YAPAY ZEKÂ TEKNOLOJİLERİNİN İÇ GÜVENLİK ALANINDA KULLANIMI

Tarık AK[1*]

Özet

Son yetmiş yılda adından en çok söz ettiren sözcüklerden birisi kuşkusuz yapay zekâdır. Özellikle son yıllarda yaşanan gelişmeler yapay teknolojilerin hem daha görünür olması sağlamış, hem de kamuoyu tarafından bilinebilirliği artırmıştır. Yapay zekâ teknolojilerinde asıl devrimsel değişikliğin, bu teknolojinin tam otomasyon sistemlere doğru evrildiğinde olacağı kabul edilmektedir. Yapay zeka teknolojilerinin ulusal güvenlik açısından etkisinin devletler üzerinde askeri, bilgi ve ekonomik üstünlük bağlamında olacağı değerlendirilmektedir. Ülkelerin iç güvenliği açısından ise; yapay zekâ teknolojilerinden faydalanmanın yöntemlerinin ulusal güvenlikten farklılık oluşturduğu açıktır. İç güvenlik eylemi, ülkede ki vatandaşlarının bizatihi kendisini merkez alan ve fiziki varlıklarının emniyetini esas alan bir yaklaşımı gerektirmektedir. Yapay zekâ teknolojilerinden istifade ederken her alanda vatandaşlarının yaşamı, huzuru ve refahını idame ettirmeyi temel alan bir politika öngörülmelidir. Bunlar iç güvenlik açısından temel işlevsel alanlar olan suçun önlenmesi ve asayişin sağlanmasından afetlerden korunmaya, kritik altyapı güvenliğinden siber tehditlere kadar yaygınlaştırılabilir. Bu bağlamda çalışma, yapay zekâ teknolojilerinin iç güvenlik alanında işlevsel olarak kullanım alanlarının tespitini amaçlamaktadır. Çalışma, literatür taraması yapılarak teorik bir zeminde yürütülmüş

1* Dr., Jandarma Genel Komutanlığı, aktrkak@gmail.com, ORCID ID: https://orcid.org/0000-0001-8452-1601

ve derlenmiştir. İlk olarak yapay zekâ teknolojilerinin ne olduğu ve güvenlikle ilişkisi açıklanacak, müteakiben ulusal güvenlik ve iç güvenliğe etkisi tanımlanacaktır. Son olarak ise; yapay zekâ teknolojilerinin iç güvenliğe işlevsel açıdan fayda sağlayacağı alanlar tespit edilecektir. Bu çalışma ile önümüzdeki on yıllarda yapay zekâ teknolojilerinin günlük hayatta güvenlik açısından oluşturacağı katkıların ve neden olacağı güvensizlik ortamının öngörülmesi hedeflenmiştir. Çalışmanın sonucunda afetlere hazırlık, terörle mücadele, sınır güvenliği gibi faaliyetlerde yapay zekâ destekli geliştirilmiş tahmine dayalı analiz sistemlerinden; asayiş grevlerinin planlanması ve afetlere yardımlarda optimizasyon ve kaynak tahsisi programlarından; sınır güvenliği, terörle mücadelede ve gümrük muhafazada ise görüş sistemleri ve biyometri yöntemleri kullanılabileceği görülmüştür.

Anahtar Kelimeler: İç Güvenlik, Kolluk, Yapay Zekâ, Ulusal Güvenlik, Güvenlik

THE USE OF ARTIFICIAL INTELLIGENCE IN THE FIELD OF INTERNAL SECURITY

Abstract

Undoubtedly, artificial intelligence is one of the most mentioned words in the last seventy years. Especially the developments in recent years have made artificial technologies more visible and increased the awareness of the public. It is accepted that the real revolutionary change in artificial intelligence technologies will occur when this technology evolves towards fully automated systems. It is evaluated that the effect of artificial intelligence technologies in terms of national security will be in the context of military, information and economic superiority on states. In terms of the internal security of the countries; It is clear that the methods of making use of artificial intelligence technologies differ from national security. Internal security action requires an approach that is centered on the citizens in the country and based on the safety of their physical assets. While benefiting from artificial intelligence technologies, a policy based on maintaining the life, peace and welfare of its citizens in every field should be envisaged. These can be extended from crime prevention and security, which are basic functional areas in terms of internal security, to protection from disasters, from critical infrastructure security to cyber threats. In

this context, the study aims to determine the functional usage areas of artificial intelligence technologies in the field of internal security. The study was conducted and compiled on a theoretical basis by literature review. Firstly, what artificial intelligence technologies are and their relationship with security will be explained, and then their effect on national security and internal security will be described. Finally, Areas where artificial intelligence technologies will benefit internal security functionally will be determined. With this study, it is aimed to predict the contribution of artificial intelligence technologies in terms of security in daily life and the environment of insecurity that they will cause in the coming decades. As a result of the study, among the predictive analysis systems supported by artificial intelligence in activities such as disaster preparedness, fight against terrorism and border security; Planning of public security strikes and optimization and resource allocation programs in disaster relief; It has been observed that vision systems and biometric methods can be used in border security, fight against terrorism and customs enforcement.

Key Words: Internal Security, Law Enforcement, Artificial Intelligence, National Security, Security

GİRİŞ

Günümüz dünyasının son yetmiş yılında, adından en çok söz ettiren sözcüklerden birisinin yapay zekâ olduğunu söylememek imkânsızdır. Özellikle son birkaç yılda yaşananlar ile yapay zekâ çalışmalarının teknoloji ve sanayinin birçok alanında kullanılmaya başlanması, bu teknolojilerin hem daha görünür olması sağlamış, hem de kamuoyu tarafından bilinebilirliği artırmıştır.

Kavram olarak yapay zekâ, en basit bir tarifle insan zekâsını modellenmesidir. Bu modelleme ile üretilecek bir yazılım veya makineden; insan gibi akıl yürütmesi, anlamlandırma yaparak genellemeye ulaşması ve geçmiş bilgilerden öğrenerek şu ana dair karmaşık bir hedefe ulaşma ve karar verme yetisine sahip olması beklenmektedir. Karmaşık bir hedefe ulaşabilme özgünlüğüne sahip olunması ise; öz farkındalık, anlayabilme, öğrenme ve problem çözme kabiliyeti gerektirmektedir. Yapay zekâ tanımında, "zekâ" kavramı icra edilmesi gerekli olan işleme atıf yaparken, "yapay" kavramı bu işlemin niteliğine yani teknolojinin üretilmiş haline vurgu yapmaktadır (Yılmaz, 2017:1-2; Tegmark, 2019: 74).

Zekâ kavramı, genellikle akıl kavramıyla karıştırılır. Zekâ, algılar ve kavramlar ile nesneler arasındaki bağı ve ilişki düzeyini anlayabilmek, bir amaç için çözümleyebilmek, bir yargı için karar verebilmek ve bir sonuca ulaşabilmeyi hedefler. Zekânın, söz konusu "işlem süreci"nde hayatın akışında karşılaşabileceği her bir durum ve koşul için kendisini adapte edebilmesi, arzu edilen bir neticedir. İnsanoğlu için zekâ, doğuştan farklılık oluşturan ve belirli oranlarda sahip olunan bir özelliktir. Zekânın merkeze alınması suretiyle ilk defa karşılaşılan bir olaya karşı insana benzer şekilde bir yazılım veya makinenin de anlayarak ve öğrenerek çözüm getirmesi, uyum göstermesi ve analiz edebilir olması beklenmektedir. Akıl ise, bir yazılım veya makine için modellemelerde geçerli olmayan bir kavram olarak görülür. Zira akıl, genetik yoldan alınan özelliklerin çevre ve toplum şartlarına göre davranışla birlikte ortaya çıktığı, zaman içinde değiştiği veya geliştirilebildiği sübjektif bir yetenektir (Yılmaz, 2017:1-2; Tegmark, 2019: 74).

Dünyada; ABD, Çin, Rusya ve İsrail gibi birçok ülke son yıllarda yapay zekâ teknolojilerini destekleyerek, kendi şirketlerini araştırma ve geliştirme çalışmaları kapsamında finanse etmeye başladılar. Yapay zekâ teknolojilerine yapılan yatırım ve elde edilen gelirler ise, bu süreci doğrulamaktadır. Dünya genelinde yapay zekâya çalışmaları ve ticaretine ilişkin elde edilen gelir 2016'da sadece 643,7 milyon dolar iken 2025 yılına kadar bu sektörde kazancın 36,8 milyar dolara olacağı tahmin edilmektedir (Allen & Chan, 2017: 14).

Yapay zekâ teknolojilerinde asıl devrimsel değişikliğin, özellikle tam otomasyon sistemlere doğru evrildiğinde ulaşılacağı öngörülmektedir. Bu teknolojinin yaratacağı tarihsel kırılmanın geçmişte karşılaşılan barutun icadı veya nükleer silah tehdidine benzer olarak güvenliğin tüm aktörlerini, stratejisini, organizasyon yapısını ve önceliklerini tümüyle değiştireceğine kesin gözüyle bakılmaktadır. Bu değişimin; ulusal güvenlik açısından diğer devletlere karşı askeri, bilgi ve ekonomik üstünlüğün artırılmasında fayda sağlayacağı değerlendirilmektedir. Günümüzde askeri açıdan yapay zekâ ve robotik teknolojilerdeki gelişmelerin, yeni silahların icadına, istihbari bilgilerin elde edilmesine ve siber tehditlere karşı asimetrik üstünlük sağlamaktadır. Diğer taraftan yapay zekâ teknolojilerine odaklanabilen nüfusu az ve küçük ülkelerin büyük ve güçlü ülkelere karşı askeri ve ekonomik açıdan bir avantaj veya rekabet edebilir olma ihtimali açısından bir fırsat oluşturduğu da iddia edilebilir (Allen & Chan, 2017: 2-15; **Çobanoğlu & Ak,** 2020).

Ülkelerin iç güvenliği açısından ise; yapay zekâ teknolojilerinden faydalanmanın yöntemleri çeşitli olmakla birlikte, kullanımında temkinli yaklaşımı gerektiren bir sürece ihtiyaç duyulmaktadır. Zira iç güvenlik faaliyetleri, ülkede ki vatandaşlarının bizatihi kendisini merkez alan ve fiziki varlıklarının emniyetini esas alan bir yaklaşımı içermektedir. Yapay zekâ teknolojilerinden istifade ederken; iç güvenlik açısından temel işlevsel alanlar olan suçun önlenmesi ve asayişin sağlanmasından afetlerden korunmaya, kritik altyapı güvenliğinden siber tehditlere kadar her alanda vatandaşlarının yaşamı, huzuru ve refahını idame ettirmeyi temel alan bir politika öngörülmelidir. Bu açıdan iç güvenliğin sağlanmasında temel aktör olan kolluk kuvvetlerinin de; toplumsal güvenliği sağlamak adına suça ilişkin önleyici ve adli görevlerinde başarıya ulaşırken ve faaliyetlerinde optimizasyon ile kaynak tahsisi yaparken, yapay zeka teknolojilerinin işlevselliğinden faydalanması önemlidir. Bu bağlamda çalışma, yapay zekâ teknolojilerinin iç güvenlik alanında işlevsel olarak kullanım alanlarının tespitini amaçlamaktadır. İlk olarak yapay zekâ teknolojilerinin ne olduğu ve güvenlikle ilişkisi açıklanacak, müteakiben ulusal güvenlik ve iç güvenliğe etkisi tanımlanacaktır. Son olarak ise; yapay zekâ teknolojilerinin iç güvenliğe işlevsel açıdan fayda sağlayacağı alanlar tespit edilecektir. Bu çalışma ile önümüzdeki on yıllarda yapay zekâ teknolojilerinin günlük hayatta güvenlik açısından oluşturacağı katkıların ve neden olacağı güvensizlik ortamının öngörülmesi hedeflenmiştir.

1. Yapay Zekâ Teknolojileri ve Gelişimi

Yapay zekânın oluşturulabilirliğine ilişkin düşüncenin temelleri 17 ve 18'nci yüzyıllara kadar uzanmaktadır. O tarihlerden bugüne insan düşüncesinin tasvir edilebileceği bir yöntem ya da insan gibi düşünebilen karar verebilen, hatta harekete geçebilen ve eylem gerçekleştirebilen bir cismin veya aracın meydana getirilebileceği üzerine hayaller kurulmuş, tartışmışlar yapılmış, eserler yazılmış ve icatlarla uğraşılmıştır. Rene Descartes, Thomas Hobbes, Gottfried Leibniz gibi düşünürler ile sonraki yüzyıllarda ki selefleri, yapay zekâ fikrine ilham verecek olan ve rasyonel düşüncenin doğasını temel alan muhakemenin ve matematiğin kurallarına indirgenebileceğine dair bir sistematik ön görmüşlerdir. Leibniz'in 1666 yılında yayınladığı Kombinasyon Sanatı Üzerine Tez *(Dissertatio De Arte Combinatoria/On the Combinational Art)* adlı kitabında insan düşüncesinin alfabeye benzetilmiş haliyle basit kavramların bir kombinasyonu olduğunu öne sürmesi bu yaklaşımın ilk evreleridir (Yonck, 2019: 53-54).

Sonraki yüz yılarda sanayileşmenin çeşitlenmesi sayesinde yapay zekânın teknolojilerine katkı yapabilecek gelişmeler farklı alanlarda da ortaya çıkmıştır. Örneğin; Nicola Tesla, 1898 yılında radyo dalgalarıyla kontrol edilebilen bir küçük maket gemiyi uzaktan yönlendirebilmiş; Karel Capek ise, edebiyat alanında 1921 yılında yayınladığı "Rossum'un Akıllı Robotları" *(Rossum's Universal Robots)* adlı eserinde robot kavramını ilk defa kullanarak sözcüğün literatüre girmesine vesile olmuştur.(Yonck, 2019: 53-59).

19 ve 20'nci yüzyılda yapay zekâya en çok katkı sağlayan gelişmeler matematiksel mantık kurallarının elektronik bilimiyle birleşmesi ve bu sayede programlama dillerinin oluşmaya başlamasıdır. Özellikle, İkinci Dünya Savaşı'nda Almanya'nın Enigma makinesi ile Japonya'nın kullandıkları şifreli mesajların çözümü üzerine harcanan çabalar bunlardan en önemlileridir. Bu süreçte yapay zekâ biliminin öncüsü kabul edilen Alan Turing'in yapay zekâya ilişkin düşünceleri pekişmiş ve onun taklit oyunu olarak bilinen Turing Testini[2] ortaya çıkmıştır. 1950'lere gelindiğinde ise, yapay zekâ fikri temelinde üretilen ve matematik problemlerin çözümüne odaklanan Mantık Teorisi *(Logic Teorist)*, Genel Problem Çözücü *(General Problem Solver)* ve LISP *(List Processing Language)* gibi programların geliştirilmesi önemli katkılar olarak görülmüştür. Ancak 1970'li yıllarda çalışmalarda daha fazla ilerleme yaşanamaması yapay zekâ çalışmalarını yavaşlatmıştır (Temuçin, 2020: 22-23).

Gordon Moore'un teknolojik ilerlemenin doğasına ilişkin bir gözlemi barındıran ve Moore yasası olarak bilinen kuralları ise, yapay zekâ alanında sonraki elli yılda elektronik biliminde iletken endüstrisine yön vermiş, elektroniğin gelişimine katkı yapmış, daha çok işlemcinin daha küçük alanlara sığdırılmasına fayda sağlayarak dijital teknolojilerin önünü açmıştır. Yakın dönemde üstel genişlemeyle ilgili ortaya sunulan Kryder yasası ve Metcalfe yasası bu çalışmalara benzer olarak oluşturulmuştur.[3] Bu sayede, sonraki yıllarda

2 Turing testi, Alan Turing tarafından 1950 yılında Mind adlı felsefe dergisinde Hesaplama Makineleri ve Zekâ *(Machinery and Intelligence)* başlıklı makalesinde bir makine açısından düşündüğünü söylemenin mantıksal olarak mümkün olup olmadığını sorgulamasıdır. Ayrıntılı bilgi için bakınız: Cem Say (2019). *50 Sorusa Yapay Zekâ*, İstanbul: Bilim ve Gelecek Kitaplığı.

3 Moore yasası, 1970'li yıllarda tümleşik devre üzerinde yer alan elektronik bileşen sayısının düzenli olarak iki katına çıktığını tespit eden dört veri noktasına sahip bir grafik sunuyordu. Moore on yıl içinde tümleşik devre yoğunluğunun 64 bileşenden 65.000 bileşene sıçrayacağına ilişki tahminleriyle tanınmıştır. Kryder yasası, sabit sürücü depolama yoğunluğunun her on üç ayda bir ikiye katlanması varsayımına dayalıdır. Metcalfe yasası, ağ değerinin sistemin bağlantılı kullanıcılarının sayısının karesiyle orantılı olduğuna ilişkin

tıp bilimi ve yapılan nörolojik araştırmaların katkılarıyla birlikte programlama sürecinde beynin elektrik sinyallerini gönderip alan bir hücreler ağına benzer iletişim şebekelerinin kullanılmasının önü açılmıştır. Rosalind Picard'ın örüntü tanıma, görüntü modelleme ve insan algısı, sinyal işleme üzerine çalışmaları ile insana benzer bir resim veya herhangi bir sahnenin içerik ve anlam çıkaracak ölçüde biyolojik görme sistemlerine benzeyecek matematiksel modellerin kurgulanmasına odaklanılabilmiştir (Yonck, 2019: 53-59; Temuçin, 2020: 22-23). Buradan hareketle, tüm bu çalışmaların sonucunda kamuoyu tarafından bilinen ve kullanımına sunulan yazılım ve robotların ortaya çıkmaya başladığı söylenebilir. Nitekim son on yıllara bakıldığında (Yılmaz, 2017:15 Eberl, 2019: 17-18; Tegmark, 2019: 119; Baraniuk, 2020);

- 1996 yılında IBM tarafından geliştirilen ve Deep Blue adı verilen bilgisayar 1997 yılında Garry Kasparov ile yaptığı satranç turnuvasını bir önceki yıl yenilmiş olmasına rağmen kazanmayı başarmış,
- Honda Şirketi, 2000 yılında Asimo adını verdiği ilk insansı robotu üretmiş,
- Alex Krizhevsky, Ilya Sutskever ve Geoffrey E. Hinton tarafından 2010 yılında AlexNet ismini verdikleri derin öğrenme olarak tanımlanabilecek bir yapay sinir ağı modeli geliştirilmiş,
- 2011 yılında ABD'de IBM Systems tarafından geliştirilmiş olan ve metinleri doğal dil olarak algılayabilen Watson yazılımı, "Kim Milyoner Olmak İster" adlı televizyon yarışmasının bir türü olan Jeopardy *(Riziko)* adlı yarışmada daha önce şampiyon olmuş insan rakiplerini mağlup etmiş,
- Apple şirketi, akıllı telefonlarda bir konuşma anlama yazılımı olan Siri'yi 2011 yılında kişisel asistan fonksiyonu olarak piyasaya sürmüş,
- 2012 yılında ABD'li Boston Dynamics firmasının saatte 45,5 kilometre hıza koşarak ulaşan Cheetah adında bir robot üretmiş,
- Google'a ait olan DeepMind şirketinin AlphaGo adlı derin öğrenme yazılımı, 2016 yılında dünyanın go oyununun şampiyonu Lee Sedol'u yenmiş,

---

çalışmadır (Yonck, 2019: 56).

- Yine aynı yıl Alfa adlı yapay zekâ savaş pilot sistemi, bir savaş simülasyonunda karar vermeden önce çeşitli seçenekleri göz önünde bulunduran bulanık mantık kavramına dayalı bir yapay zekâ türü olarak emekli bir insan savaş pilotunu hava muharebesinde yenmiştir.

Yapay zekâ yazılımı ve robotik teknolojilerinin sanayi ve hizmet sektörlerine yansıması; bu teknolojilerin Tablo-1'de gösterildiği üzere otomotiv, bankacılık, uzay, elektronik, eğlence, finans, sigortacılık, üretim ve imalat, sağlık, telekomünikasyon, robotik sistemler ve güvenlik gibi birçok iş kolunda yaygınlaşmasına vesile olmuştur.

Tablo-1 Yapay Zekâ Teknolojilerinin Kullanım Alanları (Yılmaz, 2017: 10-11)[4]

Sektörler	Kullanım Alanları
Otomotiv	Otomotiv sektöründe, otomatik yol takibi, yol rehberi, aktivite analizi, farklı yol koşullarında sürüş.
Bankacılık	Müşteri analizi, kredi değerlendirmesi.
Uzay	Uçuş simülasyonları, otomatik pilot uygulamaları.
Eğlence	Animasyonlar, efektler.
Finans	Pazar analizi, bütçe tahmini.
Robotik sistemler	Montaj ve tamir sistemleri, forklift robotları, yörünge kontrolü, uzaktan kumandalı sistemler, en iyi rotayı belirleme.
Sigortacılık	Ürün optimizasyonu, strateji geliştirme.
Üretim ve İmalat	Üretim ve imalatta işlem kontrolü, ürün dizaynı, dayanıklılık analizi, kalite kontrolü.
Sağlık	Kanser erken teşhis, tanı ve tedavisi, kalp krizi erken teşhis ve tedavisi, ilaç analizi, MR'da kalite artırımı.
Telekomünikasyon	Data karşılaştırma, filtreleme, ses ve görüntü işleme, trafik yoğunluğunun kontrolü, anahtarlama.
Elektronik ve yazılım	Çip analizi, doğrusal olmayan durumları modelleme.
Dil ve yazılım	Sözcük tanıma, yazıyı sese çevirme, dil tercüme.
Savunma ve Güvenlik	Hedef seçme, radar, sensör sonar sistemleri, retina-parmak izi-yüz tanıma, bankacılık dolandırıcılığı saptama, insansız araç ve sistemler.

4 Söz konusu tablo Atınç Yılmaz (2017). *Yapay Zekâ*, İstanbul Kodlab Yayınları, s.10-11'den yer alan bilgilerden oluşturularak hazırlanmıştır.

Günümüze kadar bakıldığında yapay zekâ teknolojilerinin ortaya çıkışında genel çerçeve olarak üç alanda görünür olduğu söylenebilir. Bunlardan;

- İlki; yapay zekâ teknolojilerinin fabrikalarda robot teknolojileri açısından kullanılmasıdır. Montaj ve tamir robotlarıyla birlikte kullanımı sayesinde üretim esnasında zamanlama, hata oranının azaltılması ile etkinlik ve verimliliğe doğrudan katkı yapılmaktadır [5] (Yılmaz, 2017: 9).

- İkincisi; yapay zekâ teknolojilerinin kamuoyu önünde daha çok bilinir olduğu ve sosyal hayat içerisinde kullanımının kolaylaştığı ürünlerle birlikte ortaya çıkmasıdır. Zekâ oyunları oynama, akıllı telefonlarda asistan fonksiyonları, hizmet sektörlerinde analiz gerçekleştirme veya dil çevirisi yapabilen yazılımlar bu tür görevler için kullanılmaktadır (Eberl, 2019: 118).

- Son olarak ise yapay zekâ teknolojilerinin güvenlik alanında kullanılmasıdır. Yapay zekâ teknolojileri, ulusal ve iç güvenliğin sağlanması açısından silahlı kuvvetler ve kolluk kuvvetleri tarafından karar destek ve analiz yazılımları ile yapay zekâ destekli insansız araç ve sistemler bağlamında kullanıldığı görülmektedir.

Günümüzün yapay zekâ çalışmalarında gelinen aşamaya "dar yapay zekâ" tanımı ile tarif edilmektedir. Yukarıda örnekleri sunulan yazılım ve robot türlerinde olduğu gibi dar yapay zekânın çerçevesinde tematik olarak insanın herhangi bir yeteneğinin onun düzeyini aşacak şekilde yapabilir hale getirebilen yazılım, sistem ve ürünler için kullanılmıştır. Hali hazırda çalışmaları yürütülen ve 2040'lı yıllarda kamuoyu önüne çıkması muhtemel olan yapay zekâ ürünleri ise "genel yapay zekâ" olarak tanımlanmaktadır. Genel yapay zekâ ürünlerinin bir insana benzer şekilde görsel algılama, ses tanıma, konuşma, eylem ve hareket ile muhasebe ve muhakeme edebilmeyi gerçekleştirebilmesi hedeflenmektedir. Gelecekte birçok görevi bir insandan daha iyi şekilde yerine getirebilecek yapay zekâ ürünleri ise "süper yapay zekâ" olarak belirtilmekte-

---

5 Ancak çok karıştırılan bir hususta tüm robotların yapay zekâ ile bütünleşik olmadığıdır. Bir robotun yapay zekâya sahip olabilmesi için algısal ve duyusal bir özelliğinin olabilmesi gerekir. Bu sayede robot çevresindeki değişkenleri ve farklılıkları algılayarak uygun tepki verebilir ve vermeyi öğrenir. Burada önemli olan davranışsal tepkinin otomatik değil, önceden kazanılmış deneyimler sonucu elde edilmiş olmasıdır (Yılmaz, 2017:9)

dir (Temuçin, 2020: 14).

Söz konusu yapay zekâ çalışmaları içinde; şimdiye kadar ki tarihsel gelişmelere ve ortaya çıkan ürünlere bakıldığında, yapay zekâya ilişkin yaşananlar şu hususlar altında çerçevelendirilebilir (Allen & Chan, 2017: 7);

- Yapay zekâ teknolojilerinin gelişmesine olanak sağlayan disiplinler arası yaklaşım,
- Bilginin işlenmesinde üstel büyüme,
- Makine öğrenimi tekniklerinin yazılım alanına katkısı,
- Büyük veri kümelerine ulaşabilme ve kullanabilme,
- Yapay zekâ teknolojilerine devletlerin sağladığı mali desteklerdir.

1.1. Yapay Zekâ teknolojilerine Disiplinler Arası Yaklaşım

Günümüzde artık, yapay zekâ teknolojilerinde bir ürüne ulaşmak için bilimin farklı birçok disiplininin katkısına ihtiyaç duyulmaktadır. Yapay zekâ çalışmalarında bilgisayar mühendisliğinden başlanarak elektronik, internet, dil bilgisi, fizyoloji, makine-uzay-uçak mühendisliği, malzeme bilimi, tıp, biyoloji, nöroloji, matematik, mantık, felsefe, psikoloji, güzel sanatların oluşturdukları müşterek bilgi ile ulaşılmaktadır. Mühendislik ve malzeme bilimleri donanım, yazılım ve mekaniğin en uygun ve etkili şartlarda işlevsel olmasını, mantık ve matematik yapay zekanın optimizasyon yeteneğini, felsefe muhakeme kararlarının gerçekliğini, psikoloji insan düşünce sisteminin tasvirini, dilbilgisi iletişim çeşitleri ve yöntemlerini, biyoloji canlı varlıklarının örnek alınmasını, sinir bilimi insan beyninin modellemesi açısından katkı sağlamaktadır (Yılmaz, 2017:10; Eberl, 2019: 43- 47; Domingos, 2019: 20).

Son yıllarda elektronik ve mekanik sistemlerde ki gelişmelerin yazılım ve robot üretimine katkısı yapay zekâ teknolojilerine de yansımıştır. Özellikle robot teknolojisinde sensörlerin, kameraların ve mekanik parçaların minyatürleşmesi, metalden yapılan robotlar yerine silikon maddeli malzemelerin kullanılması, robot motorları ve lityum iyon pillerin ucuzlaması yapay zekâ teknolojilerinin yaygınlaşmasına ve kullanımın kolaylaşmasına fayda sağlamıştır (Eberl, 2019: 43- 47).

1.2. Bilginin İşlenmesinde Üstel Büyüme

Yapay zekâ teknolojisinde bilginin işlenmesinde yaşanan gelişmeler ürünlerin imkân ve kabiliyetlerine doğrudan katkı sağlamaktadır. Yıllar içinde bu alanda önemli gelişmeler kaydedilmiştir. Örneğin; 1960 yılının üretilmiş olan ve Robot Shakey adı verilen bilgisayar o yıllarda 192 kilobaytlık bir çalışma belleği ile 12 bin hesaba dayalı işlem yapabiliyordu. 2011 yılına gelindiğinde ise; IBM'ın yazılım ürünü olan Watson bilgisayarı, Power 7 işlemcisiyle 80 trilyon işlem yapabilir seviyeye ulaşmış, 16 terabaytlık belleğe ulaşmıştır. Mikro işlemcilerde de benzer gelişmeler yaşanmıştır. Watson bilgisayarı, 1.2 milyar transistöre sahipti, oysaki 1971 yılı üretimi olan Intel 4004 adlı mikro işlemcinin transistör sayısı 2300 adettir. Watson bilgisayarının insanlı rakiplerine karşı katıldığı yarışmada insanları mağlup etmesinin sebebinin hesaplamadaki hız ve depolanabilir verilerin artışı olduğu açıktır.

Son yıllarda bellek çiplerinde kullanılan iki boyutlu yassı silisyum çipleriyle ilgili olarak; beyin yapısına benzer şekilde katmanlar oluşturulması ve bu katlar arasında çapraz bağlantılar kurulmasının sağlanması, beyindeki süreçleri elektriksel olarak taklit etmeyi sağlayan nöromorfik çiplere odaklanılması, bilgisayar çiplerinde silisyum yerine karbon grafen veya genom molekülü kullanan bilgisayarların geliştirilmesi, bilgileri elektrik yükü olarak değil elektrik direncindeki değişimle kaydeden nanobellek hücrelerinin kullanılması işlemleri üzerinde durulan çalışmalar olarak yer almıştır.

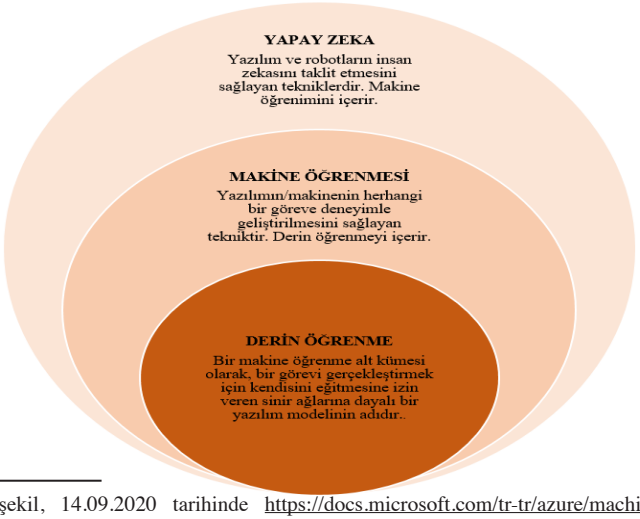
1.3. Makine Öğrenimi Tekniklerinin Yazılım Alanına Katkısı

Yapay zekâya ilişkin çalışmaların en önemli sıçraması, tahmin ve karar işlemi yapma sırasında kullanılan makine öğrenmesi ve derin öğrenme yeteneğine ulaşma ile sağlanmıştır. Önceden algoritma çalışmaları, mantıksal ve matematiksel işlemlerin kodlandığı bir işlemler bütünü iken, makine öğrenmesi açık bir programlanmaya gerek duyulmadan bilişsel işlemler yapılmasına imkân veren algoritmaların sıralanmasıyla oluşturulmaktadır. Önceden sembolik yapay zekâ evresi olarak adlandırılan algoritma çalışmaları, mantıksal ve matematiksel işlemlerin kodlandığı bir işlemler bütünü iken, makine öğrenmesi açık bir programlanmaya gerek duyulmadan bilişsel işlemler yapılmasına imkân veren algoritmaların sıralanmasıyla oluşturulmaktadır. Makine öğrenmesi ise, önceki algoritmalar gibi açık bir programlanmaya gerek duyulmadan bilişsel işlemler yapılmasına imkân veren algoritmaların sıralanmasıyla oluşturulur

ve veriden öğrenme yeteneğine kavuşturulması sağlanır (Eberl, 2019: 44- 46; HBR, 2019: 59-60; Thinktech, 2020).

Derin öğrenme ise, Şekil-1'de gösterildiği üzere yapay sinir ağları adı verilen ağ diyagramlarına dayalı hesaplamalar yaparak ve katman olarak ifade edilen verinin özel bir tür temsili ile işlev görecek şekilde makine öğrenmesinin özel bir yöntemidir. Yapay sinir ağları arasında giriş, çıkış ve gizli katmanlar sayesinde yazılım bir öğrenme süreci geçirmektedir. Her katmanda, giriş verileri bir sonraki katmanın tahmini için kullanabileceği bilgilere dönüşmektedir. Yapay sinir ağların yapısındaki giriş, çıkış ve gizli katman sayıları öğrenme sürecinin önemini gösterir. Her katman, giriş verilerini bir sonraki katmanın belirli bir tahminine dayalı görev için kullanabileceği bilgilere dönüştürecek birimleri içermektedir. Bu süreç sayesinde kendi veri işleme aracılığıyla bilgiye ulaşır. Bu katmanlar, örnek verecek olursak bizim bir bütün olarak algıladığımız bir fotoğrafın en küçük bilgi içerebilen bir parçasından tam olarak fotoğrafa dönüşene kadar her aşamasını içeren temsili varlıkları tespit ederek ilerlemesine yaramaktadır (Yonck, 2019, 86; HBR, 2019: 59-60; Thinktech, 2020).

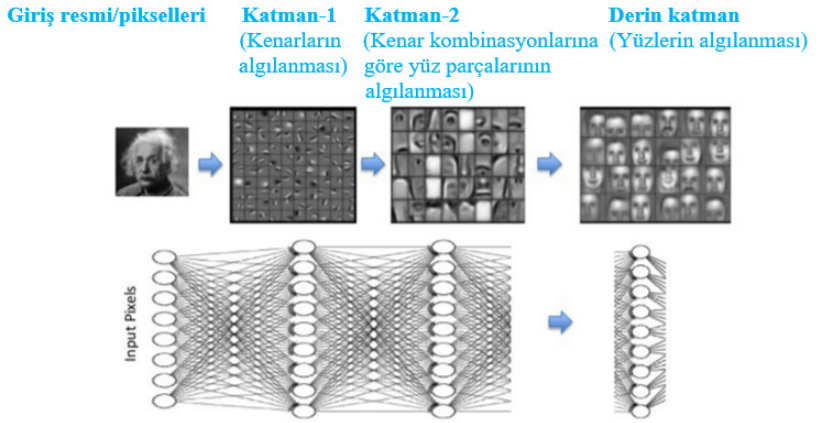
Şekil-1 Yapay Zekâ, Makine Öğrenmesi ve Derin Öğrenme İlişkisi (Microsoft,2020)[6]



6 Bu şekil, 14.09.2020 tarihinde https://docs.microsoft.com/tr-tr/azure/machine-learning/concept-deep-learning-vs-machine-learning adlı siteden alınarak geliştirilmiştir.

Yapay zekâ teknolojileri, makine öğrenmesi kapsamında derin öğrenmeyi içerecek şekilde yol almaktadır. Örneğin; Şekil-2'de yer alan derin öğrenme algoritması Albert Einstein etiketi olan veri fotoğrafını piksel boyutunda ayırarak tanımayı öğrenmektedir. Sayılara dönüştürülen bu piksellerde, 1'inci katmanda fotoğraf içinde yer alan kenarlar algılanırken, 2'nci katmanda fark edilir göz ve burun gibi hususları ayırt edilmektedir. Son katmandan ise; örnek gösterilen Einstein'e ait yüzlerce fotoğrafın ortak teması olan yüzler tespit edilmektedir. Etiketi belirli olmayan bir fotoğrafla karşılaşıldığında, bu resmin kime ait olduğunun tespitinde söz konusu işlemler geri besleme *(backpropagation)* algoritması gibi tersine mühendislik yoluyla giderilmektedir. Derin öğrenme algoritmaları, standart makine öğrenmesi algoritmalarında farklı olarak verinin yapısına göre hangi parametrelere ne ağırlık verileceğini kendisi keşfedebilmektedir (Yonck, 2019, 86; Yapayzekatr, 2020; Thinktech, 2020).

Şekil-2 Yüz Tespiti İçin Derin Öğrenme Algoritması (Thinktech, 2020)



1.4. Büyük Veri Kümelerine Ulaşabilme ve Kullanabilme

Yapay zekâya yeni bir yol açan derin öğrenme algoritmalarının hesaplama gibi işlev kazanabilmesi **için** daha fazla donanım ve veri kapasitesine ihtiyaç duyulmaktadır. Bu nedenle derin öğrenme algoritmaları için özel donanımların teminine gidilmektedir. Bu kapsamda geliştirilen bulut teknolojisi gibi bellek imkânlarının dışarıda depolanması, ihtiyaç duyulan verileri ve yazılımları dışarıdan kolaylıkla temin edilebilir hale getirmiştir. Bu sayede mobil

cihazlar artık ihtiyaç duydukları verileri ve yazılımları kendi içlerinde taşımak zorunda kalmamaktadır (Eberl, 2019: 44- 46).

Bilgisayarların iletişim performansları da fiber optik kablolu veya kablosuz olarak bir saniyede aktarılan veri miktarı bağlamında giderek gelişmektedir. Beşinci nesil 5G veri aktarım ağları sayesinde, saniyede 10 ila 50 gigabit yani saniyede on ile elli milyar arasında veri birimi aktarımı yapılması öngörülmektedir. Bu şu demek; 800 megabaytlık bir filmin 3G ile bir akıllı telefona indirilmesi dakikalarca, 4G ile bir dakika, 5G ile bir saniyeye düşmesidir. 20-25 yıl içinde mikroçiplerin işlem hızı ile bellek kapasitesi ve veri aktarım hızının bugüne göre bin katına çıkacağı değerlendirilmektedir. Bugün bir süper bilgisayarın yapabildiklerini 2040 ve 2050 yıllarında 500 dolarlık bir akıllı telefonun yapabileceği tahmin edilmektedir (Eberl, 2019: 43- 47).

1.5. Yapay Zekâ Teknolojilerine Devletlerin Sağlanan Mali Destekler

Yapay zekâya teknolojilerinin gelişmesine olanak tanıyan en önemli hususlardan biri ise; bu sektöre devletlerin savunma ve emniyet kurumlarının araştırma projeleri açısından sağladıkları finansal desteklerdir. Yapay zekâ teknolojilerinin 2030 yılına kadar küresel ekonomiye yaklaşık 15,7 trilyon dolara kadar katkıda bulunabileceği tahmin edilmektedir. 2000 ile 2015 yılları arasında, yapay zekâ teknolojileri destekli dünyada insansız askeri araçlar için yapılan harcamaların 2,4 milyar dolardan üç katına 7,5 milyar dolara çıktığı, 2025 yılına ulaşıldığında ise iki kat daha artarak harcamaların yaklaşık olarak 16,5 milyar dolara ulaşılacağı öngörülmektedir (Allen & Chan, 2017: 14).

2. Yapay Zekâ Teknolojileri Açısından Güvenlik

Günümüzde yapay zekâ teknolojileri ve güvenlik arasındaki ilişki sürekli ve etkileşim halinde bir seyir izlemektedir. Genel olarak yapay zekâ ve güvenliğin karşılıklı ilişkisi şu esaslar üzerinden tartışılmaktadır (Allen & Chan, 2017: 1-5).

- Yapay zekâ teknolojilerinin etkilerinin devletlerarasında rekabeti artırabilirliği,
- Yapay zekâ teknolojilerinin güvenlik açısından *önemi bilindikçe*, devletlerin asimetrik üstünlük kazanmak adına askeri silah sistemle-

rinde, komuta kontrol yöntemlerinde ve lojistik alanda bu teknolojilerden faydalanması,

- Bir ülkenin kamu güvenliği bağlamında yapay zekâ teknolojilerinin etkilerinin ve katkılarının iç güvenlik açısından değerlendirilmesidir.

Yapay zekâ ve güvenlik arasında kurulan söz konusu ilişki esaslarının ilk iki hususu, ülkelerin ulusal güvenliğini korumak adına odaklanacağı alanları vurgularken son husus yapay zekâ ve teknolojilerinin toplum üzerinde güvenlik açısından olumlu ve olumsuz yönlerinin iç güvenlik bağlamında değerlendirilmesini gerekli kılmaktadır. Bu kapsamda, ilk önce yapay zekâ teknolojilerinin ulusal güvenlik ve müteakiben iç güvenlik açısından bir değerlendirilmesi yapılacaktır.

2.1. Yapay Zekâ Teknolojilerinin Ulusal Güvenlik Alanında Kullanımı

Ülkelerin ulusal güvenliğini etkileyen uluslararası güvenlik ortamında yapay zekâ teknolojileri; devletlerin askeri, bilgi ve ekonomik üstünlük mücadelelerinde belirleyici olabilmektedir. Yapay zekâ teknolojilerinin askeri açıdan yeni yetenekler kazandıracağı, bu imkânların nispeten zayıf ve küçük devletler açısından bir avantaj olarak kullanılabilir olacağı, diğer taraftan organize suç ve terör örgütleri açısından da bu kabiliyetin kazanılmasının hem siber alanda hem de fiziki açıdan terör saldırılarına maruz kalınabileceği hususları önemsenen konulardır. Bilgi üstünlüğü bağlamında bakıldığında, yapay zekâ yazılımlarının her türlü verinin oluşturulması, toplanması, ilişkilendirilmesi ve analizinde yetenekleri artırdığı açıktır. Diğer taraftan bu veri artışının, ülkelerin istihbarat faaliyetlerinde gerçeği olmayandan ayırt etmelerini daha da zorlaştıracağı, ikna edici yanıltıcı emare ve davranışlarla kolaylıkla karşılaşılabileceği de kabul edilmektedir. Yapay zekâ teknolojilerini kullanan hasmın sahte ses, görsel vb. veriler ile devletin kurumsal itibar ve güvenini yıpratacak eylemlere neden olabileceği kabul edilmektedir. Ekonomik üstünlük bağlamında değerlendirmeler ise, yapay zekâ teknolojilerinde yaşanan gelişmelerin sanayi sonrası yeni bir toplum modeli ortaya çıkaracağına ilişkin görüşlerdir. Bunun da uzun vadede nüfusu az olan küçük ülkelerin ağırlıklarını artırmak için bir fırsat yaratacağı kabul edilirken nüfusu çok olan ülkelerde toplumsal dönüşümün istihdamı olumsuz olarak etkileyerek işsizliği artırmaya neden olacağı tahmin edilmektedir (Allen & Chan, 2017: 1-5). Ulusal güvenlik açısından yapay zekâyla ilgili genel olarak devletlerin;

- Teknolojik liderliğe ulaşmak için çaba sarf etmesi veya ulaşmış ise bu üstünlüğünü korumak için gayret göstermesi,
- Yapay zekâ teknolojilerinin barışçıl amaçlarla kullanılmasının teşvik edilmesi ve uluslararası barış ortamına katkı yapabilme imkânı,
- Yapay zekânın suç ve güvensizlik yaratacak yıkıcı risklerin önüne geçilmesinde liderlik etmeleri beklenmektedir.

Ülkeler çoğunlukla; yapay zekâ gibi önceden elde ettikleri teknolojik kazanımları sürdürmek veya bu imkâna sahip olmak için saldırı ve savunmaya yönelik uzun vadeli projeleri finanse etmeye gayret göstermektedir. Diğer taraftan bu teknolojilerin barışçıl kullanımının desteklenmesi amacıyla projelerde uluslararası işbirliklerin desteklenmesi de önemli bir kazanım olarak görülmektedir. Özellikle uluslararası antlaşmalarda hangi yapay zekâ teknolojilerinin kısıtlanması gerektiğine yönelik yükümlülüklerin belirlenmesi bu teknolojilerin yıkıcı etkilerinden korunmak için önemli bir avantaj olarak görülmektedir (Allen & Chan, 2017: 5-6).

Ülkelerin son yıllarda ulusal güvenliğine katkı sağlaması için askeri sistemler özelinde yapay zekâ ve robotik teknolojilerine ait araştırma ve geliştirme çalışmalarını artırdığı bilinmektedir. Ülkelerin *üzerinde çalıştıkları önemli* askeri projelerden birkaçı Tablo-2'de sunulmuştur. Söz konusu projelere bakıldığında, yapay zekânın komuta kontrol, karar destek yazılımları ve insansız otonom araçlarda kullanılabilirliğine odaklandıkları görülmektedir (Temuçin, 2020: 32-39).

Tablo-2 Askeri Alanda Yapay Zekâ Destekli Projeler (Temuçin, 2020: 40-47)[7]

Projenin Ülkesi/ Projenin Adı	Açıklamalar
ABD/Raven	Drone görüntülerinden insan ve nesneleri makine öğrenimi yönetimi ile ayırmak (İleri Keşif ve Gözetleme/Karar destek)
ABD/Mosaic Warfare	Harekât alanında yer alan askeri sistemlerin birçok silah ve sensörün bir araya getirilmesi ve bunların modüler yapıda kullanılması (Komuta Kontrol/Karar destek)
ABD/LOGSA	Her bir stryker Zırhlı araca takılı 17 sensörden alınan bilgilere dayanarak araçların bakım programlarının geliştirilmesi, böylece malzeme ve nakliye akışından tasarruf edilmesi (Lojistik/Karar destek)
ABD/ORCA	Mayına karşı tedbir, denizaltı ve su üstü savunma, elektronik harp için öngörülen otonom denizaltı aracı (Otonom araç sistemleri)
ABD/ Sea Hunter	Deniz harbi için otonom su üstü aracı (Otonom araç sistemleri)
ABD/Spot/LS3	Tekerlekli araçların kullanılamadığı arazilerde askerlere eşlik edecek 6 km hızla 150 kg malzeme taşıyan dört ayaklı katır (Otonom kara araçları)
Çin/JARI	Deniz ve hava savunma harbi için katamaran tipi, radar, lançer ve torpidoya sahip otonom su üstü aracı (Otonom deniz araçları)
İsrail/KATANA	Denizde keşif, gözetleme, arama kurtarma faaliyetleri için silah sistemlerine sahip, otonom veya 5 mürettebatlı olabilen manuel hareket edebilen otonom suüstü aracı (Otonom deniz sistemleri)
Rusya/Poseidon	Nükleer silahlara sahip, nükleer takatli otonom sualtı aracı (Otonom araç sistemleri)
Rusya/Automatic Control System	Hava sahasını tespit ve analiz eden otomatik hava savunma kontrol sistemi (Komuta Kontrol)
Rusya/Uran 9	Silah ve sensörlere sahip paletli tekerlekli insansız kara aracı (Otonom kara araçları)

Yapay zekâ teknolojileri, belirli işlevleri insan yeteneklerini aşan şekillerde öğrenebilen ve gerçekleştirebilen dijital mantık ve robotik sistemler olduğundan hasmın zayıflıkları ve kötü niyetli eylemlerinin tespiti için fırsat olarak görülmektedir. Yapay zekâ teknolojilerinin, askeri alanda ateş üstünlüğü, istihbarı bilgilerin elde edilmesi, karar destek, siber tehditlere karşı önlem geliştirilmesi gibi işlevsel alanda kullanılmasının asimetrik üstünlük sağlayacağı açıktır. Bu nedenle, uzun vadede tam otonom sistemlere doğru evrildikçe bu

7 Söz konusu tablo, Tolga Temuçin, *Yapay Zekâ Bilgi Kitapçığı*, Deniz Kuvvetleri Dergisi Eki, Sayı 630, Ankara, 2020, s.40-47 adlı eserinde bulunan tabloların kısaltılmış halidir.

teknolojilerin güvenliğe ilişkin yaklaşımları, stratejileri, tehditleri ve hukuku tümüyle değiştireceğine yönelik tahminler yapılmaktadır (HSSTAC, 2017: 1; Allen & Chan, 2017: 2-8).

2.2. Yapay Zekâ Teknolojilerinin İç Güvenlik Alanında Kullanımı

Yapay zekâ teknolojilerinin güvenlik üzerinde bir diğer etkisi de, bu teknolojilerin ***iç güvenlikte kullanılmasıdır.*** Yapay zekâ ve ***iç güvenlik arasında bir ilişki*** tanımlanmadan öncelikle olarak bir modern bir devletin iç güvenlik hizmetini yerine getirirken temel aldığı yaklaşımın tanımlanmasına ihtiyaç bulunmaktadır.

Ulusal güvenlik, temel aktörün devlet olduğu ve ülkeler arası rekabet ilişkilerine dayanan bir güvenlik yaklaşımıdır. İç güvenlik açısından ise, güvenliği sağlanan aktör devlet değil vatandaşlardır. Diğer bir ifadeyle bireyin kendisi, hak ve özgürlükleri ile maddi varlıklarının korunmasıdır. Günümüzde iç güvenliğe bakış, sadece toprağın ve devletin kendisinin korunmasının ötesinde, vatandaşın yaşamını, hak ve özgürlüklerini de teminat altına almaya yönelmiştir. Bu açıdan iç güvenlik hizmetleri, bir taraftan temel insan haklarını teminat altına almalı diğer taraftan halk sağlığının korunmasından afetlerden korunmaya, alt yapı ve sınır güvenliğinden asayiş, terörle mücadele gibi önleyici ve adli güvenlik tedbirlerine kadar güvenlik mekanizması oluşturmalıdır (Ak, 2019: 41-44). Böylece, dünyada genel olarak yapay zekâ teknolojilerinin ulusal güvenlik ve iç güvenlik açısından kullanımı arasında ki doğrudan bir ayrıma gidilmesinin temel nedeninin; ulusal güvenliğin uluslararası güvenlik ortamında ülkelerin hak ve menfaatleri korunması işleminde kullanılır iken iç güvenlikte ülkenin vatandaşının hak ve özgürlüklerinin teminat altına alacak eylemlere odaklanması olduğu anlaşılmaktadır (Ak, 2018: 88). Nitekim yapay zekâ teknolojilerinin iç güvenliğe etkisi bağlamında ki eleştiriler de burada ortaya çıkmıştır. Ulusal güvenlikten bağımsız olarak Asya'da vb. coğrafyalarda bulunan devletlerin yapay zekâ teknolojilerini otoriter rejimlerini daha da otoriter yapma aracı olarak kullanmalarına ilişkin görüşler bilinmektedir.

Yakın gelecekte, yapay zekâ teknolojilerinin ülkelerde toplumların iç güvenliğine etki edecek muhtemel tehdit ve risk alanları ise iki temel sorun üzerinden tanımlanmıştır. Bunlar;

- İlki; yapay zekâ teknolojilerinin sanayi sektöründe kullanılmasıyla artacak işsizlik ve toplumsal etkileridir. Bunlar daha çok toplumsal gösteri ve asayiş sorunları olarak ortaya çıkacaklardır.

- İkincisi; yapay zekâ teknolojilerinin kullanımı sayesinde ülkelerin kritik tesis ve altyapılarına siber saldırıların gerçekleştirilebilmesidir. Bu tesisiler nükleer tesis, baraj, bankacılık ve finans sektörü, metro hatları, elektrik ve su şebeke ve izleme sistemlerine saldırılar olarak ifade edilebilir.

Yapay zekâ teknolojilerinde yaşanan gelişmelerin yeni bir sanayi devrimiyle sonuçlanabileceği ilişkin görüşler hâkimdir. Bu değerlendirme, uzun vadede toplumda istihdam ve işgücü talebinde düşüşe neden olacağı ve işsizlik oranlarını artıracağı görüşünü desteklemiştir. Örneğin; yapay zekâ ve ilişkili robotik teknolojiler nedeniyle işgücü talebinde dramatik bir düşüşe yaşanacağı, ABD'de 25 ve 54 yaşları arasındaki erkeklerin üçte birinin bu yüzyılın yarısında işsiz kalacağı öngörülmüştür. Bunun 18'nci yüzyılda başlayan sanayi devrimine benzer olarak sermaye ve emek arasında ki ilişkiyi yeniden belirleyecek bir yola doğru ilerlediğini, sonuçta işgücü otomasyonunun sürekli artmasıyla işgücü kaynağı fazlalığına neden olacağı kabul edilmektedir. Ancak bu ifadeler şimdilik bir iddianın ötesine gitmemektedir. Almanya ise bu sürece daha olumlu bakmaktadır. İşsizliğin orta ve orta üst sınıfta gerçekleşebileceğini, bu insanların da diğer sınıflara yayılarak ve hizmet sektöründe çalışmaya başlayarak sorun olmaktan çıkacağını tahmin etmektedir (Allen & Chan, 2017: 1-5).

Aslında yapay zekâ teknolojilerinin iç güvenlik bağlamında kullanımı yukarıda açıklandığı üzere modern devletin ihtiyaç duyduğu iç güvenlik yaklaşımına katkı sağlayacak avantajlar üzerinden değerlendirilmesidir. İç güvenliğin sağlanmasında katkı sağlayacak yapay zekâ teknolojilerine bakıldığında genel olarak şu üç alanda uygulamaların gerçekleştirildiği görülmektedir (Alzou'bi vd., 2014:3).

- İlki; geliştirilmiş tahmine dayalı analiz sistemleri,
- İkincisi; geliştirilmiş görüş sistemleri ve biyometri,
- Üçüncüsü ise; optimizasyon ve kaynak tahsisidir.

Afetlere hazırlık, terörle mücadele, sınır güvenliği gibi faaliyetlerde yapay zekâ destekli geliştirilmiş tahmine dayalı analiz sistemlerden faydalanırken asayiş grevlerinin planlanması ve afetlere yardımlarda kaynak tahsislerinde optimizasyon ve kaynak tahsisi programlarından faydalanılabilir. Yapay zekâ destekli görüş ve sistemleri ve biyometri yöntemleri kullanılarak sınır güvenliğinde, terörle mücadelede, gümrük muhafazada yapay zeka destekli profil tanıma, karmaşık görüntülerin taranması ve gelişmiş sensör teknolojisinden faydalanılabilir.

Son yıllarda, iç güvenlik açısından yapay zekâ teknolojilerine ihtiyaç duymamızın en önemli nedenleri, artık devletin iç güvenlik kurumlarının görev alanlarıyla ilgili büyük miktarda dijital verilere sahip olması ve bu verilerin her geçen gün dijital sistemler vasıtasıyla yaratılıyor olması ve bu verilerin işlenmesi ihtiyacıdır. Artık iç güvenlik birimleri, görevlerinde başarıya ulaşabilmek için elde ettiği geçmiş verilerden tecrübe kazanmak ve elde ettikleri anlık verilerle doğru zamanda en uygun olan kararı almak istemektedir (HSSTAC, 2017).

İç güvenlik kurumlarında yapay zekâ yazılımlarının geliştirilmesinde ise;

- Öncelikle; veri, metin, görüntülerinden yani yığın veriden bilgi oluşturma,
- Müteakiben, bu bilgiler arası ilişki kurma,
- Son olarak ise, bu ilişki ağından geleceğe yönelik tahmin ve çıkarımlar yapma olarak gerçekleştirilmektedir.

Yapay zekânın kolluk kuvvetleri açısından kullanımı ise; icra ettikleri önleyici görevler ve adli kolluk faaliyetleri bağlamında açıklanmaktadır. Suçların işlenmesinin azaltılması için öngörülen önleyici kolluk hizmetleridir. Suçların aydınlatılması ve hukukun uygulanması ise kolluğun adli kolluk işlemleridir. Kolluk kuvvetleri, *ülkenin* anayasası ve anayasadan kaynaklanan kanunlarının yetkilendirdiği görevler bağlamında vatandaşlarının haklarını gözetmek, suç olarak öngörülmüş eylemlere karşı *önleyici tedbirler alma*k ve cezai adalet sisteminin uygulanmasını sağlamak *için bu teknolojilerden istifade edebilmektedir.*

Ancak bu hususta en önemli konunun açıklanması faydalıdır. Bu konu ise; bu faaliyetlerde yapay zekâ teknolojilerinde faydalanırken vatandaşın insan hakları hukukuna saygıda bulunulmasıdır. Yaşam hakkından, kişisel mahremiyetin korunması ve son yıllarda gittikçe önem kazanan kişisel verilerinin korunmasına dikkat edilmeli ve uyulmalıdır (Bayram, 2009: 17-43). Devletler genel olarak buna yönelik olarak kolluk kuvvetleri ve istihbarat birimlerinin *önleyici, koruyucu ve istihbari faaliyetler*inde *çerçeveyi belirleyerek bu hakların ihlal edilmemesi için yasal çerçevesini* belirlemektedir (Atlı, 2019: 5).

SONUÇ

Yapay zekâya ilişkin son birkaç yılda yaşananlar gelişmeler; bu teknolojilerin günlük hayatta ve sanayinin birçok alanında daha çok kullanılmasına vesile olmuş, bu durum ise bu teknolojilerin hem daha görünür olmasını sağlamış ve kamuoyu tarafından bilinebilirliği artırmıştır. Yapay zekâ, insan zekâsını modellenmesi olarak tarif edilmektedir. Bu modelleme ile yapay zekâ destekli bir yazılım veya makineden insan gibi anlamlandırma yapabileceği, bu bilgilerden öğrenerek bir hedefe ya da amaca dair ulaşabilme yeteneği ve karar verme yetisi beklenmektedir. Yapay zekâ teknolojilerinin barutun icadı veya nükleer silah gibi insanlık tarihine önemli bir devrimsel değişiklik yaratacağı zamanın teknolojinin tam otomasyon yeteneğine kavuştuğunda olacağı tahmin edilmektedir. Böyle bir anda bu teknolojilerin devletin güvenlik kurumlarının aktörlerinden stratejisine, organizasyon yapısından yeteneklerine kadar hepsini değiştireceğine kesin gözüyle bakılmaktadır.

Ülkelerin iç güvenliği açısından ise; yapay zekâ teknolojilerinden faydalanmanın yöntemleri benzer olmakla birlikte kullanım usullerinde farklılıklar vardır. Çünkü iç güvenlik faaliyetleri, ulusal güvenlik kurumlarından farklı olarak ülkede ki vatandaşlarının bizatihi kendisini merkez alır ve onların fiziki varlıklarının emniyetine odaklanır. Yapay zekâ teknolojilerinden istifade ederken; suçun önlenmesi ve asayişin sağlanmasından afetlerden korunma ve müdahaleye, kritik tesis ve altyapıların güvenliğinden siber savunmaya kadar öncelik vatandaşlarının yaşamı, huzuru ve refahını korumak ve idame ettirmektir. İç güvenliğin sağlanmasında yapay zekâ teknolojilerinden geliştirilmiş tahmine dayalı analiz sistemleri, görüş sistemleri ve biyometri ile optimizasyon ve kaynak tahsisi faaliyetlerinde faydalanılır. Afetlere hazırlık, terörle mücadele, sınır güvenliği gibi faaliyetlerde yapay zekâ destekli geliştirilmiş tahmine dayalı analiz sistemlerinden; asayiş grevlerinin planlanması ve afetlere yardımlarda optimizasyon ve kaynak tahsisi programlarından; sınır güvenliği, terörle mücadelede ve gümrük muhafazada ise yapay zeka destekli görüş sistemleri ve biyometri yöntemleri kullanılabilir. Diğer taraftan iç güvenlik kurumlarının görevlerini icra ederken vatandaşlarının insan hakları hukukuna saygı gösterecek şekilde yaşam hakkından, kişisel mahremiyetin korunması ve son yıllarda gittikçe önem kazanan kişisel verilerinin korunmasına kadar bağlı oldukları yükümlülüklere uyum göstermelidir.

Kaynakça

Ak, T. (2018). Dünyada ve Türkiye'de İç Güvenlik Yaklaşımının Değişimi ve İç Güvenlik Yönetimine Etkisi, *Van Yüzüncü Yıl Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 3 (6): 74-93.

Ak, T. (2019). "Yapısal Olarak İç Güvenlik Yönetimi: Türkiye'de Kolluk Örgütlenmesi", (içinde 41-72), *Türkiye'de İç Güvenlik Yönetimi*, (Ed. Tekin Avaner & Ozan Zengin), Ankara: Gazi Kitabevi.

Allen, G. & Chan, T. (2017). *Artificial Intelligence and National Security*. Harvard Kennedy School: Belfer Center for Science and International Affairs, USA.

Alzou'bi, S., Alshibly, H. & Al-Ma'aitah, M. (2014). Artificial Intelligence in Law Enforcement, *International Journal of Advanced Information Technology (IJAIT)*, 4 (4): 1-9.

Atlı, T. (2019). "Kişisel Verilerin Önleyici, Koruyucu Ve İstihbari Faaliyetler Amacıyla İşlenmesi", *Necmettin Erbakan Üniversitesi Hukuk Fakültesi Dergisi*, 2 (1): 4-22.

Baraniuk, C. (2020). AI fighter pilot wins in combat simulation, 28 June 2016, https://www.bbc. com/news/technology-36650848 23.10.2020

Bayram, Z. (2009). *Kolluğun, Suç Öncesi ve Sonrası Kişisel Veri Toplama Yetkisi*, Bahçeşehir Üniversitesi Sosyal Bilimler Enstitüsü, Kamu Hukuku Ana Bilim Dalı (Yayınlanmamış Yüksek Lisans Tezi), İstanbul.

Domingos, P. (2019). Master Algoritma, Çev.Tufan Göbekçin, Ankara: Paloma Yayınları.

Eberl, U. (2019). *Akıllı Makineler, Yapay Zekâ Hayatımızı Nasıl Değiştiriyor*, İstanbul: Poloma Yayınları.

Çobanoğlu, N. & Ak, T. (2020). "Yapay Zeka Nedeniyle Askeri Harekatta Paradigma Değişimi Yaşanır mı?.", *Global Savunma*, www.globalsavunma.com.tr/yapay-zeka-nedeniyle-askeri-harekatta-paradigma-degisimi-yasanir-mi.html (20.11.2020)

HBR/Harward Business Review (2019). *Dijital Dönüşüm Yapay Zekâ*, Çev.

Levent Göktem, İstanbul: Optimist Kitap Yayınevi.

HSSTAC/Homeland Security Science and Technology Advisory Committee (2017). *Artificial Intelligence White Paper*, Quadrennial Homeland Security Review Subcommittee.

Microsoft (2020). *Derin öğrenme ve makine öğrenimi karşılaştırması*, 05.03.2020. 12 Eylül 2020 tarihinde https://docs.microsoft.com/tr-tr/azure/machine-learning/concept-deep-learning-vs-machine-learning adlı siteden alınmıştır.

Say, C. (2019). *50 Sorusa Yapay Zekâ*, İstanbul: Bilim ve Gelecek Kitaplığı.

Tegmark, M. (2019). *Yaşam 3.0, Yapay Zekâ Çağında İnsan Olmak*, İstanbul: Pegasus Yayınları.

Temuçin, T. (2020). *Yapay Zekâ Bilgi Kitapçığı*, Deniz Kuvvetleri Dergisi Eki, Sayı 630, Ankara

Thinktech (2020). *Derin Farklar: Yapay Zekâ, Makine Öğrenmesi ve Derin Öğrenme*. 06 Ekim 2020 tarihinde https://thinktech.stm.com.tr/detay.aspx?id=182 adlı siteden alınmıştır.

Yapayzekatr (2020). *Derin Öğrenme Nedir?* 14 Eylül 2020 tarihinde https://www.yapayzekatr. com/2019/12/16/derin-ogrenme-nedir/ adlı siteden alınmıştır.

Yılmaz, A. (2017). *Yapay Zekâ*, İstanbul Kodlab Yayınları.

Yonch, R. (2019). *Makinenin Kalbi*, Çev. Tufan Göbekçin, Ankara: Paloma Yayınları.