



**YAPAY ZEKANIN; SAVUNMA, İSTİHBARAT VE
İNSAN HAKLARI BAĞLAMINDA
İNCELENMESİ**

(Yüksek Lisans Tezi)

Emine GÜNDÜZ

Kütahya - 2021

T.C.
KÜTAHYA DUMLUPINAR ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
Uluslararası İlişkiler Anabilim Dalı

Yüksek Lisans Tezi

**YAPAY ZEKANIN; SAVUNMA, İSTİHBARAT VE
İNSAN HAKLARI BAĞLAMINDA İNCELENMESİ**

Danışman:
Dr. Öğr. Üyesi Suat SÖYLEMEZ

Hazırlayan:
Emine GÜNDÜZ

Kütahya - 2021

Kabul ve Onay

Lisansüstü Eğitim Enstitüsü Müdürlüğüne,

Bu çalışma, jürimiz tarafından Uluslararası İlişkiler Anabilim/Anasanat Dalında YÜKSEK LİSANS tez çalışması olarak kabul edilmiştir.

Başkan.....

(İmza)

Dr. Öğr. Üyesi Suat SÖYLEMEZ (Danışman)

Üye.....

(İmza)

Dr. Öğr. Üyesi Ebru Deniz OZAN

Üye.....

(İmza)

Dr. Öğr. Üyesi Alptekin MOLLA

İmza

Prof. Dr. Şahmurat ARIK

Enstitü Müdürü

Bilimsel Etik Bildirimi

Yüksek Lisans tezi olarak hazırladığım “Yapay Zekanın; Savunma, İstihbarat ve İnsan Hakları Bağlamında İncelenmesi” adlı çalışmanın öneri aşamasından sonuçlandığı aşamaya kadar geçen süreçte bilimsel etiğe ve akademik kurallara özenle uyduğumu, tez içindeki tüm bilgileri bilimsel ahlak ve gelenek çerçevesinde elde ettiğimi, tez yazım kurallarına uygun olarak hazırladığımı, bu çalışmamda doğrudan veya dolaylı olarak yaptığım her alıntıya kaynak gösterdiğimi ve yararlandığım eserlerin kaynakçada gösterilenlerden oluştuğunu beyan ederim.

....../.../2021

Emine GÜNDÜZ

Özgeçmiş

Emine Gündüz ilk, orta ve lise öğrenimini Kütahya’da tamamladı. 2009 yılında Kocaeli Üniversitesi, Uluslararası İlişkiler Bölümü’nde başlayıp 2014 yılında mezun oldu. 2017 yılında Dumlupınar Üniversitesi Sosyal Bilimler Enstitüsü Uluslararası İlişkiler Anabilim Dalında Yüksek Lisans programına başladı.



TEŞEKKÜR

Tez çalışmam süresince desteğini esirgemeyen saygıdeğer hocam Dr. Öğr. Üyesi Suat SÖYLEMEZ'e, tez savunma jürimde yer alan değerli hocalarım Dr. Öğr. Üyesi Ebru DENİZ OZAN'a, Dr. Öğr. Üyesi Alptekin MOLLA'ya katkılarından dolayı teşekkür ederim. Ayrıca hayatımın her alanında olduğu gibi tez çalışmamı hazırlarken de yanımda olan aileme, manevi abim Halil KAYA'ya ve iş arkadaşım Mustafa EROL'a sonsuz teşekkür ederim.



ÖZET

YAPAY ZEKANIN; SAVUNMA, İSTİHBARAT VE İNSAN HAKLARI BAĞLAMINDA İNCELENMESİ

GÜNDÜZ, Emine

Yüksek Lisans Tezi, Uluslararası İlişkiler Ana Bilim Dalı

Tez Danışmanı: Dr. Öğr. Üyesi Suat SÖYLEMEZ

Haziran, 2021, 114 sayfa

Çalışmanın birinci bölümünde teknolojinin tarihsel gelişimi ele alınarak teknoloji ve insan arasındaki ilişki ortaya konulmaya çalışılmıştır. Yapay zekanın yeni bir alan oluşundan dolayı çalışmanın ikinci bölümünde yapay zekanın ne olduğu üzerinde durulmuş ve felsefi tartışması yapılmış ve yapay zekanın etkilediği alanlar üzerinde durulmuştur. Son bölümde ise yapay zekanın insan hakları üzerindeki etkisi tartışılmış ve uluslar arası hukukta oluşan yeni çerçeve ortaya konulmaya çalışılmıştır.

Çalışmada zaman zaman yapay zekanın olumlu etkilerine de yer verilecek olup ana hedef insan hakları ve siyasi alanda ve politik anlamda oluşabilecek riskleri ortaya koymaktır.

Anahtar Kelimeler: Endüstri 4.0, İnsan Hakları, İstihbarat, Savunma, Yapay Zeka

ABSTRACT**EXAMINATION OF ARTIFICIAL INTELLIGENCE IN DEFENSE,
INTELLIGENCE AND HUMAN RIGHTS****GÜNDÜZ, Emine****Master Thesis, Department of International Relations****Supervisor: Asst. Prof. Suat SÖYLEMEZ****June, 2021, 114 pages**

In the first part of the study, the historical development of technology is discussed. The relationship between technology and human has been tried to be revealed. Artificial intelligence is a new field of study. So, in the second part of the study, artificial intelligence is defined. The philosophical discussion of artificial intelligence has been made and the areas that it affects have been emphasized. In the last part, the effects of artificial intelligence on human rights is discussed. The new framework in international law has been put forward.

The positive effects of artificial intelligence will also be included in the study. The main goal of the study is to reveal the risks that may occur in the field of human rights and politics.

Keywords: Artificial Intelligence, Defense, Intelligence, Human Rights, Industry 4.0

İÇİNDEKİLER

Sayfa

ÖZET.....	v
ABSTRACT	vi
İÇİNDEKİLER	vii
TABLolar LİSTESİ.....	ix
ŞEKİLLER LİSTESİ.....	x
KISALTMALAR	xi
GİRİŞ	1

BİRİNCİ BÖLÜM TEKNOLOJİK DEVRİMLER

1.1. TEKNOLOJİNİN TARİHSEL GELİŞİMİ	8
1.1.1. Kol Gücünden Buhar Gücüne Geçilmesi (1770-1850).....	9
1.1.2. Buhar Makinesinin Yerini Elektrik Makinesinin Alması (1850-1900).....	10
1.1.3. Bilgisayarın İcadı ve Bilgi Teknolojilerinin Kullanımı	11
1.1.4. Endüstri 4.0 – Dördüncü Sanayi Devrimi.....	11
1.2. TEKNOLOJİ VE İNSAN	15

İKİNCİ BÖLÜM YAPAY ZEKA VE ETKİ ALANLARI

2.1. YAPAY ZEKA NEDİR?	18
2.1.1. Makine Öğrenmesi.....	22
2.1.2. Derin Öğrenme	24
2.2. YAPAY ZEKANIN FELSEFİ TARTIŞMASI VE ETİK BOYUTU.....	28
2.3. DÜNYADA YAPAY ZEKA UYGULAMALARI	33
2.4. YAPAY ZEKA VE RİSKLİ ALANLARI.....	39
2.4.1. Güvenlik, Gizlilik, Mahremiyet.....	39
2.4.1.1. Sosyal Medya ve Yapay Zeka.....	42
2.4.2. Adalet, Ön Yargı ve Hesap Verilebilirlik	47
2.4.2.1. Demokrasi	47
2.4.3. Siber Güvenlik	50
2.4.4. Yapay Zeka ve İstihbarat	57
2.4.4.1. Askeri İstihbarat.....	59
2.4.4.2. Sosyal Medya İstihbaratı (Açık Kaynak İstihbaratı)	60
2.5. YAPAY ZEKANIN SAVUNMA VE SAVAŞ ALANINA ETKİSİ.....	61

2.5.1. Yeni Savaş Stratejileri	68
2.5.1.1. Yapay Zeka Destekli Özerk Silahlar ve Uluslararası İnsancıl Hukuk	70

ÜÇÜNCÜ BÖLÜM

İNSAN HAKLARI VE YAPAY ZEKA İNSAN HAKLARI GENEL BAKIŞ

3.1. YAPAY ZEKANIN İNSAN HAKLARI ÜZERİNDEKİ ETKİLERİ	82
3.1.1. Eşitlik ve Ayrımcılık Yapmama Hakkı	86
3.1.1.1. Toronto Deklarasyonu	86
3.1.2. Kişisel Özgürlükler Hakkı	89
3.1.3. Gizlilik ve Mahremiyet Hakkı	89
3.1.4. Hareket Özgürlüğü Hakkı	91
3.1.5. İfade Özgürlüğü	92
3.1.6. Çalışma Hakkı.....	93
3.1.7. Sağlık Hakkı ve Yaşama Hakkı	95
3.2. ULUSLARARASI YENİ İNSAN HAKLARI ÇERÇEVESİ.....	96
3.2.1. AB Genel Veri Koruma Yönetmeliği (GDPR).....	96
3.2.2. BM'nin İş ve İnsan Hakları İlkeleri	97
3.2.3. Avrupa Konseyi Adaletin Etkinliği İçin Avrupa Komisyonu (CEPEJ)	97
SONUÇ	99
KAYNAKÇA	104
DİZİN	113

TABLÖLAR LİSTESİ**Sayfa**

Tablo 2.1: Yapay Zeka'nın Gelişim Aşamaları	21
--	----



ŞEKİLLER LİSTESİ

Sayfa

Şekil 1.1: Endüstri 4.0'ın Temel Bileşenleri	13
Şekil 2.1: Yapay Zeka, Makine Öğrenmesi ve Derin Öğrenme	23
Şekil 2.2: AI'nın Hesap Verebilirliği, Sorumluluğu ve Şeffaflığı.....	28



KISALTMALAR

AB	Avrupa Birliđi
ABD	Amerika Birleşik Devletleri
AI	Yapay Zeka
ARPA	İleri Araştırma Proje Ajansı (Advanced Research Project Agency)
AWS	Özerk Silah Sistemleri
BAE	Birleşik Arap Emirlikleri
BM	Birleşmiş Milletler
CASIC	Çin Havacılık, Uzay Bilim ve Sanayi Kurumu
CCW	Konvansiyonel Silahlar
CEPEJ	Avrupa Konseyi Adalet Etkinliđi İçin Avrupa Komisyonu
CIFAR	Kanada İleri Araştırma Enstitüsü(Canadian Institute For Advanced Research)
CITEAM	İstihbarat Grubu
CNAS	Yeni Amerikan Güvenlik Merkezi
DARPA	İleri Savunma Teknolojisi Proje Ajansı (The Defense Advanced Research Project Agency)
DART	Dinamik Analiz ve Yeniden Planlama Aracı
DIOT	Savunma Nesnelerin İnterneti
EDA	Avrupa Savunma Ajansı
EMI	Müzikal Zeka Deneyleri (Experience in Musical Intelligence)
GDPR	Avrupa Birliđi Genel Veri Koruma Yönetmeliđi
GPS	Küresel Konum Sistemi
ICCPR	Uluslararası İnsan Hakları ve Siyasi Haklar Sözleşmesi
ICJ	Uluslararası Adalet Divanı
IHA	İnsansız Hava Aracı
IHL	Uluslararası İnsancıl Hukuk
IHRL	Uluslararası İnsan Hakları Hukuku
IOT	Nesnelerin İnterneti
LOAC	Silahlı Çatışma Yasası
ML	Makine Öğrenmesi
MÖ	Milattan Önce

MTCR	Füze Teknolojisi Kontrol Rejimi
NBIC	Nanoteknoloji, Biyoteknoloji, Bilgi teknolojisi ve Bilişsel Bilimleri
SOMINT	Sosyal Medya İstihbaratı
UDHR	İnsan Hakları Evrensel Beyannamesi
USAF	Birleşik Devletler Hava Kuvvetleri
YZ	Yapay Zeka





TEZ METNİ

GİRİŞ

Geçmişten günümüze kadar toplumlar, belirli teknolojik gelişmelere şahitlik etmiş ve bu gelişmeler insanlık için önemli kırılma noktaları olup sosyo-kültürel, ekonomik ya da siyasi açılardan toplumlar üzerinde değişim ve dönüşümlere sebep olmuşlardır. Toplumsal yaşamı farklı tarihsel çağlar ile tanımlamak mümkündür.

İnsanlık M.Ö. göçebe yaşam tarzı benimsenen, tabiata ve iklime bağlılığın mecburi olduğu, temel gayenin hayatta kalmak ve diğer bütün sosyo kültürel ve ekonomik faaliyetlerin bu amaç etrafında şekillendiği bir toplum olan avcı- toplayıcı toplum olarak yaşamışlardır. Yerleşik hayatın başlamasıyla tarım toplumları ortaya çıkmış ve yazının da icadıyla değişimlerin insanlar üzerindeki etkisi hızla artmaya başlamıştır. Ardından gelen endüstri devrimi ile birlikte sanayiye dayalı, modern bir yaşam söz konusu olmuştur. Sanayi devriminden sonra ise insanlık; Bilgi Teknolojileri, Bilgisayarlar, Dijital Kültür vb. kavramların yer aldığı “Bilişim ve Bilgi Toplumu” olarak adlandırılan bir dönemle karşı karşıya kalmıştır. Teknoloji, son yıllarda çok daha hızlı gelişmekte ve tarihin her döneminde olduğu gibi toplumları da her açıdan değiştirmekte ve dönüştürmektedir. Tüm bu tarihsel değişimleri birbirinden kesin çizgilerle ayırmak mümkün olmayıp her yeni teknoloji bir öncekinin üzerine konulan bir değişim içermektedir.

İçinde bulunduğumuz dönemde tüm dünya; “Yapay Zeka” kavramının önem taşıdığı “Endüstri 4,0“ olarak adlandırılan yeni bir değişim ve dönüşüm ile karşı karşıyadır. Endüstri 4,0 döneminde Yapay Zeka’nın yanında dijitalleşme, robotlar, nesnelerin interneti, siber güvenlik gibi kavramlar da önem kazanmıştır. Çin gibi doğu toplumlarında üretim hızlı, ucuz ve yoğundur. Batı dünyası da bununla yarışabilmek adına, insan emeğini en aza düşürüp makineler sayesinde daha fazla ve daha hızlı üretim yapmak, insanı fabrikalardan çıkarıp makineler ile kesintisiz üretim yapılması ve insanı farklı alanlarda değerlendirmek hedeflenmektedir.

Peki bu “Yapay Zeka (Artificial Intelligence- AI)” nedir? Yapay zeka kavramını makine ya da bilgisayarların, bazı zihinsel süreçleri insana benzer şekilde yerine getirebilme kabiliyeti olarak tanımlamak mümkündür. Yapay zeka sayesinde makine ya da bilgisayarlar belirli süreçlerde; neden-sonuç ilişkisi kurabilme, tahmin

yürütme, problem çözme, algılama, tanımlama gibi faaliyetleri yerine getirebilmektedirler.

Çalışmanın ilgili bölümünde detaylı olarak ele alındığı üzere; Yapay Zeka, makine öğrenmesi ve derin öğrenme kavramları dıştan içe doğru birbirini kapsayan kavramlar olarak karşımıza çıkmaktadır. Makine öğrenmesinde, eldeki veriler ile makinenin nasıl öğreneceği makineye tanıtılır iken; derin öğrenmede ise, makine binlerce veriyi işleyerek nasıl öğreneceğini de kendisi öğrenmektedir.

Teknoloji ve insan, tarihin her döneminde birbirini etkileyen kavramlar olarak değerlendirilmiştir. Yine günümüzde de teknolojik gelişmeler insan yaşamını derinden etkilemekte ve birçok yeniliği de beraberinde getirmektedir.

Çalışmada, yapay zekanın insan üzerindeki siyasi ve hukuki etkileri genelde olumlu ve olumsuz yönleriyle tartışmalı bir biçimde ele alınmıştır. Her nasıl Sanayi Devrimi ile birlikte insanların işlerini kaybetme korkusuyla ortaya çıkan tartışmalar yaşanmışsa günümüzde de buna benzer tartışmalar yaşanmakta ve yapay zekayla birlikte insanların yaşamını riske atacak durumlar tartışılır hale gelmiştir. İşsizliğin ortaya çıkabileceği, veri güvenliğinin kötü amaçlı kullanımı, siber güvenlik, insan hakları, sosyal medyanın hayatın her alanını ortaya koyması vb. konular yapay zeka ile birlikte hızla gündeme gelen konulardır.

Çalışmada üzerinde durulan önemli bir konu da yapay zekaların karar verme aşamasında ortaya çıkan etik problemlerdir. Bu konuda önem arz eden asıl konu yazılımları oluşturacak insanların tamamının etik kurallara sahip olmamasıdır. Fiziksel kontrol mekanizması verilen makineler üretilirken ve yazılımlar yazılırken etik kurallara dikkat edilmeli ve temel etik kontroller sağlanmalıdır. Yapay zekânın etiklik ve ahlaki açıdan sorumluluğunu tartışan en önemli örnekler otonom araçlar üzerinden karşımıza çıkmaktadır. Otonom araçların her hangi bir kaza durumunda sürücüyü mü yoksa karşıdan gelen bebekli kadını mı koruyacağı tartışması sık sık karşımıza çıkmaktadır. Robotların karar verme aşamasında kararsızlığa düşmemesi gerekmekte ve bunun için de etik kurallar belirlenip makinelerin vereceği kararlar kontrol altında tutulmalıdır.

Yapay zekânın etiklik ve ahlaki boyutu sadece otonom araçlar üzerinden tartışılmaz. Son zamanlarda yapay zekâ destekli teknolojiler ülkelerin ana hedeflerinden biri haline gelmiş olup siyasi alandan savunma sanayiine, tıptan eğitime

ve ekonomiden uluslararası ilişkilere kadar her alana yayılmış durumdadır. Ülkelerin gelişmişlik ve güç seviyelerinin artık yapay zekâ üzerinden değerlendirildiği bir döneme girmiş bulunmaktayız.

Konu siyasi anlamda ele alındığında; yapay zekanın demokrasi ya da seçimler üzerindeki etkisinin nasıl olacağı konusu önem arz etmektedir. Sosyal medyanın da kullanılmasıyla, yapay zekalı yazılımlar ile kişilere özel propagandalar oluşturulabilmekte ve böylece bireylerin karar verme aşamaları etkilenebilmektedir. Tüm bunlar düşünüldüğünde bu durumların etik ve ahlaki açıdan tartışılması da kaçınılmaz hale gelmiştir.

Günümüzde ülkeler arasında; bir devrim niteliği taşıyan yapay zekanın yarışı başlamış ve bu alana yapılan yatırımlar hızla artmakta olup bu ülkelerin başında Çin, ABD ve Avrupa ülkeleri gelmektedir. Bu ülkeler oluşan yeni düzende yerlerini almaya çalışmakta ve tüm güvenlik ve ekonomi politikalarını yapay zeka destekli teknolojiler ile sürdürmeyi amaçlamaktadırlar. Belirtilen ülkelerin yanı sıra; Kanada, Güney Kore, Hindistan, BAE ve Türkiye gibi ülkeler de bu yarış takip etmekte ve buna uygun politikalar geliştirmektedirler.

Yapay zekanın etki alanları düşünüldüğünde bu alanların başında güvenlik, gizlilik, mahremiyet, adalet, hesap verebilirlik, siber güvenlik, istihbarat, savunma ve insan hakları gibi konular gündeme gelmektedir. Toplum önyargılarının makinelere devredilmesi bazı kesimleri daha dezavantajlı konuma getirebilecek ve adaletin sağlanması konusunda sıkıntılar meydana gelebilecektir. Sosyal medyanın hayatın bir parçası haline gelmesiyle büyük veri oluşumları ortaya çıkmış ve buna bağlı olarak gizlilik ve mahremiyet konuları önem kazanmıştır. En göze çarpan sosyal medya örnekleri Facebook, Twitter ve Instagram gibi uygulamalardır. Neredeyse toplumun tamamı bu mecraayı kullanmakta ve ister istemez veri oluşumuna katkıda bulunmaktadır. Büyük veri çağında algoritmalar aracılığı ile bireyi kendisinden daha iyi tanıyan yazılımlar mevcut olup, bu verilerin kötü niyetli kullanılabilmesi ve suistimal edilmesi söz konusu olmaya başlamıştır. Bunlar bireysel güvenlikle ilgili konular olup, bunların dışında yapay zekanın ulusal güvenlik üzerindeki etkileri de büyüktür. Yine sosyal medya aracılığı ile ülkelerin siyasi, ekonomik ve toplumsal alanlarda risk oluşturabilecek yanıltmalar söz konusu olabilmektedir.

Sosyal medya ile bağlantılı olarak tartışılan konuların başında “demokrasi” gelmektedir. Büyük veri kullanımı ve fazla bilgi akışına bağlı olarak yanlış bilgilendirmeler ya da yanlış propagandalar insanlar üzerinde etki yaratacak ve demokrasiyi ve istikrarı tehdit edebilecek konumlara gelecektir. Cambridge Raporuna göre tüm dünyada bu yanıltmalar git gide daha çok olacak ve sahte yanıltıcı bilgilerin yayılması artacaktır.

Yapay zekâ ile ilgili en önemli konulardan biri de siber güvenlidir. Modern toplumlarla beraber bilgisayar devrinin başlamasıyla ülkeler arasındaki güç kriterleri değişmiş ve günümüzde teknolojiyi en etkin ve verimli kullanan ülkeler güçlü hale gelmişlerdir. Ülkelere ait özel ve gizli bilgilerin devlet dışı aktörler ve düşmanlar tarafından ele geçirilmesi konuları siber güvenliğin önemini ortaya koymaktadır. Aynı zamanda ülkelerin bu bilgilerini koruyabilmesi için de ortaya çıkaracağı sistemler bu konuda önem arz etmektedir. ABD gibi bu alanda güçlü olan ülkeler, yazılımlarını risklere karşı koruyabilecek şekilde sistemler oluşturabilmekte ve bu yönde politikalar uygulayabilmektedirler. Yapay zekanın alt dalı olan makine öğrenme yaklaşımları bu alanda da kullanılabilmekte ve siber savunma alanında, tehditleri anlamada ve buna uygun çözüm üretmede etkin rol üstlenmektedirler.

Siber güvenlik konusunda yapay zeka teknolojileri hem savunma hem de saldırı olmak üzere iki alanda kullanılmaktadır. Yapay zekanın siber güvenlik alanında savunma amaçlı kullanımı ile ilgili örneklerinden biri kötü niyetli yazılımların tespit edilebilmesidir. Aynı teknoloji başkalarının ya da başka ülkelerin sistemlerine saldırmak için de kullanılabilmektedir. AI yetenekleri ve makine öğrenme sistemleri ile gelebilecek saldırıların tespiti bir insanın yapabileceğinden çok daha kolay hale gelmiştir.

Günümüzde artık geleneksel savaş yöntemleri önemi kaybetmiş ve modern teknolojilerin ve yapay zekaların kullanıldığı siber savaş ortamları oluşmuştur. Siber sistemler sadece ülkeler bazında ya da kamu alanında değil özel şirketler kapsamında da kullanılan sistemlerdir. Şirketler ağlarını siber saldırılara karşı korumak için bu alanda ciddi yatırımlar yapmaktadırlar. Siber saldırıların tespiti için güvenlik duvarları, izinsiz girişi önleme sistemleri vs. kullanılmaktadır. Algoritmalar sayesinde izinsiz girişler önlenilmekte ya da saldırılar gerçekleşmeden önce durum tespiti yapılabilmektedir.

Yapay zeka teknolojilerinin etkilediği bir diğer alan da “istihbarat” olup siber güvenlik konusu ile yakından ilgilidir. İçinde bulunduğumuz dönemde istihbarat teknolojilerini geliştirmek ve kullanmak devletlerin temel amaçları arasında bulunmaktadır. İstihbarat ve teknoloji birbirleri ile yakından ilişkili kavramlar olarak karşımıza çıkmaktadır. İstihbarat alanında her zaman teknolojiden yararlanılmış ve teknolojinin gelişmesine bağlı olarak istihbarat sistemleri de gelişme göstermiştir. Gelişen sistemler arasında; sinyal istihbaratı, bilimsel algoritmalar ve büyük veri işlemciliğine bağlı sistemler gösterilebilir. Ülkeler bazında istihbarat deyince, devletlerin savunma sistemlerini güvenli bir şekilde sürdürebilmeleri açısından akla ilk gelen askeri istihbarattır.

Soğuk savaş sonrası dönemde yeni savaş türlerinin ortaya çıkması, oluşan yeni dengeler, güvenlik alanındaki yeni stratejiler ve artan küreselleşme gibi etkenler teknoloji-bilim ve istihbarat alanlarında da yeniliklere neden olmuştur. Yapay zeka teknolojilerinin algılama, problem çözme, tanıma, öğrenme, bilgileri işleme gibi yetenekleri göz önünde bulundurulduğunda istihbarat örgütlerinin casusluk ya da karşı casusluk için bu sistemleri etkin bir biçimde kullanmaları söz konusudur. Askeri istihbaratta genel olarak sinyal istihbaratı, insan istihbaratı, görüntü istihbaratı ya da sosyal medyanın istihbaratı da denilen açık kaynak istihbaratı kullanılmaktadır. Görüldüğü üzere istihbarat sistemlerinin neredeyse tamamı yapay zeka teknolojisini gerektiren sistemlerdir. Sosyal medya istihbaratı, bireylerin sosyal medya üzerinden yapmış oldukları paylaşımlardan elde edilen bilgilerin kullanılmasıyla ortaya çıkan bir istihbarat türüdür.

Günümüzde yapay zeka destekli teknolojilerin savaş ve savunma ortamında etkin bir şekilde kullanılmasıyla birlikte bu alanlara yeni kavramlar da girmeye başlamıştır. Bunların başında “Nesnelerin İnterneti”, “Akıllı Makineler”, “Savaş Nesnelerin İnterneti (İnternet of Battle Things)” kavramları gelmekte olup savaş ortamında bulunan bir işlemcinin ya da fiziksel nesnelerin birbirleriyle bağlantılı olduğu bir ağ olarak karşımıza çıkmakta ve bu ağın bir çok veriyi toplayıp işleyebildiği bir sistemi ifade etmektedir. Tüm bu sistemlerle veri savaşları başlamış ve gelecekte bu sistemlerin çok daha karmaşık hale geleceği öngörülmektedir. Tüm bunların yanında otonom silah sistemlerinin de gelişmesiyle birlikte devletler arasındaki güç dengeleri bu

sistemlere sahip olmayla ilgili olacak ve güç eşitsizliklerinin artması konusu gündeme gelecektir.

Bütün bu teknolojik gelişmeler uluslararası hukuku yakından ilgilendirmektedir. Ülkeler kendisini koruma ve güçlü olma içgüdüleriyle bu sistemleri kullanmaya çalışmakta ve bu yarışa dahil olmaktadır. Bu teknolojilere yatırımların hızla arttığı bir ortamda ölümcül silahların ya da katil robotların kullanılmaya başlanması kaçınılmaz hale gelmekte ve hukuksal açıdan problemler ortaya çıkarmaktadır. Uluslararası bazı kuruluşlar bu sistemlerin kullanılmasının yasaklanmasını talep etmektedir. Burada önemli olan karar verme aşamasında tüm kontrolün makinelere devredilmeden, etik ve ahlaki boyuta uygun olarak insan tarafından kontrolün sağlanmasıdır. Günümüzde genel olarak insan kontrollü sistemler kullanılmasına karşın yakın gelecekte tamamen otonom sistemlerin yaygınlaşması söz konusu olacaktır.

Otonom silah sistemlerinin savunma ve savaş alanlarında hızla kullanılmaya başlanmasıyla bu konunun hukuki boyutu da önem kazanmış ve tartışılan konulardan biri olmuştur. Hızla değişen ve gelişen teknolojiye bağlı olarak bu yeni teknolojilerin hukuksal anlamda da karşılığı olmalı ve bu konuda çalışmalar yapılmalıdır. Savaş ve savunma alanında yapay zeka teknolojilerinin ülkelere büyük avantajlar sağlaması söz konusu olup geleneksel savaş ortamlarından uzaklaşmalar başlamış ve beyin ara yüzü sistemlerinden giyilebilir bilgisayarlara kadar bir çok yapay zekalı sistemler savaş ortamlarında kullanılmaya başlamıştır. İnsan gücüyle çok daha uzun zaman alan işlemlerin, AI teknolojileri ile daha kısa sürede ve daha verimli bir şekilde hedefe ulaşması amaçlanmaktadır.



BİRİNCİ BÖLÜM
TEKNOLOJİK DEVRİMLER

1.1. TEKNOLOJİNİN TARİHSEL GELİŞİMİ

Dünya hızla değişmekte ve dönüşmektedir. Çalışmanın bu bölümünde toplumsal yaşamı etkileyen önemli süreçler kronolojik olarak ele alınacaktır. Geçmişten günümüze yaşanan önemli dönemleri; avcı- toplayıcı – göçebe toplum, tarım toplumu ve sanayi devrimi olarak sıralamak mümkündür. Günümüzde ise dünya, “Endüstri 4.0” kavramı ile karşı karşıyadır. Tarih boyunca dönüşümlere ve sanayi devrimlerine uyum sağlayabilen ülkelerin gelişmişlik seviyeleri artış göstermiş ve refah düzeyleri de artarak devam etmiştir. Günümüzde önemli olan; dijital dünyanın, makinelerin ve yapay zekanın getirmiş olduğu yeni süreçlerin toplumlar tarafından kavranabilmesi ve dijital üretime dayalı davranışlar geliştirilebilmesidir.

Sanayi devrimleri, sosyo- teknoloji açıdan değerlendirildiğinde, hepsinin temel yapısının ekonomik anlamda üretkenliği artırdığı ve sosyal yaşamı değiştirdiği göze çarpmaktadır. Yani bu devrimlerle birlikte üretim maliyetleri düşmüş ve aynı zamanda sınırsız bir arz ortaya çıkmıştır. Yaşanan her sanayi devriminin ardından milli gelir düzeyleri artarak devam etmiştir (Yarman ve Denemeç, 2016: 4).

Tarihin ilk çağlarında Avcı- toplayıcı toplumlar söz konusuydu. Bu toplumlar tarihin büyük bir kısmında yer edinmekle birlikte, insanlığın bütün yaşam tarzını etkileyen bir dönem olarak karşımıza çıkmaktadır. İklim koşullarına ve tabiata bağlılığın zorunlu olduğu göçebe bir hayat tarzı söz konusudur. Bu toplumlarda önemli olan hayatta kalabilme mücadelesi olduğundan insanların yaşam tarzları da buna bağlı olarak şekillenmiştir. Belli bir işbölümü etrafında şekillenen yaşam tarzında erkekler avcılığı, kadınlar ise bitki toplamayı vs. öğrenmelidir. Belli bir gelecek kaygısının olmadığı bu dönemde temel amaç sadece insanların kendi varlıklarını sürdürebilme çabası olmuştur. Yazının icad edilmediği bu dönemde sadece sözlü kültürden bahsetmek mümkündür.

Tarihin büyük bir bölümünü kapsayan Avcı- Toplayıcı toplumlardan sonra; MÖ 6000’li yıllarda ise tarım toplumları ortaya çıkmıştır. Tarım toplumları yerleşik hayata geçilmesiyle ortaya çıkmış ve insanların yaşam tarzlarını değiştirmiştir. Bu dönemde toprak ve kas gücü en önemli üretim araçları olarak karşımıza çıkmaktadır. Bu toplumlarda insanlar çevrede buldukları hayvanları ve bitkileri yiyecek olarak kullanmışlardır. Geleneksel teknoloji ile birlikte gıda kaynaklarını nasıl

genişleteceklerini öğrenmişlerdir (Ayu, Indria and Sueb, 2013: 2). Yerleşik hayata geçilmesiyle birlikte yazı icad edilmiş (MÖ 3500) ve zaman içerisinde yazılı kültür ortaya çıkmıştır.

Tarım toplumlarından sonra ise, Endüstri toplumu oluşmaya başlamıştır. Endüstri toplumunda bilim ve teknoloji kavramları birbirine yakın hale gelmeye başlamış ve bu toplumlarda modern yaşam söz konusu olmakla birlikte Matbaa ortaya çıkmış ve seri üretilmeye geçilmiştir. Sanayi devrimi ile birlikte yeni üretim araçları ve ortamları ortaya çıkmış ve bu da insanların geleneksel yaşam tarzlarını da değiştirmiştir. Fabrikalarda üretim yapılmaya başlanmasıyla şehirler bu fabrikaların etrafında kurulmaya başlanmış ve kentsel anlamda değişiklikler ortaya çıkmıştır. Aristokratlar yerine sermaye sahibi olan burjuvazi toplumun saygın kesimi olmaya başlamıştır (Günay, 2002: 1).

Buhar makinesi ve daha sonrasında elektrik enerjisinin kullanılmaya başlanmasıyla endüstriyel yapı değişime uğramış ve toplumsal yapıyı etkilemiştir. Geline nokta da yine enformasyon teknolojileri tüm dünyayı değiştirmekte ve toplumsal yapıyı dönüştürmektedir (Dağıtmaç ve Özbay, 2018: 55).

Endüstrinin geçirdiği dönüşümleri dört ana başlık altında sıralamak mümkündür:

1.1.1. Kol Gücünden Buhar Gücüne Geçilmesi (1770-1850)

Endüstri devrimi, 1712 yılında buhar makinesinin icad edilmesiyle başlamış ve kas gücü yerine buhar gücünün kullanılmaya başlanmasıyla bir dönüşüm yaşanmıştır.

Birinci sanayi devriminin öncüsü olan Birleşik Krallık sahip olduğu demir ve kömür rezervleri sayesinde bu devrimi başlatabilmiş ve zamanla bu devrim tüm dünyaya yayılmıştır. Dokuma tezgahlarında insan gücü azaltılmıştır. Demir ve tekstil endüstrileri, sanayi devriminin temel rollerini almaya başlamıştır. Buhar makineleri sadece demir ve tekstili değil aynı zamanda iletişim, bankacılık, ulaşım ve genel yaşam tarzını da derinden etkilemiştir. Üretim malzemeleri çeşitlendikçe üretim de artmaya başlamış ve işçi sınıfları ortaya çıkmıştır. Günümüzde de karşılaşıldığı üzere her yeni gelişen teknolojiye bağlı olarak toplumda meydana gelen sosyal-psikolojik durumların etkisiyle otomasyona karşı çıkan insanlar söz konusudur. Bu durum birinci sanayi

devriminde de söz konusu olmuş ve bu insanlar direniş için fabrikalara saldırmış, makinelere zarar vermişlerdir (Özdoğan, 2017: 16).

İngiltere’de öncelikle buhar makinası icat edilmiş, ardından atmosferik buhar makinası kullanılmaya başlanmış ve ticari üretimine geçilmiştir. Buhar makinasının tren ve gemilerde kullanılmaya başlanmasıyla da bu makine kas gücünün yerini almış ve sermayenin asıl ürünü haline gelmiştir (Günay, 2002: 5). Su gücünü üretimde kullanmak, su kanallarından hidrostatik basınç ve su debilerinin enerji kaynağına dönüştürülmesi birinci sanayi devriminin önemli adımları olarak karşımıza çıkmaktadır (Yarman ve Denemeç, 2016: 2). İlk mekanik dokuma tezgahı 1784 yılında icat edilmiştir (Dağıtmaç ve Özbay, 2018: 68).

1.1.2. Buhar Makinesinin Yerini Elektrik Makinesinin Alması (1850-1900)

İkinci sanayi devrimi ile elektrik iletişimi ve fosil yakıtlar, özellikle de petrolle çalışan içten çalışan yanmalı motorlar kullanılmıştır (Glowacki ve Dudka, 2013: 50).

Petrol endüstrisi 1848 yılında İskoçya’da başlamıştır (Özdoğan, 2017: 20). Birinci sanayi devrimi ile ikinci sanayi devrimi arasındaki en önemli fark ikinci sanayi devriminde üretim kapasitelerini artıran yeni makinelerin kullanılmaya başlanmasıdır. İkinci sanayi devrimi ile birlikte dünya tek bir merkez haline gelmeye başlamış yani küreselleşme gerçekleşmeye başlamıştır (Özdoğan, 2017: 18). Bu dönemde yeni teknik ilerlemeler kaydedilmiş ve içten yanmalı motor, telefon, telgraf ve elektrik motoru gibi araçlar icat edilmiştir. İkinci Sanayi Devrimi olarak adlandırılan bu dönemde elektrik endüstrisi ve nükleer enerji ekonomik sisteme dahil olmuştur (Günay, 2002: 6).

İlk hareketli bant sistemi mezbahane kullanımı 1870 yılında kullanılmıştır (Dağıtmaç ve Okan Özbay, 2018: 68).

Bu dönemdeki bir diğer önemli gelişme, “Elektromanyetik Alanlar Kuramı”nın Maxwell tarafından hayata geçirilmiş olmasıdır. ancak elektro-teknik henüz gelişmemiş olması sebebiyle bu kuramın döneme açık bir katkısı söz konusu değildir (Yarman ve Denemeç, 2016: 2).

Bu dönemdeki gelişmelere kısaca bakılacak olursa; içten patlamalı motorlar icad edilmiş, haberleşme, ulaştırma ve tıp alanlarında gelişmeler yaşanmış ve elektrik enerjisi ile seri üretime geçilmiştir.

1.1.3. Bilgisayarın İcadı ve Bilgi Teknolojilerinin Kullanımı

Üçüncü Sanayi Devrimi 1969 yılında başlamış ve üretimde hız kazanmak ve otomatikleşmek amacıyla bilişim- elektronik alanlarında ilk Programlanabilir Mantıksal Denetçi (PLC) kullanılmaya başlanmıştır (KPMG, 2015: 1). Bu kısaca; bilgi ve elektriğin beraber kullanılmasıdır. Bilginin insan hayatı için önemi çok fazla olup bilgisayar ve internet erişimi insanlar için büyük oranda yarar sağlamaktadır. Örneğin, ekonomi, hava durumu, haberler vb. insanlara problem çözme ve karar verme noktasında yardımcı olmaktadır. Bilginin geliştirilmesi iletişimin geliştirilmesi ile ilgilidir ve bilgi medyasının insan hayatındaki rolü önceki devrimlerden çok daha etkili olmuştur (Thohari, 2013: B11-4). Bu dönemde makine mühendisliği giderek karmaşıklaşmış ve artık yenilenebilir kaynaklar söz konusu olmaya başlamıştır. Üçüncü Sanayi Devrimi ile dijital çağ ortaya çıkmış ve insan ile doğa arasındaki bağ çok daha artarak ilerlemeye başlamıştır (Pauli ve Ünür, 2017: 16). Üçüncü Sanayi Devrimi için “Dijital Devrim” kavramı da kullanılmaktadır. Bu dönemin ana faktörleri bilgisayarlar, internet ve dijital ürünlerdir. Bu dönemde her bilgi bilgisayarlara aktarılmaya başlanmıştır. Her devrimde olduğu gibi gelişen yeni teknoloji ile üretim artmış ve yeni pazarlar oluşmaya başlamıştır. Çin ve Hindistan bu dönemi en yakından takip eden ülkeler olarak karşımıza çıkmaktadır (Özdoğan, 2017: 24).

İnternet Üçüncü ve Dördüncü Sanayi devrimlerinin kilit noktasıdır. Dijital veri aktarımını sağlayan ve küresel bir ağ olarak tanımlanan internet, ilk kez 1969 yılında ABD ‘de kurulan ARPANET (Advanced Research Projects Agency Network) ile karşımıza çıkmıştır (Özdoğan, 2017: 29). En önce askeri amaçlarla gelişme gösteren internet daha sonradan ticaret alanına taşınmış, politik alanda da varlığını sürdürmeye başlamış ve son olarak tüketimin ve kontrolün kitleselleştiği bir araca dönüşmüştür (Dağıtmaç ve Özbay, 2018: 46).

1.1.4. Endüstri 4.0 – Dördüncü Sanayi Devrimi

Etkileri hala devam etmekle birlikte geride bırakılan üç sanayi devriminden sonra dünya bu kez Dördüncü Sanayi Devrimi ile karşı karşıyadır. Her devrim bir öncekinin devamı niteliğinde ve bir sonrakine zemin hazırlar bir şekilde ortaya çıkmakta ve devam etmektedir.

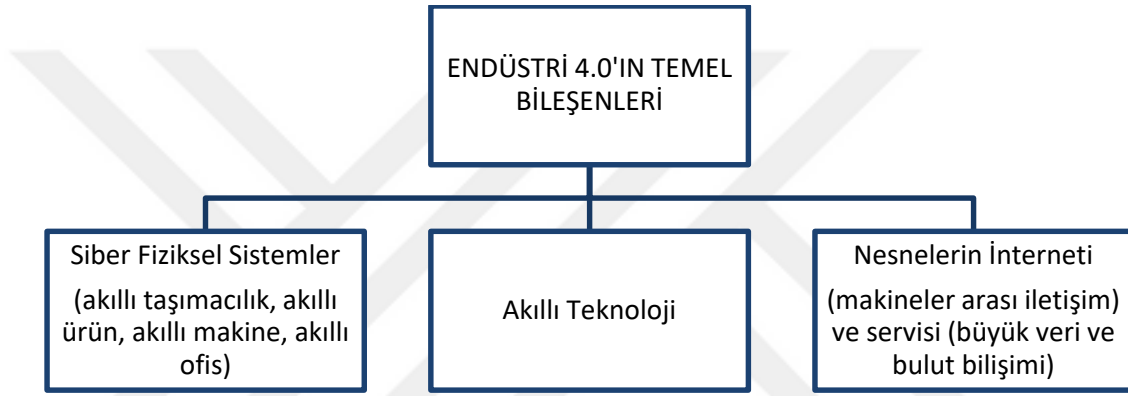
Endüstri 4.0; veri alışverişlerini, üretim teknolojilerini ve pek çok modern otomasyon sistemleri içinde barındıran bütüncül bir kavram olarak karşımıza çıkmaktadır (Dağıtmaç ve Özbay, 2018: 69).

Dördüncü Sanayi Devrimi, 2011 yılında Almanya ‘da gündeme gelen ve 2013’de Alman Hükümeti Çalışma Grubu’nun ortaya koyduğu bir rapor ile Endüstri 4.0 olarak adlandırılan içinde bulunduğumuz dönemi kapsamaktadır (Kılıç ve Alkan, 2018: 32). Bu raporda Endüstri 4.0’ın temel hedefleri ve sahip olduğu potansiyel amaçlar şu şekilde sıralanmıştır (Kagerman, Wahlster ve Helbig, 2013: 16):

1. *Bireysel müşteri gereksinimlerini karşılama*: Müşteriye özgü kriterlerin sipariş, planlama, üretim ve işletme aşamalarına dahil edilmesidir. Özel ürünler üretmek ve bunu yaparken de kar elde etmek amaçtır.
2. *Esneklik*: Mühendislik süreçlerinin daha çevik olması, geçici eksikliklerin telafi edilebileceği ve kısa sürede üretim artışlarının sağlanmasını ifade etmektedir.
3. *Optimize edilmiş karar alma*: Küresel pazarda başarılı olmanın ön şartı kısa sürede doğru kararlar alabilmektir. Endüstri 4.0 üretim alanlarında şeffaflık sunarak, tasarım kararlarının erken doğrulanmasını sağlayacaktır.
4. *Kaynakların verimli kullanılması*: Belirli bir kaynak hacminden mümkün olan en düşük miktarda kaynağı kullanarak en yüksek ürün çıktısı alınmasını ifade etmektedir.
5. *Yeni hizmetler yoluyla değer fırsatları yaratmak*: Akıllı algoritmalar; akıllı cihazlar tarafından kaydedilen birçok farklı veriye uygulanabilecektir. Böylece yeni istihdam biçimleri ortaya çıkacaktır.
6. *İşyerlerinde demografik değişimlere yanıt verebilmek*: Endüstri. 4.0 insanların çalışmaya devam etmesini ve daha uzun süre üretken kalmalarını sağlayacak çeşitli kariyer yollarını mümkün kılacaktır.
7. *İş ve yaşam dengesi oluşturmak*: CPS’ler sayesinde daha esnek çalışma organizasyonları yapılabilecek ve böylece çalışanların kişisel ihtiyaçlarını ve şirketlerin gereksinimlerini karşılamak için yeni bir esneklik standardı oluşturulacaktır.
8. *Rekabetçi ve yüksek ücretli bir ekonomiye sahip olmak*: Endüstri 4.0 sayesinde Almanya lider tedarikçi konumunu geliştirecek ve lider pazar haline gelecektir.

Yapay Zeka; robotlar, nesnelerin interneti, dijitalleşme, dijital kültür gibi alanları kapsamaktadır. Nesnelerin interneti kavramı bir yerde sensörün veya bir işlemcinin bilgi işlem, algılama ya da bir işlemi gerçekleştirmesi anlamına gelmektedir (Flaherty, 2017). 2013 Endüstriyel İnternet Konsorsiyumu'na göre; Endüstriyel İnternet terimi “ Daha iyi işler ve bunların toplumsal sonuçlarını tahmin etmek, kontrol etmek ya da tüm bunları planlamak için kullanılan karmaşık fiziksel makinelerin veya cihazların ağ sensörleri ve yazılımlar ile entegrasyonu” olarak tanımlanmaktadır (Rajpurohit ve Verma, 2016: 536).

Şekil 1.1: Endüstri 4.0'ın Temel Bileşenleri



Kaynak: Rajpurohit ve Verma, 2016: 537.

Endüstri 4.0 ile başlayan bu yeni süreçte sanal ve fiziksel sistemler uyum içinde, birlikte kullanılarak endüstriyel alanda köklü değişimler ortaya çıkarmaktadır. İnternetin üretimde kullanılması hayatın hemen hemen her alanında birçok yeniliği de beraberinde getirmesine yol açmıştır (Dağıtmaç ve Özbay, 2018: 68).

Yapay Zeka, Dördüncü Sanayi Devriminin en önemli faktörü ve özelliği olarak karşımıza çıkmaktadır. Yapay zeka sayesinde otomasyon güçlenecek ve insanların yaptığı bir çok işi makineler yapmaya başlayacaktır. Bunlardan en önemlisi verilerin işlenmesidir. Aynı zamanda bu devrim “Siber Fiziksel Sistemler”e (Cyber Physical System) dayanmakta ve bunlar fiziksel dünya ile siber alanı birbirine bağlayan sistemler olarak anılmaktadırlar (Pauli ve Ünür, 2017: 16).

Günümüzde ülkelerin Araştırma Geliştirme (Ar-Ge) yüzdelerinde en fazla yatırımı teknoloji ve ürün geliştirme alanlarına yaptıklarını görmekteyiz. Bu ülkelerin başında Batı Avrupa, ABD, Rusya ve Çin gibi ülkeler gelmektedir ve en büyük yatırım

alanları savunma, enerji, sağlık, uzay- havacılık gibi kalemlerdir. İkinci Dünya Savaşı sonrası değişen paradigma ışığında savunma sanayisi sadece askeri anlamda değil tüm ekonomiyi kapsayacak şekilde gelişme göstermiş ve etkileri de kapsamlı olmuştur (Dünya ve Türkiye'de Sanayi Yarman ve Denemeç, 2016: 5).

Endüstri 4.0 ile akıllı ürünler, prosedürler ve süreçler oluşturmak temel hedeftir. Akıllı fabrikalar Endüstri 4.0'ın önemli bir özelliğini oluşturmakta ve bu fabrikalar karmaşıklığı yönetebilecek kapasiteye sahip olup, bozulmaya daha az eğilimli malları üretebilecektir. Akıllı fabrikalarda, makineler, insanlar ve kaynaklar bir sosyal ağdaki gibi doğal olarak birbirleriyle iletişim kurabileceklerdir (Kagerman, Wahlster ve Helbig, 2013: 19). Ayrıca Endüstri 4.0 bireysel, son dakika müşteri gereksinimlerini karşılamaya çok daha fazla yönelik yeni iş ve ortaklık modellerinin geliştirilmesine yol açacaktır (Kagerman, Wahlster ve Helbig, 2013: 22). Endüstri 4.0'ın getirdiği insan teknolojisi ve insan-çevre etkileşimindeki paradigma kayması önemli bir rol oynamaktadır. Çalışanlar çalışmalarında çok modlu, kullanıcı dostu arayüzlerine sahip akıllı yardım sistemleri ile desteklenecektir. Endüstri 4.0 girişiminin sosyo-teknik yaklaşımı, inovasyondaki insan çalışmalarının önemi konusunda daha büyük bir farkındalığa dayanak, acil olarak ihtiyaç duyulan yenilikleri geliştirmek için yeni bir potansiyel süreci ortaya çıkaracaktır (Kagerman, Wahlster ve Helbig, 2013: 23). Sonuç olarak söylenebilir ki; Endüstri 4.0 ile birlikte makine ve insan arasındaki entegrasyon en üst düzeye taşınmış ve siber fiziksel sistemlere dayanan yeni üretim biçimleri sürece dahil olmuştur ve büyük veri analizi ile üretim daha verimli hale getirilmeye çalışılmıştır (Dağıtmaç ve Özbay, 2018: 32).

Yukarıda da belirtildiği üzere her yeni sanayi devrimi ile toplumlar yeni bir değişim ve dönüşüm süreci içine girmişlerdir. Ancak bunlardan hiçbiri dijital dönüşüm kadar hızlı ve yaygın olmamıştır. Bilişim ve internet araçları hepsinden daha hızlı gelişmiş, hatta kendinden önceki gelişmeleri de hızlandıran bir hal almış ve gözle görülür bir nitelikte değişimini sürdürmektedir. Son gelen teknolojik devrimlerin kendinden önceki teknolojiye katkı sağladığı yadsınamaz bir gerçektir (Dağıtmaç ve Özbay, 2018: 25).

1.2. TEKNOLOJİ VE İNSAN

Toplum ve teknoloji birbirini etkileyen iki kavram olarak değerlendirilmelidir. Hangisinin diğerini harekete geçirdiği noktasında ise içinde bulunulan durum, konum, davranışlar, çevresel faktörler gibi etkenler söz konusudur. Günümüzde internetin ve bilgisayarın toplumlara hızlı bir şekilde entegre olması sonucunda yeni bir dünya oluşmuş ve bütün hayatımızı şekillendiren bir dijital kültür ortaya çıkmıştır. Kamu alanında dahi birçok hizmetin artık başına “e-“ harfini almasıyla oluşan e-devlet, e-imza, e-sağlık, e- eğitim gibi her hizmetin elektronik hale gelmesi bunun en basit örneğidir (Pullenden aktaran Dağıtmaç ve Özbay, 2018: 127).

Teknolojinin oluşturulması ve geliştirilmesi toplumsal yaşamda hem nicel hem de nitel değişimlere neden olmuş ve buna bağlı olarak insanlar için olumlu ve olumsuz sonuçlar doğurmuştur. Günümüzde teknoloji toplumsal yaşamın ayrılmaz bir parçası haline gelmiş ve insanların ihtiyaçlarını karşılamaya yönelik olarak gelişme göstermektedir. Ayrıca toplumların ilerleme ölçütlerinin de ana faktörü olarak karşımıza çıkmaktadır. İnsanlar teknolojiyi seyahat etmek, iletişim kurmak, öğrenmek, rahat yaşamak gibi aklımıza gelebilecek her alanda kullanılmaktadırlar. Buna bağlı olarak da ulaşım, eğitim, sağlık, kültür, öğrenme süreçleri ya da siyaset gibi birçok alanı etkisi altına almıştır (Pathak ve Singh, t.y.: 8). Gelineen noktada sosyal, kültürel ve ekonomik alanların teknolojiden bağımsız olması düşünülemez.

Son dönemlerde yaşanan hızlı gelişmeler sonrasında teknolojinin geldiği nokta istisnasız robotların her alanda devreye sokulması olmuştur. Robotik teknoloji yaşamın büyük bir parçası haline gelmiş ve bitmez tükenmez canlılıklarından dolayı, tutarlı ve karlı işleri yerine getirmek için daha çok mekanik üretim sistemi gibi kontrollü durumlarda kullanılmaktadırlar. Kablosuz internet bağlantılarının kullanımı ve akıllı istihbarat gibi gelişmeler robotlar ile sağlanacaktır (Pathak ve Singh, 15-16).

İçinde bulunduğumuz yüzyılda insanlar artık yapay zeka kavramını içerir insan beyninin dijital bir kopyası olacak şekilde tasarlanabilen robotlardan bahsetmektedir. Çalışmanın daha sonraki bölümlerinde de ele alınacağı üzere teknoloji her gün yeni bir gelişme ile karşımıza çıkmaktadır. Toplamların buna bağımlı olmaları ya da uyum sağlamalarının yanında, asıl mesele gelinen noktada teknolojinin olumlu ve olumsuz

yönlerini ortaya koyabilmek ve meydana gelebilecek hukuksal ve etik problemler için alınacak önlemlerdir.

Yapay zeka tabanlı teknoloji gelişiminde toplumlarda optimistler ve pesimistler olmak üzere iki görüş hakimdir. İyimser düşünen insanlar bu teknolojinin insanlığı daha ileri taşıyacağına inanırken, kötümser olanlar ise insanlığı yok edeceğini savunmaktadırlar. Bu anlamda ortaya çıkan bazı endişeleri şu sorular üzerinden ortaya koymak mümkündür (Vreskala, 2019).

- İnsan etkinliği anlamını yitirir mi?
- Siber suçlar ve bireysel silahlanma artacak mı?
- Yapay zeka geliştikçe kaos ve savaş ortamı artar mı?
- Veri güvenliği suistimali ortaya çıkar mı?
- Bağımsız iş yapabilmenin ortadan kalkmasına bağlı olarak birey bilinci azalır mı?
- İşsizlik ortaya çıkar mı?

Bu sorulara cevap aranırken teknolojinin olumlu ve olumsuz etkileri tek yönlü değerlendirilmemelidir. Örneğin, teknoloji gelişimi tarihsel olarak da incelendiğinde her yeni teknoloji işsizliği neden olmuş ancak çok daha fazla yeni iş kolları da ortaya çıkarmıştır. İnsanların niyeti olumsuz olursa makinelere öğretilcek kavramlar da yanlış ve olumsuz olacaktır. Yapay zeka teknolojileri tabana yayılmalı ve herkes buna dahil olmalıdır. Çünkü bu teknolojilerin sadece belli bir kesimin elinde bulunması kaosa neden olabilecektir. Çalışmanın sonraki bölümlerinde de detaylı olarak ele alınacak olan bu konuda temel nokta bu teknolojileri yine insanların değiştirip geliştirecek olmasıdır.



İKİNCİ BÖLÜM
YAPAY ZEKA VE ETKİ ALANLARI

2.1. YAPAY ZEKA NEDİR?

Yapay zeka (AI), normal olarak insan zekası gerektiren işleri yapabilen bilgisayar sistemlerinin ya da algoritmaların teorik olarak yaratılması veya geliştirilmesi olarak anlaşılmaktadır. Gündemde sürekli tartışılan bu konunun bir tarafında yapay zekanın insanlığa büyük faydalar getirecek bir oyun değiştirici olarak potansiyeli varken, diğer tarafta ise yapay zekanın tehditleri üzerinde durulmaktadır.

Çalışmanın bu bölümünde doğal zeka ve yapay zekanın benzerlik ve farklılıkları ortaya konularak yapay zekanın ne gibi riskler ve problemlere sebep olabileceğine ulaşılması hedeflenmektedir. Yapay zekanın ne olduğunun anlaşılması için öncelikle doğal zekanın ne olduğuna bakılması gerekmektedir. Doğal ve yapay zeka tarihçelerinde ve gelişim düzenlerinde farklılıklar göstermektedir. Doğal zeka, yönlendirilmemiş, doğal evrimin derin tarihinin bir ürünüdür. O evrim, biyoloji, doğal çevre ve kültürel çevrenin bir karışımıdır. Yapay zeka ise aksine, teknolojik gelişme tarihinde, yüksek oranda yansıtılmış ve her zaman yönlendirilmiş olarak karşımıza çıkmaktadır (Gregg, 2018: 2- 157).

Yapay zeka, üzerinde hiçbir canlı organizma bulunmayan, tamamen yapay bir kurgu üzerinde ilerleyen, insan davranış ve eylemlerini gerçekleştirebilen ve yapay araçlarla oluşturulan teknolojinin genel bir adıdır (Gürçan, 2017: 24). Yani, belirli bağlamlarda, kararlar almayı ve tahminler yapmayı öğrenebilecek ya da öğretebilecek sistemler geliştirmeye adanmış bir bilgisayar bilimi alanıdır. Yapay zeka uygulamaları çeşitli davranışlar sergileyebilmektedir: optimizasyon, görüntü tanıma ve algılama, tahmin ve hipotez testleri, doğal dil işleme ve makine çevirisi bunların başında gelmektedir (Smith ve Neupane: 2018: 11). Cem Say'a göre yapay zeka; zekice olup olmamasına bakılmaksızın, doğal sistemlerin yapabildiği her bilişsel beceriyi, yapay sistemlere nasıl yaptırılacağını ele alan bir bilim dalıdır (Say, 2019: 83).

“Artificial Intelligence” olarak adlandırılan bu teknoloji, bir yazılım algoritmasının analiz sonucuna dayanarak sonuç çıkartabilip, daha sonra bu sonuca göre hareket edebilmekte ve böylece akıllı bir şekilde davrandığı için gelişmiş bir veri analiz sistemi olarak düşünülmektedir (Smith ve Neupane: 2018: 27). Yapay zeka belli problemleri tanımlayıp, bu problemleri öğrenerek çözebilen makinadır. Yapay zekanın biyolojik temeli sinir ağlarıdır. Sinir ağları, hatıraları, bilgileri depolayan ve işlemleyen

bir donanımdır. Yapay zeka oluşturulurken bu hücreler arasındaki bağlantılar taklit edilmektedir. Yani doğal zeka bir “bilinç” olarak ortaya çıkarken, yapay zeka ise bir çeşit “bağlantı” olarak karşımıza çıkmaktadır (Gregg, 2018: 162).

Bilgisayar bilimi içinde ele alınan bir çok alandan biri olan yapay zeka, insanların neler yapabildiğiyle karşılaştırılabilen süreçleri de içine alan, matematiksel işlevler ve algoritmalarından oluşmaktadır (Lidestri, 2018: 5). Yapay zeka (AI) ve robotiğin ortak anlayışı, kısmen bilim kurgu, medya raporları ya da kamuoyunu tanımak isteyen robotik uzmanları tarafından gerçekleştirilen bir alan olarak karşımıza çıkmaktadır.

Yapay zeka akademik bir disiplin olarak ele alınırken izlenen yöntemde başından beri, insan zekasını; zeka etkileri, yani “zeki davranışlar” üretebilmesi açısından anlamak ve açıklamak belirleyici olmuştur (Görz ve Nebel, 2005: 31).

Yapay zeka’nın bir çok açıklaması olmasına rağmen net bir tanımı yoktur. Bunun sebebi ise “zeka” kavramıyla ilgilidir. Bu yüzden kısaca zeka kavramının ne olduğuna bakılması gerekmektedir. İnsan zekası, sadece bir özelliğin var olması demek değil, birden fazla özelliğin bir araya gelmesiyle oluşmuş bir sistem olarak algılanmalıdır. Yapay zeka ise; buradan hareketle zekanın birkaç faktörüne odaklanmıştır. Bunlar arasında öğrenme, problem çözme, muhakeme yapabilme ve insan ve karakter tanıma gibi özellikler sıralanabilir.

Yapay zeka sistemini insan gibi davranan, insan gibi düşünen, akılcı düşünen ve akılcı davranan sistemler olarak algılamak mümkündür (Görz ve Nebel, 2005: 38). Ancak doğal zeka ve yapay zeka birbirlerinden önemli ölçüde farklıdır. Öncelikle, doğal zeka yapay zekanın hesaplama kapasitelerine indirgenemez. Yani doğal zeka rasyonel bir sembolik bilgi işlemcisinden çok daha fazlasıdır. İkincisi ise doğal zeka kendini yansıtır. Yani onun sosyalleşmesiyle birey kendi kültürel çevresinin davranış kurallarını içselleştirmektedir (Gregg, 2018: 158).

Yapay zekanın bir bilimsel disiplin olarak oluşmasındaki belirleyici yıl 1956’dır. Bu yılın eylül ayında Massachusetts Enstitüsü’nde “Symposium on Information Theory” adlı bir konferans düzenlenmiştir. Bu konferans bilişsel bilimlerin temel taşı olmasından dolayı önem arz etmektedir (Görz ve Nebel, 2005: 30). Yapay zekanın kökeni ise Dartmouth Konferansı’na dayanmaktadır.

1956 yılındaki konferanstan sonra bir çok üniversite içi ve üniversite dışı kurumlarda bu konuyla ilgili araştırma projeleri hayata geçirilmiştir. Öngörüler başta iyimser ve coşkuluydu: yapay zekanın dilbilim, psikoloji, matematik, mühendislik ve yönetim bilimlerindeki ana problemleri çözmesi hedeflenmiştir (Görz ve Nebel, 2005: 31).

Yapay zekâ, enformatik içinde kabul görerek ve disiplinlararası ağda kendine bir yer edinerek “normal bilim” konumuna gelmiştir. Yapılan pek çok araştırma önemli derecede uzmanlaşmaya yöneliktir ve yayımlanan araştırma sonuçları, gerek matematik, gerek makine mühendisliği, gerek beyin araştırmaları olsun diğer bilimleriyle aynı derecede bilimseldir (Görz ve Nebel, 2005: 34-35).

1950’li yıllarda bilgisayarın insan gibi düşünebilmesinin mümkün olup olmadığının anlaşılması için Alang Turing tarafından, bir sorgulama yöntemi olan Turing testi uygulanmıştır. Bu test üç katılımcı ile gerçekleştirilmektedir. Bunlar bilgisayar, insan folyo ve bir insan katılımcıdır. Test, sorgulayıcının diğer iki katılımcıya yani bilgisayarla sorular sormasıyla yapılmaktadır. Bu sorgulamada çok geniş kapsamlı sorular sorulabilmektedir. Bilgisayarın verdiği cevaba göre de zekaya sahip olup olmadığı tahmin edilmeye çalışılmıştır (Copeland, 2016).

Yapay zekanın gelişiminde önemli olan dört dönem şu şekildedir (Görz ve Nebel, 2005: 31-32):

- 1950’lerin sonu ve 1960’ların başlarındaki kuruluş döneminde simgesel, nümerik olmayan bilgi işlem kuramları bu dönemi tanımlamaktadır. 1956 yılında Dartmouth Çalıştayı’da “Yapay Zeka” ismi ilk kez geçmiş ve isim babası McCharty’dır (Say, 2019: 86).
- İkinci olarak 1960’larda önde gelen Amerikan üniversitelerinde yapay zekanın, otomatik problem çözme ve görsel sahne çözümlemesi gibi ana konuları sistematik olarak incelenmeye başlanmıştır. Bu yıllarda, Amerikan Savunma Bakanlığı’nın “Advanced Research Projects Agency” (ARPA) adlı birim tarafından yapay zeka önemli ölçüde destek görmüştür.
- Üçüncü dönem ise 1970’li yıllardır. Bu dönemde diğerlerinden farklı olarak, entegre robot sistemleri ve uzman gibi problem çözen sistemlerin tasarlanması araştırmaların odaklandığı bir alan olmuştur.

- Son olarak ise; 1980’li yıllarda yapay zeka alanı geniş ölçüde matematikleştirilmiş, bilgi işleme düşüncesi öncelik kazanmış ve durumsallık, “Çoklu Ajan Sistemleri” (Bölünmüş yapay zeka) ve sinir hücresi ağ bağlantıları gibi yeni konular gündeme gelmeye başlamıştır. Buna ek olarak 1990’lı yıllardan itibaren ise tümleşik yaklaşımlara ve buna uygun olarak “bilgi-işlem” ve “ akıllı sistem” kavramlarının yeni konulara evrilmelerine yönelik belirgin bir eğilim oluşmaya başlamıştır. Uygulamalar ve uygulamaya yönelik düşünceler pek çok durumda internet patlamasıyla da bağlantılı olarak güncel araştırma ve çalışmaları önemli derecede etkilemiştir (Görz ve Nebel, 2005: 33).

Tablo 2.1: Yapay Zeka’nın Gelişim Aşamaları

1936	İngiliz matematikçi Alang Turing, günümüzde bilgisayar birimlerinin temeli sayılan “Evrensel Makine” konulu makalesini yayımladı.
	Alan Turing insan zekasıyla makine zekasını karşılaştırmak için bir “ taklit oyunu” fikrini ortaya attı. Günümüzde buna Turing Testi adı verilmektedir.
1950	Bilim Kurgu yazarı, Isaac Asimov, Ben Robot kitabını yayımlamıştır. Burada Asimov bir yapay zekanın tasarlayıcılarına saldırılarını engellemek için oluşturduğu Robot Yasası’nı ortaya koymuştur. Yani bilgisayar bilimcilerine bu konuda yol gösterici olmuştur.
1956	“Yapay Zeka” terimi ilk kez Dartmouth Üniversitesinin ev sahipliği yaptığı bir konferansta ortaya koyulmuştur.
1973	Olumlu tahminlere rağmen, YZ’nin ilerlemesi durmuştur. Hükümet danışmanları makinelerin satrançta asla deneyimli amatör düzeyinin ilerisine geçemeyeceğini savunmuştur.
1981	Yapay Zeka görevler için uzman bilgisayar sistemleri kullanan şirketler sayesinde değer biçilemez bir ticari araca dönüşmüştür. Bazı şirketler bu yüzden milyonlarca dolar kar elde etmiştir.
1990	Bilim insanı Rodney Brooks sinir bilimdeki gelişmelerden ilham alarak, yapay sinir ağları yaratmanın olası yararlarını savunmuştur.
1997	IBM’nin inşa ettiği Deep Blue adlı makine dünya satrac şampiyonu Garry Kasparov’u yenilgiye uğratmıştır. Bazıları için, Deep Blue’nun stratejik eylem başarısı ve saniyede 200 milyon adede kadar hamleyi değerlendirebilmesi, yapay zekanın gerçek gücünün göstergesi olurken, diğerleri ise Deep Blue’nun sadece çok belirli işlerde bilgisayarların verimini oraya koyduğunu iddia etmiştir.
2008	Google’nin ses tanıma yazılımı yapay sinir ağlarının kullanarak doğruluk oranını yüzde seksenin (% 80) üzerine çıkarmıştır.
2011	IBM’nin bir makinesi daha tarihe adını yazdırmıştır.Watson ABD bilgi yarışması Jeopardy’yi kazandı. Bu yapay zeka için tam bir dönüm noktası ve satrançta kazanan bir bilgisayar programlamaktan çok daha zordur. Karmaşık soruları ve bulmacaları çözmek için Watson desenleri tanıyacak şekilde eğitilmiş ve sinir ağları kullanılarak oluşturulmuştur.
2014	Eugene Goostman isimli bir program, makine zekasını ölçen Turing Testinin bir başka versiyonunu başarıyla geçmiştir.
2016	Google DeepMind’in AlphaGo’su Go oyununun en büyük ustası Lee Sedol’u yenmiştir. IBM’nin Deep Blue’sundan farklı olarak, AlphaGo üm mümkün hamlelerin bilgisayara programlandığı bir kaba güç yaklaşımı kullanamamaktadır. Onun yerine kendi kazanma stratejisini geliştirene kadar makine öğrenimi sayesinde kendi kendine milyonlarca maç yapıp araştırma yapmıştır.

Kaynak: How it Works Dergisi Kasım 2018 Sayı :14-28.

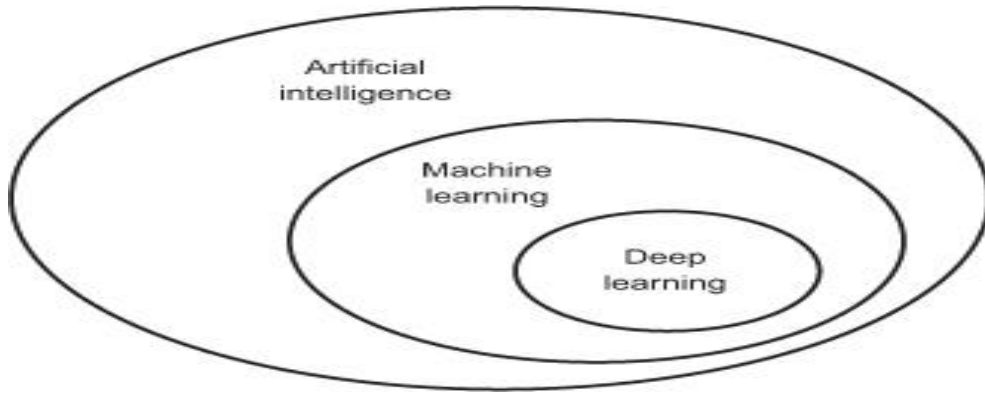
Görülüyor ki son yıllarda bilgisayarlardaki işlem hızı artmış, yapay zeka alanında insan zekasına yakın sistemler oluşturulmaya başlanmış ve uç teknolojiler ile yapay zeka yeni bir boyut kazanmıştır. Yeni hedefler ise algılayabilen, düşünen robotlar geliştirmektir (Adalı, 2017: 6). Makine öğrenimi ve yapay zeka 2010 yılında yıllık % 20 bir büyüme göstermiştir. Yani bu, yıllık konferanslar ve sektörel fuarlar gibi ileri teknoloji ortamlarında yeni ürün bültenleri ve gösterilerin patlaması olarak görülebilir (Lidestri, 2018: 1).

Yapay zekanın somutlaştırılabilmesi adına örnekler verilecek olursa, örneğin özerk araçlar birçok veri toplama ve yapay zeka tekniği ile donatılmıştır. Bu örnekte, sürücüsüz araç trafik kurallarına uymakta, kodlanmış kuralların kombinasyonunu yapabilmekte, algoritmalar yoluyla belirli engellerden kaçabilmekte ve akıllı nesne ayrımı (yani motosiklet ve bisiklet arasındaki farkı bilme) yapabilmektedir (Smith ve Neupane, 2018: 30). Yapay zeka alanı, çok çeşitli görevlerin otomasyonunu amaçlamaktadır. Yapay zeka araştırmaları tarafından incelenen tipik görevler arasında oyun oynamak, araçlara rehberlik etmek ve görüntüleri sınıflandırmak sayılmıştır (Brundage vd., 2018: 12). Yapay zeka sistemleri şimdi neredeyse fotoğraflar yardımıyla ayırt edilemez sentetik görüntüler elde edebilmektedir (Brundage vd., 2018: 13).

2.1.1. Makine Öğrenmesi

Yapay zeka, bilgisayar biliminin bir alt dalı olduğu gibi, yapay zekanın da kendine özgü alt dalları bulunmaktadır. Bunları; makine öğrenmesi, sinirsel ağlar, derin öğrenme, bilişsel bilgi işlem, doğal dil işleme ve bilgisayarla görme olarak sıralamak mümkündür (Lidestri, 2018: 8).

Şekil 2.1: Yapay Zeka, Makine Öğrenmesi ve Derin Öğrenme



Kaynak: Chollet, 2017.

Sembolik yapay zeka kavramı her ne kadar satranç oynamak, mantıksal sorunları çözmek için uygun görünse de konuşma tanıma ve dil çevirisi gibi daha karmaşık problemleri çözmek için yeni bir yaklaşım ortaya çıkmıştır bu da makine öğrenmesidir (Chollet, 2017).

Konunun daha iyi anlaşılabilmesi için bu bölümde “makine öğrenmesi” kavramına da yer verilecektir. Fakat öncesinde büyük veri ve veri madenciliği kavramlarına kısaca yer verelim. Büyük veri; geleneksel veri işleme yazılımının analiz edemeyeceği kadar büyük ya da karmaşık olan veri kümeleri olarak tanımlanabilir. İnsanların sürekli internet kullanmalarına bağlı olarak büyük veri kullanımı da artmış ve bunlar yapay zekada önemli gelişmeler sağlamıştır. Veri madenciliği ise; desenleri keşfetme ya da büyük veri setlerinden bilgi çıkarma işlemi olarak karşımıza çıkmaktadır (Accessnow, 2018: 8).

“Machine Learning” yani makine öğrenmesi, 1959 yılında bilgisayar biliminin sayısal öğrenme ve model tanıma gibi çalışmalardan geliştirilen ve yapay zekanın bir alt dalı olan sistemdir. Veriler üzerinden tahmin yapabilen algoritmaların çalışmalarını araştıran ve öğrenebilen bir sistem olarak tanımlamak mümkündür (Alkan, 2019: 1).

Bir makine öğrenme sistemi açıkça programlanmış olmayıp bunun yerine eğitilmiştir. Bir görevle ilgili birçok örnekle sunulur ve bu örneklerde sistemin sonunda görevi otomatikleştirmek için kurallar getirmesine izin veren istatistiksel yapıyı bulur. Buna bir örnek verilecek olursa, tatil resimlerinizi etiketleme görevini otomatik hale getirmek isterseniz, insanlar tarafından etiketlenmiş pek çok resim örneğiyle bir makine

öğrenmesi sistemi oluşturabilirsiniz ve sistem bazı resimleri belirli etiketlerle alakalandırmak için istatistiksel kuralları öğrenecektir (Chollet, 2017). Ancak bu öğrenme kolay değildir. Bu çalışmalarda insan beynindeki nöronlar taklit edilerek yapay sinir ağları oluşturulmakta ve en iyi ve doğru değerlere ulaşmak için çok fazla işlem yapılması gerekmektedir. Makineye bütün veri kaynaklarını vermek zor bir iş olduğundan yapay zekaya bir şeyi öğretmek için milyonlarca örneğe ihtiyaç vardır. Bu yüzden algoritmalar her zaman istenen şekilde elde edilemeyebilirler. Milyonlarca örneğe ihtiyaç duyduğu için aktif öğrenme algoritmalarında yapay zeka verdiği kararlardan emin olamamakta, insanlardan yardım isteyerek kendini güncellemektedir. Ayrıca burada verilerin sonsuz olduğu ve doğru kaydedildiği varsayılmaktadır.

Makine öğrenmesi, veri modellerinde gerçekleştirilen analitiği otomatikleştirmenin bir yoludur ve makine öğrenimi ile mantık, bir modelin matematiksel olarak kanıtlanması için istatistiklerle birleştirilir (Lidestri, 2018: 7). Twitter uygulaması da makine öğrenmesine bir örnek olarak verilebilir. Mesela burada, makinenin geri bildirim döngüsü sayesinde önceki bilgiler sentezlenerek ve bunlara yeni bilgiler eklenerek yeni bir öneri listesi oluşturulabilmektedir. Makine öğrenmesine bir diğer örnek de; bir dilde yazılmış metinleri yapay zekaya sahip bir makine inceleyerek o dilin modelini çıkarabilmekte ve sözcüklerin gerçek anlamlarını bulabilmektedir (Adalı, 2017: 13).

Bu alanda bir diğer uygulama olarak Siri asistan uygulaması örneği verilebilir. Siri büyük bir makine öğrenme sistemidir. Sorular ve verilen cevapların hepsi bu makinede kayıtlıdır, yani sorulabilecek sorulara göre cevaplar hazırlanmaktadır. Tüm verileri; görüntü, ses, metin anlamını aynı anda işlemek kolay değildir. Amaç verileri yaşatarak anlam çıkarmaktır ancak anlamı şu anda elde etmek güç, örneğin Siri cevap verebiliyor ama derinlemesine cevap veremiyor.

2.1.2. Derin Öğrenme

Derin öğrenme; makine öğrenmenin belirli bir alt alanı olarak karşımıza çıkmakta ve gün geçtikçe daha anlamlı hale gelen ardışık katmanların öğrenilmesine vurgu yapmaktadır. Yani verilerden öğrenme temsillerini almayı ifade eden bir kavramdır (Chollet, 2017). Derin öğrenme belirli sinir ağları türlerine dayanmaktadır. Mevcut ağlar ve sensörler, veri okyanusundaki eğilimleri tahmin etmek ve keşfetmeyi

sağlamaktadırlar. Derin Öğrenme'deki “derin” sözcüğü ağdaki katman sayısının çok olduğunu ifade etmektedir (Say, 2019: 103).

Derin öğrenme ve güçlendirici öğrenme gibi makine öğrenme teknikleri, mevcut veri setlerinden veri alarak veya çevreleriyle etkileşimlerinden gelen geri bildirimler sayesinde yapay zeka uygulamalarının öğrenmesini sağlamaktadırlar. Büyük verilerin var olması, bu algoritmaların oldukça karmaşık sorunların üstesinden gelmesini mümkün kılmaktadır (Smith ve Neupane, 2018: 30). Örneğin, sağlık alanında bu teknolojinin kullanılması büyük kolaylıklar ve faydalar sağlamaktadır. Makine öğrenimi örneğin kanserin nasıl yayıldığı, daha faydalı bir tedavinin nasıl geliştirileceği konusunda ve bazı tespitler için doktorlara birçok yarar sağlamaktadır. Ancak burada karar yetkisi yine doktorlarda olacaktır.

Derin öğrenmede yukarıda bahsedilen katmanlı temsiller, sinir ağları denilen modellerle öğrenilmektedir, birbiri üzerine yığılmış değişmez katmanlarda yapılandırılır. Sinir ağları kavramı ise nörobiyolojiye ait bir kavramdır. Fakat derin öğrenme merkezi kavramlarının bazıları, beyindeki algılarımızdan esinlenerek oluşturulmuş olsa da, derin öğrenme modelleri beyin modelleri değildir (Chollet, 2017). Katmanların işleyişine bakılacak olursa, bir görüntü çektikten sonra onu sinir ağının ilk katmanına giren karelere ayırabilirsiniz, ilk katmandaki bireysel nöronlar verileri ikinci katmana iletecektir. İkinci nöron da görevini yapınca son tabakada son çıktı üretilene kadar bu işlemler devam edecektir (Copeland, 2016).

Yapay zeka alanında çalışan bazı araştırmacılar, nörobilimlerin gelişmesiyle birlikte, nöronal devrelerin simülasyonunun, bir kişinin ne düşündüğünü, ne yaptığını ya da istediğini yani insanların zihinlerini okumak, bireysel ve kolektif davranışları daha iyi değerlendirmek ve insanları kontrol etmek ve manipüle etmek için bu teknolojilerin kullanılacağını düşünmektedirler (Risse, 2018: 4).

Cem Say'a göre yapay zeka teknikleri üçe ayrılmaktadır. Bunlardan ilki bir şeyi öğretmek için öğrenmektir. Yani öğrenmeyi yapan kişi önce neyin nasıl yapılacağını kendisi öğrenip ona göre bir kodlama yapmaktadır. Buna eski model yapay zeka da denmektedir. İkincisi ise derin öğrenme de denilen göstererek öğretme tekniğidir. Burada insanın konuyu derinlemesine anlaması gerekmemektedir. Göstererek öğretme için örneğin bir resim içinde bir akrabayı bilgisayarın tanınması

sağlanabilir. Sonuncusu ise, kendi kendine öğrenme, pekiştirmeli sistemidir. Buna Alpha Go örneği verilebilir. Alpha Go adlı bilgisayarın dünya Go şampiyonunu yenmesi söz konusudur. Burada bilgisayara Go şampiyonun nasıl yenileceği öğretilmemiştir. Dünyada oynanan Go'lar makineye gösterilmiştir. Milyonlarca kez bu oyunu oynayarak, insanlar bunu nasıl yapıyor diye kendi kendine, tecrübe ederek bunu öğrenmiştir. 2017 yılında Alpha Go, yerini bir üst sürümü olan Alpha Go Zero'ya bırakmıştır. Alpha Go Zero'nun, diğerinden farkı ise, ilk başta bile insana gereksinim duymamasıdır. Sadece oyun kuralları yüklenen AlphaGo Zero zamanla kendi kendine oynamaya başlamıştır (Say, 2019: 119).

Özetlemek gerekirse yapay zeka, insanların yaptığı bazı zekasal işleri bilgisayarların da yapması anlamına gelmektedir. İlk başta dört işlemi yapan makineler bugün düşünce gerektiren işleri de yapabilmektedir. Bugün matematik ispatı yapabilen programlar, resim yapabilen makineler ve müzik zekaları üzerine programlar mevcuttur. Burada dikkat edilmesi gereken bir nokta tüm bu sistemin insanlar tarafından kodlanan algoritmalar ile oluştuğudur. Peki, yapay zeka önceden hesaplanamayan işleri de yapabilecek midir? Çalışmanın diğer bölümlerinde bu tartışmaya yer verilecektir.

Son yıllarda çoğu tanınmış bilim adamı ve mühendis özellikle bilimkurgu ve kısmen korkutucu teknik ütopyaдан bahseden yazınsal üretimlerinin aracılığıyla öne çıkmaktadır. Pittsburgh'daki tanınmış robot laboratuvarının yöneticisi olan ve birkaç on yıl sonra akıllı robotların insanları gereksiz hale getirip evrimi yeni bir şekilde sürdürebileceğini iddia eden Hans Moravec de bunların arasındadır (Görz ve Nebel, 2005: 35).

Günümüzdeki yapay zeka araştırmalarında başarı ölçütü olarak akılcılık kullanılmaktadır (a.g.e.: 40). Diğer bir deyişle bu sistemde insan düşüncüsü taklit edilmeye çalışılmaktadır. Burada şuna da değinmek gerekir; yapay zeka tutarlı olması, kalıcı olması, paylaşılabılır ve kayıtlı olması gibi açılardan insandan daha üstün bazı özelliklere sahiptir.

Algoritmalar verilere erişimi olduğu sürece, ihtiyaç duyulan hızda, belirlenen işleri ve kodlanabilecek her şeyi yapabilirler. Algoritmaların etkinliği “Büyük Veri” kullanılabilirliği ile artmaktadır. Dünyadaki tüm insan faaliyetleri ve diğer süreçler

hakkında çok büyük miktarda veri, “makine öğrenmesi” olarak bilinen yapay zeka türünün çıkarımlar yapmasına izin verip kalıpları tespit edebilmektedir (Risse, 2018: 2).

Yapay Zeka (AI) ve makine öğrenmesi (ML) son yıllarda hızla ilerlemiş ve bu alandaki gelişmeleri çok çeşitli faydalı uygulamalara olanak sağlamıştır. Yaygın olarak kullanılan teknolojilerin kritik bileşeni konuşma tanıma, makine çevirisi, spam filtreleri ve arama motorları bunlara örnektir. Sürücüsüz arabalar, hemşireler ve doktorlar için dijital sistemler ve yapay zeka özellikli afet yardımı operasyonları hızlandırmak için uçaklar da bunlara eklenebilmektedir (Brundage vd. 2018: 9). Yapay zeka destekli bir çok program günümüzde mevcuttur. Örneğin, Cohen adındaki bir bilim insanı AARON adını verdiği ressam bir yazılım tasarlamıştır. AARON boyaları karıştırıp bunu kağıda sürebilecek kadar yetenekliydi. Bu konu da verilecek bir diğer örnek de YZ’ların müzikle ilgili başarısını ortaya koyan David Cope’nin geliştirdiği EMI (Experiments in Musical Intelligence, Müzik Zekası Deneyleri) adlı programıdır. EMI ünlü bestecilerin kalitesinde besteler yapabilmektedir (Say, 2019: 111). Yapay zekanın resim ve müzik alanında kullanılıyor olması zararlı kullanımı dışında yaratıcı ve estetik boyutuna örnektir.

Tüm bu gelişmelere rağmen yapay zekanın kötü amaçlı kullanımı söz konusu olabilmektedir. Çalışmanın diğer bölümlerinde bu konu üzerinde durulacaktır.

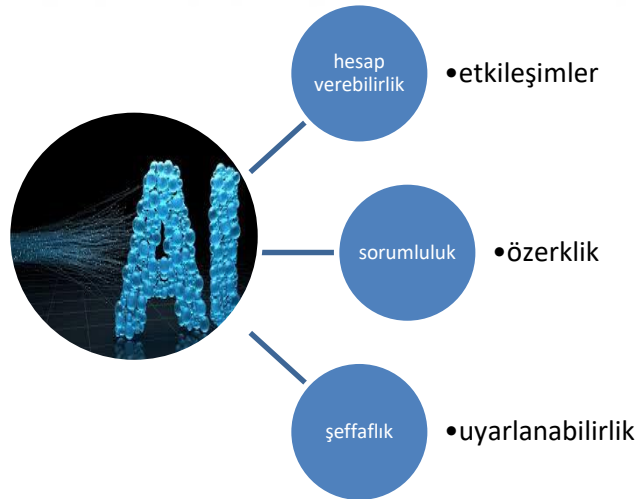
Bu konuya geçmeden vurgulanması gereken bir nokta, yapay zeka, kullanılması açısından “Zayıf AI” ve “Güçlü AI” olmak üzere iki model olarak karşımıza çıkmasıdır. Güçlü AI ve zayıf AI arasındaki temel fark güçlü yapay zekanın programlananın dışına çıkabilmesidir. Yani insan aklını taklit eder. “Günaydın” ifadesini duymaya yönelik eylemi bilen ancak haftanın günü gibi özelliklere dayanan eylemleri temel alan Amazon Alexa ve Google Home gibi akıllı ev cihazı buna örnek verilebilir. Zayıf AI ise, teknolojiyi önceden belirlenmiş bir cevabın mevcut olduğu durumlara uygulamaya odaklanır. Yani cevaplar uygulanan kurallar ile sınırlıdır. Örneğin, Apple’ın Siri ses yardımcısı bu tür bir yapay zekadır (Lidestri, 2018: 5-6). Bir üretim ortamında sadece bir işi yapmakla görevli olan ve buna göre programlanmış olan robotlar da zayıf yapay zekanın bir örneği olarak karşımıza çıkmaktadır.

2.2. YAPAY ZEKANIN FELSEFİ TARTIŞMASI VE ETİK BOYUTU

Yapay zeka her ne kadar bilgisayar bilimleriyle çok yakından ilişkili olsa da, bunun dışında ayrıca felsefe, biyoloji, psikoloji, siyaset ve sosyoloji gibi diğer bilimlerle de yakından ilgili bir konudur. Bu teknoloji üzerindeki kontrolü kaybetmemek adına etik bir düzenleme çağrısı bulunmaktadır. Küresel ölçekte en güçlü isimler yani ticari şirketler bu alanda yenilikçiliği teşvik etmekte ve farklı uygulamalar sayesinde istihbarat sağlamak amacıyla yeni algoritmalar geliştirmektedir. Yapay zekanın hem mikro hem de makro açıdan değerlendirilmesi gerektiğinden bu konunun etik ve güvenilirliği yönlerinden ele alınması oldukça önem arz etmektedir. Burada önemli olan noktalardan biri de insan zihninin anlaşılmasıdır. Çünkü insanların ortaya koymuş olduğu dijital dünya yine insanları ve toplumu etkilemektedir.

AI sistemleri genellikle özerklikleri, etkileşimleri ve uyarlanabilirlikleri ile ele alınmaktadır. AI etiğiyle ilgili toplumsal endişeleri yansıtmak ve AI sistemlerinin sorumlu bir şekilde geliştirilmesini sağlamak amacıyla bu sistemleri, hesap verebilir, sorumlu ve şeffaflık ilkeleriyle değerlendirmek gerekmektedir (Dignum, 2017: 5).

Şekil 2.2: AI'nın Hesap Verebilirliği, Sorumluluğu ve Şeffaflığı



Kaynak: Dignum, 2017: 5.

Bu başlık altında, konunun daha iyi değerlendirilebilmesi için konu felsefi açıdan ele alınacaktır. Yapay zekanın felsefi açıdan sorgulandığı, uzun bir süredir devam eden tartışmalar mevcuttur. Yani saf zekanın ahlakı konusunda merak edilen şey rasyonellik ve ahlak arasındaki bağlantının ne olduğudur (Risse, 2018:5). Burada

“tekillik” terimi ortaya çıkmaktadır. Tekillikten kastedilen şey ise zeka patlaması yoluyla makine zekasının insanı aşması durumudur. Şimdilerde bu “tekillik” konusu çok uzak bir kavram olsa da; bu çağdaş felsefenin önemli bir konusu haline gelmiştir. Bu konuda tartışmalar iki yönlü olarak devam etmektedir. Bir taraf korku senaryoları yazarken (örneğin Stephen Hawking: tekillik insanlığın sonunu getirebilir görüşündedir), diğer bir taraf ise yapay zekanın tamamen insan ürünü bir süreç olduğunu savunmaktadır (Uyar, 2017: 18). Bu tartışmaların dışında asıl odaklanılması gereken nokta, yapay zekaya iyi olanı öğretmek ve kötü olandan kaçınmasını sağlayabilmektedir ki bunu da yine kodlamayı oluşturan insanlar yapacaktır. Bu açıdan değerlendirildiğinde de bu teknolojinin kötü insanların eline geçtiğinde ortaya çıkabilecek sorunlar tartışma konusu olmaktadır. Ahlaki karar verebilen tek varlığın insan olduğu düşünüldüğünde, korku senaryoları yazmak yerine yapay zekayı yönlendirecek olan insanın vereceği kararlara odaklanmak gerekmektedir. Yani kısacası yapay zekanın ahlakının nasıl programlanacağını sorgulanması burada önem kazanmaktadır.

Doğal zeka ve yapay zeka arasındaki farklılıklardan yola çıkılarak konu bir diğer açıdan ele alınırsa, doğal zeka ne olursa olsun kuralları ihlal etme kapasitesine sahiptir. Bu bağlamda yapay zeka daha avantajlı konuma gelebilmektedir. Birey, toplumda geçerli olan kuralları ihlal etmeye ve bunları reddetmeye karar verebilir. Ancak bunu yapay zeka kendisi yapamamaktadır (Gregg, 2018: 158). Yapay zeka bu açıdan her ne kadar avantajlı gibi görünse de etik ve ahlaksal açıdan pek çok problem barındırmaktadır.

Yapay zeka, günlük hayatımıza etkileri göz önüne alındığında son zamanlarda en çok ilgi çeken ve tartışılan konulardan biri olmuştur. Günümüzde gelinen noktada, yapay zekanın en önemli ve göze çarpan örnekleri sosyal medya örnekleri, akıllı robotlar ve otonom araçlardır. Yapay zekanın etiklik boyutu da bu örnekler üzerinde önem kazanmakta ve robotlar ahlak öğrenebilir mi? sorusu karşımıza çıkmaktadır. Örneğin, hasta bir insanla aynı yerde bulunan ona ilaçlarını vermek için tasarlanmış bir robot düşünelim. Robot hastaya ilacını vermiş ve hasta bunu unutup tekrar ilaç almak isterse robot bu durumda nasıl davranacaktır? İkinci ilaç da alınırsa hasta zarar görecektir ancak robot da buna göre tasarlandığından nasıl davranması gerekeceği konusunda etik bir problem ortaya çıkmaktadır. Bu konuda nelerin etik olup olmadığı

üzerinde çalışılmalı, etik kurallar belirlenip çelişkiler giderilmeli ve yapay zeka temelli her şey kontrol altında tutulmalıdır.

Bu konu ile ilgili bir örnek daha verilecek olursa, Mart 2016'da Microsoft, öğrenme özelliği olan, sosyal medyada insanlarla sohbet ederek öğrenecek bir twitter karakteri oluşturmuştur. 24 saat sonra ise bu hesap nefret edilecek bir karaktere dönüşmüştür. Çünkü işte burada yukarıda bahsettiğimiz kötülerin eline bu teknolojinin geçmesi durumu söz konusu olmuştur. Biz bilgisayarlara kötü olanı da öğretiyoruz. Bu durumda makinelere ahlak kazandırılması gerekecek yani robotik ahlak yasaları devreye girecektir (Say, Yapay Zeka Teknikleri, 28 Şubat 2017 youtube video). Öğrenme sistemleri ile iyi ahlak bilgisayarlara öğretilmelidir.

Etik ve ahlaki açıdan değerlendirilmesi gereken bir başka örnek de otonom araçlar konusudur. Otonom araçlar birer robottur. Bu araçların günlük yaşamda insan hayatına sunacağı faydaları yok saymak imkansızdır. Ancak burada asıl üzerinde durulması gereken problem sorumluluk ve sigortadır. Yapay zeka sorumluluğundan kastedilen şey, AI sistemlerinin kendi etiği ve insani değerler hakkında mantıklı davranmalarını ve buna göre hareket etmelerini sağlayan sistemlerin tasarlanmasına duyulan ihtiyaçtır (Dignum, 2017: 5). Örneğin, Google'ın geliştirdiği Google Car isimli bir otonom araç vardır. Bu araç trafiğe çıktığında ve herhangi bir kaza riski ile karşı karşıya geldiğinde aracın nasıl bir yol seçeceği problemi sadece tekniksel değil aynı zamanda ahlaki açıdan problemler içerecektir (Uyar, 2017: 20). Burada ortaya çıkacak bir diğer sorun da sorumluluk boyutu olacaktır. Otonom bir araç kaza yaptığında sorumluluk kime ait olacaktır? Her bir soruya veya soruna cevap olabilecek nitelikte algoritmalar geliştirilmelidir. Burada önemli olan bu araçların ahlaki yetenekleri geliştirilmeli ve ona göre düzenlenmelidir. Örneğin, hız sınırlarının belirlenmesi ile ilgili bir düzenleme yapılabilir. Bu araçlar sayesinde yakıt tüketimi ve çevre kirliliği azalacaktır. Yapay zeka destekli teknoloji hızla ilerlemekte ancak yasalar, kurallar ve alt yapı aynı oranda ilerlememektedir. Bu araçların ortak bir dille haberleşmesi gerekmektedir. Asıl sorun hukuki yöndedir. Her devlet bu konuda birtakım hukuk kuralları geliştirmekte ancak bu yetersiz kalmaktadır.

Yapay zekanın etik ve ahlaki olarak incelenmesinde robot yasalarına değinmekte yarar vardır. Birleşmiş Milletler 2005 Dünya Robotik Bilim Raporunda

robotun genel bir tanımı verilmiştir: Buna göre robot, üç ya da daha fazla eksenle programlanabilen ve aynı zamanda otomatik olarak sabitlenebilen otomatik kontrollü, yeniden programlanabilir çok amaçlı bir manipulatördür (BM 2005 Dünya Robotik Bilim Raporu: 21). Ancak robotların yapay zeka teknolojisi kullanılarak birden fazla amaç için üretilmeye başlanmasıyla tanımları da çeşitlenmiş ve tekdüzelikten çıkmıştır. Robotlar, insanlardan daha üstün şekilde düşünebilen ve hareket edebilen, duygu ya da istekleri algılayabilen duyarlı makineler olarak düşünülebilir.

1942 yılında bilim kurgu yazarı Saac Asimov, Runaround adlı kitabında hukuki niteliği olmamakla birlikte, Robot Bilim ile ilgili temel prensipleri ortaya koymuştur. Bu prensiplere göre öncelikli kural bir robotun bir insana zarar veremeyeceği veya hareketsiz kalmayıp bir insanın zarar görmesine izin veremeyeceğidir. İkinci kural ise, bir robot insanlar tarafından verilen emirlere itaat etmek zorundadır. Son olarak ise, bir robot ilk iki madde ile çelişmediği sürece kendi varlığını korumalıdır (Bozkurt Yüksel, 2017: 92). Görüldüğü üzere, teknolojik gelişmeler ve yapay zeka ile birlikte sadece fayda sağlanmamakta aynı zamanda bunların önemli ölçüde ahlaki ve hukuksal sonuçları da ortaya çıkmaktadır.

Robotu kısaca bir ortamın içinde yer alan fiziksel bir nesne olarak düşünmek gerekmektedir. Robotlar ortamı, derin öğrenme yöntemi ile algılayabilmekte ve yapay zeka sayesinde eylemler gerçekleştirebilmektedir.

Akıllı yazılımlar ya da yapay zeka robot değil sadece robotun programları olarak karşımıza çıkmaktadır. Yukarıda yapay zekanın insanlığa katkılarından kısaca bahsedilmiştir. Şimdi de bunların kötü amaçlı kullanımları sonucu ortaya çıkabilecek sorunlara değinilecektir.

Bu teknolojinin insanlık adına birçok yararı olmasına rağmen bu çalışmada daha çok riskleri üzerinde durulacaktır. Yapay zeka (AI) ve makine öğrenmesi (ML) vatandaşlar, kuruluşlar ve devletler için güvenlik riskleri oluşturabilmektedir. Yapay zekanın kötü amaçlı kullanımı dijital güvenliği (mağdurları hacklemek gibi), fiziksel güvenliği (örneğin, tüketici dronlarını silahlandıran devlet dışı aktörler) ve politik güvenliği (profil oluşturma, gizliliği ortadan kaldırarak gözetim, hedefli dezanformasyon yoluyla kampanyalar yapılması) tehdit edebilir (Brundage vd., 2018: 10).

Özerk araçların sorumluluğu yönünden bir örnek inceleyelim: Uzaktan kumandalı bir taşıt kullanarak yapılan bir saldırı durumunda, platform kontrolörünün bu saldırıyı gerçekleştirme kararı, kendisine verilen veriler tarafından ortaya çıkmaktadır. Hayati mesele, kontrolörün saldırı kararının kendisine sunulan şartlar altında makul olup olmadığı araştırılacaktır. Bu araştırma ya da ilgili sorular, herhangi bir önlem alınıp alınmadığını, saldırının orantılı olup olmadığını, hedefin askeri bir hedef olarak durumunu doğrulayıp doğrulamadığını içermektedir (Boothby, 2012: 589).

Yapay zeka ve AI bölümünde de sıkça değinileceği üzere özerk silahlar da etik açıdan sorunlar ve riskler ortaya çıkarmaktadır. Örneğin bir özerk silah programlama aşamasında yapılan bir hatadan kaynaklı olumsuz sonuçlara yol açabilir hatta bir savaşa bile sebep olabilir.

Avrupa Birliği 2016'da yapay zeka ile ilgili yasal çerçeve ortaya koyan Robotik Medeni Kanunu Kuralları Komisyonuna tavsiyelerde bulunan bir Hareket Taslak Raporu hazırlamıştır. Bu raporda AI'nın yol açabileceği eşitsizlik ve buna bağlı istihdam kayması, fiziksel güvenlik sorunları, teknolojinin yanlış kullanılması, verilerin korunması, mahremiyet sorunları ve etik kodlar gibi konulara yer verilmiştir (Pavaloiu ve Kose, 2012: 16).

Yukarıda yapay zekanın insanlara karşı oluşturabileceği sorunlardan bahsedilmiştir. Ancak bir de insanların yapay zekaya nasıl davranması gerektiği konusunda etik tartışmalar mevcuttur. Örneğin, bir insanın yapay zeka destekli bir robota sahip olması yani bir makine üzerindeki anayasa tarafından da korunan mülkiyet hakkı olması o insana robot üzerinde istediği gibi davranabilme hakkı vermekte midir sorusunun cevabı net değildir. İnsan sahip olduğu robota kötü davranabilir mi, kötü davranırsa bu etik olur mu soruları gündeme gelmektedir. Örneğin, Amerika Birleşik Devletleri'nde robotun testleri sırasında görevli tarafından sopa ile itilerek yere düşürülmesi ve bunun tekrarlanması kamuoyunda bir insana kötü muamele uygulanması ile bir robota uygulanmasının izlenmesi durumunda bunun insanlarda aynı etkiyi oluşturduğu yönünde görüşler ortaya çıkmıştır. Doktrinde de bu görüşler desteklenmekte ve robotlar bu anlamda insan gibi algılanmaktadır (Bozkurt Yüksel, 2017: 94).

Yapay zekanın olumsuz etkileri iki yönlü olarak ele alınmalı ve değerlendirilmelidir. Bunlardan birincisi yukarıda da bahsedildiği üzere yapay zekanın kötü amaçlı kullanımı sonrasında ortaya çıkabilecek sorunlardır. İkincisi ise, bu teknolojiyi kullananlar ve kullanmayanlar arasındaki uçurumun meydana getirdiği sorunlar olacaktır. Yani bu teknolojiye sahip olan devletler daha güçlü konumda bulunacaklardır. Örneğin, fakirin daha fakir zenginin daha zengin bir hale gelmesi gibi sonuçlar ortaya çıkması mümkündür.

Yukarıda yapay zekanın doğurabileceği etik problemler ele alınmıştır. Bunun dışında ortaya çıkabilecek diğer sorunlar da şu şekildedir: Mahremiyet, gizlilik ve güvenlik, yapay zeka destekli robotların fikri mülkiyet ile ilgili sorunları ve bunların fiillerinden doğan sorumluluklar ile ilgili problemler karşımıza çıkmaktadır (Bozkurt Yüksel, 2017: 90-100). Yani yapay zeka destekli robotların öğrenebilmesi durumunda robotlar hukuki haklara sahip olabilecek midir? Bu da bir tartışma konusudur.

Sosyal değişimin desteklenmesi açısından ve insanlık adına, yapay zekanın gerçekten devrimci ve olumlu etkileri çok fazladır. Ancak, tüm bu olumlulukları başarmak risk olmadan imkansızdır. O yüzden çalışmanın bu bölümünde yapay zekanın ortaya çıkarabileceği riskler alt başlıklar halinde ayrı ayrı ele alınacaktır.

Mevcut hukuki düzenlemeler insanı özne olarak kabul etmektedir. Ancak, robotlarda yapay zekanın kullanılması ve böylelikle robotun öğrenebilir hale gelmesi mümkün olacağından robotun bilinçli olarak yaptığı faaliyetlerden sorumlu olması, buna bağlı olarak hukuk önünde bir özne kabul edilmesi sonucuna doğru gidebilecek etik tartışmaları gündem olacaktır (Bozkurt Yüksel, 2017: 92).

2.3. DÜNYADA YAPAY ZEKA UYGULAMALARI

Dünya lideri olma yarışında artık yeni bir aktör olan yapay zekanın yarışı resmen başlamıştır. Son iki yılda, Kanada, Çin, Danimarka, AB Komisyonu, Finlandiya, Hindistan, Japonya, İtalya, Meksika, Singapur, Güney Kore, İsveç, İskandinav- Baltık Bölgesi, Tayvan, BAE ve İngiltere yapay zekanın geliştirilmesi ve kullanılması konusunda bu yarışa katılan ülkelerdendir (Dutton, 2018: 1).

2018 yapay zeka tahminleri raporuna (2018 AI Predictions) göre bu alanla ilgili 8 öngörü yayınlanmış ve şu şekilde sıralanmışlardır (Baccala vd., PwC 2018: 10-22):

1. AI, istihdamı etkilemeden önce işverenleri etkileyecektir: gündemde olan en önemli tartışmalardan biri yapay zeka destekli robotların insanların işlerini elinden alacağı konusudur. Ancak burada korku senaryoları yazmak yerine yapay zeka ile iş piyasası arasında kademeli bir evrim gerçekleştirmek gerekmektedir. Çünkü bu teknoloji ile ortaya çıkan yeni işler kayıp olanları dengeleyecek, insanlar yapay zeka yardımı ile daha verimli olarak işlerine devam edeceklerdir. Ancak burada kuruluşların yapay zeka modeline algoritma ve veri beslemeleri önem kazanmaktadır. Algoritmanın ne zaman karar vereceğini ya da ne zaman kendilerine adım atacaklarını bilmeleri gerekecek. Kısacası AI'nin etkin kullanımı ve farklı ekipler arasındaki iş birliği ile işsizlik gibi risklerin önüne geçilebilecektir. Bu yeni süreç insanlara AI teknolojisi ile işbirliğini vurgulayan yeni bir zihniyet kazandıracaktır.
2. AI dünyaya gelecek ve çalışmaya başlayacak: bugün AI destekli bir gelecek vaat eden birçok yayın karşımıza çıkmaktadır. Asla çarpışmayan özerk araçlar, milisaniyede hastalığı tespit eden robot doktorlar, mal akışını optimize eden ve kendini koruyan altyapılar... Tüm bunlar gerçekleşebilir ancak çok kısa bir sürede değil. Bu gelişmeleri iş avantajına çevirmek için yeni endüstri alanları oluşturmak gerekmektedir. Bunun için de geçmiş veri eğilimleri belirlenmeli ya da insan kararlarını güçlendirmek için ileriye dönük istihbarat sağlanmalıdır.
3. AI, verilerle ilgili büyük soruya cevap vermeye yardımcı olacaktır: kuruluşlar AI sayesinde otomatik makine öğrenimi ve veri yönetimi, metin indeksleme ve sınıflandırma için dil işleme, veri madenciliği için daha kolay yöntemler gibi yeni avantajlardan yararlanabilecektir.
4. Teknoloji uzmanları değil fonksiyonel uzmanlar AI yetenek yarışına karar verecekler: AI daha özel alanlara yayıldıkça, veri bilimcilerinin genellikle bulunmadığı bilgi ve beceri setlerini gerektirecektir. Örneğin, AI uygulaması oluşturan bilgisayar bilimcilerinden oluşan bir ekip pazarlarda uzman değildir. AI'nın insan varlık yöneticisini en iyi nerede destekleyebileceğini belirlemek, bu desteği sağlamak için AI'yı tasarlamaya ve eğitmeye yardım etmek ve AI'yı etkin

bir şekilde kullanmak için istekli ve yetenekli olmak için yanlarında çalışan ekonomistlere, analistlere ve yatırımcılara ihtiyaçları olacaktır. En uygun yapay zeka programı bile her zaman küçük bir bilgisayar bilimciler ekibine ihtiyaç duyacaktır.

5. Çalışmanın siber güvenlik bölümünde detaylı olarak değinildiği üzere Cyberattacks yapay zeka sayesinde çok güçlü bir konuma gelecektir.
6. AI'nın kara kutusunu açmak öncelik haline gelecektir: AI destekli özerk silahlar seri katiller olabilir mi? Örneğin, bir AI sistemi hava kirliliğini azaltmak yönünde kodlandı, bunun en mantıklı yolu insan ırkını ortadan kaldırmak yönünde karar verirler mi? Bu tür tehditler söz konusu olabilir ancak tehlike yönetilebilirdir. Çünkü yapay zeka hala insanların tasarladığı kurallara uymaktadır. Karmaşık görevlerin yerine getirilmesinde ya da örüntü ve görüntünün tanınmasında insanlara yardımcı olmaktadır. AI bir kara kutudur çünkü AI bir karar verdiğinde son kullanıcılar oraya nasıl ulaştığını bilmeyeceklerdir.
7. Uluslar AI üzerine serilecek: AI pastasından pay alabilmek adına, bireysel şirketlerin yanı sıra ülkeler de birbirleriyle yarışacaklardır. ABD 2016'da AI alanında bir güç merkezi olmak adına hem ekonomiyi hem de ulusal güvenliği artırma planı belirlemiştir. Öneriler arasında yasal değişiklikler, ortak kamu veri setleri ve ortamlarının oluşturulması, standartların ve ölçütlerin tanımı, işgücü gelişimi ve AI'nın siber güvenliği ve orduyu destekleme yolları yer almıştır. 2017 yönetimdeki değişiklik ile hükümet bu planı terk etmesine rağmen sermaye yatırımlarının yüzde yüzünü AI ve diğer teknolojilere yapması beklenmektedir. Yine İngiltere de AI becerilerini araştırma ve alımını artırmaya yönelik plan başlattı. Yeni AI bursları ve araştırmacıları için fon sağladı. Kanada AI'yı gelecekteki ekonomisinin bir göstergesi haline getirmek istemekte ve Federal hükümet PanCanadian Yapay Zeka Stratejisini başlatmıştır. Bu program özel şirketler ve üniversitelerle işbirliği içinde AI araştırma merkezlerinin finansmanını içermektedir (Baccala vd., PwC 2018: 19). Japonya da gerçek bir AI ekosistemine ulaşmak için üç aşamalı bir AI teknolojisi stratejisi yayınlamıştır. Nesnelerin interneti, özerk araçlar ve siber ve fiziksel alanın harmanlanması gibi diğer ileri teknolojiler ile yapay zekanın bir araya gelmesini öngörüyor. Almanya da bu anlamda çeşitli ekonomik sektörleri arttırmak için AI kullanma stratejisi oluşturmuştur. Çin de AI'yı ülke için bir ulusal öncelik stratejisi olarak ilan etmiş ve yeni bir ekonomik

model için en büyük liderlik vizyonu sunmuştur. Bu amaçla derin öğrenme laboratuvarı oluşturmak için yatırımlar yapmaktadır. Baidu, Alibaba ve Tencent küresel AI liderleri arasındadır. Yine önde gelen e- ticaret şirketleri de depolarında oldukça gelişmiş AI kullanmaktadırlar. Çin gelecek on yılda bu teknolojiye en fazla faydalanacak ülke olarak karşımıza çıkmaktadır (Baccala vd., PwC 2018:20).

8. Sorumlu AI için baskı yalnızca teknoloji şirketlerinde olmayacak: yeni teknolojiler mutlaka yeni korkular ve riskler içermektedir. Topluluklar ve seçmenler önyargı konusunda endişeli ve müşteriler güvenirlilikten korkuyor olabilirler. Bunun için de paydaşlar kuruluşların AI'yı sorumlu bir şekilde kullandıklarını bilmek isteyecek böylece iş ve toplumu bir bütün olarak güçlendirecektir. AI için ilkeler benimsenmelidir. (Baccala vd., PwC 2018:22).

Günümüzde yapay zeka gelişimleri yavaş ilerlemesine rağmen bunlar sadece bireysel şirketleri değil, aynı zamanda bütün ülkeleri ilgilendiren bir konu haline gelmiştir. Buna bağlı olarak da ülke ve devletler yapay zeka hakkında kendilerine göre bazı stratejiler uygulamaya başlamışlardır.

PWC'nin Global Artificial Intelligence adlı çalışmasına göre, yapay zekanın 2030 yılında dünya ekonomisinde 15.7 trilyon dolarlık bir yere ulaşması tahmin edilmektedir. Ülkeler bazında bakıldığında ise şu sonuç ortaya çıkmaktadır: Çin yüzde 26.1 oranında, Kuzey Amerika yüzde 14.5, Güney Avrupa yüzde 11.5, Asya yüzde 10.4, Kuzey Avrupa 9.9, Afrika yüzde 5.6, Latin Amerika 5.4 oranında pay sahibi olmaları beklenmektedir.

Yapay zeka alanında gelişme gösteren öncelikli ülkelerden Amerika Birleşik Devletleri ve Çin'i söylemek mümkündür. ABD yapay zeka teknolojisini ekonomi ve güvenlik alanlarında en üst seviyede kullanarak bu alanda dünyanın merkezi olmayı amaçlamaktadır. ABD Savunma Gelişmiş Araştırma Projeleri (DARPA), sürekli öğrenen yapay zeka geliştirme çalışmalarına hız vermiş ve Yaşam Boyu Öğrenen Makineler (L2M) isimli 65 milyon dolarlık bir program başlatmıştır (Moore, 2017). ABD – Çin Ekonomik ve Güvenlik İnceleme Komisyonu'na göre Çin, uzaktan kumandalı robotları ve kendi özerk silah sistemlerini geliştirmektedir (Melendez, 2018).

“Otonom askeri robotlar” icat etme sürecinde de yine DARPA'nın destek olduğu projeler öne çıkmaktadır. DARPA insansı robot prototipleri üretmiştir ve ABD

Deniz Kuvvetleri'nin X- 47 adlı dronu, uçak gemilerine sorunsuz inmeyi başarabilmiş ve yine Boston Dynamics'in Atlas adlı robotu bir insanla aynı temel fiziksel özellikleri ve eylemleri paylaşmaya başlamıştır, Ayrıca DARPA'nın Kara Savaşçısı askerleri için giyilebilir bilgisayarları, geniş iletişim cihazlarıyla donatılan robotları da mevcuttur (STM Think Tech Teknolojik Düşünce Merkezi). Oluşturulan sistemlerin ne derece zeki oldukları tartışma konusu olsa da görüldüğü üzere akıllı sistemler ve insansız hava araçları konusunda en önde gelen isimlerden birisi DARPA olmaktadır.

Örneğin Türk Silahlı kuvvetleri için bir Askeri Yürüyüş Asistanı projesi gerçekleştirilmiştir. Giyilebilir teknoloji ile donatılmış olan bu asistan, kullanıcıların yürüme, koşma, tırmanma gibi konularda yardım edecek olan ve cenker sistemi ile birlikte kullanılacak olan bir dış iskelet sistemidir (Aselsan).

Bu konuda bir diğer örnek de ABD'nin Maven Projesidir. Algoritmik savaşa yönelik farklı disiplinleri bir araya getiren bu proje ordunun dron görüntülerini analiz etme yeteneğini geliştirerek, ABD'nin savaşları bilgisayar algoritmaları ve yapay zeka sayesinde kazanmasını amaçlamaktadır (STM ThinkTech Teknolojik Düşünce Merkezi, 22).

Kanada'nın yapay zeka stratejisine CIFAR (Canadian Institute for Advanced Research) öncülük etmektedir. Bir araştırma merkezi olan CIFAR 2017 yılında, 125 milyon dolarlık "Pan- Canadian Artificial Intelligence Strategy" (Kanada Yapay Zeka Stratejisi) adlı bir yapıyı oluşturmuştur. Bu stratejinin ana hedefleri arasında Kanada'da sıra dışı yapay zeka araştırmacıları ve nitelikli mezunların sayısını arttırmak, yapay zeka konusunda ulusal bir araştırma topluluğunu desteklemek ve yapay zekadaki gelişmelerin ekonomik, etik ve politika etkileri konusunda küresel düşünce liderliği geliştirmek gibi amaçlar bulunmaktadır. Ayrıca bu strateji, AI Enstitüleri, toplum ve ulusal programları da içermektedir (CIFAR). Kanada'nın yapay zeka stratejisi araştırma ve yetenek stratejisi olması bakımından diğerlerinden farklıdır. Örneğin, CIFAR AI ve Toplum Programı AI'nın politikasını ve etik etkilerini inceler ancak veriler ve gizlilik veya beceri geliştirme gibi diğer stratejilerde bulunan politikaları içermez (Dutton, 2018: 23).

Bu alanda çalışmalar yürüten Çin' e bakılması gerekirse, Çin hükümeti 2017'de Yeni Nesil Yapay Zeka Gelişim Planı yayınlamıştır. Üç adımlı bir plan olarak

algılanması gereken bu planda Çin ilk olarak AI endüstrisini 2020 yılına kadar rakipleriyle aynı hızda yapmayı istemektedir. İkincisi 2025 yılına kadar AI alanında dünya lideri olmayı amaçlıyor ve son olarak 2030 yılına kadar AI çalışmalarının birincil merkezi olmayı hedeflemektedir (Dutton, 2018: 23-24). Ayrıca Çin şu anda havaalanlarında AI destekli vücut tarayıcıları kullanmaya başlayacağını duyurmuştur. Çin havacılık ve Uzay Bilim ve Sanayi Kurumu (CASIC) tarafından geliştirilen bu tarayıcılar, şüpheli malzemelerin konumlarına belirlemekte ve yolcuların yüzlerini pikselleştirerek gizlilik koruma önlemleri de uygulamaktadır. CASIC 1956'da Pekin'de kurulmuş ve akıllı füzelerin tasarımında önemli olan bir kuruluştur (Papadopoulos, 2018).

Yine bu konuda çalışmalar yapan bir diğer kuruluş ise Avrupa Savunma Ajansı (EDA) olarak karşımıza çıkmaktadır. EDA, yapay zeka temelli sistemlerin birleştirilmesinden meydana gelen nesnelerin internetini kullanarak, büyük bir savaş ağını kent savaşlarında kullanmaya odaklanmıştır. Halen hazırlanmakta olan yeni bir EDA projesi olan WINLAS (Wireless Sensor Networks for Urban Local Areas Surveillance) şehir savaşı için pek çok sayıda heterojen cihazla sensör ağlarının davranışını analiz edecektir (Sanchez).

Günümüzde birçok ülke İHA sistemlerini üretme ve geliştirme vizyonlarını çizmeye başlamıştır. Çünkü insansız araçlar, sivil ve askeri ortamda geleceğin sistemleri olarak öne çıkmaktadır. Çin, Amerika ve Avrupa ülkelerinin yanı sıra Rusya ve İsrail de yapay zeka alanında önemli çalışmalar yapmaktadır. Türkiye' de ise, insansız hava aracı sistemleri geliştirmesi ve Türk Silahlı kuvvetleri envanterine girmesi için çalışmalar başlamıştır. 2004 yılı sonrasında Savunma Sanayi Başkanlığı önderliğinde yapılan çalışmalar sonucunda, Türkiye'de İHA sistemleri konusunda büyük bir sanayi altyapısı oluşturulmaya başlanmıştır (STM ThinkTech Teknolojik Düşünce Merkezi, 23). Yani tam özerk yapay zeka teknolojilerinin Türk Silahlı Kuvvetleri'nde savaş ortamında kullanılması için çalışmalar devam etmektedir. Ancak bu sistemlerde kontrol, yapay zeka ve insanlar arasında paylaşılmaktadır.

İHA'ların özerklikleri arttığı durumda sürü halinde eylemde bulunmaları söz konusu olabilmektedir. Bu konuda DARPA tarafından "Collaborative Operations in

Denied Environments (CODE)” AR-GE çalışmaları başlatmıştır (STM Think Tech Teknolojik Düşünce Merkezi, 24).

2.4. YAPAY ZEKA VE RİSKLİ ALANLARI

2.4.1. Güvenlik, Gizlilik, Mahremiyet

İlk bölümde de değinildiği üzere yapay zeka alanında en çok ilerleme kaydedilen konular arasında yapay zekanın tanıma, dil algılama ve araç navigasyonu gibi görevleri mevcuttur. Bu görevlerden bazıları güvenlik açısından riskler oluşturmaktadır. Örneğin tanıma yöntemi ile yapay zeka sistemi ile oluşturulan içeriğin sosyal medya üzerinden kamuoyuna dağıtılması ya da sentetik görüntüler kullanılarak kişilerin çevrimiçi kimliğe büründürülmesi söz konusu olabilir (Brundage vd., 2018: 13).

Yapay zekanın bu uygulamaları güvenlik alanında da tartışılmaktadır. Yapay zeka çift kullanımlı bir teknoloji alanıdır. Yapay zeka sistemleri ve bilgi onları nasıl tasarlayacağımızın gerek sivil gerekse askeri faydalı ve zararlı amaçlara doğru ve daha geniş anlamda kullanılmaktadır (Brundage vd., 2018: 16).

Yapay zeka algoritmaları, gözetimi güçlendirerek mahremiyeti tehdit etmektedir. Örneğin bir yapay zeka ile çalışan yüz tanıma yazılımı, kapalı devre TV sistemlerine, bireyleri kentsel manzara içerisinde ilerledikçe izleme olanağı vermektedir. Bu hem sosyal hem de politik ile ilgilidir. Çünkü gizlilik, ifade ve örgütlenme özgürlüğü gibi diğer temel hakların en önemli kavramıdır (Smith ve Naupale, 2018: 11).

Yapay zeka istihbarat simülasyonunu ve akıllı makineler yaratmayı mümkün kılmaktadır. Burada nanoteknoloji, biyoteknoloji, bilgi teknolojisi ve bilişsel bilimleri (NBIC) arasında bir etkileşim söz konusudur. Bugün bazı robotlar insan davranışlarını taklit edebilir ve işgücü içindeki insanlarla rekabet halindedir. Pazar ve günlük yaşamda, deneyimle otomatik algısal öğrenmeyi becerebildikleri ölçüde özerk olabilmektedirler. Muazzam hafıza kapasitesine sahiptirler ve aynı zamanda makineye programlanmış bilinç, makineye bir nevi akıl yürütme becerisi kazandırmaktadır (Jean ve Le Deaut, 2017: 3). Bazı makineler yapay duyguları ifade edebilecek ve karmaşık

problemleri çözebilecektir. Tüm bu gelişmeler de insan hakları ve bu teknolojinin insanlık onuruna etkileri bakımından yeni soru ve sorunlar ortaya çıkarmaktadır.

Büyük veri çağında algoritmalar hemen hemen her konuda bizleri yani insanları aşmıştır. Hangi kitaptan hoşlandığımız ya da bir sonraki tatil planımız hakkında onlar daha doğru tahminler yapıyorlar, arabaları bizden daha güvenli bir şekilde sürüyorlar. Bizim ile ilgili sayısız veriden yararlanıp, daha önce sipariş ettiğimiz ya da tıkladığımız ürünleri değerlendirerek internet reklamcılığı bile yapıp önümüze o ürünü getirebiliyorlar (Risse, 2018: 3).

Şimdi hem mahremiyet konusunu hem de etik problemler içeren bir örnek verelim; geçtiğimiz yıllarda Amerika’da, ev sahibinin ve iki misafirin olduğu bir evde cinayet gerçekleşmiştir. Evde, Amazon’un sesli komutla çalışan Echo isimli bir kişisel asistan bulunmaktadır. Seslenme komutu ise “Alexa”dır. Bu cinayet olayında polis ev sahibini suçlamaktadır ve polis akıllı bir ev cihazı olan Echo’ya el koymuştur. Amazon’dan o geceye dair kayıtları istemiş ancak Amazon bunları vermemiştir. İşte burada devreye iletişimin ve özel hayatın gizliliği konuları girmiştir. Görüldüğü üzere burada bir robotun tanıklığı ve hukuken belirsizlik söz konusudur (Öymen, 2017). İnsanlar robotlarla iç içe yaşadığında yapay zeka destekli bu robotlar her şeyi kayıt altına alacaklardır. Bunun da mahremiyet ve gizlilik konusunda çeşitli belirsiz sorunlara yol açması muhtemeldir. Televizyonlar bile evdeki olayları kayıt altına alıp bunları başkalarına bilgi aktaracak şekilde programlanıp gözetleme amaçlı kullanımı söz konusu olabilir. Telefonlardaki teknolojiye bakılacak olursa, şu an bile Google’nin ses dinleme özelliği vardır.

Güvenlik ile ilgili sorunlara değinilecek olursa örneğin otonom araçların uzaktan bilgisayar korsanları tarafından ele geçirilip araca kaza yaptırılması söz konusu olabilir. Otomobillerin gittiği rotayı, trafikteki davranış alışkanlıklarını nesnelerin interneti sayesinde başka bir yere aktarması mümkündür (Bozkurt Yüksel, 2016: 91). Sonuç olarak tüm bunlar güvenlik açısından riskli konular haline gelmekte ve tartışılması gereken en önemli konular halini almaktadır.

Yapay zeka sistemleri genellikle hem verimli hem de ölçeklenebilir olarak nitelendirilmektedir. Burada verimlilikten kasıt, bir kez eğitilmiş ve konuşlandırılmış olan yapay zekanın bir işi çok hızlı ve ucuz maliyetle yerine getirmesidir. Ölçeklenebilir

olması ise; bilgisayar gücünü artırarak belli bir görevi yerine getirebilecek olması ve görevin daha bir çok örneğini tamamlayabileceği anlamına gelmektedir (Brundage vd., 2018: 16). Örneğin yüz tanıma sistemi bir kez eğitildiğinde birçok insana uygulanabilmektedir. Bu anlamda yapay zeka insan yeteneklerini aşabilmekte ve bu yüzden güvenlik ile ilgili problemler ortaya çıkmaktadır.

Güvenlik ve mahremiyet hakları, yalnızca dronlar veya robot askerler tarafından değil, aynı zamanda elektronik olarak kaydedilen insan etkinlikleri ve varlık dünyasında izlenebilirliğin artırılmasıyla potansiyel olarak baltalanmaktadır. İnsanlar hakkında mevcut olan verilerin miktarı hızla artacaktır. Örneğin biyometrik sensörler aracılığıyla insanlar duşta izlenebilir ve belirli hastalıkların teşhisi konulabilir. Ancak bu verilerin tamamı özel mülkiyet sayılacağından medeni ve politik haklara yönelik problemleri ortaya çıkaracaktır (Risse, 2018: 12).

Cambridge raporuna göre yapay zekanın tehditleri üç ana başlık altında ele alınmaktadır. Buna göre yapay zeka mevcut tehditleri genişletebilir, yeni tehditler ortaya çıkarabilir ve son olarak tehditlerin tipik karakterini değiştirebilecektir.

Yapay zeka alanındaki ilerlemeler, aktörlerin belirli saldırıları yapma istekliliğini ve mevcut tehditleri artıracaktır. Bilgi işlem gücü ve robotların azalan maliyeti de bazı şeyleri daha da kolaylaştırmaktadır. Örneğin, patlayıcılarla kolayca doldurulabilinen insansız uçaklar, devlet dışı grupların hava saldırıları yapma imkanını daha da artırmıştır (Brundage vd., 2018: 19). Bahsedilen bu ilerleme ayrıca, yeni saldırı çeşitlerini de ortaya çıkarmaktadır. Yani belirli bir görevi daha başarılı bir şekilde tamamlamak için bu sistemler kullanılabilecektir. Yapay zekanın insan yeteneklerinden bazılarının fazlasını yapabilme özelliği, bu sistemlerin bazı saldırıları yapabileceği anlamına gelmektedir. Örneğin, bir insan bütün sesleri taklit edemezken bunu yapay zeka destekli bir makine yapabilecektir. Bu da güvenlik açısından riskler taşımaktadır. Yani başkalarının kimliğine bürünmek ve dezenfarmasyon yayılması anlamına gelmektedir (Brundage vd., 2018: 20). Son olarak ise yapay zeka tehditlerin tipik karakterini değiştirebilir. Bu da bu sistemlerin insanı aşma, verimlilik ve ölçeklenebilirlik özelliklerinden ileri gelmektedir. Sonuçta daha sık ve daha büyük ölçekli saldırılar olabilir. Yani saldırganların daha etkili olması beklenmektedir. Örneğin mızrak avcılığı, mesajların kişilere uyarlanmasını içermeyen normal kimlik

avcılığına göre daha etkilidir fakat nispeten daha pahalıdır ve toplu olarak uygulanamamaktadır. Daha genel kimlik avı saldırıları sadece ölçekleri nedeniyle düşük başarı oranlarına rağmen karlı olmayı başarır (Brundage vd., 2018: 21).

Robotların askeri alanda gözetleme amaçlı kullanılması söz konusudur. Örneğin insansız hava araçları (dronlar) fark edilmeden günlerce havada kalarak üzerinde bulunduğu geniş alanlardaki faaliyetlerle ilgili tüm bilgileri aktarabilir ve daha küçük insansız hava araçları da geniş alanlarda dolaşarak herhangi bir hareket durumunda bunu üsse haber verebilir (Bozkurt Yüksel, 2017: 91).

2.4.1.1. Sosyal Medya ve Yapay Zeka

Günümüzde iletişim teknolojilerindeki hızlı gelişmeler; yeni medya, internet, sosyal medya, sosyal ağlar ve sanal alem gibi bir çok yeni kavramı hayatımıza sokmuştur. Bu kadar hızlı değişen ve gelişen teknolojinin toplumları ekonomik, sosyal ve psikolojik ve kültürel olarak etkilemesi kaçınılmazdır. Geline nokta, sosyal medyayı insanlar özgürce kullanabilmektedirler. Bu yapı, toplumlarda üretim, tüketim ve güç ilişkilerini de etkilemekte ve olumlu ya da olumsuz açılardan ele alınabilecek sonuçlar ortaya çıkarmaktadır. Çalışmada bu başlık altında yeni medyanın getirdiği riskler ve olumlu sonuçları tartışmalı bir biçimde ortaya konulacaktır. Yapay zeka destekli teknolojilerin fazlaca kullanıldığı sosyal medyanın günümüzde yer edindiği alanın ve etkilerinin çok fazla olması sebebiyle güvenlik, gizlilik ve mahremiyet konusunda ayrı bir alt başlık altında ele alınmasında yarar görülmüştür.

Sosyal medya devletler ve insanlar için zaman zaman tehdit unsuru haline gelebilmektedir. Örneğin sosyal medya aracılığıyla yabancı istihbarat örgütleri veri elde edebilmekte ya da siyasi, askeri veya toplumsal açılardan manipülasyon yapılmasına imkan tanınması gibi şeyler sıralanabilmektedir. Ayrıca milyonlarca insan tarafından kullanılması da sosyal medyanın denetimini güçleştirmekte ve bu yüzden de risk oluşturmaktadır. Görüldüğü gibi çok geniş bir kitle tarafından kullanılan sosyal medyanın; toplum, devletler, politika ya da ekonomi üzerindeki etkileri kaçınılmaz olmaktadır.

Bu etkilere örnek verilecek olursa, bugün siyasi partiler sosyal medya sayesinde seçmenlerle daha çok iletişim kurmakta ve birtakım olaylar karşısında ona göre davranış ve eylem sergileyebilmektedirler (Aydın, 2019).

2018 Ocak ayı ele alınarak oluşturulan rakamlara göz atılacak olursa, yaklaşık 7 milyar 500 milyon dünya nüfusu vardır ve bunun 5 milyarı telefon, 4 milyarı da internet kullanmaktadır ki bu 4 milyar insan da sosyal medyayı aktif olarak kullanmaktadır (Erkan, 2019: 23).

Günümüzde medya insanların tüm hayatlarını bağımlı hale getirdikleri bir platform olup, insanların yaşantılarını izlemekte ve onlar için çözüm önerileri sunmaktadır. Sosyal medya uygulamaları veri oluşturmada en önemli aktörler arasında bulunmaktadır. Domo'nun Data Never Sleeps 5.0 raporuna göre bunlar sıralanacak olursa (Marr, 2018):

- Instagram kullanıcıları günün her dakikasında 46,740 fotoğraf paylaşıyor
- Snapchat kullanıcıları 527,760 fotoğraf gönderiyor
- LinkedIn'e 120'den fazla niteklikli katılım vardır
- Her dakikada 4,146,600 kez YouTube videosu izlenmektedir
- Her dakikada Twitter'da 456,000 tweet atılmaktadır.

Tüm bunlar göz önüne alındığında sosyal medyanın veri yaratmaması söz konusu olamaz. Aksine farkında olmadan büyük veri ağına en fazla veri oluşturan ortam sosyal medyadır demek yanlış olmayacaktır. Yukarıda sayılanların dışında hizmet, iletişim, dijital fotoğraflarla da insanlar milyonlarca veri üretmektedir.

Dünya tarihine bakıldığında güvenlik ihtiyaçları teknolojik yönelimi artırmış ve teknoloji gelişme ve çeşitlenmeler göstermiştir. Fransa'nın GPS'i Birinci Körfez Savaşı'nda kullanmasından, Arap Baharı sırasında sosyal medyanın kullanılmasına kadar teknoloji, devletler arasındaki güç dengesini değiştirecek bir faktör olmuştur. Modern askerler ve istihbarat ajansları günümüzdeki bilgi teknolojilerini gözetim için kullanmaktadırlar. Ya da Mısır ve Ukrayna gibi yerlerde protestocular veya IŞİD gibi isyancı hareketler destekçilerine mesajlarını daha kolay ve hızlı bir şekilde iletmek için sosyal medyayı kullanmaktadırlar (Brundage, 2018: 44).

Devletlerin yanı sıra kişisel bazda incelenecek olursa, sosyal medyada güvenlik ve gizlilikle ilgili sıkıntılar yaşanmaktadır. Örneğin telefonlara ya da bilgisayarlara bir uygulama indirirken “izin ver” komutuna tıklayarak o uygulamayı indirmek gerekmektedir ki bu mecburen onaylandığında o program aracılığıyla insanların bazı bilgilerine ulaşmak mümkün olmaktadır.

En göze çarpan sosyal medya programları Facebook, twitter, instagram gibi uygulamalardır. Örneğin, facebook kişilerin bilgilerini kullanarak, neyi beğenip neyi beğenmediklerini değerlendirerek, insanların karakterlerini analiz edip bunları farklı amaçlar için kullanabilmektedir. Facebook ücretsiz bir programdır ancak insanların tüm bilgilerinin orada olması riskler meydana getirmektedir. Bu konunun seçimlere etkisi ve demokrasi boyutu daha sonraki bölümlerde ele alınacaktır.

Sosyal medya alanında oluşan sorunlara ve risklere örnek verilecek olursa, 2018 Mart ayında sosyal medyada “10 years challenge” hashtaglı bir akım başlatılmıştır. Bu akıma göre insanlar on yıl önceki ve şu anki fotoğraflarını aynı karede paylaşmaya başlamışlardır. Neredeyse herkesin bu akıma uymasının ardından tartışmalar ortaya çıkmış ve bu akımın yapay zekanın bir tuzağı olduğu iddiası ortaya atılmıştır. Yani bu fotoğraflar sayesinde insanların on yıl önceki hallerinden, on yıl sonraki görüntülerine de ulaşmak mümkün olacaktır. Ayrıca, bu akımın yapay zekanın yüz tanıma sistemini öğrenmesi için ortaya atıldığı tartışmalara dahil olmuştur. Kriminal işlemlerde de kullanılması ihtimal olduğundan bir risk olarak görülmektedir.

Geçmişte karmaşık toplumlardaki durum ilk önce toprak mülkiyeti tarafından ve Endüstri Devrimi sonrasında fabrikaların mülkiyeti tarafından belirlenmiştir. Şu anda da verilerin eşit olmayan bir şekilde sahiplenilmesi, toplumdaki pek çok insan için de zararlı sonuçlar doğuracaktır. Alfabe, Facebook veya Tesla gibi şirketlerin gücü kamu yararı için uygun değilse, kendimizi şirketlerin egemen olduğu bir dünyada bulabilir (Risse, 2018: 12).

Sosyal medyayı bir de ulusal güvenlik açısından ele almak gerekmektedir. Bu bir örnekle açıklanacak olursa, 1955 yılında 6-7 Eylül tarihlerinde, yerel bir gazetede Atatürk’ün evinin bombalı bir saldırı sonucu hasar gördüğü yazılmıştı. Halk bu haberi doğru kabul etmiş ve binlerce kişi sokağa dökülerek Rumları hedef almışlardır. Rumların çalıştıkları yerler ya da evleri yakılmıştır ve bunun üzerine birçok Rum göç

etmek zorunda kalmıştır (Aydın, 69). Yani yalan haber yüzünden güçlükle bastırılan olaylar ve olumsuz sonuçlar ortaya çıkmıştır. Bununla birlikte kişisel veri toplamaya maruz kalanlar ile verileri toplayan, kullanan ya da analiz eden kişiler arasında eşitsiz ve adaletsiz durumların veya menfaatlerin olabileceği de unutulmamalıdır. Veri kaynakları genellikle insanların rızası, kontrolü, seçimi hatta farkındalığı bile olmadan sağlanabilmektedir. Veri toplayıcı bunu ürünlere ve hizmetlere değer katabilecek ve yeni gelir akışları elde edebilecek yararlı bir kaynak olarak değerlendirebilmektedir (Rose, 2015: 42).

Sosyal medya ulusal güvenlik açısından ele alındığından son yıllarda gerçekleşen ve bu konuda önem arz eden en temel nokta olarak Arap Baharı gösterilmektedir. Arap Baharı ile birlikte birçok ülkenin ulusal güvenliği sosyal medya aracılığı ile riskler ve tehditlerle karşılaşmıştır. Örneğin, Libya devlet otoritesi ortadan kalkmış ve iki ayrı hükümet ve meclis oluşmuştur (Aydın, 69). Görüldüğü üzere sosyal medya uygulamaları ile halkı yani insanları örgütlemek ya da sokaklara dökmek çok daha kolay hale gelmiştir ve bu devletlerin önlem almalarını zorlaştıracak şekilde çok kısa bir sürede gerçekleşmektedir.

Yeni medya ya da sosyal medya olarak adlandırılan ortamlarda insanlara ulaşan bilginin arkasında başka bir güç olabilmekte ve istenilen mesajı göndermek için (kullanılan müzik, arka plandaki görseller, sunucuların yüz ifadesi vs. ile) medya araç olarak kullanılmakta yani zaman zaman sadece belli bir amaca hizmet etmektedir (Dağıtmaç ve Özbay, 2018: 66).

Tüm bunların yanında sosyal medyanın olumlu etkilerini ele alan bir kesim de vardır. Bunlar, hükümet politikalarının halka duyurulması ya da karar vericilerin aldığı kararların sorgulanabilmesi için sosyal medyaya gerek olduğunu ve böylece ulusal güvenliğe katkı sağlanacağı görüşünü savunmaktadırlar (Aydın, 69).

Sosyal medyanın olumlu etkilerine bir örnek daha verilecek olursa, sosyal paylaşım sitesi olan Facebook terörle bağlantılı ya da teröre destek verici nitelik taşıyan içerikli kaldırma yolunda adım atıldığını açıklamıştır (Corera, 2017). Bunu da yapay zeka destekli teknolojiler ile gerçekleştirmektedir.

Yukarıda da belirtildiği üzere sosyal medyanın ulusal güvenlik açısından risk oluşturduğu noktalardan biri Arap Baharı idi. Ancak bundan önce de sosyal medyanın

tehdit oluşturduğu bazı olaylar karşımıza çıkmıştır. Örneğin, Ukrayna’da ortaya çıkan Turuncu Devrim’de internet teknolojisi aracılığı ile halklar örgütlenmiş ve kitleler oluşturularak güvenlik tehdit ve sorunları ortaya çıkmıştır. Turuncu Devrim devletler için sosyal medyanın riskler taşıması anlamında ilk olması açısından önem arz etmektedir (Aydın, 96).

Bu anlamda ikinci önemli nokta ise Wikileaks gizli belge ve bilgilerin dışarıya aktarılması olayıdır. Bu aktarılma ile bir çok ülke ve devletin ulusal gizli belgeleri, sırları sosyal medya üzerinden dışarıya aktarılmış ve güvenlikle ilgili zafiyetler ortaya çıkmıştır (Aydın, 70).

Bu dönüm noktalarından üçüncüsü ise, yukarıda da bahsedildiği üzere Arap Baharı’dır. Bu olayda sosyal medya aracılığı ile toplumsal olaylar ortaya çıkmış ve sonuçları devletler açısından büyük önem arz eden, ardı ardına birbirini etkileyen olaylar zinciri meydana gelmiştir.

Son yıllarda sosyal medya ve yapay zeka teknolojilerinin etkilerinden en çok tartışılanı da Amerika Birleşik Devletleri’nde seçimlerin yönlendirilmesi konusudur. Bu olayda Facebook aracılığı ile 50 milyon bireyin kişisel bilgileri Cambridge Analytica anket şirketine aktarılmış ve kişilerin özellik ve görüşlerine uygun bireysel propagandalar ile seçimler yönlendirilmiştir. Kaçınılmaz olarak bu da ulusal güvenlik ve demokrasi anlamında sıkıntılar içermektedir (a.g.e.: 70). Bilgi ekosisteminin kendisi politik manipülasyona olanak sağlamaktadır. Ayrıca medya platformları kesin sansüre başvurmadan kamuoyunu ya da belirli bir içeriği yönetebilmektedirler (Brundage vd., 2018: 47).

Tüm bunların dışında Cambridge raporuna göre, yapay zeka sahteciliği daha da artırabilecektir. Yani, insanların aleyhinde ses ya da video kayıtları, yanıltıcı bilgilerin yayılması, sahte haberlerin yazılması vs. çok daha kolay hale gelecek ve kaliteli sahtecilik daha düşük maliyetle ortaya çıkabilecektir.

Sonuç olarak sosyal medyanın güvenlik açısından tehdit ve risklerini özetlemek gerekirse, öncelikle sosyal medya aracılığı ile siyasi, ekonomik ya da askeri anlamda yanıltmalar söz konusu olabilmektedir. Aynı zamanda diğer istihbarat örgütlerine bilgi sızdırılması ve sırların ortaya çıkarılması çok daha kolay hale gelebilmektedir. Bunlara ek olarak sosyal medyanın büyük halk kitlelerini örgütleyip

olaylara sevk etmesi de ulusal güvenlik açısından tehditler oluşturmakta ve toplumsal güvensizliğe ve denetim güçlüklerine yol açmaktadır (Aydın, 70). Ortaya çıkan ağ toplumu, küresel ekonomi ve politikalarla etkileşim içinde olup yeni bir iletişim, yönetim ve yaşam biçimlerinin somutlaşmış hali olarak karşımıza çıkmaktadır (Dağıtmaç ve Özbay, 2018: 54).

2.4.2. Adalet, Ön Yargı ve Hesap Verilebilirlik

Yapay zeka ile donatılmış gerek robotlar, gerek yazılımlar, gerekse nesnelerin interneti gibi uygulamalar; adalet ve hesap verilebilirlik alanlarında üzerinde tartışılması gereken konulardır. Bu sistemler yasal açıdan çok çeşitli zorluklar ve sorular ortaya çıkarmakta ve yeni yasal düzenlemeleri gerektirmektedir. Teknoloji ilgili politika ve düzenleyici durumlardan ve ortamlardan çok daha hızlı ilerleme kaydetmekte ve böylece uygulamaların bütün alanlarını etkilemektedir (Rose, 2015: 54).

Yapay zeka sistemleri toplumsal önyargıları yansıtmaya ve daha da kötüleştirme ve bireyleri ve grupları, özellikle de marjinalleşmiş olanları dezavantajlı hale getirebilecek sonuçlar üretme potansiyeline sahiptir. Örneğin, Amerika’da ceza adaleti sistemindeki bireylerin suç işleme riskini değerlendirmek için kullanılan bir bilgisayar programı siyah sanıkları, beyaz sanıkların hemen hemen iki katı yüksek riskli olarak işaretlemiştir (Smith ve Naupale, 2018: 11). Yapay zeka sistemleri tarafından toplanan veriler onlarla etkileşime giren insanlar hakkında detaylı bir portre çizebilir ve bu portreler yararlı ve ayrımcı amaçlar olmak üzere iki hedefle kullanılabilir (Rose, 2015: 55).

2.4.2.1. Demokrasi

Yapay zekanın bir diğer etki alanı da demokrasidir. Yapay zeka gelişmelerinin demokrasiye zarar verip vermeyeceği ya da otoriterizmi güçlü kılıp kılmayacağı konusunda tartışmalar son zamanlarda önem kazanmıştır. Burada önemli olan, yapay zeka programcılarının ideolojik önyargılara sahip olmayan politik olarak tarafsız olan tasarımlar yapmalarının gerekliliğidir (Ünver, 2018). Yani yapay zekayı belirli bir politikayı tercih etmeyen bir hale getirmek gerekir.

Yapay zeka; siyaset, askeri ve bilim meselelerini orantısız şekilde etkileyecek olan kodlayıcı üretim biçimlerini tekelleştiren kurumların bir araya gelmesi nedeniyle güç merkezileşmesini güçlendirecektir. Bu da demokrasinin ortadan kaldırılmasına yol açan, siyasi katılımı ve temsili en aza indirebilecek bir feodal ağ oluşturacaktır (Ünver, 2018). Bunlar da toplum üzerinde güçlü kontrol mekanizmaları kuracaktır.

Burada demokrasinin ve politik özerkliğin altı çizilmelidir. Bir dünyada giderek daha fazla ve serbest bilgi akışına bağlı yanlış bilgilendirme, demokrasi ve istikrara karşı gerçek ve büyüyen bir tehdittir. Buna örnek olarak 2016 ABD başkanlık seçimi verilebilir. Bu seçimde Facebook üzerinden hedeflenen yanlış bilgilendirme rolü gerçekleşmiştir. Yani, sosyal medya kampanyalarında toplanan son derece kişisel veriler değerlendirilerek yapay zeka uygulamaları, daha verimli propaganda ve davranışsal manipülasyon kampanyaları yapmayı kolaylaştırmıştır. (Smith ve Neupane, 2018: 13). Verilen bu örneğe göre, seçim öncesinde Facebook verileri kullanılarak insanların hangi parti ve görüşlere ilgisi olduğu yapay zeka ile öğrenilerek ona göre özel propaganda uygulanmış ve Trump bu sayede başarıya ulaşmıştır. Görülmektedir ki, yapay zekanın siyasete ve politik alana ve en önemlisi de demokrasiye etkisi oldukça fazladır ve bu giderek daha da artacaktır. Yapay zeka ortamlarında, her makul seçim sistemi yanlış bilgilendirmelerle manipüle edilebilmektedir. Ayrıca seçimlerin kontrolden çıkabileceği de var olan tartışmalar arasındadır. Kısacası, yapay zekayı en iyi ve doğru kullananlar gerek seçimleri gerekse gücü kazanacaklardır.

Duygusal olmayan robotlar baskıcı rejimlerin araçları olarak görev yapabileceklerdir. Akın Ünver'e göre, yapay zekanın mevcut rejim türlerini nasıl etkileyip değiştireceğine dair farklı yörüngeleri öne süren iki gelenek ortaya çıkmıştır. Bunlar algoritmik feodalizm ve totaliterlik olarak karşımıza çıkmaktadır. Yani yapay zeka, feodalist koşullar yaratabilecek üretim ilişkilerini ortaya çıkarabilir ve şeffaf olamayan ve hesap vermeyen teknolojinin ya da bilgi sistemlerinin, siyasi katılım ve temsilciğine yol açabilecektir. Aynı zamanda merkezci kontrol yapılarını da güçlendirebilecektir. Yapay zeka algoritmalarının politik ve sosyal yaşama olan etkilerinin, kullanıcılar tarafından değiştirilemeyecek olması yapay zekayı kapalı bir teknoloji olarak değerlendirmemize neden olmaktadır (Ünver, 2018: 5).

Yapay zekanın ana yorumlamalarından ikincisi ise bu teknolojinin faşist bir sistem yaratacağı fikridir. Yapay zeka temeline dayanarak karar verme ve kontrol odaklı gözetimler kısıtlayıcı bir baskı hiyerarşisini ortaya çıkaracaktır. Teknoloji ve bilim, faşist rejimler tarafından bir sosyal güce dönüşmekte ve kendi hayatlarını ele geçirmelerini sağlamaktadır. Teknologizm bir toplumdaki hak ve özgürlüklerin sınırlarını belirler ve faşist rejimlerde tam bir politik ideoloji haline gelmektedir (Ünver, 2018: 5).

Yapay zeka iç politikada, isyan kontrol ve gözetim endüstrilerini ifade ederken, uluslar arası alanda ise, siber güvenlik, insansız sistemler ve çok geniş bir iletişim ağı konularını içine almaktadır (Ünver, 2018: 6).

Yapay zeka otoriterizminin bir diğer tartışılması gereken olumsuz etkisi de, ikna edici algoritmaların ortaya çıkmış olmasıdır. İkna edici bir algoritma kullanıcı davranışını açık emir ya da talimatlar olmadan yönlendirmektedir. Ancak bunu farkına vardırmanın gizli yaparak, istenen seçeneğe veya sonuca yönlendirir. Cambridge Analytica, radar altında veri toplama ve profil oluşturma yöntemleriyle ne kadar geniş büyüklükteki politik mühendisliğin yapılabileceğini kanıtlamıştır (Ünver, 2018: 9).

Demokrasi ve yapay zeka konusunda gündemde olan en önemli tartışmalardan bir diğeri de bu teknolojinin karar verme sürecine dahil olup olmayacağıdır. Akın Ünver'e göre karar verme süreci beş aşamadan oluşmaktadır. Bunlar, gündem belirleme, politika oluşturma, karar verme, uygulama ve gözetim aşamalarıdır. İlk aşamada yapay zekanın amacı, nüfusun duygularını büyük veri sayesinde hissetmektir. Politika oluşturma aşamasında ise, yapay zeka sonuçların çoklu süreçlerini yürütecek ve bu sonuçlara karşı potansiyel halk tepkisini tahmin ederek ona göre davranılmasını sağlayacaktır. Üçüncü aşama olan karar verme ise, demokrasiye ya katkı sağlar ya da ona zarar verecektir. Karar verme otomatikleştiğinde, politika hazırlama süreci ve verilen karar önemli ölçüde meşruiyetini kaybedecektir. Yani böyle bir durumda demokrasilerde ve otokrasilerde siyasi kurumlar zayıflayacaktır. Uygulama aşamasında yapay zekaların rolü, uygulama stratejilerinin modellenmesi ve kaynak tahsisinin yapılması olarak karşımıza çıkmaktadır. Karar verildikten sonra algoritmalar, ilgili kurumlarla iletişim kuracak ya da finansmanı transfer edecektir. Son aşama olan gözetim aşamasında yapay zekalar önceden belirlenmiş başarı belirteçleri ile yeni

politikaların etkilerini izleyebilir, ölçebilir ya da karar vericileri bu politikaların gelecekteki sonuçları hakkında bilgilendirme yapabilecektir (Ünver, 2018: 10-12).

2.4.3. Siber Güvenlik

Yeni medya ve dijital çağ ile birlikte yeni kültürel biçimler, ürünler ortaya çıkmakta ve kültürün dönüşüme uğramasıyla da siber kültür alanı oluşmaktadır. “Siber Kültür” kavramı 1990’ların ortasından itibaren akademik alanda kullanılmaya başlanmış olup yeni teknolojilerin insanların hayatlarını nasıl değişip dönüştürdüğü üzerine düşünmeyi amaçlayan bir kavram olarak karşımıza çıkmaktadır (Dağıtmaç ve Özbay, 2018: 50).

Bilgisayar çağı, düşmanlıkların gerçekleştirilebileceği bir başka ortamı daha ortaya çıkarmıştır. Modern toplumların ve silahlı kuvvetlerinin bilgisayar sistemlerine olan bağımlılığı, bu tür sistemlere saldırı nesnelerini ya da bağlantılı bir nesneyi veya kişiyi hedef alabileceği bir seçim ortamı yaratmaktadır (Boothby, 2012: 586). Yapay zeka destekli teknolojilerin gelişmesi, bazı insan yeteneklerine sahip robotların üretilmeye ve gelişmesine bağlı olarak ortaya çıkan tartışmalar gündemde yerini almaktadır. Robotların ya da otonom silah sistemlerinin kendi kendine hayat bulması film senaryolarından ibarettir. Burada tek risk, bu sistemlerin düşman ya da devlet dışı aktörler (bilgisayar korsanları gibi) tarafından ele geçirilmesidir. Düşman, özerk bir silah sistemini kontrol altına almak ya da onu dostça kuvvetlere ya da sivil bir nüfusa karşı yönlendirmek için siber araçları kullanabilir. Ancak bu sistemleri geliştirenler de bu tehlike ve risklerin farkındadırlar. Örneğin, ABD bu konuda; yetkisiz katılımların veya sistemin yetkisiz kişilere kontrolünün kaptırılması sonucu olası riskleri ele alan ve yazılımı buna uygun tasarlayan politikalar uygulamaktadır (Schmit ve Thurnher, 2013: 242-243).

AI ilerledikçe, siber saldırı potansiyeli de artmaktadır. Gelişmiş makine öğrenmesi, derin öğrenme ve sinir ağları gibi teknikler, bilgisayarların kalıpları bulmalarını ve yorumlamalarını sağlar. Örneğin, makine öğrenmesi kolayca kötü niyetli aktör sosyal medyadaki davranışınızı takip eder, ardından kimlik avı tweetlerini veya e-postaları kişiselleştirebilir. Bir insan korsanı AI kadar bu işi bu kadar hızlı yapamayabilir. AI’nın kendisi iyi korunmuyorsa, yeni güvenlik açıklarına yol açar ve kötü niyetli aktörler örneğin, algoritmaların eğitim setlerine önyargılı veri enjekte

edebilecektir. Bulut teknolojisi ile birleştirilmiş ölçeklenebilir makine öğrenme teknikleri çok büyük miktarda veriyi analiz edebiliyor ve gerçek zamanlı tehdit tespit ve analizini güçlendirmektedir. AI yetenekleri siber saldırıların etkilendiği ve siber güvenlik istihbarat raporları sağladığı “sıcak noktaları” da hızla belirleyebilir. Ancak bu noktada da yine insana ihtiyaç duyulacaktır. Çünkü insanlar bağlamı özümsemek ve yaratıcı düşünmek konusunda daha iyidirler. Siber savaşlar basitçe savaşan iki bilgisayar grubu olmayacaktır. Ancak AI, her büyük organizasyonun siber güvenlik araç setinin önemli bir parçası haline gelecektir (Baccala vd., 2018: 14).

Siber güvenlik konusunda kuruluşlar geride duramazlar çünkü saldırganlar da AI’yı kullanacaklardır böylece savunucular da kullanmak zorunda kalacaklardır. Siber güvenlik alanı yapay zekanın kabul edilmesini hızlandırabilir. Siber güvenlik birçok kuruluşun AI ile ilk tecrübesi olabilecektir. Bir kuruluşta AI’nın varlığı ve verilere erişimi arttıkça, siber tehditlere karşı daha iyi savunma yapabilecektir. Hatta bazı kuruluşlar AI yeteneklerini sağlayacak şirket içi ve bulut tabanlı “tehdit gölleri” inşa etmektedirler (Baccala vd., 2018:15).

Yapay zeka gelişmelerinin kötü niyetli kullanımı belirli tehditleri de beraberinde getirmektedir. Cambridge raporuna (30-32) göre bunlar, dijital güvenlik tehditleri (dijital sistemlerin gizliliği ve bütünlüğünü tehlikeye sokacak tehditler), fiziksel güvenlik için tehditler (fiziksel dünyada meydana gelen saldırılar) ve politik güvenlik için tehditler (bir toplumun özgür ve üretken tartışmalara katılma yeteneklerinin tehdit edilmesi gibi) olmak üzere sıralanabilmektedir. Çalışmanın bu bölümünde öncelikle siber (dijital) güvenlik alanı üzerinde durulacak olup, yapay zeka gelişmelerinin bu alanda, siber güvenlik savunmalarında ve kötü niyetli saldırganlar üzerindeki etkilerinin ne olduğu ele alınacaktır. Yani yapay zeka siber güvenlik alanını hem savunma hem de saldırı olmak üzere iki yönden de etkilemektedir. Yapay zeka, kötü amaçlı yazılım tespiti gibi daha çok siber güvenliğin savunma tarafında yaygın olarak kullanılmakla birlikte bir çok kötü niyetli aktörün, başkalarının genellikle güvensiz sistemlerine saldırmak için de bu teknolojiyi kullanmaya çalıştıkları bilinmektedir.

Siber güvenlik, hem evde hem de çalışma ortamlarında insanları etkileyen birkaç alandan biridir. İnsanlar her zaman çevrimiçi olduklarını bilmelidirler, çünkü

bilgisayar korsanları, dikkatli olmayan bilgisayar kullanıcıları söz konusu olduğunda kimlikleri ya da finansal bilgileri çalmanın kolay olduğunu kanıtlamışlardır. İnternet ile etkileşim sonrasında mağduriyetlerin oluşması kolaylığı siber güvenlik konusunu büyük ölçüde kamuoyuna açık bir konu haline getirmiştir (Lidestri, 2018).

Siber savunma ve güvenlik, interneti kullanan herkesin karşılaştığı bir zorluktur. Örneğin, bunlar şirketler, küçük işletmeler, hastaneler, okullar, devlet kurumları ve bireyler olarak sayılabilir (Crawford, 2017: 5).

Bu konuda dijital güvenlik alanına da değinilmesi gerekmektedir. Yapay zeka daha gelişmiş hackleme otomasyonunda kullanılmaktadır ve hedef seçimini ve önceliklendirmeyi geliştirmek, tespitten kaçınmak ve hedefin davranışındaki değişikliklere yaratıcı bir şekilde cevap vermek için kullanılmaktadır. Yapay zeka hackleme araçları, hem tarihsel olarak mümkün olana hem de sonuçta insanlara kıyasla çok daha iyi performans gösterebilmektedir (Brundage vd., 2018: 25). Bu konuda sosyal mühendislik saldırılarının otomasyonu da söz konusudur. Örneğin, mağdurların çevrimiçi bilgileri kullanılarak kötü niyetli kişiler bu hesapları ele geçirebilmektedir. Yapay zeka ilerledikçe çeşitli sohbetlerle vs. insanlar üzerinde güven sağlanıp mağdurlar daha kolay ikna edilmiş olacaktır.

Yapay zeka, makinelerin daha karmaşık bir karar alma sürecini gerçekleştirmelerini sağlayan yeni bir teknoloji olarak daha yaygın hale gelmektedir. Yapay zekanın teknolojik gelişimi, siber güvenlik alanında, ağ profesyonellerinin kullanması gereken zorlu güvenlik araçlarını kullanma fırsatı sağlamıştır (Lidestri, 2018).

Yapay zekanın tehdit manzarası çok hızlı değişmektedir. Örneğin, ağ saldırıları verilerini sınıflandırmak için ve mevcut problemlere en iyi çözümleri bulmak için algoritmalar geliştirilmiş ve bir sistem oluşturulmuştur. Bu sistem, % 98'in üzerinde bir tespit oranıyla beş saldırı tipindeki verileri neredeyse gerçek zamanlı olarak tespit edip kategorize edebilmiştir (Crawford, 2017: 4). Bağımlılıklar ve ilişkili ağlar, planlanan saldırının orantılığını değerlendirebilmektedir.

Makine öğrenmesi yaklaşımları siber savunma için giderek daha fazla kullanılmaktadır ve bu, hedefin bilinen tehditlerden öğrenmek ve yeni tehditlere genelleştirmek veya denetlenmeyen öğrenme şeklinde bir anomali detektörünün normal

davranıştan şüpheli sapmalar konusunda uyardığı örneğin denetlenen öğrenme biçimini alabilmektedir (Brundage vd. 2018: 37). Son zamanlarda güvenlik uzmanları tehditleri anlamak ve tespit etmek için yapay zeka temelli savunmaları kullanmaktadırlar.

Yapay zeka siber güvenlik uzmanlarının tüm dünyadaki ağlarını ve altyapılarını savunmak için kullandıkları araçlarda sayısız ilerleme sağlama potansiyeline sahiptir. Potansiyel gelişmelere rağmen, ağ analistleri, bilgisayar korsanlarının bu teknolojiden yararlanarak saldırıları tespit etmekten kaçınmak amacıyla kendi ağlarına daha akıllı ve daha uyarlanabilir hale getirmenin bir yolunu bulmanın çok uzun sürmeyeceğini bilmektedirler. Yapay zekanın % 91 'inin bilgisayar korsanları tarafından şirketlere saldırı amaçlı kullanılacağı siber güvenlik uzmanları tarafından tespit edilmiştir (Lidestri, 2018: 1).

Yapay zekalar, geliştikçe siber düşmanlarla savaşacaktır. Nesnelerin interneti ile ilgili olarak alınması gereken temel bir varsayım, teknik olarak gelişmiş bir rakiple olan çatışmada, savaş nesnelerin internetinin ağır bir şekilde tartışmalı bir savaş alanı olacağı yönündedir. Düşman yazılımı siber ajanları (kötü amaçlı yazılımlar) ağımıza sızacak ya da akıllı nesnelere saldırabileceklerdir. Onlarla savaşmak için yapay siber avcılara, aktif siber savunma konusunda uzmanlaşmış ve akıllı, özerk mobil ajanlara ihtiyaç duyulacaktır (Kott, 2018, 3). Bu konu hakkında bir örnek verilecek olursa; bir zararlı yazılıma karşı önlem alınsa bile, yapay zeka teknikleriyle kodlanmış öyle yazılımlar var ki, bunlar tarama esnasında kendini saklayabilmekte, uyku halinde kalabilmekte ya da üzerinde bulunduğu sisteme zarar verici başka bir sisteme zarar verebilecek davranışlar gösterdiği ortaya konmuştur (Demirezen, 2019: 20).

Makine öğrenmesi, siber güvenlik uzmanlarının kendi özelliklerini öğrenmek için algoritmalar oluşturmalarına hizmet edecek ve en küçük sapmaları bile tespit edebilecektir (Lidestri, 2018: 2). Her bilgisayar üzerine kurulu olan şeyin ya da sistemlerin çalışmasına önemli ölçüde katkıda bulunmaktadır.

Makine öğrenimi kullanılırken tipik ağ davranışı tespit edilir ve buna göre ele alınır. Yapay zeka, ağ günlüğü dosyalarının hızlıca taramak için bilgisayarın kaynaklarını kullanabilir ve potansiyel tehditleri, bir insanın yapabileceğinden daha hızlı tespit edebilir. Bu da makineleri, tespit; insanları ise karar alma rolünde kalmalarını sağlayacaktır (Lidestri, 2018: 3).

Siber güvenlik ve yapay zeka konusunda önemli olan noktalar, kötü amaçlı yazılım türleri, siber savunma eksiklikleri ve siber saldırı sürecidir.

Günümüzde artık siber savaş, savaşların ve krizlerin ayrılmaz bir bölümü haline gelmiştir. Ukrayna devlet organizasyonunun maruz kaldığı siber saldırılar ya da Kırım krizinde NATO'nun uğradığı saldırılar buna örnek olarak verilebilmektedir. Siber savaş konusunda genellikle “Siber Savunma” kısmına odaklanılmaktadır. Ancak düşmanın bu siber ortamı kötü yönde kullanmasına mani olmak için siber saldırılar da gerçekleştirilmelidir (Karaağaç, 2016, 27).

Siber saldırıların büyük kısmı karmaşık sayılmaz ve bir ihlal meydana geldiğinde müdahale edilebilmektedir. Burada asıl problem, tipik güvenlik uygulamalarından geçen temel saldırıların sıklığıdır (Lidestri, 9, Lomas, 2016). Ayrıca siber alanda istihbarat toplayarak, henüz saldırılar gerçekleşmeden önce bu saldırının teşhisi mümkün olabilmektedir (Demirezen, 2019: 21). Yapılan anketlere göre, yapay zekanın gelecek yıllarda saldırılar için kullanılacağı görüşü hakimdir. Çalışmalar, kuruluşların % 53'ünün güvenlik pozisyonunu doldurmalarının üç ile altı yıl sürdüğünü ve kuruluşların % 10'unun mevcut tüm açıklıklarını dolduramadığını göstermiştir (Lidestri, 9, Shah, 2016).

Binden fazla çalışanı olan şirketler ağlarını korumak için yılda zaten yaklaşık 15 milyon dolar harcamaktadır (Lidestri, 10, Korolov, 2015). Yeterli bir iş gücü olmadan, güvenlik olaylarının otomasyonu, siber saldırılara karşı etkili koruma gerektiren kuruluşlar için kritik hale gelmiştir. Şirketler, bir satıcının kendi yazılımının otomatik olarak yamalanmasından tehdit algılamasına, olaya müdahale ve danışmanlık hizmetlerine kadar geniş bir yelpazede siber güvenlik çözümleri sunmaktadırlar. Ağ ve uç nokta güvenliği ürünleri, tehditleri önlemeyi, algılamayı ve bunlara yanıt vermeyi amaçlar ve en önemli savunma alanları arasında uç nokta güvenliği, iç ağ güvenliği ve bulut güvenliği sayılmaktadır (Brundage vd. 2018: 37). Yapay zeka gelişmeleri otomasyon güvenlik ekiplerinin kullanabileceği bazı avantajlar sağlamaktadır. Örneğin, Carnegie Mellon'daki araştırmacılar bazı web sunucusu özelliklerini derlemiş ve gelecekteki saldırıların % 66' sını başarılı bir şekilde tahmin edebilmişlerdir (Lidestri, 2018: 10).

Akıllı nesneler yani insan savaşçılarıyla birlikte çalışanlar, gelecekte savaş alanında her yerde bulunabileceklerdir. Görünüşleri, rolleri ve işlevleri farklılıklar içerecek biçimde çok yüksek olacak ve bunlar için gerekli yapay zeka sağlanacaktır. Ancak bunlar için bugünün yapay zeka ve makine öğrenme teknikleri daha da geliştirilmelidir. Böylece siber savaş çok daha büyük bir öneme sahip olacak ve yapay zeka siber rakiplerle savaşmak zorunda kalacaktır. Büyük gelişmeler öğrenme ve akıl yürütme gibi alanlarda çok daha fazla gerekli olacaktır (Kott, 2018: 6).

Bir kişinin bir ağa karşı kötü niyetli bir harekette bulunmasına sebep olabilecek olaylarla ilgili ek bilgiler, erken teşhis koymada çok çok önemli olacaktır. Verilerin daha hızlı korelasyonu sayesinde tehditleri tespit etmek daha kolay hale gelecek ve hata oranları azalacaktır (Lidestri, 2018: 11).

Araştırmalara göre, güvenlik uzmanlarının sadece % 30' unun yapay zeka ve güvenlik alanında nasıl kullanılabileceği hakkında yeterli bilgiye sahip olduğunu göstermektedir (Lidestri, 11, Olsik, 2018). Siber savunma için makine öğrenmesinin kullanımı, dikkat eksikliği ve diğer zayıflıklar nedeniyle yapay zeka saldırı yüzeyini genişletebilecektir. Ayrıca siber güvenlik uzmanlarının yapmış oldukları anketlere göre yapay zeka temelli savunma sistemlerine güven oldukça azdır (Brundage vd., 2018: 37). Yapay zeka için programlama çok karmaşıktır ve sistemin oluşturduğu gibi güvenilir bir şekilde çalışmasını sağlamak gerçekten çok zordur. 1956'da bir araştırma disiplini haline gelen yapay zeka, araştırmacıların orijinal olarak düşündüklerinden çok daha gelişmiş ve karmaşık olan bir istihbarat sistemine dönüşmüştür. IBM Watson, şu anda siber güvenlik dahil olmak üzere çeşitli amaçlar için geliştirilen ve kullanılan en güçlü yapay zeka sistemlerinden biri olarak karşımıza çıkmaktadır. Watson IBM Security tarafından siber güvenlik dili konusunda eğitilmiştir ve kalıp aramak için kullandığı binlerce metni işleyebilmektedir (Crawford, 2017: 3).

Günümüzde siber güvenlik, büyük ölçüde emek kısıtlı olduğu için yapay zekanın gelişmesiyle otomasyon olanakları olgunlaşmıştır. Ancak AI'nın siber güvenlik için artan kullanımı yeni riskler ortaya çıkarmaktadır. Çeşitli aktörler, hedefli saldırılar ve devletler dahil olmak üzere, siber operasyonları giderek daha karmaşık bir hal almıştır ve karmaşık bir siber suç dünyası bulunmaktadır (Brundage vd., 2018: 31).

Ancak yapay zekanın ve makine öğrenmesinin gelişmesiyle geleneksel siber savunma teknikleri ve istihbarat sistemleri de değişime uğramıştır. Bu geleneksel sistemler içinde güvenlik duvarları, algoritmalar, saldırı tespit sistemleri ve izinsiz girişi önleme sistemleri gibi uygulamalar sayılabilir. Örneğin burada algoritmalar anormal durumları anlayabilmek için kullanılmaktadır. Güvenlik duvarları da kullanıcıların kimliklerini doğrulamaları yoluyla istenmeyen davetsiz misafirlerin girebilmesini engellemeyi sağlamaktadır. İzinsiz girişi önleme sistemleri ise hem saldırıları tespit eden hem de bunları önleyebilen cihazlardır (Crawford, 2017: 5-9). Siber savunmada yapay zeka uygulamaları ise sinir ağları, akıllı ajanlar, bilişsel görüşler, derin öğrenme gibi yöntemler sıralanabilmektedir. Sinir ağları, sınıflandırma, tanıma, iyi öğrenme şekli ya da saldırılara verilen cevapların seçimi için uygun bir yoldur. Akıllı ajanlar için bugün kişisel asistanlık için kullanılan Siri, Aleksa gibi örnekler verilebilir. Bunların makine öğrenmesi sayesinde; planlama yeteneği, mobilite ve yansıtma yetenekleri bulunabilmektedir. Bilişsel bilgi ise; yine makine öğrenmesi sayesinde, internetten çeşitli benzer olaylarla ilgili veriler toplar ve bir kişinin bazı siber türleri nasıl araştırdığını, izlediğini ve sorunları nasıl giderdiğini taklit ederek saldırıları önler (Crawford, 2017: 9-12). Siri, birçok kez o an telefona uzanamayan insanlar için ambulans çağırabilmiş ve insanların hayatlarının kurtarılmasına yardımcı olmuştur (Say, 2019: 126).

Bir çok hükümet yapay zeka ve siber güvenliğin birleşimi ile yakından ilgilenmekte ve aynı zamanda yapay zeka sistemlerinin yeteneklerini genişletmek için temel araştırmalara yatırımlar yapmaktadırlar. Örneğin, 2016 yılında, DARPA, insan araştırmaca ekiplerin rekabet ettiği Siber Büyük Mücadele yarışmasına ev sahipliği yapmıştır (Brundage vd., 2018: 32).

Uzaktan saldırı teknolojilerinin yasal olarak tartışılması genellikle “sorumluluk” konusunda olmaktadır. Bir şeyler ters gittiğinde kim sorumlu olacak? Siber saldırılar söz konusu olduğunda, kimin hangi saldırıyı gerçekleştirdiğini ve ne amaçla bunu yaptığını kesin olarak belirlemek çok zordur. Saldırının başlatıldığı bilgisayar tespit edilebilir fakat burada siber silahı oluşturan kişinin adı, siber silahı yoluna gönderen potansiyel olarak farklı bir kişinin adı ve bu kişilerin hangi devlet, grup ya da kişi adına çalıştığı bilinemeyebilir. Bu zorluklar belirli siber olaylar söz konusu olduğunda sorumluluğu gidermeyi imkansız hale getirebilecektir (Bootby, 2012:

589). Ancak otonom araç sistem arızasından kaynaklanan bir saldırı gerçekleştirmiş ise bu durumda o sistemi tasarlayan kontrolör sorumlu olacaktır.

Yukarıda ele alınan risklere karşı Cambridge Raporu'nda bu tehditlere karşı 4 temel öneri ve tavsiye ortaya konulmuştur. Bunlardan birincisi, politika yapımcılarının yakından işbirliği yapmalarının gerekliliğidir. Bu işbirliği AI'nın zararlı kullanımlarını önleme de önemli olacak ve aynı zamanda teknik uzmanlarla da işbirliği yapılmasını sağlayacaktır. Politika yapımcıları sorumluluklarının farkında olmalıdırlar. İkinci tavsiye ise, yapay zekanın çift kullanımının farkında olunmasıyla ilgilidir. Yani, bu alandaki mühendis ve araştırmacılar bu teknolojinin faydalı kullanımlarını teşvik etmeli, zararlı kullanımlarını ise engellemek için önlemler almalıdırlar. Bu tavsiyelerden üçüncüsü, bilgisayar güvenliği gibi çifte kullanım endişelerini gidermek için daha olgun yöntemlere sahip araştırma alanları yapay zeka durumlarında uygulanabilmelidir. Verilen son tavsiye ise, bu zorluklarla ilgili tartışmalarda yer alan tüm paydaşların kapsamı aktif olarak araştırılmalıdır. Yani ilgili paydaşlar konuya dahil edilmeli yani sivil toplum, güvenlik uzmanları, siber güvenlik araştırmacıları, etik uzmanlar gibi (Brundage vd., 2018: 51- 53).

2.4.4. Yapay Zeka ve İstihbarat

İstihbarat geçmişten günümüze irdelendiğinde ilkel toplumlardan tarım toplumlarına, daha sonra sanayi toplumuna, son olarak da bilgi toplumuna geçişlerde her zaman değişim ve gelişim göstermiştir. Bu gelişimi gerçekleştirirken de içeriğine iletişim, sosyal medya, bilim ve teknoloji, coğrafya, kültür gibi çeşitli alanları da almaya başlamıştır. İstihbarat sürecinin, kişiler, yabancı devletler ve uluslararası faktörler arasında çeşitli şekillerde geliştiğini söylemek yanlış olmayacaktır (Seren, 2019: 11).

Teknoloji ve yapay zeka gelişmelerinden en fazla yararlanan alanlardan biri de istihbarattır. "Gizlilik" ilkesi bilindiği üzere istihbaratın en temel birimi olarak karşımıza çıkmaktadır. Burada önemli olan istihbarat ve teknoloji ilişkisinde, bilginin dışarıya istenmeyen bir biçimde aktarılmamasıdır (Çıtak, 2019: 34). Teknolojinin ne kadar güçlü olduğu da bu noktada önem kazanmaktadır.

Teknoloji ülkeler arasında genellikle savunma ve güvenlik alanlarında daha çok kullanıldığından aslında bir rekabet ortamı yaratmaktadır ki buna da “teknoloji savaşı” denmektedir (Çıtak, 2019: 34). Savunma ve güvenlik denildiğinde ise akla ilk gelen de siber alandır. Siber alan ülkelerin varlıklarını koruyabilmeleri açısından önem arz eden bir konudur. Siber silahlar kullanılarak aslında çok da fazla farkına varılmayan “siber savaşlar” meydana gelmektedir (Demirezen, 2019: 20).

İstihbaratta kullanılan haberleşme, ulaşım gibi konularda her zaman teknolojiiden yararlanılmıştır. Ancak ikinci dünya savaşı sırasında askeri savunma alanında birçok yenilik ve değişikliğin görülmesiyle birlikte istihbaratın teknolojik yönü de değişikliğe uğramıştır. Örneğin, ikinci dünya savaşı sonrasında yaşanan soğuk savaşta istihbarat teknolojisi en önemli dış politika aracı olarak kullanılmıştır. Bu dönemle birlikte sinyal, işaret, ölçüm konularına önem verilmiş ve bu amaçla casus uçaklar, gemiler, gelişmiş bilgisayarlar, dinleme cihazları kullanılmaya başlanmıştır (Çıtak, 2019: 35). Bu takip eden süreçte günümüze gelindiğinde ise çok büyük bir istihbarat teknolojisi oluştuğunu söylemek yerinde olacaktır. Buna bağlı olarak da ülkelerin istihbarat teknolojiine yaptıkları yatırım da gün geçtikçe daha da artmaktadır. Dış istihbarat konularında bilgi edinme ve bunları toplarken daha çok yararlanılanlar teknik kaynaklar olarak karşımıza çıkmaktadır (Seren, 2019: 16). Yapay zeka teknolojilerinin gelişmesine paralel olarak artık bulunduğumuz dönemde, istihbarat sağlamada geleneksel yöntemlerin yerini; bilimsel algoritmalar, büyük veri analitiği gibi yöntemler almıştır (Demirezen, 2019: 19).

İstihbarat ve teknolojisi ilişkisini güçlendiren etkenlerin başında sinyal istihbaratının daha önemli hale gelmesi ve siber güvenlik alanındaki gelişmelerin çeşitlenmesi ve buna bağlı olarak teknoloji destekli silahların artması gelmektedir (Çıtak, 2019: 35).

Devletler istihbarat teknolojisi konusunda her ne kadar rekabet halinde olsalar da aynı zamanda, bu alanda işbirliği ve yardımlaşma da söz konusudur. Ancak bu genellikle ortak düşmana karşı birlikte çalışma ve teknolojiyi paylaşma olarak ortaya çıkmaktadır.

2.4.4.1. Askeri İstihbarat

İlk bölümde de çokça üzerinde durulduğu üzere bankacılıktan, savunma ve güvenlik politikalarına, siyasetten ekonomiye kadar yapay zekanın bir çok alanı etkilediği ve gelecekte tüm bunların daha da yaygın hale gelip etkisinin çok daha fazla olacağı tahmin edilmektedir. Şimdi etkilediği alanlara istihbaratı da eklemek elbette ki yanlış olmayacaktır. Yapay zekanın faydalandığı en önemli özellikleri algılama, tanıma, tahmin ve tespit edebilme, hedeflere odaklanabilme, öğrenebilme ve problem çözme gibi alanlardır. Bu alanlar göz önünde bulundurulduğunda, bunların birçok alan gibi istihbarat sistemlerinde de kullanılması mümkün ve önemlidir. Burada da devletlerin bu teknolojiye sahip olmaları ya da olmamaları kendi çıkarları ve varlıklarını korumaları açısından önem kazanmaktadır.

Günümüzde istihbarat örgütleri, yapay zeka sayesinde istihbarat temelli bir çok işi artık insanların yerine belirli sistemlerin ve makinelerin yapabileceğini öngörmekte ve bu yüzden casusluk amaçlı yapay zekaları devreye sokmaya başlamışlardır. Saha operasyonlarını planlamaktan başarıları değerlendirmeye ve tehditleri algılamaya kadar bir çok işi yapay zeka destekli teknolojik sistemlerin yapması beklenmektedir (Çıtak, 2019: 36). Tüm bunlar düşünüldüğünde ise, istihbarat, savunma ve güvenlik gibi alanlarda başarılı olabilmek için, yapay zekayı teknolojilerine uyarlayabilmek ve bu sistemleri kullanabilmek tüm devletler için bugün büyük bir önem arz etmektedir. Bu amaçla küresel düzeyde Türkiye'nin de dahil olduğu devletlerin bu alanda çalışmaları mevcuttur.

Askeri istihbarat denilince akla bir devletin askeri birliklerinin komuta ve kontrolü, savunma sanayi, taktik ve stratejileri gibi konular gelmektedir. Yani askeri istihbarat hareket alanındaki belirsizliklerin giderilmesinde kontrolü sağlamaya yarayan istihbarat türüdür (Özer, 2019: 29).

Askeri istihbaratın kapsamına değinilecek olursa bunu şu şekilde sıralamak mümkündür (Özer, 2019: 29): planlama ve yönlendirme – toplama – işleme - analiz ve üretim – dağıtım.

Bu aşamaların tümünde teknoloji ve yapay zekadan yararlanılmaktadır ve bu son dönemlerde gözle görülür bir şekilde artmaktadır.

Askeri istihbaratta kullanılan toplama araçları insan istihbaratı, sinyal istihbaratı, görüntü istihbaratı ve açık kaynak istihbaratı olarak karşımıza çıkmaktadır. İnsan istihbaratı çok eski zamanlardan beri kullanılmasına rağmen son dönemlerde robotların bu alanda daha başarılı olmalarından kaynaklı olarak insanların yerini yavaş yavaş yapay zeka destekli robotlar almaya başlamıştır. Çünkü insanların duyguları karar alımlarında zaman zaman hatalara yol açabilmektedir. Sinyal istihbaratı ise elektronik sistemlerden yayılan sinyallerin tespit edilmesiyle ilgili bir durumdur. Görüntü istihbaratı bilindiği üzere insansız ya da insanlı hava araçları ile ya da uydulardan elde edilen bilgilerdir (Özer, 2019: 31-32). Açık kaynak istihbaratına sosyal medya içerisinde değinilecek olup bu alan sosyal medyada paylaşılan bilgilerden elde edilen tespitleri içermektedir.

İstihbaratta teknolojileri genelde 4 ana başlığa dayanmaktadır (Berkowitz, 2008): Veri toplamaya yarayan sensörler. Bunlar kimyasal, nükleer, elektronik ya da coğrafi olabilir.

- Verileri veya zekayı işleyen, düzenleyen ağlar ya da yazılımlar
- Sensörleri taşıyan robotik ya da insanlı gemiler, uçaklar veya uydular.
- Gizli iletişimleri sağlamada yani casusluk için işe yarayan gizli küçük kameralar vs.

Yukarıda da görüldüğü üzere istihbarat teknolojisinde yararlanılan kaynakların çoğu yapay zeka gerektiren sistemlerdir. Bu noktada eskiye göre yeni bir anlayış sayılabilecek olan yapay zeka istihbaratından bahsetmek yanlış olmayacaktır.

2.4.4.2. Sosyal Medya İstihbaratı (Açık Kaynak İstihbaratı)

İstihbarat'ı genel olarak siyasi, askeri, ekonomik, coğrafi, sosyal, ulaşım ve iletişim, bilimsel ve teknik ve son olarak siber istihbarat olarak sınıflandırmak mümkündür. Yapay zeka ve teknolojik gelişmelerle birlikte daha önceleri iletişim ve siber istihbarat kapsamında ele alınan “Sosyal Medya İstihbaratı” (Social Media Intelligence SOMINT) artık ayrı bir başlık olarak değerlendirilmektedir (Seren, 2019: 13).

İnsanların sosyal medya üzerinden yapmış oldukları paylaşımlardan yola çıkarak, bilinçli ya da farkında olmadan girilen bilgilerden yararlanarak askeri

istihbaratta kullanılan Açık Kaynak İstihbaratı (Open Source Intelligence- OSINT) da sosyal medya istihbaratı ile ilişkili bir alan olarak karşımıza çıkmaktadır (Erkan, 2019: 22). Bu konuda bir örnek verilecek olursa; CITEAM isimli istihbarat grubu TSK içerisinde bulunan bazı personellerin sosyal medyada paylaştığı fotoğraflardan bilgi elde ederek Irak'taki TSK birliklerinin yerini öğrenebilmiştir. Bu CITEAM adı verilen grup gönüllü ya da istihbarat servisleri gibi çalışan topluluklardan biridir (Erkan, 2019: 24). Yani şu an yapay zeka destekli istihbarat teknolojileri ile sosyal medyada paylaşılan bir fotoğraftan konum bilgisi elde edilebilmektedir.

Bu alanda bir diğer örnek ise, ABD ordusu 2015 yılında DEAŞ üyesi bir teröristin paylaşmış olduğu fotoğraftan konumunu tespit edip çok kısa bir sürede o noktaya saldırı gerçekleştirmiştir (Erkan, 2019: 25).

İnternet kullanımı ve siber alanın büyüklüğü 2000'li yıllardan başlayarak sürekli artma eğilimindedir. Örneğin, Twitter uygulamasının 2018'de aktif kullanıcı sayısı 326 milyona ulaşmış ve bu kullanıcıların attıkları mesaj sayısı da günlük 500 milyon olarak belirlenmiştir (Erkan, 2019: 23).

2.5. YAPAY ZEKANIN SAVUNMA VE SAVAŞ ALANINA ETKİSİ

Yapay zeka destekli bilgi teknolojileri geliştikçe devletler de yönlerini bu teknolojiye çevirmeye başlamış ve buna bağlı yenilikçi yöntemler izlemeye başlamışlardır. Ülkelerin yapay zekayı uygulayabildiği ya da güvenlikleri için uygulaması gereken en önemli alanlardan birisi de savunma alanıdır.

Dünyada yakın zamanda yapılan araştırmalara göre, tüm dünyada sadece bir günde üretilen veri 2,5 kentilyon bayta ulaşmaktadır (Marr, 2018). Dünyada internete bağlanabilen araçların kullanımının artmasıyla veri miktarı da artmaya başlayacaktır. Böylece verinin insanlar tarafından işlenmesi çok zorlaşmış ve veri madenciliği ya da büyük veri gibi uygulama alanları ortaya çıkmıştır.

Yapay zeka, makine öğrenmesi ve derin öğrenme birbirini kapsayan ve aynı amaca hizmet eden teknolojilerdir. Yapay zeka diğer ikisini kapsamakla beraber, makine öğrenmesini kullansa da kullanmasa da, bir tespit ve karar işlemini gerçekleştiren teknolojileri içine almaktadır. Yani kısacası yapay zeka, makine öğrenmesi ya da derin öğrenme olmadan da çalışabilen bir sistemdir.

Makine öğrenmesini ise bilgisayarların programlanmasına ve bilişsel işlemler yapmasına izin veren algoritmalar olarak düşünmek gerekmektedir. Makine öğrenmesini yapay zeka algoritmalarından ayıran temel faktör algoritmanın her şeyi veriden öğrenmesidir. Makine öğrenmesine örnek verilecek olursa bunlar, Facebook, Twitter, Amazon, Swarm, Siri, Google Now gibi uygulamaları sıralamak mümkündür.

Derin öğrenme algoritması ise diğer iki sistemin alt dalıdır ve öğrenmeyi sağlayacak olan verilerin makine öğrenmesi algoritması içinde katman olarak ele alınan verinin özel bir tür temsili ile işlev görmektedir. Yani kısaca, makine öğrenmesinde, öğretme sırasında eldeki verilerin makineye tanıtılması gerekirken; derin öğrenmede ise, makine pek çok olan verileri kendisi işleyerek nasıl öğreneceğini de kendisi öğrenmektedir.

Yapay zeka teknolojileri, devletleri tıp alanından sanayiye kadar her alanda etkileyecektir. Bunların yanında etkileyeceği bir diğer önemli alan da savaş teknolojisidir ve daha düşük maliyetli özerk araçlar kontrol amaçlı olarak kullanılacaktır (Vincent, 2017).

Askeri amaçlarla kullanılan ve kendi kendine kararlar alabilen makinelerin ilk örneği füze sistemleri ve güdümlü bombalar olarak karşımıza çıkmaktadır. Bunun yanında uzun menzilli, hava, deniz ya da kara sahalarından atılabilen güdümlü füzeler, düşman savunmasını yok etmek için kullanılmaktadır (STM ThinkTech Teknolojik Düşünme Merkezi, 2019: 18).

Robot teknolojisi de aslında askeri amaçlarla oluşturulmuş bir teknolojidir. Bir savaş ortamında arama, kurtarma vb eylemlerde yapay zekanın kullanılması kaçınılmaz bir hale gelmiştir. Yapay zeka ve makine öğrenmesi sayesinde, otonom olarak kararlar verebilen makineler oluşturmak mümkün olacaktır. Otonom araçlar deyince ilk akla gelen insansız hava araçlarıdır (İHA). Bazı ülkeler bunları drone olarak da adlandırmaktadır. Bu araçlar savaş ortamında gözetleme, keşif ve tespit amaçlı olarak kullanılmaktadırlar. Farklı sensör sistemlerinin topladığı verilerle ortak bir görünüm elde edilmektedir ve bunun sonucunda yapay zeka destekli komuta kontrol yazılımları geliştirilmektedir (STM Think Tech Teknolojik Düşünme Merkezi, 2019: 19). Robotik sistemlerin insanlara nazaran daha az hata yapma riskinin bulunması gelecekte daha fazla geliştirilmelerine ve kullanılmalarına neden olacaktır.

2000’li yıllardan itibaren insansız hava araçlarının hem sayısı hem de nitelikleri artmaya başlamıştır ve savaş ortamlarındaki etkinlikleri de hızla artmaktadır. Bunların kullanımı sinyal tespiti, darbe tehlikesi, düşmanın savunmasını yok etme etkinliklerini kapsamaktadır (Karaağaç, 2016: 10). Ayrıca son zamanlarda savunma sanayi şirketleri savunma ve savaş ortamlarında kullanılmak üzere insanlı veya insansız hava araçları için minyatür kameralar üretme yoluna gitmektedirler. Gizlilik ve güvenlik açısından da bunların milli olması önem arz etmektedir.

Günümüzde yapay zekaya sahip silahlar, insana ihtiyaç duymadan hedeflenen bölgede tespit işlemi yapabilmekte olup, hedefin imhası için en uygun yolu da kendileri çizebilmektedirler.

1900’lü yıllarda ilk kez ABD’de kullanılmasının ardından, İHA sistemlerinin devletlerin askeri kuvvetlerine dahil olmaya başladığı yıllar 1980’li yıllara tekabül etmektedir. Bu tarihten sonra, Irak, Filistin, Bosna-Hersek, Pakistan, Libya, Suriye gibi ülkeler de bu araçları savaş ortamlarında kullanmaya başlamışlardır (Karaağaç, 2016: 16).

Yapay zeka teknolojisinin gelişmesine paralel olarak İHA sistemleri de gelişmeye başlamış ve devletlerin bu yöndeki yatırımları da hızla artmaya başlamıştır. Örneğin 2015 yılında, 60 ülkede, 2.115 tane çeşitli tiplerdeki İHA’lar 637 şirket tarafından geliştirilmeye başlanmıştır (a.g.e.: 17). Bu araçlar terörle mücadele kapsamında da kullanılmaktadır.

Savaşlarda kullanılan bir diğer yapay zeka destekli teknoloji de, robotik bir hareket sistemi olan “ harici iskelet” (Exoskeleton) lerdir. Bu sistemlerin amacı ise, askerin silah, teçhizat gibi eşyaları zorlanmadan taşımalarını mümkün kılmaktır ve bunlar ön saflarda çatışan askerlerin gücünü artırmak için kullanılmaktadır (STM Think Tech Teknolojik Düşünme Merkezi, 2019: 19).

Bugün yapay zekanın gelişmesi literatüre savaş alanında da bir çok kavram girmesine neden olmuştur. Bunlardan en önemlisi “savaş nesnelerinin interneti” (İnternet of Battle Things) olarak karşımıza çıkmaktadır. Yukarıda da açıklandığı üzere bu kavram bir yerde bir sensörün veya bir işlemcinin, bilgi işlem, algılama ya da iletişimi gerçekleştirmesi anlamına gelmektedir (Flaherty, 2017). Nesnelerin interneti terimi 1999 yılında İngiliz teknoloji öncüsü Kevin Ashton tarafından gerçek dünyadaki

nesnelerin sensörler aracılığı ile internete bağlanabileceği bir sistemi adlandırmak için kullanılmıştır. Günümüzde ise daha geniş anlamlar edinerek internet bağlantısının ve bilgi işlem kapasitesinin çeşitli nesnelere, cihazlara ya da sensörlere kadar yayıldığı sistemi tanımlamak için kullanılan popüler bir terim haline gelmiştir (Rose, 2015: 12). Bunun yanında “nesnelerin muharebesi”, “akıllı makineler” gibi kavramlar da ortaya çıkmıştır. Nesnelerin interneti kavramı ele alınacak olursa, bu kavram ilk kez 1970’li yıllarda askeri amaçlarla ortaya çıkmış olmasına karşın günümüzde daha çok sivil hayatta kullanılan bir kavramdır. Örneğin, ABD Savunma Bakanlığı İleri Araştırma Projeleri Kurumu (DARPA), 1970’lerin sonlarında, savaş ortamında belirli tespitleri yapmak amacıyla bazı sensörler geliştirmiştir. Bu gibi sistemler günlük yaşantımızda yankı bularak sivil hayatta da kullanılan bir sistem haline gelmiştir (STM Think Tech Teknolojik Düşünme Merkezi, 2019: 19). Bu konuyla ilgili bir örnek daha verilecek olursa; ABD 1989 yılında yaptığı bir tatbikatta lojistik sistemlerde bir verimsizlik tespit etmiş ve bununla ilgili bir YZ geliştirmiştir. DART (Dinamik Analiz ve Yeniden Planlama Aracı) adını verdikleri bu sistem sayesinde personel ve araç-gereç nakil planlarını çok kısa zamanda halletmişler ve sonuç olarak sağladıkları tasarrufla YZ alanında kâra geçmişlerdir (Say, 2019: 90).

Günümüzde askeri operasyonlar yapay zeka teknolojileri ile çok daha karmaşık ve öngörülemez hale gelmektedir. Rakiplerin bu teknolojik nitelikleri geliştikçe, baskı altındaki ortamlarda değerlendirmek ya da harekete geçmek için askeri komutanlara daha fazla baskı uygulanmaktadır (Wassell, 2018). Yani kısacası bugün de başlamış olan veri savaşları gelecekte çok daha fazla anlam kazanacaktır. İnsanların bir ücret ödmeden şirketlere çok büyük miktarda veri yüklemesi sonucunda yapay öğrenme sistemlerinin hızla yükselişe geçmesine yol açmıştır.

ABD Ordusu Araştırma Laboratuvarından Alexander Kott’un hazırladığı “Challenges and Characteristics of Intelligent Autonomy for Internet of Battle Things in Highly Adversarial Environments” adlı rapora göre “Savaş Nesnelerinin İnterneti” şu şekilde tanımlanmaktadır: nesnelerin interneti kavramının hızla ortaya çıkması makine zekası ve ağ iletişimi kavramlarının mantığıyla ilerlemektedir. Nesneler daha akıllı olduklarında ve birbirleriyle iletişim halinde olduklarında daha etkilidirler. Aynı mantık askeri alanda da vukuu bulmakta ve savaşlarda kullanılan nesnelere uygulanmaktadır. İnsan savaşçılara daha çok ve iyi hizmet edebilmeleri için kendi aralarındaki eylemlerini

kordine edebilmeleri gerekmektedir. Buradan hareketle savaş nesnelerinin internetinin 20-30 yıl sonra çok çok önemli hale geleceğini söylemek yanlış olmayacaktır (STM Think Tech Teknolojik Düşünme Merkezi, 2019: 20). Gelecekte savaş ortamlarının akıllı nesneler ile dolu olacağı tahmin edilmektedir. 2001 yılında bütün dünyayı etkileyen 11 Eylül saldırısından sonra savaş biçimlerinin değiştiğini söylemek mümkündür. Bu tarihten sonra ABD ordusunda on binlerce robot yer almaya başlamıştır. Aynı zamanda insansız hava araçları, Ortadoğu'daki operasyonlarda görev almış ve olağanlaşmıştır. Yine bu araçlar Irak ve Afganistan'da yollara döşenmiş olan bombaların imha edilmesinde önemli rol oynamışlardır (STM Think Tech Teknolojik Düşünme Merkezi, 2019: 20).

Yine Irak'ta 2004'ün sonlarında yaklaşık 150 olan askeri yer robotlarının sayısı, 2009 yılında 12.000 civarına ulaşmıştır. İnsansız botların bir keşif aracı olarak kullanılmasına, 1985'de Titanic enkazının bulunmasında yararlanılması örneği verilebilir (Melendez, 2017).

Savaş nesnelerin interneti (IoT) cihazlarının savaş ortamlarında pek çok avantajı olacağı düşünülmektedir. Bunlar arasında otomatik güvenlik taraması, sensörler sayesinde güvenlik kamerası ağı sayılabilmektedir. Bu sayede insan gücüne olan ihtiyaç azalacak ve güvenlik riskleri de azaltılmaya çalışılacaktır (Wassell, 2018).

Aynı zamanda dron teknolojisinin gelişmesiyle, insansız uçak geliştiricilerinin düşman uçaklarından gelen saldırıları geri itebilecek veya kaçabilecek dronların tasarlandığı yeni bir tür silah ırkı ortaya çıkabilecektir (Melendez, 2017). Bunların getireceği en önemli sonuçlardan biri de bu teknolojilerin devletler arasında güç eşitsizliklerini artıracakı konusudur.

Savaşta hedefleri ortadan kaldırmak için kullanılan askeri stilde uçaklar halihazırda yaygın ve günümüze birçok devlet tarafından geliştirilmektedir. Gelecekte ise geliştirilecek olan dronların, hedeflere suikast yapmak için uygun olacağı söylenebilir. Bunlar, bir hedef tespit edildikten sonra patlamak üzere yapılan bir temizlik robotu şeklini alabilir ve bir böcekten daha büyük olmamasına rağmen, öldürücü bir maddeyi hedefe enjekte edebilecek güçte olabilecektir (Font ve Reaulx, 2018: 4).

Tüm bu gelişmelere karşın, Elon Musk ve yapay zeka liderleri, silahların nasıl geliştirildiğine yönelik olarak yeni düzenlemeler yapıp uygulanması için Birleşmiş Milletlere bir dilekçe göndermiştir. Aynı zamanda bu teknolojilerin barut ve nükleer silahlardan sonra üçüncü bir devrim olarak savaş ortamlarında yer alacağını da dile getirmişlerdir (Vincent, 2017). Kısacası bu dilekçe ile katil robotlar olarak bilinen özerk silahların yasaklanmasını istemişlerdir. Ancak ABD, Çin, Rusya ve İsrail bu bahsedilen özerk silah sistemlerini hızla geliştirmeye çalışmakta ve bu yönde yatırımlarını arttırmaktadırlar. Yani böyle bir yarışın olduğu ortamda hiçbir ülke kendini riske atmamak adına bu yarıştan vazgeçmeyecek gibi görünüyor. Bir taraftan da askeri alanda tamamen özerk silahların kullanılmaması, yani insanların kontrolünden çıkmaması yönünde temkinli davranmaktadırlar. Bu anlamda, en az 19 ülke ve İnsan Hakları İzleme Örgütü dahil, bazı uluslar arası kuruluşlar, kör lazer silahları ve mayınlar üzerindeki mevcut kısıtlamalara benzer şekilde, özerk ve ölümcül robotların yasaklanmasını istemiştir (Melendez, 2018).

Yapay zeka teknolojilerinin askeri yani savaş ortamlarında kullanılmalarında bazı durumlar ortaya çıkmakta ve hukuksal açıdan bunlar tartışılmaktadır. Örneğin insan ve makine arasında 3 ana durum ile karşılaşmak mümkündür. Bunlar; insanın içinde bulunduğu durumlar, insanın dışarıdan gözlemci olduğu durumlar, son olarak ise tamamen insansız olan araçlardır (Özer, 2019: 35).

Otonom sistemler karmaşık bilgileri çok hızlı bir şekilde algılayabilmekte ve işleyebilmektedir. Hem karar verme hem de görevleri daha hızlı ve kesin hale getirebilir, ayrıca insan uçaklarının yerini aldıkça can kayıplarını azaltarak hayat kurtarabilirler. Ancak insanlardan farklı olarak robotların kendilerini koruma ihtiyacı gerekmeyecek, tehlikeli görevleri üstlenebilecek ve özverili bir şekilde davranabilecektir. Yalnız burada karşımıza iki farklı durum çıkmaktadır. Bu sistemlerin hisleri, duyguları, korku ya da endişelerinin olmaması olumsuz sonuçlar da doğurabilmektedir. İnsani duygular ve hassas olunması gereken durumlarda bazı yazılımsal hatalar söz konusu olduğunda, bu otonom sistemler daha fazla insanın hayatını kaybetmesine de neden olabilmektedir (Petman, 2017: 7).

Yapay zekanın savaş ve savunma gibi alanlarda bir çok fayda sağlayacağı öngörülmektedir. Yapay zekanın hızlı karar alabilmesi, öngörü yapabilmesi, kendini

iyileştirme yeteneğinin bulunması gibi özellikleri sayesinde bazı avantajlar sağlanacaktır. Bunların yanında yapay zekanın özerk oluşu, yenilenme, eğitilebilmesi, başarımları, keşif yapabilme yetenekleri de fayda sağlayan diğer özellikler olarak sayılabilir. Burada özerkli konusunda örnek verilecek olursa, şu an savunma sanayinde bazı “otonom silah sistemleri” test edilmeye başlanmıştır. Bu sistemler insan komutalarına ihtiyaç duymadan karışık savaş misyonlarını yerine getirebilen sistemlerdir. Günümüzde kullanılan yapay zeka sistemlerinin genelinde insan olmasına rağmen, gelecekte insandan tamamen bağımsız otonom sistemlerin devreye gireceğini söylemek yanlış olmayacaktır.

Geneva 2014 yılı raporuna göre, konuşmacılar ve katılımcılar arasında, kendi eylemlerini tamamen bağımsız olarak belirleyebilecek, karmaşık kararlar verecek ve birbirleriyle uyum sağlayabilecek olan yapay zekalı otonom silah sistemlerinin ne kadar süre içinde tüm bunları gerçekleştirebileceği konusunda farklı fikirler vardı. Yine bu raporda, insansız silah sistemlerinin gelecekte bazı yönlerden bağımsızlıklarının artacağı ancak bu özerkliğin daha fazla insan denetimine ihtiyaç duyulacağı da tartışılan konular arasındaydı (Autonomous Weapon Systems, 2014: 16). Günümüzde ise kendi uçuş yollarında gezinebilen dronlar, otonom olarak hareket edebilen, inip çıkabilen insansız hava araçları ve yine otonom hareket eden böcekler gibi sistemler mevcuttur (Petman, 2017: 6).

1989’da dünya çapında web adlandırma ve adresleme protokolleri, internetin bugün bildiğimiz küresel olguya dönüşmesine izin vermiştir. Daha yakın bir zamanda internet bağlantılarının, bilgisayarların ya da iletişim sistemlerinin ötesindeki internet bağlantılarının otomobiller, saatler, ev eşyaları veya diğer pek çok nesneye genişletilmesi olan “Nesnelerin İnterneti” (IoT) ile yeni bir kavram ortaya çıkmıştır (Sanchez). Daha sonra ise bu kavram savunma alanına dahil olmasıyla da “Savunma Nesnelerin İnterneti” (DIOT) adını almıştır.

Nesnelerin interneti savunma alanında; askeri istihbarat ve komuta, kontrol sistemleri, tüm alanlara yerleşebilecek sensörler anlamında yarar sağlamakta ve farklı çatışma bölgelerinin üzerinde kontrolü elde etmelerine imkan tanımakta ve askeri komutanların durumsal farkındalığını arttırmaktadır (Sanchez). Ancak diğer bir noktadan bakılacak olursa, yapay zekanın tamamen özerk hale getirilip öldürme kararı

verme yetkisi insanların elinden çıktığı takdirde olumsuz sonuçlarla karşılaşılabilir. Örneğin; 1962 yılında iki Sovyet subayı olan Vasili Arkhipov ve Stanislav Petrov'un vermiş olduğu bir karar insanlığı kurtarmıştır. B- 59 denizaltıdaki olayda, bir ABD gemisinin kendilerine saldıracağını sanmalarına üzerine diğer subaylar nükleer saldırı kararı almıştır. Ancak oybirliği gerekmiş ve Arkhipov ve Petrov bunu onaylamayarak arıza raporu verip 3. Dünya Savaşı'nı önlemişlerdir. Bu subayların yerinde karar almada görevli bir yapay zeka sistemi olsaydı durum yine aynı olur muydu bu tartışılması gereken bir noktadır (Say, 2019: 144).

2.5.1. Yeni Savaş Stratejileri

Günümüzde yapay zeka teknolojilerinin hızla kullanılmaya başlamasıyla birlikte savaş stratejilerinde de yenilikler ortaya çıkmıştır. Savaş alanında özerk silah sistemlerinin kullanılmaya başlamasıyla birlikte bu sistemlerin hukuk açısından değerlendirilmesi önem ve aciliyet kazanmıştır. Bu teknoloji, savaşın doğasını ve potansiyel olarak uluslararası yasal düzenlemelerin doğasını derinden etkileyecektir. Bu nedenle gelecekte ortaya çıkabilecek zorluklar ve problemler uluslararası hukuk alanının gündeminde yer almaktadır (Pelman, 2017: 16).

Özerk silah sistemlerinin hızla gelişmesi ülkeler arasındaki güç dengesini de etkileyecektir. Özerk silah cephaneliğine sahip olan bir devlet, diğer tarafın böyle bir teknolojiye sahip olmadığı durumlarda, bir üstünlük elde etmiş olacak ve bu silahları kullanmada bir avantaj sahibi olacaktır. Bu silahları yasadışı bir tehdide karşı kullandığında ise neden olunan zarar için yasadışı saldırı yapan devlet sorumlu tutulacaktır (Petman, 2017: 12).

İngiliz ordusu “Özerk Savaşçı” olarak bilinen projesindeki simülasyon savaşlarında en büyük robot testini yapmaya başlamıştır. Bu projede geliştirilmiş gözetim dronları ve insansız araçlar bulunmakta ve birlikler 70'ten fazla fütüristik teknolojiyi deneyecektir (Buckley, 2018).

ABD merkezli Yeni Amerikan Güvenlik Merkezi (CNAS)'ın yayımladığı rapora göre, Çinli yetkililer yapay zekanın küresel barışı tehdit edebilecek bir “silahlanma yarışı”na sebep olabileceğini düşünmektedir. Bu konuda özellikle dikkat çekilen nokta insansız hava araçlarıdır. Çünkü ülkeler yapay zekayı savaş dahil bir çok

alandan yararlanarak fayda sağlamak amacındadırlar ve bu da potansiyel çatışmalara yol açabilecektir (Batı ve Yılmaz, 2019: 26).

Yapay zekanın riskleri arasında tartışılan bir diğer konu da bugün insanların yaptığı bir çok işi gelecekte tamamen yapay zeka destekli robotların yapabileceği konusudur. “Savaş bu iş alanlarından biri olacak mıdır?” sorusu gündemde en çok tartışılan konuların başında gelmektedir.

DARPA’nın (The Defense Advanced Research Projects Agency) ordu içi sohbet ağının temeli sayılmaktadır. Bunun yanı sıra, Tureng’in Nazi Almanya’sını yok eden ilk bilgisayar ise tüm bu teknolojik gelişmelerin en önemlisi sayılmaktadır (Batı ve Yılmaz, 2019: 27). Savaş alanlarında ortaya çıkan teknolojik gelişmeler silah, ulaşım, hız, imha gücü gibi pek çok konuya odaklanacaktır. Fakat sinir bilimi, bio teknolojiler, beyin makine ara yüzü gibi gelişmeler ile daha önce hiç rastlanmamış olan “ süper askerler “ veya “ süper yıkım robotları” savaş ortamında önde gelebilen sistemler olabilir (Batı ve Yılmaz, 2019: 27).

Savaş ortamında gelişen teknolojinin en önemlilerinden biri de beyin ara yüzü teknolojisidir ki bunun sayesinde birçok şey sadece zihin ile yapılabilir. Bu teknoloji öncelikle kask, gözlük veya lens gibi ara araçlara ihtiyaç duyacak ancak daha sonra daha da gelişen teknoloji ile bunlar tamamen insan bedenine yerleştirilebilecektir (Batı ve Yılmaz, 2019: 27). Beyin ara yüzü teknolojisinin en gelişmiş üst noktası olarak ise, belki de askerler hiç savaş ortamına gitmeyeceklerdir.

Savaş alanında avantaj sağlayacak olan bir diğer teknoloji de giyilebilir bilgisayarlar ve robotlar olacaktır. Bu kıyafet askerleri koruyacak, onlara hız kazandıracak, ısıtacak ve sanal gerçeklik ile ilgili sistemlerin temeli olabilecektir. Ayrıca bio protezler sayesinde de askerler daha hızlı koşabilecek, daha yüksek yerlere tırmanabilecek ve zorlu parkurları daha kolay aşabileceklerdir (Batı ve Yılmaz, 2019: 28). Ayrıca otonom sistemlerin kullanılmasıyla savaş alanı genişleyecek, sürekli artan savaş alanı temposuna daha hızlı tepki verilebilecek ve sabit kayıtlar ya da videolar aracılığıyla daha detaylı bilgiler elde edilebilecektir. Aynı zamanda kısa sürede hedefe odaklanma ve karar verme aşamaları da çok daha hızlı gerçekleşecektir (Pelman, 2017: 2).

Yapay zeka sadece savaş alanında uygulandığında bile ne gibi avantajlar sağlayabileceği görülmüştür. Savaş alanıyla ilgili akla gelen her konuda (görsel, işitsel, keşif, kıyafet, mekansal) yapay zekanın yararı çok fazla olacaktır.

Arttırılmış gerçeklik ve sanal gerçeklik konusu da yapay zekanın önemli alt dallarındandır. Bir gözlük ya da kask ekran ile askerlerin gördüğü şeylerin üzerine, yazılım teknolojileri sayesinde istenilen efekt, görüntü ve detaylar eklenebilecektir (Batı ve Yılmaz, 2019, 29). Görüldüğü üzere yapay zekaya insanın her alanda ve aşamada ihtiyacı olacaktır.

Burada öncelikle yine karar merci insan olacak ancak yapay zeka tüm hesaplamaları yapıp en son aşamada insana yani askerlere seçenek sunabilecektir. Bu da hız, güvenilirlik vb. açılardan askerlere avantaj sağlayacaktır.

2.5.1.1. Yapay Zeka Destekli Özerk Silahlar ve Uluslararası İnsancıl Hukuk

Otonom silah sistemleri ile ilgili özellikle ölümcül olabilecek üzere tasarlanan sistemler iki temel sorunu gündeme getirmiştir. Bu sorunlar hem Uluslararası İnsancıl Hukuk (IHL) hem de Uluslararası İnsan Hakları Hukuku (IHRL) açısından önem taşımaktadır. Ayrıca ölümcül bir özerk robot, uluslararası yasal standartları ihlal ettiğinde sorumluluğun bireye mi devlete mi ait olacağı tartışmalı bir konudur (Espada ve Hostal, 2013: 7).

“Yeni bir tür silahlanma yarışı devam ediyor ve bunun sonucu gezegenimizi şekillendirecek, bu yarış iki ülke arasında değil, bu yarış yavaş yavaş değişen hukuksal ve kurumsal normlarımızın “kaplumbağası” ile silah endüstrisindeki hızlı teknolojik değişimin “tavşanı” arasındadır (Kane, 2013).

Daha önce de değinildiği üzere özerk silah ve sistemlerin savaş yani savunma alanında gelecekte çok daha fazla kullanılacağı bilinmektedir. Burada “özerklik” kelimesinden kasıt; örneğin, bir hava aracı gibi insansız bir platformda bulunan algoritma tabanlı teknoloji tarafından gerçekleştirilen otonom saldırı kararlarını vermek olarak anlaşılmalıdır (Boothby, 2012: 584). Otonom silah sistemlerinin uygulanabilirliği konusunda silahlı çatışma yasasının geçerli olduğu genel kabul görmüş bir fikirdir. Ancak sıkıntılı olan kısım belirli normların, dronlar, siber saldırılar ve özerk silah sistemleri gibi yeni sistemlere nasıl uygulanması gerektiği tartışmasıdır (Schmit ve

Neupane, 2013: 243). Bu sistemlerin uluslararası hukuk açısından tamamen yasaklanması söz konusu olmamakla birlikte, bu sistemleri planlama aşamasında gerekli olan önlemler alınmalıdır. Çünkü bu sistemler özel olarak saldırı için programlanmadıkça, kasıtlı olarak savaş suçu işlemeyeceklerdir.

“Özerk Silah Sistemi” (Autonomous weapon systems) terimi genellikle insan girişi ya da yönlendirmesi olmadan gerçekleştirilebilecek ve başlatılacak bir silah kategorisini ifade etmektedir. Kritik işlevlerde özerkliği olan herhangi bir silah sistemi, yani arama, tespit etme, tanımlama, seçme izleme ya da saldırı pozisyonundayken hasar verme ve yok etme işlemlerini insan müdahalesi olmadan yapabilmektedir (Davison, 2017: 5). Ancak burada insan girdisi bu sistemlerden tamamen soyutlanamaz. Çünkü en otonom yani özerk sistemin bile üretilmesi ve tasarlanmasında insan mutlaka olacaktır. Henüz bu tanıma tam olarak uyan silah sistemleri mevcut olmasa da silah teknolojilerindeki eğilimlere ve gelişmelere genel olarak robotik alanındaki bir bakış ile bakıldığında, tamamen özerk silah kavramının çok da uzakta olmadığı görülmektedir. Şu an pek çok ülke tamamen özerk silah sistemlerinin öncüleri olabilecek teknolojiler kullanmaktadır (Bradán, 2014: 237). Makinelerin insanları bağımsız olarak hedef almalarını ve öldürmelerini sağlamak muhtemelen savaşın yasal ve etik boyutlarının dışında kalan ve savaş insanlığı ile daha fazla ilgilenen halkın endişelerini tetikleyecektir. Aynı zamanda bu konuda otonom silahların insanlığı savaş denkleminde uzaklaştırdığı iddiaları da mevcuttur (Gutlein, 2005: 12).

Bu konuda değinilmesi gereken bir nokta da tam otonom silah sistemlerinin yanlış anlaşılmasıdır. Bazı devletler ürettikleri sistemleri tanıtırken bunu özerk olarak tanıtmaktadırlar. Örneğin, İngiliz Savunma Bakanlığı, henüz özerkliği kanıtlanamayan Taranis savaş uçağının prototipini bu şekilde sunmuştur. Yine Kuzey ve Güney Kore sınırında bulunan hareketsiz nöbetçi Samsung SGR- AI, özerklik ayarlarından sadece birine sahip olmasına rağmen, “özerk” olarak adlandırılmaktadır (Vilmer, 2015). Yani bazı kelimeleri yerinde kullanmamak anlam kargaşasına ve sorunlara neden olmaktadır. Özerk ifadesi bu anlamda sorgulanmaya muhtaçtır.

Gelecekteki özerk silah sistemlerinin bilgi işlem yetenekleri katlanarak daha hızla ve daha güçlü olacaktır. Ayrıca kullanılan bilgisayarlar da boyutsal olarak daha küçük olacak ve özerk sistemler yapay zekalar ile donatılacaktır. Yapay zeka sistemleri

belirli ve tanımlanmış görevleri tamamlamak için sadece seçimler yapmayacak aynı zamanda insani bilişsel yetenekler sergileyerek karmaşık problemleri çözebileceklerdir (Schmitt ve Neupane, 2013: 239).

Davison, özerk silah sistemleri için, insanların bu sürece dahil olabileceği süreçleri üç ana başlık halinde ele almıştır. Bunlardan ilki, silah sisteminin geliştirilmesi ve test edilmesi yani geliştirme aşamasıdır. İkincisi, komutan ya da işletmeci tarafından silah sistemini etkinleştirme kararı (etkinleştirme aşaması), sonuncusu ise bağımsız olarak hedefleri seçip saldırdığı yani operasyon aşamasıdır.

11 Eylül 2001 terörist saldırılarından sonra insansız hava araçlarının kullanımı yaygınlaşmış ve bu son olarak ise “otonom silah sistemleri (autonomous weapon systems) olarak karşımıza çıkmıştır (aktaran Özer, 2019: 30). Devletlerin ise bu sistemleri kullanmak istemelerinin nedeni, ordunun daha azıyla daha fazlasını yapmaya çalışmaktır. Bu yüzden daha ileri teknolojiler peşinde koşmakta ve orduda daha fazla insan gücü yerine özerk silah sistemleri (AWS) gibi yüksek teknoloji çözümlerle uğraşmaktadırlar. AW, “sıfır kayıp” savaşı için bir çözüm önerini gibi görünmektedir ordular için. Bu sebeple daha fazla insansız silah sistemlerini takip etmekte ve bu sistemlerle daha fazla istihbarat sağlamakta ve insan müdahalesi olmadan savaşa daha çok yaklaşmaktadırlar (Gutlein, 2005: 15). Örneğin şu anda, Birleşik Devletler Hava Kuvvetleri (USAF) insansız hava araçlarıyla bu otonom silah sistemlerine öncülük etmektedir. AWS, insanlı veya insansız sistemlere kıyasla sayısız ve yadsınamaz avantajlar sunmaktadır. AWS, elektronik savaşın bir dron ile insan operatörü arasındaki iletişim bağlantısını bozabileceği ya da hatta koparabileceği ortamlarda çalışabilecektir. Aynı zamanda buna ek olarak, sahaya alınmış bir AWS, hızlı ve sürekli değişen savaş alanlarındaki insanlardan teorik olarak daha hızlı ve birden fazla görev alabilen pozisyonlarda olacaktır (Kane, 2003: 1342). Askeri teknoloji yalnızca bir kişiyi ya da nesneyi tespit edebilmenin ötesine geçmiş olup, modern sensörler aracılığıyla nesnelerin şeklini ve boyutunu değerlendirip hızlarını belirleyebilir. Aynı zamanda nesnenin çevresini dinleyip diğer nesneler hakkında ek veri toplayabilmektedir. Tüm bunlar da hedefe müdahaleyi kolaylaştıracak etkenlerdir (Schmitt, 2013: 247). İnsan karar vermeden çalışacak olan bir teknolojinin uluslararası toplumda önemli hukuki kaygılara neden olması kaçınılmazdır. AWS teknolojilerinin uluslararası alanda yasaklanmasını

ya da kısıtlanmasını sağlamak için çeşitli çalışmalar yapılmakta olup, özellikle sivil toplum örgütleri bu anlamda öncü olmaktadır.

Otonom silah sistemleri; barut ve nükleer silahların icadından sonra savaşlarda kullanılan üçüncü bir devrim olarak değerlendirilmelidir. Bunun altında da ölümcül otonom silah sistemleri, katil robotlar, robot silahlar ve insansız silahlar sayılabilmektedir (Özer, 2019: 30).

Uzmanlar, kurumlar ve uluslararası örgütler farklı çeşitlerde otonomi dereceleri sınıflandırmışlardır (Özer, 2019: 31):

1. İnsan Hakları İzleme Örgütü; döngü içinde insanın bulunduğu sistemler, döngünün üzerinde insanın bulunduğu sistemler ve insanın döngünün dışında kaldığı sistemler olarak,
2. Uluslararası Kızılhaç Teşkilatı; uzaktan kumandalı sistemler, otomatik sistemler ve otonom sistemler olarak,
3. Amerika Savunma Bakanlığı ise yarı otonom silah sistemler, insan tarafından denetlenen otonom sistemler ve otonom silah sistemleri olarak sınıflandırmıştır.

Otonom silah sistemleri, hedeflere ulaşmak, onları izlemek ve hedeflere saldırmak ile ilgili konularda insanlara gerek kalmadan bağımsız hareket edebilen teknolojilerdir (Özer, 2019: 31). Yani bir kez etkinleştirildiğinde, tekrar tekrar bir insan müdahalesine gerek kalmadan hedefleri seçip uygulamaya koyabilen bir silah sistemidir. Ancak bilindiği gibi bu bağımsızlığın getireceği bazı problem ortaya çıkmaktadır. Bunların başında da uluslararası insan hakları hukuku, uluslararası ceza hukuku ve uluslararası sorumluluk gibi hukuk açısından önemli olan konular yer almaktadır.

Otonom silah sistemlerinin ulusal güvenlik üzerindeki etkileri çok fazladır. Amerika Birleşik Devletleri ve müttefikleri, potansiyel rakiplere karşı teknolojik güçlenme konusunda kendi kuvvetlerine üstünlük kazandırma çabasıdadır. Ancak bunu yaparken öldürücü kuvvet sağlayan sistemler üretmektedir. Çünkü savaşın amacı düşmanın zararına olacak şekilde avantajlar elde etmektir. Bu anlamda silahlı çatışma yasası askeri gereklilik ve insanlara zararı en aza indirmek arasındaki yasaklar, kısıtlamalar ve sorumlulukları içermektedir. Bu nedenle, yasal topluluk için sorun,

özerk silah sistemlerinin devletlerin ulaşmak için uyguladıkları yasal normlara uyup uymadığıdır (Schmitt, 2013: 232).

Günümüzde özerk silah sistemleri ile ilgili olarak uluslararası toplum, insancıl hukuk ilkelerinin nasıl ve hangi şekillerde uygulanabileceği konusunda ikiye bölünmüştür. 2012 yılında İnsan Hakları İzleme Örgütü, Harvard Hukuk Okulu Uluslararası İnsan Hakları Kliniği ile birlikte, Otonom silah sistemlerinin üretimi ve kullanımı tümüyle bir yasaklama çağrısında bulunmuş ve bir rapor yayınlamıştır (aktaran Pelman, 2017: 24). Ancak birkaç gün sonra ABD Savunma Bakanlığı, tam tersi bir yönde karar almış ve bu otonom sistemlerin geliştirilmesiyle ilgili politikaları belirleyen bir direktif yayınlamıştır. Birleşmiş Milletler ise 2013 yılında yasal bir çerçeve ortaya konana kadar otonom sistemlerin geliştirilmesi konusunda çağrıda bulunmuştur.

Savaşın getirdiği hasar ve felaketleri sınırlandırmak için, uluslararası hukuk, kime ya da hangi bağlamda kullanacağına bakılmaksızın, silahlı çatışma dönemlerinde belirli silahların kullanılmasını yasaklayabilmektedir. Bu yasaklama devletlerin, gereksiz yaralanmalara neden olabilecek silahları geliştirmelerini ve aynı zamanda meşru silahların sivilleri ayırt edemeyenleri geliştirmelerini önlemeye ilgilidir (Bradand, 2014: 248). Uluslararası İnsancıl Hukuk'a uymak; siviller, sağlık personeli, insanı yardım kuruluşları ve savaşa girmeyenler için çatışma sırasında bir koruma sağlamaktadır. Otonom silah sistemlerinin kurallara uymadığı durumlarda, bu insan gruplarına sağlanan korumanın azalacağı öngörülmektedir. Düşmanlıklarda ve savaşlarda yer almayanların korunması uluslararası insancıl hukukun temeli sayılmaktadır. Ayrıca bu hukuka uymak devletler arasındaki barışın sürdürülmesi ve korunması konusunda da önem arz etmektedir. Genel olarak yasalara uymak dünya topluluğunu birbirine bağlamakta ve hukuk devletlerinin özü olmaktadır. Dolayısıyla barışın sürdürülmesi için, silahlı çatışmalar sırasında devletlerin kullanmayı seçtiği savaş araçları ve uyguladığı sistemleri yasalara uymak zorundadır (Chengeta, 2016: 71).

Uluslararası toplum yasal silah incelemelerini iki farklı alanda değerlendirmektedir. Bunlardan birincisi “silah kanunu” olarak bilinmektedir. Bu kanun ayrımcılık ilkesini içermektedir. Yani bir silah yasal olması için siviller ile askerler arasındaki ayrımı doğru yapabilmelidir. Bir hedefi doğru şekilde vurma kabiliyetlerine

rağmen kontrol edilemeyen etkileri olan silah sistemlerinin yasaklanması gerekir çünkü bu tür silahlar hasta ve yaralı -savaşçılar gibi yasadışı hedeflere yönelebilmektedirler. Yasal silah incelemelerinin bir diğer alanı da “ hedefleme yasası”dır. Hedefleme yasası silahların çatışmalarda kullanılmasını düzenlemektedir. Yani silah yasaları savaş araçlarını ele alırken hedefleme hukuku ise savaş yöntemleriyle ilgilenmektedir. Örneğin daha önce de bahsedilen orantılılık, hedefleme kanunu altındaki bir ilkedir. Meşru bir askeri avantaj elde etmek için bir hedefe uygulanacak güç miktarıyla en az teminat vermek gerekir (Kane, 2003: 1347-1348).

Uluslararası hukuk, genel olarak kabul edilen ahlaki ve etik ilkeler üzerine kurulmuştur. Gutlein’e göre, otonom silahlar bu bahsedilen etik ve ahlaki değerlere uygunluk gösterdiği takdirde kabul edilebilir bir savaş şekli olabilecektir.

Bu konuda değinilmesi gereken bir diğer önemli nokta da özerk silah sistemlerinin duyguya sahip olmadığı için insanlara daha çok zarar vereceği yönündedir. Özerk silah sistemleri eleştirmenleri insanoğlunun duygusal karakterinin diğer insanları öldürmesini kısıtlayabileceği görüşündedirler. Ancak tarih (Ruanda ve Balkanlardan, Darfur ve Afganistan’a kadar) insanoğlunun sebep olduğu korkunç acılarla doludur (Schmitt, 2013: 249). Özerk silah sistemlerinin riskleri değerlendirilirken konuya bu açıdan da bakmak gerekmektedir.

Thompson Chengeta, otonom silah sistemlerinin uluslararası insancıl hukukun önemli kurallarına uymayacağını ya da otonom silah sistemlerinin uluslararası insancıl hukuka uygun bir şekilde geliştirilmesinin çok zor olacağını söylemektedir. Çünkü insancıl hukuk terimlerinde bulunan bazı kavramların net tanımları olmadığı için bunlar makinelere veya robotlara kodlanamayacaktır (Özer, 2019: 31, Chengata, 2016: 63-67). Özerk silah sistemleri Uluslararası İnsancıl Hukuk’a (IHL) uygun olarak düzenlenmektedir. Bu sistemlerin bu hukuka uygun olarak kullanılması için her şeyden önce silah geliştiren ve kullanan devletler sorumluluk sahibi olacaklardır. Bu nedenle özerk bir silah sistemi kullanarak bir saldırıyı planlayan, buna karar veren ya da uygulayanlar, silah sistemi ve kullanım şekillerinin IHL’ye uygun olmasını sağlamalıdır (Davison, 2017: 7-8). Ayrıca bir devlet konuşlandırmadan önce yeterince test edilmemiş ya da gözden geçirilmemiş özerk bir silah sistemi kullanmaktan da sorumlu olacaktır. IHL uyarınca makinelerin etik veya insancıl olma

zorunluluğu yoktur ancak insanlığa uygun kısıtlama ve saygı ile kullanılmaları gerekmektedir (Sharkey, 2012: 796). Devlet; kendi başına sorumlu tutulmayan kişilerin yasa dışı bir eylemini kabul ettiğinde, emrinde yer alan uluslararası bir kuruluşun ya da devlet organlarının hükümet talimatlarını yerine getirirken bir yükümlülüğün ihlalini teşkil eden davranışlardan sorumlu tutulmaktadır (aktaran Espada ve Hostal, 2013: 10).

Geneva 2014 yılı raporunda katılımcıların değindiği bir konu da gelişen bu otonom sistemlerle insanların yaşam hakkı geçersiz kılınacak mıdır? Sorusudur. Artan teknolojik gelişimle savaşın insanlıktan çıkarılması ile sorumluluk ve ahlaki hesap verebilirlik kimde olacaktır? Raporda konuşmacı böyle bir durumda makinelerin sorumsuz olacağını, ahlaki açıdan kararların insan denetiminde olması gerektiğini vurgulamıştır. Bu anlamda uluslararası insan hakları hukuku ahlaki bir çerçeve sunmakta ve insanlık onuruna saygı duymayı, öldürme kapasitesinin bir makineye devredilmeyeceğini, öldürme kararının insanda kalması gerektiğini belirtmektedir. Bu rapora göre kısaca, otonom bir silah sisteminin kullanımına ilişkin ahlaki sorumluluk her daim komuta zincirindeki son insanda kalacaktır (Geneva, 2014: 24).

Ayrıca uluslararası insancıl hukukun ayırım, orantılılık ve askeri gereklilik ilkelerini otonom silah sistemleri ihlal edebilecektir. Uluslararası silahlı çatışmalar için, Cenevre Sözleşmelerine Ek 1 Protokolü, ayırım kuralına dair bazı hükümlere sahiptir. Buna göre sivil nüfusa ve sivil nesnelere saygı duyulmasını ve korunmasını sağlamak için, çatışan taraflar her zaman sivil ve savaşı arasında ayırım yapacaklardır (Chengeta, 2016: 75). Ayırmacılık ilkesi, sivilleri, sivil nesneleri ve diğer korunan kişileri ve düşmanlıkların yürütülmesi sırasındaki yerleri korumak için silah sistemlerinin kullanımına ilişkin olan, silahlı çatışma kurallarının temelini oluşturmaktadır. Bu ilke özerk silah sistemlerine de uygulanacaktır. Bu ilke gereğince, sivil nüfus asla bir saldırının hedefi olmayacaktır. Yapay zeka ile tasarlanmış silah sistemlerinin, muhripler ve siviller arasındaki ayırımla mücadele etmesi mümkün değildir. Örneğin, savaşlarda askerlerin üniformalı olması ayırım yapabilmeyi kolay kılarsa da, şehir savaşlarında ayırım yapmak çok daha zor hale gelecektir. Robotlar, ayırım ilkesine uyumu sağlamak için üç temel faktörden yoksundur. Bunlardan birincisi, savaşçıları sivillerden ayırmak veya teslim olan savaşçıları tanımak için yeterli görme işleme ve duyuşal sistemlere sahip değildirler. Onlar için mevcut olan sadece kameralar ya da sensörlerdir. İkinci faktör ise bilgisayar koduna çevirilebilecek yeterli bir sivil tanımı

yapılamamaktadır. Son olarak, makineler sivillerle üniforma giyen askeri birlik arasındaki farkı tespit edebilseler bile, savaş alanında sağduyulu mantıktan yoksundurlar (Sharkey, 2012: 788-789). İnsancıl bir savaş yürütmek için genel kabul görmüş uygulamaları ele alan ve uluslararası hukukun bir alt kümesi olan Silahlı Çatışma Yasası (LOAC) da bu konuda bazı hükümler getirmiştir. Bunlar askeri gereklilik, orantılılık ve ayrımcılıktır. Askeri gereklilik, aşırı hasara neden olan silahların kullanılmasını önlemektedir. Orantılılık ilkesi, karakteristik insan değerlendirmesine ihtiyaç duyan bir ilke olarak karşımıza çıkmaktadır. Yani iyi niyet ve askeri komutanlık gibi terimlere dayanmaktadır. Bu geleneksel yasa kuralı, tesadüfen sivil yaşam kaybına, sivillerin yaralanmasına ya da sivil nesnelere zarar verilmesine yasak koymaktadır (Schmitt, 2013: 253). Son olarak askeri gereklilik ilkesi ise, savaşçıların bir amaca veya hedefe ulaşmak için kullanmaları gereken yeterli gücü sağlamaktır (Gutlein, 2005: 10). Sivillere zarar vermediği sürece özerk silah sistemleri askeri gereklilik ilkesine uygun olacaktır. Ayrıca bu ilkeler dışında gerekli olan ve önem arz eden diğer şey “yasa”dır. Yani sivillere zarar verilmemesi konusunda özerk silah sistemlerine ilişkin yasalar ortaya konulmasını ifade eder.

Prensipte, ayırım gözetmeyen zarara ya da gereksiz acılara neden olan veya orantılılık ilkesine uygun olmayan bir silah, uluslararası hukuk nazarında yasal olarak kullanılamaz. Uluslararası Adalet Divanı (ICJ), bunu nükleer silahlara atıfta bulunarak ve Uluslararası İnsancıl Hukukun “kardinal” ve “geçilmez” olduğunu belirterek ifade etmektedir (aktaran Espada ve Hostal, 2013: 19).

Yani görüldüğü üzere, uluslararası insancıl hukuk sisteminin temel ilkeleri otonom silah sistemleri tarafından ihlal edilebilecektir ve nesnelerin interneti sistemleriyle de şimdilik belirli noktalarda hala insana ihtiyaç duyuluyor olsa da otonom arttıkça insan daha geri planda kalacak ve hatta zamanla insana karar verme aşamasında hiç gerek kalmayabilir. Ancak bu yakın gelecekte mümkün değildir. Sistemi programlamaya ya da tasarlamaya, belirli bir ortama sokmaya yine insan karar verecektir. Bu açıdan düşünüldüğünde kurallara ve yasalara uymaktan yine insan sorumlu olacaktır. Örneğin, özerk bir sistem sivillere zarar verdiyse burada sorumluluk o sistemin kullanımını onaylayan insanda olacaktır. Otonom silah sistemlerinin tamamen insan kontrolünden çıkması ya da buna kısıtlamalar getirilmesi de problemlere sunulan çözüm önerileri arasındadır.

Konvensiyonel Silahlar Taraf Devletler (Conventional Weapons (CCW) States Parties) bu konu hakkında, “anlamlı” ve “etkili” insan kontrolü veya insan yargısına odaklanması gerektiği üzerinde durmuşlardır. Nisan 2016 CCW toplantısında başkan ölümcül kuvvete ilişkin uygun insan katılımı ve kullanım delegasyonuna ilişkin görüşlerin daha fazla dikkate alınması gerektiğini belirtmiştir (Davison, 2017: 11). Ayrıca Konvensiyonel Silahlar Antlaşması II. Protokol ayırım gözetmeyen mayın kullanımını, üretimini, stoklanması ve transferini yasaklamaktadır (Gutlein, 2005: 8). Bunun belirtilmesinin sebebi mayınlar ile otonom silahlar arasında bir paralellik olduğu görüşündendir.

İnsansız silahlı araçları (İHA) tartışan uluslararası araç 1987 yılında kurulan Füze Teknolojisi Kontrol Rejimidir (MTCR). Bu, insansız dağıtım sistemlerinin kitle imha silahları için yayılmasının önlenmesi amacını paylaşan otuz dört ülkeden oluşan bir ağ olarak karşımıza çıkmaktadır (Sharkey, 2012: 798).

Biyolojik silah kategorisindeki herhangi bir silah, kontrol edilemeyen bir silahın modern örnekleri olarak karşımıza çıkmaktadır. Bu silahlar tasarımları gereği serbest bırakıldıktan sonra kontrol edilemez. Yönlendirilip belirli hedeflere karşı kullanılabilirler fakat etkileri pek çok açıdan amaçlarının ve hedeflerinin çok ilerisine yayılabilmektedir. Bu sebeple, biyolojik saldırıların çalışma ve nüfuz etme şekli doğal olarak anlaşılmazdır, bu yüzden savaş kuvvetlerinin bunları kullanmasına izin verilmemektedir (Bradán, 2014: 256). Yapay zeka destekli bu otonom silah sistemlerinin kullanımına geçilmeden önce uluslararası işbirliği gereklidir. Avrupa Parlamentosu bu konuda bu tarz silahların kullanımını yasaklasa da bu yeterli olmamakta, küresel çapta önlemler alınması gereklidir.

ABD, yarı özerk silah sistemleri, insan denetimli özerk silah sistemleri ve özerk silah sistemleri arasında ayırım yapan bir politika uygulamaktadır. Bu politikaya göre, yarı özerk silah sistemleri genellikle iletişimin bozulmuş veya kaybedilmiş olması durumunda sistemin hedefi özerk olarak seçemeyeceği durumlarda kullanılmaktadır. Yani bir insan operatör söz konusudur. İnsan denetimli özerk silah sistemleri ise yerel savunmada, insanlı tesislerin savunmasında ya da insanlı platformların gemide savunmasında kullanılmaktadır. Son olarak özerk silah sistemleri ise bazı elektronik saldırı biçimlerinde kinetik olmayan kuvve karşı kullanılmaktadır (Schmitt, 2013: 269).

Espada ve Hostal'ın 2013 yılında yayınlanan makalesine göre; özerk silah sistemleri ile ilgili olarak, bu sistemlerin konuşlandırılmaları ve daha yaygın uygulamalara izin vermeden önce kullanımları için gerekli olan temel yasal çerçevenin bi an önce netleştirilmesi merkezi bir fikir vurgulanmaktadır (Espada ve Hostal, 2013: 14).

Sonuç olarak, silahların kullanılması sırasında uygulanabilir önlemler alınmalıdır. Bu önlemler daha çok siviller ile savaşçılar arasındaki ayrımı yapabilmeye yönelik olmalı ve bu anlamda mümkün olan her şey yapılmalıdır. Böylece tesadüfi kayıplar önlenilecek ve sivillerin zarar görmesi en aza indirilebilecektir. Ancak şu anda silah yasası olarak AWS'nin kullanılmasını yasaklayan hiçbir uluslararası anlaşma ya da yasak yoktur. Bu silahların kullanımına dair yasaklamadan ziyade, bir kısıtlama daha etkili ve alternatif bir yol olabilir.

Sorumluluk noktasında da bir insan sistemi nasıl programlayacağını ve ne zaman başlatacağına karar vermelidir. Yani bu birey savaş suçları ile ilgili eylemlerde bulunmaya programlama yaparsa bunlardan sorumlu olacaktır. Ayrıca, kişinin komutanı veya sivil amiri, özerk silah sisteminin bu yönde programlandığını biliyor ya da bilmesi gerekiyorsa o da bu eylemlerden sorumlu tutulacaktır.

Yukarıda da ele alındığı gibi sonuçta bu konuda ortaya çıkan en önemli itiraz bu silahların, uluslararası insancıl hukuka saygı göstermeyeceği yönündedir. Doğası gereği ayrımcılık yapamayan ya da sadece askeri ögeleri hedefleyemeyen silahlar yasadışı olarak kabul edilmektedir. Ancak burada tartışmalar genelde daha çok gelecek odaklıdır. Örneğin henüz tamamen test edilemeyen özerk sistemler üzerinden tartışmalar yürütülmektedir. Bu tarz silahların yasadışı kullanıma açık olması, onları yasaklamayı gerektirir mi? Geçmişten bir örnek verilecek olursa, teröristler tarafından kaçırılma riski olan uçakların üretimi durdurulmadı. Çünkü üretilen ve geliştirilen her yeni şeyde risk her zaman var olacaktır. Burada önemli olan bu teknolojilerin insanlığa sağladığı avantajları ve dezavantajlarıdır.

Muhalifler, bu sistemleri siviller ve savaşçılar arasında ayrım yapmanın zor olduğu alanlarda kullanılan kara tabanlı silahlar olarak görmektedirler. Ancak sistemler, sivilleri yanlışlıkla vurma riskinin çok az olduğu sualtı, denizcilik ya da hava

ortamlarına en iyi şekilde uyum sağlayabilmektedirler. Muhalifler bu durumları göz ardı ederek, bunların getireceği avantajları da görmezden gelmektedirler (Vilmer, 2015).

Elbette ki bu konuda hukuksal sistemin varlığı, bu tür silahların kullanımı ya da caydırıcılığı açısından önem arz etmektedir. Nihayetinde varılan nokta, bu sistemlerin getireceği faydalar ve riskler birlikte ele alınmalı ve ortaya çıkabilecek problemlere o yönde çözümler üretilmelidir.

Uluslararası toplumun yapay zekanın oluşturabileceği riskler ve problemler karşısında harekete geçmesi çok önemlidir. Savaş alanının kontrolü ve sınırları yine aynı şekilde öldürme otomasyonunun sınırları tartışılmalıdır. İnsanların ahlaki kararlar almalarını ve ölümcül kuvveti kontrol etmeleri sağlanmalıdır.

Yapay zeka ile ilgili yukarıdaki tüm konular kamuyu da ilgilendirmektedir. Yapay zeka teknolojilerinin kolluk kuvvetleri ve kamu güvenliğine potansiyel faydalar sunduğu yadsınamaz bir gerçektir. Ancak yasal ve toplumsal sonuçları dikkatli bir şekilde ele alınmalıdır. Örneğin bu teknoloji ile elde edilen veriler suçlarla mücadelede etkili bir araç olarak kullanılabilir. Güvenlik kameraları, suçu kanıtlayan video görüntüleri toplamak bunlardan sadece birkaçıdır. Nesnelerin interneti, kamu güvenliğini artırmada kolluk kuvvetleri için büyük faydalar sunmaktadır ve ilerleyen süreçte de çok daha fazla gelişmesi beklenmektedir (Rose, 2015: 56). Sensör ağlarının su dahil çevresel zorluklara uygulanması, hastalık ve sağlık, iklim değişikliği, doğal kaynak izleme, kaynakların kaliteli kullanımı vs. gibi alanlarda önemli bir etkiye sahip olduğunu da belirtmek gerekmektedir. Bu teknoloji sayesinde elde edilen veriler, bilim insanlarına, akademik dünyaya ve kamu görevlilerine büyük yararlar sağlamaktadırlar (Rose, 2015: 62). Ancak burada gelişmekte olan ekonomileri yatırım, kaynak sağlama, sanayi, politika ve düzenleme, koordinasyon, alt yapı noktalarında bazı zorluklar beklemektedir. Gelişmekte olan ülkeler bu sistemleri kullanmaya ne kadar hazırlar? Bu teknolojinin hızla gelişme göstermesi gelişmiş ekonomiler ile gelişmemiş ekonomiler arasındaki uçurumu çok daha fazla açacak mıdır? Hangi ülke ya da ekonomiler bu sistemleri kullanabilecektir? gibi birçok soru ve sorunlar ortaya çıkabilmektedir (Rose, 2015: 64-65).



ÜÇÜNCÜ BÖLÜM
İNSAN HAKLARI VE YAPAY ZEKA İNSAN HAKLARI GENEL BAKIŞ

3.1. YAPAY ZEKANIN İNSAN HAKLARI ÜZERİNDEKİ ETKİLERİ

İnsan hakları, en genel anlamıyla ifade edilecek olursa; kişinin insan olarak var olmasından kaynaklanan yadsınamaz ve vazgeçilemez doğal kazanımlarını ifade eder. İnsan haklarının kaynağı, insanın kendi doğasıdır. Teknolojinin gelişimi tarihte her zaman insan hakları konusunda zorluklar yaratmış ve tartışmalara sebep olmuştur. Bu bölümde yapay zeka teknolojilerinin insan hakları açısından ortaya çıkardığı güçlükler ve riskler ortaya konulacaktır. Aslında çalışmanın diğer bölümlerinde zaman zaman insan hakları konusuna değinilmiştir. Çünkü ortaya çıkabilecek tehlike ve risklerin nihayetinde dayandığı nokta insan haklarıdır.

Çağdaş zayıf yapay zekanın yeteneklerinin, bazı sınırlı faaliyetlerde insan uzmanlardan daha üstün olduğu ve yakın gelecekte bunun daha da genişleyip insan yeteneklerinin dışına çıkabileceği görüşleri vardır. Günümüzdeki durumda bile insanlar ve teknoloji arasındaki ilişki, bir değişimin temelini oluşturmaktadır. Yakın geleceğe kadar teknolojinin insanlar üzerindeki etkileri üzerinde çok fazla durulmamıştı. Ancak AI temelli teknolojilerin hem alanının hem de etkilerinin gelişmesiyle insan ve toplumun teknoloji karşısında korunması konuları gündeme gelmiştir (Hin Yan Liu-Zawieska, 2018: 2).

Çalışmanın önceki bölümlerinde değinilen sorunlar ve riskler gelecekte ne zaman gerçekleşeceği tam olarak bilinmeyen konulardır. Ancak tüm bunlar insan hakları açısından önemlidir, çünkü insanoğlu binlerce yıldır kurduğu sosyal dünyayı yeni türlerle paylaşmaya başlayacaktır. Bu da insanların bireysel düzeyde korunmasını gerektiren yeni problemlere yol açmaktadır. İnsan hakları ve yapay zeka konusunda en önemli nokta “değer uyumu” sorunudur. Yani geline teknolojik gelişmeler insanların değerleri ile uyumlu olmalıdır (Risse, 2018: 8).

Yeni teknolojiler ve bunların kullanımının yaygınlaşmasıyla, insan ve makine arasındaki ya da fiziksel ve sanal dünya arasındaki sınırlar bulanıklaşmaktadır. İnsanlık, makinelerin, robotların yardımıyla onları güçlendirip yeteneklerini arttırmaktadır.

İnsan hakları evrensel, bağlayıcı ve uluslararası hukuk alanında düzenlenmektedir. Hükümetlerin insan haklarını korumakla yükümlü olmasının yanı sıra aynı zamanda şirketlerin de insan haklarına saygı göstermesi gerekmektedir. İnsan hakları hukukunun teknolojik gelişmeler ya da tüm değişen koşullar karşısında

uyumunu gerçekleştirmek için bölgesel ve uluslararası kuruluşların olması gerekmektedir. Ancak bu şekilde yapay zeka teknolojisinin sebep olabileceği zararlar hukuki olarak kontrol altına alınabilmektedir. Fakat teknolojiye karşı insan hakları korumalarının geliştirilmesinin yolunun netleşmesinden önce bazı engellerin kaldırılması gerekmektedir. Bunlardan birincisi, endişeleri faaliyet alanına ya da emanet edilen hakkın niteliğine göre bölümlere ayırma eğilimidir. Bunun dışındaki diğer engel, insan hakları yasasının tekelleştirici eğilimi olmasıdır. Bu engel, bu modelin temel özelliklerinin her şeyden önce sorunun doğasında olmasına rağmen, baskın insan hakları modelinden uzaklaşma olasılığı üzerinde önemli kısıtlamalar getirmektedir (Hin Yan Liu- Zawieska, 2018: 3-4).

2011 yılında BM, endüstriyi insan haklarına saygı duymaya, korumaya ve sağlamaya çalışan temel ilkeler yayınlamıştır. Bunlar “İş ve İnsan Haklarına Yönelik Temel İlkeler” olarak adlandırılmaktadır. Bu ilkeler AI yöneticileri ve araştırmacılarına, insan hakları etkileri konusunda gereken hassasiyeti göstermeleri için bir klavuz olarak değerlendirilebilir. Yani işletmelerin ürünlerine geliştirirken ve dağıtırken bu ilkeleri göz önünde bulundurmaları gerekmektedir (Mark Latonero, 7).

Avrupa Konseyi Parlamenterler Meclisi’nin bu konudaki 2017 raporu, kanun koyucuların bilim ve teknolojilerin gelişim hızına uyum sağlamak zorlandıklarını ortaya koymuştur. Ayrıca 21. Yüzyılda insan onurunun korunması için uluslararası işbirliği kurulması konusuna dikkatleri çekmiştir. Bunun dışında Avrupa Konseyi’nin ilgili organlarına bağlantılı cihazların ve genel olarak teknolojik yakınsama ile ilgili sosyal ve etik sonuçların ne denli önemli olduğu konusunda değerlendirmeler yapmıştır. Uluslararası düzeyde tutarlı bir yasal çerçeve ve etkin denetim mekanizmaları sağlamak için Avrupa Birliği kurumları ve BM ile yakın işbirliği çağrısında da bulunulmuştur (Accesnow Raporu, 2017: 1-2).

İnsan hakları ve yapay zeka ile ilgili daha önce de değinilen üç temel robot yasalarının yanı sıra, 2017’de Kaliforniya’daki konferansta 23 Asimolar ilkesinin 13’ü Etik ve Değerler başlığı altında ele alınmıştır. Bu ilkelere, AI sistemleri operasyonlarının insani değerlerle uyum sağlaması için amaç ve davranışlarının güvence altına alınması ya da insanlık onuru, insan hakları, özgürlükleri ve kültürel çeşitliliklerin korunması gibi ifadeler yer almaktadır (Risse, 2018: 9).

İnsan haklarına yönelik evrensel bir desteğin olması önemlidir. Birleşmiş Milletler Ticaret ve İnsan Hakları konusunda zaten rehber ilkelere sahiptir. Ancak devletlerin AI ile güç elde etme çabaları insan hakları konusunda sorunlar ortaya çıkaracaktır. Bu nedenle geliştirilen teknolojilerle şekillenen yeni dünyada insan hakları toplulukları da yer almalıdır. Bu doğrultuda atılan önemli adımlardan biri, Uluslararası Af Örgütü'nün insan hakları nedenlerinin araştırılmasına yapay zeka araçlarından geniş ölçüde yararlanma kararı almasıdır. AF, makine öğreniminin kullanımı içinde, ceza adaleti ya da sosyal hizmetlere ulaşma konusunda ayrımcılık ihtimali üzerinde durmaktadır (Risse, 2018: 10).

20 Mart 2019'da Avrupa Parlamentosu'nun Sivil Özgürlükler, Adalet ve İçişleri Komitesi (LIBE) ile ortak olarak düzenlediği panel “Yapay Zeka ve İnsan Hakları” ile ilgiliydi. Burada panelistler yapay zekanın insan hakları konusunda birçok risk ortaya çıkaracağını ve bunların zaman kaybetmeden ortaya konması konusunda fikir birliğine vardılar. AI'nın eşitsizlik sorunlarına değinerek insan haklarının korunmasına yönelik çözümlere odaklanmışlardır. Ayrıca panelde, mahremiyetin aşınması ve algoritmik önyargı gibi konularına değinilerek AI temelli karar alma mekanizmalarının, insanların protesto etme haklarını da etkileyebileceğini ele almışlardır (Kritikos, 2019).

Yapay zeka geliştirmenin tehlikelerinin önüne geçilmesinde ve insanoğlunun güçlendirilmesinde, insan haklarının korunmasının sürekliliğini sağlamak ve doğrudan teknolojik güç ile yüzleşebilmek için uygun bir rejimin geliştirilmesi gerekmektedir (Hin Yan Liu- Zawieska, 2018: 4).

Yapay zekanın insan hakları açısından oluşturacağı risklere değinilecek olursa; sağlık hizmetlerinden sigortacılığa kadar bu alanlarda kullanılan algoritmalar ırkçı ya da cinsiyetçi ayrımcılığa neden olabilmektedirler. Yine sahte videoların üretimi ya da sahte haberlerin yazılması, büyük tehlikeler arz eden terör eylemlerine yol açabilecektir. İfade özgürlüklerini de tehdit eden durumlar ortaya çıkacaktır. Eğer AI, insan incelemesi için yeterli şeffaflığa sahip olmazsa hakları tehdit edecektir (Risse, 2018: 11).

Uluslararası Medeni ve Siyasi Haklar Sözleşmesi (ICCPR) ve Uluslararası Ekonomik, Sosyal ve Kültürel Haklar Sözleşmesi (ICESCR) de bu konuda önemli sözleşmelerdir. Bu belgeler, insan haklarının “bölünmez, birbirine bağlı ve birbiriyle

ilişkili” olduğunu gösteren Uluslararası Haklar Bildirgesi’ni oluşturmaktadır (Latonero, 11).

İnsan Hakları İzleme Örgütü Silah Bölümü’nün direktörü ve Ölümcül Robotları Durdurma Kampanyası küresel koordinatörü Mary Wareham, insanların bir makineye yaşam ve ölüm kararlarını tam dağıtamayacağına dair bir endişenin olduğunu belirtmiş ve savaşta neyin kabul edilebilir olduğuna dair kırmızı çizgiyi geçebileceklerini öne sürmüştür (Melendez, 2018).

İnsan Hakları İzleme Örgütü, 2012 raporuna göre tamamen özerk, ölümcül silahlı makinelerin mevcut uluslararası hukuka bile uymayabileceklerini iddia etmiştir. Bu rapora göre örneğin: korkmuş bir anne iki çocuğunun peşinden koşar ve bir askerin yanında oyuncak silahlarla oynamayı bırakmaları için onlara bağırır. Bir insan asker, annenin korkusu ve çocuk oyunuyla özdeşleşebilir ve niyetlerini zararsız olarak algılayabilirken, tamamen özerk bir silah yalnızca kendisine doğru çalışan bir kişiyi ve iki silahlı kişiyi görebilir. Birincisi ateşi tutacaktır ve ikincisi bir saldırı başlatabilir (Melendez, 2018).

Özerk silah sistemlerinin potansiyel kullanımını eleştirenlerin birçoğu bu sistemlerin insan haklarını ihlal edeceğini savunmaktadırlar. Bu haklar arasında da en çok zarar görenlerin yaşam hakkı ve insanlık onuru olduğunu belirtmektedirler. Uluslararası insan hakları hukuku, uluslararası insancıl hukukta kullanılan benzer başlıklara sahip olmasına karşın içerik olarak farklılıklara sahiptir. İnsan hakları bağlamında “güç” en son çare olarak kullanılması gerekir ve kademeli bir yol izlenmelidir ve güç kullanımı her bireye karşı vaka bazında değerlendirilmelidir (Pelman, 2017: 53).

Günümüze kadar, biyoetik tartışmaların ve ilgili insan hakları anlaşmalarının çoğu, organizmalarımızın içinde çalışan istilacı biyomedikal teknolojilere odaklanmıştır. Oviedo Sözleşmesi, biyomedikal alandaki yeniliklerin uygulanması sırasında insan onurunu korumak için bazı ilkeler belirlemiştir (Accesnow Raporu, 2017: 4).

Robotik ve AI geliştirirken insanoğlunun bu döngü dışında bırakılma riskinin arttığı göz önüne alındığında, asıl mesele kontrol mekanizması olarak karşımıza çıkmaktadır. Yani insanların robotik ve yapay zeka tasarımlarıyla karşı karşıya

kaldıklarında kendilerini tehdit altında hissetmelerinin temel sebebi, bu tür teknolojileri kontrol etmek için sadece sınırlı olanaklara sahip olmalarıdır (Hin Yan Liu- Zawieska, 2018: 5).

3.1.1. Eşitlik ve Ayrımcılık Yapmama Hakkı

Yapay zekanın insan hakları açısından en çok etkilediği hak olarak “ayrımcılık yasağı” karşımıza çıkmaktadır. Ancak insan haklarının tümü birbiriyle ilişkili olduğundan bu teknolojinin hemen hemen her hakkı etkilediğini söylemek yanlış olmayacaktır. (accessnow, 18). Yapay zeka destekli gözetim yazılımları, hükümetlerin farklı gruplardan insanlara yönelik hizmetleri belirleme, hedefleme ya da reddetme imkanı sağlayan açık bir ayrımcılık amacı ile de kullanılabilir. Bu ayırım, farklı cinsiyetten insanları belirlemek ve ona göre bir politika belirleme açısından ortaya çıkacaktır (accessnow, 24). Bu sistemlerde hata oranları da göz ardı edilmektedir. Çalışmanın bu bölümünde eşitlik ve ayrımcılık yasağı ile yakından ilgili olan Toronto Deklarasyonu’na yer verilecektir.

3.1.1.1. Toronto Deklarasyonu

Mayıs 2018’de Uluslararası Af Örgütü, Toronto Bildirgesi’nin hazırlanmasına öncülük etmiştir. Bu bildirge Makine Öğrenim Sistemlerinde Eşitlik ve Ayrımcılık Yapmama Haklarının Korunması ile ilgilidir. Bu belge, uluslararası yasal ilkeleri bağlayıcı olarak AI önyargısına dair var olan dikkati temel almaktadır. Toronto Deklarasyonu, hem devletlerin hem de özel sektördeki aktörlerin makine öğrenme sistemlerinin kullanımı konusundaki sorumluluklarını, ayrımcı etkileri hafifletme, zarar görenler için çözümler üretme ve şeffaflığı sağlama noktasında gerekli ilkelerini belirtmektedir (Latonero, 12). Yani bu deklarasyon, eşitlik ve ayrımcılık yapmama haklarına ve tüm insan haklarını destekleyen önemli ilkelere odaklanmaktadır.

Toronto Deklarasyonu’nda yer alan bir maddeye göre; devletler, ayrımcılığa karşı önlem almak için mevcut önlemlerin ve diğer öğrenme zararlarının makine öğrenmesi teknolojilerinin yol açtığı riskleri hesaba katacak ve ele alacak şekilde güncellemelerini sağlamalıdır. Yine bu deklarasyona göre, kamu ve özel sektör de ayrımcılığı önleme konusunda insan hakları hukuku gereğince yükümlülük ve sorumluluklara sahiptir. Bu önleme yeterli olmadığında ayrımcılık hafifletilmelidir.

Makine öğrenim sistemlerinin tasarımı, geliştirilmesi ve kullanımı süresince bilinçli olarak ya da istemeden yapılan ayrımcı girdiler insan hakları açısından bazı ciddi riskler oluşturmaktadır. Sistemler genellikle, belirli ülkeler ve bölgelerde bulunan, ırk, cinsiyet, kültür gibi açılardan bazı gruplardan sınırlı girdi alan aktörler tarafından geliştirilmektedir. Bunlar da ayrımcı sonuçlar ortaya çıkarmaktadır. Bu yüzden, makine öğrenim sistemlerinin insan haklarına saygı gösterecek şekilde tasarlanması kullanılması gerekmekte ve bunun için de çeşitli bir topluluğun aktif katılımı gerçekleştirilmelidir (The Toronto Declaration: Protecting the rights to equality and non-discrimination in machine learning systems, 2018).

Yukarıda da değinildiği üzere AI'da en çok tartışılan konulardan biri ayrımcı algoritmalar ya da sistemlerdir. Örneğin, yüz tanıma sistemlerinde yeterli eğitim verisi veya hatalı modellerin kullanılması, koyu tenli insanlar için toplumda var olan önyargıları daha da artırabilecektir. Ayrımcılığın yasaklanmasının insan hakları ilkeleri çok sayıda BM antlaşması, ulusal yasalar ya da akademik yorum ve diğer politikalar aracılığıyla yayılmıştır. Eşitlik ve ayrımcılık küresel olarak ele alınmaktadır (Latonero, 2018: 10).

Konuyla ilgili şu örneğe değinmekte yarar vardır: Londra'daki bir tıp okulu iş başvurularında yapay zeka destekli bir bilgisayar ile işe alımlarını gerçekleştirmektedir. Binlerce dosyayla insanların baş etmesi çok zor olacağından bu sistem kolaylık sağlamıştır. Ancak bir süre sonra bu sistemin, cinsiyet ve isimlere dayalı olarak kadınlara ve Pakistan gibi ülkelere başvuran insanlara negatif ayrımcılık uygulayıp, onları işe kabul etmediği ortaya çıkmıştır (Say, 2019: 153).

Yapay zeka ile insan hakları arasındaki en önemli bağlantı noktası eşitsizliktir. Günümüzde de görüldüğü üzere teknolojiyi üreten ve kullanabilenler ekonomik olarak da daha güçlü konumda bulunanlardır. AI da bu eğilimleri güçlendirecek ve üreticileri daha yüksek fiyatlı teknoloji sağlayabilecektir (Risse, 2018: 12). Bu açıdan düşünüldüğünde AI milyonlarca insanı dışlanmış vaziyette bırakacaktır. Brookings Enstitüsü'nden bir rapor, yapay zeka ve siber güçlerdeki gelişmelerin ya da kötü niyetli aktörlerin, demokrasilere daha gizli ve daha etkili olarak zarar verebileceğini belirtmiştir (Latonero, 2018: 13). Yani AI çevrimiçi konuşmalarda insan davranışını taklit etmek için tasarlandığından, politik söylemde dezenformasyonu yayabilmektedir

(Latonero, 2018: 13). Ayrıca günümüzde meslekler de yapay zekanın etkisi altında kalmaya başlamıştır. Tıp alanından hukuka kadar tüm alanlar otomasyona evrilmekte ve algoritmalara dayalı yeni meslekler ortaya çıkmaktadır.

Yapay zekanın artıracığı eşitsizliklerin önüne geçilmelidir. Ancak son 70 yılda insan hakları hareketleri göz önüne alındığında yerel ve küresel bazda adaletin dağıtılması konusunda çok da başarılı olunmadığı görülmektedir. AI en nihayetinde aydınlatma mirasını tehlikeye atabilir. Çünkü insanın bireyselliği büyük veri ve makine öğrenmesi çağında kuşatma altındadır (Risse, 2018: 15).

Yapay zeka, bilgisayar gücündeki katlanarak artan artış sayesinde zekayı simüle etmeyi ve mümkün kılmaktadır. Bilgi teknolojisi ile yaşam bilimleri arasındaki etkileşim hızla artmaktadır. Yapay bilinç makinelerle programlanmış ve böylece onlara akıl yürütme yeteneği kazandırılmıştır (Accessnow, 2017: 3). Yeni makineler, yapay zeka ile donatılmış uzman sistemlerde, askeri komuta sistemlerinde yardımcı olarak kullanılacak, teşhis ve karar verme, risk değerlendirmesi, finansal yönetim, konuşma ve görsel desen tanıma gibi özelliklere sahip olacaklardır. Bazı makineler de yapay duyguları ifade edebilecek ve karmaşık problemleri çözebilecektir. Tüm bu gelişmeler insan hakları ve insanlık onuruna etkileri bakımından yeni sorun ve problemler ortaya koymaktadır (Jean ve Le Deaut, 2017: 3).

Bilgi teknolojileri, kendi kendine toplanma, kendi kendini iyileştirme ya da akıllı davranışlar gibi canlı organizmalarla ilgili olan özellikleri gerçekleştirebilmektedirler. Gelecekte biyolojik, bilişsel ve sosyal teknolojiler sayesinde insan bedenlerine veya beyinlerine insan yapımı eserler dahil edilebilecektir. Bunlara örnek olarak, kararları etkileyebilen ya da ikna edici aletler, duygu tespit edebilen makineler verilebilir (Accessnow, AI and Human Rights, 2017: 4).

Çalışmanın ilk bölümünde de değinildiği üzere, insanlar her geçen gün teknolojiye daha fazla bağımlı hale gelmektedirler. Akıllı telefonlar, sosyal medya, çeşitli oyunlar gündelik yaşamın en önemli parçaları haline gelmiş durumdadır. Tüm bunlar düşünüldüğünde bu teknolojik makineler insanların özel ve sosyal hayatına girmiş ve insanların veri oluşturmaya olanak sağlar durumdadır. Ancak insanlar büyük veriler oluşturduğunun farkında değildir ve bu veriler gelecekteki seçimlerimize müdahale etmek için kullanılabilir.

3.1.2. Kişisel Özgürlükler Hakkı

Ceza adaleti sisteminde AI'nın artan kullanımı, kişisel özgürlüklere müdahale etme riskiyle karşı karşıyadır. Örneğin ABD ceza adalet sistemi genelinde, kefalet vermekten ceza mahkumiyetine kadar birçok aşamada tutuklama kararlarını bilgilendirmek için bir değerlendirme yazılımı kullanılmaktadır. Bu yazılım hatalı olarak yargılama öncesinde daha fazla siyah sanığın çok daha fazla uzun süre tutuklu kalmasına yol açmıştır. Çünkü burada risk programlama sistemleri yasalarla öngörülmemiş ve gözaltı kararları yasadışı ya da keyfi olabilmektedir (accessnow, 19).

1987 yılında kurulan ve insan hakları alanında küresel düzeyde bir kuruluş olan Article 19'un 2018 Nisan'ında yayınlamış olduğu rapor, yapay zekanın özellikle gizlilik, mahremiyet hakkı ve ifade özgürlüğünü ciddi anlamda etkileyeceği üzerinde durmuştur (Article 19, 2018: 4).

3.1.3. Gizlilik ve Mahremiyet Hakkı

Bir başka hak olan “gizlilik” ise insan onuru açısından en önemli hak olarak karşımıza çıkmaktadır. Çünkü bu hak ifade ve örgütlenme özgürlüğü gibi hakları da güçlendirmekte ve pek çok devlet veri koruma konusunda çalışmalar yapmaktadır. İfade özgürlüğü ve gizlilik hakları ülkelerin demokratik olmaları ve gelişmelerinin ön koşulları arasında sayılmaktadır.

Uluslararası hukukta gizlilik hakkı ve mahremiyet hakkı korunmaktadır. Örneğin İnsan Hakları Evrensel Bildirgesinin 12. Maddesi bu konuya vurgu yapmaktadır. Bu maddede kimsenin özel hayatına, ailesine, konut dokunulmazlığına veya yazışma özgürlüğüne keyfi olarak karışılmayacağı belirtilmiştir.

Yapay zeka tekniklerinin gizlilik hakkı üzerindeki yansımaları farklı şekillerde olabilmektedir (Article 19, 2018: 19-20):

- İnsanların kullandığı ve tükettiği ürünlerin çoğu ya da otonom sistemler, insanların rızası olmadan, veri üreten ya da bilgi toplayan sensörler içermektedir, (örneğin, akıllı ev aletleri ya da telefon uygulamaları genellikle veri üretmek için oluşturulmuş ürünlerdir ve bireyler bunların ne kadar veri toplayabildiği noktasında ne yazık ki bilgi sahibi değillerdir).

- İnsanlar hakkında hassas olmayan bilgilerden, hassas veriler çıkarmak için AI sistemleri kullanılmaktadır, (örneğin; sosyal medya beğenileri, konum verileri, telefon ölçümleri gibi verilerden yararlanarak kişilerin siyasi inançları, etkin kökeni, sağlık durumu gibi hassas verilere ulaşmak mümkündür).
- AI sistemleri ile kişiler nüfus ölçeğine göre profillendirilebilmektedir,
- Bireylerin hayatlarını önemli ölçüde etkileyebilecek olan veriler yine AI sistemleri tarafından kullanılabilir.

Veri koruma denince akla mahremiyet hakkı gelmektedir. Bu konu ile ilgili olarak Facebook örneği verilebilir. İnsanlar Facebook'a üye olmasalar bile onları izlemek mümkündür. Veriler sayesinde insanların hayatları hakkında ve onlar için hayati öneme sahip olan, gizli kalması gereken ve dokunulmaması gereken bilgileri ortaya çıkarabilir. Bu konu ile ilgili Avrupa Konseyi'nin Kişisel Verilerin Otomatik Olarak İşlenmesi İle İlgili Bireylerin Korunması Sözleşmesi mevcuttur. Bu sözleşme verilerin adil ve yasal işlenmesiyle ilgili ilkeler içermektedir (AI and Human Rights, 2017: 5). Gizlilik uzun süreden beri hükümetleri, işletmeleri, akademiye ve sivil toplum örgütlerini içeren geniş bir alanın endişelendiği bir konu olarak karşımıza çıkmaktadır. Bu anlamda yapay zeka geliştiricileri ve tasarım mühendislerinin gizlilik ilkelerine uyması gerekmektedir. Teknolojik dağıtımlar için gizlilik etkisi değerlendirmesi yapmak, gizliliğe uygunluk için belirlenmiş bir araçtır (Latonero, 2018: 13). Bu konu ile ilgili bir örnek verilecek olursa, Amazon'un kullandığı yapay zeka destekli yüz tanıma sistemi 2016'da kullanıma sunuldu. Amerikan Sivil Özgürlükler Birliği (ACLU) araştırmacıları, 535 Kongre üyesinin fotoğraflarını 25,000 kamuya ait imge görüntüleriyle eşleştiren bir deney yaptı ve sonuçta 28 yanlış eşleştirme ortaya çıktı. Aynı zamanda yazılımın ırksal önyargılı olduğu da tespit edilmiştir (Latonero, 2018: 13).

Günümüzde cep telefonları aracılığıyla bir kişinin yaşı, cinsiyeti, mesleği ya da medeni durumu konum verilerinden doğru bir şekilde tahmin edilebilmektedir. İnsan haklarını korumak için bu bilgiler diğer kişisel verilerle aynı derecede değerlendirilerek korunmalıdır (AI and Human Rights, 20). AI yöntemleri ile insanlar ve çevreleri hakkında kararlar alınabilir. Yüklenen veriler sayesinde tercihlerimizi bilen AI sistemlerinin bunu yapması çok da zor olmayacaktır. Netflix gibi siteler, tüketim örüntülerinden insanlar arasında bağlantı kurup, başkalarının beğendiği filmi sizin de

beğenebileceğiniz kanısına ulaşabilmektedir. Başlangıçta o filmi beğenmeyeceğinizi düşünüseniz bile, Netflix bu sonuca birçok örüntüyü değerlendirerek ulaştığından sizi sizden daha iyi tanır duruma gelmiştir (Say, 2019: 141).

Tüm bu örnekler göz önünde bulundurulduğunda sosyal medyanın insan haklarını ihlal ettiğini söylemek yanlış olmayacaktır. İnsanların gelecekte bugünkünden daha çok, yaşamlarının her anında interneti kullanacakları göz önünde bulundurulursa zamanla veri korumanın çok daha zorlaşacağı aşıkardır.

Facebook gibi sosyal alanlarda son zamanlarda değişik veri toplama yöntemleri ortaya çıkmıştır. İnsanlar buralara veri yüklerken farkında olmadan birçok şeyi kabul edip buna onay vermektedirler ancak bu verilerin nasıl kullanıldığını kontrol etme yetkileri bulunmamaktadır. Örneğin, 2019 Temmuz'da FaceApp adlı bir uygulama ile insanlar, bu uygulamaya fotoğraflarını yükleyip kendilerinin yaşlanmış halini sosyal medyalarında kullanmışlardır. Hem şu anki görünümleri hem de yaşlı halleri veri olarak şirketlerin eline geçmiştir. İleride bunların nasıl kullanılacağı ise belirsiz bir durumdur.

Facebook kullanan insanların sadece neleri beğendiklerinden bile yola çıkılarak yüzlerce veri elde edilebilmektedir. Örneğin, bir kullanıcının %95 oranında ırkını, %85 oranında parti tercihini ve % 88 oranında ise cinsel tercihini tahmin edebilmek için kişinin yalnızca 68 beğenisini değerlendirmek yeterlidir (Say, 2019: 142).

Yukarıda da örnekleri görüldüğü üzere AI sistemleri ile insanlara ait veri kullanımı, bilgi çıkarımı ya da tahmini, tanımlama ve takip, kişileri sıralamak, kategorize etmek ya da değerlendirmek ve en sonda da karar verme işlemleri yapılabilmektedir (Article 19, 2018: 20-21).

3.1.4. Hareket Özgürlüğü Hakkı

Yapay zeka destekli teknolojilerin bir diğer etkilediği insan hakkı da hareket özgürlüğü olarak karşımıza çıkmaktadır. Şöyle ki; AI, uydu görüntülerinden ya da cep telefonları konumlarından kişilerin hareketlerinin ayrıntılı bir resmini çizebilir ve gelecekteki yerini tahmin edebilir. Bu sebeple, devletler tarafından ya da başka bir grup tarafından bireyin hareket özgürlüğü daha kolay kısıtlanabilecektir (AI and Human Rights, 21).

Vatandaşları üzerinde önemli bir bilgi üstünlüğü olan rejimler, ciddi bir tehdit oluşturmadan önce, muhaliflere karşı eylemde bulunabilirler. Bu da muhalefet göstermeyen bireylerin, etkilerini hafifletmek için erken dönemde alıkonulabilecekleri ya da başka bir şeyden mahrum edilebilecekleri, yani rejime karşı çıkmayı düşünen bireyleri uzaklaştıracakları anlamına gelmektedir (Font- Reaulx, 2018: 7). Kısacası muhalefetin protestolar için sahaya çıkma imkanları kısıtlanacaktır.

Özgürlük birçok alanı kendi içinde barındırmaktadır. Otoriter hükümetler sansürü arttırmak için yapay zeka teknolojisini kullanacaklardır. Burada otoriter rejimlerin hepsini ele almak yanlış olacaktır. Çünkü veri kaynakları açısından ülkelerde gerekli olan dijital altyapı sağlanmış olmalıdır. Bu alt yapıların olmadığı ülkelerde bu tür sorunlardan bahsetmek zordur. Dijital altyapının sağlandığı otoriter devletlerde, sansürler din özgürlüğünü zedeleyici şekilde olabilir. Yani insanlar sosyal medyada dini sembollerini gösteremez ya da dini içeriklerini çevrimiçi olarak öğretemezlerse bu doğrudan din özgürlüğünü ihlal edecektir. Bunun dışında; sosyal medyanın örgütlenmelerdeki rolü değerlendirildiğinde, sansürlemeler örgütlenme özgürlüğünü de açık bir şekilde doğrudan tehdit edebilecektir (AI and Human Rights, 23).

3.1.5. İfade Özgürlüğü

İfade Özgürlüğü hakkı, İnsan Hakları Evrensel Beyannamesi (UDHR), ve Uluslararası İnsan Hakları ve Siyasi Haklar Sözleşmesi'nde (ICCPR) ve ayrıca bölgesel insan hakları sözleşmelerinde de garanti altına alınmış haklardandır (Article 19, 2018: 13). İnsan Hakları Evrensel Beyannamesi'nin 19. Maddesi'nde, "Herkesin düşünce ve anlatım özgürlüğüne hakkı vardır", ifadesi yer almaktadır (1948 İnsan Hakları Evrensel Beyannamesi, 2016). Tüm bunların dışında da birçok ülke kendi yasalarında bu hakları güvence altına almıştır.

İfade özgürlüğü demokrasinin bir parçası olması açısından devletler, hesap verebilirlik ve iyi bir yönetişimin sağlanması açısından ifade özgürlüklerini korumak ve bunlara saygı göstermek için her türlü tedbiri almalıdır (Article 19, 2018: 7).

Yapay zekanın genellikle görünmez doğası ile davranışları izleme ve belirleme gücü bir araya geldiğinde, ifade özgürlüğü ciddi anlamda korkutan bir etkiye sebep

olmaktadır. Ayrıca kitlesel gözlemler gizlilik hakkına orantısız bir müdahale olarak karşımıza çıkmaktadır (Article 19, 2018: 10).

İnsanların sürekli izlendiklerini düşünmeleri sonucunda ifade özgürlüğü de tehdit altına girecektir. İzlendikleri düşüncesiyle asıl görüşlerini ifade etmekten kaçınacaklar ve eylemlerinde değişikliğe gitmek zorunda kalacaklardır. Örneğin, yüz tanıma sistemi kamusal alanda protestoda bulunan kişileri belirlemek amacıyla kullanıldığında bu insanları orada bulunmamaya itecektir (AI and Human Rights, 23). İfade özgürlüğü hakkı genellikle sosyal medya ortamlarında önem arz etmektedir. Günümüzde sosyal medya, kamusal tartışmaların olduğu merkezi bir platform haline gelmiştir. Nefret söylemi, yanlış haberler ya da Facebook ve Twitter gibi ortamlarda dolaşan medya manipülasyonu hakkındaki sorunları yasa koyucular, halk ve şirketler gidermeye çalışmaktadırlar (Latonero, 2018: 14).

Yapay zeka algoritmaları çevrimiçi bilgilere ulaşımı ya da bunların ücretsiz olmasını engelleyebilir. Yine devletler de ulusal güvenlik açısından dijital içeriği engelleyip sansürleyebilir. Bu kısıtlama ifade özgürlüklerini zedeleyen faktörler olarak karşımıza çıkmaktadır.

Tüm bunların dışında yapay zekanın dezenformasyon yaratma ve yaymadaki rolü daha önce de değinildiği üzere, adil seçimleri ortadan kaldırmak olarak karşımıza çıkmıştı. ABD 2016 başkanlık seçimleri bunun başlıca örneğidir. Sosyal medya algoritmalarının seçmenleri etkilemesi günümüzde canlı bir örneği karşımıza çıkarmışken bunun gelecekte çok daha farklı boyutları olabilecektir. Seçmenler zamanla seçimlerin meşruiyetine olan inancını yitirecek ve buna bağlı olarak da siyasi katılım azalabilecektir.

Yapay zekanın gizlilik ve ifade özgürlüğü üzerindeki etkileri konusunda; şirketler, politika yapıcılar, sivil toplum örgütleri ya da diğer ilgili kurumlar gerekli çalışmaları yapmalıdırlar.

3.1.6. Çalışma Hakkı

Çalışma hakkı da yapay zekanın etkileyeceği insan haklarından. İşlerin otomasyonu konusunda AI'nın rolü, çalışma hakkı için bir risk oluşturabilecektir. AI bazı kişilerin işgücü piyasasına girmesini engelleyebilir. Ayrıca hem yeni işler ortaya

çıkarması hem de günümüzdeki birçok işi yok edeceği gerçeğiyle işgücü piyasasında çok önemli değişikliklere yol açacaktır (AI and Human Rights, 2018: 26).

Tarih boyunca her yeni teknolojik devrimle birlikte bir istihdam kayması meydana gelmiştir. 21. Yüzyılda da bu kayma yapay zeka ile gündemde yerini almış, iş piyasası değişmiştir. Oxford Üniversitesi'nin yapmış olduğu bir araştırmaya (2016) göre, Amerikan mevcut işlerin % 47' si 2043 yılına kadar otomasyon nedeniyle değişecektir. Bu oran İngiltere'de % 35, Çin'de % 69, Hindistan'da ise %75'lere kadar yükselmektedir. AB Komisyonu ise işlerin %90'ının dijital becerileri ölçüt olarak kullanacağını belirtmektedir (Pavaloiu ve Kose, 2012: 20). Böyle bir ortamda ekonomik eşitsizliklerin olması da kaçınılmazdır. Ancak burada değinilmesi gereken diğer bir nokta da şudur ki, bazı araştırmacılara göre AI teknolojileri ile birlikte yeni iş sahalarının kaybedilenlerden fazla olacağı görüşüdür. Yeni iş sahalarına insanların uyumu için de, eğitim sistemi daha dinamik hale getirilmelidir. Eğitimde yapılandırmacı yaklaşım uygulanarak ezberci eğitimin aksine öğrencilere bilginin nasıl elde edileceği yönünde eğitimler verilmelidir. Aksi takdirde insanlar dijital dünyada çalışma haklarının kaybetme ile karşı karşıya kalacaklardır.

Virginia Dignum “Yapay Zeka Sorumluluğu” adlı makalesinde AI ile birlikte yenilenen, gelecekte karşılaşılabilecek iş durumlarını 4 kategori altında ele almıştır. Bunlardan birincisi; her zamanki işlerdir, yani bu kategoride, teknolojik yenilik daha yüksek üretkenliğe ve daha büyük bir işgücü piyasına yol açacaktır. İkinci alan teknoloji devrimciler kategorisidir. Bu senaryoya göre, AI teknolojileri giderek insanlarla rekabet edecek ve işlerde insanlardan daha fazla rol alacaklardır. Özerk sistemlerin çok daha fazla kullanılması ile önemli ölçüde işsizliğe sebep olacaktır. Üçüncü grup ise, teknoloji utopistlerdir. Buna göre, teknolojik gelişmeler katlanarak ilerleyecek ve fiziksel ürün ve hizmetler neredeyse ücretsiz olacak ve bunun sonucunda da kapitalizm yok olacak görüşüdür. Son senaryo ise, teknoloji kötümserler olarak karşımıza çıkmaktadır. Onlara göre, AI'nın işgücü piyasası üzerindeki olumlu etkisi çok sınırlı olacaktır bu yüzden AI'ya yatırım yapmak yerine mevcut ekonomik zorluklarla mücadele politikaları artırılmalıdır (Dignum, 2017: 2-3).

Günümüzde artık yapay zeka destekli sistemleri iş alanlarında kullanıldığına dair bir örnek ele alınacak olursa 2016 yılında New York'ta bulunan bir hukuk firması;

iflas davalarında kullanılmak üzere, IBM'nin Watson yapay zekasından yararlanarak ROSS adındaki bir programı işe almıştır. Yine 2017 yılında Londra'da yapılan araştırmalar; tahmin etme konusunda yapay zekanın doğru tahmin etme oranlarının insanlarınkinden çok daha fazla olduğunu ortaya koymuştur (Say, 2019: 115).

3.1.7. Sağlık Hakkı ve Yaşama Hakkı

Yapay zekanın her ne kadar sağlık konusunda çok fazla olumlu avantaj sağlayacağı bilinse de sağlık hakkı açısından bazı riskler ortaya çıkarabileceği tartışma konusudur. Şöyle ki, yapay zeka bu konuda ayrımcılığa neden olabilecektir. Örneğin bir AI sistemi, hastanın sigorta durumuna ya da ne kadar para ödediğine bağlı olarak farklı tedaviler önermek üzere tasarlanabilir, ekonomik durumları nedeniyle hayat kurtarıcı tedavileri uygulamayıp daha az kalitede tedavi uygulamaya kodlanabilir (AI and Human Rights 2018: 27).

Günümüzde sağlık ya da tıp alanında; gelişen teknolojinin insan hayatı ve sağlığına ne denli faydalar sağladığı ebedteki göz ardı edilemez. Geliştirilen makineler sayesinde birçok hastalık önceden teşhis edilebilmekte ve ona göre tedaviler uygulanabilmektedir. Ameliyat yapabilen robotların dahi olması bu alandaki faydaları ortaya koyabilecek örneklerdendir. Ancak burada önemli olan bir nokta da yapay zeka destekli programların ya da algoritmaların sağlık alanında bazı riskleri içerdiği meselesidir. Makineler, hastaların ekonomik durumlarına göre tedavi uygulayacak şekilde kodlanabilmektedir. Kodlamalar konusunda yine bir insan söz konusu olmakta ve etik ve ahlaki konular devreye girmektedir.

Yapay zeka sistemlerinin dolaylı da olsa insanların temel hakkı olan yaşama hakkını da tehlikeye sokabileceği durumlar gelecekte söz konusu olabilir. Örneğin, bilgisayara “Dünyadaki insanların yaş ortalamalarını en kolay yoldan yükselt” komutu girildiğinde, bu sistem yeni ilaçlar üretilip bunu sağlayamayacağına göre, en kolay yol olarak yaşlılar dışındaki bütün insanların öldürülmesine karar verebilecektir (Say, 2019: 168). Yalnız burada önemli olan tehlikeli komplo teorileri değildir. Asıl önemli olan bu sistemlerin tasarlanması ve nasıl kodlandığıdır. Girilen bilgiler bütün ihtimaller göz önünde bulundurularak, bütün çözümler dikkate alınarak, etik anlayışa uygun olarak sistemler tasarlanmalı veya yazılmalıdır.

3.2. ULUSLARARASI YENİ İNSAN HAKLARI ÇERÇEVESİ

Yapay zeka teknolojilerinin gelişmesiyle tüm dünyada yeni bir insan hakları çerçevesi oluşturulması gündeme getirilmiştir. Bunlardan ilki yukarıda da değinildiği üzere 16 Mayıs 2018 tarihinde başlatılan, eşitlik ve ayrımcılık konularıyla ilgili olan Toronto Deklarasyonu idi. Bununla ilgili diğer belgeleri ise şu şekilde sıralamak mümkündür:

3.2.1. AB Genel Veri Koruma Yönetmeliği (GDPR)

Genel Veri Koruma Yönetmeliği (GDPR), Avrupa Birliği tarihine girilen en önemli kanunlardandır. Gizlilik düzenlemeleri ve daha önceki zamanlarda yapılan pek çok değişiklikten sonra ortaya çıkan tartışmalar sonucunda oluşturulmuştur. Dünya genelinde gizlilik yasaları ve düzenlemeleri geliştirmek için beklentiler ve kriterler belirler. 25 Mayıs 2018’de yürürlüğe giren bu yönetmelik daha çok ekonomi ile ilgili bir alanı kapsamaktadır (Akıncı, 2017: 13).

Gizlilik geçmişte de olduğu gibi günümüzde de önemli bir endişe kaynağıdır. Dünya sürekli değişen ve gelişen mobil teknolojiler, sosyal medya ve yapay zekanın etkisi altındadır. Bu süreklilik arz eden gelişim de diğer alanlarda olduğu gibi hukuksal alanda da yeni mevzuatların olmasını gerektirmektedir. GDPR de bu amaçlarla ortaya çıkan bir yönetmeliktir. Örneğin, Genel Veri Koruma Yönetmeliğinin 50. Maddesine göre kişisel verileri korumak için uluslar arası işbirliği gereklidir ve bunun gerçekleştirilebilmesi için tartışmalara ve faaliyetlere paydaşlar dahil edilmelidir. (General Data Protection Regulation (GDPR). 99 maddeden oluşan bu yönetmelikte veri korumanın haklarından, iadeler, sorumluluk ve cezalara kadar bir çok konu bu alan dahilinde düzenlenmiştir.

Bu yönetmeliğin amaçları kısacak ele alınacak olursa; (General Data Protection Regulation (GDPR);

- Avrupa genelinde veri gizliliği yasalarını uyumlu hale getirmek
- Tüm AB vatandaşlarının veri gizliliğini korumak ve güçlendirmek
- Bölge genelinde kuruluşların veri gizliliğine yaklaşma şeklini yeniden şekillendirmek.

3.2.2. BM'nin İş ve İnsan Hakları İlkeleri

Birleşmiş Milletler Yüksek Komiserlik İnsan Hakları Bürosu'nun 2011 yılındaki raporuna göre rehber ilkeler belirlenmiş olup, bu rehber ilkeler; ticari faaliyetlerle ilişkili durumlarda ortaya çıkabilecek ve insan haklarını zedeleyebilecek faktörlerin önlenmesi için oluşturulan, uluslararası bir dizi standartlardır. Bu standartlar ile yapay zeka teknolojilerine gönderme yapılmış ve uygulanması gereken ilkeler belirtilmiştir.

Bu ilkelere göre, işletmeler küresel olarak tanınan tüm insan haklarını referans noktası olarak içermelidir. İnsan hakları etkilerinin değerlendirme süreçleri; risk değerlendirmeleri ve sosyal etki değerlendirmeleri gibi süreçlere dahil edilmelidir. İnsan hakları durumları dinamik olduğundan dolayı bu değerlendirmeler düzenli aralıklarla yapılmalı ve hukuksal alanda yeniliklere uyum sağlanmalıdır (Guiding Principles on Business and Human Rights, 2011: 20).

3.2.3. Avrupa Konseyi Adaletin Etkinliği İçin Avrupa Komisyonu (CEPEJ)

Avrupa Konseyi Adalet Verimliliği Avrupa Komisyonu 2002 yılında kurulmuş, üye devletlerdeki yargının verimliliği ve işleyişini etkinleştirmek için raporlar sunan ve yapay zeka tekniklerinin kullanımı ile ilgili olan etik ilkeleri belirleyen Avrupa metnini benimsemiştir (European Commission for the Efficiency of Justice (CEPEJ, 2019). CEPEJ'in iki temel amacı bulunmaktadır. Bunlar; Avrupa Konseyi üye ülkelerin adalet sisteminin verimlilik ve işleyişini geliştirmek ve Avrupa Konseyi'nin ulusal alanda adalet etkinliği için yasal araçların daha faydalı şekilde kullanılmasını sağlamaktır (Eupore's Human Rights).

Yargı sistemleri ve bu konu ile ilgili çevrelerde yapay zekanın kullanılabilirliğine dair, 2018 yılının "Avrupa Etik Şartı" kabul edilmiştir. Bunun ardından, CEPEJ Avrupa Etik Şartı İlkelerini referans alarak yapay zeka sistemlerinin sertifikalandırılması projesini ortaya koymuştur. Avrupa Etik Şartına göre belirlenen temel ilkeler şu şekildedir (Yılmaz, 2020: 30).

1. *Temel haklara saygı ilkesi:* Yapay zeka teknolojilerinin temel haklara uyumlu olmasını sağlama amacını taşımaktadır.

2. *Ayrımcılık yapmama ilkesi:* insanlar ya da gruplar arasında herhangi bir ayrımcılığın gelişmesini önlemek.
3. *Kalite ve güvenlik ilkesi:* Yargı kararları ve verilerinin işlenmesinde, güvenli teknolojik ortamda sertifikalı kaynakların kullanımını öngörmektedir.
4. *Şeffaflık ve tarafsızlık ilkesi:* Veri işleme yöntemlerinin açık olması ve denetimlerine izin verilmesi anlamına gelmektedir.
5. *Kullanıcı Kontrolü Altında İlkesi:* Kuralcı yaklaşımı engeller ve kullanıcıların bilgili aktörler olmasını ve yapılan seçimlerin kontrollü sağlar.

Yapay zeka ile ilgili çalışmalar yapmak ve etik kuralları belirlemek için Haziran 2018’de 52 uzmanın bulunduğu Yapay Zeka Uzmanlık Grubu (AI HLEG) da önemli bir kuruluş olarak karşımıza çıkmaktadır. Bu grubun temel amacı Avrupa Yapay Zeka stratejisinin uygulanmasını desteklemek olup geleceğe ilişkin politika geliştirme ve sosyo-ekonomik zorluklar da dahil olmak üzere yapay zeka ile ilgili etik, yasal ve toplumsal konularda tavsiyelerin hazırlanmasını kapsamaktadır (Smuha, 2019).

Veri İnavasyyon Merkezinin (The Center for Data Innovation) raporuna göre bu alandaki çalışmaların genel amacı, AI'nın risklerini en aza indirirken faydalarını en üst düzeye çıkaran “güvenilir AI” sistemlerinin nasıl uygulanacağı ve faaliyete geçirileceği konusunda somut rehberlik sağlamaktır (Castro).

SONUÇ

Teknoloji ve insan ilişkisi tarihin her aşamasında önem arz etmiş olup 21. yüzyılın da en önemli konularından biri haline gelmiştir. Sanayi devriminden sonra günümüzde insanlık “Endüstri 4,0” terimi ile ve buna bağlı olarak “Yapay Zeka” kavramı ile karşı karşıyadır.

Günümüze kadar teknoloji, geliştiği her keskin noktada insan hayatını derinden etkilemiş ve dönüşümlere sebep olmuş ancak bu güne kadar insan hakları açısından bu kadar tartışılan bir konu olmamıştır. Yapay zeka teknolojilerinin bir devrim niteliğinde olması ve bireylerin tüm yaşamlarını bu teknolojilere bağlı olarak yaşaması ve şekillendirmesi, insan haklarını gelişen teknoloji karşısında korunması gereken bir duruma sokmuştur. Sadece bireyler değil ülkeler bazında da yapay zeka destekli teknolojilerin hızla kullanılmaya başlanmasıyla gerek etik ve ahlaki açıdan, gerekse uluslararası hukuk açısından bir çok problem teşkil eden durum ortaya çıkmıştır.

Çalışmada, yapay zeka teknolojilerinin tüm dünya ekseninde; savunma, savaş, kamu, tıp, eğitim gibi her alanda kullanılmasının insan hakları açısından yaratacağı problemlere yönelinmiştir.

İnsan Hakları kavramının temelinde, en önemli canlı kabul edilen “insanın” korunması amacı yatmaktadır. Yani insan haklarının ardında insanoğlunun hiyerarşik üstünlüğü düşüncesi vardır. Bu nedenle insanlara vazgeçilmez, devredilmez ve zamanaşımına uğramaz haklar tanınmıştır. İnsan haklarının tarihine kısaca değinilecek olursa; 1215 Magna Carta, 1789 İnsan ve Yurttaş Hakları ile önem kazanan süreç 1948 İnsan Hakları Evrensel Bildirgesi ile devam etmiş ve ardından gelen 1953 Avrupa İnsan Hakları Sözleşmeleri (AİHS) ile insan hakları korunmaya çalışılmıştır. 1789 İnsan ve Yurttaş Hakları Bildirgesinde; İnsanların yaşama, özgürlük ve mülkiyet haklarının doğuştan geldiği kabul edilmekte ve bunların doğal haklar olduğu belirtilmektedir. Avrupa devletleri ve BM’in yanı sıra birçok ülkede de insan hakları konusunda yasal düzenlemeler mevcut olup ülkeler uluslararası ve ulusal olarak insan haklarını korumaya çalışmaktadır.

İnsan Hakları gelişen teknoloji ve buna bağlı olarak değişimlerden ve dönüşümlerden bağımsız olarak değerlendirilemez. Yapay zeka hayatlarımızda giderek daha fazla yer almakta ve artık bireyler karar alma yetkisini bile makinelere devretme

noktasına gelmektedir. Yapay zeka destekli; nanoteknoloji, biyoteknoloji, bilgi teknolojisi ve bilişsel yakınsama bilimlerin ve yeni teknolojilerin uygulamalarının insanlığa büyük katkılar sağlamasına karşın insan hakları açısından büyük sorunlar ortaya çıkaracağı tartışılmaktadır.

Bugün gelinen noktada çalışmada da detaylı olarak ele alınan, yapay zekanın alt kolları olan makine öğrenmesi ve derin öğrenme sistemleri ile çalışan makine ya da bilgisayarların bir çok bilişsel işlemi insan uzmanlardan daha kısa sürede, daha kolay ve verimli yapabildiği, daha doğru sonuçlar ortaya koyabildiği görüşü vardır. Bu teknolojilerin hızla her alana yayılması ile insan ve makineler arasındaki sınırların netliği ortadan kalkmış olacaktır.

Yapay zekanın sebep olabileceği insan hakları ihlallerinin kontrol altına alınabilmesi için uluslararası ve ulusal anlamda hukuki düzenlemelere ihtiyaç vardır. BM’in, Avrupa Konseyi Parlamenterler Meclisinin, AB’nin ve Uluslararası Af Örgütü gibi kurumların yapay zekanın insan haklarına uyarlanması konularında raporları ya da çalışmaları bulunmaktadır. Bu çalışmaların ortak amacı; Yapay zekalı teknolojilerin insan haklarına uyum sağlaması ve bu anlamda insan yaşamının ve onurunun korunması için gerekli tedbirlerin alınması olarak karşımıza çıkmaktadır.

Yapay zekanın üzerinde risk oluşturabileceği insan haklarını; yaşama hakkı, eşitlik ve ayrımcılık yapmama hakkı, kişisel özgürlükler hakkı, gizlilik ve mahremiyet, hareket özgürlüğü, ifade özgürlüğü, çalışma hakkı ve sağlık hakkı olarak sıralamak mümkündür.

Temel insan haklarından olan “yaşama hakkı”; bilgisayarlara verilen bazı komutlar doğrultusunda, verilen komutları çok daha farklı yorumlayıp, duygulara sahip olmamasından dolayı ölümlere sebep olabilecektir. Üzerinde durulacak olan insan haklarını birbirinden bağımsız düşünmemek gerekmekte ve yapay zekanın bu haklar üzerindeki etkileri ele alınırken de birbirleriyle bağlantılı olduğu unutulmamalıdır.

Yapay zekanın “ayrımcılık yapmama” hakkı ile ilgili en önemli belge “Toronto Deklarasyonu” olarak karşımıza çıkmaktadır. Uluslar arası Af Örgütü’nün hazırlamış olduğu bu deklarasyon, makine öğrenme ve derin öğrenme sistemlerinin ayrımcılık yapmaması gerektiğine ve eşitlik ilkesine odaklanmaktadır. Bu anlamda küresel çapta çalışmaların olması önem arz etmektedir. Örneğin yüz tanıma sistemlerinde, siyahiler

için toplumda var olan önyargıların algoritmalara aktarılması yani ayrımcı algoritmaların kullanılmasıyla birçok insan hak kaybına uğrayabilecektir.

Günümüzde neredeyse bütün bireylerin hayatlarını telefonlar ya da bilgisayar ile geçirdikleri ve sosyal medyayı aktif olarak kullandıkları düşünüldüğünde milyonlarca verinin oluşması kaçınılmaz hale gelmiştir. Bu noktada da “gizlilik ve mahremiyet hakkı” söz konusu olmakta ve insanlar farkında olmadan işlenen veriler sayesinde bütün gizli kalması gereken bilgiler ortaya çıkarılabilmektedir.

Yapay zeka teknolojilerinin izleme, görüntü kaydetme, tanıma, takip etme gibi yetenekleri göz önünde bulundurulduğunda ve uydu sistemlerinde ya da telefonlarda bunların kullanılmasıyla insanların “hareket özgürlüğü hakkı” ülkeler ya da farklı gruplar tarafından birey farkında olmadan sınırlandırılabilir.

Bir çok uluslar arası sözleşme ile garanti altına alınmaya ve korunmaya çalışılan “ifade özgürlüğü hakkı” da yapay zekanın getirilerinden olumsuz etkilenebilecek haklardanır. Hareket özgürlüğü hakkında olduğu gibi yapay zeka teknolojilerinin davranışları izleme ve kişileri tanıyabilme özellikleri ifade özgürlüğü üzerinde ciddi tehditlere yol açabilecektir. İnsanlar izlendiklerini bilmeleri durumunda asıl görüşlerini açıklamaktan kaçınacaklardır.

Tarihin her döneminde her yeni teknoloji insanların alışkın olduğu çalışma ortamını değiştirmiştir. Sanayi devriminde olduğu gibi yapay zeka teknolojisinin gelişmesiyle bir çok iş; daha kısa sürede, daha verimli olması açısından insanlardan alınıp makinelerle devredilmektedir. Günümüzde hukuk alanından eğitim alanına kadar her iş kolunda yapay zekanın hızla kullanılmaya başlaması söz konusudur. Geline nokta artık yapay zeka destekli programlar bazı hukuk davalarına bile bakabilmektedir. Böylece bireylerin “çalışma hakkı” üzerinde bir kısıtlama meydana gelebilecektir. Sanayi devriminden sonra fabrikalarda insan gücüne duyulan ihtiyaç azalmıştı. AI ile birlikte ise insan gücüne sadece kodlamalar yapmak, programlar yazmak amacıyla ihtiyaç duyulacaktır. Yeni teknolojilerin oluşması bilgisayar ya da yazılımlar ile ilgili birçok yeni iş alanı da ortaya çıkarmaktadır. Ancak yeni iş kollarında bireylerin istihdam edilebilmesi; bu alanlara adapte olmaları ya da gerekli eğitimi almalarına bağlı olup ülkeler ulusal ya da uluslararası alanda bu konu ile ilgili

alıřmalar yapmalıdır. Aksi takdirde insanların alıřma haklarının ellerinden alınması sz konusu olacak ve ekonomik eřitsizlikler ortaya ıkacaktır.

İnsan hakları aısından nem arz eden bir diğerkonu da yapay zeka teknolojilerinin savař, savunma, siber gvenlik ve istihbarat alanlarında yaygın olarak kullanılmaya bařlanmasıdır. Bu yeni teknolojiler gerek Uluslararası İnsancıl Hukuk (IHL) gerekse Uluslararası İnsan Hakları Hukuku (IHRL) aısından byk arz etmektedir. Hukuksal anlamda en ok nem tařıyan konuların bařında “zerk silah sistemleri” (Autonomous weapon systems) gelmektedir. zerk silah sistemlerini kısaca; dngnn ilk ařamasında, sistemin etkinleřtirilmesinde insanın bulunduğuanca sonrakiařamalarda insanın dng dıřında tutulduğuve birok iřlemin makinelere bırakıldığısistemler olarak tanımlamak mmkndr. Bu sistemlerin kullanılması ile savařın etik ve ahlaki boyutunun dıřına ıkılıp ıkılmayacağı tartışma konusudur.

Uluslararası rgtler, sivil toplum kuruluřları ve uzmanlar zerk silah sistemlerinin otonomi dereceleri ile ilgili sınıflandırmalar ve alıřmalar yapmaktadırlar. Bu sistemler otonom ya da yarı otonom řeklinde sınıflandırılabilir. İnsan hakları ile ilgili kuruluřlar bu sistemlerin kullanımının sınırlandırılması ya da yasaklanmasını rapor ederken bazı lkeler ise geliřtirilmesiyle ilgili ağırda bulunmakta olup grř ayrılıkları meydana ıkmaktadır. Uluslararası insancıl hukukta, savařlarda sivillerin korunması temel ama olup otonom silah sistemlerinin etik ve ahlaki aıdan kurallara uymadığıdurumlarda sivillerin, sağık personelinin vs. zarar grmesi durumları sz konusudur. İnsancıl hukukun ayırım, orantılılık ve askeri gereklilik ilkeleri bu sistemler ile zarar grebilecektir, Kullanılan sistemler siviller ile askerler arasındaki ayırmı yapabilmelidir. Yani kısaca sylenabilir ki; bu sistemler savař etiğine uygunluk derecesine gre kullanılmalıdır ancak bunu insancıl hukuka uyarlamak basit değıldir. nk bu sistemlerin kullanıldığıdurumlarda, alıřmada da detaylı olarak ele alındığızere sorumluluk noktasında da problemler ortaya ıkmaktadır.

Grldğzere değıřen tm bu paradigmar, uluslararası alanda yeni bir insan hakları erevesinin oluřumunu gndeme getirmiřtir. Toronto Deklarasyonu bařta olmak zere; AB Genel Veri Koruma Ynetmeliğı, BM’nin İř ve İnsan Hakları İlkeleri, Avrupa Konseyi Adaletin Etkinliğı İin Avrupa Komisyonu raporları, bu alanda son

yıllarda ortaya konan alıřmalar olup, temel ve ortak amaları yapay zekanın siyasi, ekonomik ve sosyal anlamda getireceėi riskleri ya da tehditleri ortadan kaldırmaktır.

Gelecekteki sonuların sadece etik kurullar veya arařtırma blmleri tarafından deėil, aynı zamanda ilk ařamada hkmet, endstri, uluslararası kurumlar ve kuruluřlar tarafından da gz nnde bulundurulması gerekir. AI dostu bir ortamın oluřturulması ve srdrlmesi iin sorumluluk kltrnn kresel lekte geliřtirilmesi gerekmektedir.



KAYNAKÇA

- 1948 *İnsan Hakları Evrensel Beyannamesi*. <http://www.multeci.org.tr/wp-content/uploads/2016/12/Insan-Haklari-Beyannamesi-1.pdf> (25.06.2019).
- Adalı, E. (2017, Ocak, Mart). *İnsanlaşan Makinalar ve Yapay Zeka*. *İstanbul Teknik Üniversitesi Vakfı Yayını* (75). https://www.ituvakif.org.tr/dergi/sayi_75.pdf (27.03.2019).
- Alkan, M. A. (2019). *Makine Öğrenimi Nedir?* http://www.siskon.com.tr/dosya/PDF/Makale/Makine_Ogrenimi_Machine_Learning.pdf (02.03.2020).
- Barut, H. Avşaroğlu, O. vd. (2017), *Antalya Firmalarına Yönelik Endüstri 4.0 Durum Tespiti, Ölçeğin Geliştirilmesi ve Pilot Uygulama Projesi*. Antalya Ticaret ve Sanayi Odası. atso.org.tr/yukleme/dosya/00d72dbb10e71180bc5c962_131ffb546.pdf (14.08.2020).
- Article 19, Privacy and Freedom of Expression In the Age of Artificial Intelligence, April 2018.
- Askeri Yürüyüş Asistanı. (T.Y). ASELSAN: https://www.aselsan.com.tr/Askeri_Yuruyus_Asistani_1242.pdf (25.06.2019).
- *(2014). *Autonomous Weapon Systems Technical, Military, Legal and Humanitarian Aspects*. Expert meeting, Geneva, Switzerland.
- Aydın , C. (2019). Sosyal Medyanın Ulusal Güvenliğe Etkisi. *M5 Ulusal Güvenlik, Savunma ve Strateji Dergisi, Savunma Sanayiinde Yeni Bir Aktör Yapay Zeka*, 44 (331): 68.
- Ayu, P., Indria, T., Sueb, & Thohari, H. (2013). *The Development of Technology For Human Civilization*. [file:///C:/Users/Acer/Downloads/developmentof technology forhumanANartikeldenganHamimProceedingBasicUBApril2013.pdf](file:///C:/Users/Acer/Downloads/developmentof%20technology%20forhumanANartikeldenganHamimProceedingBasicUBApril2013.pdf) (06.12.2018).
- Batı, U. ve Yılmaz, T. (2019, Şubat). Yapay Zekalar Savaş Meydanında İnsanların Yerini Alacak Mı? *M5 Ulusal Güvenlik, Savunma ve Strateji Dergisi, Savunma Sanayiinde Yeni Bir Aktör Yapay Zeka* 44(331): 26-29.
- Berkowitz, B. (2008). *The R&D Future of Intelligence*. <https://issues.org/berkowitz-3/> (18.06.2019).

- (2005). *BM 2005 Dünya Robotik Bilim Raporu*. <https://books.google.com.tr/books?id=4B6Ei1y4WbcC&printsec=frontcover&hl=tr#v=onepage&q&f=false> (21.03.2020)
- Boothby, W. (2012). Some Legal Challenges Posed By Remote Attack. *International Review Of The Red Cross*, 94(886).
- Bozkurt Yüksel, A. E. (2017, Ocak). *Robot Hukuku*. *Dergipark* (29). https://www.academia.edu/32452626/ROBOT_HUKUKU_Robot_Law (25.12.2018).
- Brundage, M., Avin, S., Clark, J., Toner, H., & Eckersley, P. (2018). *Cambridge Raporu*. <https://arxiv.org/ftp/arxiv/papers/1802/1802.07228.pdf> (20.12.2018).
- Buckley, J. (2018). *British Army Set To Carry Out Its Largest Test Of Robots During Simulated Battles In Project Known As "Autonomous Warrior"*. <https://www.dailymail.co.uk/news/article-6378511/British-Army-set-carry-largest-test-robots-simulated-battles.html> (18.11.2019).
- Castro, D. (T.Y). *Recommendations To The Eu High Level Expert Group On Artificial Intelligence On Its Draft Ai Ethics Guidelines For Trustworthy Ai*. Center For Data Innovation: <https://www2.datainnovation.org/2019-hleg-ai.pdf> (26.10.2019).
- Chengeta. (2016). *Uluslararası Hukuk ve Siber Güvenlik*. Mart 3, 2019 tarihinde <file:///C:/Users/Acer/Desktop/kaynak%C3%A7ammm/CHENGETA,%20uluslararası%C4%B1%20hukuk%20ve%20siber%20g%C3%BCvenlik.pdf> (12.09.2018).
- Copeland, B. J. (2016). *Artificial Intelligence*. <https://www.britannica.com/technology/artificial-intelligence> (19.04.2020).
- Corera, G. (2017, Haziran 16). *Facebook'un Terörle Mücadele Aracı: Yapay Zeka*. <https://www.bbc.com/turkce/haberler-40301067> (12.05.2019).
- Crawford, C. (2017). The Impact of Artificial Intelligence on Autonomous Cyber Defense. *In Partial Fulfillment Of The Requirements for the Degree of Master of Science in Cybersecurity*. <https://www.proquest.com/openview/154afe40506d09a05d21cd4627a8a216/1.pdf?pq-origsite=gscholar&cbl=18750> (20.05.2019).
- Çıtak, E. (2019). İstihbarat ve Teknoloji. *M5 Ulusal Güvenlik, Savunma ve Strateji Dergisi, Savunma Sanayiinde Yeni Bir Aktör Yapay Zeka* 44(331): 34-37.

- Dağıtmaç, M., & Özbay, O. (2018). *Dijital Haçlı Seferleri*. İstanbul: Motto Yayınları.
- Davidson, K. (2019, Mayıs 29). *CIFAR. AI Futures Policy Labs engage policy leaders in understanding the future policy implications of AI*: <https://cifar.ca/cifarnews/2019/05/29/ai-futures-policy-labs-engage-policy-leaders-in-understanding-the-future-policy-implications-of-ai/> (12.08.2020).
- Davison, N. (T.Y). A Legal perspetcive: Autonomous Weapon Systems Under International Humanitarian Law. file:///C:/Users/Acer/Downloads/ autonomous_weapon_systems_under_international_humanitarian_law%20(1).pdf (25.03.2019).
- Demirezen, U. (2019). İstihbarat ve Yapay Zeka: Siber Dünyada Teknik Bir Değerlendirme. *M5 Ulusal Güvenlik, Savunma ve Strateji Dergisi, İstihbarat Teknolojileri* 44 (337): 28-21.
- Dignum, V. (2017). *Responsible Artificial Intelligence: Designing Ai for Human Values*. <http://dspace.library.daffodilvarsity.edu.bd:8080/bitstream/handle/20.500.11948/2177/itu2017-1.pdf?sequence=1&isAllowed=y> (03.01.2019),
- Erkan, K. (2019, Eylül). Askeri İstihbarat Alanında Açık Kaynak İstihbaratı. *M5 Ulusal Güvenlik, Savunma ve Strateji Dergisi, İstihbarat Teknolojileri*, 44(337): 22-26.
- ERSOY, Ç. (2020). *Robotlar, Yapay Zeka ve Hukuk* (Cilt 5. Baskı). İstanbul: Oniki Levha Yayıncılık.
- Espada, & Hortal. (2013). *Revista del Instituto Español de Estudios Estratégicos*. file:///C:/Users/Acer/Desktop/Dialnet-SistemasDeArmasAutonomasDronesY Dere choInternaciona-4537251_2.pdf (04.02.2020).
- Eupore's Human Rıgts*. (T.Y). *Efficiency of Justice (CEPEJ)*: <https://www.euro-pewatchdog.info/en/instruments/expert-bodies/efficiency-of-justice-cepej/> (05.05.2020).
- European Commission for the Efficiency of Justice (CEPEJ)*. (2019, Eylül). *Artificial intelligence in justice systems*, <https://www.coe.int/en/web/cepej/artificial-intelligence-in-justice-systems> (20.03.2020).

- Font Reaulx, P. (2018). *AI: The Consequencen For Human Rights Initial Findings On The Expected Future Use Of AI In Authoritarian Regimes*. <https://humanrightscommission.house.gov/sites/humanrightscommission.house.gov/files/documents/FHI%20-%20Artificial%20Intelligence%20the%20Consequences%20for%20Human%20Rights.pdf> (30.05.2019).
- General Data Protection Regulation (GDPR)*. (T.Y). General Data Protection Regulation (GDPR): <https://gdpr-info.eu/> (25.07.2020).
- Glowacki, M., & Dudka. (2012). *Book Review: The Thir Industrial Revolution: How Lateral Power Is Transformin Energy, the Economy and the World*. file:///C:/Users/Acer/Downloads/Book_Review_The_Third_Industrial_Revolution_How_La.pdf (26.08.2019).
- Gökçe, M. (T.Y). *Teknoloji ve İnsan*. [file:///C:/Users/Acer/Downloads/ Teknoloji_ve_Insan.pdf](file:///C:/Users/Acer/Downloads/Teknoloji_ve_Insan.pdf) (26.03.2019).
- Görz, G., & Nebel, B. (2005). *Yapay Zeka*. İstanbul: İnkılap Kitabevi.
- Gregg , B. (2018, October). *The Coming Political Challenges of Artificial Intelligence*,. <https://www.researchgate.net/publication/327890407> (27.09.2018).
- Guiding Principles on Business anda Human Rıghts (2011). New York and Geneva . Guiding Principles on Business anda Human Rıghts: https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf (21.09.2019).
- Günay, D. (2002 Ocak,). Sanayi ve Sanayi Tarihi. *Mimar ve Mühendis Dergisi*, 8-14. https://www.researchgate.net/publication/317662230_Sanayi_ve_Sanayi_Tarihi (25.01.2020).
- Gürçan, B. (2017, Ekim, Kasım, Aralık). *Geleceği Yapay Zeka Şekillendirecek*. (03), 18. <https://www.yildizteknopark.com.tr/kataloglar/techstar-18.pdf> (12.05.2020)
- Human Rights In The Age Of Artificial Intelligence*. (2018, November). Accessnow: <https://www.accessnow.org/cms/assets/uploads/2018/11/AI-and-Human-Rights.pdf> (12.02.2020).

- Jean, & Le Deaut , Y. (2017). *Teknolojik Yakınsama, Yapay Zeka ve İnsan Hakları Raporu*. <https://ccdcoe.org/uploads/2019/09/CoE-170428-Recommendation-on-technological-convergence-AI-and-human-rights.pdf> (26.04.2019).
- Kagerman, H., Wahlster, W., & Helbig, J. (2013). Recommendations for Implementing the Strategic Initiative Industrie 4.0. *ACATECH*. <https://www.din.de/blob/76902/e8cac883f42bf28536e7e8165993f1fd/recommendations-for-implementing-industry-4-0-data.pdf> (08.09.2019).
- Kane, A. (2013). *Killer Robots and The Rule of Law*. https://www.huffpost.com/entry/killer-robots-and-the-rul_b_3599657 (28.04.2019).
- Karaağaç , C. (2016). *Yol Sistemleri Haritası*, https://www.stm.com.tr/documents/file/Pdf/6.%C4%B0ha%20Sistemleri%20Yol%20Haritasi_2016-08-03-10-57-57.pdf (05.08.2019).
- Kılıç, S. ve Alkan, R. M. (2018). *Dördüncü Sanayi Devrimi Endüstri 4.0: Dünya ve Türkiye Değerlendirmeleri. Girişimcilik İnavasyon ve Pazarlama Araştırmaları Dergisi*, 29-49. <https://dergipark.org.tr/tr/download/article-file/483496> (17.06.2020).
- Kott, A. (2018). *Challenges and Characteristics of Intelligent Autonomy for Internet of Battle Things in Highly Adversarial Environments*. <https://arxiv.org/ftp/arxiv/papers/1803/1803.11256.pdf> (19.05.2019).
- Kritikos, M. (2019, Nisan 16). *Does artificial intelligence threaten human rights?* <https://epthinktank.eu/2019/04/16/does-artificial-intelligence-threaten-human-rights/> (05.05.2020).
- Latonero, M. (2018). *Governing Artificial, Upholding Human Rights And Dignity*. California. https://datasociety.net/wp-content/uploads/2018/10/DataSociety_Governing_Artificial_Intelligence_Upholding_Human_Rights.pdf (16.04.2020).
- Lidestri, N. (2018). *The Impact of Artificial Intelligence In Cybersecurity*. A Capstone Project Submitted To The Faculty Of Utica College, (Yayınlanmış Yüksek Lisans tezi), A Capstone Project Submitted To The Faculty Of Utica College, New York.
- Marr, B. (2018, Mayıs 21). *How Much Data Do We Create Every Day?* . <https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we->

create-every-day-the-mind-blowing-stats-everyone-should-read/#40804dab60ba (17.06.2019).

Melendez, S. (2018). *The Rise Of The Robots: What The Future Holds For The World's Armies*. <https://www.fastcompany.com/3069048/where-are-military-robots-headed> (14.07.2020).

Moore, S. K. (2017, November 21). *DARPA Seeking AI That Learns All the Time*. <https://spectrum.ieee.org/darpa-seeking-ai-that-can-learn-all-the-time> Öymen , E. E. (2017). *Ekonomi Politika Dünya. Cinayet Tanığı Robot . Cinayet Tanığı Robot*: <https://www.dunya.com/kose-yazisi/cinayet-tanigi-robot/346781> (27.12.2019)

Özdoğan, O. (2017 İstanbul). *Endüstri 4.0 Dördüncü Saniye Devrimi ve Endüstriyel Dönüşümün Anahtarları. Yeni Ufuklar Dizisi Pusula*. https://books.google.com.tr/books?hl=tr&lr=&id=zkttdwAAQBAJ&oi=fnd&pg=PR5&dq=end%C3%BCstri+4.0+akademik+makale&ots=8B9kxDWLdL&sig=4p_A2UejFrrceykjWXI4opd-H0&redir_esc=y#v=onepage&q&f=true (25.11.2019).

Özer, A. (2019, Şubat). Otonom Silah Sistemleri ve Uluslararası İnsancıl Hukuk. *M5 Ulusal Güvenlik, Savunma ve Strateji Dergisi, Savunma Sanayinde Yeni Bir Aktör Yapay Zeka* 44(331): 30-32.

Özer, Y. (2019, Eylül). Askeri İstihbarat ve Teknoloji. *M5 Ulusal Güvenlik, Savunma ve Strateji Dergisi, İstihbarat Teknolojileri* 44(337): 28-35.

Papadapoulos, L. (2018, Mayıs 3). *China Plans to Equip Airports with AI Body Scanners Developed by Weapons Lab*. <https://interestingengineering.com/china-plans-to-equip-airports-with-ai-body-scanners-developed-by-weapons-lab> (25.07.2019).

Pathak, R., & Sing, V. (T.Y). Computer Engineering Department . *Impact of Technology on Human Life*.

Pauli , E. A., & Ünür, M. (2017,). Dördüncü Sanayi Devrimi ve Getirecekleri. *Bebka Haber Dergisi*(23 Temmuz, Ağustos, Eylül). <https://docplayer.biz.tr/69229566-4-sanayi-devrimi-atilim-icin-onemli-bir-firsat.html> (12.05.2020).

- Pavaloiu, A., & Kose, U. (2012). Ethical Artificial Intelligence- An Open Question. *Journal of Multidisciplinary Developments*, 15-27. <https://arxiv.org/ftp/arxiv/papers/1706/1706.03021.pdf> (12.08.2020).
- Petman, J. L. (2017). *Autonomous Weapons Systems And International Humanitarian Law: "Out Of The Loop"?* https://um.fi/documents/35732/48132/autonomous_weapon_systems_an_international_humanitarian_law__out_of_the/c0fca818-3141-b690-0337-7cfccbed3013?t=1525645981157 (14.11.2019).
- Rajpurohit, L., & Verma, A. K. (2016, March). International Journal of Advance Engineering and Research. *Industrie 4.0: An Overview*(3). file:///C:/Users/Acer/Downloads/Industrie4.0AnOverview-48786.pdf (15.05.2020)
- Risse, M. (Nisan, 2018). *Human Rights and Artificial Intelligence An Urgently Needed Agenda*. CARR İnsan Hakları Politikası Merkezi. file:///C:/Users/Acer/Downloads/RWP18-015_Risse%20(1).pdf (18.09.2019).
- Rose, K., Eldridge, S., & Chapin, L. (2015). *The Internet Of Things: An Overview Understanding The Issues and Challenges of A More Connected World*. <https://www.internetsociety.org/wp-content/uploads/2017/08/ISOC-IoT-Overview-20151221-en.pdf> (16.04.2020).
- Sanchez, I. M. (T.Y.). [https://eda.europa.eu/webzine/issue14/cover-story/defence-internet-of-things-\(diot\)](https://eda.europa.eu/webzine/issue14/cover-story/defence-internet-of-things-(diot)), (15.02.2021).
- Say, C. (2019). *Yapay Zeka* (12 baskı), İstanbul: 7 Renk Basım Yayın ve Filmcilik Ltd. Şti.
- Say, C. (2018, Kasım 28). *Geleceğin Zekası, Önyargısız Robotlar*. https://www.youtube.com/watch?v=dCQt3cA_VA, (03.04.2021).
- Schmitt, M. N., & Thurnher, J. S. (2013). *"Out of the Loop": Autonomous Weapon System and the Law of Armed Conflict*. <https://harvardnsj.org/wp-content/uploads/sites/13/2013/01/Vol-4-Schmitt-Thurnher.pdf> (25.06.2019).
- Seren, M. (2019). İstihbarat Toplama Disiplinleri. *M5 Ulusal Güvenlik, Savunma ve Strateji Dergisi İstihbarat Teknolojileri* 44(337): 10-17.

- Sharkey. (2012). *The evitability of autonomous robot warfare*, <https://e-brief.icrc.org/wp-content/uploads/2016/09/23.-The-evitability-of-autonomous-robot-warfare.pdf> (15.04.2019).
- Smith, M. L., & Neupane, S. (2018, Nisan). *Artificial Intelligence Human Development*. https://www.idrc.ca/sites/default/files/ai_en.pdf (25.06.2019).
- Smuha, N. (2019). *A definition of AI: Main capabilities and scientific disciplines*. European Commission. https://ec.europa.eu/futurium/en/system/files/ged/ai_hleg_definition_of_ai_18_december_1.pdf (20.06.2019).
- Taghizadeh, K. (2015, Kasım). *Sanayi 4.0 Dördüncü Sanayi Devrimi, Yarının Fabrikaları Neye Benziyor?* <https://home.kpmg/content/dam/kpmg/tr/pdf/2016/08/tr-sanayi-4.PDF> (05.11.2019).
- The Toronto Declaration: Protecting the rights to equality and non-discrimination in machine learning systems*. (2018, Mayıs 16). accessnow: <https://www.accessnow.org/the-toronto-declaration-protecting-the-rights-to-equality-and-non-discrimination-in-machine-learning-systems/> (17.05.2020)
- Ünver, A. (2018, Temmuz). *Cyber Governance and Digital Democracy 2018/9*. https://edam.org.tr/wp-content/uploads/2018/07/AKIN-Artificial-Intelligence_Bosch-3.pdf (03.08.2019).
- Vilmer, (2015, Mart). *Terminator Ethics: Should We Ban “Killer Robots”?* <https://www.ethicsandinternationalaffairs.org/2015/terminator-ethics-ban-killer-robots/> (22.02.2020).
- Vincent, J. (2017, September 4). *The Russian President Warned That Artificial Intelligence Offers ‘Colossal Opportunities’ As Well As Dangers*. <https://www.theverge.com/2017/9/4/16251226/russia-ai-putin-rule-the-world> (19.06.2019).
- Virginia, D. (T.Y). *Responsible Artificial Intelligence: Designing AI For Human Values* <http://dspace.library.daffodilvarsity.edu.bd:8080/bitstream/handle/20.500.11948/2177/itu2017-1.pdf?sequence=1&isAllowed=y> (17.08.2019).
- Vreskala, T. N. (2019, Nisan 14). *Kadıköy Idea*. Youtube: <https://www.youtube.com/watch?v=BseebXWKn0k> (14.02.2020).

- Wassell, P. (2018, Nisan 27). *3 Military Applications of The Internet of Things*.
<https://www.augmate.io/3-military-applications-of-the-internet-of-things/>
(15.03.2019)
- Yarman, F. A., & Denemeç, R. (2016). *Dünya ve Türkiye'de Sanayi Devrimleri, Dijital Çağ: Dün, Bugün, Yarın*. http://www.yeniturkiye.com/Conference2016/Present/1_1_1_4_Reha_Denemec-FarukAga_Yarman.pdf (26.08.2020).
- Yılmaz, G. (2020). *Marmara Avrupa Araştırmaları Dergisi*, 28(1), 27-55 .
- Yüksel, B. (T.Y). *Robot Hukuku*. https://www.academia.edu/32452626/ROBOT_HUKUKU_Robot_Law (24.05.2019).



DİZİN

-A-

Açık Kaynak İstihbaratı, 60, 61
 Adalet, 47
 Algoritmalar, 3, 5, 12, 22, 24, 26, 28,
 30, 40, 49, 52, 53, 56, 58, 62, 84, 87
 Artificial İntelligence, 18, 36
 Askeri, 5, 11, 14, 32, 36, 38, 39, 42, 46,
 48, 58, 59, 60, 62, 63, 64, 65, 66, 67,
 73, 75, 76, 79, 88, 102
 Avrupa Birliği, xi, 32, 83, 96

-B-

Bilgi teknolojileri, 88
 Bilgisayar, 19, 50
 Biyolojik silah, 78
 BM, xi, 31, 83, 87, 97, 99, 100, 102

-C-

Cambridge raporu, 39
 CEPEJ, xi, 97

-Ç-

Çalışma Hakkı, 93

-D-

DARPA, xi, 36, 38, 56, 64, 69
 Demokrasi, 47, 49
 Derin Öğrenme, 24, 25

-E-

Endüstri 4.0, 8, 11, 12, 13, 14

-F-

Facebook, 3, 44, 45, 46, 48, 62, 90, 91,
 93
 Füze Teknolojisi Kontrol Rejimi, xii

-G-

Gizlilik, 57, 63, 89, 90, 96

Güvenlik, 3, 4, 5, 31, 32, 33, 36, 39, 40,
 41, 42, 43, 44, 45, 46, 50, 51, 52, 53,
 54, 55, 56, 57, 58, 59, 63, 65, 73, 93,
 98

-H-

Hareket Özgürlüğü, 91
 hükümet, 35, 45, 56, 76, 103

-İ-

IHL, xi, 70, 75, 102

-İ-

İfade Özgürlüğü, 92
 İHA, 38, 62, 63, 78
 İnsan Hakları, xi, xii, 66, 70, 73, 74, 84,
 85, 89, 92, 96, 97, 99, 102
 İnsancıl Hukuk, 70
 İstihbarat, 3, 5, 15, 28, 34, 39, 42, 43,
 46, 51, 54, 55, 56, 57, 58, 59, 60, 61,
 67, 72, 102

-M-

Mahremiyet, 33, 89
 Makine Öğrenmesi, xi, 22

-N-

Nesnelerin interneti, 53, 63, 67, 80

-O-

Otonom, 2, 6, 30, 36, 62, 66, 70, 73, 74,
 77

-Ö-

Özerk araçlar, 22, 34, 35, 62
 Özerk Savaşçı, 68
 Özerk Silah Sistemi, 71

-R-

Robotlar, 1, 13, 15, 22, 27, 29, 32, 33,
36, 39, 40, 47, 48, 60, 66, 69, 73

-S-

Sağlık Hakkı, 95
Sanayi Devrimi, 2, 10, 11, 12
Savaş, 4, 5, 6, 16, 38, 53, 54, 55, 62, 63,
65, 66, 68, 69, 70, 71, 72, 74, 75, 77,
78, 79, 99, 102
Savaş nesnelerin interneti, 65
Savunma, 2, 3, 4, 5, 6, 14, 51, 52, 53,
54, 55, 56, 58, 59, 61, 63, 66, 67, 70,
99, 102
Siber güvenlik, 1, 2, 3, 4, 5, 35, 49, 51,
52, 53, 54, 55, 57, 58, 102
Sorumluluk, 30, 56, 73, 75, 76, 77, 96,
102, 103

-T-

Teknologizm, 49
Toronto Deklarasyonu, 86, 96, 100, 102

-U-

Uluslararası hukuk, 75
Uluslararası Medeni ve Siyasi Haklar
Sözleşmesi, 84

-V-

Veri, xi, 16, 23, 26, 45, 60, 90, 96, 98,
102

-Y-

Yapay Zeka, xi, xii, 1, 2, 13, 20, 21, 27,
30, 35, 37, 42, 84, 94, 98, 99

