya sınıf etiketi olmaksızın verideki yapısal ilişkileri keřfetmeyi amaçlayan bir yaklaşımdır. Bu yöntem, verileri benzerlik ölçütlerine göre gruplandırarak kümeleme algoritmaları ve veri içindeki örüntüleri ortaya çıkaran boyut indirgeme teknikleriyle çalışmaktadır (Özkul ve Aydın, 2015: 38). Model, etiketsiz veri üzerinde insan müdahalesine gerek kalmadan, verideki doğal düzenlilikleri keřfederek öğrenme sürecini sürdürür (Croitoru vd., 2019: 1299-1300).

Sinir ağı perspektifinden bakıldığında, denetimsiz öğrenme, girdilerdeki istatistiksel örüntüleri doğru etiketler olmadan keřfetmekte ve temsil kalitesini artırmayı hedeflemektedir (Becker, 1991: 17-18). Bu tür ağlar, veriyi katmanlı biçimde temsil ederek kendiliğinden kodlama (self-encoding) yeteneği kazanır. Böylece, görevden bağımsız şekilde bilgi çıkarımı yapabilir ve ölçeklenebilir öğrenme kapasitesi geliřtirebilir.

Denetimsiz öğrenmenin iki temel avantajı öne çıkmaktadır: İlki, büyük veri ortamlarında etiketleme maliyetini ortadan kaldırması; ikincisi ise modellerin genelleřtirilebilir temsil uzayları oluřturmasına olanak tanımasıdır (Croitoru vd., 2019; Özkul ve Aydın, 2015). Bu nedenlerle, denetimsiz öğrenme çağdař YZ sistemlerinin vazgeçilmez bileřenlerinden biri haline gelmiřtir.

#### **2.4.3 Yarı-Denetimli öğrenme**

Yarı-denetimli öğrenme (YDÖ), az sayıdaki etiketli veriyi çok daha geniř bir etiketsiz veri kümesiyle birlikte kullanarak öğrenme sürecini zenginleřtiren bir yaklaşımdır. Bu yöntem, denetimli öğrenmenin yönlendirici gücüyle, verinin doğal yapısında gizli bulunan istatistiksel düzenlilikleri bir araya getirir (Gökalp, 2022: 8). Bu sayede, sınırlı sayıda “etiket–hedef” eřleřmesinden elde edilen bilgi, geniř veri uzayına genelleřtirilerek modelin temsil gücü artırılmakta ve etiketleme maliyeti önemli ölçüde azalmaktadır (Turan ve Polat, 2024b: 93).

Kuramsal düzlemde YDÖ, denetimli ve denetimsiz öğrenme paradigmalarının kesiřim noktasında yer almaktadır. Etiketli örnekler, karar sınırlarını belirlemek için doğrudan yönlendirici bir sinyal saęlarken; etiketsiz örnekler, bu sınırların veri manifolduna uyumlu biçimde geniřletilmesini kolaylařtırır (Van Engelen ve Hoos, 2020: 373-375). Bu bütünleřik yaklaşım, her iki veri kaynağındaki bilgiyi ortak bir temsil uzayında birleřtirerek sınıflandırma performansını yükseltmeyi hedefler (Gökalp, 2022; Turan ve Polat, 2024b).

Sonuç olarak, yarı-denetimli öğrenme, yüksek etiketleme maliyetlerinin azaltılmasına katkı sunarken, aynı zamanda genelleme yeteneğini güçlendiren dengeli bir öğrenme stratejisi olarak değerlendirilmektedir.

#### **2.4.4 Pekiştirmeli öğrenme**

Pekiştirmeli öğrenme (PÖ), bir etmenin (agent) çevresiyle etkileşime girerek aldığı geri bildirimlerden (ödül veya ceza) hareketle karar politikasını geliştirdiği bir makine öğrenmesi yöntemidir (Aksu ve Karaköse, 2022: 484). Etmen, her durumda olası eylemlerden birini seçer; çevre, bu eyleme karşılık yeni bir durum ve sayısal bir ödül sinyali üretir. Etmen, bu sinyalleri kullanarak gelecekteki eylem seçimlerini iyileştirir (İmamoğlu vd., 2009: 1-2).

Bu süreçte etmen, “doğru cevap” veya etiketli veri olmadan, yalnızca aldığı ödülleri maksimize etmeyi hedefleyen bir strateji geliştirir. Denetimli öğrenmeden farklı olarak doğrudan doğruya bir hedef çıktıya değil, uzun vadeli ödül toplamına odaklanır. Denetimsiz yaklaşımlardan ayrıldığı nokta ise öğrenme sürecinin amaca yönelik geri bildirimlerle yönlendirilmesidir (Aksu ve Karaköse, 2022: 484).

Dolayısıyla PÖ, uzun vadeli ödül birikimini azami kılacak bir politika geliştirmeyi amaçlayan, adaptif ve deneyime dayalı bir öğrenme biçimi olarak öne çıkmaktadır (İmamoğlu vd., 2009; Öztürk vd., 2022).

#### **2.4.5 Derin öğrenme**

Derin öğrenme (DÖ), ham veriden çok katmanlı yapılar aracılığıyla hiyerarşik temsiller çıkaran bir makine öğrenmesi yaklaşımıdır. Bu mimari, metin, görüntü ve ses gibi yüksek boyutlu verilerde, geleneksel yöntemlere göre daha yüksek doğruluk oranları elde etmektedir (Janiesch vd., 2021: 685-687). Her katmanda uygulanan doğrusal olmayan işlemlerle, bir önceki çıktının girdi olarak kullanılması, verinin giderek soyutlaşan çok katmanlı temsillerinin öğrenilmesini sağlar (Şeker vd., 2017: 48). Bu özellik, derin ağların hem denetimli hem de denetimsiz görevlerde esnek biçimde uygulanabilmesine olanak tanır. Ayrıca, gürültülü ve belirsiz sinyallerin anlamlı yapılara dönüştürülmesi sayesinde, derin öğrenme YZ’yi gerçek dünya problemlerine bağlayan işlevsel bir köprü işlevi görmektedir (Sejnowski, 2020: 3033-3035).

Beynin katmanlı işlem biçiminden esinlenen bu modeller, sınırlı etiketli veriyle birlikte geniş etiketsiz veri yığınlarından da öğrenme yapabilmektedir. Bu nedenle gözlem, analiz ve karar döngüsünü taklit eden veri-yoğun uygulamalarda yaygın biçimde tercih edilmektedir (Akın ve Şahin, 2024: 27).

#### 2.4.6 Transfer öğrenme

Transfer öğrenme (TÖ), bir görevde veya veri alanında edinilen bilginin, benzer ancak tam olarak örtüşmeyen bir başka göreve aktarılmasını sağlayan bir yaklaşımdır (Pan ve Yang, 2010: 1346). Bu yöntem, önceden eğitilmiş modellerin parametrelerini veya özellik uzaylarını yeni bir görevde yeniden kullanarak, öğrenme süresini kısaltır ve doğruluğu artırır. Ayrıca, sınırlı etiketli veri koşullarında bile etkili performans sergileme potansiyeline sahiptir (Islam, 2024: 1-2; Zhuang vd., 2021: 2).

Kuramsal olarak transfer öğrenme üç temel ekseninde incelenmektedir:

- Özellik tabanlı transfer, kaynak ve hedef verilerin ortak veya dönüştürülmüş bir temsilde hizalanmasını sağlar;
- Parametre tabanlı transfer, kaynak modelin ağırlıklarının hedef modelde dondurularak veya ince ayarlanarak (fine-tuning) kullanılmasını içerir;
- Örnek tabanlı transfer ise kaynak verinin belirli alt kümelerinin hedef eğitim sürecine yeniden dahil edilmesine dayanır (Pan ve Yang, 2010: 1346).

Bu stratejiler, bilgisayarla görme, doğal dil işleme ve tıbbi görüntü analizi gibi birçok alanda başarıyla uygulanmaktadır. Bununla birlikte, negatif transfer olarak bilinen ve kaynak–hedef farkının aşırı büyük olması nedeniyle performansı düşüren durumlar da göz önünde bulundurulmalıdır. Bu nedenle, modelin alan uyumluluğunu ölçmek ve aktarımın yarar-maliyet dengesini değerlendirmek için uygun doğrulama protokollerinin geliştirilmesi önem taşımaktadır (Islam, 2024: 1-2). TÖ, sınırlı veri ortamlarında hızlı prototipleme ve maliyet etkin model geliştirme için esnek ve ölçeklenebilir bir çerçeve sunmakta, modern YZ sistemlerinde derin öğrenmenin başarısında önemli bir rol oynamaktadır.

YZ'nin öğrenme yöntemleri bütüncül bir biçimde değerlendirildiğinde, YZ sistemlerinin verimliliğini, genelleme kapasitesini ve uyarlanabilirliğini artırmakta; insan benzeri bilişsel işlevleri taklit edebilen, çevresel değişimlere tepki verebilen daha gelişmiş YZ mimarilerinin geliştirilmesine katkı sunmaktadır.

#### 2.5 Yapay Zekanın Önemi

Araştırmalar, YZ'nin yeni yetenekler kazandırmasının yanı sıra mevcut imkanları daha fazla aktör için ulaşılabilir kılarak askeri, ekonomik ve zihinsel güç dengesini değiştirdiğini göstermektedir. YZ'nin özellikle robotik ve otonom sistemlerde sunduğu ölçeklenebilirlik, ticari sektörlerdeki teknolojik yeniliklerle birleşerek, askeri kapasitenin yalnızca üst düzey kurumlarda değil, daha geniş bir operasyonel tabanda da uygulanabilir hale gelmesini



kolaylaştırmaktadır (Allen ve Chan, 2017: 1-3). Bu eğilimi destekleyen biçimde, ABD Ulusal Güvenlik Ajansı ve Siber Komutanlığı Direktörü Oramiral Michael Rogers, YZ ve makine öğrenmesinin siber güvenliğin “temel bileşeni” olacağını vurgulamış; “Bu bir ‘eğer’ meselesi değil, yalnızca ‘ne zaman’ meselesi” sözleriyle, teknolojinin ulusal güvenlik yapılarında yüksek düzeyde ve kaçınılmaz biçimde benimseneceğini açıkça ifade etmiştir (Allen ve Chan, 2017: 18).

Benzer biçimde, Çin Devlet Konseyi 20 Temmuz 2017 tarihinde yayımladığı “Yeni Nesil Yapay Zekâ Gelişim Planı”nda, YZ’yi “uluslararası rekabetin yeni odak noktası” olarak tanımlamış ve bu teknolojiyi geleceğin stratejik liderliğini belirleyecek temel bir güç kaynağı olarak konumlandırmıştır (Webster vd., 2017a). Aynı dönemde Rusya Devlet Başkanı Vladimir Putin’in “Bu alanda lider olan, dünyanın hâkimi olacaktır.” sözü, YZ liderliğinin küresel güç dengelerini doğrudan etkileyen belirleyici bir unsur haline geldiğini göstermektedir (Press, 2017).

ABD Başkanı Donald Trump da farklı dönemlerde yaptığı konuşmalarda ve yayımladığı başkanlık emirlerinde, “Yapay zeka alanında Amerikan liderliğinin sürdürülmesi, ülkenin ekonomik refahı ve ulusal güvenliği açısından büyük önem taşımaktadır.” ifadeleriyle, YZ’nin yalnızca ekonomik büyüme aracı değil, aynı zamanda güvenlik politikalarının stratejik çekirdeği olduğunu vurgulamıştır (OSTP, 2019).

Michael C. Horowitz (2018), devletlerin YZ geliştirme konusunda hızla rekabete girdiğini ve bu teknolojinin uluslararası güç dengesini dönüştürecek ölçüde yapısal bir etki yarattığını belirtmektedir. Horowitz’e göre YZ, tekil bir mühimmat değil, birçok sektörün dönüşümünü mümkün kılan genel amaçlı bir “kolaylaştırıcı teknoloji”dir; tıpkı elektriğin geçmişte üretim, ulaşım ve iletişim alanlarını dönüştürmesi gibi, YZ de mevcut sanayilerin modernleşmesini hızlandırmakta ve yeni endüstrilerin doğuşunu teşvik eden temel bir itici güç işlevi görmektedir (Horowitz, 2018: 40-55).

YZ’nin dönüştürücü potansiyeli yalnızca ulusal stratejilerde değil, uluslararası kuruluşların politika belgelerinde de güçlü biçimde vurgulanmaktadır. NATO, 2021 yılında kabul ettiği Yapay Zeka Stratejisi’nde, YZ’yi hem geleneksel askeri kabiliyetleri hem de hibrit tehdit alanlarını etkileyen kesişen bir teknoloji olarak tanımlamıştır. Zoe Stanley-Lockman ve Edward Hunter Christie’nin NATO personeliyle yaptıkları görüşmelerde strateji şu şekilde özetlenmiştir: “YZ, hem geleneksel askeri yetenekleri hem de hibrit tehdit alanlarını etkileyen geniş bir uluslararası güvenlik yelpazesi oluşturmakta, aynı zamanda bu tehditlere karşı yeni fırsatlar yaratmaktadır.” NATO’nun “Bu temel teknolojiyle ilişkili vaatler ve riskler, herhangi

bir aktörün tek başına yönetemeyeceği kadar büyüktür.” değerlendirmesi, YZ’ye atfedilen stratejik önemin kapsamını ve çok taraflı yönetim gerekliliğini açık biçimde göstermektedir (Stanley-Lockman ve Christie, 2021).

Bu değerlendirmeler bir arada ele alındığında, ülkelerin YZ teknolojisini yalnızca teknolojik bir yenilik değil, aynı zamanda stratejik bir güvenlik önceliği olarak konumlandıkları görülmektedir. Aşağıda yer alan belgeler, bu küresel stratejik yönelimin zaman çizelgesini özetlemektedir:

- ABD: National Artificial Intelligence Research and Development Strategic Plan – Ekim 2016 (NSTC, 2016).
- Japonya: Artificial Intelligence Technology Strategy – 31 Mart 2017 (Strategic Council for AI Technology, 2017).
- Çin: A New Generation Artificial Intelligence Development Plan – Temmuz 2017 (Webster vd., 2017a).
- Hindistan: National Strategy for Artificial Intelligence (AIForAll) – Haziran 2018 (NITI Aayog, 2018).
- Güney Kore: National Strategy for Artificial Intelligence – 17 Aralık 2019 (MSIT, 2019a).
- Türkiye: Ulusal Yapay Zekâ Stratejisi (2021–2025) – 20 Ağustos 2021 tarihli Resmî Gazete Genelgesi; kamuoyu lansmanı 24 Ağustos 2021 (STB ve CBDDO, 2021).

### **3. TÜRKİYE’DE YAPAY ZEKA VE İÇ GÜVENLİK ETKİLEŞİMİNİN DEĞERLENDİRİLMESİ**

Bu bölüm, 1950’lerden günümüze YZ’nin iç güvenlik alanına entegrasyon sürecini küresel ölçekte özetlemeyi ve temel gelişim aşamalarını ortaya koymayı amaçlamaktadır. ARPANET’in ortaya çıkışı, otonom sistemlerin ilerleyişi, siber savunma kapasitesinin artışı, yüz tanıma teknolojileri ve etik-hukuki tartışmalar bu sürecin başlıca dönüm noktalarını oluşturmaktadır.

Çalışmada, ABD, Çin, Hindistan, Güney Kore ve Japonya örnekleri üzerinden ulusal YZ politikalarının iç güvenlik uygulamalarına yansımaları değerlendirilmektedir. Ardından Türkiye’nin UYZS (2021–2025), Kişisel Verilerin Korunması Kanunu (KVKK), kalkınma planları, Dijital Dönüşüm Ofisi (DDO) düzenlemeleri, YZ kanun girişimleri ve Siber Güvenlik Kanunu gibi yasal ve idari çerçeveler incelenmektedir.

Bölüm ayrıca, iç güvenliği doğrudan etkileyen strateji ve programları ele alarak Ulusal Siber Güvenlik Stratejisi (USGS), Türkiye Siber Güvenlik Kümelenmesi (TSGK) ve Savunma Sanayii Bakanlığı (SSB) stratejik planlarındaki yönelimleri açıklamayı hedeflemektedir. Son olarak, İçişleri Bakanlığı birimlerinde kullanılan gözetim, biyometrik tanıma, video analitiği, plaka tanıma, öngörüşel analitik, siber güvenlik ve göç yönetimi sistemleri incelenmektedir.

Bu yapı, yapay zekâ uygulamalarının güçlü yönleri ile politika ve uygulama arasındaki boşlukları görünür kılarak, karar vericiler için dengeli ve bütüncül bir değerlendirme zemini oluşturmayı amaçlamaktadır.

#### **3.1 YZ ve İç Güvenlik**

İç güvenlik (anavatan güvenliği) kavramı, genel olarak bir devletin kendi sınırları içindeki topraklarını terörizm, doğal afetler ve diğer acil durumlar gibi tehditlerden koruma çabalarını ifade etmektedir. Amerika Birleşik Devletleri örneğinde bu kavram, “sivil savunma, acil durum yönetimi, kolluk kuvvetleri, gümrük, sınır devriyesi ve göç gibi geleneksel kamu görevleri ile gelişen tehditlerin kesişim alanı” olarak tanımlanmıştır (Kahan, 2013: 6).

ABD İç Güvenlik Bakanlığı tarafından gerçekleştirilen Dört Yıllık İç Güvenlik İncelemesi sonucunda, iç güvenliğin yalnızca terörle mücadeleyle sınırlı olmadığı; bunun yanı sıra siber tehditler, doğal afetler ve sivil nüfusu etkileyen tüm tehlikeleri kapsayan geniş bir güvenlik anlayışını ifade ettiği belirtilmiştir (Kahan, 2013: 6). Bu bağlamda, iç güvenlik kavramı tehdit

türleri arasında bütüncül bir yaklaşımı benimsemekte ve devletin krizlere karşı direncini artırmayı hedeflemektedir.

“İç güvenlik” terimi, ulusal güvenliğin alt bir alanı olarak ilk kez Şubat 2001’de yayımlanan “21. Yüzyılda ABD Ulusal Güvenliğı Hakkındaki Ulusal Komisyon Raporu”nda, özellikle terörle mücadele çerçevesinde kullanılmıştır. Ancak kavramın kurumsal düzeyde yaygınlık kazanması, 11 Eylül 2001 terör saldırılarının ardından gerçekleşmiştir. Bu tarihten sonra, ABD’de yurt içi tehditlerle mücadele “iç güvenlik yönetimi” başlığı altında yeniden yapılandırılmış ve bu süreç, iç güvenlik politikalarının kurumsal temellerinin atıldığı dönem olarak kabul edilmiştir (Yılmaz, 2012: 20).

Tarihsel olarak ABD dış politika belgelerinde iç savunma; siyasi, diplomatik, ekonomik ve askerî araçların yanı sıra sivil polis, paramiliter güçler ve karşı-ayaklanma operasyonlarını da kapsayan, iç istikrarı korumaya yönelik bütüncül bir stratejik eylem programı olarak tanımlanmıştır (FRUS, 1962). Bu yaklaşıma göre iç savunma, devletin kamu düzenini ve toplumsal istikrarını iç kaynaklı tehditlere karşı koruma hedefini taşımaktadır. Bu tehditler arasında iç terörizm, organize suç yapıları ve toplumsal huzursuzluklar yer almaktadır. Dolayısıyla iç savunma, sivil nüfusun ve kritik altyapıların korunmasına odaklanan iç güvenlik politikalarını tamamlayıcı bir işlev üstlenmektedir.

Türkiye’de iç güvenlik, ülke sınırları içinde kamu düzeninin sağlanması, vatandaşların can ve mal güvenliğinin korunması ve toplumsal huzurun sürdürülmesi amacına yönelik faaliyetlerin bütünüdür. Bu kapsamda suçların önlenmesi, kamu asayişinin sağlanması, terörle mücadele, trafik güvenliği ve benzeri alanlardaki uygulamalar iç güvenlik hizmetlerinin temel bileşenlerini oluşturmaktadır.

Türkiye’deki iç güvenlik yapılanması, tarihsel olarak Osmanlı İmparatorluğu’nun son dönemlerinde gerçekleştirilen idari reformlar ile kurumsallaşmaya başlamış, Cumhuriyet dönemiyle birlikte modern bir yapıya kavuşmuştur. Bu süreçte iç güvenlikle sorumlu üç ana kurumun temelleri atılmıştır:

1839 yılında Jandarma Teşkilatı, 1845 yılında Polis Teşkilatı kurulmuş; bu iki kuruma 1982 yılında teşkilat yapısına dahil edilen Sahil Güvenlik Komutanlığı eklenmiştir (Aydın ve Özel, 2016: 46).

Türkiye’de iç güvenlik hizmetlerinin yürütülmesi İçişleri Bakanlığı’nın yetki ve sorumluluğundadır. Bakanlık, bu hizmetleri Emniyet Genel Müdürlüğü, Jandarma Genel Komutanlığı ve Sahil Güvenlik Komutanlığı gibi bağlı kuruluşlar aracılığıyla yerine

getirmektedir (İçişleri Bakanlığı, t.y.). Ayrıca, il düzeyinde valiler, ilçe düzeyinde ise kaymakamlar, mülki idare amirleri olarak iç güvenlik faaliyetlerinin yerel düzeyde koordinasyonundan sorumlu merciler olarak görev yapmaktadır (Aydın ve Özel, 2016: 46).

### **3.2 YZ'nin İç Güvenlik Alanına Entegrasyonunun Tarihçesi**

YZ teknolojilerinin iç güvenlik alanına entegrasyonu, tarihsel olarak hem kurumsal hem de operasyonel düzeyde önemli bir dönüşüm sürecini temsil etmektedir. Erken dönem araştırmalardan başlayarak 2010'lu yıllarda yaygınlaşan uygulamalar ve günümüzde tartışılan etik–hukuki boyutlar, YZ'nin güvenlik politikalarının şekillenmesinde belirleyici bir rol üstlendiğini göstermektedir. Bu tarihsel ilerleyiş, teknolojinin yalnızca savunma kapasitesini değil, aynı zamanda iç güvenlikte karar döngülerini hızlandırma, gözetim kapasitesini artırma ve operasyonel etkinliği dönüştürme potansiyelini de açıkça ortaya koymaktadır.

#### **3.2.1 Araştırma ekosisteminin doğuşu ve kurumsal temeller**

1950'li ve 1960'lı yıllar, YZ'nin iç güvenlik alanına yön verecek teknolojik temellerin atıldığı dönem olmuştur. 1957'de Sovyetler Birliği'nin Sputnik uydusunu fırlatmasının ardından, ABD Savunma Bakanlığı teknolojik üstünlüğünü yeniden tesis etmek amacıyla ARPA (daha sonra DARPA) adlı kurumu kurmuştur (DARPA, t.y.). Bu kurum, doğal dil işleme ve ilkel robotik projelerine yaptığı erken yatırımlarla savunma sistemlerinde yapay zekânın kullanım potansiyelini araştırmış, böylece bilimsel araştırma ile güvenlik politikası arasında yeni bir bağ kurmuştur.

Buna paralel olarak Stanford Araştırma Enstitüsü'nde geliştirilen Shakey the Robot (1966–1972) projesi, sensör verilerini kullanarak bağımsız hareket edebilen ilk otonom sistemlerden biri olarak öne çıkmıştır (Abby, 2021; Keay ve Silicon Valley Robotics, 2017). Shakey, çevresel algı ve hareket kabiliyeti sayesinde gelecekte iç güvenlikte devriye ve keşif gibi görevlerin otomatikleştirilmesine öncülük etmiştir.

Aynı dönemde ARPANET Projesi (1969), araştırma kurumları arasında veri paylaşımını mümkün kılarak YZ araştırmalarında ağ tabanlı iş birliğinin zeminini oluşturmuştur (Leiner vd., 2009: 22-27). Dolayısıyla bu dönemdeki girişimler, yalnızca savunma teknolojilerinin ilerlemesine değil, YZ'nin karar destek, simülasyon ve gözetim sistemlerine entegre edilmesine de yön vermiştir.

### 3.2.2 Otonom sistemler ve operasyonel uygulamalar

2000’li yılların sonlarına doğru YZ, araştırma aşamasından operasyonel uygulamalara geçmiştir. Bu dönemde Güney Kore, Samsung SGR-A1 adlı robotik nöbetçi sistemini Askerden Arındırılmış Bölge (DMZ) içinde konuşlandırmış ve insan müdahalesi olmaksızın sınır güvenliği sağlamıştır (NBC NEWS, 2014; The Telegraph, 2010). Bu sistem, otonom hedef tespiti ve angajman kabiliyetiyle YZ’nin sınır gözetiminde kullanılabileceğini göstermiştir (Velez-Green, 2015).

Bununla birlikte, Santa Cruz Polis Departmanı (2011), suç tahmin algoritmalarına dayalı öngörülü polislik (PredPol) uygulamasını devreye almıştır (K. Thompson, 2011). Artan nüfus ve sabit kalan personel sayısı karşısında kaynakların daha etkin kullanılmasını amaçlayan bu sistem, suç yoğunluklarını tahmin ederek devriye planlamasını optimize etmiştir (Friend, 2013; Mohler vd., 2011: 1-15)

Ancak etik kaygılar nedeniyle Santa Cruz 2017’de uygulamayı sonlandırmış, buna karşın New York Polisi benzer algoritmalarla programı sürdürmüştür (Levine vd., 2017: 4-13).

### 3.2.3 Biyometrik gözetim ve etik gerilimler

YZ’nin iç güvenliğe etkisinin belirginleştiği bu dönemde, biyometrik tanıma ve gözetim teknolojileri öne çıkmıştır. FBI Yeni Nesil Kimlik Belirleme (NGI) Sistemi (2014), yüz tanıma algoritmalarıyla ulusal düzeyde kimlik tespiti yapılmasına olanak sağlamış, kolluk kuvvetlerinin operasyonel kabiliyetini genişletmiştir (FBI, 2014). Ancak belirli gruplarda hata oranlarının yüksekliği, mahremiyet ve tarafsızlık konularında tartışmaları beraberinde getirmiştir (Bedoya, 2017: 3-16).

Benzer biçimde, Çin’in SKYNET Programı (2017) milyonlarca CCTV kamerasına YZ destekli yüz tanıma sistemleriyle entegre etmiş ve kamu güvenliği izleme kapasitesini artırmıştır (Goyal, 2017). Bu gelişme, kitlesel gözetimin etkinliğini artırırken bireysel özgürlüklerin sınırlandırılması endişelerini de güçlendirmiştir.

Daha sonraki yıllarda, Clearview AI (2020) vakası, sosyal medya platformlarından izinsiz biçimde milyarlarca görüntü toplayarak kolluk kuvvetlerine yüz tanıma yazılımı sunulmasının, etik yönetim ve yasal çerçeve gerekliliğini ortaya koymuştur (Hill, 2020). Böylece biyometrik teknolojilerin kontrolsüz kullanımı, bireysel mahremiyet ve kamu güvenliği arasında yeni bir denge arayışını gündeme getirmiştir.

### 3.2.4 Ulusal stratejiler ve jeopolitik rekabet

2010’lu yılların sonuna gelindiğinde YZ, devletlerin iç güvenlik stratejilerinin merkezine yerleşmiştir. Çin’in Yeni Nesil Yapay Zekâ Gelişim Planı (2017), 2030 yılına kadar küresel liderliği hedefleyen üç aşamalı bir yol haritası belirlemiştir (Armutlu, 2024; Esen, 2024). Bu strateji, yalnızca ekonomik kalkınmayı değil, otonom sistemler, dronlar ve siber savunma teknolojileri aracılığıyla ulusal güvenliğin yeniden yapılandırılmasını da içermektedir.

ABD’de ise Project Maven (2018) tartışmaları ve San Francisco’nun 2019 yüz tanıma yasağı (D. Lee, 2019), demokratik denetim ile teknolojik yenilik arasındaki hassas dengeyi gündeme taşımıştır. Google çalışanlarının protestolarıyla sonlanan Project Maven süreci (PBS News, 2018; Shane ve Wakabayashi, 2018; Wakabayashi ve Shane, 2018), kamu–özel sektör iş birliğinde etik ilkelerin belirleyici rolünü öne çıkarmıştır.

### 3.2.5 Uluslararası normlar ve sorumlu YZ

2020’li yıllarda, YZ’nin güvenlik uygulamalarına ilişkin etik standartların geliştirilmesinin uluslararası gündemde öncelik kazandığı görülmektedir. 2023’te Lahey’de düzenlenen Küresel Askerî Alanda Sorumlu Yapay Zekâ Zirvesi (REAIM), yaklaşık 60 ülkenin katılımıyla gerçekleştirilmiş ve bağlayıcı nitelikte olmayan bir “Eylem Çağrısı” metni kamuoyuna sunulmuştur (REAIM, 2023: 1-2).

Zirve sonunda yayımlanan “Eylem Çağrısı” bildirgesinde, insan kontrolünün korunması, otomasyon yanlılığının azaltılması ve hesap verebilirliğin güçlendirilmesi gibi ilkelerin vurgulandığı anlaşılmaktadır. Bildirgenin hukuken bağlayıcı olmamasıyla birlikte, bu ilkelerin ileride oluşabilecek uluslararası norm tartışmalarına katkı sağlayabileceği değerlendirilmektedir.

YZ’nin iç güvenlik alanına entegrasyonu, araştırma altyapılarından başlayarak otonom sistemlere, biyometrik gözetim teknolojilerine, ulusal stratejilere ve uluslararası etik girişimlere uzanan çok katmanlı bir dönüşümü yansıtmaktadır. Bu süreç, yalnızca teknolojik ilerlemeyi değil, aynı zamanda yönetim, hukuk ve etik arasındaki ilişkinin yeniden tanımlanması gerekliliğini de ortaya koymaktadır. Zaman içinde YZ, karar döngülerini hızlandıran, veri analizini derinleştiren ve operasyonel verimliliği artıran bir araç olarak iç güvenlik kurumlarında giderek daha fazla benimsenmiştir. Bununla birlikte, teknolojinin yaygınlaşması önyargı, mahremiyet, hesap verebilirlik ve insan denetimi gibi konuların önemini artırmış; güvenlik hedefleriyle temel hak ve özgürlükler arasındaki dengenin dikkatle korunması gerektiğini göstermiştir. Bu bağlamda, iç güvenlikte sürdürülebilir ilerleme, yalnızca teknik

kapasitenin artırılmasıyla değil, aynı zamanda şeffaf, çok paydaşlı ve sorumlu bir yönetim anlayışının güçlendirilmesiyle mümkün görünmektedir.

### **3.3 Seçilmiş Ülkelerin Güncel Yapay Zeka Politikaları**

YZ teknolojilerinin 21. yüzyılda iç güvenlik stratejilerinde yarattığı dönüşümler, etik ve toplumsal sorumluluk tartışmalarıyla birlikte küresel ölçekte farklı yaklaşımların ortaya çıkmasına neden olmuştur. Ülkeler, sahip oldukları ekonomik kapasite, kurumsal yapı ve teknolojik olgunluk düzeyine göre bu sürece özgün yönlerden katkıda bulunmaktadır. ABD ve Çin, yüksek Ar-Ge yatırımları ve sivil-askerî “ikiz kullanım” ekosistemleriyle küresel ölçekte yön belirleyici iki aktör konumundadır. Ancak iki ülkenin politika yaklaşımı arasında önemli bir fark göze çarpar; ABD piyasa temelli ve çok paydaşlı bir standartlaşma sürecini benimserken, Çin devlet merkezli yönlendirmeye hız ve ölçek üretmektedir. Japonya ve Güney Kore, kalite güvencesi, sertifikasyon ve standartlaştırma kültürleriyle uygulama öncesi test süreçlerine ve uygunluk değerlendirmelerine kurumsal değer kazandıran modeller sunmaktadır. Hindistan ise geniş nüfusu, dijital kamu hizmetleri ve düşük maliyetli altyapı çözümleriyle ölçeklenebilir ve erişilebilir YZ uygulamalarının incelenmesine olanak tanımaktadır. Bu ülkelerin izlediği güncel politikalar, YZ’nin iç güvenlik alanında etik, hukuki ve yönetim boyutlarının anlaşılması için karşılaştırmalı bir çerçeve oluşturmakta; Türkiye açısından da ulusal politikaların geliştirilmesinde dikkate alınabilecek örnekler sunmaktadır.

#### **3.3.1 Amerika Birleşik Devletleri**

Amerika Birleşik Devletleri’nin YZ politikası, bütüncül bir federal yasa modelinden ziyade, yürütme organı öncülüğünde geliştirilen risk temelli standartlar, mevcut sektör mevzuatının genişletilmesi ve stratejik Ar-Ge yatırımlarının bir arada yürütülmesine dayanmaktadır. 30 Ekim 2023 tarihli 14110 sayılı Başkanlık Kararnamesi, YZ sistemlerinin güvenli, emniyetli ve ayrımcılıktan uzak biçimde geliştirilmesini sağlamak amacıyla neredeyse tüm federal kurumlara görevler yüklemiş; gelişmiş modeller için güvenlik testi, hassas verilerin korunması ve iş gücü etkilerinin izlenmesi gibi düzenlemeler getirmiştir (Executive Office of the President, 2023a). 20 Ocak 2025’te göreve gelen yeni yönetim ise 23 Ocak 2025 tarihli 14179 sayılı Kararname ile önceki düzenlemelerde “yenilik önünde engel” oluşturabilecek hükümlerin gözden geçirilmesini ve gerektiğinde askıya alınmasını istemiş, böylece piyasa dinamikleriyle daha uyumlu bir yaklaşımı benimsemiştir (The White House, 2025a). Bu doğrultuda federal politika, güvenlik odaklı ilkeler ile rekabetçiliği önceleyen esneklik arayışı arasında dengeli bir yönelim izlemektedir.



ABD'nin YZ stratejisinin temel bileşenlerinden biri, büyük ölçekli finansman ve altyapı yatırımlarıdır. CHIPS and Science Act (P.L. 117-167, 2022) kapsamında yarı iletken üretimi ve ilgili Ar-Ge çalışmaları için 52,7 milyar dolar kaynak ayrılmış, bu yolla ileri YZ donanım ekosisteminin ülke içinde kalması hedeflenmiştir (Reuters, 2025c; Tim, 2022). Ulusal YZ Girişimi Yasası (2020) ile kurulan Ulusal YZ Girişimi Ofisi, NSF, DARPA ve diğer ajansların projelerini koordine etmekte; bütçe destekleri aracılığıyla yeni YZ araştırma enstitüleri, sivil-askerî ortak projeler ve açık inovasyon konsorsiyumlarına kaynak sağlamaktadır. Ayrıca yönetim, Çin'e yönelik ileri seviye GPU ihracat kısıtlamalarını sürdürerek, YZ tedarik zincirinin jeostratejik boyutunu politika gündeminin bir parçası hâline getirmiştir (Reuters, 2025c).

ABD'nin genel YZ politikası, federal düzeyde bağlayıcı bir "AI Kanunu" bulunmamasına rağmen, yeniliği destekleme ve kamu yararını koruma hedeflerini bir arada gözetten çok katmanlı bir yönetim yapısı sunmaktadır.

### 3.3.2 Çin Halk Cumhuriyeti

Çin'in YZ politikası, uzun vadeli bir devlet stratejisi ile kısa vadeli, esnek düzenleyici araçların birleşiminden oluşmaktadır. Bu yaklaşımın temelini, Çin Devlet Konseyi tarafından Temmuz 2017'de yayımlanan Yeni Nesil Yapay Zekâ Geliştirme Planı oluşturmaktadır. Söz konusu plan, Çin'i 2030 yılına kadar YZ alanında küresel yenilik merkezi konumuna taşımayı ve çekirdek YZ endüstrisinin ekonomik değerini 1 trilyon RMB düzeyine ulaştırmayı hedeflemektedir (Webster vd., 2017a). Plan, teknolojik ilerlemeleri ulusal güvenlik, sanayi modernizasyonu ve toplumsal yönetim hedefleriyle bütünleştirerek "tek elden tasarım" anlayışını stratejik bir ilke hâline getirmiştir.

Takip eden yıllarda merkezi yönetim, bu stratejiyi destekleyecek biçimde risk temelli ve hızlı tepki veren düzenleyici araçlar geliştirmiştir. 2019 tarihli YZ Yönetişim İlkeleri, "güvenli, denetlenebilir ve insana faydalı YZ" vizyonunu ortaya koyarken (CAC, 2019), 2023'te yürürlüğe giren Generatif YZ Geçici Tedbirleri, kamuya açık üretken YZ hizmetlerinde güvenlik testi ve algoritma tescili yükümlülüğü getirmiştir (CAC, 2023). Aynı dönemde yayımlanan derin sentetik medya kuralları ile Eylül 2025'te yürürlüğe girecek "AI ile Üretilmiş İçeriklerin Etiketlenmesi" düzenlemeleri, yapay araçlarla üretilen tüm metin, görsel ve ses içeriklerinin açık biçimde işaretlenmesini zorunlu kılmıştır (CAC, 2023; Reuters, 2025b).

Sanayi yönlendirmesi ve standart geliştirme süreçleri de Çin'in YZ politikasında öncelikli alanlar arasında yer almaktadır. Aralık 2024'te kurulan YZ Standardizasyon Teknik Komitesi, büyük dil modelleri ve risk değerlendirme konularında ulusal standart çalışmalarını başlatmıştır (Reuters, 2024). Finansman boyutunda ise Ocak 2025'te oluşturulan 60,1 milyar RMB tutarındaki Ulusal YZ Endüstri Yatırım Fonu, erken aşama çip üretimi ve model geliştirme projelerine kaynak sağlamayı amaçlamaktadır (Global Times, 2025).

Genel olarak Çin'in YZ politikası, yeniliği teşvik eden uzun vadeli stratejik planlamayı, hızlı ve risk temelli düzenlemelerle birleştirerek, devlet gözetimi altında küresel liderlik ve stratejik özerklik hedefleyen bütüncül bir yönetim modeli ortaya koymaktadır.

### 3.3.3 Hindistan

Hindistan'ın "Herkes için YZ (AI for All)" yaklaşımı, kalkınma önceliklerini tarım, sağlık, eğitim ve kentsel hizmetler gibi toplumsal alanlara yönlendirerek kapsayıcı bir çerçeve ortaya koymaktadır. NITI Aayog'un 2018 tarihli UYZS, YZ'yi bu sektörlerde verimliliği ve erişilebilirliği artıracak bir araç olarak konumlandırırken, "açık kaynak-açık veri-açık inovasyon" ekosistemiyle yeniliği teşvik etmeyi ve yüksek maliyetli düzenleyici engelleri asgariye indirmeyi amaçlamıştır (NITI Aayog, 2018).

Henüz kapsamlı bir YZ yasası bulunmamakla birlikte, dijital ekosistemin veri mahremiyetine dayalı altyapısının temeli 2023 tarihli Dijital Kişisel Verilerin Korunması Yasası ile atılmıştır. Aynı yıl Elektronik ve Bilgi Teknolojileri Bakanlığı (MeitY) tarafından yayımlanan AI Governance Guidelines taslak raporu, güvenlik, hesap verebilirlik ve insan merkezli tasarım ilkelerine dayanan bir yönetim çerçevesi sunarak sektöre rehberlik etmektedir (IndiaAI, 2025).

Mart 2024'te onaylanan IndiaAI Misiyonu, beş yıllık bir plan kapsamında 10.372 crore ₹ (yaklaşık 1,26 milyar ABD doları) bütçeyle desteklenmiştir. Bu kapsamda (a) 18.000'den fazla GPU'dan oluşan ulusal süper bilgi-işlem altyapısının kurulması, (b) çok dilli büyük dil modellerinin geliştirilmesi, (c) IndiaAI Veri Platformu üzerinden anonimleştirilmiş kamu verilerinin araştırmacılara açılması ve (d) bin yerli YZ girişimine tohum sermayesi desteği sağlanması planlanmıştır (Mathew, 2025; PIB Delhi, 2024).

Uluslararası düzeyde Hindistan, 2023 G20 Başkanlığı döneminde yayımlanan Yeni Delhi Bildirgesi aracılığıyla "Güvenilir YZ" ve dijital kamu altyapılarını ön plana çıkarmış; ayrıca Küresel Yapay Zekâ Ortaklığı (GPAI) zirvesine ev sahipliği yaparak çok paydaşlı yönetim alanında aktif bir liderlik üstlenmiştir (Elbashir ve Desikachari, 2025). Bunun yanı sıra, ABD

ile İleri Teknolojiler Ortaklığı (iCET) ve Quad çerçevesinde yürütülen çalışma grupları, Hindistan'ın standartlara uyumlu ve değer temelli YZ vizyonunu uluslararası iş birliğiyle güçlendirmektedir (Arslan, 2024; IndiaAI, 2023).

### **3.3.4 Güney Kore**

Güney Kore, son yıllarda YZ alanında risk temelli bir hukuki çerçeveyi ve “AI G3” ulusal vizyonunu eş zamanlı olarak yürürlüğe koymuştur. 24 Mart 2025'te onaylanan Yapay Zekânın Geliştirilmesi ve Temeli Oluşturma Temel Yasası (AI Basic Act), dört kademeli bir risk sınıflandırması öngörmekte; tüm YZ sistemleri için asgari düzeyde risk yönetimi şartı getirirken, yüksek etki, generatif ve çok büyük ölçekli modeller için ek yükümlülükler (ön sertifikasyon, kullanıcı bilgilendirmesi, model kartı, kayıt saklama vb.) tanımlamaktadır (Gesser vd., 2025; MSIT, 2024d). Yasa, geniş bir coğrafi etki alanı tanımlayarak Güney Kore pazarında faaliyet gösteren yabancı işletmelere de uygulanabileceğini belirtmekte; tam yürürlük tarihi ise 22 Ocak 2026 olarak belirlenmiştir. Paralel biçimde Bilim ve ICT Bakanlığı (MSIT), 26 Eylül 2024'te Başkan Yoon Suk-yeol başkanlığında toplanan Ulusal Yapay Zekâ Komitesi aracılığıyla yayımladığı Policy Directions for National AI Strategies belgesinde, ülkeyi “Küresel YZ Merkezi” hâline getirme hedefini açıklamıştır (MSIT, 2024b).

Düzenleyici reformların yanı sıra Güney Kore, uluslararası diplomasi alanında da etkin bir rol üstlenmiştir. 21 Mayıs 2024'te Birleşik Krallık ile ortaklaşa düzenlenen AI Seoul Summit sonunda yayımlanan Seul Bildirgesi, 27 ülke ve Avrupa Birliği'nin YZ alanında “güvenli, yenilikçi ve kapsayıcı” ortak ilkeler üzerinde mutabakata vardığını ilan etmiştir. Bu girişim, 2023 tarihli Bletchley Park AI Güvenlik Zirvesinin devamı niteliğinde olup Güney Kore'yi küresel YZ yönetiminde kolaylaştırıcı bir aktör konumuna taşımıştır (Department of Industry Science and Resources, 2025).

Sonuç olarak Güney Kore'nin YZ politikası, risk temelli AI Basic Act ile hukuki netliği; AI G3 stratejisi ile altyapı ve finansman yatırımlarını; Seul Bildirgesi aracılığıyla da çok taraflı iş birliği çerçevesini bir arada yürütmektedir. Bu bütünleşik yapı, ülkenin 2030 yılına kadar küresel ölçekte ilk üç YZ gücü arasında yer alma hedefini somut strateji ve düzenlemelerle desteklemektedir.

### **3.3.5 Japonya**

Japonya'nın YZ politikası, zaman içinde gönüllü uyum ve rehber temelli “yumuşak hukuk” yaklaşımından, ulusal düzeyde bağlayıcı bir çerçeve yasaya doğru evrilen bir yönelim göstermektedir (METI, 2024: 2). Şubat 2025'te Meclis'e sunulan “Yapay Zekâ İlgili

Teknolojilerin Araştırma, Geliştirme ve Kullanımının Teşviki Yasası Tasarısı”, Başbakanlık bünyesinde YZ Strateji Merkezi kurulmasını ve YZ Temel Planı hazırlanmasını öngörerek bu dönüşümün yasal zeminini oluşturmuştur (Tatsuno ve Takahashi, 2025).

YZ Strateji Merkezi’nin yetkilerini güvence altına alan bu düzenleme, beş yıllık YZ Temel Planı’nın düzenli güncellenmesini zorunlu kılarak politika tutarlılığı ve uzun vadeli vizyonun sürdürülebilirliğini sağlamaktadır (Ops Today, 2025). Bu çerçeve, yenilikçi teknolojilerin gelişimini desteklerken, sektör paydaşlarına risk değerlendirme, raporlama ve yönetim mekanizmalarına katılım konularında kurumsal sorumluluk yüklemektedir (Matsumoto, 2025).

Japonya, bu düzenlemelerle katı yasaklar ve cezai yaptırımlara dayalı bir model yerine, esnek fakat yasal temele dayanan bir yönetim yaklaşımını benimsemektedir (Austin, 2025). Bu strateji, yüksek etki potansiyeline sahip generatif sistemler için kamu alımları ve rehber dokümanlar aracılığıyla risk yönetimini güçlendirirken, ilerleyen süreçte yayımlanacak ikincil mevzuatlarla sektör uyumunun daha da derinleşmesine zemin hazırlamaktadır (CPDS, 2025: 1).

Sonuç olarak Japonya’nın güncel YZ politikası, inovasyonu koruyan, toplumsal güveni güçlendiren ve uyarlanabilir düzenlemeleri teşvik eden dengeli bir regülasyon modeli yönünde olgunlaşmaktadır.

### **3.4 Seçilmiş Ülkelerin İç Güvenliğine Dair Geliştirdikleri Yapay Zeka Politikaları ve Uygulamaları**

Amerika Birleşik Devletleri, Çin Halk Cumhuriyeti, Hindistan, Güney Kore ve Japonya’nın yapay zekâ alanında iç güvenliğe yönelik geliştirdikleri stratejiler bu bölümde incelenir. Her ülkenin hedefleri, kurumsal yapılanmaları ve politika öncelikleri sistematik biçimde ortaya konur. Bu inceleme, ülkeler arasındaki benzerlikleri ve farklılıkları karşılaştırmalı biçimde değerlendirerek, küresel YZ yönetişiminin genel dinamiklerine ilişkin bütüncül bir çerçeve sunar. Elde edilen bulgular, Türkiye’nin iç güvenlik alanında YZ tabanlı çözümlere yönelik politikalarının geliştirilmesi için karşılaştırmalı bir referans niteliği taşır.

#### **3.4.1 Amerika Birleşik Devletleri’nin YZ uygulamaları ve sistemleri**

ABD, YZ politikasını federal düzeyde koordinasyon, kaynak seferberliği ve stratejik önceliklerle şekillendirmiştir. 2019 yılında yürürlüğe giren 13859 sayılı Başkanlık Kararnamesi ile başlatılan Amerikan Yapay Zekâ Girişimi, ülkenin ekonomik ve ulusal güvenlik kapasitesini güçlendirmeyi amaçlamış, araştırma-geliştirme faaliyetleri, iş gücü dönüşümü ve uluslararası iş birliği alanlarını kapsayan bütüncül bir politika çerçevesi sunmuştur (Executive Office of the

President, 2019). Aynı dönemde Savunma Bakanlığı, bu stratejiyle uyumlu biçimde yayımladığı Yapay Zekâ Strateji Belgesi ile YZ'yi modernizasyonun temel unsuru olarak konumlandırmış, 2018'de kurulan Ortak Yapay Zekâ Merkezi (Joint Artificial Intelligence Center – JAIC) aracılığıyla savunma ve istihbarat projelerini koordine etmeye başlamıştır (DoD, 2018).

Bu dönemde yayımlanan 13960 sayılı Başkanlık Kararnamesi, federal kurumların yapay zekâ araçlarını güvenli, tarafsız ve şeffaf biçimde kullanmasını zorunlu kılmış, etik yönetişimin politika düzeyine taşınmasını sağlamıştır (Executive Office of the President, 2020). Savunma Bakanlığı 2020 yılında YZ'ye dair beş temel etik ilkeyi (sorumlu, hakkaniyetli, izlenebilir, güvenilir ve yönetilebilir) kabul ederek, bu teknolojilerin savaş ve barış dönemlerinde insan kontrolüne tabi biçimde kullanılmasını güvence altına almıştır (Lopez, 2020). Bu yaklaşım, YZ uygulamalarında hesap verebilirliğin kurumsal kültür haline getirilmesi açısından dönüm noktası olmuştur.

YZ'ye yönelik politikalar, 2021 yılında Ulusal Güvenlik Komisyonu'nun (NSCAI) yayımladığı raporla stratejik bir yön kazanmıştır. Raporda, ABD'nin YZ çağında hazırlıksız olduğu vurgulanmış, rekabet üstünlüğünü sürdürmek için araştırma, test altyapısı ve yetkinlik gelişimine kapsamlı yatırım yapılması önerilmiştir. Bu doğrultuda, federal bütçede yapay zekâ projelerine ayrılan kaynaklar artırılmış, Savunma Bakanlığı'nın yenilikçi projeleri hızlandırılmıştır (Brookings Institution, 2021, ss. 2-13). Böylece YZ, hem ulusal güvenlik hem de savunma stratejisinin merkezinde konumlanmıştır.

Biden yönetimi döneminde bu stratejik çerçeve büyük ölçüde korunmuş, ancak "sorumlu inovasyon" ilkesi ön plana çıkarılmıştır. Beyaz Saray Bilim ve Teknoloji Politikası Ofisi'nin 2022 yılında yayımladığı Yapay Zekâ Haklar Bildirgesi Taslağı, bireysel hakların ve mahremiyetin korunmasını teşvik etmiş, federal düzeyde etik standartlara yön vermiştir (The White House, 2022). Aynı dönemde Savunma Bakanlığı, Sorumlu Yapay Zekâ Stratejisi ve Uygulama Planı ile sistem testleri, kullanıcı eğitimi ve risk azaltma mekanizmalarını zorunlu hale getirmiştir. Bu süreçte, Pentagon'un dijital modernizasyon çabalarını bütünleştirmek amacıyla Baş Dijital ve Yapay Zekâ Ofisi (CDAO) kurulmuş ve veri temelli karar alma süreçlerinin koordinasyonu güçlendirilmiştir (CDAO, 2022).

Etik yönetişim çerçevesi, Ocak 2023'te güncellenen 3000.09 sayılı Savunma Bakanlığı Direktifi ile daha da güçlendirilmiştir. Belge, otonom silahların yalnızca insan muhakemesi altında kullanılabileceğini açıkça belirtmiş, yüksek riskli sistemlerin devreye alınmadan önce üst düzey inceleme süreçlerinden geçmesini zorunlu kılmıştır (Garamone, 2023). Bu yaklaşım,

ölümcül otonomi sistemlerinin insan kontrolünden tamamen bağımsız biçimde çalışmasını yasaklayan bir güvenlik standardı ortaya koymuştur.

2023 yılının sonlarında imzalanan 14110 sayılı Güvenli, Emniyetli ve Güvenilir Yapay Zekâ kararnamesi, ticari ve ulusal güvenlik uygulamalarında güvenlik, şeffaflık ve hesap verebilirlik ilkelerini merkezine almıştır (Executive Office of the President, 2023b). Bu çerçevede Beyaz Saray, 2024 yılında yayımladığı Ulusal Güvenlik Sistemlerinde Yapay Zekâ Kullanımına Dair Memorandum (NSM) ile savunma ve istihbarat kurumlarında “sorumlu hız” yaklaşımını benimsemiştir. Bu belge, ulusal güvenliğin teknolojik yenilikle birlikte etik sorumluluk temelinde sağlanabileceğini vurgulamıştır (Covington, 2024).

Aynı dönemde Yönetim ve Bütçe Ofisi (OMB) tarafından yayımlanan M-24-10 Memorandumu, federal kurumlar için YZ risk yönetimi, veri güvenliği ve tedarik ilkelerini belirlemiş, kamuda güvenilir YZ çözümlerinin tercih edilmesini teşvik etmiştir (Dori vd., 2024). Böylece federal yönetim modeli hem etik hem rekabetçi hedefleri eş zamanlı gözetin esnek bir yapıya kavuşmuştur.

2025 yılında 14179 sayılı “Yapay Zekâ Alanında Amerikan Liderliğinin Önündeki Engelleri Kaldırmak” başlıklı kararname yürürlüğe girmiştir. Bu düzenleme, önceki kısıtlayıcı hükümlerin gözden geçirilmesini ve yenilik önündeki bürokratik engellerin azaltılmasını öngörmüştür (The White House, 2025b). Kararnamenin uygulama süreci, özel sektör, akademi ve kamu arasında daha dinamik bir danışma yapısının kurulmasına zemin hazırlamış, ancak politika sürekliliği ve hesap verebilirlik açısından yeni risk alanları da yaratmıştır (Executive Office of the President, 2025).

Tüm bu gelişmeler, ABD’nin yapay zekâ politikalarının yalnızca teknolojik yenilikleri hızlandırmakla kalmadığını, aynı zamanda etik ilkelere dayalı bir yönetim anlayışını da kurumsallaştırdığını göstermektedir. Savunma Bakanlığı Müsteşarı Sasha Baker’ın da belirttiği üzere, Amerika Birleşik Devletleri on yılı aşkın süredir YZ ve otonominin sorumlu askerî kullanımında küresel bir referans noktası hâline gelmiştir (Vergun, 2023). ABD modeli, teknolojik rekabet gücünü korurken insan merkezli denetim, hesap verebilirlik ve uluslararası normlara uyum arasında denge kurmayı hedefleyen çok katmanlı bir politika yapısı ortaya koymaktadır.

### 3.4.1.1 ABD'nin sınır güvenliği için YZ uygulamaları

ABD'nin sınır güvenliği, özellikle Meksika ile güney sınırında, son yıllarda gelişmiş teknolojilerle desteklenen çok katmanlı bir yapıya dönüşmüştür. YZ, bu süreçte hem fiziksel sınır gözetimi (otonom gözetleme kuleleri, İHA'lar, sensör ağları) hem de risk temelli analiz (otomatik hedefleme sistemleri, biyometrik tanıma, veri analitiği) alanlarında kullanılmaktadır. Bu sistemler, yasa dışı geçişleri önceden tespit etmek, göç akışlarını analiz etmek ve güvenlik tehditlerini sınıflandırmak amacıyla tasarlanmıştır.

Bu kapsamda geliştirilen Automated Targeting System (ATS), ABD Gümrük ve Sınır Koruma Birimi (CBP) tarafından yolcu, araç ve kargo hareketlerini risk temelli biçimde analiz etmek için kullanılan otomatik bir veri işleme ve karar destek sistemidir (ACLU, 2006). ATS, federal kurumlar arası veri paylaşımını esas alarak, havayolu kayıtları, sınır geçiş logları ve taşıma bilgileri gibi geniş veri kümelerini bir araya getirir. Toplanan veriler, önceden tanımlanmış risk kuralları ve izleme listeleriyle karşılaştırılır; sistem potansiyel olarak yüksek riskli kişi veya gönderileri belirleyerek ek incelemeye yönlendirir. ATS, hem kural tabanlı hem de örüntü tanıma esaslı analizler gerçekleştirebilmekte, CBP ve Ulaştırma Güvenliği İdaresi gibi kurumların operasyonel karar süreçlerinde kullanılmaktadır. Bununla birlikte, sistemin risk puanlama yöntemleri, doğruluk oranı veya yanlış alarm istatistiklerine ilişkin kamuya açık, bağımsız veya ampirik değerlendirme raporlarının sınırlı olması, şeffaflık konusundaki tartışmaları sürdürmektedir (DLP, 2022; Lewvinson-Waldman ve Gutierrez, 2023).

CBP, 2018 yılından itibaren uluslararası havalimanları başta olmak üzere çeşitli sınır geçiş noktalarında YZ destekli yüz tanıma teknolojilerini uygulamaya koymuştur (Carey, 2018). Bu sistem, yolcuların yüz biyometrik verilerini kameralar aracılığıyla kaydederek, pasaport veya vize fotoğraflarıyla otomatik biçimde eşleştirir. Gelişmiş bilgisayarlı görü ve derin öğrenme algoritmalarına dayanan bu uygulama, kimlik doğrulama süreçlerini hızlandırmış, temassız kontrolü mümkün kılmış ve sahte kimlik tespitinde etkili bir araç hâline gelmiştir. CBP verilerine göre, program kapsamında milyonlarca yüz taraması yapılmış; sistem özellikle vize süresini aşan yolcuların tespiti ve kimlik doğrulamada önemli bir rol oynamaktadır (CBP, 2020). Ancak nihai doğrulama kararı, her durumda insan görevliler tarafından verilmektedir.

Fiziksel sınır gözetiminde CBP, 2019 yılından itibaren özel sektör iş birliğiyle YZ destekli Otonom Gözetleme Kuleleri kurmaya başlamıştır. 2020'de resmi envanter programına alınan bu kuleler, güneş enerjisiyle çalışan, radar ve elektro-optik/termal kameralarla donatılmış sabit ünitelerden oluşmaktadır (Anduril, 2024). Kuleler, radarları aracılığıyla çevresindeki alanı sürekli izler ve bir hareket tespit edildiğinde Kuleler, radarları aracılığıyla çevredeki hareketi

sürekli izlemekte, tespit edilen anormalliklerde kameralar otomatik biçimde yönlendirilmektedir. Gömülü YZ algoritmaları, görüntüleri analiz ederek nesneleri insan, hayvan veya araç olarak sınıflandırır ve insan hareketlerini devriye ekiplerine gerçek zamanlı olarak bildirir (Beaumont, 2022). Bu sistem, kablo altyapısı gerektirmemesi, bağımsız enerji kaynağıyla çalışabilmesi ve taşınabilir yapısı sayesinde farklı coğrafi koşullarda esnek biçimde kullanılabilir.

CBP'nin 2023 raporlarına göre, yaklaşık 300 otonom kule aktif durumdayken, 1 Mayıs 2025 itibarıyla 564 kule ABD-Meksika sınırının belirli bölümlerinde devreye alınmıştır (Maass, 2023). Bu altyapı, sınır devriyelerinin erişimini genişletmiş ve fiziki bariyerlerin yetersiz kaldığı alanlarda sürekli gözetim kapasitesi sağlamıştır. Bununla birlikte, sistemlerin etkinliği, veri gizliliği, yanlış alarm oranları ve insan denetiminin yeterliliği konularında tartışmalar sürmektedir.

#### **3.4.1.2 Siber savunma ve tehdit tespiti için YZ**

Siber uzay, modern güvenlik anlayışında kara, deniz, hava ve uzayın ardından beşinci operasyonel alan olarak kabul edilmekte; bu bağlamda YZ, hem yeni tehdit biçimlerinin ortaya çıkmasına yol açan bir unsur hem de savunma kapasitesini güçlendiren bir çözüm olarak öne çıkmaktadır. ABD Savunma Bakanlığı (DoD) ve bağlı kuruluşlar, son yıllarda siber güvenlik altyapısında YZ ve otomasyon temelli sistemlerin entegrasyonuna öncelik vermektedir.

Bu yaklaşımın dikkat çekici örneklerinden biri, Savunma İleri Araştırma Projeleri Ajansı (DARPA) tarafından 2016'da düzenlenen Cyber Grand Challenge (CGC) yarışması olmuştur. Etkinlik, tamamen otonom sistemlerin siber güvenlik alanında insan müdahalesi olmadan rekabet ettiği ilk büyük ölçekli uygulamadır. Yarışmada finale kalan yedi takım, geliştirdikleri YZ destekli siber ajanlar aracılığıyla yazılım zafiyetlerini tespit etmiş, aynı anda kendi sistemlerindeki açıkları otomatik olarak onarmıştır (Pellerin, 2016). CGC'de kullanılan sistemler, daha önce analiz edilmemiş yazılımlarda güvenlik açıklarını belirleme, otomatik yama üretme ve istismar kanıtı oluşturma yeteneğiyle insan temelli süreçlerden çok daha yüksek bir hız ve ölçek sunmuştur. Program yöneticisi Mike Walker, insan müdahalesiyle açıkların ortalama 312 gün boyunca fark edilmeden kalabildiğini belirterek, otonom sistemlerin bu süreci dramatik biçimde kısalttığını ifade etmiştir (Szoldra, 2016). Bu yarışma, otonom siber savunma alanında makine tabanlı tekniklerin potansiyelini göstermiş ve sonraki yıllarda hem kamu kurumlarında hem de özel sektörde otomatik tehdit tespiti ve savunma sistemlerinin geliştirilmesine zemin hazırlamıştır.



ABD Siber Komutanlığı (Cybercom) ve bağılı Ordu Siber Komutanlığı (ARCYBER), DoD ağlarının ve kritik bilgi altyapılarının korunmasında YZ ve makine öğrenmesi tabanlı çözümlerin kurumsal düzeyde benimsenmesi için kapsamlı çalışmalar yürütmektedir. Cybercom'un geliştirdiği YZ yol haritası, büyük dil modelleri ve makine öğrenimi algoritmalarının yaklaşık yüz farklı operasyonel göreve entegre edilmesini öngörmekte ve bu teknolojilerin sistematik biçimde test edilmesini hedeflemektedir. Bu çerçevede Siber Ulusal Misyon Gücü (CNMF) bünyesinde kurulan AI Görev Gücü, doksanar günlük değerlendirme döngüleriyle pilot projeler yürütmekte; kullanılan YZ tabanlı araçların işlevsellik, ölçeklenebilirlik ve güvenilirlik düzeylerini analiz etmektedir (D. B. Johnson, 2025).

Bu girişimlerin öne çıkan örneklerinden biri, ARCYBER tarafından pilot olarak geliştirilen Panoptic Junction platformudur. Sistem, ağların ve dijital platformların kesintisiz biçimde izlenmesini sağlayan; tehdit istihbaratı ile olay verilerini birleştirerek potansiyel riskleri belirleyen bir YZ ve makine öğrenimi tabanlı analiz altyapısıdır. Pilot uygulama sürecinde, Panoptic Junction'ın operasyonel verimliliği artırdığı, risk tespitini hızlandırdığı ve güvenlik önerilerini gerçek zamanlı olarak üretebildiği rapor edilmiştir (Harper, 2024).

Cybercom, aynı zamanda DARPA ile yürütülen Constellation ortaklığı kapsamında, Savunma Bakanlığı Bilgi Ağı (DoDIN)'ın sürekli izlenmesi ve siber savunma kapasitesinin artırılmasına yönelik yeni YZ çözümlerinin geliştirilmesi için özel sektörle iş birliği yapmaktadır (Harper, 2024; D. B. Johnson, 2025). Panoptic Junction'ın başarılı sonuçları, sistemin DoD genelinde yaygınlaştırılması ve diğer siber savunma süreçlerine entegre edilmesi yönünde planlamaları da beraberinde getirmiştir. Bu gelişmeler, ABD'nin siber savunma stratejisinde YZ'nin yalnızca bir teknoloji bileşeni değil, bütüncül bir güvenlik paradigması olarak konumlandırıldığını göstermektedir.

#### **3.4.1.3 İç Güvenlik Analitiği ve Suç Tahmini YZ Sistemleri**

Amerika Birleşik Devletleri'nde iç güvenlik kurumları ve kolluk kuvvetleri, suçla mücadele süreçlerinde büyük veri analitiği ve YZ tabanlı araçları giderek artan ölçüde kullanmaktadır. Bu kapsamda prediktif polislik algoritmaları, sosyal medya analiz sistemleri, plaka ve yüz tanıma teknolojileri ile bütünleşik istihbarat platformları operasyonel karar süreçlerine entegre edilmiştir.

Bu dönüşümün merkezinde yer alan Palantir Technologies, iç güvenlik ve kolluk faaliyetlerinde büyük hacimli ve karmaşık veri kümelerinin yönetimi ve analizi konularında stratejik bir rol üstlenmektedir. Şirketin geliştirdiği yazılım çözümleri, farklı kurumlardan gelen dağınık veri

kaynaklarını birleştirerek anlamlı ilişki ağları kurmakta ve olaylar arasında bağlantı tespitine olanak tanımaktadır. Özellikle Uyuşturucuyla Mücadele Dairesi (DEA) ve Göçmenlik ve Gümrük Muhafaza (ICE) tarafından yürütülen Operation Fallen Hero operasyonu, bu teknolojinin somut bir örneğini oluşturur. Palantir yazılımı aracılığıyla kartel üyeleri arasındaki ağ yapıları analiz edilmiş, kilit aktörler belirlenmiş ve operasyon sonucunda yüzlerce tutuklama gerçekleştirilmiş; yüklü miktarda kokain, metamfetamin ve silah ele geçirilmiştir (Harris, 2012). Bu başarının ardından Palantir çözümleri, FBI ve DHS gibi federal kurumların yanı sıra LAPD ve NYPD gibi yerel polis teşkilatlarında da yaygın biçimde kullanılmaya başlanmıştır (Dastin, 2023; Reuters, 2020). Palantir'in sistemleri yalnızca ABD'de değil, Birleşik Krallık gibi ülkelerde de güvenlik kurumları tarafından benimsenmiştir (Everquill, 2024).

YZ'nin iç güvenlikteki bir diğer kullanım alanı, prediktif polislik (öngörüsül polislik) uygulamalarıdır. Bu yöntem, geçmiş suç verilerini analiz ederek gelecekte suç işleme olasılığı yüksek bölgeleri ve zaman aralıklarını tahmin etmeye çalışır. Bu amaçla geliştirilen en bilinen yazılımlardan biri PredPol olmuştur. Los Angeles ve Chicago gibi büyük şehirlerde pilot uygulamalarda kullanılmış, ancak etkinliği ve tarafsızlığına ilişkin önemli eleştirilerle karşılaşmıştır (Rubin, 2010). 2018'de New Jersey'nin Plainfield kentinde yapılan bağımsız bir analizde, PredPol'un 23.631 tahmininden yalnızca %0,5'inin gerçek suçlarla örtüştüğü belirlenmiştir (Sankin ve Mattu, 2023). Bu sonuçlar, algoritmanın önyargı riskleri ve doğruluk düzeyi hakkında ciddi tartışmalar doğurmuştur. Artan kamuoyu baskısının ardından PredPol, 2021 yılında adını Geolitica olarak değiştirmiştir.

2023 yılında SoundThinking, Geolitica'nın mühendislik ekibini ve belirli fikrî mülkiyet haklarını devralarak, yeni bir platform olan ResourceRouter'ı geliştirmiştir. Bu sistem, polis kaynaklarının sınırlı olduğu bölgelerde devriye görevlerini risk düzeyine göre optimize etmeye odaklanmaktadır. Suç verilerinden elde edilen analizler doğrultusunda memurların görevlendirmeleri planlanmakta ve sahadaki personele kritik bilgilerin mobil cihazlar üzerinden anlık iletimi sağlanmaktadır. Doğu Chicago Polis Departmanı örneğinde, personel sayısındaki azalmaya rağmen ResourceRouter sayesinde operasyonel verimlilik korunmuş ve sistem, birim içinde dönüştürücü bir araç olarak değerlendirilmiştir (Police1, 2025).

İç güvenlikle YZ destekli tanıma sistemleri de önemli bir yer edinmiştir. Otomatik Plaka Tanıma (ALPR) teknolojileri, araç plakalarından elde edilen verileri gerçek zamanlı olarak analiz ederek şüpheli araç ve kişilerin tespitini hızlandırmaktadır. Bu sistemler, bir aracın belirli bir suç mahalline yakınlığını konum ve zaman bilgileriyle ilişkilendirerek soruşturmaların doğruluk ve etkinliğini artırmaktadır (Garner, 2022). Geleneksel yöntemlerle günler

sürebilecek analizler, ALPR ile dakikalar içinde tamamlanabilmektedir. Ayrıca, farklı kurumların ALPR verilerini paylaşabilmesi, ajanslar arası iş birliğini güçlendirmekte ve şüpheli şahısların daha kapsamlı biçimde izlenmesini mümkün kılmaktadır (Police1, 2018; Stenquist, 2023: 4-5).

Bu bilgiler doğrultusunda, ABD’de iç güvenlik kurumları YZ teknolojilerini yalnızca operasyonel hız ve verimlilik sağlamak için değil, aynı zamanda veri temelli karar destek süreçlerini geliştirmek amacıyla da kullanmaktadır. Bununla birlikte, prediktif algoritmaların önyargı riski, veri gizliliği ve şeffaflık gibi etik boyutları, bu teknolojilerin yönetiminde sürekli bir tartışma alanı oluşturmaktadır.

### **3.4.2 Çin Halk Cumhuriyeti’nin YZ uygulamaları ve sistemleri**

Çin, YZ alanında küresel bir lider olma ve bu teknolojileri ekonomik büyüme, savunma ve iç güvenlik hedefleri doğrultusunda kullanma amacıyla kapsamlı bir politika çerçevesi uygulamaya koymuştur. Devlet Konseyi tarafından 2017 yılında yayımlanan Yeni Nesil Yapay Zekâ Gelişim Planı (NGAIDP) bu çerçevenin temel belgelerinden biridir. NGAIDP, 2020’ye kadar önde gelen YZ ülkelerini yakalamayı, 2025’e kadar teorik ve teknolojik atılımlar gerçekleştirmeyi ve 2030 yılına dek dünyanın birincil YZ inovasyon merkezi hâline gelmeyi öngörmektedir. Plan, askeri-sivil bütünleşme (MCF) yaklaşımını merkezine alarak, YZ destekli komuta-kontrol sistemleri, simülasyon ve gelişmiş silah teknolojilerinin geliştirilmesini teşvik etmektedir. 2025 yılına kadar YZ’nin akıllı üretim, akıllı şehirler ve ulusal savunma uygulamalarında yaygın biçimde kullanılması beklenmektedir. Bu yönelim, Çin’in YZ’yi hem toplumsal hem de ulusal güvenlik politikalarının merkezinde konumlandıran stratejik yaklaşımını göstermektedir (Webster vd., 2017b).

YZ ekosisteminin diğer önemli yapıtaşı, 2015 yılında başlatılan Made in China 2025 girişimidir. Bu plan, yeni nesil bilgi teknolojisi, robotik, havacılık ve askeri teçhizat gibi on stratejik sektörde yüksek teknolojlili üretimi ve inovasyonu teşvik etmektedir (Li, 2022: 105). YZ, bu sektörlerin tamamında ortak bir unsur olarak konumlanmakta; yarı iletken, sensör ve otomasyon teknolojilerindeki ilerlemelerle birlikte savunma sanayinin YZ entegrasyon kapasitesini güçlendirmektedir. Made in China 2025 ve NGAIDP birlikte, Çin’in YZ’ye yönelik üst düzey taahhüdünü kurumsallaştırarak hem ekonomik hem de askeri alanlarda teknolojik kapasitenin artırılmasını hedeflemektedir (Li, 2022; Webster vd., 2017b).

14. Beş Yıllık Plan (2021–2025), bu politikaların devamı niteliğinde olup, YZ’yi ulusal savunma ve iç güvenlik hedefleriyle bütünleşmiş biçimde ele almaktadır. Planda, YZ, kuantum bilişim ve büyük veri “geleceğin temel unsurları” olarak tanımlanmakta; Ar-Ge faaliyetlerine öncelik verilmesi gerektiği vurgulanmaktadır (Bresnick, 2024: 12). Aynı zamanda, sivil dijital dönüşüm süreçlerinin ulusal güvenlik uygulamalarıyla eşgüdümlü ilerlemesi gerektiği belirtilmekte; bu yaklaşım, “ulusal savunmanın ve silahlı kuvvetlerin modernizasyonu” hedefiyle ilişkilendirilmektedir (Bresnick, 2024: 131). Bu doğrultuda, teknolojik ilerlemeyi askeri kapasite artışıyla bağlantılandıran “zengin ülke–güçlü ordu” anlayışı güçlenmiştir.

MCF stratejisi, sivil sektörde geliştirilen yeniliklerin askeri uygulamalara aktarılmasını sağlayan iki yönlü bir teknoloji transfer mekanizması sunmakta ve yüksek verimliliğe sahip bütüncül bir entegrasyon modeli kurmayı amaçlamaktadır (Bresnick, 2024: 125-131). Plan aynı zamanda YZ çipleri gibi çekirdek teknolojilerde dışa bağımlılığı azaltmak ve “bağımsız inovasyon kapasitesi” oluşturmak hedefini öne çıkarmaktadır. Böylece Çin, dış ticaret kısıtlamalarına ve ihracat kontrollerine karşı dayanıklı bir üretim altyapısı kurarak ekonomik ve askeri özerkliği güçlendirmeye çalışmaktadır (Bresnick, 2024; Li, 2022).

Bu politikalar, Çin’in savunma ve iç güvenlik hedefleriyle doğrudan uyum içindedir. Halk Kurtuluş Ordusu (PLA)’nın stratejik doktrini, YZ’nin geleceğin askeri üstünlüğünün merkezinde yer alacağını öngören “akıllı savaş (intelligentized warfare)” kavramı etrafında şekillenmektedir. Başkan Xi yönetiminde PLA’nın 21. yüzyılın ortalarına kadar tamamen modernize edilmesi ve “dünya standartlarında” bir ordu hâline gelmesi hedeflenmiş; bu süreçte YZ, geleneksel güç dengelerini dönüştürme potansiyeli taşıyan bir araç olarak konumlandırılmıştır (Li, 2022: 105-106). 2019 tarihli Savunma Beyaz Kitabı da bu yaklaşımı destekleyerek “askeri zekânın entegre gelişimi” ilkesini vurgulamaktadır.

İç güvenlik alanında YZ, kamu düzeni ve rejim istikrarının korunmasında önemli bir rol üstlenmektedir. Ülke genelinde yüz tanıma, biyometrik tanımlama ve büyük veri analitiği temelli gözetim sistemleri inşa edilmiştir. Skynet ve Keskin Gözler programları kapsamında milyonlarca kameradan oluşan ağ, şehir ve kırsal alanlarda konuşlandırılmış; bu kameralar YZ algoritmalarıyla desteklenerek şüpheli davranışların ve kişilerin otomatik tespitine olanak sağlamaktadır (Kharpal, 2019; Laursen, 2023). Bu sistemler, suç önleme, kamu güvenliği ve siyasi istikrar hedeflerine hizmet eden iç güvenlik araçları olarak değerlendirilmektedir.

Son dönemde Çin, ulusal savunma ve iç güvenlik stratejilerinde “akıllılaşma (intelligentization)” olarak adlandırılan yeni bir aşamaya geçiş sürecini benimsemiştir. Bu süreç, mekanizasyon ve dijitalleşmeden sonra üçüncü evreyi temsil etmekte; YZ, otonom

sistemler ve büyük veri entegrasyonu aracılığıyla savaşın karakterini dönüştürmeyi ve ileri seviye gözetim kapasitesi kurmayı amaçlamaktadır (Baughman, 2024: 29). Devlet Başkanı Xi Jinping'in belirlediği yol haritasına göre, 2027 yılına kadar mekanizasyon ve dijitalleşmenin tamamlanması, 2049 yılına kadar ise PLA'nın "dünya standartlarında" bir kuvvete erişmesi hedeflenmektedir (Stokes, 2024).

#### **3.4.2.1 Çin'in otonom ve sürü insansız hava/deniz/kara araçları**

Çin, 2010'lu yılların ortalarından itibaren insansız ve sürü (swarm) teknolojilerini çok katmanlı bir savunma ekosistemi oluşturacak biçimde sistematik olarak geliştirmektedir. Kara platformlarında bu sürecin erken örneklerinden biri, Ulusal Savunma Bilim-Teknoloji Üniversitesi (NUDT) ile özel sektör işbirliğinde geliştirilen AnBot güvenlik robotudur. AnBot, sekiz saate kadar devriye süresi, gerçek zamanlı yüz tanıma kapasitesi ve düşük amperli elektroşok aparatıyla, kritik tesis korumasında insan-makine işbirliğine dayalı YZ tabanlı erken bir model olarak öne çıkmıştır (PDO, 2016). Bu uygulama, Çin'in YZ destekli statik güvenlik çözümlerini operasyonel düzeye taşımadaki kurumsal kararlılığını göstermektedir.

Hava platformlarında Elektronik ve Bilgi Teknolojisi Akademisi (CAEIT) tarafından 2017 yılında gerçekleştirilen 120 ve 200 mini-İHA'lı iki ayrı sürü uçuşu, merkezi komuta yerine ağ tabanlı görev paylaşımı ilkesinin pratik uygulanabilirliğini ortaya koymuştur. Bu teknolojik doğrulama, Eylül 2020'de tek bir kamyon platformundan 48 mühimmat yüklü mini-İHA'nın birkaç saniye içinde fırlatıldığı "intihar sürüsü" denemesiyle daha da geliştirilmiştir. Söz konusu denemeler, düşük maliyetli ve yüksek hacimli saldırı konseptlerinin, geleneksel hava savunmalarını zayıflatma potansiyeline sahip bir kuvvet çarpanı olarak değerlendirilebileceğini göstermektedir (Trevithick, 2020). 2024 yılında havacılık şirketi AVIC tarafından tanıtılan 16 tonluk Jetank adlı "ana gemi" İHA modeli ise gövdesindeki kovan modülünden çok sayıda mikro-İHA'yı havada serbest bırakarak "sürü içinde sürü" konseptini operasyonel seviyeye taşımıştır (Xuanzun vd., 2024).

Deniz alanında, Zhu Hai Yun insansız araştırma gemisinin 2022 yılında devreye alınması, geniş deniz alanlarının uydu bağlantılı rota planlamasıyla otonom biçimde devriye edilmesine imkân tanımıştır. Söz konusu platform, güvertesinden eş zamanlı biçimde hava, yüzey ve sualtı dronlarını sevk edebilen YZ mimarisiyle, kara ve hava sürülerini deniz ortamına entegre eden yeni bir kuvvet çarpanı yaklaşımını temsil etmektedir (Parken ve Trevithick, 2022). Kara alanında ise 2024 yılında duyurulan ve kamuoyunda "robo-wolf" olarak anılan silahlı dört bacaklı robot sürüleri, dar alan keşfi ve hafif taarruz görevlerinde kullanılmak üzere test edilmeye başlanmıştır (Xuanzun, 2025).

Bu teknolojik ilerlemelerin operasyonel geçerliliği, 2024 yılında gerçekleştirilen PLA NBC tatbikatlarında İHA sürülerinin, robotik köpeklerin ve bomba imha robotlarının müşterek senaryolarda eşgüdümlü olarak kullanılmasıyla gözlemlenmiştir. Aynı yıl yapılan Golden Dragon (Çin–Kamboçya) ve Çin–Nepal ortak tatbikatlarında ise keşif ve lojistik görevlerin insansız sistemlere devredilmesiyle uygulama alanı genişletilmiştir (Xuanzun, 2025). Bu gelişmeler, Çin'in devlet şirketleri (CETC, AVIC, NORINCO, CSIC) ile özel sektör arasındaki hibrit yenilik modelini kullanarak kara, hava ve deniz unsurlarını tek bir otonom savaş ağı altında bütünleştirmeye yönelik teknik temeli güçlendirdiğini göstermektedir.

### **3.4.2.2 YZ tabanlı istihbarat ve gözetleme sistemleri**

Çin'in modern gözetim mimarisi, 2005 yılında başlatılan Skynet (Tianwang) Projesi ile şekillenmeye başlamıştır. Projenin ilk aşamasında amaç, yerleşik CCTV kameraları aracılığıyla kamusal alanlarda suçun önlenmesine yönelik bir izleme altyapısı kurmaktır (Bertolotti, 2018). Ancak bu dönemde sistemler büyük ölçüde pasif nitelikteydi; insan operatörlere bağımlı çalışıyor ve veri analitiği kapasitesi sınırlı kalıyordu.

Gözetim ağının 2015 sonrasında niteliksel bir dönüşüm geçirdiği görülmektedir. Bulut bilişimin yaygınlaşması ve derin öğrenme algoritmalarının olgunlaşmasıyla birlikte Skynet, yüksek çözünürlüklü kameralar üzerinden yüz tanıma, plaka tanıma, yürüyüş analizi ve kalabalık davranış analizi gibi gerçek zamanlı özelliklerle donatılmıştır (Liyanage, 2025). Aynı dönemde SenseTime, Megvii (Face++), Yitu ve CloudWalk gibi teknoloji şirketleri, güvenlik birimlerine satılmak üzere derin öğrenme tabanlı tanıma motorları geliştirmiştir (Candariam, 2021: 13). Bu şirketlerin geliştirdiği algoritmalar, uluslararası standartlardaki değerlendirmelerde dikkat çekici bir başarı göstermiştir. ABD Ticaret Bakanlığı'na bağlı Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) tarafından yürütülen Yüz Tanıma Satıcı Testi (FRVT) sonuçlarına göre, 2018 yılında dünyanın önde gelen 39 yüz tanıma algoritması arasında ilk beş sırayı Çin merkezli firmalar paylaşmıştır. Özellikle Yitu Technology'nin algoritmalarının geniş ölçekli veri kümelerinde yüksek doğruluk oranına ulaştığı rapor edilmiştir (Xuanzum, 2018).

YZ destekli gözetim sistemlerinin etkinliği, 2018 yılında 60.000 kişilik bir konser kalabalığında aranan bir şüphelinin dakikalar içinde tespit edilip gözaltına alınması gibi olaylarla kamuoyuna yansımıştır (Wang, 2018). Bu sistemler, ülkenin Kamu Güvenliği Bakanlığı (MPS) ile yerel emniyet birimlerinin yürüttüğü Güvenli Şehir (Safe City) ve Keskin Göz (Sharp Eyes) projelerinin temelini oluşturmaktadır. Sharp Eyes Projesi, şehirlerden kırsal alanlara kadar uzanan 24 saatlik izleme kapasitesine sahip bir gözetim ağı kurmayı hedeflemiştir. Bu sistem, vatandaşların evlerindeki ekranlardan mahalle kameralarına erişerek şüpheli durumları

bildirmelerine olanak tanıyan kitle temelli bir gözetim modelini de içermektedir (Peterson, 2021; A. Thompson, 2021). Böylece resmi istihbarat altyapısına ek olarak, toplumsal düzeyde bir “halk gözetimi” mekanizması kurulmuştur.

Skynet ve Sharp Eyes gibi sistemler yalnızca görüntü verileriyle sınırlı kalmamakta; cep telefonu konumları, çevrimiçi aktiviteler, seyahat kayıtları ve diğer veri türleriyle de entegre çalışmaktadır. Bu çok kaynaklı veriler, “Polis Bulutu (Police Cloud)” adı verilen merkezi bir platformda toplanmakta ve YZ destekli analizlerle işlenmektedir (Baptista, 2022; Thompson, 2018). Böylece güvenlik birimleri, olası tehditlerin erken tespiti için gerçek zamanlı istihbarat üretme kapasitesi kazanmıştır. Bu yapı, Çin’in iç güvenlik stratejisinde veri merkezli yönetim anlayışının kurumsallaşmasına zemin hazırlamaktadır.

### **3.4.2.3 Sınır güvenliği ve göçmen izleme sistemleri**

Çin, sınır güvenliği ve göçmen hareketliliğinin izlenmesi alanlarında YZ tabanlı sistemlerin entegrasyonunu hızla artırmaktadır. Özellikle istikrarsız bölgelere komşu kara sınırlarında, çok katmanlı “akıllı sınır” altyapıları inşa edilmiştir. Bu yapılar; termal kameralar, fiber-optik yer sensörleri, hareket ve ses algılayıcıları, insansız devriye araçları ve gelişmiş yüz tanıma terminalleri gibi bileşenlerden oluşmaktadır (PTI, 2018; Tibetanreview, 2015). Bu teknolojiler, sınır bölgelerinde sürekli gözetim sağlayarak hem yasa dışı geçişleri hem de sınır ötesi tehditleri erken aşamada tespit etmeyi amaçlamaktadır.

Sınır bölgelerinde toplumsal katılım temelli gözetim yaklaşımı da sürdürülmektedir. Keskin Göz Projesi’nin bir uzantısı olarak, sınır kasabalarında yerel halkın kamuya açık kamera görüntülerine erişimi sağlanmış ve şüpheli durumların kolluk birimlerine bildirilmesi teşvik edilmiştir.

Sınır kapılarında devreye alınan biyometrik geçiş sistemleri, yolcu kimlik doğrulamasını hızlandırmış ve güvenlik denetimlerinin doğruluk oranını yükseltmiştir. Bu sistemler, yüz tanıma ve parmak izi doğrulama teknolojilerini pasaport verileriyle eşleştirerek kimlik teyidini otomatikleştirmekte, aynı zamanda bireylerin geçmiş seyahat bilgileri üzerinden risk profili analizleri gerçekleştirmektedir (Hassan, 2018; Jia ve Yan, 2017). Bu uygulama, sınır yönetiminde veri odaklı bir kontrol anlayışına geçişin önemli bir göstergesi olarak değerlendirilmektedir.

Gümrük geçiş noktalarında ise YZ tabanlı tehdit algılama yazılımları ve X-ray tarama cihazları kullanılmaktadır. Çin Gümrükleri Genel İdaresi (GACC) tarafından uygulamaya alınan bu sistemler, şüpheli eşya ve maddelerin tespitinde güvenlik kapasitesini önemli ölçüde artırmıştır.

YZ destekli analiz mekanizmaları sayesinde çok sayıda kaçakçılık girişiminin engellendiği, bu sayede insan kaynağını artırmaya gerek kalmadan denetim süreçlerinin verimliliğinin yükseldiği raporlanmaktadır (WCO News, 2024).

#### **3.4.2.4 Siber savunma ve tehdit tespiti**

Çin’de siber savunma faaliyetleri, Merkezi Askeri Komisyon (CMC), Kamu Güvenliği Bakanlığı (MPS) bünyesindeki siber birimler ve Siber Uzay İdaresi (CAC) tarafından eşgüdümlü biçimde yürütülmektedir. Bu yapı, sivil-asker füzyonu ilkesine dayanmakta ve özel siber güvenlik şirketlerinin devlet projelerine entegrasyonunu teşvik etmektedir. Böylece tespit edilen güvenlik açıklarının Devlet Güvenlik Bakanlığı (MSS)’ye iletilmesi sağlanmakta, bu süreç 2021 tarihli Ağ Ürünü Güvenlik Açığı Yönetim Yönetmeliği ile kurumsal bir zorunluluk hâline getirilmiştir. Yönetmelik, kuruluşlara her “sıfır-gün” açığını en geç 48 saat içinde ilgili makamlara bildirme yükümlülüğü getirmektedir (Benincasa, 2024).

Ülkede YZ destekli güvenlik firmaları siber savunma ekosisteminde giderek daha belirgin rol oynamaktadır. Qi An Xin şirketinin “Tianyan” sistemi, QAX-GPT adlı büyük dil modeli aracılığıyla ağ trafiği, varlık envanteri ve tehdit istihbaratını tek bir havuzda bütünleştirerek yanlış alarm oranlarını önemli ölçüde azaltmış; olayların kesintisiz ve önceliklendirilmiş biçimde incelenmesini sağlamıştır (Qianxin, 2025). Grup, ağ algılama ve yanıtlama alanında Çin’in önde gelen sağlayıcılarından biri olup, bankacılık ve kritik altyapı sektörleri dâhil yüzlerce kurumda kullanılmaktadır (Qianxin, 2024).

Bir diğer önemli aktör olan 360 Security, “YZ ile güvenliği yeniden şekillendirme” vizyonuyla sektörün ilk operasyonel güvenlik büyük modelini geliştirmiştir. Bu model, 2024 yılında gerçekleştirilen bir saldırı simülasyonunda insan müdahalesine gerek kalmadan tespitte bulunarak doğruluğunu kanıtlamış; 2025’te DeepSeek ile bütünleştirilerek otomatik tehdit avı kapasitesi genişletilmiştir (360, 2025). Şirketin 360 DNS Threat Analysis (DTA) ve Passive DNS gibi alt platformları da büyük veri ve YZ tekniklerinin geniş ölçekli ağ güvenliğine uygulanmasında öncü bir konum kazandırmıştır.

Qi An Xin ve 360 gibi kuruluşlar, güvenlik operasyonlarının otomasyonunda SOAR sistemlerinden yararlanmakta; QAX-GPT ve 360-GPT modelleriyle analistlere doğal dilde öneriler sunarak karar verme süreçlerini desteklemektedir (Qianxin, 2025). Bu sistemler, insan operatörlerin yanında çalışan yapay zekâ “asistanları” olarak tanımlanmaktadır.

Bu firmalar, tespit ettikleri güvenlik açıklarını Çin Ulusal Zafiyet Veritabanı (CNNVD)’ye iletmekte; MSS bu verileri istihbarî kullanıma göre sınıflandırarak hem savunma hem de



proaktif tehdit avı süreçlerinde değerlendirmektedir (Benincasa, 2024). Böylece Çin'in siber savunma mimarisi, devlet kurumları, özel güvenlik şirketleri ve YZ büyük modelleri arasındaki bütünleşik işleyiş üzerine kurulmuş bir yapıya dönüşmüştür.

#### **3.4.2.5 İç güvenlik ve polis uygulamaları**

Çin'de YZ tabanlı teknolojiler, iç güvenlik yönetiminin temel direği haline gelerek MPS, CAC ve yerel kamu güvenliği bürolarının stratejik kapasitesini dönüştürmüştür. Daha önceki alt bölümlerde de belirtildiği üzere, Skynet ve Keskin Gözler gibi ulusal gözetim programlarıyla entegre edilen milyonlarca kamera ve yüz tanıma algoritması, yalnızca suç önleme süreçlerini değil; aynı zamanda toplumsal istikrarın korunmasını hedefleyen kapsamlı bir gözetim mimarisi oluşturmuştur. Yapılan analizler, küresel güvenlik kameralarının yarısından fazlasının Çin sınırları içerisinde bulunduğunu ve bunların büyük bölümünün YZ destekli tanımlama yeteneğine sahip olduğunu göstermektedir (Tokson, 2025). Bu altyapının ulusal kimlik veri tabanlarıyla entegre biçimde çalışması, suç şüphelilerinin yanı sıra muhalif grupların ve etnik azınlıkların da sistematik olarak izlenmesine olanak tanımakta ve “sosyal yönetim” anlayışının teknik temelini güçlendirmektedir (Tokson, 2025).

Gözetim mimarisi, akıllı polislik platformlarıyla bütünleşmiş durumdadır. Birçok metropol, kapalı devre kamera kayıtlarını, biyometrik verileri, seyahat ve finansal kayıtları Polis Bulutu adı verilen merkezi veri gölleri aracılığıyla bir araya getirerek “bir kişi, bir dosya” sistemini işler hâle getirmiştir. Bu platformlar, makine öğrenmesi algoritmaları sayesinde artan veri hacmine paralel olarak doğruluk oranlarını yükseltmekte, düşük çözünürlüklü ya da kısmen maskelenmiş yüzleri dahi tanımlayabilmekte ve kişilerin farklı zaman ve mekânlarda izlenmesini mümkün kılmaktadır (Baptista, 2022).

Gözetimin en yoğun biçimde uygulandığı bölgelerden biri olan Sincan Uygur Özerk Bölgesinde, yüz tanıma ve iris tarayıcılarla donatılmış kontrol noktaları ile akıllı telefon tarama uygulamaları eşgüdüm içinde çalışmaktadır. Bu sistemler, bölge sakinlerinin hareketlerini sürekli olarak kaydetmekte ve belirlenen alanların dışına çıkılması durumunda anlık uyarılar üretmektedir. Uygulamalarda yer alan YZ sınıflandırıcıları, belirli içerikleri otomatik olarak tespit ederek yetkililere iletmekte ve böylece bölgedeki denetim kapasitesini artırmaktadır (Andersen, 2020).

YZ tabanlı iç güvenlik uygulamaları yalnızca gözetim alanıyla sınırlı değildir. Jiangsu eyaletinin Kunshan kentinde 2024 yılında faaliyete geçen Kunpeng Yapay Zekâ Ekibi, on yıllık veri setlerinden üretilen 220'nin üzerinde model aracılığıyla suç kalıplarını gerçek zamanlı

olarak analiz etmekte ve özellikle telekomünikasyon dolandırıcılığı vakalarında yüksek başarı sağlamaktadır. Bu uygulama birkaç ay içinde 609 vakayı çözmüş, yaklaşık 32 milyon yuan tutarındaki zararı önlemiş ve vaka çözüm oranını yüzde 62 oranında artırmıştır (Nanjing ve Xiaomin, 2024).

Benzer biçimde, alışveriş merkezleri, havalimanları ve tren istasyonlarında devriye gezen yarı özerk polis robotları, YZ destekli yüz tanıma sistemleriyle aranan şahısları tespit ederek insan memurları bilgilendirmekte; bazı modellerin öldürücü olmayan silahlarla şüphelileri etkisiz hâle getirebildiği Çin medyasında rapor edilmiştir (Tokson, 2025). Bu teknolojiler, makine görüşü ve tahmine dayalı analitikten yararlanan yazılımlarla birleştiğinde, suç yoğunluğu yüksek bölgelerin veya yeniden suç işleme olasılığı fazla bireylerin tespitini kolaylaştırmakta ve yerel kamu güvenliği bürolarının karar destek süreçlerine doğrudan katkı sunmaktadır (Nanjing ve Xiaomin, 2024).

### **3.4.3 Hindistan YZ Uygulamaları ve Sistemleri**

Hindistan'ın YZ alanındaki kapsamlı politika çerçevesi, ilk kez 2018 yılında NITI Aayog tarafından yayımlanan YZ için Ulusal Strateji (NSAI) belgesiyle şekillenmiştir (Amitabh, 2018). NSAI, sağlık, tarım, eğitim, akıllı şehirler ve akıllı mobilite olmak üzere beş öncelikli sektörde “Herkes İçin YZ” temasını benimsemiş; ekonomik dönüşüm ve kapsayıcı kalkınma odaklı bir yaklaşım ortaya koymuştur (Amitabh, 2018). Ancak bu ilk strateji, güvenlik ve savunma alanlarına dair kapsamlı bir yol haritası sunmadığı gerekçesiyle eleştirilmiştir (Chatterjee, 2020: 771). Aynı yıl Savunma Bakanlığı (MoD), savunma alanında YZ kullanımına ilişkin ayrı bir politika girişimi başlatmış; Şubat 2018’de Savunma Üretim Departmanı bünyesinde çok paydaşlı bir Görev Gücü oluşturulmuştur (Banerjee, 2025; PIB Delhi, 2022a).

Görev Gücü, Haziran 2018’de sunduğu raporda, küresel eğilimleri ve Hindistan’ın stratejik gereksinimlerini dikkate alarak savunma planlamasına YZ entegrasyonuna yönelik öneriler geliştirmiştir. Bu raporda, savunmada YZ kullanımının hızlandırılması, veri altyapısının güçlendirilmesi, yeni kurumsal birimlerin oluşturulması ve kamu-özel iş birliğinin artırılması gibi hedefler yer almıştır (PIB Delhi, 2022a). Ayrıca, ABD ve Çin gibi büyük aktörlerin askeri YZ alanındaki ilerlemeleri dikkate alınarak, Hindistan’ın bu alandaki yatırımlarını artırması gerektiği vurgulanmıştır (Chatterjee, 2020; Fernandes ve Abosata, 2024; Khalid ve Masood, 2024; Khurshid, 2022; Khurshid ve Zaman, 2024).

Şubat 2019’da, bu önerileri hayata geçirmek amacıyla Savunma YZ Konseyi (DAIC) ve Savunma Yapay Zeka Proje Ajansı (DAIPA) yürütme emriyle kurulmuştur (Khalid ve Masood, 2024; Khurshid, 2022; Khurshid ve Zaman, 2024; Sehgal, 2024). DAIC, politika düzeyinde strateji geliştirme ve uyumdan sorumlu iken; DAIPA, YZ projelerinin koordinasyonunu ve uygulama süreçlerini yürütmektedir (Khalid ve Masood, 2024; Sehgal, 2024). Bununla paralel olarak Savunma Araştırma ve Geliştirme Organizasyonu (DRDO) bünyesinde faaliyet gösteren Yapay Zeka ve Robotik Merkezi (CAIR) de savunma odaklı YZ projelerini yürütmeye devam etmektedir (Khalid ve Masood, 2024; Khurshid ve Zaman, 2024; Sehgal, 2024). Bu süreçte 2024’e kadar 25 savunma odaklı YZ projesinin tamamlanması hedefi konmuştur; bu projeler arasında insansız hava araçları, otonom tanklar, elektronik harp sistemleri ve siber güvenlik uygulamaları gibi alanlar öne çıkmaktadır (Khurshid, 2022: 141).

Savunma alanında YZ’nin temel kullanım alanları arasında sınır güvenliğinin güçlendirilmesi, iç güvenlik operasyonlarının etkinliğinin artırılması ve terörle mücadelede karar destek sistemlerinin geliştirilmesi bulunmaktadır (Khalid ve Masood, 2024; Khurshid ve Zaman, 2024). Özellikle Cammu Keşmir ve Kuzeydoğu bölgelerinde gözetim, hedef takibi ve veri analitiği süreçlerinde YZ tabanlı sistemlerin kullanımının operasyonel etkinliği artıracığı öngörülmektedir (Sehgal, 2024: 2). Hindistan, 2019 sonrasında ordu bünyesinde veri yönetimi, analitik yetkinlik ve personel eğitimi konularına odaklanmış; 2021 yılında Askerî Telekomünikasyon Mühendisliği Koleji (MCTE) bünyesinde bir Yapay Zekâ Mükemmeliyet Merkezi kurarak bu alandaki kapasitesini kurumsallaştırmıştır (IMR, 2022).

YZ uygulamalarının etik, yasal ve toplumsal boyutları da bu süreçte giderek önem kazanmıştır. Hindistan, 2020 yılında katıldığı Yapay Zekâ Küresel Ortaklığı (GPAI) aracılığıyla uluslararası normlarla uyumlu, sorumlu YZ kullanımını teşvik etmektedir (GPAI, 2020). 2021’de NITI Aayog tarafından yayımlanan “Herkes İçin Sorumlu Yapay Zekâ” yaklaşım belgesi, şeffaflık, hesap verebilirlik, adillik ve gizlilik ilkelerinin tüm sektörlerde, dolayısıyla savunma alanında da geçerli olması gerektiğini vurgulamıştır.

YZ destekli siber güvenlik alanında ise makine öğrenmesi temelli tehdit tespiti ve simülasyon modelleri geliştirilmiştir. Ancak bu alanda henüz kapsamlı bir ulusal yol haritası oluşturulamamıştır. 2023 tarihli Dijital Kişisel Veri Koruma Yasası’nın bazı hükümlerinin siber güvenlik konularını da kapsamı olumlu karşılanmış; bununla birlikte veri gizliliği ve kişisel verilerin korunması konusunda daha kapsamlı düzenlemelere ihtiyaç duyulduğu belirtilmiştir (Fernandes ve Abosata, 2024: 1-2).

Bu kapsamda, Elektronik ve Bilgi Teknolojileri Bakanlığı (MeitY) tarafından atanan bir komite, Yapay Zekâ Yönetim Yönergeleri taslağını hazırlamış ve 2025 yılı başlarında kamuoyu istişarelerine açmıştır. Taslak, deepfake’ler, siber saldırılar ve YZ kaynaklı dezenformasyon gibi konuları da kapsamakta; özellikle savunma ve ulusal güvenlik açısından kritik öneme sahip riskleri ele almaktadır (Lexplosion, 2025). Böylece Hindistan, 2020’lerin ortasına gelindiğinde hem sivil hem de askeri YZ uygulamalarını kapsayan çok katmanlı bir strateji oluşturmuştur.

Ulusal ve uluslararası etik ilkelerden yararlanılarak geliştirilen bu strateji, savunma modernizasyonunu desteklemeyi ve aynı zamanda güvenlik, gizlilik ile insan hakları arasında dengeli bir yönetim anlayışı kurmayı amaçlamaktadır. Hindistan, YZ teknolojilerini ulusal savunma stratejisinin merkezine yerleştirirken, bölgesel güvenlik tehditleri, sınır anlaşmazlıkları ve terörle mücadele gibi dinamikleri öncelikli faktörler olarak değerlendirmektedir (Thakur, 2024). Bu yönelim, Çin ve ABD gibi rakip ülkelerin askeri YZ yatırımlarına karşı rekabet gücünü artırma ve teknolojik özerklik sağlama hedefleriyle de doğrudan ilişkilidir.

Bu doğrultuda Savunma Bakanlığı (MoD), Şubat 2018’de “Ulusal Güvenlik ve Savunma için Yapay Zekânın Stratejik Uygulaması” başlıklı Görev Gücü’nü oluşturmuştur. Görev Gücü’nün Haziran 2018’de sunduğu rapor doğrultusunda, 2019 yılında Savunma Yapay Zekâ Konseyi (DAIC) ve Savunma Yapay Zekâ Proje Ajansı (DAIPA) resmen kurulmuştur. DAIC, Savunma Bakanı başkanlığında; üç kuvvet komutanı, Savunma Sekreteri, Ulusal Siber Güvenlik Koordinatörü, savunma sanayii temsilcileri ve akademisyenlerden oluşmaktadır. DAIPA ise YZ projelerinin teknik standartlarını belirleme ve uygulama süreçlerini denetleme sorumluluğunu üstlenmiştir (PIB Delhi, 2022b).

#### **3.4.3.1 İç Güvenlik ve Polislik Uygulamaları**

Hindistan’ın iç güvenlik mimarisinde de YZ sistemleri giderek artan bir rol oynamaktadır. Bu çerçevede İçişleri Bakanlığı (MHA) ve bağlı güvenlik birimleri, terörle mücadele, suç önleme, sınır güvenliği ve kamu düzeninin sağlanması alanlarında YZ tabanlı sistemleri uygulamaya koymuştur.

Hindistan’da 26/11 Mumbai terör saldırılarının ardından başlatılan National Intelligence Grid (NATGRID) projesi, MHA bünyesindeki 17–18 farklı kurumun veri tabanlarını birbirine bağlayarak istihbarat paylaşımını gerçek zamanlı hâle getirmeyi hedeflemiştir (The Tribune, 2019; Vajiram ve Ravi, 2023). Göçmenlik işlemleri, banka hareketleri, telekomünikasyon kayıtları ve vergi beyanları gibi çok sayıda kaynaktan elde edilen veriler üzerinde YZ destekli

varlık birleştirme (entity resolution) algoritmaları çalıştırılarak aynı kişiye ait farklı kayıtlar otomatik biçimde eşleştirilmekte ve soruşturma kapsamındaki kişi sayısı önemli ölçüde azaltılmaktadır. NATGRID'in kendine ait bir veri havuzu bulunmamakta, bağlı olduğu ağ üzerinden doğrudan sorgulama yaparak güvenlik birimlerinin manuel kontrollerini YZ destekli çapraz analizlerle hızlandırmaktadır (The Tribune, 2019).

Delhi Polis Teşkilatı, 2018'de kayıp çocukların tespiti amacıyla temin ettiği İsrail menşeli yüz tanıma yazılımını, 2019 yılında Başbakan Narendra Modi'nin Ramlila Maidan mitinginde ilk kez toplu tarama amacıyla kullanmış ve bu uygulama daha sonra 2020 Kuzeydoğu Delhi olayları ile 2022 Jahangirpuri soruşturmalarında da kullanılmıştır. Söz konusu teknoloji, Cumhuriyet Günü, Bağımsızlık Günü ve 2023 G20 Zirvesi gibi yüksek güvenlikli etkinliklerde kalıcı biçimde yer almıştır (Singhal, 2025). Bu deneyim, Haziran 2025'te faaliyete geçecek olan C4I merkezinin altyapısının oluşumuna katkı sağlamıştır. Elektronik ve Bilişim Teknolojileri Bakanlığı'na bağlı Centre for Development of Advanced Computing tarafından geliştirilen yerli yazılım mimarisi, yaklaşık 10.000 yüksek çözünürlüklü kameradan ve belediye ile özel ağlardan gelen görüntüleri bütünleştirerek yüz tanıma, otomatik plaka okuma ve davranışsal risk analitiğini beş saniyeden kısa sürede gerçekleştirebilmektedir. Böylece silah sesi algılama, kalabalık yoğunluğu izleme ve baygın kişi tespiti gibi durumsal farkındalık işlevleri otomatikleşmekte; e-Challan, telekom ve bankacılık verileriyle yapılan çapraz analizler olasılıksal suç önleme modellerini desteklemektedir (Singhal, 2025).

Hindistan, sınır güvenliği ve eyalet düzeyindeki iç güvenlik birimlerinde YZ odaklı gözetim, akıllı çit sistemleri, insansız hava araçlarına (İHA) karşı savunma ve trafik-suç analitiği programlarını hızla genişletmektedir. Sınır Güvenlik Gücü (BSF) tarafından yürütülen Kapsamlı Entegre Sınır Yönetim Sistemi (CIBMS) ağları, Brahmaputra ve Jammu pilot bölgelerinde termal kameralar, yer sarsıntı sensörleri ve YZ destekli kontrol merkezleriyle sınır hattını kesintisiz biçimde izlemektedir (PTI, 2019, 2025). Bunun yanında yerli üretim Dronaam adlı lazer-karıştırıcı sistemle Pakistan kaynaklı İHA sızmalarının yaklaşık %55'i etkisiz hâle getirilmiştir (Sharma, 2024). MHA, 2024 yılı itibarıyla Hindistan-Pakistan sınır hattının dört yıl içinde tamamen elektronik denetime geçirilmesini hedeflemektedir.

Eyalet düzeyinde Punjab, Telangana, Delhi, Tamil Nadu ve Odisha polis teşkilatları, YZ destekli yüz tanıma, plaka okuma, akıllı CCTV ve drone karşıtı platformları devreye alarak suç önleme ve hızlı müdahale kapasitesinde önemli ilerlemeler kaydetmiştir.

### 3.4.4 Güney Kore'nin YZ Sistem ve Uygulamaları

Güney Kore'nin YZ'yi ulusal bir öncelik olarak resmen benimsemesi 2016 yılına dayanmaktadır. Bu yönelimin en dikkat çekici dönüm noktası, aynı yıl Google tarafından geliştirilen AlphaGo adlı sistemin, 18 kez dünya şampiyonu olan Koreli Go ustasını mağlup etmesidir. Bu olay, yalnızca teknolojik bir başarı olarak değil, aynı zamanda YZ'nin insan bilişsel kapasitesini aşabileceğine dair güçlü bir simge olarak kamuoyunda yankı bulmuştur (BBC, 2019). Şampiyonun bu yenilgi sonrası profesyonel kariyerini sonlandırması, teknolojinin birey üzerindeki potansiyel etkilerine ilişkin toplumsal farkındalığı artırmıştır.

YZ alanındaki hızlı ilerleme ve “Dördüncü Sanayi Devrimi”nin doğurduğu yeni dinamikler karşısında, dönemin Devlet Başkanı Park Geun-hye yönetimi 2016 yılında “Akıllı Bilgi Topluma Hazırlık için Orta ve Uzun Vadeli Ana Plan” belgesini yürürlüğe koymuştur. Bu plan, YZ'ye yönelik büyük ölçekli kamu yatırımlarının yapılacağını duyurmuş ve ülke çapında “insan merkezli akıllı bilgi toplumu” vizyonunu ortaya koymuştur (AIDA, 2021). Plan, teknoloji, endüstri ve toplum olmak üzere üç ana ekseninde on iki temel görev belirlemiştir; bu kapsamda savunma ve kamu güvenliği, YZ'nin öncelikli uygulama alanları arasında tanımlanmıştır (IFS, 2017). Ayrıca, kamu hizmetlerinin önleyici biçimde dijitalleşmesi, stratejik veri kullanımının yaygınlaştırılması ve savunma alanında araştırma-geliştirme kapasitesinin güçlendirilmesi planın temel hedefleri arasında yer almıştır.

Bu politika çerçevesi doğrultusunda 2017 yılında Başkan Moon Jae-in liderliğinde kurulan Dördüncü Sanayi Devrimi Başkanlık Komitesi (PCFIR), yenilikçi teknolojilerin yaygınlaştırılması ve düzenleyici çerçevenin uyumlaştırılması sürecinde merkezi bir rol üstlenmiştir (STIP, 2021). Aynı dönemde, hükümetin Ar-Ge yatırımlarını artırarak ulusal rekabet gücünü yükseltmeyi ve stratejik teknolojik üstünlük elde etmeyi hedeflediği görülmektedir (Jae-in, 2018; Stangarone, 2020).

2018 yılında Bilim ve Bilgi ve İletişim Teknolojileri Bakanlığı (MSIT) tarafından yayımlanan YZ Ar-Ge Yatırım Stratejisi, bu hedeflerin kurumsal bir plana dönüşmesini sağlamıştır. Strateji, beş yıl içerisinde yaklaşık 2 trilyon won (yaklaşık 1,8 milyar ABD doları) tutarında yatırım yapılmasını öngörmüş ve üç ana amaç belirlemiştir: temel YZ teknolojilerinin geliştirilmesi, büyük ölçekli projelerin başlatılması ve 2022 yılına kadar en az 5.000 nitelikli YZ uzmanının yetiştirilmesi (Won-chang, 2018). Aynı yıl yürürlüğe konulan ulusal sanayi dönüşüm planı ise, 2030 yılına kadar 2.000 YZ destekli “akıllı fabrikanın” kurulmasını hedeflemiş ve YZ'nin ekonomik kalkınma politikalarındaki rolünü güçlendirmiştir (Ji-hye, 2019).

2019 yılında, MSIT öncülüğünde dokuz bakanlığın katılımıyla yayımlanan Yapay Zekâ Ulusal Stratejisi, ülkenin on yıl içinde küresel ölçekte bir YZ güç merkezi hâline gelmesini amaçlamıştır (C.-D. Lee, 2019). Strateji, eğitim, işgücü, ekosistem ve düzenleme alanlarında dokuz ana eksen altında yüz temel görev tanımlamış; 2030 yılına kadar Güney Kore'nin YZ sektöründe dünyanın en rekabetçi üçüncü ülkesi konumuna ulaşmasını hedeflemiştir (MSIT, 2019b; Stangarone, 2020). Bu yaklaşım, yalnızca teknik inovasyona değil, aynı zamanda YZ'nin ekonomik, toplumsal ve güvenlik boyutlarını da kapsayan bütüncül bir kalkınma vizyonuna dayanmıştır.

2019 yılının ortalarında, yeni nesil yarı iletken teknolojilerine ilişkin ulusal bir vizyon açıklanmıştır. MSIT öncülüğünde, toplam dokuz bakanlığın katılımıyla oluşturulan bu strateji kapsamında, YZ çipleri ve diğer ileri düzey yarı iletkenlerin geliştirilmesine yönelik Ar-Ge çalışmalarına ₩1 trilyon (yaklaşık 860 milyon ABD doları) yatırım yapılması planlanmıştır. Ayrıca, ₩100 milyar tutarında bir fabless girişim fonunun kurulmasına karar verilmiştir (Hayan, 2019). Bu stratejik yönelim, yalnızca ekonomik büyümeyi değil, aynı zamanda savunma kapasitesini de doğrudan ilgilendirmektedir. Zira yüksek performanslı ve enerji verimli işlemciler, ileri düzey askeri YZ uygulamalarının geliştirilmesine olanak tanımakta; aynı zamanda ülkenin yabancı yarı iletken teknolojilerine olan bağımlılığını azaltma hedefini desteklemektedir.

Başkan Moon Jae-in'in DEVIEW 2019 konferansındaki konuşması, bu vizyonun siyasi düzeyde de güçlü bir biçimde sahiplenildiğini göstermiştir. Moon, YZ'nin ulusal kalkınma için stratejik bir öncelik olarak belirlendiğini ve hükümetin altyapı yatırımlarından hukuki düzenlemelere, insan kaynağı geliştirmeden etik ilkelere kadar geniş bir alanda etkin rol üstleneceğini belirtmiştir (Korea.net, 2019).

COVID-19 pandemisi, Güney Kore'yi dijitalleşme odaklı bir kalkınma stratejisine yöneltmiştir. 2020 yılında başlatılan Kore Yeni Düzeni (K-New Deal), ülkenin ekonomik modelini dijital dönüşüm, yeşil kalkınma ve teknolojik özerklik ekseninde yeniden yapılandırmayı hedeflemiştir (MOEF, 2020). Plan üç temel yapıdan oluşmaktadır: Dijital Yeni Düzen, Yeşil Yeni Düzen ve bu iki alanı bütünleştiren Endüstriyel Yakınsama Projeleri. Özellikle Dijital Yeni Düzen kapsamında veri altyapılarının geliştirilmesi, YZ destekli kamu hizmetlerinin yaygınlaştırılması ve akıllı sağlık sistemlerinin kurulması önceliklendirilmiştir. 2020–2022 döneminde 67,7 trilyon won (yaklaşık 56,4 milyar ABD doları) yatırım öngörülmüş ve bu miktarın yaklaşık yarısının kamu kaynaklarından karşılanması planlanmıştır (MOEF, 2020).

Bu plan yalnızca ekonomik büyümeyi teşvik etmeyi değil, aynı zamanda ulusal güvenliğini güçlendirmeyi de hedeflemiştir. Ancak Güney Kore'nin YZ alanındaki liderliği, özellikle ABD ve Çin gibi teknoloji öncülerıyla karşılaştırıldığında sınırlı kalmıştır (Stangarone, 2020). İnsan kaynağı yetersizliği, yazılım geliştirme kapasitesinin sınırlılığı ve araştırma altyapısının kısıtlılığı, bu farkın temel nedenleri arasında yer almaktadır. Bu eksikliklerin giderilmesi amacıyla burs programları, lisansüstü eğitim girişimleri ve araştırma destekleri devreye alınmıştır. Böylece ülkenin yabancı teknolojiye bağımlı olmaksızın yerli ve savunma odaklı YZ projelerini geliştirebilmesi amaçlanmıştır.

2020 sonrasında Güney Kore, YZ politikalarını sürekli güncelleyerek özellikle savunma uygulamalarına yönelik ilgisini artırmıştır. MSIT tarafından 2021 yılında yayımlanan İnsansız Araç Teknolojisi Geliştirme Planı, kara ve hava tabanlı otonom sistemlerin savunma kurumlarıyla iş birliği içinde geliştirilmesini öngörmüştür (Heehyun, 2021). 2017–2021 yılları arasında Ulusal Savunma Bakanlığı'nın YZ odaklı projelere ayırdığı bütçenin düzenli olarak arttığı, 2023 itibarıyla bu eğilimin daha da güçlendiği gözlemlenmiştir (Park, 2024: 506). Bu artış, savunma odaklı YZ projelerinin olgunluk aşamasına ulaştığını göstermektedir.

Güney Kore'nin savunma YZ'sine yaklaşımının özgün yönlerinden biri, sivil-asker fonlama modelidir. MSIT gibi sivil kuruluşların da destek verdiği bu projelerde, farklı bakanlıkların katkılarıyla toplam harcama düzeyi yükselmiştir (Park, 2024: 506). Bu model, sivil inovasyonun askeri gelişmelerle bütünleştiği tersine inovasyon anlayışını temsil etmektedir.

2022'de göreve gelen Cumhurbaşkanı Yoon Suk-yeol yönetimi, önceki politikaların sürekliliğini korurken yenilikçi yönelimler de benimsemiştir. Yoon, Bilgi ve İletişim Teknolojileri ile YZ'yi hem ekonomik kalkınmanın hem de ulusal güvenliğin temel unsurları olarak tanımlamış ve 2022 yılında Savunma İnovasyonu 4.0 Programını başlatmıştır. Bu program, YZ'nin askeri reform süreçlerinin merkezine yerleştirilmesini ve otonom sistemler, karar destek yazılımları ile gerçek zamanlı veri işleme kapasitesinin artırılmasını amaçlamıştır (Park, 2024: 506-507).

Yoon döneminin bir diğer önemli girişi, Dijital Platform Hükümeti vizyonudur. Bu politika, kamu hizmetlerinin YZ ve büyük veri teknolojileriyle entegre edilmesini, hizmetlerin şeffaf, hızlı ve etkili biçimde sunulmasını ve savunma alanında veri paylaşımının güçlendirilmesini hedeflemiştir (Park, 2024: 508).



2023 itibarıyla YZ politikalarının koordinasyonu, Bilim ve Teknoloji Başkanlık Danışma Kurulu tarafından yürütülmektedir. Bu dönemde özellikle üretici YZ (generative AI) teknolojilerine yönelik stratejiler geliştirilmiş ve etik, hukuki ve toplumsal etkilerin değerlendirilmesine yönelik yüksek düzeyli danışma konseyleri oluşturulmuştur (MSIT, 2024a). Cumhurbaşkanı Yoon Suk-yeol, 26 Eylül 2024'te gerçekleştirilen Ulusal Yapay Zekâ Komitesi toplantısında, ülkenin gelecekteki vizyonunu şekillendirecek Ulusal YZ Stratejisi Politik Yönelimleri belgesini kamuoyuna açıklamıştır (MSIT, 2024c).

Yoon yönetimi döneminde Güney Kore'nin YZ politikaları çok katmanlı, bütüncül ve ileriye dönük bir yapıya evrilmiştir. Politika çerçevesi; ulusal stratejiler, sektörel uygulama planları ve savunma odaklı yol haritalarından meydana gelmektedir. Bu çok boyutlu stratejik yaklaşım, Güney Kore'yi yalnızca sivil alanda değil, aynı zamanda ulusal güvenlik ve askeri planlama bağlamında da YZ temelli dönüşümün merkezine konumlandırmıştır.

#### **3.4.4.1 İç güvenlik ve polislik uygulamaları**

Güney Kore, iç güvenlikte YZ uygulamalarını kamusal güvenlik, suç önleme, istihbarat ve acil durum yönetimi gibi alanlarda hızla yaygınlaştırmaktadır. Bu kapsamda İçişleri ve Güvenlik Bakanlığı (MOIS), Kore Ulusal Polis Teşkilatı (KNP), Ulusal İstihbarat Servisi (NIS) ve Kore Sahil Güvenlik (KCG) gibi kurumlar, farklı düzeylerde YZ destekli sistemler geliştirmekte veya uygulamaya koymaktadır.

Elektronik ve Telekomünikasyon Araştırma Enstitüsü (ETRI) tarafından geliştirilen Dejaview platformu, bu dönüşümün dikkat çeken örneklerinden biridir. Sistem, gerçek zamanlı video akışını geçmiş suç istatistikleriyle birleştirerek potansiyel suç faaliyetlerini önceden belirlemeye yönelik öngörüselsel bir analiz aracı sunmaktadır (NRCSNT, 2024). Ulusal Polis Teşkilatı ve yerel yönetimlerin katılımıyla yürütülen ortak Ar-Ge çalışması sonucunda 12 Eylül 2024'te tanıtılan sistem, kapalı devre kamera ağlarını pasif izleyici konumundan çıkararak devriye yönlendirmelerinde aktif bir sensör bileşeni haline getirmiştir (NRCSNT, 2024; Richard, 2024).

Kore Ulusal Polis Teşkilatı (KNP), gerçek zamanlı yüz tanıma (FRT) ve davranış analizi teknolojilerini akıllı şehir altyapısına entegre ederek kalabalık alanlarda şüpheli kişi tespiti, riskli eylem belirleme ve dinamik devriye planlaması hedeflemektedir (Werner, 2025). 2021 yılında Bucheon kentinde başlatılan pilot uygulamada, 10.820 kameradan elde edilen görüntüler YZ tabanlı yüz veritabanlarıyla eşleştirilmiş ve sistem COVID-19 temaslılarının

takibinde etkin biçimde kullanılmıştır (Cha, 2021). Aynı sistemin, benzer biçimde şüpheli şahıs takibini kolaylaştıracak şekilde genişletilmesi planlanmaktadır.

2023 yılında Seoul Metro, görüntü-açıklama tabanlı bir model kullanarak baygınlık, hırsızlık veya bıçaklı saldırı gibi olayları otomatik biçimde algılayan ve operatöre cümle halinde bildirim gönderen bir anomali tespit çözümünü Line-5 istasyonunda test etmiştir (Joo-heon, 2023). Benzer şekilde Han Nehri üzerindeki köprülerde yer alan kameralar, intihar girişimlerine işaret eden davranış örüntülerini analiz ederek itfaiyeye anlık uyarı göndermeye başlamıştır (SBN, 2021). Bu örnekler, Güney Kore'nin yüz tanıma ve davranış analizi temelli YZ sistemleri aracılığıyla suç önleme, erken müdahale ve kamu güvenliği süreçlerinde somut ilerlemeler kaydettiğini göstermektedir.

Güney Kore, göç ve sınır güvenliği alanlarında da YZ temelli çözümler geliştirmektedir. Adalet Bakanlığı (MOJ) tarafından yürütülen ve 2019 yılında başlatılan YZ Göçmen Projesi, yasa dışı göç ve sahte kimlik tespitini hedeflemekte olup, 2023 itibarıyla 170 milyon yüz görüntüsü ve parmak izinden oluşan geniş bir veri tabanına dayanmaktadır (AIID, 2019; Fennel, 2022). u veriler, özel şirketlerle iş birliği çerçevesinde YZ algoritmalarının eğitimi için paylaşılmıştır. Proje 2024 yılı sonunda hukuki inceleme sürecine alınmış olsa da, Incheon Havalimanı 2023 yılında Alchera şirketinin derin öğrenme tabanlı yüz tanıma yazılımını içeren Smart Pass sistemini devreye sokmuştur. IATA ölçümlerine göre, bu sistemin boarding süresini ortalama yüzde 40 oranında azalttığı bildirilmiştir (Song, 2023; Teo, 2024).

Bu gelişmeler, Güney Kore'nin iç güvenlikte YZ teknolojilerini yalnızca denetim ve gözetim amacıyla değil, aynı zamanda operasyonel verimliliği artırma, riskleri önceden belirleme ve acil müdahaleyi hızlandırma aracı olarak konumlandığını ortaya koymaktadır.

### **3.4.5 Japonya'nın YZ uygulamaları ve sistemleri**

Japonya'nın "Süper Akıllı Toplum" vizyonu olan Toplum 5.0, 2016 yılından bu yana ulusal teknoloji politikalarının yönünü belirleyen temel çerçeveyi oluşturmaktadır. Bu vizyon, 5. Bilim ve Teknoloji Temel Planı kapsamında, ekonomik büyümeyi teşvik ederken toplumsal sorunlara çözüm üretmeyi hedefleyen, siber ve fiziksel alanların entegrasyonuna dayalı insan merkezli bir toplum modeli olarak tanıtılmıştır (Council for Science vd., 2015: 1). Ardıl belge niteliğindeki 6. Temel Plan (2021) ise toplumu "tehditlere ve öngörülemez durumlara karşı sürdürülebilir ve dirençli hale getirme" amacını ön plana çıkararak, güvenlik ve dayanıklılık ilkelerini stratejik bir çerçeveye yerleştirmiştir (NICT, 2022: 1-3). Bu yaklaşım, YZ'nin

güvenlik dahil olmak üzere çok sayıda sektördeki rolünü güçlendirmek için güçlü bir temel oluşturmuştur (Council for Science vd., 2015: 13).

Bu doğrultuda Japon hükümeti, özel YZ stratejileri geliştirerek Kabine Ofisi'ne bağlı Bilim, Teknoloji ve İnovasyon Konseyi aracılığıyla YZ Stratejisi 2019 belgesini yayımlamıştır. Strateji; eğitim, araştırma-geliştirme ve YZ'nin toplumsal uygulamaları alanlarında kapsamlı politika paketleri içermektedir. Ayrıca aynı yıl yayımlanan İnsan Merkezli YZ İlkeleri, insan kaynağının geliştirilmesi, veri altyapısının güçlendirilmesi ve etik standartların oluşturulmasına yönelik öncelikleri belirlemiştir. Sonraki güncellemeler olan YZ Stratejisi 2021 ve YZ Stratejisi 2022, ortaya çıkan yeni güvenlik ve etik sorunlara odaklanmıştır. Özellikle YZ Stratejisi 2021'de "Ulusal Dayanıklılık için YZ" temasıyla afet yönetimi, kriz yanıtı ve kritik altyapı güvenliği konuları ön plana çıkmış; "Sorumlu YZ" ilkesi, güvenilirlik ve siber güvenliğin sağlanmasında temel bir gereklilik olarak vurgulanmıştır (NICT, 2022: 1-17).

Japonya'nın YZ politikaları, insan onurunu ve toplumsal faydayı merkeze alırken, stratejik boyutları da dolaylı biçimde içermektedir. Bu stratejiler, kritik altyapıların korunması, afet ve kriz yönetimi, kamu güvenliği gibi alanlarda YZ kullanımını teşvik etmekte ve savunma ile sivil koruma arasındaki sınırı giderek geçirgen hale getirmektedir (NICT, 2022: 2-17). Genel olarak Japonya, Toplum 5.0 vizyonu ve Yeniden Canlandırma Stratejileri aracılığıyla otonomi, büyük veri, robotik ve siber güvenlik gibi alanlarda Ar-Ge faaliyetlerini destekleyerek YZ'nin savunma uygulamaları için uygun bir ekosistem yaratmaktadır.

Japonya'nın YZ yol haritaları ağırlıklı olarak sivil odaklı olsa da bu teknolojilerin savunma ve güvenlik üzerindeki etkileri açık biçimde kabul edilmektedir. Ulusal Savunma Programı Yönergeleri (NDPG) 2018 ve buna bağlı Orta Vadeli Savunma Programı (MTDP) 2019–2023, gelişmekte olan teknolojilerin savunma planlamasına entegrasyonu açısından dönüm noktası olmuştur. Bu programlarda YZ ve otonomi temelli sistemlerin geliştirilmesi öncelikli alan olarak belirlenmiş; Japon Öz Savunma Kuvvetleri (SDF) bünyesinde veri işleme, komuta-kontrol ve karar destek mekanizmalarına YZ'nin dâhil edilmesi hedeflenmiştir. MTDP ayrıca, Güvenlik için Yenilikçi Bilim ve Teknoloji Girişimi kapsamında YZ gibi stratejik teknolojilere yönelik Ar-Ge faaliyetlerini önceliklendirmiştir. Bu girişim, hem sivil hem askeri kullanım potansiyeli taşıyan teknolojilerin finansmanına yönelik bir program olarak konumlanmıştır (Ministry of Defense, 2018: 1-22). Böylece Japonya, yalnızca kara ve deniz operasyonlarında değil, aynı zamanda uzay, siber ve elektromanyetik alanlarda da etkinlik gösteren ve ağ merkezli harekât kabiliyetine sahip bir "Çok Alanlı Savunma Gücü" inşa etmeyi hedeflemiştir.

YZ teknolojilerinin gelişmiş biçimlerde uygulanması, Japonya'nın uzun vadeli savunma stratejisinin temel unsurlarından biri haline gelmiştir. 2019 sonrasında yayımlanan güvenlik belgelerinde de bu yaklaşım güçlenmiştir. Defense of Japan 2023 ve 2024 Beyaz Kitapları, YZ'nin komuta-kontrol sistemleri, istihbarat analizi ve otonom platformlarda kullanımına özel olarak yer vermekte; bu teknolojiyi bilgi üstünlüğü ve kuvvet modernizasyonunun merkezine yerleştirmektedir (Ministry of Defense, 2025).

Japonya'nın savunma politikası, YZ'yi hem demografik kısıtların yarattığı insan gücü açığını azaltmak hem de ABD ve Çin gibi ülkelerin teknolojik ilerlemeleriyle rekabet edebilmek için kritik bir unsur olarak görmektedir. Bu anlayış, Savunma Bakanlığı'nın Temmuz 2024'te kabul ettiği YZ Politikası ile kurumsal nitelik kazanmıştır. Politika, YZ kullanımını doğrudan personel verimliliğinin artırılmasına bağlamış; yaşlanan nüfusun yarattığı insan kaynağı kısıtlarını dengelemeyi stratejik bir hedef olarak belirlemiştir. Savunma Bakanı Minoru Kihara, “personelin daha verimli kullanılmasının büyük önem taşıdığını” ve “YZ'nin bu zorlukların üstesinden gelmede kilit bir potansiyele sahip olduğunu” ifade etmiştir (J. Johnson, 2024).

Bu çerçevede Japonya, yapay zekâyı ulusal güvenliğin dayanıklılığını güçlendiren ve savunma kapasitesinin etkinliğini artıran temel bir unsur olarak konumlandırmaktadır. Bununla birlikte, bu süreç ülkenin pasifist doktrini ve insan merkezli etik ilkeleri doğrultusunda yürütülmekte; teknolojik ilerleme ile anayasal sınırlar arasındaki denge titizlikle korunmaktadır.

#### **3.4.5.1 İç güvenlik ve polis uygulamaları**

Japonya Ulusal Polis Teşkilatı (NPA) ve ona bağlı yerel birimler, suçun önlenmesi, kamu düzeninin korunması ve afet dönemlerinde güvenliğin sağlanması amacıyla YZ destekli uygulamaları kademeli biçimde hayata geçirmektedir. 2024 yılı Polis Beyaz Kitabı'nda, siber uzayın artan önemi, anonim suç ağlarının oluşumu ve ileri teknolojilerin suç amaçlı kullanımının getirdiği yeni tehditler ayrıntılı biçimde ele alınmaktadır. Bu kapsamda NPA, hem suçla mücadelede YZ tabanlı analiz araçlarını kullanmakta hem de derin sahte videolar veya otomatik siber saldırılar gibi teknolojik tehditlere karşı önleyici stratejiler geliştirmektedir (NPA, 2024: 3-16).

NPA, tahmine dayalı polislik alanında da pilot projeler yürütmüştür. 2020 Tokyo Olimpiyatları öncesinde Kanagawa Emniyeti tarafından başlatılan programda, geçmiş suç verilerini ve olaylar arası ilişkileri derin öğrenme algoritmalarıyla analiz eden bir sistem test edilmiştir. Bu sistemin, belirli suçların aynı fail tarafından işlenip işlenmediğini karşılaştırmalı biçimde belirleyebildiği ve olası sonraki eylemleri öngörebildiği rapor edilmiştir (Kyodo News, 2018). Aynı dönemde

geliştirilen Crime Nabi yazılımı, teorik fizik temelli istatistiksel modellerle zaman ve mekâna göre suç gerçekleşme olasılıklarını tahmin etmeyi amaçlamıştır(UTokyo, 2024). Crime Nabi, Japonya'daki düşük suç oranları nedeniyle sınırlı uygulanabilmiş olsa da, Orta ve Güney Amerika'daki bazı güvenlik birimlerinde %50'nin üzerinde isabet oranı sağlamıştır(Hiebert ve Tang, 2025). Japonya'da ulusal ölçekte uygulanmasa da, bazı yerel emniyet birimleri hırsızlık ve kundaklama gibi olayların yoğunlaştığı bölgelerde devriye planlamasını optimize etmek amacıyla veri analitiği araçlarından yararlanmaktadır.

Polis yetkilileri, YZ'nin yalnızca karar destek aracı olarak değerlendirildiğini ve nihai kararın insan unsuru tarafından verilmesi gerektiğini vurgulamaktadır. Üst düzey bir NPA temsilcisi, “daha gelişmiş polis faaliyetleri için denemeleri agresif biçimde sürdürüyoruz; ancak memurların nihai kararı verebilmesi için her şeyi YZ'ye bırakma planımız yok” açıklamasını yapmıştır (Yoshida, 2021). Bu ifade, polis teşkilatının YZ'ye temkinli bir iyimserlikle yaklaştığını ve insan denetimini merkezde tutarak teknolojiden yararlanmayı hedeflediğini göstermektedir.

NPA, soruşturma süreçlerini hızlandırmak ve kanıt toplama kapasitesini artırmak amacıyla görüntü tabanlı YZ uygulamalarını da yaygınlaştırmaktadır. 2019'da başlatılan pilot çalışma, sabit kameralardan alınan görüntülerdeki araçları marka–model bazında eşleştirebilen bir modelle sınırlıydı. 2021'e gelindiğinde sistem, yaklaşık 1000 farklı araç modelini içeren bir veri tabanına genişletilmiş ve video akışlarını tarayarak şüpheli araçlara ait sahneleri otomatik biçimde ayıklayabilecek şekilde geliştirilmiştir (Yoshida, 2021). Aynı dönemde, kalabalık analizine odaklanan bir modül, büyük etkinliklerdeki kameraları gerçek zamanlı izleyerek olağandışı hareketleri saptamayı hedeflemiştir. Pilot uygulamalar, algoritmanın seyrek bölgelerde yüksek doğrulukla çalıştığını, ancak kalabalık ortamlarda performansın azaldığını göstermiştir. 2020 sonrasında bu deneyim, devriye noktalarına yerleştirilen kameralarla aylıklık, uzun süreli bekleme veya silah çekme gibi riskli davranışları algılayan erken uyarı sistemlerine aktarılmıştır (Yoshida, 2021).

NPA, bu süreçte insan denetimini temel alan bir otomasyon anlayışını benimsemektedir. YZ, karar verici konumunda değil; yüksek hacimli görüntülerin önceliklendirilmesinde hız ve doğruluk artışı sağlayan bir destek unsuru olarak konumlandırılmıştır (Yoshida, 2021). Bu yaklaşım, delil tespiti ve kimliklendirme süreçlerinde insan hatasını azaltmakta, kaynakların daha etkin biçimde yönlendirilmesini sağlamaktadır.

2017'de NPA'ya yaklaşık 400 bin şüpheli finansal işlem raporu iletilmiştir. Bu yoğunluk, klasik inceleme yöntemlerinin yetersiz kaldığı durumlarda YZ destekli analizlerin gerekliliğini ortaya

koymuřtur (Mainichi, 2018). 2019 sonrasında devreye alınan makine öğrenmesi çözümleri, bu raporların ön elemenden geçirilmesini sağlayarak 2024 itibarıyla kara para aklama soruşturmalarında standart uygulama haline gelmiştir (Kustom Signals, 2019; Yoshida, 2021).

Ağustos 2024'te NPA, 2025 mali yılı için yaklaşık 5,96 milyar yen ek ödenek talep etmiş ve siber tehditlere karşı kapasite artırımı planını açıklamıştır. Bu bütçenin bir bölümü, sahte web sitelerini gerçek zamanlı tespit edebilecek generatif YZ tabanlı bir sistemin geliştirilmesine ayrılmıştır. Sistem, sürekli öğrenme yaklaşımıyla kimlik avı saldırılarında kullanılan sahte banka veya e-devlet portallarını tanımlayarak hem kullanıcıları hem de yetkilileri uyarmaktadır (Japantimes, 2024). Aynı dönemde yürürlüğe giren Aktif Siber Savunma Yasası, güvenlik birimlerinin potansiyel tehditler gerçekleşmeden önce düşman sunuculara müdahale etmesine imkân tanımıştır. Bu düzenleme, Japonya'nın geleneksel olarak savunma odaklı siber güvenlik anlayışından proaktif bir yaklaşıma geçişini temsil etmektedir (Martin, 2025).

Polis teşkilatı, afet sonrası yağma ve hırsızlık vakalarını önlemek amacıyla YZ destekli İHA'ları da kullanıma sokmuştur. 2024'te başlatılan bu uygulama, tahliye edilen geniş alanlarda suç girişimlerinin hızlı biçimde tespit edilmesini hedeflemektedir. İHA'lar, YZ tabanlı görüntü analitiğiyle afet bölgelerinde şüpheli davranışlar sergileyen bireyleri belirleyip, yer ekiplerine anlık konum bilgisi iletmektedir. Bu girişimin güvenliği artırma potansiyeli yüksek olmakla birlikte, Criminal Justice Future düşünce kuruluşundan Shinichi Ishizuka, polise tanınan bu geniş yetkinin kötüye kullanım riski taşıdığına dikkat çekmiştir (Ryall, 2024). Uygulama yalnızca afet bölgeleriyle sınırlı kalmayıp, devriye faaliyetlerinin zor olduğu geniş park ve dağlık alanlarda da test edilmektedir.

Bu gelişmeler, Japonya'nın kamu güvenliği alanında YZ'yi insan merkezli denetim ilkesiyle birleştirerek etik sınırları koruduğunu ve teknolojiyi yalnızca karar destek aracı olarak konumlandığını göstermektedir.

### **3.5 Türkiye'nin Yapay Zeka Politikası**

Türkiye'nin YZ alanındaki ilk kapsamlı politika belgesi olan UYZS (2021–2025), Ağustos 2021'de Cumhurbaşkanlığı Dijital Dönüşüm Ofisi ile Sanayi ve Teknoloji Bakanlığı iş birliğinde yayımlanmıştır (CBDDO, 2024). Strateji belgesi, On Birinci Kalkınma Planı (2019–2023) ve 2021 Cumhurbaşkanlığı Yıllık Programı'nda yer alan hedeflerle uyumlu biçimde hazırlanmış; 2025 yılı perspektifini merkeze alan bütüncül bir vizyon ortaya koymuştur (OECD, 2025).

Belgenin temel amacı, ulusal ölçekte yürütülen YZ faaliyetlerini ortak bir çerçevede bütünleştirmek ve bu faaliyetlerin etkin şekilde uygulanmasını sağlayacak kurumsal bir yönetim mekanizması oluşturmaktır. Stratejinin uygulama boyutunu oluşturan UYZS Eylem Planı, belirlenen hedeflere ulaşmak üzere somut adımlar ve bir yol haritası sunarak Türkiye'nin YZ ekosisteminin gelişimini hızlandırmayı hedeflemektedir (CBDDO, 2024).

### **3.5.1 Ulusal Yapay Zeka Stratejisi hedefleri ve temel ilkeleri**

UYZS, Türkiye'yi 2025 yılına kadar küresel ölçekte ilk yirmi YZ ülkesi arasında konumlandırmayı amaçlamakta; bu hedef doğrultusunda altı stratejik öncelik ve bunlara bağlı nicel göstergeler ortaya koymaktadır. UYZS, insan merkezli ve güvenilir YZ anlayışını esas almakta; ölçülülük (orantılılık), güvenlik, tarafsızlık, mahremiyet, şeffaflık, hesap verebilirlik, veri egemenliği ve yönetim gibi normatif ilkelere dayanmaktadır. Bu çerçevede belge, kişisel verilerin korunmasını, etik değerlere uygun sistemlerin geliştirilmesini ve YZ uygulamalarının insan haklarına saygılı, güvenilir ve veri mahremiyetine duyarlı biçimde tasarlanmasını temel bir gereklilik olarak vurgulamaktadır (STB ve CBDDO, 2021: 1-15).

UYZS, nitelikli insan kaynağının geliştirilmesini stratejik bir öncelik olarak tanımlamakta ve bu amaca yönelik ölçülebilir hedefler belirlemektedir. Stratejiye göre, 2025 yılına kadar YZ alanında 50 bin kişilik toplam istihdam sağlanması, kamu kurumlarında ise en az 1000 YZ uzmanının görevlendirilmesi öngörülmektedir. Ayrıca lisansüstü düzeyde 10 bin YZ mezunu, alanda 5 bin aktif akademisyen yetiştirilmesi ve en az 1000 yüksek lisans veya doktora tezinin YZ odaklı olması planlanmaktadır. Girişimcilik ekosistemi açısından, 2025 yılına dek 1000 YZ girişiminin faaliyete geçmesi ve kamu alımlarında yerli çözümlerin önceliklendirilmesi yoluyla en az beş yenilikçi “filiz şirketin” (start-up) ortaya çıkması hedeflenmiştir. Ayrıca, doğal dil işleme (NLP) alanında küresel ölçekte rekabet edebilecek en az bir Türk girişiminin ortaya çıkması öncelikli hedefler arasında yer almaktadır (STB ve CBDDO, 2021: 66-70).

UYZS, veri yönetimi ve altyapı alanlarında hem kamu hem özel sektörün yüksek nitelikli verilere erişimini artırmaya yönelik adımlar öngörmektedir. Bu kapsamda, “Kamu Veri Alanı (KVA)” adıyla güvenli bir veri paylaşım platformunun oluşturulması, en az on sektörel bulut sisteminin hayata geçirilmesi ve Açık Veri Portalı (AVP) aracılığıyla binden fazla veri setinin kamuya sunulması hedeflenmektedir. Ayrıca YZ araştırmacılarının kullanımına açık yüksek başarılı hesaplama (HPC) altyapılarının yaygınlaştırılması planlanmaktadır. Türkiye Açık Kaynak Platformu (TAKP) çatısı altında en az 1000 geliştiricinin YZ projelerine katkı vermesi teşvik edilerek yerli açık kaynak ekosisteminin güçlendirilmesi de öncelikli hedeflerden biridir (STB ve CBDDO, 2021: 70-71).

UYZS, Türkiye'nin uluslararası iş birliği kapasitesinin güçlendirilmesini stratejik bir zorunluluk olarak tanımlamaktadır. Belge, 2025 yılına kadar 100'ü aşkın sınır ötesi Ar-Ge projesine katılım sağlanmasını ve "güvenilir ve sorumlu YZ" alanında en az iki uluslararası rapor çalışmasında Türkiye'nin aktif rol üstlenmesini öngörmektedir. Ayrıca OECD, Avrupa Birliği (AB) ve Birleşmiş Milletler (BM), UNESCO dâhil uluslararası çerçevelerle uyumlu politikalar geliştirilmesi taahhüt edilerek hem küresel normlarla entegrasyonun hem de uluslararası görünürlüğün artırılması hedeflenmiştir (STB ve CBDDO, 2021: 10-76). Böylece, ulusal bilim ve teknoloji politikalarında dile getirilen YZ hamlesi, ilk kez kurumsal ve bütüncül bir politika belgesiyle somutlaştırılmıştır.

### **3.6 Türkiye'de Yapay Zeka Alanını Düzenleyen ve Destekleyen Çeşitli Yasal ve İdari Belgeler**

Bu bölüm alt başlıklarında Türkiye'de YZ alanında çıkarılan Kanun, Cumhurbaşkanlığı Kararnamesi, Yönetmelik/Genelge ve Strateji güncellemeleri gibi belgeler kronolojik bir sırayla ele alınmaktadır.

#### **3.6.1 2015-2018 Bilgi Toplumu Stratejisi ve Eylem Planı**

2015–2018 Bilgi Toplumu Stratejisi ve Eylem Planı (BTS-EP), Türkiye'nin Onuncu Kalkınma Planı (2014–2018) çerçevesinde hazırlanmış olup, dijital dönüşümü makroekonomik büyümeyi ve istihdamı destekleyen temel bir politika aracı olarak konumlandırmaktadır. Belge, bilgi toplumuna geçiş sürecini hızlandırmak amacıyla sekiz stratejik eksen etrafında şekillenen eylem setlerini ayrıntılı biçimde tanımlamaktadır.

Bu kapsamda; kamu hizmetlerinin dijitalleşmesi, yüksek kapasiteli genişbant ağlarının yaygınlaştırılması, sektör odaklı Ar-Ge ve yerlileştirme programları, büyük veri analitiği ile veri mahremiyetine ilişkin düzenlemeler ve siber güvenlik standartları stratejinin temel odak alanlarını oluşturmaktadır. Her ne kadar belge içinde YZ kavramı doğrudan kullanılsa da, büyük veri analizi, bulut bilişim, akıllı kent uygulamaları, 5N haberleşme altyapısı ve ileri Ar-Ge teşvikleri gibi YZ ekosisteminin temel bileşenleri sistematik biçimde ele alınmıştır. Özellikle Sosyal Güvenlik Kurumu (SGK) ve sağlık sektörü için öngörülen büyük veri pilot projeleri, veri bilimi yetkinliklerinin geliştirilmesine yönelik müfredat güncellemeleri ve akıllı kent inisiyatifleri; öngörücü analitik, makine öğrenmesi ve karar destek mekanizmalarının kurumsal ölçekte benimsenmesine elverişli bir zemin hazırlamaktadır (BTDB, 2015: 15-132).



Dolayısıyla BTS-EP, veri altyapısından insan kaynağına, güvenlikten yenilikçi uygulamalara kadar uzanan bütüncül yaklaşımıyla Türkiye'nin dijital ekonomisini ölçeklendirmeyi ve YZ ekosisteminin ön koşullarını oluşturan nitelikli veri, gelişmiş altyapı, yetkin beşerî sermaye ve güvenilir hukuki çerçeveyi inşa etmeyi hedeflemektedir.

### **3.6.2 6698 Sayılı Kişisel Verilerin Korunması Kanunu**

Veri odaklı teknolojilerin hızla yaygınlaşması, kişisel verilerin korunmasını hem hukuki hem de etik açıdan stratejik bir öncelik haline getirmiştir. Türkiye'de 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK), 24 Mart 2016 tarihinde kabul edilmiş ve 7 Nisan 2016 tarihli Resmî Gazete'de yayımlanarak yürürlüğe girmiştir.

KVKK, kişisel verilerin işlenmesinde “başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumayı” amaçlayan ilk kapsamlı ulusal düzenleme olma özelliğini taşımaktadır. Böylece, daha önce dağınık biçimde yer alan mevzuat hükümleri sistematik bir çatı altında toplanmış ve veri işleme faaliyetleri için yeknesak bir standart oluşturulmuştur.

Kanun, “YZ” terimini doğrudan kullanmamakla birlikte kişisel veri işleyen tüm teknik sistemleri kapsamakta, dolayısıyla YZ algoritmalarını da hukuki denetim alanına dâhil etmektedir (KVKK, 2016: 1). Bu bağlamda YZ geliştiricileri ve işletmecileri açısından üç temel yükümlülük öne çıkmaktadır:

- Açık Rıza: Kişisel veriler, kural olarak ilgili kişinin açık rızası alınmadan işlenemez (Madde 5/1). Bu hüküm, YZ modellerinin eğitimi için kullanılan verilerin edinilmesinde şeffaflık ve gönüllülük esaslarını zorunlu kılmaktadır (KVKK, 2016: 2).
- Veri Minimizasyonu: Genel ilkeler, verilerin işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olmasını öngörmektedir (Madde 4/2-ç). Bu ilke, YZ projelerinde yalnızca amaca hizmet eden asgari veri kümesinin kullanılmasını gerektirmektedir (KVKK, 2016: 2).
- Veri Güvenliği: Veri sorumluları, kişisel verilerin yetkisiz erişim ve işlenmesini önlemek amacıyla uygun teknik ve idari tedbirler almakla yükümlüdür (Madde 12). Bu hüküm, YZ sistemlerinin uçtan uca güvenliğini yasal bir sorumluluk haline getirmektedir (KVKK, 2016: 6).

KVKK, aynı zamanda idari ve mali özerkliğe sahip Kişisel Verileri Koruma Kurumu (KVKK)'nu kurmuştur (Madde 19). Bu kurum, düzenleyici işlemler yapma, denetim gerçekleştirme ve ihlaller karşısında yaptırım uygulama yetkisine sahiptir. Kanuna aykırılıklar halinde Türk Ceza Kanunu (TCK) hükümleri çerçevesinde cezai yaptırımlar (Madde 17) ve 1

milyon Türk lirasına kadar idari para cezaları (Madde 18) uygulanabilmektedir (KVKK, 2016: 9).

6698 sayılı Kanun, Türkiye’de kişisel veri işleyen tüm sistemler için asgari bir etik ve hukuki temel oluşturmaktadır. YZ projeleri, veri toplama, işleme ve modelin devreye alınması dâhil tüm aşamalarda KVKK’nın açık rıza, veri minimizasyonu ve güvenlik ilkelerine uymakla yükümlüdür. Bu yönüyle Kanun, gelecekte geliştirilecek YZ uygulamalarında mahremiyetin korunması ve bireysel hakların gözetilmesi açısından temel bir referans çerçevesi işlevi görmektedir.

### **3.6.3 On Birinci Kalkınma Planı**

On Birinci Kalkınma Planı (2019–2023), “Millî Teknoloji Hamlesi” başlığı altında YZ, nesnelerin interneti (IoT), artırılmış gerçeklik (AR), büyük veri, robotik ve kuantum teknolojileri dâhil olmak üzere on üç kritik teknoloji alanından biri olarak tanımlamaktadır. Plan, bu alanlar için yol haritalarının oluşturulmasını, altyapı yatırımlarının yapılmasını ve nitelikli insan kaynağının yetiştirilmesini öngörmektedir (SBB, 2019: 172).

Belgede yer alan “YZ teknolojilerinin üretilmesi ve kullanımının yaygınlaştırılmasına yönelik ulusal politika belirlenecektir” ifadesi, ekonominin tüm sektörlerini kapsayacak ulusal bir YZ yol haritasının hazırlanacağını hüküm altına almaktadır (SBB, 2019: 109). Bu hüküm, YZ’nin sadece Ar-Ge alanında değil, üretimden kamu hizmetlerine kadar uzanan geniş bir uygulama yelpazesinde konumlandırılacağını göstermektedir.

Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK) bünyesindeki araştırma merkezlerinin kapasitesinin artırılması, özel sektörle yeni teknoloji ve ürün geliştirme projelerinin yürütülmesi ve yüksek teknoloji platformlarının kurulması hedefleri, YZ dâhil öncelikli alanlarda uzmanlaşmış araştırma enstitülerinin temellerini oluşturmaktadır (SBB, 2019: 77). Bu çerçevede YZ’nin de içinde yer aldığı kritik teknoloji alanlarında mevcut kabiliyetlerin analiz edilmesi, uzun vadeli arz-talep projeksiyonlarının hazırlanması ve yetkinlik boşluklarını kapatmaya yönelik beceri haritalarının oluşturulması öngörülmektedir (SBB, 2019: 79).

Öncelikli sektörlerde kurulması planlanan endüstriyel bulut platformları üzerinde YZ, ileri veri analitiği ve simülasyon hizmetlerinin geliştirilmesi amaçlanmaktadır. Bu hizmetlerden yararlanacak küçük ve orta ölçekli işletme (KOBİ) sayısının 2023 yılı itibarıyla on bine ulaşması hedeflenmiştir (SBB, 2019: 75-76). Bu hedef, sanayi sektörünün dijital dönüşüm kapasitesini artırmayı ve YZ tabanlı üretim süreçlerini yaygınlaştırmayı hedeflemektedir.

Belge, e-Devlet süreçlerinin modernizasyonunda büyük veri, bulut bilişim, mobil platformlar, IoT ve YZ uygulamalarından yararlanılmasını öngörmektedir. Bu yaklaşım, kamu hizmetlerinin dijital altyapısını güçlendirmeyi ve hizmet kalitesini artırmayı amaçlamaktadır (SBB, 2019: 182).

Tarımsal alanda da Tarımsal Bilgi Sistemleri (TBS)'nin dijitalleşmesi ve YZ tabanlı karar destek mekanizmalarıyla güçlendirilmesi planlanmıştır. Böylece tarımsal girdi ve ürün fiyatlarındaki dalgalanmalar izlenebilir hale gelecek, üreticiler ve karar vericiler için veri temelli bir izleme altyapısı oluşturulacaktır (SBB, 2019: 88).

Ulusal düzeyde açık kaynak ekosisteminin geliştirilmesiyle yerli YZ yazılımlarına insan kaynağı yetiştirilmesi ve siber güvenlik projeleri kapsamında yüksek katma değerli YZ çözümlerinin açık kaynak kodlu biçimde paylaşılması desteklenmektedir (SBB, 2019, ss. 109-110). Üniversite-sanayi iş birliği ile doktora düzeyinde araştırmacı yetiştirilmesi ve bu araştırmacıların özel sektörde istihdamının teşvik edilmesi de planın bilim-teknoloji eksenindeki önemli hedeflerinden biridir. Aynı doğrultuda YZ odaklı lisansüstü programların sayısının artırılması ve YZ projeleri yürütecek mükemmeliyet merkezlerinin kurulması öngörülmektedir (SBB, 2019: 76).

Son olarak plan, e-Devlet kurumsal mimarisi, ulusal veri envanteri ve açık veri portalı aracılığıyla YZ uygulamalarını besleyecek ortak veri standartları ile paylaşım mekanizmalarının oluşturulmasını hedeflemektedir (SBB, 2019: 183-184).

Genel olarak On Birinci Kalkınma Planı, YZ'ye ilişkin çok katmanlı bir politika çerçevesi ortaya koymakta; stratejik yönelimlerden sektörel uygulamalara, insan kaynağından veri yönetişimine kadar geniş bir yelpazede YZ ekosisteminin bütüncül gelişimini amaçlamaktadır. Bu kapsamda plan, Türkiye'nin yüksek katma değerli üretim ve dijital dönüşüm vizyonunda YZ'nin merkezi rolünü açık ve sistematik biçimde tanımlamaktadır.

#### **3.6.4 Dijital Dönüşüm Ofisi**

24 Ekim 2019 tarihli ve 48 sayılı Cumhurbaşkanlığı Kararnamesi ile Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Başkanlığı (CBDDO) resmî olarak kurulmuş ve görevleri tanımlanmıştır. CBDDO'nun oluşturulması, YZ başta olmak üzere dijital teknolojilerin kamu kurumlarında yaygınlaştırılmasını hızlandırmayı amaçlamaktadır.

Ofisin görevleri arasında kamuda veri analitiği ve YZ uygulamalarının kullanımını teşvik etmek, dijital dönüşüm süreçlerine rehberlik etmek ve veri güvenliği standartlarını güçlendirmek yer almaktadır (CBDDO, 2019). Bu yetki alanı, YZ'nin kurumsal düzeyde

sahiplenilmesi ve politika süreçlerine dâhil edilmesi açısından önemli bir dönüm noktasına işaret etmektedir.

Söz konusu düzenleme, 2019 yılı itibarıyla YZ politikalarının dağınık biçimde yürütülmesi yerine kurumsal bir çatı altında koordine edilmesini sağlamış; böylece YZ'nin kamu yönetimi, dijital hizmetler ve veri yönetişimi alanlarında stratejik bir araç olarak değerlendirilmesinin önünü açmıştır.

### **3.6.5 Ulusal Yapay Zeka Stratejisi Genelgesi**

Daha önceki bölümlerde ve alt başlıklar da açıklandığı üzere, 20 Ağustos 2021 tarihli ve 2021/18 sayılı Cumhurbaşkanlığı Genelgesi ile UYZS resmî olarak yürürlüğe girmiştir. Söz konusu genelge, stratejinin temel çerçevesini duyurmakla kalmamış, aynı zamanda uygulama sorumluluğunu Sanayi ve Teknoloji Bakanlığı (STB) ile Cumhurbaşkanlığı Dijital Dönüşüm Ofisi (CBDDO)'na vermiştir. Bu belge, yürütme erkinin YZ stratejisini tüm kamu kurumlarına tevdi ettiği ilk kapsamlı politika metni niteliğini taşımaktadır.

UYZS'nin uygulanmasını sağlamak amacıyla STB, 2022 ve 2023 yıllarında yayımladığı genelge ve yönetmeliklerle eylem planlarını güncellemiştir. 2023 Cumhurbaşkanlığı Yıllık Programı, stratejinin hedeflerine ulaşılması için yürütülecek projeleri ve faaliyetleri ayrıntılı biçimde listelemiştir (SBB, 2022: 91-362).

Bu çerçevede 2024 yılında, UYZS'nin orta vadeli revizyonu niteliğinde olan 2024–2025 Eylem Planı yayımlanmış ve ilgili kamu kurumlarına dağıtılmıştır. Plan, her bir stratejik öncelik için somut eylemleri, sorumlu ve ilgili kurumları ile performans göstergelerini tablo biçiminde tanımlamaktadır (STB, 2024).

UYZS Genelgesi, bu yönüyle yalnızca stratejik hedeflerin ilanını değil, aynı zamanda uygulama süreçlerinin kurumsal sorumluluklar çerçevesinde somutlaştırılmasını sağlamıştır. Böylece Türkiye'de YZ politikalarının planlama aşamasından yürütme düzeyine geçişi kurumsal bir çerçeveye oturtulmuştur.

### **3.6.6 On İkinci Kalkınma Planı(OKP)**

On İkinci Kalkınma Planı (OKP, 2024–2028), YZ'yi yeşil ve dijital dönüşüm ekseninde rekabetçi üretimin temel itici gücü olarak konumlandırmakta ve bu yaklaşımı 2053 vizyonu ile ilişkilendirmektedir (STB, 2023: 81). Plan, UYZS (2021–2025) ile kurduğu süreklilik sayesinde politika bütünlüğünü korumakta; kurumlar arası veri sözlüğü, güvenli Kamu Veri Alanı (KVA) ve API tabanlı paylaşım altyapıları yoluyla ölçeklenebilir YZ projeleri için sağlam

bir yönetim omurgası inşa etmektedir (STB, 2023: 114-216). Bu veri odaklı mimari, kamu ve özel sektörün yüksek nitelikli verilere erişimini iyileştirerek YZ çözümlerinin hızla ticarileştirilmesini amaçlamaktadır. Planın sektörel boyutu, küçük ve orta ölçekli işletmelerin de içinde yer aldığı tüm imalat kollarında YZ, büyük veri ve otomasyonun entegrasyonunu; model fabrikalar ve beşinci nesil (5G) tabanlı üretim hatlarıyla verimliliğin artırılmasını öngörmektedir (STB, 2023: 8-83).

Eğitim alanında, veriye dayalı yönetim anlayışıyla desteklenen 25.000 doktora mezunu hedefi, nitelikli araştırma-geliştirme (Ar-Ge) iş gücünü besleyen stratejik bir bileşen olarak ön plana çıkmaktadır. Sağlıkta anonimleştirilmiş büyük veri, biyoteknolojik ilaç geliştirme ve robotik uygulamalar aracılığıyla küresel rekabet gücünün artırılması hedeflenmektedir. Dijital devlet ve yargı alanlarında ise e-Devlet kullanım oranının %80'e çıkarılması, sınai mülkiyet tescil süreçlerinin hızlandırılması ve karar destek sistemlerinin YZ tabanlı hale getirilmesi öngörülmektedir (STB, 2023: 3-236).

Savunma, enerji, tarım ve lojistik sektörlerinde yerleştirilmiş çip tasarımı ve sensör teknolojilerinin yaygınlaştırılması stratejinin temel bileşenleri arasında yer almaktadır (STB, 2023: 19-90). Bu çabaları destekleyici biçimde, 2028 yılında devreye alınacak dijital Türk lirası uygulamasının finansal şeffaflığı artırması ve yeşil yatırımları desteklemesi öngörülmektedir. Bununla birlikte, bütüncül siber güvenlik politikaları milli YZ ürünlerinin kullanımıyla bilgi güvenliği standartlarının güçlendirilmesini amaçlamaktadır (STB, 2023: 20-130).

İnsan kaynağı ve inovasyon ekosisteminin güçlendirilmesi kapsamında plan, yeşil ve dijital dönüşüm odaklı 10.000 patent hedefi ile 5.000 uluslararası başvuru öngörmektedir. Kamu-üniversite-sanayi iş birliği ekseninde YZ, siber güvenlik ve savunma sanayisine yönelik yetenek havuzlarının oluşturulması ve yüksek teknoloji ihracatında KOBİ payının %3'e çıkarılması hedeflenmektedir. Ayrıca girişim yatırımlarının 4 milyar ABD dolarına ulaşması ve YZ çip tasarımı ile yarı iletken Ar-Ge çalışmalarının stratejik öncelikler arasında yer alması planlanmaktadır (STB, 2023: 90-128). Son olarak kamu tedarik süreçlerinde güvenilir YZ etik ilkelerinin uygulanması, AB dijital düzenlemeleriyle uyumun sağlanması ve mahremiyete duyarlı açık veri politikalarının benimsenmesi planın temel ilkeleri arasında sayılmaktadır (STB, 2023, ss. 20-72).

Genel olarak OKP, YZ'yi yalnızca bir teknoloji alanı olarak değil, Türkiye'nin uzun vadeli kalkınma vizyonunu yönlendiren stratejik bir kalkınma kaldıracı olarak tanımlamaktadır. UYZS ile kurduğu süreklilik, yönetim yapısı, insan kaynağı politikası, veri ekosistemi ve etik çerçeve arasında güçlü bir eşgüdüm sağlayarak politika bütünlüğünü korumaktadır. Böylece

YZ projeleri için ölçeklenebilir veri altyapısı, nitelikli iş gücü ve yenilikçi girişimler desteklenirken, siber güvenlik ve mahremiyet standartları da kalkınma hedeflerinin ayrılmaz bir parçası haline gelmektedir. Bir bütün olarak değerlendirildiğinde OKP, Türkiye'nin küresel rekabet gücünü artırmayı, sürdürülebilir büyüme ile insan haklarına duyarlı teknoloji yönetimini dengeleyen tutarlı ve ileriye dönük bir YZ politika mimarisi kurmayı hedeflemektedir.

### **3.6.7 TBMM Yapay Zeka Kanun Teklifi ve Yapay Zeka Araştırma Komisyonu**

25 Haziran 2024 tarihli Türkiye Büyük Millet Meclisi (TBMM) Yapay Zekâ Kanun Teklifi, ulusal YZ politikasını yalnızca stratejik belgelerle tanımlanan yumuşak yönetim alanından çıkararak bağlayıcı bir hukuki zemine taşıyan dönüm noktası niteliğindedir. Teklif, YZ'nin güvenli, etik ve adil biçimde kullanılmasını sağlama amacını doğrudan kanun düzeyine yerleştirerek, daha önce UYZS (2021–2025) ve OKP (2024–2028) kapsamında belirlenen ilke ve hedeflere normatif kesinlik kazandırmaktadır. Bu gelişme, yüksek teknoloji yatırımlarını teşvik eden yeşil ve dijital dönüşümle rekabetçi üretim vizyonunun ilk kez yasal düzeyde pekiştirilmesi anlamına gelmektedir.

Kanun teklifi, “YZ sistemi”, “sağlayıcı”, “dağıtıcı” ve “YZ operatörü” gibi temel kavramları tanımlayarak düzenleyici belirsizliği azaltmakta; risk temelli bir sınıflandırma mekanizması aracılığıyla yüksek riskli sistemlere özel kayıt, uygunluk değerlendirmesi ve sürekli izleme yükümlülükleri getirmektedir (TBMM, 2024: 6-13). Bu yaklaşım, hem Avrupa Birliği Yapay Zekâ Tüzüğü ile normatif uyumu güçlendirmekte hem de Türkiye'yi küresel pazarlar açısından teknik mevzuat eşdeğerliğine yaklaştırmaktadır.

Buna paralel biçimde, 35 milyon Türk lirasına veya küresel cironun %7'sine kadar ulaşabilen idari para cezaları(TBMM, 2024: 10), etik ilkelere aykırı ya da yasaklanmış YZ uygulamalarını caydırıcı nitelikte tasarlanmıştır. Bu düzenleme, yüksek riskli teknolojilerin kullanımında hem geliştirici hem de kullanıcı düzeyinde sorumluluk bilincini güçlendirmeyi hedeflemektedir.

Denetim ve uyumluluk hükümleri, strateji belgelerinde yer alan kurumsal yönetim anlayışını somutlaştırarak, ilgili kurumlara geniş denetim ve yaptırım yetkileri tanımaktadır. Bu yönüyle teklif, KVKK ile mevcut veri koruma rejimini YZ bağlamında tamamlayıcı biçimde genişletmektedir. Ortaya çıkan bu bütüncül çerçeve, kullanıcı güvenliğini ve piyasa öngörülebilirliğini artırarak Ar-Ge yatırımlarının önünü açmayı amaçlamaktadır. Yapay Zekâ Kanun Teklifi, Türkiye'nin dijital dönüşüm sürecinde YZ alanındaki kurumsal olgunluğu ileri bir aşamaya taşımakta ve politika–hukuk bütünlüğünü sağlamayı hedeflemektedir. Bu sayede

YZ, yalnızca stratejik planlamanın değil, aynı zamanda hukuki ve etik denetimin de konusu haline gelmiştir.

Bu kanun teklifinin ardından, 2 Ekim 2024 tarihinde TBMM Genel Kurulu'nda alınan kararla, YZ teknolojilerinin toplum, hukuk ve kamu politikalarına etkilerinin incelenmesi amacıyla TBMM Yapay Zekâ Araştırma Komisyonu kurulmuştur. Komisyonun görevi, YZ'nin kamu, özel sektör ve bireyler üzerindeki etkilerini değerlendirmek ve gerekli yasal düzenlemeler konusunda öneriler sunmaktır (Harman, 2025; MDN, 2025).

Komisyonun üyeleri 2025 yılının başında belirlenmiş, uzmanları, kamu kurumlarını ve sivil toplum kuruluşlarını (STK) dinleyerek kapsamlı bir rapor taslağı oluşturmuştur (Mete, 2025; TBMM, 2025). Bu süreç, Türkiye'de YZ politikalarının mevzuat boyutunda sistematik biçimde ele alınmasını sağlayan ilk parlamento girişimi olarak değerlendirilmektedir.

### **3.6.8 183 Sayılı Cumhurbaşkanlığı Kararnamesi**

183 Sayılı Cumhurbaşkanlığı Kararnamesi, Cumhurbaşkanlığı teşkilatında yapılan kapsamlı yeniden yapılandırma sonucunda yürürlüğe girmiştir. Bu düzenleme ile Dijital Dönüşüm Ofisi, İnsan Kaynakları Ofisi ve Finans Ofisi lağvedilmiş, yalnızca Yatırım Ofisi yeniden teşkilatlandırılmıştır. YZ ile dijital dönüşümün eşgüdümünden sorumlu yetkiler, görev alanı genişletilen Siber Güvenlik Başkanlığına devredilmiştir. Böylece Başkanlık, yalnızca siber tehditlerle mücadele eden teknik bir yapı olmaktan çıkarak, kamunun dijital dönüşüm süreçlerine yön verme, e-Devlet hizmetlerinin yaygınlaştırılmasını sağlama ve YZ uygulamalarını teşvik etme görevlerini üstlenmiştir. Bu kurumsal yeniden yapılanma, Başkanlığa güvenlik odaklı işlevlerin ötesine geçen stratejik bir rol kazandırmış; kamu kurumları arasındaki koordinasyonun güçlendirilmesi, veri yönetişiminin bütüncül biçimde yürütülmesi ve yenilikçi teknolojilerin kamu altyapısına entegrasyonu açısından önemli bir adım oluşturmuştur (Dağıstanlı ve Sarica, 2025; ICT Media, 2025).

### **3.7 Türkiye'nin İç Güvenlik Alanına Etki Eden Yapay Zeka Belgeleri ve Stratejileri**

Türkiye'de 2010'lu yıllardan günümüze, savunma ve iç güvenlik alanlarında, siber güvenlikle otonom sistemlere uzanan geniş bir yelpazede, YZ ve dijital teknolojilere ilişkin dijital dönüşüm politikaları şekillendirilmiştir ve şekillendirilmeye de devam etmektedir.

### **3.7.1 Ulusal Siber Güvenlik Stratejisi**

Türkiye'nin ilk ulusal siber güvenlik vizyonu, Ulusal Siber Güvenlik Stratejisi ve 2013–2014 Eylem Planı ile ortaya konmuştur. Strateji, bilgi sistemlerinin giderek artan önemine paralel olarak ulusal siber savunma kapasitesini güçlendirmeyi, kurumlar arasında koordinasyonu sağlamayı ve kesintisiz müdahale kabiliyeti oluşturmayı amaçlamıştır. Bu doğrultuda Ulusal Siber Olaylara Müdahale Merkezi (USOM) ile birlikte kamu, özel sektör ve kritik altyapı işletmelerinde Siber Olaylara Müdahale Ekipleri (SOME) kurulması hedeflenmiştir. Yirmi dokuz maddeden oluşan eylem planı; mevzuatın güncellenmesi, kurumsal kapasitenin artırılması, kritik altyapıların korunması ve nitelikli insan kaynağının yetiştirilmesi gibi başlıkları kapsamaktadır (RG, 2013: 1-30).

Her ne kadar 2013–2014 Stratejisi doğrudan “yapay zekâ” veya “siber hijyen” terimlerini içermese de belgede tanımlanan gizlilik, bütünlük ve erişilebilirlik ilkeleri ile oluşturulan USOM ve SOME ağ yapıları, yürürlüğe konulan yasal düzenlemeler, kapasite geliştirme programları ve standartlaştırma çalışmaları günümüzün YZ destekli savunma ve iç güvenlik sistemlerinin güvenilir, kesintisiz ve hukuka uygun biçimde çalışabilmesi için gerekli altyapıyı oluşturmuştur.

### **3.7.2 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2016-2019**

2016–2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı, yerli ürün ve hizmetlerin kullanımını teşvik ederek teknolojik egemenliğin güçlendirilmesini, araştırma–geliştirme (Ar-Ge) desteklerinin yaygınlaştırılmasını ve siber güvenliğin millî güvenliğin ayrılmaz bir parçası olarak toplumsal düzeyde benimsenmesini hedeflemiştir. Bu çerçevede kritik altyapıların korunması, kurumlar arasında etkin koordinasyon sağlanması ve proaktif siber savunma yeteneklerinin geliştirilmesi planın öncelikli alanları arasında yer almıştır (UDHB, 2016, ss. 11-14).

Strateji, risk yönetimini esas alan ve sürekli değerlendirme ile iyileştirme süreçlerine dayalı bütüncül bir siber güvenlik modeli benimsemiştir. Bu model, değişen tehdit ortamında teknik ve yönetsel önlemlerin sürekliliğini sağlayarak sürdürülebilir bir güvenlik düzeyi oluşturmayı amaçlamıştır. Açıklık analizi ve sertifikasyon çalışmalarının kurumsallaştırılması, tehdit unsurlarının saldırı gerçekleştirmeden önce bertaraf edilmesi ve ulusal düzeyde proaktif savunma kapasitesinin artırılması hedeflenmiştir. Bu yaklaşımla siber güvenlik ekosisteminin güçlendirilmesi, stratejinin temel bileşenlerinden biri olarak tanımlanmıştır (UDHB, 2016: 14).



Belge ayrıca siber güvenlik alanında yetkin personel yetiştirilmesini ve uzmanlaşma teşviklerini ön plana çıkarmış; böylece insan sermayesinin güçlendirilmesiyle birlikte teknolojik projelerin ve kurumsal güvenlik yapısının uzun vadeli sürdürülebilirliği güvence altına alınmıştır (UDHB, 2016: 14).

2016-2019 Stratejisi doğrudan YZ terimini içermese de, belgede yer alan açıklık analizi, risk yönetimi, proaktif savunma, etik yönetim ve bütüncül güvenlik ilkeleri YZ destekli savunma ve iç güvenlik sistemlerinin güvenli, kesintisiz ve hukuka uygun biçimde çalışabilmesi için kurumsal ve teknik bir temel oluşturmuştur. Bu yönüyle strateji, dolaylı biçimde YZ tabanlı sistemlerin korunması, hesap verebilirliğin sağlanması ve etik sorumluluğun kurumsallaştırılması açısından öncül bir referans niteliği taşımaktadır.

### **3.7.3 Türkiye Siber Güvenlik Kümelenmesi Projesi**

Türkiye Siber Güvenlik Kümelenmesi, 2017 yılında Cumhurbaşkanlığı Savunma Sanayii Başkanlığı (SSB) öncülüğünde kurulmuştur. Kümelenme, savunma sanayiinde yerli ve millî yapay zekâ (YZ) ile siber güvenlik teknolojilerinin geliştirilmesini teşvik etmek amacıyla tedarikçiler, girişimciler, akademi ve kamu kurumlarını tek çatı altında bir araya getirmiştir. Bu yapı, Türkiye’de siber güvenlik alanında ekosistem temelli iş birliklerinin güçlendirilmesini, millî ürünlerin rekabet gücünün artırılmasını ve savunma sanayiinde teknoloji tabanlı bağımsızlığın desteklenmesini hedeflemektedir. 1 Şubat 2021 tarihinde SSB ile Cumhurbaşkanlığı Dijital Dönüşüm Ofisi (CBDDO) arasında imzalanan protokol sonucunda Kümelenme, iki kurumun ortak yürütücülüğünde faaliyet göstermeye başlamıştır (Fidancıoğlu, 2025).

Fidancıoğlu’nun belirttiği üzere, Kümelenme’nin 2017’de SSB koordinasyonu ile başlatılması ve 2021’den itibaren CBDDO ile birlikte yürütülmeye başlanması, Türkiye’nin siber güvenlik ve YZ politikalarında kurumsal bütünlüğün sağlanması açısından önemli bir dönüm noktasını temsil etmektedir.

### **3.7.4 Siber Güvenlik Kurulu’nun kaldırılması ve kurumsal değişim**

Siber Güvenlik Kurulu, 2012 yılında kurulmuş ve Türkiye’nin erken dönem siber güvenlik politikalarının koordinasyonundan sorumlu olmuştur. Ancak 2 Temmuz 2018 tarihli ve 703 sayılı Kanun Hükmünde Kararname (KHK) ile Cumhurbaşkanlığı Hükûmet Sistemi’ne geçiş sürecinde kapsamlı bir kurumsal yeniden yapılanma gerçekleştirilmiş, bu düzenleme kapsamında Kurul feshedilmiştir. Kurulun Başbakanlığa bağlı olarak yürüttüğü yetki ve sorumluluklar, söz konusu KHK ile Cumhurbaşkanınca oluşturulacak yeni idari yapılara

devredilmiştir (Fidancıoğlu, 2025). Bu değişim, siber güvenlik alanındaki stratejik koordinasyonun Cumhurbaşkanlığı uhdesinde yeniden yapılandırılmasını ve yetkilerin doğrudan yürütme erki altında toplanmasını sağlamıştır.

Böylece Türkiye’de siber güvenlik politikaları, 2018 sonrasında daha merkezi ve bütünlük bir yönetim yapısı içinde yürütülmeye başlanmış; YZ tabanlı tehditlerle mücadele, dijital altyapıların korunması ve veri güvenliği alanlarında kurumsal sürekliliğin güçlendirilmesi hedeflenmiştir.

### **3.7.5 Ulusal Siber Güvenlik Stratejisi ve 2020-2023 Eylem Planı**

Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020–2023), Türkiye’nin savunma ve iç güvenlik alanında kullandığı YZ tabanlı sistemler için çok katmanlı bir güven ve sürdürülebilirlik çerçevesi oluşturmayı hedeflemiştir. Belgede, “paydaşlar şeffaflığı, hesap verebilirliği ve etik değerleri göz önünde bulundurur” ilkesi vurgulanarak, algoritmaların hukuka ve temel haklara uygun biçimde tasarlanması gerekliliği açıkça belirtilmiştir (UAB, 2020: 18).

Stratejiye paralel olarak geliştirilen YZ destekli AVCI, AZAD ve KASIRGA hızlı tespit ve erken müdahale sistemleri, proaktif savunma yaklaşımının somut uygulamaları olarak öne çıkmıştır. Bu sistemler, kritik ağların 7/24 izlenmesini sağlayarak kesintisiz işleyişi güvence altına almakta ve ulusal güvenlik mimarisine dinamik bir tepki kapasitesi kazandırmaktadır (UAB, 2020: 15). Bu teknik kabiliyetle birlikte, “kritik altyapıların 7/24 korunması” ve “yerli ve millî teknolojik imkânların geliştirilmesi” hedefleri stratejik düzeyde güçlendirilmiştir (UAB, 2020, ss. 15-22).

Strateji aynı zamanda kurumsal sürdürülebilirliği risk temelli yönetim anlayışıyla ilişkilendirmiştir. Belgede “sektörel ve ulusal ölçekte risk yönetimi anlayışıyla tehditlerin en aza indirilmesi” hedefine ve SOME olgunluk ölçümlerine yer verilmiş, düzenli tatbikat ve eğitim döngüsünün YZ savunma kapasitesini dinamik tehdit ortamına uyarlanabilir kıldığı vurgulanmıştır. İnsan kaynağına yönelik programlar, siber güvenlik uzmanlığının kurumsal kültürün bir parçası haline gelmesini sağlayarak uzun vadeli uzman havuzu oluşturmayı amaçlamaktadır (UAB, 2020: 24).

Bu yönüyle strateji, etik ve hukuki ilkeleri, ileri teknik çözümleri ve yetkin insan kaynağını tek çatı altında bütünleştirerek YZ temelli savunma uygulamalarının güvenli, kesintisiz ve sorumlu biçimde işletilmesini mümkün kılan bütüncül bir sistem modeli sunmuştur.

### 3.7.6 Ulusal Siber Güvenlik Stratejisi ve 2024-2028 Eylem Planı

2024–2028 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı, YZ ve büyük veri altyapılarının siber savunma süreçlerine entegrasyonuna dayalı bir mimari öngörmektedir. Belgede, “YZ ve büyük veri altyapılarının değerlendirilmesi ile önemli ölçüde ilerleme kaydedilmesi sağlanacaktır” ifadesiyle bu yönelim açık biçimde belirtilmiştir (UAB, 2024: 17). Aynı bölümde, “sıfır güven (zero trust) yaklaşımının benimsenmesi” ifadesiyle donanım ve yazılım katmanlarına güvenliğin gömülmesi hedeflenmiştir (UAB, 2024: 22).

Planın “Ulusal Siber Güvenlik Hedefleri” başlıklı bölümünde, “ulusal standardizasyon ve test mekanizmalarının geliştirilmesi” hedefiyle yerli ve millî sertifikasyon zincirinin oluşturulması öngörülmüştür (UAB, 2024: 27). “İnsan Odaklı Siber Güvenlik Yaklaşımı” başlıklı kısımda ise bireysel farkındalık ile kurumsal kültürün yerleşmesi ve eğitim-tatbikat döngülerinin yaygınlaştırılması hedeflenmiş, bu sayede insan kaynağının güçlendirilmesi amaçlanmıştır (AUB, 2024a: 13-27).

Belge her ne kadar USOM ve SOME ağlarının organik bir siber güvenlik ekosistemi haline getirilmesinden doğrudan söz etmese de, ulusal ve uluslararası tehdit istihbaratının sürekli akışını sağlama ihtiyacı yönetim katmanının bütüncül modeline uygun bir gereklilik olarak değerlendirilmiştir. Bu bağlamda 2024–2028 Eylem Planı, YZ ve büyük veri temelli erken tespit ve önleme kabiliyetlerini, sıfır güven yaklaşımıyla donanım ve yazılım katmanlarına entegre edilen güvenlik mekanizmalarını, ulusal test ve sertifikasyon süreçlerini, çok katmanlı eğitim-tatbikat döngülerini ve yerli-millî teknolojileri bir araya getirerek savunma ve iç güvenlik ağlarının uçtan uca güvenliğini ve sürdürülebilirliğini sağlamayı amaçlamaktadır.

### 3.7.7 Siber Güvenlik Kanunu No. 7545

7545 sayılı Siber Güvenlik Kanunu, 18 Mart 2025 tarihinde yayımlanmış ve 32846 sayılı Resmî Gazete’de yürürlüğe girmiştir. Kanun metninde doğrudan YZ veya YZ altyapılarına ilişkin bir hüküm bulunmamaktadır. Mevzuatın temel amacı, Türkiye’nin siber uzaydaki millî güvenliğini korumak, siber tehditlerin tespit ve bertarafına ilişkin esasları belirlemek ve Siber Güvenlik Kurulu’nun kuruluşunu düzenlemektir (RG, 2025, Madde 1).

Bununla birlikte kanunun tanımlar bölümü, siber tehdit istihbaratını; “siber uzaydaki varlıklara yönelik mevcut veya potansiyel siber tehdit unsurları ile siber saldırılar hakkında bir araya getirilmiş, dönüştürülmüş, analiz edilmiş, yorumlanmış veya zenginleştirilmiş bilgi” olarak tanımlamaktadır (RG, 2025, Madde 3). Bu tanım, YZ destekli tehdit istihbarat sistemlerinin

devlet düzeyinde kavramsal olarak öngörüldüğünü göstermekte; ancak metin doğrudan YZ teknolojilerine atıfta bulunmamaktadır.

Kanun ayrıca “siber güvenlik millî güvenliğin ayrılmaz bir parçasıdır” ve “hukukun üstünlüğü, temel insan hak ve özgürlükleri ile mahremiyetin korunması ilkeleri esas kabul edilir” ifadeleriyle temel ilkelerini ortaya koymaktadır (RG, 2025, Madde 4). Bu çerçeve, gelecekte geliştirilecek YZ tabanlı siber güvenlik çözümlerinin hukuka uygunluk, etik sorumluluk ve insan hakları temelli ilkelere bağlı biçimde tasarlanması için normatif bir zemin oluşturmaktadır.

Tüm bu bilgiler doğrultusunda 7545 sayılı Kanun, YZ kavramını doğrudan düzenlememekle birlikte; siber tehdit istihbaratının devlet politikası hâline getirilmesi, hukuki ve etik ilkelerin güvenlik uygulamalarına entegre edilmesi ve millî siber güvenlik mimarisinin bütüncül biçimde tanımlanması yoluyla Türkiye’nin YZ eksenine dolaylı biçimde güçlü bir hukuki altyapı ve kurumsal çerçeve kazandırmıştır.

### **3.8 Türkiye’nin İç Güvenlik Alanında Kullandığı YZ Sistemleri ve Uygulamaları**

Türkiye, dijital dönüşüm vizyonu doğrultusunda YZ teknolojilerini ulusal güvenlik stratejisinin temel bileşenlerinden biri olarak konumlandırmıştır. Bu yaklaşım, YZ’nin yalnızca teknolojik kapasiteyi artıran bir unsur değil, aynı zamanda iç güvenlik politikalarının stratejik yapı taşı olarak görülmesini sağlamıştır. UYZS, güncellenen Ulusal Yapay Zekâ Eylem Planı, YZ Taslak Kanunu ve 7545 sayılı Siber Güvenlik Kanunu gibi belgeler aracılığıyla savunma ve güvenlik alanlarında YZ uygulamalarının yasal ve kurumsal çerçevesi oluşturulmuştur. Bu belgeler, insan haklarına duyarlı, güvenilir ve hesap verebilir teknoloji kullanımını teşvik eden ortak bir yönetim zemini inşa etmektedir. Türkiye, SSB, TÜBİTAK ve özel sektör iş birliğiyle savunma ve iç güvenlik alanlarında geliştirilen YZ destekli sistemleri hızla envanterine katmakta; böylece karar süreçlerinde hız, öngörü ve operasyonel etkinliği artıran bütüncül bir güvenlik altyapısı oluşturmaktadır.

#### **3.8.1 İç güvenlikte kullanılabilecek askeri YZ sistemleri**

Türkiye, son yıllarda savunma sanayiinde YZ tabanlı sistemlerin geliştirilmesine hız kazandırmıştır. Türk Silahlı Kuvvetleri (TSK) envanterine giren veya araştırma-geliştirme aşamasında bulunan birçok platformda YZ kabiliyetleri etkin biçimde kullanılmaktadır. Bu sistemler, Türkiye’nin operasyonel karar destek süreçlerinde ve sahadaki durumsal farkındalık kapasitesinde önemli ilerlemeler sağlamaktadır.

HAVELSAN tarafından geliştirilen Bulut Altı keşif ve gözetleme platformu BAHA, 2021 yılında Anadolu Kartalı tatbikatında tanıtılmıştır (Alemdar, 2021; Dougherty, 2025). 2024 yılında ilk partisi TSK'ya teslim edilen sistem, 2023 ve 2024 yıllarında Nijerya ile Orta Asya ülkelerine ihraç edilmiştir (HAVELSAN, 2025). BAHA, sınır güvenliği, keşif-gözetleme, afet yönetimi ve kritik altyapı izleme görevlerinde kullanılmakta ve Türkiye'nin istihbarat toplama kabiliyetini güçlendirmeyi hedeflemektedir (Helou, 2025).

Savunma Teknolojileri Mühendislik ve Ticaret A.Ş. (STM) tarafından geliştirilen döner kanatlı otonom mühimmat sistemi KARGU, 2017 yılında ilk uçuşunu gerçekleştirmiş ve 2018 yılında TSK envanterine girmiştir (STM, 2021). Yükseltilmiş KARGU-2 (Block II) modeli 2019 yılında sahaya çıkarılmış, üçüncü nesil KARGU-3 (Block III) sistemi ise EFES-2024 tatbikatında tanıtılmıştır (Mehmet, 2024). Her iki sistem de ihracat başarısı elde ederek Türkiye'nin otonom sistemler alanındaki küresel görünürlüğünü artırmıştır. KARGU, asimetrik savaş koşullarında personel güvenliğini korumak ve küçük çaplı hedefleri yüksek hassasiyetle imha etmek amacıyla kullanılmaktadır (AT, 2021). KARGU ve BAHA sistemleri birlikte değerlendirildiğinde, Türkiye'nin terörle mücadele, sınır güvenliği, afet yönetimi ve kritik altyapı gözetimi alanlarında birbirini tamamlayan YZ temelli yetenekler kazandığı görülmektedir.

Baykar firmasının Bayraktar TB2, Bayraktar AKINCI TİHA ve Bayraktar TB3 sistemleri; Türkiye'nin İHA-SİHA ekosistemini taktik MALE sınıfından, gemiden kalkabilen TİHA/UCAV segmentine kadar genişleterek keşif-istihbarat, hassas taarruz, SEAD/DEAD ve deniz yetki alanı gözetimi gibi çok katmanlı roller sunmaktadır (Baykar, 2014, 2021, 2023; Özberk, 2025). TB2 modeli, düşük edinim maliyeti ve sahada kanıtlanmış performansıyla Türkiye'nin ihracat başarısında önemli bir rol oynamaktadır. AKINCI, yüksek faydalı yük kapasitesi, gelişmiş görev bilgisayar mimarisi ve havadan-havaya/satha seyir füzesi entegrasyonu ile Türkiye'yi "insansız taarruz uçağı" dönemine taşımıştır (Baykar, 2022). TB3 ise kısa pistli amfibi gemilerden kalkış ve iniş kabiliyeti sayesinde TCG Anadolu'yu insansız hava platformları için bir kuvvet projeksiyon üssü hâline getirmeyi hedeflemektedir (Özberk, 2025). Bu gelişmeler neticesinde Baykar firması, Türkiye'nin hem askeri operasyonel ihtiyaçlarını hem de ekonomik-jeopolitik hedeflerini eş zamanlı desteklemektedir.

Türkiye'nin çok boyutlu güvenlik gereksinimleri terörle mücadele, sınır ve deniz yetki alanlarının korunması, hızla çeşitlenen hava-kara tehdit spektrumu, yerli ve katmanlı bir savunma mimarisini zorunlu kılmaktadır. ASELSAN'ın geliştirdiği HİSAR, GÖKDENİZ,

KORKUT, SARP, İHTAR ve GEZGİN-120 sistemleri, bu gereksinime ortak bir ekosistem yaklaşımıyla yanıt vererek ulusal savunma kapasitesini bütüncül biçimde pekiştirir.

HİSAR hava savunma ailesi, kısa ve orta menzilli tehditlere karşı yerli füze mimarisiyle kritik tesislerin korunmasına hizmet etmektedir (Armyrecognition, 2025). GÖKDENİZ yakın hava savunma sistemi, deniz platformlarının savunma katmanını millileştirerek Türkiye'nin deniz yetki alanlarında caydırıcılığını artırmaktadır (Cankı, 2019). KORKUT, hareketli birlikleri düşük irtifa tehditlerine karşı koruyarak müşterek harekâta manevra kabiliyetini artırmaktadır (Şahin, 2023). SARP uzaktan kumandalı silah istasyonları, personelin doğrudan tehlikeye maruz kalmadan hassas angajman gerçekleştirmesini sağlayarak sınır güvenliği operasyonlarında kuvvet korumasını güçlendirmektedir (Valpolini, 2023). İHTAR sistemi, artan insansız hava aracı tehditlerine karşı modüler ve ölçeklenebilir bir çözüm sunmaktadır (Aselsan, 2024). GEZGİN-120 elektro-optik sensör sistemi ise ileri gözetleme ve hedef işaretleme kabiliyetiyle taktik seviyede durumsal farkındalığı artırmaktadır (Aselsan, 2025).

Bu sistemler bir bütün olarak değerlendirildiğinde, Türkiye'nin savunma sanayiinde YZ tabanlı çözümlerle operasyonel etkinliğini ve stratejik özerkliğini güçlendirdiği görülmektedir. Yüksek yerlilik oranı, lojistik ve siber güvenlik risklerini azaltırken, sürdürülebilir ihracat geliri ve yerli Ar-Ge kapasitesi oluşturma hedeflerini desteklemektedir. Böylece Türkiye, asimetrik savaş koşullarına uyum sağlayan, esnek, katmanlı ve bağımsız bir savunma mimarisi inşa etme yönünde önemli bir aşama kaydetmiştir.

### **3.8.2 İç güvenlikte iç işleri bakanlığına bağlı birimlerde kullanılan YZ uygulamaları**

Türkiye'de YZ teknolojilerinin kullanımı yalnızca askerî alanla sınırlı değildir. İçişleri Bakanlığı koordinasyonunda faaliyet gösteren Emniyet Genel Müdürlüğü (EGM), Jandarma Genel Komutanlığı (JGK), Sahil Güvenlik Komutanlığı ve Göç İdaresi Başkanlığı gibi iç güvenlik kurumları, kolluk faaliyetlerinde YZ tabanlı sistemlerden giderek artan ölçüde yararlanmaktadır.

#### **3.8.2.1 YZ entegrasyonu ve kurumsal dönüşüm**

Türkiye'nin iç güvenlik kurumları, 2010'lu yılların sonundan itibaren veri yoğun operasyonel süreçlerini YZ temelli altyapılarla bütünleştirmeye başlamıştır. Bu dönüşümün kurumsal omurgasını, 2018 yılında hizmete giren Güvenlik ve Acil Durumlar Koordinasyon Merkezi (GAMER) oluşturmuştur. GAMER, yüz tanıma, plaka tanıma ve sosyal medya verilerini 7/24 analiz eden bütünsel bir tahmin ve analiz platformu olarak tasarlanmıştır (İçişleri Bakanlığı, 2018).

### 3.8.2.2 Biyometrik tanıma sistemleri

Türkiye’de biyometrik tanıma kapasitesi, EGM ve JGK başta olmak üzere Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü ile Göç İdaresi Başkanlığı verilerinin entegrasyonu sonucu OPTES–AFİS/APFIS karşılıklı sorgulama mimarisiyle kurumsal düzeyde bütünleşmiştir (Gemici, 2019; İçişleri Bakanlığı, 2019; Papon, 2019). Bu entegrasyonun, soruşturma çevrimini kısalttığı ve delil-şüpheli eşleştirme kapasitesini artırdığı resmi verilerle ortaya konmuştur. 2018’in son iki ayı ile 2019’un ilk ayında 2.765 faili meçhul olay aydınlatılmış, olay yerinden alınan 7.844 iz 3.687 kişiyle eşleştirilmiştir (İçişleri Bakanlığı, 2019). OPTES-AFİS entegrasyonunun ardından 15 ay içinde 12.950 olay çözümlenmiş ve 16.040 şüpheli hakkında işlem yapılmıştır (Gemici, 2019). 2022 yılında İçişleri Bakanlığı tarafından yapılan açıklamaya göre, entegrasyon sonrası terör (3.430), narkotik (8.237) ve asayiş (149.260) dahil olmak üzere toplam 196.852 olayda faillerin tespiti sağlanmış, DNA verilerinin kurumsal entegrasyonu ile yaklaşık 23.715 bulgu irtibatlandırılmıştır (İçişleri Bakanlığı, 2022a). Bu veriler, kurumlar arası veri federasyonu ve birlikte çalışabilirlik sayesinde biyometrik tanımanın Türkiye’nin iç güvenlik mimarisinde çekirdek bir kapasiteye dönüştüğünü göstermektedir.

Yüz tanıma sistemleri ilk olarak pasaport kontrolü ve göç yönetimi gibi alanlarda, ardından iç güvenlik uygulamalarında kullanıma alınmıştır. 2019 yılında İstanbul Havalimanı’nda devreye giren yüz tanıma tabanlı pasaport geçiş sistemi, YZ’nin hem güvenlik etkinliğini hem de işlem hızını artırma potansiyelini somut biçimde ortaya koymuştur (NTV, 2019). Bu gelişme, 2020 yılında Biyoteksan-HAVELSAN ortaklığında geliştirilen Ulusal Biyometrik Veri Sistemi projesiyle güçlendirilmiştir. Proje, yüz, iris ve damar izi gibi çoklu biyometrik modaliteleri tek bir veri havuzunda birleştirmeyi hedeflemektedir (İçişleri Bakanlığı, 2020).

Biyoteksan tarafından HAVELSAN mühendislik desteğiyle geliştirilen yerli parmak izi tanıma altyapısı, Ulusal Biyometrik Veri Yönetim Sistemi kapsamında aşamalı biçimde yaygınlaştırılmıştır. Sistem ilk olarak 26 Mart 2021’de Göç İdaresi Genel Müdürlüğü’nde uygulanmış, 7 Ocak 2022 itibarıyla Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü üzerinden 81 ilde devreye alınmış, Mayıs 2024’te ise EGM tarafından ülke genelinde kullanılmaya başlanmıştır (Yıldırım, 2024). Bu gelişmeler, biyometrik verilerin yerli yazılımlarla bütüncül ve ölçeklenebilir biçimde yönetilerek kurumsal standardizasyonun güçlendirildiğini göstermektedir.

### **3.8.2.3 Gözetim, video analitiği ve plaka tanıma sistemleri**

EGM, şehir meydanları ve kritik kamu alanlarında kurulu MOBESE/KGYS kameralarını 7/24 izleme esasına dayalı olarak kullanmaktadır. Bu sistemin verimliliğini artırmak amacıyla TÜBİTAK 1007 Programı kapsamında 30 Ekim 2013'te yayımlanan çağrı ile "KGYS görüntülerinden anlamlı sonuçlar çıkaracak akıllı analiz yazılımları" geliştirilmesi hedeflenmiştir (TÜBİTAK, 2014). Bu kapsamda ASELSAN ve HAVELSAN gibi savunma şirketleri video analitiği alanına yatırım yapmıştır. HAVELSAN tarafından geliştirilen Eyeminer Video Analiz Sistemi, kamera görüntülerini analiz ederek güvenlik kuvvetlerini ve acil durum ekiplerini anlık olarak uyarmayı amaçlamaktadır (Karakuş, 2023). Sistem, makine öğrenmesi tabanlı nesne ve olay tanıma altyapısıyla sahipsiz paket, kavga, silahlı şahıs ve şüpheli araç gibi durumları gerçek zamanlı olarak algılayabilecek yeteneklere sahiptir.

ASELSAN tarafından geliştirilen Odin Akıllı Video Analiz Birimi gibi YZ modüllerinin KGYS merkezlerine entegre edildiği bilinmektedir (TSKGV, 2024; Yıldırım, 2022). EGM, 7 Mayıs 2025 tarihinde 13.000 yüz tanıma kamerası ve 2.500 ağ anahtarını içeren bir ihale ile KGYS altyapısını ülke genelinde genişletme hedefini sürdürmüştür (Adal, 2025). Jandarma KGYS Projesi kapsamında ise 2023 itibarıyla 11 il ve 20 ilçede tamamlanan kamera kurulumları, pilot uygulama olarak ülke geneline ölçeklenmiştir (İçişleri Bakanlığı, 2023: 49). Ayrıca İçişleri Bakanlığı 2025 yılı içinde tüm kolluk personeline YZ destekli yüz tanıma yaka kamerası tahsis etmeyi planlamaktadır (İstiklal, 2025).

### **3.8.2.4 Öngörüye dayalı analitik ve siber savunma**

Öngörüye dayalı analitik sistemler, iç güvenlik operasyonlarında giderek daha olgun hale gelmiştir. EGM'nin 2024 yılında Antalya'da başlattığı ÖNGÖZ pilot projesi, sosyal medya akışlarını, ihbar metinlerini ve geçmiş suç kayıtlarını analiz ederek coğrafi risk haritaları ve şüpheli profilleri üretmektedir (Adam, 2024). Bu sistem, yasa dışı bahis, dolandırıcılık ve terör propagandası gibi suçları anlık olarak tespit edip ilgili birimlere alarm vermektedir. 2021 yılında Emniyet Narkotik Daire Başkanlığı tarafından geliştirilen ASENSA yazılımı ise makine öğrenmesi ile suç örüntülerini analiz ederek uyuşturucu suçlarında öngörüye dayalı operasyonlara olanak tanımıştır (İçişleri Bakanlığı, 2022b). Mart 2021'den itibaren aktif olan sistem, 14 ay içinde 300 milyon sorgu çalıştırmış ve 9.020 riskli durumu tespit etmiştir. Bu öngörüler doğrultusunda gerçekleştirilen operasyonlarda tonlarca uyuşturucu ve silah ele geçirilmiştir (İçişleri Bakanlığı, 2022b).



JGK tarafından 2023 yılında başlatılan KÂHİN Projesi, hırsızlık, kaçakçılık ve terör gibi suç türlerine ilişkin zamansal ve mekânsal risk modellemesi yaparak önleyici tedbirlerin alınmasını sağlamaktadır (Ünal ve Aslanhan, 2023). Bu sistem, uzmanlar tarafından tanımlanan suç kalıplarını analiz ederek anomalileri tespit etmeye ve erken müdahaleyi mümkün kılmaya yöneliktir.

Ulusal Siber Olaylara Müdahale Merkezi (USOM) tarafından geliştirilen Avcı, Azad, Kasırga, Atmaca ve Kule sistemleri, kritik altyapılarda 7/24 anomali tespiti ve zafiyet taraması yapmaktadır (Aselsan, 2021; AUB, 2024). Ayrıca ASELSAN'ın "Siber Zırh" çözümü, kurum içi savunma katmanlarını risk temelli bir yaklaşımla güçlendirmekte; 2023 yılında Bilgi Teknolojileri ve İletişim Kurumu (BTK) desteğiyle geliştirilen Sosyal Medya Dolandırıcılığı Tespit Sistemi ise afet sonrası artan sahte hesap ve dolandırıcılık vakalarını YZ yardımıyla erken tespit etmektedir (Oktay, 2023).

### **3.8.2.5 Çeşitlenen uygulama alanları**

YZ destekli güvenlik ekosistemi, klasik asayişin ötesinde göç yönetimi, deniz ve kıyı güvenliği ile siber savunma alanlarında da yaygınlaşmaktadır. JGK'nın 2024 yılında başlattığı Jandarma Akıllı Devriye Uygulaması (JADU), devriyelerdeki göğüs kameralarına YZ tabanlı yüz ve plaka sorgulama yeteneği kazandırmıştır. ASELSAN'ın ATEŞ adlı zırhlı mobil gözetleme sistemi, sınır devriye araçlarında sensör verilerini YZ ile işleyerek riskli hareketleri tespit etmektedir (Ekomim, 2025; Yıldırım, 2020).

Kadın Destek (KADES) uygulamasının tek tuşla konum paylaşımına dayalı ihbar sistemi, devriye birimlerinin olay yerine varış süresini belirgin biçimde azaltmıştır (Karadağ, 2025). Göç İdaresi Başkanlığı, 2024 yılında devreye aldığı GöçBil uygulamasıyla yabancı statülü kişilerin işlemlerini hızlandırırken düzensiz göç analizlerini YZ ile otomatize etmektedir (Trthaber, 2024). Aynı yıl başlatılan YZ Destekli Sahil Güvenlik Kıyı Gözetleme Sistemi projesi, radar ve elektro-optik sensör akışlarını akıllı algoritmalarla işleyerek Türk karasularındaki yasa dışı faaliyetleri anlık olarak izlemeyi hedeflemektedir (SGK, 2025: 54-103).

Sınır güvenliği ve göç yönetiminde de 2015 sonrasında özellikle Suriye sınırına yönelik entegrasyon projeleri yürütülmüştür. AB destekli ASELSAN Sınır Gözetleme Projesi (2019–2022), Hakkari'den Edirne'ye 352 kritik noktaya YZ destekli 7/24 izleme sensörleri kurulmuştur (Yıldırım, 2022). Bu kapsamda 4K kameralar, termal sensörler, radar ve akustik algılayıcılar MİRSAD yazılımına entegre edilerek hudut hattında insan/araç tespiti,

sınıflandırması ve atış yeri tespiti otomatik hale getirilmiştir (Yıldırım, 2022). Ayrıca, 2023'te TÜBİTAK tarafından geliştirilen DerinGÖRÜ algoritması, deprem sahalarında refakatsiz çocukların kimlik eşleştirmesinde kullanılmıştır (Denge, 2023).

Bu bütüncül ekosistem, biyometrik tanıma, öngörüşel devriye, çok katmanlı siber savunma ve sınır-kıyı gözetimi gibi işlevleri entegre ederek Türkiye'nin iç güvenlik kapasitesini niteliksel olarak dönüştürmektedir. Bu gelişmeler, kolluk kuvvetlerinin sahadaki etkinliğini artırmakta ve karar alma döngüsünü hızlandırarak veri odaklı güvenlik yönetimi anlayışını güçlendirmektedir.



## 4. TÜRKİYE’NİN İÇ GÜVENLİĞİNDE YAPAY ZEKAYA İLİŞKİN ETİK SORUNLAR

YZ teknolojilerinin iç güvenlik alanına entegrasyonu, güvenlik hedefleri ile temel hak ve özgürlükler arasındaki dengeyi yeniden tanımlamayı gerektiren karmaşık bir süreçtir. Bu nedenle YZ etiği kavramı, tarihsel temelleriyle ele alınmakta; erken dönem tartışmaların günümüz etik çerçevelerine etkisi ortaya konmaktadır. Ardından uluslararası kuruluşların etik ilkeleri ve politika yaklaşımları incelenerek Avrupa Birliği, Elektrik ve Elektronik Mühendisleri Enstitüsü (IEEE), Ekonomik İşbirliği ve Kalkınma Teşkilatı (OECD), Birleşmiş Milletler Eğitim, Bilim ve Kültür Örgütü (UNESCO) ve Birleşmiş Milletler’in (BM) etik perspektifleri değerlendirilmektedir. Bu incelemeyi takiben Türkiye’nin yaklaşımı ile UYZS (2021–2025) kapsamındaki değerler ve ilkeler açıklanmaktadır. Sonraki kısımda, ulusal strateji ile uluslararası etik belgeleri karşılaştırılarak yöntemsel farklılıklar tablo destekli bir biçimde analiz edilmektedir. Bölümün sonunda ise, seçilmiş ülkeler ile Türkiye’nin etik belgeleri benimseme düzeyi karşılaştırmalı olarak sunulmaktadır.

### 4.1 Yapay Zeka Etiği

YZ etiği kavramı yeni değildir; temelleri 20. yüzyılın ortalarındaki düşünsel tartışmalara dayanmaktadır. Etik ilkelerin teknolojik sistemlere uygulanmasına yönelik ilk örneklerden biri, 1942 yılında yazar Isaac Asimov tarafından kaleme alınan Runaround adlı öyküde yer almaktadır. Bu eserde tanıtılan “Üç Robotik Yasası”, robotların insanlara zarar vermesini önlemeye yönelik etik güvenlik ilkelerini ortaya koyarak akıllı makinelere yönelik normatif düşüncenin ilk örneklerinden biri olmuştur (Britannica, 2025a). Bu yasalar kurguya dayanmakla birlikte, sonraki dönemlerde YZ etiği tartışmalarında önemli bir referans noktası haline gelmiştir.

Sibernetik kuramının öncülerinden Norbert Wiener, otonom bilgi işleme sistemlerinin yaşam, sağlık ve mutluluk gibi temel insani değerlere yönelik etkilerini vurgulamış ve etik gözetimin yalnızca arzu edilen değil, zorunlu bir gereklilik olduğunu belirtmiştir (Schriffert, 2018). Wiener’in yaklaşımı, bilgisayar teknolojilerinin toplumsal sonuçlarını sistematik biçimde değerlendiren erken dönem analizlerden birini sunmuş ve ilerleyen yıllarda YZ’ye ilişkin normatif tartışmalara zemin hazırlamıştır.

YZ etiğinin gelişiminde bir diğer dönüm noktası, Joseph Weizenbaum’un Computer Power and Human Reason (1976) adlı eserinde görülmektedir. Weizenbaum, karar verme süreçlerinin

bütünüyle makinelere devredilmesinin insan muhakemesini zayıflatabileceğini belirterek YZ özerkliğinin sınırlandırılması ve insan denetiminin korunması gerektiğini savunmuştur (Capurro, 2022). Bu yaklaşım, insan onurunun ve toplumsal refahın korunması amacıyla etik ilkelerin teknoloji tasarım süreçlerinde öncelikli biçimde gözetilmesi gerektiğini ortaya koymuştur.

Bu erken dönem düşünceler, akıllı sistemlerin etik tasarımının ve sorumlu kullanımının isteğe bağlı bir tercih değil, olası zararları önlemek ve insan haklarını korumak açısından zorunlu bir gereklilik olduğunu vurgulamaktadır. Ancak YZ teknolojisinin henüz sınırlı bir gelişmişlik düzeyine sahip olması nedeniyle bu tartışmalar uzun süre teorik düzeyde kalmıştır. Buna rağmen, YZ etiğinin felsefi temelini oluşturmaya önemli bir katkı sağlamıştır.

YZ etiğine ilişkin çağdaş tartışmalar, 2010’lu yılların başında makine öğrenmesine dayalı uygulamaların sağlık, finans, eğitim ve kamu hizmetlerinde hızla yaygınlaşmasıyla ivme kazanmıştır. Bu dönemde klinik karar desteği, dolandırıcılık tespiti ve kamu hizmetlerinin dijitalleştirilmesi gibi alanlarda toplumsal fayda üreten uygulamalar ortaya çıkarken, aynı teknolojilerin denetlenmediğinde eşitsizlikleri derinleştirme ve hak ihlallerine yol açma riski de fark edilmiştir (IBM, 2024).

2016 yılında ProPublica tarafından yayımlanan araştırma, Amerika Birleşik Devletleri’nde kullanılan COMPAS risk puanlama algoritmasının Siyah sanıkların sistematik biçimde yüksek riskli sınıfa dahil ettiğini ortaya koyarak kamuoyunda geniş yankı uyandırmıştır (Angwin vd., 2016). Bu bulgu, algoritmik kararların şeffaflığına ve hesap verebilirliğine yönelik küresel farkındalığın ivme kazanmasına öncülük etmiştir.

Jobin, Ienca ve Vayena’nın (2019) 84 ulusal ve uluslararası etik rehberi haritalayan çalışması, YZ etiğinin hızla kurumsallaşmakta olduğunu göstermiştir. Araştırmada şeffaflık, hesap verebilirlik, adalet ve insan hakları gibi ilkelerin evrensel bir normatif çekirdek oluşturduğu tespit edilmiştir (Jobin vd., 2019: 390-392).

Bu kurumsallaşma eğilimini izleyen süreçte, 2021 yılında kabul edilen UNESCO, “Yapay Zekâ Etiği Tavsiye Kararı”, insan hakları temelli yaklaşımı resmileştirerek şeffaflık, denetlenebilirlik ve kapsayıcılığı küresel standart haline getirmeyi amaçlamıştır (UNESCO, 2021a). Böylece YZ etiği, toplumsal güvenin tesis edilmesi ve sistemlerin hukuki normlar ile değerler dizgesiyle uyumlu hale getirilmesi için temel bir düzenleyici çerçeveye dönüşmüştür.

Günümüzde YZ etiği, tasarım, geliştirme ve uygulama süreçlerinde temel insani değerleri ve evrensel hakları önceleyen bir normatif ilke bütünüdür. Bu ilkeler, teknolojik

yeniliği ahlaki sorumlulukla dengeleyerek hak ihlali ve toplumsal zarar riskini azaltırken, somut toplumsal faydayı en üst düzeye çıkarmayı amaçlamaktadır (IBM, 2024; UNESCO, 2021a).

2020’li yılların ortasına gelindiğinde YZ etiği, hukuk, sosyoloji ve felsefe gibi disiplinleri kapsayan çok boyutlu bir alan olarak olgunlaşmıştır. Güncel tartışmalar, işe alım veya kredi değerlendirmesi gibi alanlarda kullanılan algoritmik modellerin etik koruma önlemleri olmadan ayrımcılığa ya da gizlilik ihlaline yol açabileceğini vurgulamaktadır. Bu nedenle insan gözetimi, model denetimi ve etki değerlendirmelerinin kurumsal süreçlere entegre edilmesi önerilmektedir (DeMarco, 2024). Böylece YZ etiği, inovasyonu teşvik ederken aynı anda insan onurunu, güvenliğini ve toplumsal adaleti koruyan dinamik bir normatif altyapı olarak konumlanmıştır.

## **4.2 Yapay Zeka Etiğinin Çerçevesi Uluslararası Kuruluşlar**

YZ teknolojilerinin etik, adil ve insan haklarına saygılı biçimde geliştirilmesi ile uygulanması günümüzün en kritik yönetim alanlarından biri haline gelmiştir. Bu doğrultuda, küresel ölçekte ortak bir anlayış ve düzenleyici çerçevenin oluşturulması amacıyla çeşitli uluslararası kuruluşlar rehberlik edici ilkeler ve politika belgeleri yayımlamaktadır. AB, IEEE, OECD, UNESCO ve BM bu alanda öne çıkan kurumlardır. Bu kuruluşlar, YZ’nin yalnızca teknik bir alan olarak değil, toplumsal refah, adalet, güvenlik ve insan haklarıyla doğrudan ilişkili bir dönüşüm aracı olarak ele alınmasını sağlamaktadır. Bu kapsamda geliştirilen etik kılavuzlar hem normatif standartların belirlenmesine hem de teknolojinin sorumlu kullanımına yönelik evrensel bir değer zemininin oluşturulmasına katkı sunmaktadır. Bu girişimler, YZ uygulamalarının teknik güvenliğin ötesinde etik meşruiyet kazanmasına ve toplumla uyumlu biçimde yönetim süreçlerine entegre edilmesine rehberlik etmektedir.

### **4.2.1 Avrupa Birliği**

AB’de YZ yönetişiminin etik çerçevesi, Nisan 2019’da Avrupa Komisyonu bünyesindeki Yapay Zekâ Yüksek Düzeyli Uzman Grubu tarafından yayımlanan Güvenilir Yapay Zekâ için Etik Kılavuzlar ile kurumsal bir yapı kazanmaya başlamıştır. Kılavuz, insan özerkliğine saygı, zararın önlenmesi, adalet ve açıklanabilirlik olmak üzere dört evrensel etik ilkeyi temel alarak bu ilkeleri yedi somut gerekliliğe dönüştürmüştür. Bu gereklilikler; teknik sağlamlık ve güvenlik, gizlilik ve veri yönetimi, şeffaflık, çeşitlilik ve ayrımcılık yapmama, toplumsal ve çevresel refah, insan özerkliği ile denetimi ve hesap verebilirlik başlıkları altında toplanmıştır. Bu ilkeler hem tasarım sürecine hem de sistemlerin yaşam döngüsü yönetimine etik rehberlik sağlamıştır (EC, 2019).

Yönergelerin “yumuşak hukuk” niteliği, Avrupa endüstrisinde gönüllü standartlar oluştururken, aynı zamanda küresel ölçekte diğer devletlerin ve çokuluslu kuruluşların etik kodlarına yön vermiştir. Bu etik çerçeve, 2024 yılında yürürlüğe giren (AB) 2024/1689 sayılı Yapay Zekâ Yasası (AI Act) ile bağlayıcı bir düzenleme haline gelmiştir. Yasa, Avrupa Komisyonu’nun 21 Nisan 2021 tarihli taslağından başlayarak 13 Mart 2024’te Avrupa Parlamentosu tarafından onaylanmış, 21 Mayıs 2024’te Avrupa Birliği Konseyi tarafından kabul edilmiş, 12 Temmuz 2024’te Resmî Gazete’de yayımlanmış ve 1 Ağustos 2024 itibarıyla yürürlüğe girmiştir (EU, 2024a).

AI Act, 2019 tarihli kılavuzda yer alan yedi gerekliliği korumuş ancak bunları risk temelli bir mimariyle hukuki yükümlülüklerle dönüştürmüştür. Bu kapsamda sistemler yasak, yüksek riskli, sınırlı riskli ve asgari riskli olmak üzere dört kategoriye ayrılmış; özellikle yüksek riskli sistemler için güvenlik, şeffaflık ve zorunlu insan denetimi koşulları getirilmiştir. Ayrıca genel amaçlı YZ modelleri için şeffaflık raporlaması ve teknik belgelendirme zorunlulukları tanımlanmış, uygunluk değerlendirmesi, piyasa gözetimi ve caydırıcı yaptırımlar yoluyla hesap verebilirlik güçlendirilmiştir. Böylece 2019 tarihli etik kılavuzun oluşturduğu temel, 2024 düzenlemesiyle normatif kapsamını genişletmiş ve yasal bağlayıcılık kazanarak AB’nin güvenilir YZ vizyonunu tasarımdan uygulamaya kadar bütüncül biçimde somutlaştırmıştır.

#### **4.2.2 Elektrik ve Elektronik Mühendisleri Enstitüsü**

Elektrik ve Elektronik Mühendisleri Enstitüsü (IEEE), otonom ve zekâ sistemlerinin insan merkezli değerlerle uyumlu biçimde tasarlanmasını sağlamak amacıyla Nisan 2016’da IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems programını başlatmıştır. Bu çok yıllık girişim, “etikle uyumlu tasarım” anlayışını somut standartlara ve uygulanabilir kılavuzlara dönüştürmeyi hedeflemiştir. 2016 ve 2017 yıllarındaki taslak sürümlere gelen geri bildirimler doğrultusunda olgunlaştırılan Etik İlkelere Uygun Tasarım (EAD) First Edition belgesi, Mart 2019’da yayımlanmıştır. Beş kıtadan 250’den fazla uzmanın katkısıyla hazırlanan ve yaklaşık 290 sayfa uzunluğundaki bu belge, YZ ekosistemine insan hakları temelli bir vizyon kazandırmıştır (IEEE, 2019: 288).

EAD belgesi, tüm otonom ve zekâ sistemlerinin sekiz temel etik ilkeyi karşılamasını tavsiye etmektedir. Bu ilkeler insan hakları, iyi oluş (well-being), veri ajansı, etkinlik, şeffaflık, hesap verebilirlik, kötüye kullanım farkındalığı ve yeterlilik olarak sıralanmaktadır (IEEE, 2019: 11). Belge, özellikle YZ sistemlerinin uluslararası tanınan insan haklarına saygı göstermesini ve insan refahını önceliklendirmesini zorunlu bir etik koşul haline getirerek, soyut ilkeleri açık teknik hedeflere dönüştürmüştür.

IEEE'nin yaklaşımı, yalnızca normatif ilkelerin belirlenmesiyle sınırlı kalmamış; aynı zamanda bu ilkelerin mühendislik süreçlerinde ölçülebilir standartlara dönüştürülmesini de amaçlamıştır. Bu kapsamda şeffaflık için P7001, veri gizliliği için P7002 gibi alt standartların geliştirilmesine başlanmıştır. Böylece IEEE, “değerleri tasarım kararlarına bağlama” hedefiyle hareket etmiş, ilk aşamada kapsayıcı bir vizyon belgesi yayımlayarak her etik ilkeyi ölçülebilir kriterlere çeviren P7000 standartları ailesini geliştirmiştir (IEEE, 2019: 285-286). Bu yaklaşım, küresel uzman topluluğunu seferber eden açık erişimli bir süreç aracılığıyla YZ etiği tartışmasını normatif düzeyden doğrulanabilir mühendislik uygulamalarına taşımayı başarmıştır.

#### **4.2.3 Ekonomik İşbirliği ve Kalkınma Örgütü**

OECD, YZ alanındaki etik tartışmalarını ilk kez 17 Kasım 2016 tarihinde düzenlenen Technology Foresight Forum etkinliğiyle kurumsal düzeye taşımıştır. Bu forum, YZ'nin ekonomik ve toplumsal etkilerinin tartışıldığı ilk çok-paydaşlı platform olarak, örgütün “güvenilir YZ” anlayışının temellerini atmıştır. Ancak bu kavram o dönemde henüz resmi bir politika terimi olarak kullanılmamıştır. 26–27 Ekim 2017 tarihlerinde gerçekleştirilen AI: Intelligent Machines, Smart Policies konferansı ise, YZ'nin sunduğu fırsat ve risklerin dengeli biçimde yönetilebilmesi için normatif ilkelere dayalı bir politika çerçevesine duyulan gereksinim konusunda uluslararası uzlaşa sağlamıştır. Bu sürecin devamında 2018'de kurulan AI Expert Group at the OECD (AIGO), yürütülen tartışmaları kurumsal bir taslağa dönüştürerek Konsey'e nihai öneriler sunmuştur (OECD, 2024b).

OECD Konseyi, 22 Mayıs 2019 tarihinde beş temel değere dayanan OECD YZ İlkelerini oybirliğiyle kabul ederek tarihteki ilk hükümetler arası YZ etik standardını oluşturmuştur. İlkeler, kapsayıcı büyüme ve sürdürülebilir kalkınma, insan merkezli değerler ve adalet, şeffaflık ve açıklanabilirlik, sağlamlık ve güvenlik ile hesap verebilirlik eksenlerinde sorumlu YZ yönetişiminin çerçevesini tanımlamıştır. Ayrıca, Ar-Ge yatırımlarının artırılması, beceri gelişimi ve uluslararası işbirliğinin güçlendirilmesi gibi politika tavsiyeleri de içermiştir. Bu ilkeler kısa sürede OECD dışındaki ortak ülkelerce de benimsenmiş ve 2019 G20 Osaka Zirvesi'nde “G20 Yapay Zekâ İlkeleri” adıyla kabul edilerek küresel meşruiyet kazanmıştır. Bu gelişme, farklı hukuk geleneklerine sahip ülkeler arasında etik değerler bakımından ortak bir zemin oluşturmuştur (OECD, t.y.).

İlkelerin uygulanmasını sağlamak amacıyla Şubat 2020'de OECD.AI Policy Observatory platformu ile çok-paydaşlı OECD Network of Experts on AI (ONE AI) ağı faaliyete geçirilmiştir (OECD, 2021: 29). Bu yapılar, üye ve partner ülkelerin politika verilerini derleyerek karşılaştırmalı analizler yapmakta, rehber dokümanlar geliştirmekte ve ilkelerin

uygulanma düzeyini izlemektedir. Aynı dönemde başlatılan AI-WIPS programı ise YZ'nin iş gücü, beceriler ve verimlilik üzerindeki etkilerini inceleyerek etik ilkelerin sektörel yansımalarını değerlendirmiştir (OECD, 2021: 67).

Üretken ve genel amaçlı YZ modellerinin yaygınlaşmasıyla birlikte enerji tüketimi, veri yoğunluğu ve dezenformasyon gibi yeni risklerin öne çıkması üzerine OECD, Mayıs 2024'te ilkelerini güncellemiştir. Bu güncelleme kapsamında çevresel sürdürülebilirlik, kapsayıcı büyüme ilkesine dâhil edilmiştir. İnsan merkezli değerler ilkesi, "hukukun üstünlüğü, insan hakları ve demokratik değerlere saygı" biçiminde yeniden formüle edilmiştir. Ayrıca sağlamlık ilkesine güvenli devre dışı bırakma ve bilgi bütünlüğü koşulları eklenmiş; hesap verebilirlik ilkesi ise sürekli risk yönetimi ve sorumlu iş uygulamalarını kapsayacak biçimde genişletilmiştir (OECD, 2024a). Revizyon, beş politika tavsiyesinin bütünlüğünü koruyarak ilke-politika sürekliliğini sağlamış ve hızla evrilen YZ teknolojilerine uyumlu kalmayı hedeflemiştir.

OECD'nin süreç odaklı yaklaşımı, normatif istikrarı ve uyarlanabilirliği birleştirerek YZ etiği yönetişimine esnek ancak güvenilir bir referans çerçevesi kazandırmıştır. Bu yaklaşım, üye ve ortak ülkeler arasında ortak bir etik dilin oluşmasını sağlamış; politika gözlemi, veri paylaşımı ve uzman ağları aracılığıyla ilkelerin uygulanabilirliğini sürekli güçlendirmiştir.

#### 4.2.4 UNESCO

UNESCO Genel Konferansı, 23 Kasım 2021 tarihinde 193 üye devletin oybirliğiyle Yapay Zekâ Etiğine İlişkin Tavsiye belgesini kabul ederek evrensel ölçekte bağlayıcılığı olan ilk YZ etik çerçevesini oluşturmuştur. 2023 yılında Amerika Birleşik Devletleri'nin yeniden üyeliğe dönmesiyle UNESCO'nun üye sayısı 194'e yükselmiştir (M. Lee, 2023).

Bu belge, YZ'nin geliştirilmesi ve kullanımını dört temel değere dayandırmaktadır. Bu değerler; insan hakları ve insan onuru, çevrenin ve ekosistemlerin korunması, kapsayıcılık, barış ve adalet ile kültürel çeşitliliktir. Belge bu temel değerleri, ölçülülük ve zarar vermeme, güvenlik, mahremiyet ve veri koruması, çok paydaşlı yönetişim, sorumluluk ve hesap verebilirlik, şeffaflık ve açıklanabilirlik, insan gözetimi, sürdürülebilirlik, adil erişim ve uluslararası iş birliği olmak üzere on etik ilkeye dönüştürmektedir (UNESCO, 2021a).

UNESCO'nun Yapay Zekâ Etiğine İlişkin Tavsiye belgesi, bu ilkeleri somut uygulama alanlarına taşıyarak politika düzeyinde eylem çağrıları sunmaktadır. Bu uygulama alanları arasında veri yönetişimi, eğitim ve araştırma, çalışma hayatı, sağlık ve refah, kültür ve medya, çevre ve iklim, toplumsal cinsiyet eşitliği, barış ve güvenlik, dijital yönetişim, inovasyon ve



ekonomi ile uluslararası iş birliği yer almaktadır (UNESCO, 2023b: 12). Böylece belge, YZ'nin toplumsal ve ekolojik sistemlerle bütünleşik biçimde ele alınmasını sağlayan kapsamlı bir yönetim çerçevesi oluşturmuştur.

UNESCO ayrıca üye devletlerin bu Tavsiye'yi iç hukuklarına ve ulusal stratejilerine ne ölçüde entegre edebildiklerini değerlendirmek amacıyla iki temel ölçüm aracı geliştirmiştir. Bunlardan ilki, ülkelerin genel kurumsal kapasitesini ölçen makro düzey Hazırlık Ölçüm Metodolojisi (RAM); diğeri ise belirli uygulamaların etik uygunluğunu değerlendirmeye yönelik mikro düzey Etik Etki Değerlendirmesi (EIA) aracıdır (UNESCO, 2023a, 2023a). Bu yöntemler, üye devletlerin etik yönetim kapasitelerini izlemeyi, politika boşluklarını belirlemeyi ve küresel ölçekte normatif uyumu güçlendirmeyi hedeflemektedir.

#### **4.2.5 Birleşmiş Milletler**

BM Genel Sekreteri tarafından Haziran 2020'de yayımlanan Dijital İş Birliği Yol Haritası belgesi, YZ teknolojilerinin küresel yönetiminde insan hakları ve sürdürülebilir kalkınma ilkelerini öncelikli normatif referanslar olarak belirlemiştir. Belgede, YZ uygulamalarının insan haklarını zedelememesi ve Sürdürülebilir Kalkınma Amaçları'na (SKA) hizmet etmesi gerektiği açık biçimde vurgulanmıştır (UN, 2020: 18). Özellikle ölümcül otonom sistemler, yüz tanıma teknolojileri ve dijital kimlik çözümleri gibi alanlarda ciddi etik ve hukuki riskler bulunduğu dikkat çekilmiş; bu tür teknolojilerin uluslararası insan hakları hukuku ile tam uyum içinde tasarlanması ve uygulanması gerektiği ifade edilmiştir.

Belgenin dikkat çeken unsurlarından biri, BM öncülüğünde çok-paydaşlı küresel bir YZ danışma organının kurulmasına yönelik taahhüttür. Bu yapı; üye devletlerin yanı sıra özel sektör, sivil toplum, akademi ve ilgili BM kurumlarının katılımıyla oluşturulacak ve YZ'nin güvenilir, insan haklarına dayalı, barışçıl ve sürdürülebilir gelişimini yönlendirecektir (UN, 2020: 25). Bu yaklaşım, yalnızca teknolojik kapasiteyi değil, aynı zamanda değer temelli dijital yönetimi de öne çıkarmaktadır.

Ekim 2023'te kurulan Yüksek Düzeyli Yapay Zekâ Danışma Kurulu (HLAB-AI), 39 uzmandan oluşan bir kadro ile çalışmaya başlamış ve 2024 yılı içinde yayımladığı Ara ve Nihai Raporlar ile BM'ye "küresel YZ mimarisi"ne ilişkin kapsamlı bir taslak sunmuştur (GPD, 2024; UN, 2024).

BM Genel Kurulu, 21 Mart 2024 tarihinde "Seizing the Opportunities of Safe, Secure and Trustworthy Artificial Intelligence Systems for Sustainable Development" başlıklı ilk YZ kararını oybirliğiyle kabul etmiştir. ABD öncülüğünde hazırlanan ve Çin dâhil 123 ülke

tarafından desteklenen bu karar, BM tarihinde YZ alanında kabul edilen ilk Genel Kurul kararı olması bakımından tarihi bir nitelik taşımaktadır (Lederer, 2024). Karar, insan hakları ve veri koruma ilkelerini yeniden teyit etmekte, dijital uçurumun kapatılmasını ve YZ'nin sürdürülebilir kalkınma hedeflerine ulaşmada kullanılmasını teşvik etmektedir.

Bu karar, BM Genel Kurulu'nun YZ konusunda kabul ettiği ilk karar olması açısından tarihi bir öneme sahiptir. İnsan hakları ve veri koruma ilkelerini teyit etmekte ve dijital uçurumun kapatılmasını hedeflemektedir. Ayrıca, YZ'nin sürdürülebilir kalkınma hedeflerine ulaşmada kullanılmasını teşvik etmektedir.

Uluslararası Telekomünikasyon Birliği (ITU) tarafından 2017'den bu yana yürütülen AI for Good girişimi, BM'ye bağlı 40'tan fazla kurumun standart geliştirme, kapasite inşası ve politika diyalogu ekseninde eşgüdümünü sağlamaktadır. BM'nin 2024 tarihli YZ kararının ardından gerçekleştirilen AI for Good Zirvesinde, yönetişimin yalnızca ilkesel beyanlarla sınırlı kalmaması gerektiği, bunun yerine uygulanabilir ve güvenilir teknik standartlarla desteklenmesi zorunluluğu vurgulanmıştır. Zirve kapsamında düzenlenen "AI Governance Day" etkinliğinde, YZ yönetişiminin "ilkelerden uygulamaya" taşınması gerektiği ve insan merkezli, kapsayıcı standartların hayata geçirilmesi konusunda küresel bir mutabakat çağrısı yapılmıştır (AI for Good, 2024: 2-9).

Ayrıca, ITU, Uluslararası Standardizasyon Örgütü (ISO) ve Uluslararası Elektroteknik Komisyonu (IEC) tarafından başlatılan iş birliğiyle, derin sahte (deepfake) tespiti, dijital filigranlama ve içerik doğrulama konularında küresel teknik standartların geliştirilmesi hedeflenmiştir. Bu girişim, etik ilke ve yönetim normlarının teknik standartlara dönüştürülmesi yönünde somut bir adım olarak değerlendirilmektedir (AI for Good, 2024: 16). Tüm bu gelişmeler, BM'nin YZ kararının yalnızca normatif bir çerçeve değil, aynı zamanda uygulamaya dönük çok taraflı teknik bir dönüşüm sürecinin parçası olduğunu ortaya koymaktadır.

#### **4.3 Türkiye ve Yapay Zeka Etiği**

Türkiye'nin UYZS (2021-2025) hazırlık süreci, uluslararası düzeyde kabul görmüş ilke-temelli YZ etik çerçeveleriyle uyumlu biçimde yürütülmüştür. Bu çerçeveler, OECD, G20, AB ve UNESCO tarafından benimsenen "insan hakları, demokratik değerler ve hukukun üstünlüğü" temelli yaklaşımları içermektedir. Strateji belgesi, "güvenilir ve sorumlu YZ" anlayışını merkeze alarak, merkezi ve yerel kamu kurumları, özel sektör, akademi, sivil toplum ve uluslararası örgütlerin katılımıyla oluşturulan çok paydaşlı bir istişare süreci sonucunda

şekillenmiştir (CDDO ve STB, 2021: 9-58). Bu katılımcı yaklaşımda insan onuru ve toplumsal fayda temel ortak değer olarak benimsenmiş; böylece ulusal vizyon, küresel etik ilkelerle uyumlu biçimde eşgüdüm ve iş birliği ekseninde somutlaştırılmıştır.

UYZS (2021-2025), YZ etiğini teknolojik ilerlemenin insan hakları, toplumsal değerler ve adalet ilkeleriyle uyumlu biçimde ele alınmasını zorunlu kılan çok boyutlu bir alan olarak tanımlamaktadır (CDDO ve STB, 2021: 1-59). Strateji, güvenlik, şeffaflık ve toplumsal faydanın öncelikli kılınmasını; ayrımcılığın ve hak ihlallerinin önlenmesini etik sorumluluğun temel unsuru olarak kabul etmektedir (CDDO ve STB, 2021: 15-61). Etik, bu yaklaşımda yalnızca bir rehber değil, YZ ekosisteminin güvenli, sorumlu ve adil biçimde işlemesini sağlayacak kurumsal bir zorunluluk olarak kavramsallaştırılmıştır.

Strateji, YZ'nin gelişimini yönlendiren dört temel etik değeri şu şekilde tanımlamıştır (STB ve CBDDO, 2021: 59):

- **İnsan Hakları, Demokrasi ve Hukukun Üstünlüğüne Saygı:** YZ sistemleri insan onurunu korumalı, hiçbir aşamada bireylere fiziksel ya da psikolojik zarar vermemelidir.
- **Çevreyi ve Biyolojik Ekosistemi Geliştirmek:** Sistemler, yaşam döngüsü boyunca çevresel sürdürülebilirliği gözetmeli ve doğal kaynakların korunmasını öncelemelidir.
- **Çeşitliliğin ve Kapsayıcılığın Sağlanması:** YZ uygulamaları, ayrımcılığın önlenmesini ve toplumsal çeşitliliğin korunmasını amaçlamalı; dezavantajlı grupların hak ve ihtiyaçlarını gözeterek herkes için adil ve erişilebilir bir hizmet sunmalıdır.
- **Barışçıl, Adil ve Birbirine Bağlı Toplumlarda Yaşamak:** YZ yalnızca zararı önlemeye değil, aynı zamanda pozitif toplumsal ve çevresel katkı sunmaya yönelmelidir. İnsan, doğa ve teknoloji arasındaki etkileşimi bir bütün olarak ele almalı; akıllı olduğu kadar sorumlu ve duyarlı bir aktör olarak tasarlanmalıdır.

UYZS (2021-2025), bu dört temel değeri destekleyen sekiz etik ilke belirlemiş ve bunları yönetim düzeyinde çerçevelemiştir (CDDO ve STB, 2021: 60-61):

- **Ölçülülük:** YZ sistemleri etik ve yasal sınırlar içinde kalmalı; bağlam duyarlılığı gözetilmeli ve insan ile çevreye zarar verme olasılığı bulunan durumlarda önleyici tedbirler alınmalıdır. Kullanılacak yöntemler hem amaca uygun hem de temel değerlere aykırı sonuçlar doğurmayan biçimde seçilmelidir.
- **Emniyet ve Güvenlik:** Sistemler, insanın ve çevrenin güvenliğini tehlikeye atabilecek zafiyetlerden arındırılmalı; sağlamlık ve istikrar ilkeleri esas alınmalıdır. Bu güvenlik yalnızca kullanım anında değil, yaşam döngüsünün tüm aşamalarında risk

değerlendirmeleriyle sürdürülmelidir. Mahremiyeti koruyan ve sürdürülebilir veri yönetimi sağlayan altyapılarla desteklenmesi gerekmektedir.

- **Tarafsızlık:** YZ sistemleri, hukukun üstünlüğü ve temel haklar çerçevesinde, tüm bireylere eşit hizmet verecek biçimde tasarlanmalıdır. Algoritmik kararların herhangi bir grup üzerinde ayrımcılık yaratmaması için izleme ve hesap verebilirlik mekanizmaları sürece entegre edilmelidir.
- **Mahremiyet:** Kişisel verilerin toplanması, işlenmesi ve saklanması süreçlerinde etik ilkeler gözetilmeli; sistemlerin karar mekanizmaları şeffaf ve denetlenebilir olmalıdır. Mahremiyetin korunması, bireylerin özerkliği ve onurunun güvencesidir.
- **Şeffaflık ve Açıklanabilirlik:** YZ sistemlerinin işleyişi anlaşılır olmalı; bireyler algoritmik kararların dayandığı veri ve süreçler hakkında bilgi talep etme hakkına sahip olmalıdır. Bu süreçler teknik uzmanlığı olmayan kullanıcılar için dahi açık biçimde ifade edilmelidir.
- **Sorumluluk ve Hesap Verebilirlik:** YZ sistemlerinin tüm yaşam döngüsünden sorumlu kişi ve kurumların rolleri açık biçimde tanımlanmalıdır. Kararlar ve sonuçları, etki-risk analizine dayalı denetim mekanizmalarıyla izlenmeli ve üçüncü tarafların denetimine açık tutulmalıdır.
- **Veri Egemenliği:** Veri akışı, ulusal mevzuat ve uluslararası yükümlülüklerle uyumlu biçimde yürütülmeli; güvenli veri dolaşımını garanti altına alan teknik ve hukuki önlemlerle desteklenmelidir. Her durumda insan hakları ve etik ilkelere dayalı hak-temelli bir yaklaşım benimsenmelidir.
- **Çok Paydaşlı Yönetişim:** Kamu, özel sektör, akademi, sivil toplum ve bireylerin sürece katılımı, yönetişimin meşruiyetini ve kapsayıcılığını güçlendirmektedir. Bu katılım, teknolojik çözümlerin farklı toplumsal ihtiyaçlarla uyumunu da kolaylaştırmaktadır.

Türkiye'nin etik ilkeleri, yalnızca teknik uyumluluk kontrolü amacı taşımamakta; inovasyon ve ekonomi dengesinde insan haklarını ve kamu yararını öncelemeyi hedefleyen kapsamlı bir yönetişim vizyonu sunmaktadır. İnsan merkezilik ve temel haklara saygı ilkeleri, otomatik kararların nihai denetiminin insanda kalmasını ve algoritmik süreçlerin birey özerkliğini zedeleme riskinin azaltılmasını öngörmektedir. Bu yaklaşım, dijital dönüşüm süreçlerinde toplumsal güvenin güçlendirilmesi ve YZ sistemlerinin demokratik meşruiyetinin artırılması açısından önem taşımaktadır.

Tarafsızlık ile şeffaflık-açıklanabilirlik ilkeleri, sistemlerin denetlenebilirliğini ve hesap verebilirliğini güçlendirmeyi amaçlamakta; vatandaşların hak arama yollarını netleştirirken kurumlara somut sorumluluk yüklemektedir. Mahremiyet, veri egemenliği ve güvenlik ilkeleri ise stratejik verilerin korunması, siber tehditlerin önlenmesi ve veri-enerji maliyetlerinin sürdürülebilir biçimde yönetilmesi bakımından kritik alanlar olarak öne çıkmaktadır.

Çevresel sürdürülebilirlik ve çok paydaşlı yönetim ilkeleri, Türkiye'nin YZ ekosistemini küresel normlarla uyumlu hale getirme yönündeki çabaları desteklemekte; bu doğrultuda ülkenin geleceğin yeşil ve kapsayıcı dijital pazarlarında rekabet gücünü artırması hedeflenmektedir. Akademi, sivil toplum, özel sektör ve kamu kurumları arasında geliştirilen istişare mekanizmaları, etik ilkeleri statik metinler olmaktan çıkararak uygulamaya dönük bir politika döngüsüne dönüştürme potansiyeli taşımaktadır. Bu bağlamda Türkiye, OECD, UNESCO ve AB standartlarıyla kademeli biçimde uyumlu hale gelen, inovasyonu teşvik ederken toplumsal faydayı ve insan haklarını korumayı amaçlayan “güvenilir, adil ve sürdürülebilir YZ” vizyonunu geliştirmektedir.

#### **4.4 Türkiye'nin Ulusal Yapay Zeka Stratejisi Etik İlkeleri ile Uluslararası Etik Çerçevenin Karşılaştırılması**

Türkiye'nin benimsediği YZ etik ilkelerinin şekillenmesinde, ulusal düzenlemelerin yanı sıra uluslararası etik belgeler de önemli bir referans işlevi görmektedir. Ulusal düzeyde geliştirilen stratejik yaklaşımlar, uluslararası normatif çerçevelerde yer alan insan hakları, şeffaflık, hesap verebilirlik ve çok paydaşlı yönetim ilkeleriyle büyük ölçüde örtüşen bir yönelim sergilemektedir. Bu bağlamda, OECD, AB, UNESCO, IEEE ve G20 tarafından geliştirilen etik belgeler, Türkiye'nin UYZS (2021–2025) ile ortak ilkeler üzerinden ilişkilendirilebilir.

Karşılaştırmalı inceleme, ulusal stratejinin bazı etik ilkeleri açık biçimde benimsediğini, bazılarını ise bağlamsal yorumlar aracılığıyla dolaylı biçimde içerdiğini göstermektedir. Etik ilkelerin dağılımı değerlendirildiğinde, “●” işareti ilkenin belgede açık biçimde yer aldığını, “○” işareti dolaylı atıf bulunduğunu, “–” işareti ise herhangi bir tespit yapılamadığını göstermektedir.

Yapay Zeka Etik Çerçevesini Oluşmasını Katkı Sağlayan Uluslararası Kurumlar

Tablo 2.3.1. Yapay Zeka Etik Çerçevesini Oluşmasını Katkı Sağlayan Uluslararası Kurumlar

| İlke / Belge                        | Ulusal YZ<br>Stratejisi<br>(2021-25) | OECD AI<br>(2019) | UNESCO<br>(2021) | G20 AI<br>(2019) | IEEE EAD<br>(2019) | AB AI Act<br>(2024) |
|-------------------------------------|--------------------------------------|-------------------|------------------|------------------|--------------------|---------------------|
| Ölçülülük                           | •                                    | ○                 | •                | ○                | ○                  | •                   |
| Emniyet ve Güvenlik                 | •                                    | •                 | •                | •                | •                  | •                   |
| Tarafsızlık                         | •                                    | •                 | •                | •                | •                  | •                   |
| Mahremiyet                          | •                                    | •                 | •                | •                | •                  | •                   |
| Şeffaflık ve Açıklanabilirlik       | •                                    | •                 | •                | •                | •                  | •                   |
| Sorumluluk ve Hesap<br>Verebilirlik | •                                    | •                 | •                | •                | •                  | •                   |
| Veri Egemenliği                     | •                                    | —                 | ○                | —                | —                  | —                   |
| Çok-Paydaşlı Yönetişim              | •                                    | •                 | •                | •                | ○                  | ○                   |

(Bu tablo tarafımdan oluşturulmuştur)

Ölçülülük ilkesi, incelenen belgelerde kavramsal açıklık, bağlayıcılık düzeyi ve uygulama kapsamı bakımından farklı biçimlerde ele alınmaktadır. UYZS (2021–2025), ölçülülüğü doğrudan tanımlamakta; veri işleme ve karar süreçlerinin yalnızca meşru amaçlar doğrultusunda ve gerekli sınırlar içinde yürütülmesi gerektiğini belirtmektedir (STB ve CBDDO, 2021: 60). AB AI Act ise risk temelli bir mimari benimseyerek ölçülülüğü “orantılı ve etkili bağlayıcı kurallar” aracılığıyla düzenlemekte, bu yönüyle etik ilkedен normatif gerekliliğe geçiş sağlamaktadır (EU, 2024: 7-101). UNESCO, “Proportionality and Do No Harm” başlığı altında hiçbir YZ sürecinin meşru amacı aşmaması ve bağlama uygun olması gerektiğini vurgulamaktadır (UNESCO, 2021b: 20). OECD Tavsiyesi ve onu kelimesi kelimesine devralan G20 AI İlkeleri, risklerin “bağlama uygun mekanizmalar ve sistematik risk yönetimi” yoluyla ele alınmasını önermekte; kavramı doğrudan adlandırmaları da orantılılık anlayışını yansıtmaktadır (G20, 2019: 11-12; OECD, 2019: 8-9). IEEE EAD belgesi ise, “minimum veri” ve dinamik onam çağrılılarıyla ölçülülük ilkesini tasarım düzeyinde

kurumsallaştırmayı önermektedir (IEEE, 2018: 107-108). Bu yönüyle ölçülülük, bağlayıcılığın değişen düzeylerine rağmen tüm belgelerde risk yönetimi ve amaç-araç dengesi ekseninde ortak bir etik yaklaşım olarak yer almaktadır.

Emniyet ve güvenlik ilkesi, incelenen tüm politika belgelerinde ortak bir değer olarak yer almakla birlikte, uygulanma biçimi ve hukuki bağlayıcılığı açısından farklılık göstermektedir. UYZS (2021-2025), bu ilkeyi doğrudan tanımlayarak YZ sistemlerinin sağlam, istikrarlı ve güvenilir biçimde çalışması gerektiğini; ortaya çıkabilecek risklerin sürekli izlenmesi ve yönetilmesi zorunluluğunu vurgulamaktadır (STB ve CBDDO, 2021: 60). AI Act ise bu ilkeyi en ayrıntılı ve bağlayıcı biçimde düzenlemekte; özellikle 15. maddede yüksek riskli sistemlerin doğruluk, sağlamlık ve siber güvenlik açısından yaşam döngüsü boyunca güvence altına alınmasını zorunlu kılmaktadır (EU, 2024: 21-61). OECD ve G20 metinleri, “güvenlik, sağlamlık ve emniyet” değerlerini evrensel bir değer olarak kabul etmekte; öngörülebilir hatalar ve kötüye kullanımlar karşısında sistematik risk yönetimi ve devre dışı bırakma mekanizmalarını önermektedir (G20, 2019: 12; OECD, 2019: 8-9). UNESCO, emniyet ilkesini “Proportionality and Do No Harm” ilkesiyle temellendirerek, YZ sistemlerinin yaşam döngüsü boyunca zarar ihtimaline karşı risk değerlendirmesi ve önleyici tedbirlerin alınmasını etik bir zorunluluk haline getirir. 27. maddede ise bu ilke, güvenlik ve emniyetin sadece fiziksel değil, aynı zamanda çevresel ve dolaylı olarak psikolojik zararları da kapsayacak şekilde genişletilmesini öngörmektedir (UNESCO, 2021b: 20). IEEE EAD, raporu ise sistemlerin arızalandığında güvenli biçimde devre dışı kalmasını, kullanıcı müdahalesine izin vermesini ve saldırılara dayanıklı olmasını önermekte; teknik sağlamlığı etik güvenliğin bir unsuru olarak konumlandırmaktadır (IEEE, 2018: 76-107). Sonuç olarak, AI Act güvenlik ilkesini hukuken bağlayıcı hale getirirken, UYZS bu ilkeyi sürekli risk izleme ve yönetim gerekliliğiyle ulusal bağlama taşır. OECD ve G20 daha çok yol gösterici ve evrensel ilkeler ortaya koyarken, UNESCO insan odaklı “zarar vermeme” anlayışını öne çıkarır; IEEE ise mühendislik rehberi sunar. Tüm belgelerde ortak olan, teknik sağlamlığın ve sürekli risk yönetiminin vurgulanmasıdır; esas fark ise bu gerekliliklerin tavsiye, politika veya yasal zorunluluk olarak ele alınmasındadır.

Tarafsızlık ilkesi, altı temel politika metninde ortak bir değer olarak benimsenmekte; ancak kavramsal derinliği ve yaptırım gücü açısından farklı düzeylerde düzenlenmektedir. UYZS (2021-2025) ilkeyi doğrudan “Tarafsızlık” başlığı altında tanımlar ve YZ kararlarının demografik gruplar üzerinde ayrımcı veya haksız etkiler oluşturmamasını öngörmekte ve bu amaçla sürekli izleme ve düzeltme mekanizmalarının kurulmasını şart koşmaktadır (STB ve

CBDDO, 2021: 60). AI Act, bu kavramı en yüksek bağlayıcılıkla ele almakta; yüksek riskli sistemlerde önyargısız veri seti kullanımını zorunlu kılmakta ve sosyal skorlama ile hassas biyometrik kategorizasyon gibi uygulamaları sınırlamaktadır (EU, 2024: 52-27). OECD ve G20 AI İlkeleri hukukun üstünlüğü ve insan hakları ilkeleriyle bağlantılı olarak adalet ve ayrımcılık yapmama yönünde politika çağrısında bulunmaktadır (G20, 2019: 12; OECD, 2019: 8-9). UNESCO (2021) ise madde 28-29’da “AI aktörleri her türlü ayrımcılığı en aza indirmekle yükümlüdür” diyerek kapsayıcı erişim, etkili telafi mekanizmaları ve yaşam döngüsü boyunca önyargı azaltma önlemleri getirir (UNESCO, 2021b: 20). Mühendislik odaklı EAD doğrudan “ayrımcılık yapmama, eşitlik, kapsayıcılık” ilkesini savunur; ayrıca P7003 Algoritmik Yanlılıkla İlgili Hususlar standardına atıfla şirketlere algoritmik önyargı denetimi ve etik denetim çağrısında bulunur (IEEE, 2018: 4-185). Sonuç olarak, AI Act veri önyargısı analizini zorunlu kılarak ve belirli ayrımcı uygulamaları kısmen yasaklayarak en sert hukuki çerçeveyi sunar; UYZS benzer kavramsal kapsamı somut politika hedefleriyle ulusal düzeye taşır fakat yaptırım mekanizmasını henüz “yumuşak hukuk” seviyesinde bırakır. UNESCO insan-merkezli kapsamı derinleştirirken, OECD/G20 çok-paydaşlı risk yönetimiyle küresel politika standardı oluşturur; IEEE ise pratik tasarım rehberliği sağlayarak teknik topluluğun önyargı sorumluluğunu kurumsallaştırır. Böylece tarafsızlık ilkesi, kavramsal ortaklığa rağmen belge-belge değişen bağlayıcılık ve uygulama araçlarıyla katmanlı bir küresel etik mimarisi ortaya koyar.

Mahremiyet ilkesi, belgeler arasında normatif güç bakımından farklılık gösterse de tamamlayıcı bir tutarlılık içinde ele alınmaktadır. UYZS (2021-2025) mahremiyeti doğrudan bir başlıkta tanımlar; kişisel verilerin “toplanmasından silinmesine” kadar tüm döngüde gizlilik gözetimini, “gizlilik tasarımdan itibaren” yaklaşımıyla KVKK (6689)’a da atıfta bulunarak kısmen zorunlu yapar. AI Act, mahremiyet ilkesini bağımsız ve ayrı bir etik ilke olarak öne çıkarmaktan ziyade, AB’nin köklü veri koruma mevzuatıyla eksiksiz biçimde bütünleşerek sistemin temeline yerleştirir. AI Act, gerekçe 10’da bu bütünleşmeyi açıkça vurgularken, gerekçe 69 ve m.2(7)-(12) gibi düzenlemelerle veri minimizasyonu gibi ilke ve yükümlülükleri YZ sistemlerinin tüm yaşam döngüsüne bağlayıcı olarak yayar. Böylece mahremiyet, AI Act’in mimarisinde doğrudan “etik ilke” olarak değil; ancak AB’nin veri koruma hukukuyla sıkı bağlarla, teknik ve organizasyonel zorunluluklar şeklinde, dolaylı fakat en güçlü bağlayıcı normlardan biri olarak kurumsallaşır (EU, 2024: 3-46). Bu mimari sayesinde, YZ sistemlerinde mahremiyet koruması yalnızca teorik bir etik değer olmaktan çıkıp, hukuken zorunlu, uygulamada sürekli izlenebilir ve denetlenebilir bir norm haline gelmiştir. OECD değerler bölümünde “insan hakları, demokratik değerler ve mahremiyet dahil veri koruması” hükmünü bütün paydaşlara yönelik



temel ilke olarak yerleştirir (OECD, 2019: 8). Bu metnin G20 versiyonu da kamu yararı için açık veri çağrısını “gizlilik ve veri korumasına saygı” şartına bağlayarak yineler (G20, 2019: 11-13). UNESCO, mahremiyet ilkesini yalnızca teknik bir gereklilik olarak değil, doğrudan insan onuru, özerklik ve eylemlilikle bağlantılı temel bir insan hakkı olarak çerçeveler. Ayrıca 32, 33 ve 34. maddelerde, kişisel verilerin toplanması, kullanımı, arşivlenmesi ve silinmesi süreçlerinde uluslararası veri koruma standartlarına uygun bir yönetim yapısının kurulması önerir. Mahremiyeti, YZ sistemlerinin tüm yaşam döngüsü boyunca korunmasını etik bir yükümlülük haline getirir (UNESCO, 2021: 21-22). Böylece mahremiyet, yalnızca bireysel bir koruma alanı değil, aynı zamanda YZ sistemlerinin insan haklarına uygunluğunu sağlayan temel bir ilkedir. IEEE EAD (2019) raporu, teknik düzeyde 'Kişisel Veri Hakları ve Bireysel Erişim Kontrolü' bölümünde asgari veri ilkesini, dinamik rıza yönetimini ve P7002 'Veri Gizliliği Süreci' standardını önererek mühendislik süreçlerine mahremiyet kontrolleri gömer (IEEE, 2018: 6-106). Bu çıkarımlar, mahremiyet ilkesinin tüm belgelerde açıkça yer aldığını gösterir; ancak normatif kuvvet ve ayrıntı seviyesi değişir: UYZS ve AI Act somut yasa-regülasyon bağlantısıyla en yüksek bağlayıcılığı sunarken, UNESCO ve OECD/G20 evrensel hak çerçevesi çizip uygulamayı üye devletlere bırakır; IEEE ise geliştirme pratiğine odaklanarak teknik rehberlik sağlar. Böylece AB-Türkiye ekseninde güçlü bir “yatay uyum” zemini oluşurken, uluslararası yumuşak hukuk metinleri kavramsal tutarlılık ve iyi uygulama repertuarı sunar.

AI Act, insanla etkileşimli ve yüksek-riskli sistemlere şeffaflık etiketi, kayıt tutma ve karar izlenebilirliği yükümlülükleri getirerek en yüksek hukuki zorunluluk düzeyini oluşturur (EU, 2024: 49-83). UNESCO, şeffaflık ve açıklanabilirliği insan haklarının korunmasının önkoşulu olarak tanımlar. Bu ilkeleri yalnızca teknik düzeyde değil; adalet, hesap verebilirlik ve demokratik denetim gibi boyutlarıyla birlikte ele alarak en kapsamlı etik çerçevelerden birini sunar (UNESCO, 2021b: 22). OECD ve G20 AI ilkeleri, şeffaflığı YZ sistemlerinin anlaşılabilirliğini ve hesap verebilirliğini sağlayan bir unsur olarak tanımlar; bu yönüyle şeffaflık, temel hakların etkin şekilde kullanılabilmesine katkı sunan bir araç işlevi görür (G20, 2019: 11; OECD, 2019: 8). IEEE, “Algoritmik Şeffaflık” ilkesini etik açıdan önceler ayrıca P7001 standardı aracılığıyla bu ilkenin tasarım sürecine teknik ölçütler ve olgunluk seviyeleriyle entegre edilmesini önerir (IEEE, 2018: 30-69). UYZS (2021-2025), bu ilkeye ayrı bir başlıkta değinmektedir. YZ sistemlerinin “neden, nasıl, nerede ve hangi amaçla” bilgileri kullandığını son kullanıcıya sunmayı hedefler (STB ve CBDDO, 2021: 61). Bu kapsamda, şeffaflık ilkesi küresel ölçekte normatif bir süreklilik oluşturmakta; AB’nin bağlayıcı yapısı ile

UNESCO’nun geniş etik çerçevesi arasında Türkiye stratejisi yumuşak-zorunlu bir denge sunmaktadır.

Sorumluluk ve Hesap Verebilirlik ilkesi, altı temel belgenin tamamında ortak payda olmakla birlikte bağlayıcılık ve teknik ayrıntı bakımından katmanlı bir yapı sergiler. AI Act, kavramı doğrudan başlıklandırmasa da kalite-yönetim sistemi ile her bir rolün görev tanımını, kayıt tutma ve AB veri tabanına açık beyan yükümlülüklerini belirleyerek; ayrıca sürekli gözetim ve geri çağırmaya imkan veren “Pazar sonrası izleme” düzeniyle hesap verebilirliği sert hukuk düzeyine çıkarır (EU, 2024: 62-101). OECD ve G20 AI ilkeleri aynı numaralı maddelerde 'YZ aktörleri rollerine uygun olarak sistemin düzgün işleyişinden ve etik ilkelerin uygulanmasından sorumludur' diyerek izlenebilirlik-risk yönetimi zincirini öngörür (G20, 2019: 12; OECD, 2019: 9). UNESCO, 42 ve 43. madde de insan hakları temelli sorumluluğu nihai olarak insan aktörlere bağlar; kapsamlı etki analizi, denetim, ihbarcı koruması ve düzenleyici kum havuzları çağrısıyla karma denetim modelini detaylandırır (UNESCO, 2021: 22-23). IEEE EAD (2019), hesap verebilirliği sadece kavramsal bir etik değer olarak değil, aynı zamanda mühendislik süreçlerine entegre edilmesi gereken somut pratikler olarak tanımlar. Geliştirici-operatör zincirinin şeffaf ve sorumlu biçimde kurgulanması çağrısında bulunur (IEEE, 2018: 27-160). UYZS (2021-2025), ilkeye doğrudan bir başlık altında yer vermiştir. YZ sistemlerinin yaşam döngüsü boyunca insan denetimi, izlenebilirlik ve üçüncü taraf denetimini tabi olmalı gerektiği ayrıca amaç kısmında algoritmik hesap verebilirlik rehberleri ve denetim araçları geliştirme sözü verir (STB ve CBDDO, 2021: 61-72), fakat bağlayıcı yaptırımı gelecek ikincil mevzuata bırakır. Bu bilgiler doğrultusunda, AI Act, rol-bazlı zorunlu uyum mekanizmasıyla en yüksek hukuki seviyeyi, UNESCO’nun insan hakları odaklı en geniş çerçeveyi, OECD/G20’nin çok-paydaşlı politik standardı ve IEEE’nin teknik uygulama rehberini sunduğunu; Türkiye’nin ise ulusal stratejide kavramsal uyumu sağlamakla birlikte, hesap verebilirliği sertifikasyon veya sektör-üstü otorite yoluyla bağlayıcı kılacak düzenleyici boşluğu halen doldurması gerektiği gözlenmektedir.

Veri egemenliği ilkesini açık biçimde yalnızca UYZS (2021-2025)’de başlıklaştırılır; strateji, kritik verilerin yerli altyapıda saklanması ve veri diplomasisi geliştirilmesini ulusal stratejik çıkar olarak konumlandırır (STB ve CBDDO, 2021: 61). UNESCO, “ulusal egemenliği” 49-50 ve 52. maddeler arasında uluslararası hukuk bağlamında tanıyarak kavrama doğrudan “sovereignty” ifadesiyle atıf yapar, ancak ilkeyi başlıklaştırmaz (UNESCO, 2021b: 26). OECD ve G20 metinleri veri koruma güvenceli serbest sınır-ötesi veri akışı kavramını (G20, 2019: 3), IEEE ise ilkeyi “bireysel veri ajansı” olarak savunur; hiçbir “data sovereignty” terimini kullanmaz (IEEE, 2018: 109). AI Act, GDPR uyumlu veri yönetişimi ve birlik içinde serbest

veri dolaşımı ilkelerine odaklanır; metinde egemenlik söylemi yer almaz (EU, 2024: 4-57). Bu doğrultuda, veri egemenliğinin şu aşamada Türkiye’ye özgü ve AB’nin serbest akış paradigmasıyla potansiyel müzakere gerektiren bir politika alanı olduğunu ortaya çıkarır.

Çok-Paydaşlı Yönetişim ilkesi, OECD tarafından ilk taslaktan nihai kabul aşamasına kadar katılımcı bir süreçle geliştirilmiş; bu ilke, ‘tüm paydaşlara açık ve disiplinler arası diyalog’ anlayışıyla hem hazırlık sürecine yön vermiş hem de II. Bölüm, 2.5 numaralı hükümde ulusal politikalara yönelik bir tavsiye olarak kurumsallaştırılmıştır (OECD, 2019: 3-10). G20 AI ilkeleri, Osaka Zirvesi’nde bu metni benimseyerek hükümetleri uluslar-ötesi, sektörler-arası, açık çok-paydaş girişimleri desteklemeye çağırır (G20, 2019: 2-14). UNESCO, 54., 55. ve 56. maddelerde ‘katılımcı, çok düzeyli ve çok-paydaşlı yönetim’ anlayışını etik yönetişimin temel bileşeni olarak tanımlamaktadır. Belge, ulusal strateji metinlerinden etik sertifikasyon süreçlerine kadar her aşamada kamu, özel sektör, sivil toplum ve akademinin temsil edildiği kapsayıcı mekanizmaların oluşturulmasını önermektedir (UNESCO, 2021b: 27). IEEE, geliştirici topluluğuna dönük olarak etik inceleme kurulları, atölyeler ve kamu katılımı yoluyla “çeşitli disiplin ve toplumsal bakış açılarını sisteme dahil eden” gönüllü standartlaştırmayı önerir (IEEE, 2018: 5-70). AI Act, resmi otoriteler ile paydaşların bir arada yer aldığı karma bir yönetim mimarisi kurmaktadır. Bu kapsamda, Üye Devlet temsilcilerinden oluşan AI Board ile dengeli sivil ve ticari katılıma dayalı Advisory Forum’u çift kanatlı bir katılımcı yapı olarak tasarlamaktadır. Bununla birlikte, ulusal ‘AI regulatory sandbox’ların çok-paydaşlı yapıya sahip olması, yasal düzenlemeyle güvence altına alınmıştır (EU, 2024: 88-97). UYZS (2021-2025), çok paydaşlı yönetim ilkesini hem ilkesel düzeyde hem de kurumsal yapı önerisi olarak ele almaktadır. Şekil 22 ve 23’te tanımlanan Yönlendirme Kurulu, YZ Ekosistemi Danışma Grubu ve Eylem Planı Koordinasyon Grupları, sadece kamu temsilcileriyle değil, özel sektör, STK’lar ve akademiyle de iş birliği içinde çalışacak şekilde yapılandırılmıştır (STB ve CBDDO, 2021: 62-85). Ancak bu yapılar henüz yasal olarak tanımlanmış kurumsal yapılar değil, strateji düzeyinde önerilen yönetim bileşenleridir. Sonuç olarak UNESCO metni ilkeyi en geniş normatif kapsamla tanımlarken, OECD/G20 uluslararası politika koordinasyonunun omurgasını oluşturur; AI Act bağlayıcı bir yarı-katılımcı model çizer; IEEE teknik topluluk merkezli gönüllü standartlar önerir; UYZS ise ulusal ölçekte somut kurumlaşmış mekanizmalar getirmekle birlikte, yeni kurum yapılanmaları ışığında katılımcılık düzeyini koruma gereksinimi taşır.

Yapılan karşılaştırmada, Türkiye’nin YZ etiği prensiplerinin OECD, UNESCO, IEEE, AB ve G20 gibi uluslararası kaynaklardan doğrudan etkilendiğini göstermektedir. Bu etkiler, ulusal stratejinin hem kavramsal yönelimini hem de uygulama hedeflerini şekillendirmekte;

Türkiye'nin etik ilkeleri küresel normatif sistemle bütünleşik bir yapıda konumlandırılmaktadır.

#### 4.5 Seçilmiş Ülkeler ve Türkiye'nin Uluslararası Etik Belgelerle Karşılaştırılması

Bu bölümde, her bir ülkenin beş uluslararası YZ etik ve düzenleyici belgesini nasıl benimsediği tablo halinde sunulacaktır. Ardından, tablodan ortaya çıkan benzerlik ve farklılıkları sistematik biçimde ele alarak, incelenen altı ülkenin YZ etiğine yaklaşımındaki ortak yönleri ve ayrışan noktaları ayrıntılı olarak değerlendirilecektir.

Tablo 3.3.2. Tablo Seçilmiş Ülkeler ve Türkiye'nin Uluslararası Etik Belgelerle Karşılaştırılması

| Ülke \ Belge | IEEE EAD | OECD AI İlkeleri | UNESCO AI Tavsiyesi | AB AI Act | G20 AI İlkeleri |
|--------------|----------|------------------|---------------------|-----------|-----------------|
| Türkiye      | ○        | ✓                | ✓                   | ●         | ✓               |
| ABD          | ●        | ✓                | ○                   | ●         | ✓               |
| Çin          | ○        | ●                | ✓                   | ●         | ✓               |
| Japonya      | ○        | ✓                | ✓                   | ●         | ✓               |
| G. Kore      | ○        | ✓                | ✓                   | ●         | ✓               |
| Hindistan    | ○        | ●                | ✓                   | ●         | ✓               |

(Tablo tarafımdan oluşturulmuştur.)

(Simgelerin Anlamı  
 ✓ Resmen kabul etmiş    ● Dolaylı benimsemiş    ● Destekleyici / kısmen uygulamış  
 ● Alternatif sistem geliştirmiş    ○ Sessiz / resmi atıf yok)

IEEE EAD belgesi, devletler tarafından doğrudan resmi olarak ulusal mevzuat veya politika belgelerine atıf yapılan bir metin değildir. Ancak, EAD'de yer alan uzmanların OECD, Avrupa Komisyonu'nun Yüksek Düzeyli Yapay Zeka Uzman Grubu(HLEG) ve IBM gibi kuruluşlarda da aktif rol oynaması sayesinde gibi kuruluşlarda aktif rol üstlenmeleri, bu belgede geliştirilen etik ilkelerin ve bilgi birikiminin söz konusu kurumların YZ etik politika geliştirme süreçlerine dolaylı biçimde yansıdığını göstermektedir. Bu nedenle, EAD'nin küresel ölçekte önemli bir başvuru kaynağı olarak değerlendirildiği ve etik politika üretiminde dikkate alınan bilgi

kaynaklarından biri olarak kabul edildiği görülmektedir (Havens, 2019). EAD’de ortaya konan ilkelerin, Google, Microsoft ve IBM gibi teknoloji şirketlerinin YZ etik rehberlerinde ve kurumsal etik komitelerinde dolaylı biçimde referans alındığı anlaşılmaktadır (Singh, 2025). Ayrıca, ABD ordusuna hizmet sağlayan Microsoft’un, şirket içinde IEEE EAD ilkelerinden esinlenen etik prensipleri benimsemesi, bu çerçevenin ABD kamu kurumlarının YZ uygulamaları üzerinde dolaylı bir etkiye sahip olabileceğini düşündürmektedir (Reuters, 2025a).

OECD ilkeleri, Türkiye, ABD, Japonya ve Güney Kore’nin de aralarında bulunduğu 39 OECD üyesi ülke tarafından Mayıs 2019’da YZ alanındaki ilk uluslararası hükümetler arası prensip seti olarak onaylanmıştır (NTIA, 2019). OECD üyesi olmayan Çin ve Hindistan bu prensipleri doğrudan imzalamamıştır; ancak aynı ilkeleri G20 platformu aracılığıyla dolaylı biçimde benimsemiştir. 2019 Osaka Zirvesi’nde Çin ve Hindistan’ın, G20 ülkeleriyle birlikte OECD’nin hazırladığı insan merkezli YZ prensiplerini G20 İlkeleri adıyla destekledikleri görülmektedir (Arcesati, 2021; MOFA, 2019).

UNESCO YZ Etiği Tavsiyesi, Kasım 2021’de 193 üyenin oy birliği ile kabul edilmiştir. Seçili ülkeler arasında yalnızca ABD, 2017 yılında UNESCO’dan ayrıldığı için 2021 tarihli bu küresel YZ etik tavsiyesine taraf olmamıştır. ABD’nin 2023 yılında UNESCO’ya yeniden katılma kararı almasının ardından Temmuz 2023 itibarıyla üyeliği resmen yeniden başlamıştır (Euronews, 2023). Bununla birlikte, UNESCO belgesinin ABD’de ulusal düzeyde doğrudan referans alınmadığı görülmektedir.

Türkiye’nin Avrupa Birliği ile sürdürdüğü ticari ve ekonomik ilişkiler, AB’nin AI Act düzenlemesinin Türkiye’deki YZ uygulamaları üzerinde dolaylı etkiler yaratabileceğini göstermektedir (Candan, 2024). Türkiye’nin, söz konusu düzenlemeye ilişkin olarak “iç pazarın işleyişinin geliştirilmesi” ve “insan odaklı, güvenilir YZ teknolojilerinin benimsenmesi” hedeflerine vurgu yapan değerlendirmeleri, AB mevzuatına yönelik olumlu bir yaklaşım sergilediğini düşündürmektedir (ABB, 2024). AB’nin yasa ile öne çıkardığı temel hakların, güvenliğin ve çevrenin korunmasına ilişkin ilkelerin Türkiye tarafından da benimsendiği göz önüne alındığında, bu düzenlemenin dolaylı biçimde desteklendiği söylenebilir.

ABD ile AB arasında YZ risk yönetimi alanında kavramsal düzeyde önemli bir uyum bulunduğu, her iki aktörün de risk temelli yaklaşımı ve güvenilir YZ’nin temel ilkelerini benimsediği görülmektedir. Bununla birlikte, uygulama düzeyinde iki sistem arasında yapısal açıdan belirgin farklılıklar ortaya çıkmaktadır. Brookings Enstitüsü’nün analizleri, AB’nin bütüncül ve zorunlu bir düzenleme olan AI Act’i benimsemesine karşın, ABD’nin daha çok

sektörel düzenlemeler, mevcut kurumsal yapıların uyarlanması, gönüllü standartların, örnek olarak NIST Risk Yönetim Çerçevesi gibi, teşviki ve Ar-Ge yatırımlarının artırılması gibi esnek politika araçlarını tercih ettiğini göstermektedir. Bu durum, ABD'nin doğrudan mevzuat çıkarmak yerine, mevcut düzenleyici yapıların geliştirilmesine öncelik verdiğini göstermektedir (Engler, 2023).

Çin, AB'nin AI Act kapsamında yürürlüğe koyduğu kapsamlı düzenlemeyi yakından izlemekte, ancak kendi hukuki ve ekonomik sistemine uygun özgün bir düzenleyici çerçeve geliştirmektedir. AB'nin AI Act'ini, genel bir yasa oluşturmaktan ziyade belirli YZ uygulamalarına yönelik özel kurallar getirmektedir. Çin'in yaklaşımı ise YZ yönetiminde devlet kontrolünü, ulusal güvenliği ve toplumsal istikrarı merkeze alan bir yapıya dayanmaktadır (Arcesati, 2021). Bu durum, AB'nin temel haklar odaklı ve risk temelli denetim yaklaşımından belirgin biçimde ayrıştığını göstermektedir. Çin, AI Act'ini ne resmen desteklemiş ne de reddetmiştir; bunun yerine kendi iç düzenlemeleriyle uyumlu, paralel bir sistem oluşturmuştur. Bu sistem, etik ilkeler bakımından AB ile bazı ortak yönler taşısa da uygulama düzeyinde devletin merkezi rolünü koruması açısından farklılık göstermektedir.

Japonya, AB'nin AI Act düzenlemesini yakından izlemekte ancak mevcut aşamada benzer biçimde kapsamlı ve yatay bir yasal çerçeve oluşturmak yerine esnek ve sektör bazlı bir yönetim modeli benimsemektedir. Japon hükümetinin YZ regülasyonunda uyguladığı “agile governance” yaklaşımı, şirketlerin gönüllü uyumunu ve çok paydaşlı diyalogu esas almakta; bağlayıcı hükümler yerine rehber ilkeler ve sektöre özgü düzenlemelere ağırlık vermektedir. Bu yaklaşım, inovasyonu teşvik etmeyi ve düzenlemelerin teknolojik gelişmelere uyumlu biçimde güncellenmesini amaçlamaktadır. Japonya, OECD ve G20 ilkeleriyle uyumlu olarak şeffaflık, güvenlik ve hesap verebilirlik değerlerine öncelik vermekte; yüksek riskli YZ uygulamaları için rehberler hazırlamakta ve gerektiğinde sektörel yasalarda güncellemeler yapmaktadır. Ayrıca Japonya, AB ve diğer G7 ülkeleriyle teknik standartlar ve uluslararası iş birliği alanlarında ortak hedefler doğrultusunda hareket etmekte, YZ alanında insan haklarının korunması ve güvenilir teknolojilerin teşviki yönündeki hedefleri paylaşmaktadır. Bununla birlikte, ulusal düzeyde Japonya, AB'nin katı ve bağlayıcı düzenlemeleri yerine inovasyonu destekleyen ve dinamik bir regülasyon tarzını sürdürmektedir (Habuka, 2023).

Güney Kore, AB'nin AI Act düzenlemesini doğrudan iç hukukuna aktarmamış olsa da insan hakları ve güvenliğe dayalı risk sınıflandırma modelini politika tasarımıyla önemli bir referans noktası olarak değerlendirmektedir. Bilim ve BT Bakanlığı'nın “Herkes için Güvenilir YZ Stratejisi” belgesinde, AB'nin Nisan 2021 tarihli AI Bill taslağı ayrıntılı biçimde tanıtılmış ve

yüksek riskli sistemlere ilişkin yükümlülüklerin Kore açısından kritik bir örnek teşkil ettiği belirtilmiştir (MSIT, 2021). Bu yönelim, 22 Ocak 2026’da yürürlüğe girecek Yapay Zekânın Geliştirilmesi ve Güven İnşasına İlişkin Temel Kanun (AI Basic Act) ile kurumsallaşacaktır. Söz konusu kanun, risk değerlendirmesi, şeffaflık ve kullanıcı bilgilendirme yükümlülükleri getirerek AB’nin risk temelli yaklaşımıyla içeriksel paralellik göstermektedir. Kore İletişim Komisyonu’nun 28 Şubat 2025’te yayımladığı Üretken YZ Hizmetleri için Kullanıcı Koruma Kılavuzu ise insan onuru, önyargıların önlenmesi ve açıklanabilirlik ilkelerine dayanarak AI Basic Act’i tamamlayıcı gönüllü standartlar ortaya koymaktadır (Kimchang, 2025). Dolayısıyla Güney Kore, AI Act’i küresel bir referans çerçevesi olarak görmekte; benzer risk temelli ilkeleri inovasyonu destekleyen ve esnek bir düzenleme ekosistemi içinde uygulamayı tercih etmektedir.

Hindistan, AB’nin AI Act düzenlemesiyle aynı kapsam ve bağlayıcılığa sahip bir mevzuat oluşturmuş değildir; ancak tüzüğün risk temelli yaklaşımını ve temel hakları koruma amacını paylaşmaktadır. Bilişim Bakan Yardımcısı Rajeev Chandrasekhar, Tokyo’daki 2023 GPAI toplantısında “yeterli korkuluklar sağlayarak YZ’nin gücünü insanlık yararına kullanma” gereğini vurgulamış ve bu yönüyle AB’nin zarar önleyici yaklaşımına açık destek vermiştir (IndiaAI, 2022). Bununla birlikte, Yeni Delhi ağır düzenlemeler yerine inovasyonu teşvik eden esnek bir yaklaşım benimsemekte, 2023 yılında Parlamento’da yaptığı açıklamada “YZ büyümesini düzenleyecek ayrı bir yasa düşünmüyoruz” ifadesiyle bu tutumunu ortaya koymaktadır. Mart 2024’te yayımlanan, yüksek riskli sistemleri tanımlayıp daha sonra geri çekilen tavsiye metni de aynı yaklaşımın bir yansıması olmuştur (Mohanty ve Sahu, 2024). Aynı doğrultuda, İletişim ve BT Bakanı Ashwini Vaishnaw, Ekim 2024’te “AB ve ABD’deki kadar sıkı YZ düzenlemeleri Hindistan için uygun değildir; inovasyona alan bırakılmalıdır” açıklamasını yapmıştır (Lobo, 2024). Bu doğrultuda Hindistan, AI Act’in hedeflediği insan hakları ve güvenlik odaklı ilkeleri ilkesel düzeyde desteklemekte; ulusal kalkınma önceliklerine uygun, esnek ve sektörel temelli bir düzenleyici ekosistem geliştirmekte, kapsamlı bir AB tipi yasa yerine mevcut yasaları ve gönüllü çerçeveleri uyarlayarak koruyucu bir politika yapısı oluşturmaktadır.

Seçilmiş ülkeler ve Türkiye, 2019 yılında Osaka’da düzenlenen G20 Zirvesi’nde YZ için belirlenen ilkeleri konsensüsle kabul etmiştir (MOFA, 2019).

## 5. SONUÇ

Bu tez, YZ'nin Türkiye'nin iç güvenlik alanına entegrasyonunu etik yönetim odağında incelemektedir. Çalışma, YZ'nin karar döngüsünü hızlandırdığını, tehdit tespitini güçlendirdiğini ve operasyonel erişimi genişlettiğini göstermektedir. Bulgular, ABD, Çin, Hindistan, Güney Kore ve Japonya örnekleriyle örtüşmüş, küresel eğilim doğrulanmıştır. Türkiye, UYZS, OKP ve ilgili düzenlemelerle YZ'yi stratejik bir öncelik olarak tanımlamıştır. SSB, TÜBİTAK ve yerli sanayi iş birliği, envanterde YZ tabanlı çözümleri yaygınlaştırmıştır. GAMER temelli kurumsal omurga, KGYS, biyometrik tanıma, akıllı video analitiği, plaka tanıma, öngörüsül polislik ve siber savunma araçları ile bütünleşmiştir. Bu mimari, birlikte çalışabilir yapılarla karar süreçlerini kısaltmış ve sahada ölçülebilir etkinlik üretmiştir.

Etik yönetim açısından genel çerçeve büyük ölçüde şekillendirilmiştir. UYZS, insan hakları, demokrasi, hukukun üstünlüğü ve çevresel sürdürülebilirliği temel değerler olarak tanımlar. Ölçülülük, emniyet-güvenlik, tarafsızlık, mahremiyet, şeffaflık-açıklanabilirlik, sorumluluk-hesap verebilirlik, veri egemenliği ve çok-paydaşlı yönetim, ilke setini oluşturur. Bu yaklaşım, AB, OECD, UNESCO, IEEE ve BM ile genel uyum içindedir. Karşılaştırmalı analiz, uyum düzeyinin yüksek olduğunu, fakat bağlayıcılık, denetim ve standardizasyon alanlarında güçlendirme gereksinimi bulunduğunu göstermektedir. AI Act, risk temelli bağlayıcı hükümlerle güvenlik ve şeffaflık yükümlülüklerini somutlaştırmaktadır. Türkiye'de 2024 tarihli Yapay Zekâ Kanun Teklifi ile 2025 tarihli Siber Güvenlik Kanunu önemli adımlardır. Yüksek riskli kullanım alanlarında anlamlı insan denetiminin kapsamı, sorumluluk zincirinin işleyişi ve hesap verebilirlik süreçleri açık ve ölçülebilir protokollerle tanımlandıkça kurumsal öngörülebilirliğin güçlenmesi beklenmektedir.

Türkiye'nin veri egemenliği vurgusunun güçlü olduğu görülmektedir. UYZS, kritik verilerin yerli altyapılarda korunmasını ulusal düzeyde stratejik bir çıkar olarak konumlandırmaktadır. Bu tercih, AB'nin veri serbestisi yaklaşımı ile müzakere gerektiren bir fark yaratmaktadır. KVKK, açık rıza, veri minimizasyonu ve veri güvenliği ilkeleri ile sağlam bir dayanak sunmaktadır. İç güvenlikte kullanılan biyometrik sistemler, yüz tanıma, video analitiği ve öngörüsül polislik, büyük hacimli kişisel veriye erişim gerektirmektedir. Bu gereksinim, veri egemenliği hedefi sürerken dahi mahremiyet riskleri doğurabilir. Uluslararası örnekler, kitlesel gözetim tartışmalarının hızla meşruiyet sorununa dönüştüğünü göstermektedir. Bu nedenle tasarımdan itibaren mahremiyet yaklaşımı zorunlu hale gelmelidir. Kurumlar, veri yaşam döngüsünün her aşamasında minimizasyon, amaçla sınırlılık ve güvenlik kontrollerini



işletmelidir. YZ projelerinde sistematik mahremiyet etki değerlendirmesi yürütülmelidir. Sonuçlar, bağımsız denetime açılmalı ve düzenli şeffaflık raporları ile kamuoyuna sunulmalıdır. KVKK ile uyumlu kurumsal standartlar, disiplinler arası etik kurulların gözetiminde uygulanmalıdır.

Anlamlı insan denetimi konusu, YZ'nin güvenlik alanındaki kullanımında giderek daha fazla önem kazanmaktadır. Türkiye'nin YZ destekli askeri ve iç güvenlik sistemlerinde otonomi düzeyi artmaktadır. Sivil kayıpları önlemek, suistimalleri engellemek ve Uluslararası İnsancıl Hukuk(IHL) ile uyumu korumak için insan-içi-döngü ilkesi açık biçimde tanımlanmalıdır. Kural setleri, devre dışı bırakma yetkisi, görev iptali ve anomali tespiti için insan müdahalesi, zorunlu asgari gereklilikler olarak belirlenmelidir. Kayıt tutma, izlenebilirlik ve olay sonrası denetim, uygulama zorunluluğuyla güvenceye alınmalıdır. Model kartları, veri kartları ve değişiklik günlükleri, teknik izlenebilirlik altyapısını tamamlamalıdır. Bu unsurlar, hesap verebilirlik mekanizmalarını somutlaştırmakta ve hatalardan öğrenmeyi kurumsallaştırmaktadır.

Çok-paydaşlı yönetim anlayışının uygulama düzeyinde güçlendirilmesi önem taşımaktadır. UYZS'de önerilen yapıların yasal bağlayıcılığa kavuşması gerekmektedir. Bağımsız bir Ulusal YZ Etik ve Yönetişim Kurulu kurulmalıdır. Kurul, STK, akademi, meslek örgütleri, ilgili kamu birimleri ve sektör temsilcilerinden dengeli bir katılım ile yapılandırılmalıdır. Kurul, yüksek riskli projelerde ön etki değerlendirmesini yapmakla yükümlü olmalıdır. Uygunluk denetimlerini yürütmeli ve şeffaflık raporlarını izlemelidir. İhlal durumlarında yaptırım tavsiyesi sunmalı ve iyi uygulama rehberlerini yayımlamalıdır. Bu yönetim modeli, toplumsal güvenin artmasına ve meşruiyet düzeyinin güçlenmesine katkı sağlayacaktır.

İnsan kaynağı boyutu, YZ ekosisteminin sürdürülebilir gelişimi açısından stratejik bir öneme sahiptir. UYZS, istihdam ve mezun hedefleri ile nicel kapasiteyi artırmayı amaçlamaktadır. Bu hedefin nitelik boyutu güçlendirilmelidir. Kamu, akademi ve özel sektörün ortaklığıyla disiplinler arası eğitim ve araştırma merkezleri kurulmalıdır. Bu merkezler, YZ etik uzmanları, veri bilimcileri, hukukçular, sosyologlar ve güvenlik analistlerini aynı programlarda buluşturmalıdır. TÜBİTAK ve YÖK iş birliği ile YZ Etiği ve Yönetişimi başlıklı lisansüstü programlar teşvik edilmelidir. Kurum içi sertifika programları, proje yaşam döngüsüne gömülü etik ve hukuk modülleri ile zorunlu hale getirilmelidir. Bu yaklaşım, saha uygulamalarında standartlaşmayı hızlandıracak ve olası risklerin azaltılmasına yardımcı olacaktır.

Teknik ve kurumsal standartların birbirini tamamlayacak biçimde eşzamanlı olarak geliştirilmesi önem taşımaktadır. Yüksek riskli projelerde veri yönetişimi politikaları, güçlü anonimleştirme, erişim kontrolü, güvenli model yaşam döngüsü ve saldırı dayanımı gerektirmektedir. Adalet ve tarafsızlık ölçümleri düzenli olarak raporlanmalıdır. Pilot uygulamalar, sınırlı bir ölçekte yürütülmeli; elde edilen verilerle sistemin gerçek dünyadaki teknik, etik ve toplumsal etkileri ayrıntılı biçimde değerlendirilmelidir. Sonuçlar, tekrarlanabilirlik ilkesiyle doğrulanmalıdır. Tedarik süreçleri, etik ve hukuk kriterleri içeren ihale şartnameleri ile güncellenmelidir. Ürün kabul testleri, güvenlik ve etik uygunluk metriklerini içermelidir.

Türkiye'nin YZ tabanlı iç güvenlik mimarisi, stratejik uyum ve kurumsal kapasite bakımından son yıllarda önemli bir ilerleme göstermektedir. Ulusal belgeler ve kurumsal stratejiler, uluslararası etik ve normatif çerçevelerle yüksek bir yakınsama düzeyi sergilemektedir. Bununla birlikte, bağlayıcı kuralların kapsamının genişletilmesi, bağımsız denetim mekanizmalarının kurumsal güvence altına alınması, yüksek riskli sistemlerde anlamlı insan denetiminin açık biçimde tanımlanması ve mahremiyetin tasarımdan itibaren güvenceye alınması geliştirilmeye açık başlıca alanlardır.

Veri egemenliği ilkesinin, KVKK ile uyumlu mahremiyet standartlarıyla birlikte işletilmesi, meşruiyetin ve toplumsal güvenin güçlendirilmesi açısından belirleyici önemdedir. Çok-paydaşlı yönetim yapılarının yasal zemine taşınması hem uygulama kapasitesini artıracak hem de kurumsal sürekliliği teminat altına alacaktır. Disiplinler arası insan kaynağı programlarının oluşturulması ise bu dönüşümün kalıcı hale gelmesini sağlayacaktır.

Bu tez, söz konusu alanlarda kanıta dayalı bir değerlendirme çerçevesi sunmakta ve uygulanabilir politika önerileri geliştirmektedir. Sonuçlar, Türkiye'nin güvenilir, hak-uyumlu ve hesap verebilir bir YZ ekosistemi kurmasına katkı sağlayacak niteliktedir. Gelecek çalışmalarda, kurumsal denetim mekanizmalarının etkinliği, toplumsal algı dinamikleri ve saha temelli metriklerin uzun dönemli etkileri ölçülerek bu çerçeve daha da derinleştirilebilir.

## KAYNAKÇA

360. (2025, Şubat 11). 360 Küresel Gelişmiş Tehdit Araştırması Raporunu Yayımladı: Ülkemdeki 14 Önemli Endüstri Yabancı APT Tehditleriyle Karşı Karşıya. <https://360.net/about/news/article67adb367acc2700020e0e9ad>
- ABB. (2024, Temmuz 12). AB Yapay Zeka Yasası Yayımlandı. [https://www.ab.gov.tr/ab-yapay-zeka-yasasi-yayimlandi\\_53836.html](https://www.ab.gov.tr/ab-yapay-zeka-yasasi-yayimlandi_53836.html)
- Abby. (2021, Ocak 4). Shakey the Robot Explained: Everything You Need to Know. History-Computer. <https://history-computer.com/technology/shakey-the-robot/>
- ACLU. (2006, Kasım 26). Automated Targeting System. American Civil Liberties Union. <https://www.aclu.org/documents/automated-targeting-system>
- Adal, H. (2025, Mart 27). Emniyet, 13 bin kameralık yüz tanıma sistemi alımı için ihale açtı. <https://bianet.org/haber/emniyet-13-bin-kameralik-yuz-tanima-sistemi-alimi-icin-ihale-acti-305918>
- Adam, G. (2024, Mayıs 25). Siber polisin sanal devriyesinde suçlular “Öngöz”e takılıyor. <https://www.aa.com.tr/tr/gundem/siber-polisin-sanal-devriyesinde-suclular-ongoze-takiliyor/3230051>
- AI for Good. (2024). 2024 AI for Good Global Summit Snapshot Report. AI for Good. <https://aiforgood.itu.int/newsroom/publications-and-reports/>
- AIDA. (2021, Nisan 26). The Republic of Korea –“Pali-Pali” Innovation. Ai4da.Com. <https://ai4da.com/south-korea/>
- AIID. (2019, Haziran 1). Incident 441: Korea Developed ID Screening System Using Airport Travelers’ Data without Consent. <https://incidentdatabase.ai/cite/441/>
- Akbulut, U. (2012). İLK MEKANİK HESAP MAKİNESİNİ PASCAL İCAT ETTİ. <https://www.uralakbulut.com.tr/wp-content/uploads/2012/12/pascal.pdf>
- Akın, E., & Şahin, M. E. (2024). Derin Öğrenme ve Yapay Sinir Ağı Modelleri Üzerine Bir İnceleme. <https://dergipark.org.tr/tr/pub/emobd/issue/83029/1338066>
- Aksu, M., & Karaköse, E. (2022). İnsansız Hava Araçlarında Pekiştirmeli Öğrenme Kullanılarak. [https://fen.firat.edu.tr/subdomain\\_files/fen.firat.edu.tr/files/28/UH\\_83.pdf](https://fen.firat.edu.tr/subdomain_files/fen.firat.edu.tr/files/28/UH_83.pdf)
- Alasu, S., & Talu, M. F. (2024). Bilgisayarlı Görüde Öz-Denetimli Öğrenme Yöntemleri Üzerine Bir İnceleme. Düzce Üniversitesi Bilim ve Teknoloji Dergisi, 12(2), 1136-1165. <https://doi.org/10.29130/dubited.1201292>
- Alemdar, A. (2021, Haziran 30). HAVELSAN’ın B30 Bulut Altı İnsansız Hava Aracı (BİHA) Anadolu Kartalı 2021 Tatbikatı’nda. DefenceTurk. <https://www.defenceturk.net/havelsan-bulut-alti-insansiz-hava-araci-biha-anadolu-kartali-2021-tatbikatinda>
- Allen, G., & Chan, T. (2017). Artificial Intelligence and National Security. National Security.
- Amitabh, U. (2018, Haziran 14). India is a latecomer to AI. Here’s how it plans to catch up. World Economic Forum. <https://www.weforum.org/stories/2018/06/india-latecomer-artificial-intelligence-niti-aayog/>
- Andersen, R. (2020, Temmuz 29). The Panopticon Is Already Here. The Atlantic. <https://www.theatlantic.com/magazine/archive/2020/09/china-ai-surveillance/614197/>
- Anduril. (2024, Eylül 26). Anduril Deploys 300th Autonomous Surveillance Tower (AST), Advancing Capability for Border Security. <https://www.anduril.com/anduril-deploys-300th-autonomous-surveillance-tower-ast-advancing-capability-for-border-security/>

- Angwin, J., Larson, J., Mattu, S., Kirchner, L., & ProPublica. (2016, Mayıs 23). Machine Bias. ProPublica. <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>
- Apple. (2017, Haziran 5). HomePod reinvents music in the home. Apple Newsroom. <https://www.apple.com/newsroom/2017/06/homepod-reinvents-music-in-the-home/>
- Arcesati, R. (2021, Haziran 24). Lofty principles, conflicting incentives: AI ethics and governance in China | Merics. <https://merics.org/en/report/lofty-principles-conflicting-incentives-ai-ethics-and-governance-china>
- Armutlu, D. A. (2024, Aralık 7). Çin'in 2030 Yapay Zekâ Stratejisi: Küresel Liderliğe Doğru - Uluslararası Diplomatik İlişkiler, Akademik Araştırmalar ve Eğitim Derneği. <https://udiad.org/cinin-2030-yapay-zeka-stratejisi-kuresel-liderlige-dogru/>
- Armyrecognition. (2025, Şubat 10). Hisar-A A+ SAM. <https://armyrecognition.com/military-products/army/air-defense-systems/air-defense-vehicles/hisar-a-short-range-surface-to-air-defense-missile-system-data>
- Arslan, A. C. (2024). Tekno-Politik Rekabette QUAD Cephesi: 2024 Liderler Zirvesinin Söyledikleri. Kriter Dergi. <https://kriterdergi.com/dis-politika/tekno-politik-rekabette-quad-cephesi-2024-liderler-zirvesinin-soyledikleri>
- Artlab EPFL. (2018). Thinking Machines. Ramon Llull and the ars combinatoria. EPFL. [https://www.epfl.ch/campus/art-culture/ramon-llull\\_en/](https://www.epfl.ch/campus/art-culture/ramon-llull_en/)
- Aselsan. (2021, Ekim 14). Siber Zırh Programı. [https://cdn.aselsan.emrg.me/api/file/SIBER\\_ZIRH\\_TR-\(1\)-\(1\).pdf](https://cdn.aselsan.emrg.me/api/file/SIBER_ZIRH_TR-(1)-(1).pdf)
- Aselsan. (2024, Ekim 22). ASELSAN LAUNCHES NEW ANTI-DRONE SYSTEMS AT SAHA EXPO. Aselsan. <https://www.aselsan.com/en/news/detail/235/aselsan-launches-new-antidrone-systems-at-saha-expo-2024>
- Aselsan. (2025, Nisan 9). GEZGİN 120. Aselsan. <https://www.aselsan.com/tr/savunma/urun/3804/gezgin-120>
- AT. (2021, Haziran 4). Kargu Rotary-Wing Attack Drone, Turkey. Airforce Technology. <https://www.airforce-technology.com/projects/kargu-rotary-wing-attack-drone/>
- AUB. (2024, Ekim 16). Sosyal Medya Tehdit Alanı Olmayacak—Bütün Haberler—Strateji Geliştirme Başkanlığı. <https://sgb.uab.gov.tr/haberler/sosyal-medya-tehdit-alani-olmayacak>
- Austin, D. (2025, Mayıs 30). Japan's AI Promotion Bill and How It Differs from the EU AI Act. <https://ediscoverytoday.com/2025/05/30/japans-ai-promotion-bill-and-how-it-differs-from-the-eu-ai-act-artificial-intelligence-trends/>
- Aydin, A. H., & Özel, M. (2016). Türkiye'de İç Güvenlik Aktörlerinin İç Güvenlik Yönetiminde Halka Hesap Verebilirlik Sorununa İlişkin Algıları ve Çözüm Önerileri. [https://dergi.kmu.edu.tr/userfiles/files/2016Aral%C4%B1k/6-M\\_%20%C3%96zel\\_T%C3%BCrkiye'de%20%C4%B0%C3%A7%20G%C3%BCvenlik.pdf](https://dergi.kmu.edu.tr/userfiles/files/2016Aral%C4%B1k/6-M_%20%C3%96zel_T%C3%BCrkiye'de%20%C4%B0%C3%A7%20G%C3%BCvenlik.pdf)
- Banerjee, A. (2025, Nisan 11). Eyes That Think: AI-Driven ISR is Reshaping the Indian Army's Operational Edge. The Sunday Guardian Live. <https://sundayguardianlive.com/investigation/eyes-that-think-ai-driven-isr-is-reshaping-the-indian-armys-operational-edge>
- Baptista, E. (2022, Nisan 8). Insight: China uses AI software to improve its surveillance capabilities. Reuters. <https://www.reuters.com/world/china/china-uses-ai-software-improve-its-surveillance-capabilities-2022-04-08/>
- Baughman, J. (2024). The Path to China's Intelligentized Warfare: Converging on the Metaverse Battlefield. [https://cyberdefensereview.army.mil/Portals/6/Documents/2024-Fall/Baughman\\_CDRV9N3-Fall-2024.pdf](https://cyberdefensereview.army.mil/Portals/6/Documents/2024-Fall/Baughman_CDRV9N3-Fall-2024.pdf)

- Bayes, T., & Price, null. (1997). LII. An essay towards solving a problem in the doctrine of chances. By the late Rev. Mr. Bayes, F. R. S. communicated by Mr. Price, in a letter to John Canton, A. M. F. R. S. *Philosophical Transactions of the Royal Society of London*, 53, 370-418. <https://doi.org/10.1098/rstl.1763.0053>
- Baykar. (2014). Bayraktar TB2. <http://baykartech.com/tr/uav/bayraktar-tb2/>
- Baykar. (2021). Bayraktar AKINCI. <http://baykartech.com/en/uav/bayraktar-akinci/>
- Baykar. (2022, Haziran 14). Milli İHA ve SİHA'lar ihracat şampiyonunu değiştirdi. <https://www.baykartech.com/tr/press/milli-ihave-sihalar-ihracat-sampiyonunu-degistirdi/>
- Baykar. (2023). Bayraktar TB3. <http://baykartech.com/tr/uav/bayraktar-tb3/>
- BBC. (2019, Kasım 27). Go master quits because AI “cannot be defeated”. <https://www.bbc.com/news/technology-50573071>
- Beaumont, H. (2022, Eylül 16). ‘Never sleeps, never even blinks’: The hi-tech Anduril towers spreading along the US border. *The Guardian*. <https://www.theguardian.com/us-news/2022/sep/16/anduril-towers-surveillance-us-mexico-border-migrants>
- Becker, S. (1991). Unsupervised learning procedures for neural networks. *International Journal of Neural Systems*, 02(01n02), 17-33. <https://doi.org/10.1142/S0129065791000030>
- Bedoya, A. (2017, Mart 22). Law Enforcement’s Use of Facial Recognition Technology. Federal Bureau of Investigations.
- Benincasa, E. (2024, Eylül 3). From World Champions to State Assets: The Outsized Impact of a Few Chinese Hackers. *War on the Rocks*. <https://warontherocks.com/2024/09/from-world-champions-to-state-assets-the-outsized-impact-of-a-few-chinese-hackers/>
- Berkeley, E. C. (2022, Eylül 14). Giant brains; or, Machines that think. [www.gutenberg.org/cache/epub/68991/pg68991-images.html](http://www.gutenberg.org/cache/epub/68991/pg68991-images.html)
- Bertolotti, C. (2018). The military applications of Artificial Intelligence. <https://www.startinsight.eu/en/tag/skynet/>
- Biography. (2021, Mayıs 6). Ada Lovelace—Quotes, Children & Facts. Biography. <https://www.biography.com/scholars-educators/ada-lovelace>
- Bloch, L. (2019). L’arithmétique binaire, par Leibniz. <https://www.laurentbloch.org/MySpip3/L-arithmetique-binaire-par-Leibniz-98>
- Boole, G. (2005). An Investigation of the Laws of Thought On which are founded the mathematical theories of logic and probabilities. <https://www.gutenberg.org/ebooks/15114>
- Bostrom, N. (2017). *Superintelligence: Paths, dangers, strategies*. Oxford University Press.
- Breazeal, C., Edsinger, A., Fitzpatrick, P., & Scassellati, B. (2001). Active vision for sociable robots. *IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans*, 31(5), 443-453. <https://doi.org/10.1109/3468.952718>
- Bresnick, S. (2024, Haziran). China’s Military AI Roadblocks. Center for Security and Emerging Technology. <https://cset.georgetown.edu/publication/chinas-military-ai-roadblocks/>
- Britannica. (2022). Pascaline | Mechanical Calculator, Addition Device, Subtraction | Britannica. Encyclopedia Britannica. <https://www.britannica.com/technology/Pascaline>
- Britannica. (2024, Ağustos 3). Joseph-Marie Jacquard | Biography, Loom, Invention, Computers, & Facts | Britannica. Encyclopedia Britannica. <https://www.britannica.com/biography/Joseph-Marie-Jacquard>
- Britannica. (2025a, Nisan 25). Three laws of robotics | Definition, Isaac Asimov, & Facts | Britannica. <https://www.britannica.com/topic/Three-Laws-of-Robotics>

- Britannica. (2025b, Mayıs 20). R.U.R. | Robot, Automation, Science Fiction | Britannica. <https://www.britannica.com/topic/RUR>
- Brookings Institution. (2021, Mayıs 17). A national strategy for AI innovation. Brookings. <https://www.brookings.edu/events/a-national-strategy-for-ai-innovation/>
- Brown, T. B., Mann, B., Ryder, N., Subbiah, M., Kaplan, J., Dhariwal, P., Neelakantan, A., Shyam, P., Sastry, G., Askell, A., Agarwal, S., Herbert-Voss, A., Krueger, G., Henighan, T., Child, R., Ramesh, A., Ziegler, D. M., Wu, J., Winter, C., ... Amodei, D. (2020). Language Models are Few-Shot Learners (arXiv:2005.14165). arXiv. <https://doi.org/10.48550/arXiv.2005.14165>
- BTDB. (2015, Mart 6). 2015-2018 BİLGİ TOPLUMU STRATEJİSİ VE EYLEM PLANI. [http://www.sp.gov.tr/upload/xSPTemelBelge/files/uqSFE+2015-2018\\_Bilgi\\_Toplumu\\_Stratejisi\\_ve\\_Eylem\\_Plani.pdf](http://www.sp.gov.tr/upload/xSPTemelBelge/files/uqSFE+2015-2018_Bilgi_Toplumu_Stratejisi_ve_Eylem_Plani.pdf)
- CAC. (2019, Eylül 9). China: AI Governance Principles Released [Web page]. Library of Congress, Washington, D.C. 20540 USA. <https://www.loc.gov/item/global-legal-monitor/2019-09-09/china-ai-governance-principles-released/>
- CAC. (2023, Temmuz 10). China: Generative AI Measures Finalized [Web page]. Library of Congress, Washington, D.C. 20540 USA. <https://www.loc.gov/item/global-legal-monitor/2023-07-18/china-generative-ai-measures-finalized/>
- Candan, O. (2024, Ağustos 20). AB yapay zeka yasası Türkiye'yi nasıl etkiler? paradergi. <https://www.paradergi.com.tr/teknoloji/2024/08/21/ab-yapay-zeka-yasasi-turkiyeyi-nasil-etkiler>
- Candariam. (2021, Mart). Facial Recognition and Human Rights: Investor Guidance. [https://www.candariam.com/siteassets/medias/publications/brochure/research-papers/facial-recognition/2021\\_03\\_facial\\_recognition\\_en\\_web.pdf](https://www.candariam.com/siteassets/medias/publications/brochure/research-papers/facial-recognition/2021_03_facial_recognition_en_web.pdf)
- Cankı, B. (2019, Nisan 30). Yerli hava savunma sistemi Gökdeniz resmen tanıtıldı. DonanimHaber. <https://www.donanimhaber.com/Yerli-hava-savunma-sistemi-Gokdeniz-resmen-tanitildi--110316>
- Capurro, R. (2022, Nisan). Joseph Weizenbaum: A Parrhesiastes in the Digital Age. <https://www.capurro.de/weizenbaum.html>
- Carey, M. (2018, Ağustos 24). Biometrics Worked! U.S. Border Patrol Celebrates Success of Early Tech. Condé Nast Traveler. <https://www.cntraveler.com/story/biometrics-worked-us-border-patrol-celebrates-success-of-early-tech>
- CBDDO. (2019, Ekim 24). Türkiye Cumhuriyeti Cumhurbaşkanlığı Dijital Dönüşüm Ofisi—Hizmet Birimlerimiz ve Görevleri. <https://cbddo.gov.tr/hizmet-birimlerimiz/>
- CBDDO. (2024). Türkiye Cumhuriyeti Cumhurbaşkanlığı Dijital Dönüşüm Ofisi—Ulusal Yapay Zekâ Stratejisi 2021-2025. <https://cbddo.gov.tr/uyzs>
- CBP. (2020). Simplified Arrival Overview. [https://www.portseattle.org/sites/default/files/2020-08/Simplified\\_Arrival\\_Overview\\_CBP\\_Field\\_Ops\\_presentation.pdf](https://www.portseattle.org/sites/default/files/2020-08/Simplified_Arrival_Overview_CBP_Field_Ops_presentation.pdf)
- CDAO. (2022, Haziran 22). Department's Responsible Artificial Intelligence Strategy and Implementation Pathway Maps. Chief Digital and Artificial Intelligence Office. <https://www.ai.mil/Latest/Blog/Article-Display/Article/3940350/departments-responsible-artificial-intelligence-strategy-and-implementation-pat/>
- CDDO, & STB. (2021). Türkiye Cumhuriyeti Cumhurbaşkanlığı Dijital Dönüşüm Ofisi—Ulusal Yapay Zekâ Stratejisi 2021-2025. <https://cbddo.gov.tr/uyzs>
- Cha, S. (2021, Kasım 13). South Korea to test AI-powered facial recognition to track Covid cases—The Economic Times. <https://economictimes.indiatimes.com/tech/tech-bytes/south-korea-to-test-ai-powered-facial-recognition-to-track-covid-cases/articleshow/88254104.cms?from=mdr>

- Chatterjee, S. (2020). AI strategy of India: Policy framework, adoption challenges and actions for government. *Transforming Government: People, Process and Policy*, 14(5), 757-775. <https://doi.org/10.1108/TG-05-2019-0031>
- Chowdhery, A., Narang, S., Devlin, J., Bosma, M., Mishra, G., Roberts, A., Barham, P., Chung, H. W., Sutton, C., Gehrmann, S., Schuh, P., Shi, K., Tsvyashchenko, S., Maynez, J., Rao, A., Barnes, P., Tay, Y., Shazeer, N., Prabhakaran, V., ... Fiedel, N. (2022). PaLM: Scaling Language Modeling with Pathways (arXiv:2204.02311). arXiv. <http://arxiv.org/abs/2204.02311>
- Cinicioğlu, E. N., Önsel, Ş., & Ulengin, F. (2015). (PDF) BAYES AĞ YAPISININ OLUŞTURULMASINDA FARKLI YAKLAŞIMLAR: NEDENSEL BAYES AĞLARI VE VERİDEN AĞ ÖĞRENME. İçinde ResearchGate. [https://www.researchgate.net/publication/289335611\\_BAYES\\_AG\\_YAPISININ\\_OLUSTURULMASINDA\\_FARKLI\\_YAKLASIMLAR\\_NEDENSEL\\_BAYES\\_AGLARI\\_VE\\_VERIDEN\\_AG\\_OGRENME](https://www.researchgate.net/publication/289335611_BAYES_AG_YAPISININ_OLUSTURULMASINDA_FARKLI_YAKLASIMLAR_NEDENSEL_BAYES_AGLARI_VE_VERIDEN_AG_OGRENME)
- Computerhistory, M. (t.y.-a). 1801: Punched cards control Jacquard loom | The Storage Engine | Computer History Museum. Geliş tarihi 03 Kasım 2024, gönderen <https://www.computerhistory.org/storageengine/punched-cards-control-jacquard-loom/>
- Computerhistory, M. (t.y.-b). Shakey—CHM Revolution. Geliş tarihi 05 Kasım 2024, gönderen <https://www.computerhistory.org/revolution/artificial-intelligence-robotics/13/289>
- Copeland, B. J. (t.y.). MYCIN | Expert System, Medical Diagnosis & Treatment | Britannica. Geliş tarihi 01 Haziran 2025, gönderen <https://www.britannica.com/technology/MYCIN>
- Council for Science, Technology and Innovation Cabinet Office, & Government of Japan. (2015, Aralık 18). Toplum 5.0. Cabinet Office Home Page. [https://www8.cao.go.jp/cstp/english/society5\\_0/index.html](https://www8.cao.go.jp/cstp/english/society5_0/index.html)
- Covington. (2024, Kasım 13). White House Issues National Security Memorandum on Artificial Intelligence (“AI”). <https://www.cov.com/en/news-and-insights/insights/2024/11/white-house-issues-national-security-memorandum-on-artificial-intelligence-ai>
- CPDS. (2025, Mayıs 27). 20250527\_resources\_standard\_guidelines\_guideline\_04.pdf. [https://www.digital.go.jp/assets/contents/node/basic\\_page/field\\_ref\\_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/6e45a64f/20250527\\_resources\\_standard\\_guidelines\\_guideline\\_04.pdf](https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/6e45a64f/20250527_resources_standard_guidelines_guideline_04.pdf)
- Croitoru, I., Bogolin, S.-V., & Leordeanu, M. (2019). Unsupervised Learning of Foreground Object Segmentation. *International Journal of Computer Vision*, 127(9), 1279-1302. <https://doi.org/10.1007/s11263-019-01183-3>
- Dağıstanlı, H. C., & Sarica, A. (2025, Mart 28). Cumhurbaşkanlığına bağlı ofis ve politika kurullarına ilişkin düzenlemeler Resmi Gazete’de. <https://www.aa.com.tr/tr/gundem/cumhurbaskanligina-bagli-ofis-ve-politika-kurullarina-iliskin-duzenlemeler-resmi-gazetede/3522186>
- DARPA. (t.y.). About DARPA | DARPA. Geliş tarihi 26 Şubat 2025, gönderen <https://www.darpa.mil/about>
- DARPA. (2014, Mart 13). The DARPA Grand Challenge: Ten Years Later. <https://www.darpa.mil/news-events/2014-03-13>
- Dartmouth. (2006). Artificial Intelligence (AI) Coined at Dartmouth | Dartmouth. <https://home.dartmouth.edu/about/artificial-intelligence-ai-coined-dartmouth>
- Dastin, J. (2023, Şubat 2). Ukraine is using Palantir’s software for “targeting,” CEO says. Reuters. <https://www.reuters.com/technology/ukraine-is-using-palantirs-software-targeting-ceo-says-2023-02-02/>
- Deepmind. (2022, Mayıs 12). A Generalist Agent. Google DeepMind. <https://deepmind.google/discover/blog/a-generalist-agent/>

- DeMarco, M. (2024, Ekim 4). Ethical AI Development: Balancing Innovation with Responsibility. <https://www.phenom.com/blog/ethical-ai-development>
- Denge. (2023, Şubat 13). “DERİNGÖRÜ” YAZILIMI DEVREDE. DENGİ GAZETESİ. <https://www.dengegazetesi.com.tr/deringoru-yazilimi-devrede-162641h.htm>
- Department of Industry Science and Resources. (2025, Mart 6). The Seoul Declaration by countries attending the AI Seoul Summit, 21-22 May 2024 | Department of Industry Science and Resources [Partnership or agreement]. <https://www.industry.gov.au/publications/seoul-declaration-countries-attending-ai-seoul-summit-21-22-may-2024>
- Dickmanns, E. D. (1997). Vehicles Capable of Dynamic Vision. <https://www.ijcai.org/Proceedings/97-2/Papers/117.pdf>
- DLP. (2022, Ekim 31). The Data Liberation Project—Automated Targeting System Documentation. <https://www.data-liberation-project.org/requests/automated-targeting-system-documentation/>
- DoD. (2018, Ocak 1). 2018 DoD Artificial Intelligence Strategy Harnessing AI to Advance Our Security and Prosperity. <https://media.defense.gov/2019/Feb/12/2002088964/-1/-1/1/DOD-AI-STRATEGY-FACT-SHEET.PDF>
- Dori, Y., Huffman, R., Burnette, R., Ponder, J., & Lauber, V. (2024, Nisan 1). OMB Issues First Governmentwide AI Policy for Federal Agencies. Inside Privacy. <https://www.insideprivacy.com/artificial-intelligence/omb-issues-first-governmentwide-ai-policy-for-federal-agencies/>
- Dougherty, R. (2025, Nisan 29). 2021 concept to 2025 product: BAHA drones enter service with Turkish Armed Forces. <https://www.defenceconnect.com.au/air/15945-2021-concept-to-2025-product-baha-drones-enter-service-with-turkish-armed-forces>
- Dreyfus, S. E. (1990). Artificial neural networks, back propagation, and the Kelley-Bryson gradient procedure. *Journal of Guidance, Control, and Dynamics*, 13(5), 926-928. <https://doi.org/10.2514/3.25422>
- EC. (2019, Nisan 8). Ethics guidelines for trustworthy AI | Shaping Europe’s digital future. <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai>
- Ekonomim. (2025, Mayıs 22). Otoyol denetimlerinde yapay zeka görevde! Radarda yüz tanıma sistemi kullanılıyor—Ekonomim. <https://www.ekonomim.com/sektorler/teknoloji/otoyol-denetimlerinde-yapay-zeka-gorevde-radarda-yuz-tanima-sistemi-kullaniliyor-haberi-819815>
- Elbashir, M., & Desikachari, K. B. (2025, Mart 13). India’s path to AI autonomy. Atlantic Council. <https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/indias-path-to-ai-autonomy/>
- Engelking, C. (2017, Aralık 13). The “Driverless” Car Era Began More Than 90 Years Ago. *Discover Magazine*. <https://www.discovermagazine.com/technology/the-driverless-car-era-began-more-than-90-years-ago>
- Engler, A. (2023, Nisan 25). The EU and U.S. diverge on AI regulation: A transatlantic comparison and steps to alignment. Brookings. <https://www.brookings.edu/articles/the-eu-and-us-diverge-on-ai-regulation-a-transatlantic-comparison-and-steps-to-alignment/>
- Esen, F. S. (2024). Yeni Yüzyılın Soğuk Savaşı: ABD-Çin Arasındaki Yapay Zekâ Temelli Teknopolitik Rekabet. *Kriter Dergi*. <https://kriterdergi.com/dis-politika/yeni-yuzyilin-soguk-savasi-abd-cin-arasindaki-yapay-zek-temelli-teknopolitik-rekabet>
- EU. (2024a, Temmuz 12). Regulation—EU - 2024/1689—EN - EUR-Lex. <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng>



- EU. (2024b, Temmuz 12). Regulation—EU - 2024/1689—EN - EUR-Lex. <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng>
- Euronews. (2023, Temmuz 25). ABD, eski Başkan Trump'ın 2017'de çıktığı UNESCO'ya yeniden döndü. euronews. <https://tr.euronews.com/2023/07/25/abd-eski-baskan-trumpin-2017-de-ciktigi-unescoya-yeniden-dondu>
- Everquill, R. (2024, Ekim 24). Secretive US tech firm Palantir scoops contract with Leicestershire Police. Leicester Gazette. <https://www.leicester.news/secretive-us-tech-firm-palantir-scoops-contract-with-leicestershire-police/>
- Executive Office of the President. (2019, Şubat 14). Maintaining American Leadership in Artificial Intelligence. Federal Register. <https://www.federalregister.gov/documents/2019/02/14/2019-02544/maintaining-american-leadership-in-artificial-intelligence>
- Executive Office of the President. (2020, Aralık 8). Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government. Federal Register. <https://www.federalregister.gov/documents/2020/12/08/2020-27065/promoting-the-use-of-trustworthy-artificial-intelligence-in-the-federal-government>
- Executive Office of the President. (2023a, Kasım 1). Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence. Federal Register. <https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence>
- Executive Office of the President. (2023b, Kasım 1). Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence. Federal Register. <https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence>
- Executive Office of the President. (2025, Ocak 31). Removing Barriers to American Leadership in Artificial Intelligence. Federal Register. <https://www.federalregister.gov/documents/2025/01/31/2025-02172/removing-barriers-to-american-leadership-in-artificial-intelligence>
- FBI. (2014, Eylül 15). FBI Announces Full Operational Capability of the Next Generation Identification System—FBI [Press Release]. <https://www.fbi.gov/news/press-releases/fbi-announces-full-operational-capability-of-the-next-generation-identification-system>
- Fennel, M. (2022, Şubat 10). Korea's Biometric Data Dilemma | Asia Society. <https://asiasociety.org/korea/koreas-biometric-data-dilemma>
- Fernandes, Y., & Abosata, N. (2024). Analysing India's Cyber Warfare Readiness and Developing a Defence Strategy (arXiv:2406.12568). arXiv. <https://doi.org/10.48550/arXiv.2406.12568>
- Fidancıoğlu, D. (2025, Mart 19). Türkiye'nin Siber Güvenlik Tarihi. <https://tr.linkedin.com/pulse/t%C3%BCrkiyenin-siber-g%C3%BCvenlik-tarihi-duygu-fidanc%C4%B1o%C4%9Flu-om5gf>
- Foxx, C. (2017, Haziran 5). Apple reveals HomePod smart speaker. <https://www.bbc.com/news/technology-40158158>
- Friend, Z. (2013, Eylül 4). Predictive Policing: Using Technology to Reduce Crime. FBI: Law Enforcement Bulletin. <https://leb.fbi.gov/articles/featured-articles/predictive-policing-using-technology-to-reduce-crime>
- Frumer, Y. (2020, Mayıs 21). The Short, Strange Life of the First Friendly Robot. IEEE Spectrum. <https://spectrum.ieee.org/the-short-strange-life-of-the-first-friendly-robot>
- FRUS. (1962, Ağustos 24). Historical Documents—Office of the Historian. <https://history.state.gov/historicaldocuments/frus1964-68v10/d204>
- G20. (2019, Haziran 9). G20 AI Principles. <https://oecd.ai/en/wonk/documents/g20-ai-principles>

- Gao, Y., Pan, Z., Wang, H., & Chen, G. (2018). Alexa, My Love: Analyzing Reviews of Amazon Echo (s. 380). <https://doi.org/10.1109/SmartWorld.2018.00094>
- Garamone, J. (2023, Ocak 25). DOD Updates Autonomy in Weapons System Directive. U.S. Department of Defense. <https://www.war.gov/News/News-Stories/Article/Article/3278065/dod-updates-autonomy-in-weapons-system-directive/>
- Garner. (2022, Şubat 28). News | Town of Garner, NC. <https://www.garnernc.gov/Home/Components/News/News/1599/>
- Gasparetto, A., & Scalera, L. (2019). From the Unimate to the Delta Robot: The Early Decades of Industrial Robotics. İçinde B. Zhang & M. Ceccarelli (Ed.), *Explorations in the History and Heritage of Machines and Mechanisms* (C. 37, ss. 284-295). Springer International Publishing. [https://doi.org/10.1007/978-3-030-03538-9\\_23](https://doi.org/10.1007/978-3-030-03538-9_23)
- Gemici, O. O. (2019, Kasım 3). Parmak izinde entegrasyonla faili meçhuller bir bir çözüyor. <https://www.aa.com.tr/tr/turkiye/parmak-izinde-entegrasyonla-faili-mechuller-bir-bir-cozuluyor/1634121>
- Gesser, A., Xu, M., Hirst, M., Sharp, C., Bernabei, D., & Shen, M. (2025, Mart 24). South Korea Enacts New AI Law – Debevoise Data Blog. <https://www.debevoisedatablog.com/2025/03/24/south-korea-enacts-new-ai-law/>
- Global Times. (2025, Ocak 20). China sets up 60 billion yuan investment fund to accelerate AI innovations: Media report - Global Times. <https://www.globaltimes.cn/page/202501/1327233.shtml>
- Goyal, N. (2017, Aralık 29). Chinese Surveillance Network Tracks Down BBC Reporter. Industry Tap. <https://www.industrytap.com/chinas-cctv-surveillance-network-took-just-7-minutes-track-bbc-reporter/44526>
- Gökalp, Ö. (2022). Makine Öğrenmesi—Machine Learning (s. 14). [https://www.researchgate.net/publication/357974983\\_Makine\\_Ogrenmesi\\_-\\_Machine\\_Learning](https://www.researchgate.net/publication/357974983_Makine_Ogrenmesi_-_Machine_Learning)
- GPAI. (2020, Haziran). About—GPAI. <https://oecd.ai/en/about/about-gpai>
- GPD. (2024, Eylül 30). The Final Report of HLAB-AI: our analysis and thoughts – Global Partners Digital. <https://www.gp-digital.org/news/the-final-report-of-hlab-ai-our-analysis-and-thoughts/>
- Günel, A., & Bakırcı, Ç. M. (2021, Mayıs 8). Ada Lovelace Kimdir? Bilgisayarın Olmadığı Bir Çağda İlk Bilgisayar Algoritmasını Geliştiren Bir Vizyoner! Evrim Ağacı. <https://evrimagaci.org/ada-lovelace-kimdir-bilgisayarin-olmadigi-bir-cagda-ilk-bilgisayar-algoritmasini-gelistiren-bir-vizyoner-10442>
- Habuka, H. (2023). Japan's Approach to AI Regulation and Its Impact on the 2023 G7 Presidency. <https://www.csis.org/analysis/japans-approach-ai-regulation-and-its-impact-2023-g7-presidency>
- Harbou, T. V., & Lang, F. (Direktörler). (1927). *Metropolis* (1927)—Plot—IMDb [Video recording]. <https://www.imdb.com/title/tt0017136/plotsummary/>
- Harman, E. (2025, Ocak 29). TBMM Yapay Zeka Araştırma Komisyonu Kurulmasına İlişkin Meclis Tutanakları – Av. Ertuğrul Harman. <https://harman.av.tr/tr/2025/01/29/tbmm-yapay-zeka-arastirma-komisyonu-kurulmasina-iliskin-meclis-tutanaklari/>
- Harper, J. (2024, Ekim 30). Cybercom seeing successes with Panoptic Junction artificial intelligence capability. DefenseScoop. <https://defensescoop.com/2024/10/30/cybercom-army-cyber-command-panoptic-junction-artificial-intelligence/>
- Harris, S. (2012, Temmuz 31). Palantir Technologies spots patterns to solve crimes and track terrorists. Wired. <https://www.wired.com/story/joining-the-dots/>

- Hassan, M. (2018, Haziran 3). Facial recognition Technology to Deploy in Chinese Airports. M2SYS Blog On Biometric Technology. <https://www.m2sys.com/blog/biometric-resources/facial-recognition-technology-to-deploy-in-chinese-airports/>
- HAVELSAN. (2025, Nisan 25). HAVELSAN - BAHA Unmanned Aerial Vehicle Officially Inducted into Turkish Land Forces Inventory! HAVELSAN. <https://www.havelsan.com/en/news/baha-uav-inducted-turkish-land-forces-inventory>
- Havens, J. C. (2019, Ekim 22). Ethically Aligned Design: A Personal Side of “From Principles to Practice” (Part One) | LinkedIn. <https://www.linkedin.com/pulse/ethically-aligned-design-personal-side-from-practice-john-c-havens/>
- Haverford, C. (t.y.). 1.8 Leibniz ve Kademeli Hesaplayıcı | Parça Parça. Geliş tarihi 03 Kasım 2024, gönderen <http://ds-wordpress.haverford.edu/bitbybit/bit-by-bit-contents/chapter-one/1-8-leibniz-and-the-stepped-reckoner/>
- Ha-yan, C. (2019, Mayıs 1). Moon announces system semiconductor “vision and strategy” to match Samsung investment. Hankyoreh. [https://english.hani.co.kr/arti/english\\_edition/e\\_business/892289.html](https://english.hani.co.kr/arti/english_edition/e_business/892289.html)
- Hebb, D. O. (2005). The organization of behavior: A neuropsychological theory. Psychology press. [https://pure.mpg.de/rest/items/item\\_2346268\\_3/component/file\\_2346267/content](https://pure.mpg.de/rest/items/item_2346268_3/component/file_2346267/content)
- Heehyun, K. (2021, Aralık 29). MSIT to invest 51.8 billion won (US\$ 44 million) in innovative unmanned vehicle technology. [https://www.msit.go.kr/eng/bbs/view.do?RLS\\_YN=&bbsSeqNo=42&formMode=&mId=4&mPid=2&nttSeqNo=608&pageIndex=1&sCode=eng&searchCtgry1=&searchCtgry2=&searchCtgry3=&searchOpt=ALL&searchTxt=](https://www.msit.go.kr/eng/bbs/view.do?RLS_YN=&bbsSeqNo=42&formMode=&mId=4&mPid=2&nttSeqNo=608&pageIndex=1&sCode=eng&searchCtgry1=&searchCtgry2=&searchCtgry3=&searchOpt=ALL&searchTxt=)
- Helou, A. (2025, Nisan 25). Turkish military officially accepts BAHA “sub-cloud” drone into service. Breaking Defense. <https://breakingdefense.com/2025/04/turkish-military-officially-accepts-baha-sub-cloud-drone-into-service/>
- Hendler, J. (2008). (PDF) Avoiding Another AI Winter. ResearchGate. <https://doi.org/10.1109/MIS.2008.20>
- Hiebert, K., & Tang, J. (2025, Mayıs 22). The Promises and Perils of Predictive Policing. Centre for International Governance Innovation. <https://www.cigionline.org/articles/the-promises-and-perils-of-predictive-policing/>
- Hill, K. (2020, Ocak 18). The Secretive Company That Might End Privacy as We Know It. The New York Times. <https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html>
- Horowitz, M. C. (2018, Mayıs 15). Artificial Intelligence, International Competition, and the Balance of Power. Texas National Security Review. <https://tnsr.org/2018/05/artificial-intelligence-international-competition-and-the-balance-of-power/>
- Hu, K. (2023, Şubat 2). ChatGPT sets record for fastest-growing user base—Analyst note. Reuters. <https://www.reuters.com/technology/chatgpt-sets-record-fastest-growing-user-base-analyst-note-2023-02-01/>
- IBM. (2024, Eylül 17). What is AI Ethics? | IBM. <https://www.ibm.com/think/topics/ai-ethics>
- ICT Media. (2025, Mart 28). Dijital Dönüşüm Ofisi kapatıldı, görevler Siber Güvenlik Başkanlığına devredildi. ICT Media. <https://ictmedia.com.tr/haber/dijital-donusum-ofisi-kapatildi-gorevler-siber-guvenlik-baskanligina-devredildi>
- İçişleri Bakanlığı. (t.y.). T.C. İçişleri Bakanlığı—Hakkımızda. Geliş tarihi 02 Mayıs 2025, gönderen <https://www.icisleri.gov.tr/hakkimizda>
- İçişleri Bakanlığı. (2018). Güvenlik ve Acil Durumlar Koordinasyon Merkezi Projesi (GAMER). <https://www.icisleri.gov.tr/guvenlik-ve-acil-durumlar-koordinasyon-merkezi-gamer>

- İçişleri Bakanlığı. (2019, Şubat 4). T.C. İçişleri Bakanlığı—Parmak İzi İle Faili Meçhul Olaylar Aydınlatılıyor. <https://www.icisleri.gov.tr/parmak-izi-ile-faili-mechul-olaylar-aydinlatiliyor>
- İçişleri Bakanlığı. (2020, Mayıs 28). BVS - Biyometrik Veri Sistemi. <https://www.icisleri.gov.tr/bilgiteknolojileri/bvs-biyometrik-veri-sistemi-projesi>
- İçişleri Bakanlığı. (2022a, Nisan 27). T.C. İçişleri Bakanlığı—Parmak İzi Teşhis Sisteminin Ortak Kullanımıyla 196 Bin 852 Olayın Faili Tespit Edildi. <https://www.icisleri.gov.tr/parmak-izi-teshis-sisteminin-ortak-kullanimiyla-196-bin-852-olayin-faili-tespit-edildi>
- İçişleri Bakanlığı. (2022b, Haziran 2). T.C. İçişleri Bakanlığı—Yapay Zeka ASENA Uyuşturucunun İzini Sürüyor. <https://www.icisleri.gov.tr/yapay-zeka-asena-uyusturucunun-izini-suruyor>
- İçişleri Bakanlığı. (2023). YAPAY ZEKA DESTEKLİ JANDARMA KGYS PROJESİ. [https://www.icisleri.gov.tr/kurumlar/icisleri.gov.tr/IcSite/strateji/raporlar/ButceSunumlari/2023\\_ILK6AySunum.pdf](https://www.icisleri.gov.tr/kurumlar/icisleri.gov.tr/IcSite/strateji/raporlar/ButceSunumlari/2023_ILK6AySunum.pdf)
- IEEE. (2018, Mart 22). ETHICALLY ALIGNED DESIGN A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems (Intelligent Systems, Control and Automation: Science and Engineering). The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems. [https://doi.org/10.1007/978-3-030-12524-0\\_2](https://doi.org/10.1007/978-3-030-12524-0_2)
- IEEE. (2019). The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems. İçinde ETHICALLY ALIGNED DESIGN (C. 95, s. 295). Springer International Publishing. [https://doi.org/10.1007/978-3-030-12524-0\\_2](https://doi.org/10.1007/978-3-030-12524-0_2)
- IFS, P. (2017, Şubat 18). Akıllı Bilgi Toplumu için Orta ve Uzun Vadeli Kapsamlı Plan'ın Tanıtım Yönü. [https://www.ifs.or.kr/bbs/board.php?bo\\_table=research&wr\\_id=428&scrape=true](https://www.ifs.or.kr/bbs/board.php?bo_table=research&wr_id=428&scrape=true)
- İmamoğlu, N., Eresen, A., & Efe, M. Ö. (2009, Eylül 7). Döner Ters Sarkaç Sisteminin Pekiştirmeli Öğrenme Algoritmaları ile Kontrolü. [https://www.researchgate.net/profile/Aydin-Eresen/publication/266504884\\_Doner\\_Ters\\_Sarkac\\_Sisteminin\\_Pekistirmeli\\_Ogrenme\\_Algoritmaları\\_ile\\_Kontrolu/links/545953520cf2bccc4912bad4/Doener-Ters-Sarkac-Sisteminin-Pekistirmeli-Oegrenme-Algoritmaları-ile-Kontrolue.pdf](https://www.researchgate.net/profile/Aydin-Eresen/publication/266504884_Doner_Ters_Sarkac_Sisteminin_Pekistirmeli_Ogrenme_Algoritmaları_ile_Kontrolu/links/545953520cf2bccc4912bad4/Doener-Ters-Sarkac-Sisteminin-Pekistirmeli-Oegrenme-Algoritmaları-ile-Kontrolue.pdf)
- IMR. (2022, Ocak 15). Army Strides Into Emerging Technologies. IMR. <https://imrmedia.in/army-strides-into-emerging-technologies/>
- IndiaAI. (2022, Kasım 22). India to assume the Council Chair of Global Partnership on AI (GPAI). IndiaAI. <https://indiaai.gov.in/news/india-to-assume-the-council-chair-of-global-partnership-on-ai-gpai>
- IndiaAI. (2023, Şubat 3). Critical and Emerging Technology (iCET): An India-US initiative to elevate technology partnership. IndiaAI. <https://indiaai.gov.in/news/critical-and-emerging-technology-icet-an-india-us-initiative-to-elevate-technology-partnership>
- IndiaAI. (2025, Ocak 6). Report on AI governance guidelines development. IndiaAI. <https://indiaai.gov.in/article/report-on-ai-governance-guidelines-development>
- İrobot. (2002). iRobot Hakkında. iRobot. <https://www.irobot.com.tr/irobot-hakkında/>
- Islam, Md. M. (2024). The Impact of Transfer Learning on AI Performance Across Domains. Journal of Artificial Intelligence General science (JAIGS) ISSN:3006-4023, 1(1). <https://doi.org/10.60087/jaigs.v1i1.37>
- İstiklal. (2025, Mart 12). Emniyet'te yeni dönem: Polislere yüz tanıma sistemli yaka kamerası. İstiklal Gazetesi | Günlük Siyasi Gazete ve Son Dakika Haberleri. <https://www.istiklal.com.tr/emniyette-yeni-donem-basliyor-polislere-yuz-tanima-sistemli-yaka-kamerasi-takilacak>
- Jae-in, M. (2018, Kasım 1). Presidential Speeches: Korea.net : The official website of the Republic of Korea. <https://www.korea.net/Government/Briefing-Room/Presidential-Speeches/view?articleId=164960&pageIndex=1>

- Jain, P. (2024, Nisan 19). Breakdown: Simplify AI, ML, NLP, Deep Learning, Computer Vision. Medium. <https://medium.com/@jainpalak9509/breakdown-simplify-ai-ml-nlp-deep-learning-computer-vision-c76cd982f1e4>
- Janiesch, C., Zschech, P., & Heinrich, K. (2021). Machine learning and deep learning. *Electronic Markets*, 31(3), 685-695. <https://doi.org/10.1007/s12525-021-00475-2>
- Japantimes. (2024, Ağustos 29). Japan's police agency requests ¥6 billion to tackle cyberattacks. The Japan Times. <https://www.japantimes.co.jp/news/2024/08/29/japan/crime-legal/japan-cyber-crime-budget/>
- Jia, C., & Yan, Z. (2017, Ekim 2). New fingerprint system to tighten security. [https://english.www.gov.cn/policies/policy\\_watch/2017/02/10/content\\_281475563781937.htm](https://english.www.gov.cn/policies/policy_watch/2017/02/10/content_281475563781937.htm)
- Ji-hye, S. (2019, Haziran 19). South Korea to map out AI strategy this year, build 2,000 AI-based factories by 2030. The Korea Herald. <https://www.koreaherald.com/article/2028270>
- Jobin, A., Ienca, M., & Vayena, E. (2019). The global landscape of AI ethics guidelines. *Nature Machine Intelligence*, 1(9), 389-399. <https://doi.org/10.1038/s42256-019-0088-2>
- Johnson, D. B. (2025, Nisan 2). Cyber Command touts AI-driven gains in cybersecurity, network monitoring. CyberScoop. <https://cyberscoop.com/cyber-command-ai-gains-cybersecurity-network-monitoring/>
- Johnson, J. (2024, Temmuz 2). Japan's Defense Ministry unveils first basic policy on use of AI. The Japan Times. <https://www.japantimes.co.jp/news/2024/07/02/japan/sdf-cybersecurity/>
- Joo-heon, K. (2023, Ekim 11). Seoul to develop AI solution for detection of hecklers at subway stations. <https://m.ajupress.com/view/20231010151430483>
- Kahan, J. H. (2013). What's in a Name? The Meaning of Homeland Security. <https://www.semanticscholar.org/paper/What%27s-in-a-Name-The-Meaning-of-Homeland-Security-Kahan/eeb7fe0a62820ce0b066aae88285696ffbd7ae44>
- Kamer, V., & Ural, Ş. (2009). Yapay Zekâ ve Monoton-olmayan Mantık [İstanbul Üniversitesi]. [https://tez.yok.gov.tr/UlusalTezMerkezi/tezDetay.jsp?id=0\\_7KFdT7KfVsj2xOKGMciQ&no=x\\_fmEzL5Jf2WUEfjY4BSCYQ](https://tez.yok.gov.tr/UlusalTezMerkezi/tezDetay.jsp?id=0_7KFdT7KfVsj2xOKGMciQ&no=x_fmEzL5Jf2WUEfjY4BSCYQ)
- Karadağ, A. (2025, Ocak 17). KADES'i cep telefonuna indiren kadın sayısı 7 milyon 830 bine ulaştı. <https://www.aa.com.tr/tr/gundem/kadesi-cep-telefonuna-indiren-kadin-sayisi-7-milyon-830-bine-ulasti/3453131>
- Karakuş, E. (2023, Nisan 25). Yerli yapay zeka suç ile mücadele ediyor. <https://www.trthaber.com/haber/dunya/yerli-yapay-zeka-suc-ile-mucadele-ediyor-762573.html>
- Keay, A., & Silicon Valley Robotics. (2017, Şubat 28). Shakey is first robot to receive IEEE Milestone award—Robohub. <https://robohub.org/shakey-is-first-robot-to-receive-ieee-milestone-award/>
- Khalid, M. U., & Masood, S. (2024). Military Application and Integration of AI: Implications for South Asian Security Paradigm. *Journal of Policy Research*, 10(2), Article 2. <https://doi.org/10.61506/02.00255>
- Kharpal, A. (2019, Ekim 8). China's surveillance tech is spreading globally, raising concerns about Beijing's influence. CNBC. <https://www.cnbc.com/2019/10/08/china-is-exporting-surveillance-tech-like-facial-recognition-globally.html>
- Khurshid, T. (2022). The Impact of Artificial Intelligence Militarization on South Asian Deterrence Dynamics. *Contemporary Security Policy*, 43(3), 407-435. <https://doi.org/10.1080/13523260.2022.2075665>
- Khurshid, T., & Zaman, M. H. (2024). AI INTEGRATION IN INDIAN MILITARY: APPRAISAL OF SECURITY APPREHENSIONS FOR SOUTH ASIA. *NDU Journal*, 38(1), Article 1. <https://doi.org/10.54690/ndujournal.38.179>

- Kimchang. (2025, Mart 7). The Korea Communications Commission Issues the Guidelines on the Protection of Users of Generative AI Services—Kim & Chang. [https://www.kimchang.com/en/insights/detail.kc?sch\\_section=4&idx=31605](https://www.kimchang.com/en/insights/detail.kc?sch_section=4&idx=31605)
- Korea.net. (2019, Ekim 28). Presidential Speeches: Korea.net : The official website of the Republic of Korea. <https://www.korea.net/Government/Briefing-Room/Presidential-Speeches/view?articleId=178629>
- Kustom Signals. (2019, Ağustos 30). News and Events | How AI is Assisting Police with Non-Violent Crime (Lessons from Dubai, Japan & Spain). Kustom Signals Inc. <https://kustomsignals.com/blog/how-ai-is-assisting-police-with-non-violent-crime-lessons-from-dubai-japan>
- KVKK. (2016, Nisan 7). KİŞİSEL VERİLERİN KORUNMASI KANUNU. <https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=6698&MevzuatTur=1&MevzuatTertip=5>
- Kyodo News. (2018, Ocak 29). Police in Japan eye AI-assisted predictive policing before Olympics. Kyodo News+. <https://english.kyodonews.net/news/2018/01/5890d824baaf-kanagawa-police-eye-ai-assisted-predictive-policing-before-olympics.html>
- Landymore, F. (2025, Nisan 2). An AI Model Has Officially Passed the Turing Test. Futurism. <https://futurism.com/ai-model-turing-test>
- Laursen, L. (2023, Ağustos 22). China's AI-Tocracy Quells Protests and Boosts AI Innovation—IEEE Spectrum. <https://spectrum.ieee.org/china-facial-recognition>
- Lecun, Y., Bottou, L., Bengio, Y., & Haffner, P. (2023). Gradient-based learning applied to document recognition. *Proceedings of the IEEE*, 86(11), 2278-2324. <https://doi.org/10.1109/5.726791>
- Lederer, E. M. (2024, Mart 21). The UN adopts a resolution backing efforts to ensure artificial intelligence is safe. AP News. <https://apnews.com/article/united-nations-artificial-intelligence-safety-resolution-vote-8079fe83111cced0f0717fdecefffb4d>
- Lee, C.-D. (2019, Ekim 28). Moon declares S. Korea's AI-gov't vision, with "AI national strategy" in the making. Yonhap News Agency. <https://en.yna.co.kr/view/AEN20191028002200315>
- Lee, D. (2019, Mayıs 14). San Francisco is first US city to ban facial recognition. <https://www.bbc.com/news/technology-48276660>
- Lee, M. (2023, Temmuz 11). US formally rejoins UNESCO after five-year absence. AP News. <https://apnews.com/article/us-unesco-6380e9bfc62c02e6669d227590d44341>
- Lenchner, J. (2014). Analysis of Watson's Strategies for Playing Jeopardy! [https://www.academia.edu/78378913/Analysis\\_of\\_Watsons\\_Strategies\\_for\\_Playing\\_Jeopardy](https://www.academia.edu/78378913/Analysis_of_Watsons_Strategies_for_Playing_Jeopardy)
- 
- Levine, E. S., Tisch, J., Tasso, A., & Joy, M. (2017). The New York City Police Department's Domain Awareness System. *Interfaces*, 47(1), 70-84. <https://doi.org/10.1287/inte.2016.0860>
- Lewvinson-Waldman, R., & Gutierrez, J. G. (2023, Ekim 24). DHS Must Overhaul Its Flawed Automated Systems | Brennan Center for Justice. <https://www.brennancenter.org/our-work/analysis-opinion/dhs-must-overhaul-its-flawed-automated-systems>
- Lexplosion. (2025, Ocak 17). MeitY invites public comments on AI Governance Guidelines; recommends comprehensive framework to tackle cybersecurity, deepfakes, bias and IP challenges in India's emerging AI ecosystem. Lexplosion. <https://lexplosion.in/meity-invites-public-comments-on-ai-governance-guidelines-recommends-comprehensive-framework-to-tackle-cybersecurity-deepfakes-bias-and-ip-challenges-in-indias-emerging-ai-ecosystem/>
- Li, J. (2022). Artificial Intelligence Technology and China's Defense System. <https://www.airuniversity.af.edu/JIPA/Display/Article/2980879/artificial-intelligence-technology-and-chinas-defense-system/>

- Liyanage, C. (2025, Ocak 16). Tyranny of City Brain: How China Implements Artificial Intelligence to Upgrade its Repressive Surveillance Regime. Illiberalism.Org. <https://www.illiberalism.org/tyranny-of-city-brain-how-china-implements-artificial-intelligence-to-upgrade-its-repressive-surveillance-regime/>
- Lobo, S. (2024, Ekim 7). India to avoid heavy AI regulation as in EU, US: Ashwini Vaishnaw. MEDIANAMA. <https://www.medianama.com/2024/10/223-ai-regulation-data-privacy-law-approach-it-minister-ashwini-vaishnaw/>
- Lopez, C. T. (2020, Şubat 25). DOD Adopts 5 Principles of Artificial Intelligence Ethics. U.S. Department of Defense. <https://www.war.gov/News/News-Stories/article/article/2094085/dod-adopts-5-principles-of-artificial-intelligence-ethics/>
- Maass, D. (2023, Mart 20). CBP Is Expanding Its Surveillance Tower Program at the U.S.-Mexico Border—And We’re Mapping It. Electronic Frontier Foundation. <https://www.eff.org/deeplinks/2023/03/cbp-expanding-its-surveillance-tower-program-us-mexico-border-and-were-mapping-it>
- Mainichi. (2018, Ağustos 30). National Police Agency to experiment with AI to predict crimes—The Mainichi. <https://mainichi.jp/english/articles/20180830/p2a/00m/0na/014000c>
- Marsh, A. (2022, Mayıs 27). Charles Babbage’s Difference Engine Turns 200. IEEE Spectrum. <https://spectrum.ieee.org/charles-babbage-difference-engine>
- Martin, A. (2025, Mayıs 16). Japan enacts new Active Cyberdefense Law allowing for offensive cyber operations. <https://therecord.media/japan-enacts-new-law-allowing-offensive-cyber-operations>
- Mathew, J. (2025, Mart 4). IndiaAI Mission: Can India’s very own AI push earn global recognition? Fortune India. <https://www.fortuneindia.com/long-reads/indiaai-mission-can-indias-very-own-ai-push-earn-global-recognition/120531>
- Matsumoto, Y. (2025, Mayıs 29). [Flash Report] Japan Enacts AI Promotion Act: Overview and Implications for Businesses | ZeLo. <https://zelojapan.com/en/lawsquare/56899>
- McCarthy, J. (1996, Haziran 26). Introduction. <https://www-formal.stanford.edu/jmc/history/lisp/node1.html#SECTION00010000000000000000>
- McCarthy, J., Minsky, M. L., Rochester, N., Corporation, I. B. M., & Shannon, C. E. (1955). A PROPOSAL FOR THE DARTMOUTH SUMMER RESEARCH PROJECT ON ARTIFICIAL INTELLIGENCE. <http://jmc.stanford.edu/articles/dartmouth/dartmouth.pdf>
- Mcculloch, W. S., & Pitts, W. (1943). A logical calculus of the ideas immanent in nervous activity. California State University. <https://home.csulb.edu/~cwallis/382/readings/482/mcculloch.logical.calculus.ideas.1943.pdf>
- McDermott, D. (1985). The Dark Ages of AI: A Panel Discussion at AAAI-84.
- MDN. (2025, Ocak 16). TBMM’de yapay zekâ komisyonu—MarineDeal News. <https://www.marinedealnews.com/tbmmde-yapay-zeka-komisyonu/>
- Mehak, Rahul Kumar, & Dr. Ashima Mehta. (2023). Artificial Intelligence. International Journal of Advanced Research in Science, Communication and Technology, 20-30. <https://doi.org/10.48175/IJARSCT-9466>
- Mehmet, F. (2024, Haziran 6). STM’den yeni kamikaze İHA çalışması: KARGU-3. DefenceTurk. <https://www.defenceturk.net/stmden-yeni-kamikaze-ih-a-calismasi-kargu-3>
- Mete, A. (2025, Mayıs 13). AK Partili Dönmez: Raporumuz, Türkiye’nin yapay zeka politikalarına yön verecek. DHA | Demirören Haber Ajansı. <http://www.dha.com.tr/politika/ak-partili-donmez-raporumuz-turkiyenin-yapay-zeka-politikalarina-yon-verecek-2638675>
- METI. (2024, Nisan 19). AI Guidelines for Business Ver 1.0 Compiled. [https://www.meti.go.jp/english/press/2024/0419\\_002.html](https://www.meti.go.jp/english/press/2024/0419_002.html)

- Milestone. (t.y.). Nouvelle arithmetique binaire. - Explication de l'arithmétique binaire, qui se sert des seuls caracteres 0 & 1; avec des remarques sur son utilité, & sur ce qu'elle donne le sens des anciennes figures. Milestones of Science Books. Geliş tarihi 03 Kasım 2024, gönderen <https://www.milestone-books.de/pages/books/003257/gottfried-wilhelm-leibniz/nouvelle-arithmetique-binaire-explication-de-larithmetique-binaire-qui-se-sert-des-seuls>
- Ministry of Defense. (2018, Aralık 18). Japan Ministry of Defense. Japan Ministry of Defense. <https://www.mod.go.jp/en/>
- Ministry of Defense. (2025). Japan Ministry of Defense. Japan Ministry of Defense. <https://www.mod.go.jp/en/>
- MOEF. (2020, Temmuz 14). Press Releases—Government Announces Overview of Korean New Deal. <https://english.moef.go.kr/pc/selectTbPressCenterDtl.do?boardCd=N0001&seq=4940>
- MOFA. (2019, Haziran 29). G20 Osaka Leaders' Declaration | Documents and Materials. G20 Osaka Summit 2019. [https://mofa.go.jp/policy/economy/g20\\_summit/osaka19/documents/final\\_g20\\_osaka\\_leaders\\_declaration.html](https://mofa.go.jp/policy/economy/g20_summit/osaka19/documents/final_g20_osaka_leaders_declaration.html)
- Mohanty, A., & Sahu, S. (2024, Kasım 21). India's Advance on AI Regulation. Carnegie Endowment for International Peace. <https://carnegieendowment.org/research/2024/11/indias-advance-on-ai-regulation?lang=en>
- Mohler, G. O., Short, M. B., Brantingham, P. J., Schoenberg, F. P., & Tita, G. E. (2011). Self-Exciting Point Process Modeling of Crime. *Journal of the American Statistical Association*, 106(493), 100-108. <https://doi.org/10.1198/jasa.2011.ap09546>
- MSIT. (2019a, Haziran 11). AI strategy 2019—AI for Everyone: People, Industries, Regions and Governments. <https://www8.cao.go.jp/cstp/ai/aistratagy2019en.pdf>
- MSIT. (2019b, Aralık 17). National Strategy for Artificial Intelligence. <https://www.msit.go.kr/bbs/view.do?sCode=eng&nttSeqNo=9&bbsSeqNo=46&mId=10>
- MSIT. (2021, Mayıs). MSIT announced 「Strategy to realize trustworthy artificial intelligence」. <https://www.msit.go.kr/eng/bbs/view.do?sCode=eng&mId=4&mPid=2&pageIndex=&bbsSeqNo=42&nttSeqNo=509>
- MSIT. (2024a, Nisan 4). Korea Establishes the High-Level Consultative Council on Artificial Intelligence Strategy as the top-level governance structure for AI. <https://www.msit.go.kr/eng/bbs/view.do?nttSeqNo=994&bbsSeqNo=42&mId=4>
- MSIT. (2024b, Eylül 26). Blueprint for Korea's Leap to Become One of the Top Three Global AI Powerhouse (AI G3). <https://www.msit.go.kr/eng/bbs/view.do?bbsSeqNo=42&mId=4&nttSeqNo=1037&sCode=eng>
- MSIT. (2024c, Eylül 26). MSIT Presents Blueprint for Korea's AI Innovation to Achieve AI G3 Status. <https://www.msit.go.kr/eng/bbs/view.do?sCode=eng&mId=4&mPid=2&pageIndex=&bbsSeqNo=42&nttSeqNo=1040&searchOpt=ALL&searchTxt=>
- MSIT. (2024d, Ekim 11). Blueprint for Korea's Leap to Become One of the Top Three Global AI Powerhouse (AI G3). <https://www.korea.net/Government/Briefing-Room/Press-Releases/view?articleId=7606&type=O&insttCode=>
- Nanjing, G. J. in, & Xiaomin, Z. (2024, Ekim 23). "AI police" improve rate of solving crime. <https://www.chinadaily.com.cn/a/202410/23/WS6718580ca310f1265a1c9146.html>
- NBC NEWS. (2014, Mayıs 16). Future Tech? Autonomous Killer Robots Are Already Here. NBC News. <https://www.nbcnews.com/tech/security/future-tech-autonomous-killer-robots-are-already-here-n105656>



- Ng-Thow-Hing, V., Lim, J., Wormer, J., Sarvadevabhatla, S. R. K., Rocha, C., Fujimura, K., & Sakagami, Y. (2008). The Memory Game: Creating a human-robot interactive scenario for ASIMO (s. 786). <https://doi.org/10.1109/IROS.2008.4651095>
- NICT. (2022, Nisan 22). AI strategy 2022. <https://www8.cao.go.jp/cstp/ai/aistrategy2022en.pdf>
- Nilsson, N. J. (2009). The Quest for Artificial Intelligence (1. bs). Cambridge University Press. <https://doi.org/10.1017/CBO9780511819346>
- NITI Aayog. (2018, Haziran). National Strategy for Artificial Intelligence. <https://www.niti.gov.in/sites/default/files/2023-03/National-Strategy-for-Artificial-Intelligence.pdf>
- NPA. (2024). Police White Paper 2024. [https://www.npa.go.jp/english/publication/r06\\_english\\_hakusyo.pdf](https://www.npa.go.jp/english/publication/r06_english_hakusyo.pdf)
- NRCSNT. (2024, Aralık 9). Korean researchers develop AI CCTVs to detect, predict criminal activities. <https://techxplore.com/news/2024-09-korean-ai-cctvs-criminal.html>
- NSTC. (2016, Ekim). The National Artificial Intelligence Research and Development Strategic Plan. [https://www.nitrd.gov/pubs/national\\_ai\\_rd\\_strategic\\_plan.pdf](https://www.nitrd.gov/pubs/national_ai_rd_strategic_plan.pdf)
- NTIA. (2019, Mayıs 22). U.S. Joins with OECD in Adopting Global AI Principles | National Telecommunications and Information Administration. <https://www.ntia.gov/blog/us-joins-oecd-adopting-global-ai-principles>
- NTV. (2019, Haziran 18). İstanbul Havalimanı'nda yeni dönem (Pasaport kontrolü 18 saniyeye düşüyor). <https://www.ntv.com.tr/galeri/teknoloji/istanbul-havalimaninda-yeni-donem-pasaport-kontrolu-18-saniyeye-dusuyor.jIyImduxHUyM8EP5bkGBSA>
- OECD. (t.y.). AI Principles Overview. Geliş tarihi 09 Mayıs 2025, gönderen <https://oecd.ai/en/principles>
- OECD. (2019, Mayıs 22). OECD Legal Instruments. <https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449>
- OECD. (2021, Haziran 17). State of implementation of the OECD AI Principles. OECD. [https://www.oecd.org/en/publications/state-of-implementation-of-the-oecd-ai-principles\\_1cd40c44-en.html](https://www.oecd.org/en/publications/state-of-implementation-of-the-oecd-ai-principles_1cd40c44-en.html)
- OECD. (2024a, Mayıs 3). OECD updates AI Principles to stay abreast of rapid technological developments. OECD. <https://www.oecd.org/en/about/news/press-releases/oecd-updates-ai-principles-to-stay-abreast-of-rapid-technological-developments.html>
- OECD. (2024b, Haziran). Background. <https://oecd.ai/en/about/background>
- OECD. (2025). Community on smart data and digital technology in education. OECD Events. <https://www.oecd-events.org/smart-data-and-digital-technology-in-education>
- Oktay, Ş. (2023, Şubat 18). Deprem sonrası artan sosyal medya dolandırıcılığı yapay zekayla tespit edilecek. <https://www.aa.com.tr/tr/bilim-teknoloji/deprem-sonrasi-artan-sosyal-medya-dolandiriciligi-yapay-zekayla-tespit-edilecek/2823729>
- OpenAI. (2015, Aralık 11). Introducing OpenAI. <https://openai.com/index/introducing-openai/>
- Oppy, G., & Dowe, D. (2003). The Turing Test. <https://plato.stanford.edu/entries/turing-test/>
- Ops Today. (2025, Mayıs 29). Yapay Zeka Tanıtım Yasası Kabul Edildi: Yasanın İçeriği ve Şirketlerin Alması Gereken Eylemlerin Açıklaması. <https://ops-today.com/topics-12586/>
- OSTP. (2019, Şubat 11). Accelerating America's Leadership in Artificial Intelligence – The White House. <https://trumpwhitehouse.archives.gov/articles/accelerating-americas-leadership-in-artificial-intelligence/>

- Özarpa, C., Avcı, İ., & Kara, S. A. (2021). Otonom Araçlar İçin Siber Güvenlik Risklerinin Araştırılması ve Savunma Metotları. *European Journal of Science and Technology*. <https://doi.org/10.31590/ejosat.911468>
- Özberk, T. (2025, Nisan 25). BAYRAKTAR TB3 UCAV Completes Four Successful Autonomous Sorties Aboard TCG Anadolu. *Naval News*. <https://www.navalnews.com/naval-news/2025/04/bayraktar-tb3-ucav-completes-four-successful-autonomous-sorties-aboard-tcg-anadolu/>
- Özcan, E. I., & Sütçü, S. S. (2023). AKDENİZ ÜNİVERSİTESİ SOSYAL BİLİMLER ENSTİTÜSÜ. Akdeniz Üniversitesi.
- Özdemir, A. (2022). Yapay zeka'nın grafik tasarıma ve tasarımcıya etkisi. *Hitit Sosyal Bilimler Dergisi*, 15(2), 628-637. <https://doi.org/10.17218/hititsbd.1205445>
- Özkul, A. E., & Aydın, S. (2015). VERİ MADENCİLİĞİ VE ANADOLU ÜNİVERSİTESİ AÇIKÖĞRETİM SİSTEMİNDE BİR UYGULAMA. 05.
- Öztemel, E. (2020). Bilişim Teknolojileri ve İletişim: Birey ve Toplum Güvenliği (M. Şeker, Y. Bulduklu, & C. Korkut, Ed.). *Turkish Academy of Sciences*. <https://doi.org/10.53478/TUBA.2020.002>
- Öztürk, A., Çakır, H. S., Mercimek, M., & Engin, Ş. (2022, Aralık). (PDF) Döner Kanatlı İnsansız Hava Araçlarının Görme Tabanlı Derin Pekistirmeli Öğrenme Yöntemi ile Otonom İnişi Autonomous Landing of Rotary Wing Unmanned Aerial Vehicles with Vision Based Reinforcement Learning Method. *ResearchGate*. [https://www.researchgate.net/publication/373019658\\_Doner\\_Kanatli\\_Insansiz\\_Hava\\_Araclari\\_nin\\_Gorme\\_Tabanli\\_Derin\\_Pekistirmeli\\_Ogrenme\\_Yontemi\\_ile\\_Otonom\\_Inisi\\_Autonomous\\_Landing\\_of\\_Rotary\\_Wing\\_Unmanned\\_Aerial\\_Vehicles\\_with\\_Vision\\_Based\\_Reinforcement\\_Lea](https://www.researchgate.net/publication/373019658_Doner_Kanatli_Insansiz_Hava_Araclari_nin_Gorme_Tabanli_Derin_Pekistirmeli_Ogrenme_Yontemi_ile_Otonom_Inisi_Autonomous_Landing_of_Rotary_Wing_Unmanned_Aerial_Vehicles_with_Vision_Based_Reinforcement_Lea)
- Pan, S. J., & Yang, Q. (2010). A Survey on Transfer Learning. *IEEE Transactions on Knowledge and Data Engineering*, 22(10), 1345-1359. <https://doi.org/10.1109/TKDE.2009.191>
- Papilon. (2019, Şubat 2). 2765 Faili Meçhul Olay Papilon Parmak İzi Sistemi ile Aydınlanıyor | Papilon.com.tr. <https://papilon.com.tr/tr/haberler/2765-faili-mechul-olay-papilon-parmak-izi-sistemi-ile-aydinlaniyor>
- Park, Y. (2024). Will the One Ring Hold? Defense AI in South Korea. İçinde H. Borchert, T. Schütz, & J. Verbovsky (Ed.), *The Very Long Game: 25 Case Studies on the Global State of Defense AI* (ss. 505-527). Springer Nature Switzerland. [https://doi.org/10.1007/978-3-031-58649-1\\_23](https://doi.org/10.1007/978-3-031-58649-1_23)
- Parken, O., & Trevithick, J. (2022, Mayıs 27). China Launches Drone Ship That Acts As A Mothership For More Drones. *The War Zone*. <https://www.twz.com/china-launches-drone-ship-that-acts-as-mothership-for-more-drones>
- PBS News. (2018, Haziran 3). Amid pressure from employees, Google drops Pentagon's Project Maven account. *PBS News*. <https://www.pbs.org/newshour/show/amid-pressure-from-employees-google-drops-pentagons-project-maven-account>
- PDO. (2016, Eylül 22). China's first intelligent security robot starts work at Shenzhen Airport—People's Daily Online. <https://en.people.cn/n3/2016/0922/c90000-9118480.html>
- Pellerin, C. (2016, Ağustos 6). Three Teams Earn Prizes in DARPA Cyber Grand Challenge. U.S. Department of Defense. <https://www.war.gov/News/News-Stories/Article/Article/906931/three-teams-earn-prizes-in-darpa-cyber-grand-challenge/>
- Persson, S. (1964). An Introduction to Artificial Intelligence. *Ekonomisk Tidskrift*, 66(2), 88. <https://doi.org/10.2307/3438581>
- Peterson, D. (2021, Ekim 23). How China harnesses data fusion to make sense of surveillance data. *Brookings*. <https://www.brookings.edu/articles/how-china-harnesses-data-fusion-to-make-sense-of-surveillance-data/>

- PIB Delhi. (2022a, Mart 28). TASK FORCE FOR IMPLEMENTATION OF AI. <https://pib.gov.in/pib.gov.in/Pressreleaseshare.aspx?PRID=1810442>
- PIB Delhi. (2022b, Mart 28). TASK FORCE FOR IMPLEMENTATION OF AI. <https://www.pib.gov.in/www.pib.gov.in/Pressreleaseshare.aspx?PRID=1810442>
- PIB Delhi. (2024, Mart 7). Cabinet Approves Ambitious IndiaAI Mission to Strengthen the AI Innovation Ecosystem. <https://www.pib.gov.in/www.pib.gov.in/Pressreleaseshare.aspx?PRID=2012355>
- Police1. (2018, Aralık 6). 7 cases solved thanks to ALPR data. <https://www.police1.com/police-products/traffic-enforcement/license-plate-readers/articles/7-cases-solved-thanks-to-alpr-data-doayALt3VGwqCIN5/>
- Police1. (2025, Nisan 16). SoundThinking more than doubles ResourceRouter adoption. <https://www.police1.com/police-products/police-technology/soundthinking-more-than-doubles-resourcerouter-adoption>
- Press, T. A. (2017, Eylül 1). Putin: Leader in artificial intelligence will rule world. C4ISRNet. <https://www.c4isrnet.com/international/2017/09/01/putin-leader-in-artificial-intelligence-will-rule-world/>
- Prinz, I. (2023, Mayıs 15). The very first calculating machine. ADP ReThink Q. <https://rethinkq.adp.com/artifact-first-calculating-machine/>
- Prorok, M. (2022). Applications of artificial intelligence systems. *Deliberationes*, 15(Különszám), 76-88. <https://doi.org/10.54230/Delib.2022.K.SZ.76>
- PTI. (2018, Temmuz 13). China deploys radars, drones on borders to curb infiltration. *The Economic Times*. <https://economictimes.indiatimes.com/news/defence/china-deploys-radars-drones-on-borders-to-curb-infiltration/articleshow/49688679.cms?from=mdr>
- PTI. (2019, Mart 4). Electronic surveillance of Indo-Bangla border to begin Tuesday. *The Economic Times*. <https://economictimes.indiatimes.com/news/defence/electronic-surveillance-of-indo-bangla-border-to-begin-tuesday/articleshow/68254084.cms>
- PTI. (2025, Mayıs 27). CIBMS delivered encouraging results along IB: Inspector General of Border Security Force. *The Economic Times*. <https://economictimes.indiatimes.com/news/defence/cibms-delivered-encouraging-results-along-ib-inspector-general-of-border-security-force/articleshow/121441804.cms?from=mdr>
- Qianxin. (2024). Tehdit İzleme ve Analiz Sistemi (Sky Eye). <https://www.qianxin.com/product/detail/pid/328>
- Qianxin. (2025, Mayıs 20). Yapay zeka güçlendirmesi + çoklu senaryo işlevi yükseltmesi, Qi'anxin Tianyan'ın yeni sürümü resmen yayınlandı. [https://www.qianxin.com/news/detail?news\\_id=13457](https://www.qianxin.com/news/detail?news_id=13457)
- Quevedo, T. (t.y.). *The Chess Player: The First Computer Game in History*. Google Arts & Culture. Geliş tarihi 03 Kasım 2024, gönderen <https://artsandculture.google.com/story/the-chess-player-the-first-computer-game-in-history/CQURBJHKlccLIA>
- REAM. (2023). Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy.
- Reuters. (2020, Eylül 30). Palantir valued at \$20 billion in choppy stock exchange debut. Reuters. <https://www.reuters.com/article/business/palantir-valued-at-20-billion-in-choppy-stock-exchange-debut-idUSKBN26L3DQ/>
- Reuters. (2024, Aralık 13). China sets up AI standards committee as global tech race intensifies. Reuters. <https://www.reuters.com/technology/china-sets-up-ai-standards-committee-global-tech-race-intensifies-2024-12-13/>

- Reuters. (2025a, Şubat 11). Anduril takes over Microsoft's \$22 billion US Army headset program. Reuters. <https://www.reuters.com/technology/anduril-takes-over-microsofts-22-billion-us-army-headset-program-2025-02-11/>
- Reuters. (2025b, Mart 14). Chinese regulators issue requirements for the labeling of AI-generated content. Reuters. <https://www.reuters.com/world/asia-pacific/chinese-regulators-issue-requirements-labeling-ai-generated-content-2025-03-14/>
- Reuters. (2025c, Haziran 5). Trump renegotiating Biden-era Chips Act grants, Lutnick says | Reuters. <https://www.reuters.com/world/us/trump-administration-renegotiating-overly-generous-biden-chips-act-grants-2025-06-04/>
- RG. (2013, Haziran 20). Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı. Resmi Gazete. <https://www.resmigazete.gov.tr/eskiler/2013/06/20130620-1-1.pdf#page=1.00>
- RG. (2025, Mart 12). SİBER GÜVENLİK KANUNU. <https://www.resmigazete.gov.tr/eskiler/2025/03/20250319-1.htm>
- Richard, I. (2024, Eylül 14). Korea's "Dejaview" Is an AI for CCTVs That Can Detect, Predict Crimes Using "Change-Based Approach". Tech Times. <https://www.techtimes.com/articles/307506/20240914/koreas-dejaview-ai-powered-cctv-detect-predict-crimes-using-change.htm>
- Rubin, J. (2010, Ağustos 21). Stopping crime before it starts. Los Angeles Times. <https://www.latimes.com/archives/la-xpm-2010-aug-21-la-me-predictcrime-20100427-1-story.html>
- Russell, S. J., & Norvig, P. (with Davis, E., & Edwards, D.). (2016). Artificial intelligence: A modern approach (Third edition, Global edition). Pearson.
- Ryall, J. (2024, Ağustos 27). Japan's police to deploy AI-powered drones in disaster-hit areas to deter looters | South China Morning Post. <https://www.scmp.com/week-asia/politics/article/3276075/japans-police-deploy-ai-powered-drones-disaster-hit-areas-deter-looters>
- Sankin, A., & Mattu, S. (2023, Ekim 2). Predictive Policing Software Terrible At Predicting Crimes – The Markup. <https://themarkup.org/prediction-bias/2023/10/02/predictive-policing-software-terrible-at-predicting-crimes>
- SBB. (2019, Temmuz 18). On Birinci Kalkınma Planı 2019-2023. Strateji Bütçe Başkanlığı.
- SBB. (2022, Ekim 25). 2023 Yılı Cumhurbaşkanlığı Yıllık Programı. Resmi Gazete.
- SBN. (2021, Temmuz 5). Seoul using AI-based CCTV to prevent suicide attempts on bridges -. Seoul Metropolitan Government. <https://world.seoul.go.kr/seoul-using-ai-based-cctv-to-prevent-suicide-attempts-on-bridges/>
- Schrieffert, D. (2018, Ağustos 31). Norbert Wiener's Foundation of Computer Ethics – The Research Center on Values in Emerging Science and Technology. <https://rcvest.southernct.edu/norbert-wieners-foundation-of-computer-ethics/>
- Sciencemuseum. (2023, Temmuz 18). Charles Babbage's Difference Engines and the Science Museum | Science Museum. <https://www.sciencemuseum.org.uk/objects-and-stories/charles-babbages-difference-engines-and-science-museum>
- Sehgal, V. (2024). Integration of Artificial Intelligence in Indian Military Operations: An Overview (2024). 6(4). <https://www.ijfmr.com/papers/2024/4/26311.pdf>
- Sejnowski, T. J. (2020). The unreasonable effectiveness of deep learning in artificial intelligence. Proceedings of the National Academy of Sciences, 117(48), 30033-30038. <https://doi.org/10.1073/pnas.1907373117>

- SGK. (2025). Sahil Güvenlik Komutanlığı 2024 Yılı Faaliyetleri ve 2025 Yılı Hedefleri. <https://www.sg.gov.tr/kurumlar/sg.gov.tr/komutanlik/yayinlar/Sahil-Guvenlik-Komutanligi-2024-Yili-Faaliyetleri-ve-2025-Yili-Hedefleri.pdf>
- Shane, S., & Wakabayashi, D. (2018, Nisan 4). ‘The Business of War’: Google Employees Protest Work for the Pentagon. The New York Times. <https://www.nytimes.com/2018/04/04/technology/google-letter-ceo-pentagon-project.html>
- Sharma, N. (2024, Aralık 8). Dronaam, India’s Anti-Drone Gun, Neutralised 55% Of Drones: Amit Shah. Wwww.Ndtv.Com. <https://www.ndtv.com/india-news/dronaam-indias-anti-drone-gun-neutralised-55-of-drones-amit-shah-7200958>
- Singh, R. (2025, Mayıs 6). Corporate Ethics in the Age of Artificial Intelligence: A Comprehensive Analysis of Evolution, Frameworks, and Regulatory Impacts | LinkedIn. <https://www.linkedin.com/pulse/corporate-ethics-age-artificial-intelligence-analysis-singh-kwptf/>
- Singhal, U. (2025, Nisan 6). AI in the sky: Police to soon deploy facial recognition tech across Delhi. The Indian Express. <https://indianexpress.com/article/cities/delhi/ai-in-the-sky-police-to-soon-deploy-facial-recognition-tech-across-delhi-9927353/>
- Song, D. (2023, Temmuz 17). Facial Recognition AI solution ‘Alchera’ to participate in Incheon Airport Smart Pass System project—KoreaTechDesk | Korean Startup and Technology News. <https://koreatechdesk.com/facial-recognition-ai-solution-alchera-to-participate-in-incheon-airport-smart-pass-system-project>
- Stangarone, T. (2020, Aralık 7). COVID-19 Underscores the Benefits of South Korea’s Artificial Intelligence Push. <https://thediplomat.com/2020/12/covid-19-underscores-the-benefits-of-south-koreas-artificial-intelligence-push/>
- Stanley-Lockman, Z., & Christie, E. H. (2021, Ekim 25). NATO Review—An Artificial Intelligence Strategy for NATO. NATO Review. <https://www.nato.int/docu/review/articles/2021/10/25/an-artificial-intelligence-strategy-for-nato/index.html>
- STB. (2023, Ekim 31). On İkinci Kalkınma Planı 2024-2028.
- STB. (2024, Temmuz 24). Ulusal Yapay Zeka Stratejisi 2024-2025 Eylem Planı.
- STB, & CBDDO. (2021, Ağustos). Türkiye Ulusal Yapay Zeka Stratejisi2021-2025. <https://cbddo.gov.tr/SharedFolderServer/Genel/File/TR-UlusalYZStratejisi2021-2025.pdf>
- Stenquist, K. (2023, Haziran 27). Discussion and Direction for Acquisition of Automated License Plate Readers (ALPRs). <https://d3n9y02raazwpg.cloudfront.net/belmont-ca/d3a8276e-0654-11ee-95dd-0050569183fa-89cb9f1d-714d-41af-9cfc-900baeef572-1687555048.pdf>
- STIP, C. (2021, Eylül 13). The Presidential Committee on the 4th Industrial Revolution | STIP Compass. <https://stip.oecd.org/stip/interactive-dashboards/policy-initiatives/2021%2Fdata%2FpolicyInitiatives%2F16688>
- STM. (2021, Temmuz 21). STM - Milli Gururumuz KARGU’dan İlk İhracat Başarısı. STM. <https://www.stm.com.tr/medya/basin-bultenleri/milli-gururumuz-kargudan-ilk-ihracat-basarisi>
- Stokes, J. (2024, Şubat 1). Military Artificial Intelligence, the People’s Liberation Army, and U.S.-China Strategic Competition. CNAS. <https://www.cnas.org/publications/congressional-testimony/military-artificial-intelligence-the-peoples-liberation-army-and-u-s-china-strategic-competition>
- Strategic Council for AI Technology. (2017, Mart 31). Artificial Intelligence Technology Strategy. [https://ai-japan.s3-ap-northeast-1.amazonaws.com/7116/0377/5269/Artificial\\_Intelligence\\_Technology\\_StrategyMarch2017.pdf](https://ai-japan.s3-ap-northeast-1.amazonaws.com/7116/0377/5269/Artificial_Intelligence_Technology_StrategyMarch2017.pdf)

- Sugano, S., & Kato, I. (1987). WABOT-2: Autonomous robot with dexterous finger-arm--Finger-arm coordination control in keyboard performance. *Proceedings. 1987 IEEE International Conference on Robotics and Automation*, 4, 90-97. 1987 IEEE International Conference on Robotics and Automation. <https://doi.org/10.1109/ROBOT.1987.1088025>
- Suryawanshi, R., & Singh, S. (2024). Artificial Intelligence and Its Applications. *International Journal of Advanced Research in Science, Communication and Technology*, 654-660. <https://doi.org/10.48175/IJARSCT-18975>
- Swift, J. (2006). *Gulliver's Travels*.
- Szoldra, P. (2016, Temmuz 13). A bunch of computers will try to hack each other in Vegas for a \$2 million prize. *Business Insider*. <https://www.businessinsider.com/darpar-cyber-grand-challenge-2016-7>
- Şahin, A. (2023, Ocak 1). KORKUT Alçak İrtifa Hava Savunma Sistemi (AİHSS). <https://www.savunmasanayist.com/korkut-alcak-irtifa-hava-savunma-sistemi-aihss/>
- Şeker, A., Diri, B., & Balık, H. H. (2017). Derin Öğrenme Yöntemleri ve Uygulamaları Hakkında Bir İnceleme. *Gazi Mühendislik Bilimleri Dergisi*.
- Tatsuno, D., & Takahashi, A. (2025, Mayıs 27). Japan's AI Bill Advances Toward Enactment. *Connect On Tech*. <https://connectontech.bakermckenzie.com/japans-ai-bill-advances-toward-enactment/>
- TBMM. (2024, Haziran 24). Yapay Zeka Kanun Teklifi. <https://www.tbmm.gov.tr/Yasama/KanunTeklifi/e21539a0-888a-4500-81be-01904a918c53>
- TBMM. (2025, Ocak 16). TBMM KARARI - KOMİSYON ÜYE SEÇİMİ. <https://www.resmigazete.gov.tr/eskiler/2025/01/20250116-1.pdf>
- TDK. (2025). Yapay zekâ ne demek TDK Sözlük Anlamı. [https://sozluk.gov.tr/?kelime=yapay zekâ](https://sozluk.gov.tr/?kelime=yapay%20zek%C3%A1)
- Tecuci, G. (2012). Artificial intelligence. *WIREs Computational Statistics*, 4(2), 168-180. <https://doi.org/10.1002/wics.200>
- Teo, W. (2024, Kasım 14). Skip queues at Incheon Airport checkpoints with new SmartPass service. *The Straits Times*. <https://www.straitstimes.com/asia/east-asia/skip-queues-and-breeze-through-checkpoints-with-incheon-airport-s-new-facial-recognition-service>
- Teslauniverse. (2023, Aralık 22). Nikola Tesla ABD Patenti 613.809—Hareketli Araç veya Araçların Mekanizmasını Kontrol Etme Yöntemi ve Aparatı—Sarmalayıcılar | Tesla Evreni. <https://teslauniverse.com/nikola-tesla/patents/us-patent-613809-method-and-apparatus-controlling-mechanism-moving-vehicle-or/wrappers>
- Thakur, S. P. (2024, Haziran 12). Integrating AI in India's Defence Sector—Bloomsbury Intelligence and Security Institute (BISI). Bloomsbury Intelligence & Security Institute (BISI). <https://bisi.org.uk/reports/integrating-ai-in-indias-defence-sector>
- The Telegraph. (2010, Temmuz 12). South Korea deploys robot capable of killing intruders along border with North. The Telegraph. <https://www.telegraph.co.uk/news/worldnews/asia/southkorea/7887217/South-Korea-deploys-robot-capable-of-killing-intruders-along-border-with-North.html>
- The Tribune. (2019, Eylül 23). NATGRID rollout by early next year. The Tribune. <https://www.tribuneindia.com/news/archive/nation/natgrid-rollout-by-early-next-year-836634/>
- The White House. (2022, Ekim 22). Blueprint for an AI Bill of Rights | OSTP | The White House. <https://bidenwhitehouse.archives.gov/ostp/ai-bill-of-rights/>
- The White House. (2025a, Ocak 23). Removing Barriers to American Leadership in Artificial Intelligence. The White House. <https://www.whitehouse.gov/presidential-actions/2025/01/removing-barriers-to-american-leadership-in-artificial-intelligence/>

- The White House. (2025b, Ocak 23). Removing Barriers to American Leadership in Artificial Intelligence. The White House. <https://www.whitehouse.gov/presidential-actions/2025/01/removing-barriers-to-american-leadership-in-artificial-intelligence/>
- Thompson, A. (2021, Mart 2). China's 'Sharp Eyes' Program Aims to Surveil 100% of Public Space. Center for Security and Emerging Technology. <https://cset.georgetown.edu/article/chinas-sharp-eyes-program-aims-to-surveil-100-of-public-space/>
- Thompson, K. (2011, Kasım 1). The Santa Cruz Experiment: Can a City's Crime Be Predicted and Prevented? Popular Science. <https://www.popsci.com/science/article/2011-10/santa-cruz-experiment/>
- Thompson, K. M. (2015). I, Robot: Nikola Tesla's Telautomaton [UCLA]. <https://escholarship.org/uc/item/4xr9r7rm>
- Thompson, T. (2018, Kasım 12). Minority report: Machine learning and crime prevention in China. Technology and Operations Management. <https://d3.harvard.edu/platform-rctom/submission/minority-report-machine-learning-and-crime-prevention-in-china/>
- Tibetanreview. (2015, Kasım 9). China deploys radars, drones to enhance border surveillance. Tibetan Review. <https://www.tibetanreview.net/china-deploys-radars-drones-to-enhance-border-surveillance/>
- Tim, R. (2022, Eylül 8). H.R.4346 - 117th Congress (2021-2022): CHIPS and Science Act (2021-07-01). <https://www.congress.gov/bill/117th-congress/house-bill/4346>
- Tokson, M. (2025). The Authoritarian Risks of AI Surveillance. Lawfare. <https://www.lawfaremedia.org/article/the-authoritarian-risks-of-ai-surveillance>
- Trevithick, J. (2020, Ekim 14). China Conducts Test Of Massive Suicide Drone Swarm Launched From A Box On A Truck. The War Zone. <https://www.twz.com/37062/china-conducts-test-of-massive-suicide-drone-swarm-launched-from-a-box-on-a-truck>
- Trthaber. (2024, Aralık 6). Düzensiz göçe yeni önlem: GÖÇBİL. <https://www.trthaber.com/haber/gundem/duzensiz-goce-yeni-onlem-gocbil-890721.html>
- TSKGV. (2024, Eylül 20). ASELSAN'ın Kent Güvenlik Yönetim Sistemi: Akıllı Teknolojilerle Kamu Güvenliği - Türk Silahlı Kuvvetlerini Güçlendirme Vakfı. <https://tskgv.org.tr/savunmasanayiigundem/aselsanin-kent-guvenlik-yonetim-sistemi-akilli-teknolojilerle-kamu-guvenligi>
- Turan, A. K., & Polat, H. (2024a). Yarı denetimli makine öğrenmesi yöntemini kullanarak müzik türlerinin tespiti. Gazi Üniversitesi Fen Bilimleri Dergisi Part C: Tasarım ve Teknoloji, 12(1), 92-107. <https://doi.org/10.29109/gujsc.1352477>
- Turan, A. K., & Polat, H. (2024b). Yarı denetimli makine öğrenmesi yöntemini kullanarak müzik türlerinin tespiti. Gazi Üniversitesi Fen Bilimleri Dergisi Part C: Tasarım ve Teknoloji, 12(1), 92-107. <https://doi.org/10.29109/gujsc.1352477>
- Turing, A. M. (1937). On Computable Numbers, with an Application to the Entscheidungsproblem. Proceedings of the London Mathematical Society, s2-42(1), 230-265. <https://doi.org/10.1112/plms/s2-42.1.230>
- Turing, A. M. (1950). Computing Machinery and Intelligence. Mind, New Series, 59(236), 433-460.
- TÜBİTAK. (2014). Kent Güvenlik Yönetim Sistemlerinden (KGYS) Elde Edilen Video Görüntülerinden Anlamlı Sonuçlar Çıkarmaya Yarayacak Akıllı Destek Yazılımları Geliştirilmesi. <https://tubitak.gov.tr/sites/default/files/1007-egm-2013-01.pdf>
- UAB. (2020, Aralık 29). ULUSAL SİBER GÜVENLİK STRATEJİSİ VE EYLEM PLANI 2020-2023. <https://hgm.uab.gov.tr/uploads/pages/strateji-eylem-planlari/ulusal-siber-guvenlik-stratejisi-ve-eylem-plan-2020-2023.pdf#page=19.40>

- UAB. (2024, Ekim 7). ULUSAL SİBER GÜVENLİK STRATEJİSİ VE EYLEM PLANI 2024-2028. <https://hgm.uab.gov.tr/uploads/pages/strateji-eylem-planlari/ulusal-siber-guvenlik-stratejisi-2024-2028.pdf>
- UCLA. (2016, Ocak 31). Leibniz Arte Combinatoria. <https://www.math.ucla.edu/~pak/hidden/papers/Quotes/Leibniz-Arte-Combinatoria.pdf>
- UDHB. (2016, Ekim 9). ULUSAL SİBER GÜVENLİK STRATEJİSİ 2016-2019. <https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/2016-2019guvenlik.pdf#page=1.00&gsr=0>
- UN. (2020). Roadmap for digital cooperation: Report of the Secretary-General. UN. <https://digitallibrary.un.org/record/3978036>
- UN. (2024). About. United Nations; United Nations. <https://www.un.org/en/ai-advisory-body/about?>
- UNESCO. (2021a, Kasım 23). Ethics of Artificial Intelligence | UNESCO. <https://www.unesco.org/en/artificial-intelligence/recommendation-ethics>
- UNESCO. (2021b, Kasım 23). Recommendation on the Ethics of Artificial Intelligence—UNESCO Digital Library. <https://unesdoc.unesco.org/ark:/48223/pf0000381137>
- UNESCO. (2023a). Ethical Impact Assessment | Global AI Ethics and Governance Observatory. <https://www.unesco.org/ethics-ai/en/eia>
- UNESCO. (2023b). UNESCO's Recommendation on the Ethics of Artificial Intelligence: Key facts. <https://unesdoc.unesco.org/ark:/48223/pf0000385082.page=12>
- UTokyo. (2024, Mart 14). Physicist's crime prediction system reduces perturbing experiences. The University of Tokyo. <https://www.u-tokyo.ac.jp/focus/en/features/entrepreneurs23.html>
- Uzun, T. (2020). YAPAY ZEKÂ VE SAĞLIK UYGULAMALARI. İzmir Katip Çelebi Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 3(1), 80-92.
- Ünal, E. C., & Aslanhan, U. (2023, Temmuz 26). SSB'den yeni yapay zeka destekli proje. <https://www.aa.com.tr/tr/gundem/ssbden-yeni-yapay-zeka-destekli-proje/2954755>
- Vajiram ve Ravi. (2023, Eylül 28). What is the National Intelligence Grid (NATGRID)? Vajiram & Ravi. <https://vajiramandravi.com/>
- Valle-Cruz, D., & Sandoval-Almazan, R. (2018). Towards an understanding of artificial intelligence in government. Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age, 1-2. dg.o '18: 19th Annual International Conference on Digital Government Research. <https://doi.org/10.1145/3209281.3209397>
- Valpolini, P. (2023, Eylül 19). DSEI 2023—Aselsan SARP Next Gen dual RCWS will be available in late 2024. EDR Magazine. <https://www.edrmagazine.eu/aselsan-sarp-next-gen-dual-rcws-will-be-available-in-late-2024>
- van Engelen, J. E., & Hoos, H. H. (2020). A survey on semi-supervised learning. Machine Learning, 109(2), 373-440. <https://doi.org/10.1007/s10994-019-05855-6>
- Velez-Green, A. (2015). The Foreign Policy Essay: The South Korean Sentry—A “Killer Robot” to Prevent War. Lawfare. <https://www.lawfaremedia.org/article/foreign-policy-essay-south-korean-sentry%E2%80%9494-killer-robot-prevent-war>
- Venn, J. (1880). I. On the diagrammatic and mechanical representation of propositions and reasonings. The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science, 10(59), 1-18. <https://doi.org/10.1080/14786448008626877>
- Vergun, D. (2023, Kasım 22). U.S. Endorses Responsible AI Measures for Global Militaries. U.S. Department of Defense. <https://www.war.gov/News/News-Stories/Article/Article/3597093/us-endorses-responsible-ai-measures-for-global-militaries/>



- Vinge, V. (1993). The Coming Technological Singularity: How to Survive in the Post-Human Era. Whole Earth Rewiew. <https://edoras.sdsu.edu/~vinge/misc/singularity.html>
- Wakabayashi, D., & Shane, S. (2018, Haziran 1). Google Will Not Renew Pentagon Contract That Upset Employees. The New York Times. <https://www.nytimes.com/2018/06/01/technology/google-pentagon-project-maven.html>
- Wallace, R. S. (2009). The Anatomy of A.L.I.C.E. İçinde R. Epstein, G. Roberts, & G. Beber (Ed.), Parsing the Turing Test (ss. 181-210). Springer Netherlands. [https://doi.org/10.1007/978-1-4020-6710-5\\_13](https://doi.org/10.1007/978-1-4020-6710-5_13)
- Wang, A. B. (2018, Nisan 13). A suspect tried to blend in with 60,000 concertgoers. China's facial-recognition cameras caught him. The Washington Post. <https://www.washingtonpost.com/news/worldviews/wp/2018/04/13/china-crime-facial-recognition-cameras-catch-suspect-at-concert-with-60000-people/>
- Waseda. (t.y.). Humanoid History -WABOT-. Geliş tarihi 06 Kasım 2024, gönderen [https://www.humanoid.waseda.ac.jp/booklet/kato\\_2.html](https://www.humanoid.waseda.ac.jp/booklet/kato_2.html)
- WCO News. (2024, Ocak 25). Automating image analysis: China Customs implements new model for the development and deployment of algorithms. WCO News. <https://mag.wcoomd.org/magazine/wco-news-104-issue-2-2024/automating-image-analysis-china-customs-implements-new-model-for-the-development-and-deployment-of-algorithms/>
- Webster, G., Creemers, R., Kania, E., & Triolo, P. (2017a, Ağustos 1). Full Translation: China's "New Generation Artificial Intelligence Development Plan" (2017). DigiChina. <https://digichina.stanford.edu/work/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017/>
- Webster, G., Creemers, R., Kania, E., & Triolo, P. (2017b, Ağustos 1). Full Translation: China's "New Generation Artificial Intelligence Development Plan" (2017). DigiChina. <https://digichina.stanford.edu/work/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017/>
- Weizenbaum, J. (1983). ELIZA — a computer program for the study of natural language communication between man and machine. Communications of the ACM, 26(1), 23-28. <https://doi.org/10.1145/357980.357991>
- Werner, J. (2025, Mart 26). South Korea Faces Human Rights Concerns Over Expanding Public Sector Use of AI. BABL AI. <https://babl.ai/south-korea-faces-human-rights-concerns-over-expanding-public-sector-use-of-ai/>
- Wiederhold, G., & McCarthy, J. (1992). Arthur Samuel: Pioneer in Machine Learning. IBM Journal of Research and Development, 36(3), 329-331. <https://doi.org/10.1147/rd.363.0329>
- Wiener, N. (2019). Cybernetics or Control and Communication in the Animal and the Machine. <https://direct.mit.edu/books/oa-monograph/4581/Cybernetics-or-Control-and-Communication-in-the>
- Won-chang, Y. (2018, Mayıs 16). Korean Gov.t to Invest 2.2 Tril. Won in AI by 2022. Businesskorea. <https://www.businesskorea.co.kr/news/articleView.html?idxno=22291>
- Xuanzum, L. (2018, Ekim 20). China a world leader in facial recognition algorithms—Global Times. <https://www.globaltimes.cn/page/201811/1128177.shtml>
- Xuanzun, L. (2025, Şubat 20). PLA deploys UAVs, robotic dogs, explosive ordnance disposal robots in NBC defense drill—Global Times. <https://www.globaltimes.cn/page/202502/1328764.shtml>
- Xuanzun, L., Wei, F., & Zhuhai, M. J. in. (2024, Kasım 17). China unveils heavy "swarm carrier" UAV at airshow—Global Times. <https://www.globaltimes.cn/page/202411/1323238.shtml>
- Xue, J., Wang, Y.-C., Wei, C., Liu, X., Woo, J., & Kuo, C.-C. J. (2023). Bias and Fairness in Chatbots: An Overview (arXiv:2309.08836; Versiyon 2). arXiv. <http://arxiv.org/abs/2309.08836>

- Yıldırım, G. (2020, Nisan 29). Turkey: Aselsan delivers border surveillance systems. <https://www.aa.com.tr/en/economy/turkey-aselsan-delivers-border-surveillance-systems/1822794>
- Yıldırım, G. (2022, Şubat 28). Türkiye sınırları ASELSAN teknolojileriyle donatılıyor. <https://www.aa.com.tr/tr/gundem/turkiye-sinirlari-aselsan-teknolojileriyle-donatiliyor/2518149>
- Yıldırım, G. (2024, Mayıs 17). Emniyetteki biyometrik veriler milli yazılıma emanet. <https://www.aa.com.tr/tr/bilim-teknoloji/emniyetteki-biyometrik-veriler-milli-yazilima-emanet/3222744>
- Yılmaz, D. S. (2012). Türkiye'nin İç Güvenlik Yapılanmasında Değişim İhtiyacı. Çukurova Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 21(3), Article 3.
- Yoshida, S. (2021, Eylül 2). Japan's police to increasingly partner up with AI to fight crime | The Asahi Shimbun: Breaking News, Japan News and Analysis. <https://www.asahi.com/ajw/articles/14421414>
- Zhuang, F., Qi, Z., Duan, K., Xi, D., Zhu, Y., Zhu, H., Xiong, H., & He, Q. (2021). A Comprehensive Survey on Transfer Learning. Proceedings of the IEEE, 109(1), 43-76. <https://doi.org/10.1109/JPROC.2020.3004555>

## ÖZGEÇMİŞ

Adı Soyadı : Fatih Kaan BOZER

Yabancı Dili : İngilizce

### Eğitim Durumu

Lise : Anadolu Teknik Lisesi, 2012

Ön Lisans : Polis Meslek Yüksekokulu, 2015

Lisans : Anadolu Üniversitesi, 2018

Yüksek Lisans :

### Mesleki Deneyim

İş Yeri : Samsun İl Emniyet Müdürlüğü