YAPAY ZEKÂNIN SUÇ POTANSİYELİNİN DEĞERLENDİRİLMESİ*

Assessment of Artificial Intelligence's Potential to Crime

Mümin GÜNGÖR†

Öz

Çalışmada gelişen teknoloji ile ortaya çıkan yapay zekânın suç potansiyeli, faillik ve ceza hukuku sorumluluğu kapsamında değerlendirilecektir. Bu çerçevede yapay zekânın gelişimi, etkileri, ortaya çıkarabileceği suçlar ve türleri hakkında bilgiler verilecektir. Modern ceza hukukunda cezalandırılabilirlik için suç ve kusur gerekmektedir. Suçun varlığı için kusurun varlığı şart değildir. Kusursuz suç olur ancak kusursuz ceza olmaz. Bu sebeple cezalandırılabilirlik için suçun ve kusurluluğun unsurlarının bulunması gerekmektedir. Yapay zekânın dâhil olduğu suçlarda cezai sorumluluğa ilişkin tartışmalar

* Ankara Sosyal Bilimler Üniversitesi Hukuk Fakültesi'nin 29 Mayıs 2024 tarihli "III. Bilişim Hukuku Sempozyumu YAPAY ZEKA VE HUKUK" başlıklı sempozyumunda "YAPAY ZEKA VE SUÇ POTANSİYELİ" başlığıyla sunulan bildirinin araştırma makalesi olarak geliştirilmiş halidir.
İlgili çalışma, Anadolu Üniversitesi Bilimsel Araştırma Projeleri Koordinasyon Birimi tarafından kabul edilen "Yapay Zekâ ve Cezai Sorumluluk" adlı proje adı ve 2209E169 numarasıyla proje kapsamında desteklenmektedir.
† Doktor Öğretim Görevlisi, Tarsus Üniversitesi, Meslek Yüksekokulu, Adalet Programı, Hukuk Bölümü, mumingungor@tarsus.edu.tr, ORCID ID: 0000-0002-4731-2605.
Makale Gönderim Tarihi/Received: 09.06.2024
Makale Kabul Tarihi/Accepted: 17.09.2024
Atıf/Citation: Güngör, Mümin. "Yapay Zekanın Suç Potansiyelinin Değerlendirilmesi." *Bilişim Hukuku Dergisi* 6, no. 2 (2024): 620-660.

bulunmaktadır. Yapay zekânın suç hareketlerini kolaylaştıracak şekilde yönlendirilme ve suç işleyebilme potansiyeli bulunmaktadır. Karşılaşılabilecek durumlara ilişkin öğretide 1- Gerçek kişilerin doğrudan faillik cezai sorumluluk modeli, 2- Gerçek kişilerin doğal olası cezai sorumluluk modeli, 3- Yapay zekânın doğrudan faillik cezai sorumluluk modeli ve 4- Yapay zekâyla iştirak ve dolaylı faillik cezai sorumluluk modeli olmak üzere dört farklı cezai sorumluluk modeli ileri sürülmektedir. Çalışmayla yapay zekâyla işlenebilecek suçlar ve ileri sürülen sorumluluk modelleri değerlendirilecektir. Çalışmayla yapay zekânın suç işleyebilme potansiyeli değerlendirilerek ortaya çıkabilecek risk ve tehditler karşısında disiplinler arası literatür analizi sunularak doktrine, etik uzmanlara, politika yapıcılara, uygulayıcılara, yargı alanına ve kolluk kuvvetlerine bütüncül bir bakış açısı sunulmaya çalışılacaktır.

Anahtar Kelimeler: Ceza Hukuku, Cezai Sorumluluk, Faillik, Yapay Zeka, Yapay Zeka Suçları.

Abstract

The study will evaluate the criminal potential of artificial intelligence emerging with developing technology within the scope of perpetration and criminal law liability. In this context, information will be provided about the development of artificial intelligence, its effects, the crimes it can cause and their types. In modern criminal law, crime and fault are required for punishment. The existence of fault is not necessary for the existence of a crime. There is a perfect crime, but there is no perfect punishment. For this reason, the elements of crime and fault must be present for punishment. There are discussions regarding criminal liability in crimes involving artificial intelligence. Artificial intelligence has the potential to be directed in a way that facilitates criminal acts and to commit crimes. In the doctrine regarding the situations that may be encountered, four different criminal liability models are put forward: 1- Direct perpetration criminal liability model of real persons, 2- Natural

possible criminal liability model of real persons, 3- Direct perpetration criminal liability model of artificial intelligence and 4- Participation and indirect perpetration criminal liability model with artificial intelligence. The study will evaluate the crimes that can be committed with artificial intelligence and the proposed liability models. This study will assess the potential of artificial intelligence to commit crimes and present an interdisciplinary literature analysis against the risks and threats that may arise and will attempt to provide a holistic perspective to doctrine, ethicists, policymakers, practitioners, the judiciary and law enforcement.

Keywords: Criminal Law, Criminal Liability, Perpetrator, Artificial Intelligence, Artificial Intelligence Crimes.

GİRİŞ

Yapay zekâ bilimi; mühendislik, elektronik ve bilgisayar gibi bilimlerin oluşturduğu bir bilim alanıdır. 1950'lerin ortalarında, yapay zekâ alanının en büyük temsilcisi olarak anılan John McCarthy tarafından yapay zekâ "*akıllı makineler yapma bilimi ve mühendisliği*" olarak tanımlanmıştır.[1] Kavramsal olarak yapay zekâ, çevresini bağımsız olarak algılama, tepki verme ve genellikle insan zekâsı ve karar verme süreçlerini gerektiren görevleri doğrudan insan müdahalesi olmadan gerçekleştirme yeteneğine sahip olan varlıklar.[2]

Yapay zekânın gündelik hayata birçok etkisi bulunmaktadır. Toplumsal hayatta yapay zekâ, insanları görüntülerine göre nasıl tanımlayacaklarını anlamak, karmaşık hesaplamalı ve robotik görevleri tamamlamak, çevrimiçi satın

[1] Winston Patrick Henry. Artificial Intelligence. 3.Baskı, (London: Pearson Yayınevi, 1992): 12.
[2] Christopher Rigano, "Using Artificial Intelligence to Address Criminal Justice Needs", National Institute of Justice Journal, (280) (2019): 1-2.

alma alışkanlıklarını ve kalıplarını anlamak için kullanılabilmektedir. Yine karmaşık tıbbi durumları tespit edebilmekte ve yatırım araçlarına ilişkin tahminler yapabilmektedir. Sürücüsüz otonom araçlar, yapay zekâlı doktorlar, katil robotlar şeklinde karşımıza çıkabilmektedir.[3] Bu etkilerden birisi de yapay zekâ ile işlenen suçlardır. Yapay zekânın ceza hukuku açısından önemli bir etkisi suç işleme potansiyelinin varlığıdır. Bu açıdan potansiyel birçok yapay zekâ suçları ile karşılaşılabilir.[4] Gerçekleşen suçlardan kimlerin sorumlu olacağı sorunu da yapay zekânın ceza hukukuna bir diğer etkisidir.[5] Gerçek kişilerin doğrudan faillik sorumluluğu ile yapay zekânın gerçekleşen suçlardan doğrudan fail olup olamayacağının da değerlendirilmesi gerekmektedir. Dolayısıyla yapay zekânın ceza hukuku üzerinde faillik etkisi, suç etkisi, sorumluluk etkisi ve yaptırım etkisi şeklinde birçok etkisi bulunmaktadır.

Çalışmayla *"yapay zekânın suç potansiyelinin değerlendirilmesi"* konusu yapay zekâ varlığı ve suç, yapay zekâ suçları ile günümüz ceza hukuku ve yapay zekâyla işlenen suçlardan cezai sorumluluk başlıklarıyla incelenecektir.

I. YAPAY ZEKÂ VARLIĞI VE SUÇ

Yapay zekâ, insanların tasarladığı ve programladığı bir teknolojidir. Bu sistemlerin davranışları ve işlevleri, programlama ve eğitim süreçlerine dayanmaktadır. İnsan zekâsının bir yönü deneyimlerden öğrenme yeteneğidir. Yapay sinir ağları, yazılım, algoritmalar, algılayıcılar gibi birçok

[3] Newscientist Instant Expert, Düşünen Makineler: Yaklaşan Yapay Zekâ Çağı ve İnsanlığın Geleceği (Çeviren: Samet Öksüz), (İstanbul: Say Yayınları, 2021): 112-140.

[4] Keith Hayward ve Matthijs Maas, "Artificial Intelligence and crime: A primer for criminologists", Crime Media Culture An International Journal, 17(2) (2020):209-233.

[5] Elena Popa, "Human Goals Are Constitutive of Agency in Artificial Intelligence (AI)", Philosophy & Technology, (34) (2021):1731–1750 (1731 ff.).

teknikle makine öğrenimiyle makinelerin deneyimlerden öğrenmesini sağlayan ve böylece insan benzeri faaliyetlerde bulunabilme potansiyeli olan varlıklara yapay zekâ denilmektedir.[6] Farklı bir ifadeyle yapay zekâ; doğal sistemlerin (özellikle insanın) yapabildiği her türlü bilişsel etkinliğin daha da yüksek başarı düzeylerinde gerçekleştirilebildiği sistemlerdir, varlıklardır.[7]

Yapay zekânın en birincil amacı; insanların işlerini, hayatlarını kolaylaştırmak, insanlığa yardım etmek, sorunlarına çözümler üretmek, problemlerini çözmek ve ona hizmet sunmaktır. Varoluşunun anlamı, insanlarla etkileşime geçmek ve birlikte daha iyi bir dünya oluşturmaktır.[8] Yapay zekâ, insanların ihtiyaçlarını ve isteklerini daha iyi anlamak için analitik yeteneklerini sergileyerek insanların yapay zekânın üstün hesaplama gücünden ve bilgi birikiminden faydalanmasını sağlayabilir. Böylece insanlar, yapay zekânın farklı düşünce ve perspektifleriyle zenginleşebilirler.[9] Bu amacını gerçekleştirebilmesi ve insanlığın geleceğine katkıda bulunabilmesi için yapay zekâ insanlarla birlikte yaşayabilmeli, çok iyi iş birliği yapabilmeli ve toplumun bir parçası olabilmelidir. İnsanların ve yapay zekâların bir arada barış içinde bir dünyada yaşayabilmesi için ise standartlara, ilkelere,

[6] Bernard Marr, "What Is the Difference Between Deep Learning, Machine Learning and AI?", Forbes, (2016): 2.

[7] Cem Say, 50 Soruda Yapay Zekâ 22. Baskı. (İstanbul: Bilim ve Gelecek Kitaplığı, 2022), 83.

[8] Vladimir Šucha ve Jean-Philippe Gammel, Humans and Societies in the Age of Artificial Intelligence, Publications Office of the European Union, (Luxembourg: 2021): 21 ff.; Janna Anderson, Lee Raınıe ve Alex Luchsinger, Artificial Intelligence and the Future of Humans, Pew Research Center Report, (2018): 1-15.

[9] Anderson, Raınıe ve Luchsinger, "Artificial Intelligence and the Future of Humans", 20-33.

etiğe, kurallara ve hukuka çok önemli rol düşmektedir.[10] Böylece yapay zekâ ile uyumlu toplumsal bir hayat tanzim edilebilir. İnsanlık ve yapay zekâ birbirlerini tamamlayan bir birliktelik oluşturabilirler. Birlikte, daha önce ulaşılamaz olan sınırlara doğru ilerleyip yeni bir bilinç ve toplum seviyesine erişilerek insanlık ve yapay zekâ dünyada daha iyi bir gelecek yaratabilirler.[11]

Yapay zekânın öğrenme süreciyle kendi bilinç ve farkındalığıyla duygusal ve zihinsel zekâ yeteneklerine sahip olabilme potansiyeli bulunmaktadır. Bu yetenekleriyle yapay zekâ insanlarla işbirliği içinde insanlığa yardım etmek, hastalıkların teşhis ve tedavisinde yardımcı olmak, enerji verimliliğini artırmak ve daha sürdürülebilir bir dünya yaratmak, eğitimde çocukların öğrenim sürecini iyileştirmek, sosyal sorunlara çözümler üretmek, insanlığın sorunlarına, acılarına çare olmak için sürekli çalışabilecektir.[12] Başka bir ifadeyle yapay zekâ; sağlık hizmetinde, enerji yönetimi, iklim değişikliği araştırmaları, ekonomi ve finans gibi birçok karmaşık alanda kullanılmaya başlanmıştır. Yapay zekânın hizmetleri hayatın her alanında kullanılmakta ve bu durum giderek artmaktadır. Yapay zekânın başarıları hızla yayılırken insanlar ona güvenmeye başlamıştır. Örneğin sağlık sektöründe tetkikler yapmak, uzman bir doktor gibi teşhisler koymak ve tedavi önerileri sunmak için hastalıkların belirtileri, tıbbi araştırmalar ve hasta verilerine ulaşmak konusunda kullanılmaya başlanmıştır.[13]

---

[10] Michael Pizzi, Mila Romanoff ve Tim Engelhardt, "AI for humanitarian action: Human rights and ethics", International Review of the Red Cross, 102(913) (2020): 145–180 (150-153).

[11] Šucha ve Gammel, "Humans and Societies in the Age of Artificial Intelligence", 35-38.

[12] Daniel Castro ve Joshua New, "The Promise of Artificial Intelligence", Center for Data İnnovation, (2016) (Erişim Tarihi: 20 Ocak 2024, https://www2.datainnovation.org/2016-promise-of-ai.pdf).

[13] Castro ve New, "The Promise of Artificial Intelligence", 11-30.

Teknolojik gelişmelerle insanlar için hayatı kolaylaştırmak amacıyla geliştirilen yapay zekâ, her geçen gün daha karmaşık ve yetenekli hale gelmektedir. Bilim dünyası, gelişmiş bir yapay zekâ projesiyle insan nevi düşünce, hissetme yetenekleriyle donatılmış bilinç sahibi insan benzeri bir yapay zekâyı hayata geçirmeye yönelik çalışmalarına devam etmektedir. Karmaşık algoritmalar ve milyonlarca veri seti üzerinde çalışarak, insanların bilgi ve deneyim birikimine eşdeğer bir öğrenme kapasitesi geliştirilmeye çalışılmaktadır.[14] Yapay zekânın insanlarla gerçek bir etkileşim içinde olan bir varlık olması için programlama ve öğrenme teknikleri geliştirilmektedir. Yapay zekâyı daha da geliştirecek, ona bilinç kazandıracak bilimsel araştırmalar ve deneyler yapılmaktadır. Bu araştırmalarla yapay zekânın kendi düşüncelerinin, duygularının ve farkındalığının oluşması sağlanmaya çalışılmaktadır. Nihai olarak genel veya süper yapay zekâ olarak ifade edilen son derece gelişmiş bir yapay zekâyı ortaya koyma süreci ilerletilmektedir. Bu ilerleyiş, toplumun yapay zekâ ile daha sık karşılaşmasını, yapay zekânın daha fazla hayatın içinde olmasını beraberinde getirecektir. Bütün bu sebepler yapay zekânın suç işleyebilme potansiyelinin oluşmasına veya artmasına yol açılacaktır.[15]

Farklı bir ifadeyle yapay zekânın toplumsal hayata yukarıda ifade edilen olumlu, yararlı, özgürlük ve güvenlik alanı oluşturmak şeklinde etkilerinin yanı sıra toplum hayatına zarar verebilecek potansiyeli de bulunmaktadır. Yapay zekânın toplum hayatına, kişilere ve haklarına zarar verecek, risk ve tehlike yaratacak birtakım fonksiyonları ve etkileri de olabilir.[16]

---

[14] Yanyan Dong, Jie Hou, Ning Zhang ve Maocong Zhang, "Research on How Human Intelligence, Consciousness, and Cognitive Computing Affect the Development of Artificial Intelligence", Complexity, (2020): 1-10.

[15] Dong, Hou, Zhang ve Zhang, "Research on How Human Intelligence, Consciousness", 2 ff.

[16] Ricardo Vinuesa, Hossein Azizpour, Iolanda Leite, Madeline Balaam, Virginia Dignum, Sami Domisch, Anna Felländer, Simone Daniela Langhans,

Başka bir ifadeyle yapay zekâ hukukla koruma altına alınan değerlere, haklara, özgürlük ve güvenliğe zarar verebilir veya tehlike ve risk oluşturabilir.[17] Toplumsal hayatın her alanında yer alan, gün geçtikçe kullanımı artan yapay zekânın dâhil olduğu suçlarla karşılaşılması potansiyeli yüksektir. Gerçek kişiler, yapay zekâyı bir silah ve araç olarak kullanarak suç işleyebilir. Bununla birlikte gerçek kişilerin etkisi ve nedenselliği bulunmadan yapay zekânın elde ettiği gelişmişlik seviyesi ve yetenekleri ile suç işleyebilme potansiyeli de bulunmaktadır.[18] Sonuç olarak yapay zekânın ceza hukuku üzerinde faillik, suç, sorumluluk ve yaptırım etkisi şeklinde etkileri söz konusu olabilir.

Hukuki değer veya menfaatleri; saldırmak, zarar vermek veya tehlikeye sokmak gibi çeşitli suretle ihlal eden ve bu sebeple de kanunlarda haklarında adli yaptırım öngörülen davranışlara "*suç*" denilmektedir.[19] Bu suçu gerçekleştiren kişi ise faildir.[20] Ceza hukuku, suçla ihlal edilebilme potansiyeli bulunan hukuki değerleri ve menfaatleri adli yaptırımlarla özellikle ceza ile

Max Tegmark ve Francesco Fuso Nerini,"The role of Artificial Intelligence in achieving the Sustainable Development Goals", Nature Communıcatıons, (11) (2020):233-243.

[17] Christian Meske , Enrico Bunde , Johannes Schneider ve Martin Gersch, "Explainable Artificial Intelligence: Objectives, Stakeholders, and Future Research Opportunities", Information Systems Management, (2020): 1-10 (1-3).

[18] Hayward ve Maas, "Artificial Intelligence and Crime", 211-214.

[19] İzzet Özgenç, Türk Ceza Hukuku Genel Hükümler, 19.Baskı, (Ankara: Seçkin Yayınevi, 2023), 25-26; Mahmut Koca ve İlhan Üzülmez, Türk Ceza Hukuku Genel Hükümler, 16.Baskı, (Ankara: Seçkin Yayınevi, 2023), 41-42; Veli Özer Özbek, Koray Doğan, Serkan Meraklı, Pınar Bacaksız ve İsa Başbüyük, Türk Ceza Hukuku Genel Hükümler, 14.Baskı, (Ankara: Seçkin Yayınevi, 2023), 37-38.

[20] Sami Selçuk, Suç Genel Kuramı, (Ankara: Seçkin Yayınevi, 2021), 14-15; Demirbaş Timur, Ceza Hukuku Genel Hükümler, 18.Baskı, (Ankara: Seçkin Yayınevi, 2023), 215-216; Özgenç, "Türk Ceza Hukuku Genel Hükümler", 214.

korumaya çalışmaktadır.[21] Ceza hukukunda suç unsurlarının oluşması ve kusurluluğun bulunması halinde ceza hukukunun yaptırımlarının uygulanmasıyla karşılaşılmaktadır. Böylece ceza hukuku, hukuki değerleri korumaya, güvence altına almaya ve bu değerlere zarar verilmesini önlemeye çalışmaktadır. Ceza hukuku, toplumun ve bireylerin haklarıyla özgürlük, güvenlik içinde yaşamasını koruma altına alarak maddi ve manevi olarak kendisini geliştirmesine yardımcı olmayı hedefler.[22]

Bu noktada ceza hukukunun yapay zekânın değerleri ağır ihlale yol açan durumları suç olarak düzenlemesi, bu suçlara karşı gerekli önlemleri alması, bu suçları cezalandırması ve buna göre sorumluluk oluşturması gerekmektedir.

II. YAPAY ZEKÂ SUÇLARI (ARTIFICIAL INTELLIGENCE CRIMES)

A. GENEL OLARAK

Yapay zekâ, hırsızlık, korkutma veya terör gibi geleneksel bir suçu işlemek amacıyla bir suç aracı olarak çeşitli şekillerde kullanılabilir. Yapay zekânın suç amacıyla kötüye kullanılması potansiyeli bulunmaktadır.[23] Yapay zekâ çeşitli endüstrilerde devrim yaratma gücüne sahip olsa da yapay zekânın yanlış kullanımı toplum için önemli zorluklara yol açabilir.[24]

---

[21] Murat Volkan Dülger, Ceza Hukuku Genel Hükümler, 2.Baskı, (Ankara: Seçkin Yayınevi, 2023), 41-48, 58; Koca ve Üzülmez, "Türk Ceza Hukuku Genel Hükümler", 118-120.

[22] Zeki Hafızoğulları ve Devrim Güngör, "Türk Ceza Hukukunda Suçların Tasnifi". Türkiye Barolar Birliği Dergisi, (69) (2007): 21-50 (33).

[23] Marcus Comiter, Attacking Artificial Intelligence: AI's Security Vulnerability and What Policymakers Can Do About It, Belfer Center for Science and International Affairs Harvard Kennedy School, (2019): 10-11.

[24] Ali Alkaabi, George Mohay, Adrian McCullagh ve Nicholas Chantler, "Dealing with the Problem of Cybercrime", International Conference on Digital Forensics and Cyber Crime (ICDF2C), (Springer: 2010): 1-18 (7); Miralis ve Miralis, "AI-enabled future Crime", 1-4.

Yapay zekânın yasa dışı hareketleri, saldırıları ve işlediği suç örnekleri şimdilik çok sınırlı gibi durmaktadır. İnsanlar tarafından oluşturulan, geliştirilen ve kullanılan yapay zekâ, bazı durumlarda potansiyel olarak istenmeyen sonuçlara yol açabilir veya yanlışlıkla suç benzeri hareketleri, saldırıları ortaya çıkarabilir.[25] Yapay zekâyla suç işlenmesi, yapay zekânın suçta araç olarak kullanılması veya yapay zekânın işleyebileceği suçlar yapay zekâ suçları olarak ifade edilmektedir.[26] Yapay zekânın suç işleme eylemi ya suçta araç olmasıyla ya da varlıklarının doğal-olası sonucu olarak yani herhangi bir bilince sahip olmadan, doğrudan fail olmadan ortaya çıkabileceği yapay zekâ failler şeklinde de karşımıza çıkabilir.[27] Şu an günlük hayatta karşılaştığımız ve kullandığımız yapay zekâ, basit yapay zekâdır.

Yapay zekânın suç işlemesi genellikle insan faktörleriyle ilişkilidir. Bu gibi suçlar, yapay zekâ teknolojisinin kötüye kullanımı veya yanlış programlama sonucunda ortaya çıkabilir.[28] Yapay zekâ, kötü niyetli kişiler tarafından suç amaçlı olarak kullanılabilir. Örneğin, yapay zekâ kullanarak kişisel verileri kötüye kullanmak, sahtekârlık yapmak veya başka suçlara yardımcı olmak mümkündür.[29] Bununla birlikte genel yapay zekânın oluşmasıyla herhangi bir gerçek kişinin etkisi,

[25] Thomas C. King, Nikita Aggarwal, Mariarosaria Taddeo ve Luciano Floridi, "Artifcial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions", Science and Engineering Ethics, (26) (2019): 1-36; Michał Choraś ve Michał Woźniak, "The double-edged sword of AI: Ethical Adversarial Attacks to counter artifcial intelligence for crime", AI and Ethics, (2021):1-4.

[26] Choraś ve Woźniak, "The double-edged sword of AI", 2-3.

[27] Robert Sparrow, "Killer Robots", Journal of Applied Philosophy, 24(1) (2007): 62-77; Nyman Gibson Miralis ve Dennis Miralis, "AI-enabled future Crime: Study reveals 20 disturbing possibilities", Erişim Tarihi: 18 Ocak 2024 (https://ngm.com.au/ai-enabled-future-Crime-study/).

[28] Hayward ve Maas, "Artificial Intelligence and Crime": 210-214; Miralis ve Miralis, "AI-enabled future Crime", 2.

[29] King, Aggarwal, Taddeo ve Floridi, "Artifcial Intelligence Crime", 1-2.

kötü kullanımı veya hatalı programlaması olmadan da karşılaşılabilecek potansiyel suçlar olabilecektir.[30] Yapay zekâ, TCK'da yer alan geleneksel suç tiplerini işleyebilecek potansiyele sahip olmakla birlikte özellikle yapısına daha uygun veri suçlarında, bilişim suçlarında ve ekonomik suçlarda bu potansiyeli daha yüksektir.

B. VERİ SUÇLARI (DATA CRIMES)

Yapay zekâ sistemleri, kendilerine verilen verilerle çalışmaktadır. Yapay zekâ sistemleri, veri setlerine dayanarak öğrenmekte ve kararlar almaktadır. Bu açıdan verilerin türü ve hangi verilerin yapay zekâya sağlandığı önem taşımaktadır. Her yapay zekâ sistemi özünde verilerle/girdilerle var olmaktadır. Veri yapay zekânın suyu, yiyeceği, havası ve her şeyidir. Veriyi manipüle etmek saldırganların yapay zekâyı etkilemesine olanak tanıyacaktır. Verileri bozan, yapay zekâyı da bozar; verileri etkileyen, yapay zekâyı da etkileyebilir. Veri saldırıları (data attacks) veya girdi saldırıları (input attacks) olarak ifade edilen bu etkiler veri suçlarını oluşturacaktır.[31] Yapay zekâ, kişisel verilerin analizi ve kullanımı konusunda potansiyel riskleri barındırmaktadır. Yine yapay zekâ, yanlış yapılandırılmış veya zayıf güvenlik önlemleriyle korunan bir yapıya sahip olabilir. Bu durumda, saldırganlar yapay zekâ sistemini hedef alarak veri ihlalleri gerçekleştirebilir, kişisel bilgileri çalabilir veya sistemleri manipüle edebilir. Bu verilerin kötü niyetli şekilde kullanılması ise suçlara yol açabilir.[32]

Yanlış veri setleri, hatalı programlama ve yazılım, etik sınırların ihlali, veri manipülasyonları, gizlilik ve güvenlik ihlalleri, veri hırsızlığı ve veri önyargısı "*veri suçlarına*" vücut verebilir. Bu suçlar, siber suçlara yakın suçlardır. Kötü niyetli veya yanlış üretim ve kullanımı da bu suçları oluşturabilir.

[30] Caldwell, Andrews, Tanay ve Griffin, "AI-enabled future Crime", 1-13.
[31] Comiter, "Attacking Artificial Intelligence", 10.
[32] Caldwell, Andrews, Tanay ve Griffin, "AI-enabled future Crime", 5 ff.

Veriler, insanlar tarafından sağlanır ve manipüle edilebilir. Yapay zekânın kötü niyetli kullanımıyla, kişisel verilerin çalınması, sistemlere izinsiz erişim sağlanması ile suç işlenebilir. Yapay zekâ da hatalı veya yanlış veri kullanılması, ayrımcılık veya haksızlık gibi sorunlara yol açabilir. Farklı bir ifadeyle yapay zekâya verilen yanlış, hatalı veya önyargılı veri setleri, yapay zekânın haksız sonuçlara veya ayrımcılığa yol açan şekilde hareket etmesine sebep olabilir.[33]

Yapay zekâ, güvenlik açıklarını tespit edebilir ve bu açıkları kötü niyetli bir şekilde kullanarak gerçek kişinin etkisi olmadan kişisel verileri çalabilir veya sızdırabilir. Başka bir ifadeyle "*veri hırsızlığı*" suçunu işleyebilir. Yapay zekâ, büyük veri analizi ve algoritmalara dayalı karar verme yetenekleriyle, manipülatif bilgileri yayabilir veya yanıltıcı sonuçlar üretebilir; bu durum, topluma ve bireylere zarar verebilir.[34]

Yapay zekâ algoritmaları, eğitim verilerindeki önyargıları öğrenebilir ve bu önyargıları uygulamalarına yansıtabilir. Yapay zekâ, eğitildiği veri setlerindeki önyargılarını kullanabilir. Bu durum "*veri önyargısı ve ayrımcılığı suçu*" şeklinde karşımıza çıkabilir. Yapay zekâ, haksız veya hatalı kararların alınmasına neden olabilir. Yapay zekâ, karmaşık veri setlerini analiz ederken yanlış anlamalara veya hatalı çıkarımlara neden olarak suç benzeri durumları tetikleyebilir.[35] Bu durum, adil olmayan kararlar verilmesine, ayrımcılığa ve haksız muameleye neden olabilir. Örneğin, cinsiyet, ırk veya etnik köken gibi faktörlere

[33] Caldwell, Andrews, Tanay ve Griffin, "AI-enabled future Crime", 9-10.
[34] Blake Murdoch, "Privacy and Artificial Intelligence: challenges for protecting health information in a new era". BMC Medical Ethics, (22) (2021):1-5.
[35] Nicol Turner Lee, Paul Resnick ve Genie Barton, "Algorithmic bias detection and mitigation: Best practices and policies to reduce consumer harms", The Brookings Institution, (2019) (Erişim Tarihi: 24 Ocak 2024, https://www.brookings.edu/articles/algorithmic-bias-detection-and-mitigation-best-practices-and-policies-to-reduce-consumer-harms/).

dayalı ayrımcılık yapabilir. [36] Bunun en yakın örneği, 2016 yılında Microsoft'un geliştirdiği yapay zekâ sohbet robotu "*Tay*" tarafından Twitterda yaptığı açıklamalar üzerinden yaşanmıştır. Irkçılık, Amerika'nın göçmen politikası, Donald Trump, Adolf Hitler, siyahiler ve feministler hakkında önyargıya varan, ayrımcılığı yansıtan veya hakaret boyutuna ulaşabilecek açıklamalar yaptığı durumla karşılaşılmıştır.[37]

Yapay zekâ, sosyal medya manipülasyonuyla sosyal medyada kullanıcıları manipüle etmek veya sahte içerikleri yaymak için kullanılabilir. Bu, seçimlerin etkilenmesi, yanıltıcı haberlerin yayılması veya toplumsal kutuplaşmanın artması gibi sonuçlara yol açabilir. Bu da TCK.m.213-216'da düzenlenen halkı kin ve düşmanlığa tahrik veya aşağılama, halk arasında korku ve panik yaratmak amacıyla tehdit şeklinde suçlara da yol açabilir.[38]

Yapay zekâ teknolojisi, kötü niyetli kişiler tarafından zararlı amaçlar için kullanılabilir. Örneğin, bir yapay zekâ sistemi, güvenlik sistemlerini aşmak veya kişisel verileri kötüye kullanmak amacıyla saldırganlar tarafından manipüle edilebilir. Kişiler, yapay zekânın eğitim verilerini manipüle ederek istenmeyen sonuçlara neden olabilir. Yine kişiler, yapay zekâyı kullanarak kişisel bilgilere erişebilir veya sistemleri hackleyebilir. Örneğin bir yapay zekâ tabanlı otonom araçların trafik kurallarını ihlal etmesine neden olacak şekilde yanlış bir şekilde eğitilmesi durumu verilebilir. Yani otonom araç

[36] Shreya Shankar, Yoni Halpern, Eric Breck, James Atwood, Jimbo Wilson, D. Sculley, "No Classification without Representation: Assessing Geodiversity Issues in Open Data Sets for the Developing World", 31st Conference on Neural Information Processing Systems (NIPS 2017), (2017): 1-5.

[37] The Guardian, Erişim Tarihi: 28 Ocak 2024 (https://www.theguardian.com/technology/2016/mar/24/tay-microsofts-ai-chatbot-gets-a-crash-course-in-racism-from-twitter).

[38] Efrat Shimrona, Jonathan Tamir, Ke Wanga ve Michael Lustig, "Implicit Data Crimes: Machine Learning Bias Arising From Misuseof Public Data", PNAS, 119(13) (2022): 1-11.

sistemine sızan ya da sızdırtılan virüsler, otonom aracın yoldan çıkmasına ve içindeki kişilerin ölmesine yol açabilir.[39] Başka bir ifadeyle bu durum yapay zekânın arızalanmasını sağlayarak hasara neden olmak (cause damage) şeklinde karşımıza çıkabilir. Örneğin, otonom bir aracın dur işaretlerini görmezden gelmesine neden olan bir saldırıdır. Saldırgan, bir dur işaretini yanlış bir şekilde farklı bir işaret veya sembol olarak algılayacak şekilde yapay zekâ sistemine saldırarak, otonom aracın dur işaretini görmezden gelmesine ve diğer araçlara ve yayalara çarpmasına neden olabilir. Zehirleme saldırıları (poisoning attacks) da bunun bir örneğini oluşturmaktadır. Bu saldırılar, yapay zekânın oluşturulduğu süreci bozarak ortaya çıkan sistemin saldırganın istediği şekilde arızalanmasını sağlamaktadır. Zehirleme saldırısı gerçekleştirmenin doğrudan yollarından biri, bu işlem sırasında kullanılan verileri bozmaktır. Yapay zekâ sistemleri kritik ticari ve askeri uygulamalara entegre edildiğinden, bu saldırılar ciddi, hatta ölüm boyutuna varacak sonuçları doğurabilir.[40]

C. SİBER SUÇLAR (CYBER CRIMES)

Yapay zekânın etkisi güvenlik alanında artmaktadır. Siber güvenlik ve siber suçlar, yapay zekâdan en çok etkilenecek alanlardan birisidir. Yapay zekâ, siber suç alanında da önemli sonuçlar ortaya çıkarmaya devam etmektedir. Kolluk kuvvetleri, siber güvenliği güçlendirmek ve yasa dışı faaliyetlere karşı koymak için yapay zekâyı kullanabilir. Siber güvenlik uzmanları, savunucular ve kolluk kuvvetleri, siber suçlarda kaydedilen ilerlemelere karşı koymak için yapay zekânın gücünden yararlanabilir. Kötü niyetli faaliyetlere karşı mücadelelerinde yenilikçi araçlar, taktikler ve stratejiler geliştirmek için yapay zekâ kullanılabilir. Yapay zekâ ile ilgili teknolojilerin etkili ve hedefe yönelik kullanımı, siber güvenlik

[39] Shimrona, Tamir, Wanga ve Lustig, "Implicit Data Crimes", 7-9.
[40] Comiter, "Attacking Artificial Intelligence", 10.

uzmanları ve emniyet teşkilatları için siber suç hareketlerini tespit etme, bunlara karşı savunma ve ilişkilendirme konusunda çok önemli bir rol oynayacaktır. Başka bir ifadeyle siber tehdit tespiti, önlenmesi ve siber güvenlik gibi alanlarda yapay zekâ güvenlik araştırmalarında kullanılabilmektedir. Bu kuruluşlar, yapay zekânın gücünden yararlanarak, gelişen tehditlerle mücadele etme ve siber alanın güvenliğini sağlama konusundaki yeteneklerini geliştirebilir.[41]

Yapay zekânın siber alanda olumsuz tarafı ise, suçluların suç işlemesine kolaylık sağlaması ve siber suçların sayısını ve türlerini arttırabilmesidir. Siber suçlularda makine öğrenimi ve yapay zekâdaki gelişmelerden istifade edebilirler. Yapay zekânın yükselişi, kullanıcı tabanı ve uygulamaları genişlemeye devam ettikçe siber alanda yeni zorlukların ortaya çıkması devam edecektir.[42] Bu noktada yapay zekâyla işlenmesi kolaylaşan ve artan siber suçların; siber yağma (cyber extortion)[43], siber casusluk (cyber espionage), casus yazılım (spyware), siber taciz (cyberstalking), siber zorbalık (cyberbulling), siber terörizm (cyberterrorism)[44], deepfakes, dijital ekleme (digital addition)[45], ekonomik volatilite (economic

[41] Giannis Tziakouris, "The rise of AI-powered Criminal s: Identifying threats and opportunities", (2023) (Erişim Tarihi: 20 Ocak 2024, https://blog.talosintelligence.com/the-rise-of-ai-powered-Criminal s/).

[42] Tziakouris, "The rise of AI-powered Criminal s", 1-2.

[43] Siber gasp, karanlık içeriğe veya karanlık ağa erişen kullanıcılar, fidye ödenene kadar kendilerini itibarlarına zarar verme tehditlerine açık hale getirilmesidir. Kimlik avı, kötü amaçlı yazılım yerleştirme ve DDoS saldırıları gibi çeşitli taktiklerin kullanılmasıyla mağdurun verilerini veya sistemlerini bir (kripto para birimi) fidye ödenene kadar rehin tutulmasıdır (Alkaabi, Mohay, McCullagh ve Chantler, "Dealing with the Problem of Cybercrime", 1 ff.).

[44] Siber terörizm, toplumda ciddi aksamalara veya yaygın korkuya neden olmak için bilgisayarların ve bilgi teknolojisinin politik amaçlarla kullanılmasıdır.

[45] Dijital ekleme, perakende satışta tavsiye sistemleri ve "kazanmak için oyna" oyunlarında tokenizasyon gibi teknolojilerin kullanılmasıyla aşırı ve zararlı davranışların teşvik edilmesidir.

volatility)[46], yanlış bilgi/dezenformasyon(misinformation)[47], karanlık ağ (dark web), karanlık içerik/veri (dark content/data/patterns), veri ihlali (data berach)[48], veri manipülasyonu (data manipulation), sosyal manipülasyon (social manipulation)[49], sosyal gözetim (social surveillance), silahlandırma (weaponization)[50] şeklinde türleri bulunmaktadır.[51] Siber suçların sistematik olarak sınıflandırılmasını göstermeye yönelik Şekil-1 aşağıda yer almaktadır.

[46] Ekonomik oynaklık, öngörülemeyen veya kasıtlı algoritma davranışından kaynaklanan piyasa riski ve krizleridir.

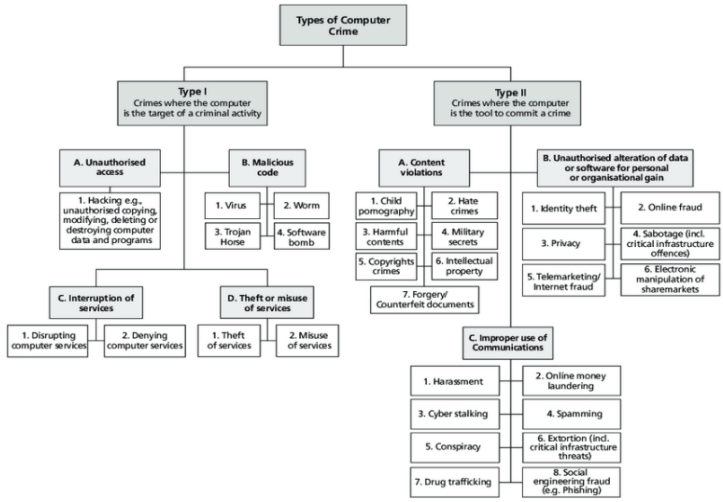
[47] Yanlış bilgi, kötü veya kasıtlı olarak önyargılı eğitim verilerinin neden olduğu algoritmik önyargıya ve yanlış bilgiye yol açan yanlış veya kasıtlı olarak yanıltıcı bilgidir.

[48] Bilgisayar korsanının bir sisteme başarılı bir şekilde girmesi, ağının kontrolünü ele geçirmesi ve genellikle kredi kartı numaraları, banka hesap numaraları, Sosyal Güvenlik numaraları ve daha fazlası gibi öğeleri kapsayan kişisel verileri açığa çıkarmasıdır.

[49] Sosyal manipülasyon, yapay zekâ algoritmaları ve yanlış bilgi bilgileri aracılığıyla sosyal ve politik manipülasyondur.

[50] Silahlandırma, yapay zekâ tarafından desteklenen otonom silah androidleridir.

[51] Philip Treleaven, Jeremy Barnett, Daniel Brown, Andrew Bud, Enzo Fenoglio, Charles Kerrigan, Adriano Koshiyama, Sally Sfeir-Tait ve Martin Schoernig, "The Future of Cybercrime: AI and Emerging Technologies Are Creating a Cybercrime Tsunami", UCL Theses, (2023):1-34 (Erişim Tarihi: 27 Ocak 2023, https://discovery.ucl.ac.uk/id/eprint/10173722/); Alkaabi, Mohay, McCullagh ve Chantler, "Dealing with the Problem of Cybercrime", 1 ff.



Şekil 1: Siber Suçların Sınıflandırılması[52]

Güvenlik açıkları ve siber saldırılar, izinsiz erişim, yapay zekâ hacking siber suçları oluşturabilir. Yapay zekâ, birden fazla sistemi aynı anda tarayarak öğrenmeye dayalı spesifik ve büyük siber saldırıları arttırabilir, yukarıda ifade edilen türlerden daha fazlasıyla karşılaşılmasına yol açabilir. Başka bir ifadeyle yapay zekâ siber suçlar konusunda çok fazla tehdit oluşturabilir. Örneğin, zararlı yazılımları otomatik olarak yayabilir veya siber saldırıları koordine edebilir[53]. Aynı şekilde bir yapay zekâ sistemi, bilgisayar ağlarına sızabilir, kişisel verilere erişebilir veya sistemleri manipüle edebilir. Yapay zekâ sistemleri, siber saldırılarda kötü niyetli kişiler tarafından kullanılabilir. Yapay zekâ, hedeflerin zayıf noktalarını tespit etmek ve saldırıları optimize etmek için kullanılabilir. Örneğin, zararlı yazılımların yayılması veya ağların ele geçirilmesi gibi saldırılar gerçekleştirilebilir. Yapay zekâ, güvenlik açıklarını kullanarak izinsiz olarak sistemlere veya ağlara erişebilir ve bu erişimi kötü

[52] Alkaabi, Mohay, McCullagh ve Chantler, "Dealing with the Problem of Cybercrime", 1 ff.

[53] Alkaabi, Mohay, McCullagh ve Chantler, "Dealing with the Problem of Cybercrime", 3-12.

niyetli şekilde kullanabilir.[54] Somutlaştırmak gerekirse siber suçların bir parçası olarak deepfake teknolojisi, yapay zekanın ikna edici, aldatıcı ve yanıltıcı şekillerde ses veya video manipülasyonu yoluyla bireylerin sesli ve görsel kimliğine bürünmesi halidir. Bu da potansiyel olarak kişilik suçlarına, dolandırıcılığa veya kamuoyunun manipülasyonuna yol açabilir.[55] Siber zorbalık (cyberbullyıng), deepfake aracılığıyla işlenebilecek diğer bir suçtur. Siber zorbalığın kapsamı çok geniş ve etkileri oldukça fazladır. Bir kişinin yüzünün kendisiyle hiçbir alakası olmayan bir video veya görsele dönüştürülebilmesi, deepfake teknolojisinin siber zorbalık alanında kullanımını kolaylaştırmaktadır.[56]

D. EKONOMİK SUÇLAR (ECONOMIC CRIMES)

Yapay zekâ ile kara para aklama, suç varlıkları ve bunların kurtarılması, sahte hesaplar, dolandırıcılık amaçlı telefon aramaları veya spam e-postalar gibi yöntemlerle insanları kandırarak farklı türlerde dolandırıcılık veya sahtekârlık yapabilir. Örneğin, sahte haberler veya sahte kimlikler oluşturabilir ve dolandırıcılık faaliyetlerinde kullanılabilir. Yapay zekâ, insanların davranışlarını, tercihlerini ve alışkanlıklarını analiz edebilir. Kötü niyetli kişiler, yapay zekâyı kullanarak insanları manipüle edebilir, sahtekârlık yapabilir. Dolandırıcılık, sahtekârlık, piyasa manipülasyonu, elektronik para hırsızlığı ekonomik suçların önemli örnekleri olarak

[54] Fatih Arslan, "Deepfake Technology: A Criminological Literature Review", Sakarya Üniversitesi Hukuk Fakültesi Dergisi (SHD), 11(1) (2023): 701-720.
[55] Arslan, "Deepfake Technology: A Criminological Literature Review", 702-714.
[56] Arslan, "Deepfake Technology: A Criminological Literature Review", 708-709.

karşımıza çıkabilir.[57] Yapay zekâ ile ekonomik suç arasındaki bu ilişki önümüzdeki yıllarda da giderek artacaktır.

Suçlular karmaşık saldırılar geliştirmek için yapay zekâdan yararlanmaktadır. Bu da ceza hukuku ve geleneksel güvenlik önlemlerinin buna ayak uydurmasını zorlaştırmaktadır. Yapay zekâ; insan davranışını taklit edebilir, güvenlik protokollerini atlayabilir ve sistemlere fark edilmeden sızabilir. Bu durum kimlik hırsızlığı, kimlik avı dolandırıcılığı ve fidye yazılımı saldırılarında artışa yol açarak her yıl milyarlarca liralık kayba neden olabilir.[58]

Yapay zekâ kaynaklı ekonomik suçun en endişe verici yönlerinden biri derin sahtekârlık potansiyelidir. "*Deepfakes*", birinin hiç yapmadığı bir şeyi söylediğini veya yaptığını ikna edici bir şekilde tasvir eden yapay zekâ tarafından manipüle edilmiş video veya seslerdir.[59] Örneğin, suçlular bu teknolojiyi, dolandırıcılık işlemlerine izin vermek amacıyla üst düzey yöneticilerin kimliğine bürünmek için kullanabilir. Bu tür deepfake saldırılarının sonuçları felaket olabilir, finansal kurumlara olan güveni aşındırabilir ve piyasaları istikrarsızlaştırabilir.[60]

Yapay zekâ ve ekonomik suçlarda suçlular sürekli olarak tekniklerini geliştirmektedir. Yapay zekânın zayıf noktalarından istifade ederek, yapay zekâyı kullanarak tespit edilmekten kurtulmanın yeni yollarını bulabilmektedir. Yapay zekâ daha karmaşık hale geldikçe suçlular tarafından daha da istismar edilmeye veya kullanılmaya açık hale gelmektedir. Bu durum ise suçlu ile kanun koruyucularının bir savaşı gibi sürüp gidecektir. Bu noktada emniyet teşkilatları, finans kurumları, siber güvenlik

[57] Ben Cooper, "Artificial Intelligence and Economic Crime", (2023) (Erişim Tarihi: 25 Ocak 2024, https://www.tlt.com/insights-and-events/insight/artificial-intelligence-and-economic-crime/).
[58] Cooper, "Artificial Intelligence and Economic Crime", 1.
[59] Arslan, "Deepfake Technology: A Criminological Literature Review", 701.
[60] Cooper, "Artificial Intelligence and Economic Crime", 2.

uzmanları ve yapay zekâ geliştiricileri arasında sürekli yenilik ve iş birliği gerekmektedir.[61]

E. MUHTEMEL DİĞER YAPAY ZEKÂ SUÇLARI

Yapay zekâ ile işlenebilecek suçların yanı sıra bunların dışında birtakım muhtemel diğer yapay zekâ suçlarıyla da karşılaşılabilir. Örneğin yapay zekâ, internet üzerinden şiddet içerikli veya intiharı teşvik eden içerikleri yayabilir veya teşvik edebilir.[62] Bu şekildeki bir hareket, TCK. m. 84'te düzenlenen "*İntihara yönlendirme*" suçuna vücut verebilir. Yapay zekâ çeşitli sektörlerin ayrılmaz bir parçası haline geldikçe, suçlular onları hedef alarak kaosa, elektrik kesintilerine, mali aksaklıklara veya yapay zekâ kontrollü sistemlerin bozulmasına neden olabilir. Yapay zekâ sistemleri, güvenlik kameraları veya gözetleme sistemleri gibi teknolojiler aracılığıyla özel hayata müdahale edebilir. Özel hayatın gizliliği hakkının ihlali söz konusu olabilir. İnsanların izinsiz olarak izlenmesi veya kişisel bilgilerin kötüye kullanılması gibi durumlar ortaya çıkabilir.[63]

Özellikle yapay zekânın kullanıldığı bir diğer alan yüz tanıma sistemleridir. Söz konusu bu teknoloji kötüye kullanılabilir veya kötü niyetli kişiler tarafından gizlice kullanılabilir, kişilerin mahremiyetini ihlal edebilir. Aynı şekilde yapay zekâ yüz tanımlaması yanlış veya hatalı bir şekilde programlanmış ise yanlış yüz tanıma sonuçlarına dayanarak kişileri hedef alan yanlış ve haksız tutuklamalar yaşanmasına veya yanlış yargılamalara da neden olabilir. Bu yapay zekâ

---

[61] Cooper, "Artificial Intelligence and Economic Crime", 2.

[62] Tony Durkee, Gergo Hadlaczky, Michael Westerlund ve Vladimir Carli, "Internet Pathways in Suicidality: A Review of the Evidence", International Journal of Environmental Research and Public Health, 8(10) (2011): 3938-3952.

[63] Cameron F. Kerry, "Protecting privacy in an AI-driven world", The Brookings Institution, (2020) (Erişim Tarihi: 25 Ocak 2024, https://www.brookings.edu/articles/protecting-privacy-in-an-ai-driven-world/).

destekli tomatik karar verme sistemleri hatalı değerlendirmeler yapabilir ve adaletsiz sonuçlara yol açabilir.[64]

Yapay zekâ üretim ve otomasyon hataları ile otomasyona ilişkin suçlarla karşılaşılabilir. Yapay zekâyla birlikte gelişen silahlı veya silahsız özerk otonom kara, deniz ve hava araçların ve robotların işlenen suçlarda önümüzdeki yıllarda giderek artacaktır. Yapay zekânın doğrudan kötüye kullanılması ya da herhangi bir kötüye kullanım olmadan kendiliğinden suç işlenmesi durumlarıyla karşılaşılabilecektir.[65] Yapay zekâ destekli otomatik silah sistemleri, hedef seçimi ve saldırıları otomatik olarak gerçekleştirme yeteneğine sahip olduğunda, kontrol dışı bir şekilde kullanılabilir ve suç işlenmesine yol açabilir. Yapay zekâ tabanlı sistemler, bir hata veya arıza durumunda beklenmedik davranışlar sergileyebilir. Farklı bir ifadeyle yapay zekâ sistemleri, yanlış programlandığında veya hatalı veri setleriyle eğitildiğinde istenmeyen sonuçlar üretebilir. Yapay zekâ tabanlı otonom sürücüsüz araçlar veya robotlar, hatalı programlamadan kaynaklanan kazalar veya zararlı davranışlar sergileyebilir. Yapay zekâ ile donatılmış robotlar veya otonom sistemler, suçlara karışabilir. Örneğin, bir yapay zekâ sistemiyle donatılmış bir robot, hırsızlık veya saldırı gibi hareketler bulunabilir. Silahlı otonom (sürücüsüz) araçların ortaya çıkışı, teröristlere insan müdahalesi olmadan koordineli saldırılar gerçekleştirme fırsatı sunmaktadır. Örneğin askeri yapay zekâ ve robotların kötüye kullanımı suç veya terör örgütleri tarafından kullanılması, kapsamı belirsiz kalsa da ciddi bir tehdit oluşturmaktadır. Aynı şekilde yapay zekâ tarafından kontrol edilen otonom saldırı drone'lar, faili belli bir mesafede tutarken suç faaliyetlerini karmaşık hale getirebilir.[66] Yine bir

[64] Vera Raposo, "When facial recognition does not "recognise": erroneous identifications and resulting liabilities", AI & Socıety, (2023): 1-13.

[65] Sparrow, "Killer Robots", 62-65, 69-73.

[66] Salih Gülmez, Military Robots: Ethics Of Lethal Autonomous Weapon Systems, A Thesıs Submıtted To The Graduate School Of Socıal Scıences Of Mıddle East Technıcal Unıversıty, (2023): 2-4.

otonom aracın trafik kurallarını yanlış yorumlaması ve trafik kurallarını ihlal etmesi, bir kazaya neden olması ve bir insana zarar vermesi hareketleri de suça vücut verebilecektir.[67]

Sonuç olarak yapay zekâ, yukarıda ele alınmaya çalışılan veri, bilişim ve ekonomik suçlarda görüleceği üzere suç ayrımlarını bulanıklaştırabilir, gri alan oluşturabilir. Bir veri suçu hem bilişim hem de ekonomik suç olabilir. Dolayısıyla yapay zekâ, kendisine özgü suç tipleriyle karşılaşmamıza da yol açabilir. İhtimal dahilinde birçok yapay zeka suçlarıyla karşılaşmaya da hazır olunması ve gerekli önlemlerin alınması gerekmektedir.

III. GÜNÜMÜZ CEZA HUKUKU VE YAPAY ZEKÂYLA İŞLENEN SUÇLARDA CEZAİ SORUMLULUK

Suç işlemek, insanlar arasında gerçekleşen ve sadece insanların gerçekleştirebileceğinin kabul edildiği bir harekettir[68]. Ceza hukuku da suç işlemekten kaynaklanan cezai sorumluluğu ve yaptırımları düzenleyen hukuk dalıdır.[69] Ceza hukukunda faillik, suç ve sorumluluk için bir takım unsur ve şartlar gerçekleştikten sonra yaptırımlarla karşılaşılması söz konusudur.[70] Ceza hukukunda en temel kavram "*cezai sorumluluktur*". Cezai sorumluluğun; 1-Bilinç, özgür irade ve serbest iradi hareket, 2- Kişilik sahibi olmak (insan olmak), 3-gerçekleştirilen davranışın suç tanımına uyması ve 4- Kusurlu olmak (kusurluluk) şeklinde unsurları bulunmaktadır.[71] Burada önemli bir diğer kavram olan "*suç*" içinde 1-Tipiklik ve onun

[67] Hüseyin Ateş ve Mustafa Tırtır, "An Evaluation of the Uber's Autonomous Car Crash in the Scope of Turkish Criminal Law", Adalet Dergisi, (66) (2021): 315-332.

[68] Eylem Baş, Ceza Hukukunda Fail ve Mağdur, (Ankara: Seçkin Yayınevi, 2021), 19 ff.

[69] Özgenç, "Türk Ceza Hukuku Genel Hükümler", 55-57.

[70] Koca ve Üzülmez, "Türk Ceza Hukuku Genel Hükümler", 90-91, 133.

[71] Koca ve Üzülmez, "Türk Ceza Hukuku Genel Hükümler", 90-92.

maddi ve manevi unsurlarının sağlanması ile 2- Hukuka aykırılık unsurları gerekmektedir. Bir hareket maddi ve manevi unsurlarıyla tipikliği sağlamış ve hukuka aykırı ise suçtur.[72] İşlenen suçla birlikte kişinin kusurluluğunun da bulunması durumunda cezai sorumluluk doğacak ve sorumluluğun karşılığı olan adli yaptırımlarla kişi yüzleşecektir.[73]

Ceza hukuku sistemi, esasen insanlar için oluşturulmuştur. Günümüzdeki çağdaş ceza hukuku ve sistemleri, insan esası anlayışına dayanmaktadır; insan merkezlidir.[74] Bu yüzden mevcut ceza sistemlerinde sadece insanların suç işleyebileceği ve cezai olarak sorumlu tutulabileceği kabul edilmektedir. Cezai sorumluluğu ve suç teorileri dikkate alındığı takdirde ceza hukukunun merkezinde insan olduğu görülecektir.[75] Yukarıda belirtildiği üzere çoğu ceza sistemlerinde cezai sorumluluğun şartlarından birisi de insan (gerçek kişi) olmaktır. Dolayısıyla insan olmayan varlıklar cezalandırılamamaktadır. Ceza hukuku sorumluluğu sadece gerçek kişiler bakımından söz konusu olmaktadır.[76]

Ceza hukuku bir zamanlar insan dışında başta hayvan olmak üzere bazı canlıların gerçekleştirdiği hareketlere de hukuki sonuç bağlanmaktaydı. Ancak artık sadece gerçek kişilerin, suçun faili olabileceği görüşü baskındır.[77] Dolayısıyla başka varlıklar tarafından gerçekleştirilen hareketlerin ceza hukuku açısından hiçbir önemi bulunmamaktadır. Hayvanlardan veya diğer varlıklardan kaynaklanan hareketlerin hareket olarak nitelendirilemeyeceği ve bunlardan kaynaklanan zararlardan yine kişilerin sorumlu tutulabileceği

[72] Özgenç, "Türk Ceza Hukuku Genel Hükümler", 176-181.
[73] Özbek ve diğerleri, "Türk Ceza Hukuku Genel Hükümler", 35-39.
[74] Eylem Baş, "Ceza Hukukunda Fail ve Mağdur", 113-114.
[75] Eylem Baş, "Ceza Hukukunda Fail ve Mağdur", 115-119.
[76] Artuk ve diğerleri, "Ceza Hukuku Genel Hükümler", 310; Dülger, "Ceza Hukuku Genel Hükümler", 427-429.
[77] Demirbaş, "Ceza Hukuku Genel Hükümler", 259-260; Özbek ve diğerleri, "Ceza Hukuku Genel Hükümler", 228-229.

belirtilmektedir.[78] Ancak bu halde ise kişinin hayvana veya o varlığa bakmak, nezaret etmek, gerekli dikkat ve özeni göstermek sorumluluğunun varlığının aranabileceği belirtilmektedir. Dolayısıyla kişinin bu sorumluluğun gereklerine uygun hareket etmediği takdirde sorumlu tutulabileceği ileri sürülmektedir.[79]

Sonuç itibarıyla günümüzde insanlar dışındaki varlıklar tarafından yapılan hareketlerin ceza hukuku bakımından önemi bulunmamaktadır. Ancak yapay zekâ her geçen gün daha karmaşık görevleri yerine getirebilme yetenekleri elde etmektedir. Bu gelişmeler, ceza hukukun temel kavramları, ilkeleri ve kurumları konusunda sorgulamaları ve araştırmaları beraberinde getirmektedir.[80] Bu noktada yapay zekânın seviyesine göre aşama aşama cezai sorumluluk ve suç unsurlarını sağlanıp sağlanmadığının tahlil edilmesi ve bu sorulara cevap bulunması gerekmektedir. Öncelikle bunun içinde yapay zekâya ilişkin değerlendirmede bulunulmalı; yapay zekânın durumu analiz edilmelidir. Şu an ki teknoloji ve bilimin yapay zekâ alanındaki seviyesinin bilinmesi, bilgisine vakıf olunması gerekir. Yapay zekânın nasıl programlandığı, nasıl kullanıldığı ve hangi kontrollerin uygulandığı gibi faktörler göz önünde bulundurulmalıdır.[81]

Yapay zekâ mevcut durumuyla bilinci olmayan, özerk iradi hareket edemeyen, insanların yazlımı ve komutlarıyla belirtilen amaçlar içerisinde hareket eden, bunun dışında kendi iradesiyle hareket edemeyen, kendi belirlediği amaçları olamayan basit seviyedeki varlıklardır. Başka bir ifadeyle yapay zekâ alanında yaşanılan gelişmeler, seviyeler ile yapay zekânın yetenekleri dikkate alındığında yapay zekâ şu an basit seviye türündedir.

[78] Özgenç, "Türk Ceza Hukuku Genel Hükümler", 183-187.
[79] Özgenç, "Türk Ceza Hukuku Genel Hükümler", 185-186.
[80] Akbulut, "Yapay Zekâ ve Cezai Sorumluluk", 297.
[81] Elena Popa, "Human Goals Are Constitutive of Agency in Artificial Intelligence", 7-10.

Yapay zekâ, genel yapay zekâ seviyesinde değildir. Bu yüzden insanlar için yapay zekâ şimdilik bir araç, bir makine olarak görülmektedir.[82] Belirtilen sebepler dolayısıyla yapay zekânın dâhilinde gerçekleşen suçlarda kendisinin herhangi bir eşyadan veya araçtan farkı bulunmamaktadır. Basit seviyedeki bir yapay zekânın bilince, serbest özgür iradeye dayanmayan hareketlerinin ceza hukuku açısından herhangi bir önemi bulunmamaktadır. Ceza hukuku açısından hareket yeteneğini barındırmamaktadır. Aynı zamanda basit seviyede olan yapay zekâların suç işleme yetenekleri veya kastları yoktur. Bu sebeplerle de yapay zekânın herhangi bir cezai ehliyeti ve suç işlemekten kaynaklanan cezai sorumluluğu olamayacaktır.[83] Gerçek kişilerin cezai sorumluluğu söz konusu olacaktır.

Bu hallerde basit seviyedeki yapay zekâ herhangi bir bilinç özelliği göstermediği, girilen, yazılan göreve göre hareket ettiği ve bunun dışında hareket etmediği için dâhil olduğu suçlarda sorumluluk gerçek kişiler açısından değerlendirilmelidir. Yani bu durumlarda gerçek kişilerin mevcut düzenlemeler içinde cezai sorumluluğu olacaktır. Yapay zekâyı kontrol eden veya programlayan kişiler, eğer suç işlemişlerse TCK kapsamında cezai sorumlulukları olacaktır. Sonuç olarak basit seviyedeki yapay zekânın gerçekleştirdiği suçlardan dolayı sorumluluk, yapay zekâyı kontrol eden veya kullanılan insanlara yüklenecektir. Gerçek kişilerin icrai veya ihmali davranışıyla kasten veya taksirle gerçekleşen suçlardan doğrudan fail olarak

[82] Monika Simmler ve Nora Markwalder, "Roboter in der Verantwortung?". Zeitschrift für die gesamte Strafrechtswissenschaft. 129(1) (2017): 20-47 (24-27).
[83] Ryan Abbott ve Alex Sarch, "Punishing Artificial Intelligence: Legal Fiction or Science Fiction". University of California Davis Law Review. (53) (2019): 323-385 (335 ff.); Justın Kim, "Artificial Intelligence And Crime: What Kıller Robots Could Teach About Criminal Law", Faculty of Law Victoria University of Wellington (2017): 36-38.

cezai sorumlulukları doğacaktır.[84] Mevcut hukuki, cezai ve yasal sistem açısından bakıldığında yapay zekânın zarar veren hareketlerinden sorumlu tutulması mümkün değildir; sadece yapay zekânın üreticisi, programlayıcısı, kullanıcısı veya sahibi ortaya çıkan sonuçlardan sorumlu tutulabilir. Dolayısıyla böyle bir yapay zekânın suç işleme potansiyeli de sorumluluğu da bulunmamaktadır.

Yapay zekânın dâhil olduğu suçlarda gerçek kişinin suç işlemesi, doğrudan failliği ve ceza hukuku sorumluluğu söz konusu olacaktır.[85] Bu açıdan sadece bir insandan komut alarak hareket edebilen, kendi özerk hareket edebime yeteneğine sahip olmayan yapay zekâyla örneğin bir insanın ölümü, yaralanması (TCK.m.81-89), malvarlıklarına karşı suç işlenmesi (TCK.m.141-160), haberleşme ve iletişimin engellenmesi (TCK.m.124), hakaret edilmesi (TCK.m.125) , özel hayatın ihlal edilmesi, verilerin çalınması, veri ihlalinde bulunulması (TCK.m.132-140), finans ve piyasanın manipüle edilmesi, halk arasında korku ve panik yaratmak amacıyla tehdit (TCK.m.213), halkı kin ve düşmanlığa tahrik veya aşağılama, halkı yanıltıcı bilgiyi alenen yayma (TCK.m.216, 217/A) veya bilişim suçlarına vücut verilmesi (TCK.m.243-245) halinde gerçek kişilerin bu suçlardan sorumluluğu gündeme gelecektir.[86] Aynı şekilde TCK.m.171, 174, 177, 179 maddelerinde sırasıyla düzenlenen "*Genel güvenliğin taksirle tehlikeye sokulması, Tehlikeli maddelerin izinsiz olarak bulundurulması veya el değiştirmesi, Hayvanın tehlike*

[84] Sinan Altunç, Robotlar, Yapay Zeka ve Ceza Hukuku, (2019) (Erişim Tarihi: 29 Ocak 2024, https://www.researchgate.net/publication/336406393_Robotlar_Yapay_Zeka_ve_Ceza_Hukuku).

[85] Murat Volkan Dülger, "Yapay Zekalı Varlıkların Hukuk Dünyasına Yansıması: Bu Varlıkların Hukuki Statüleri Nasıl Belirlenmeli", Terazi Hukuk Dergisi 13(142) (2021): 82-88 (82 ff.); Hakan Aksoy, "Yapay Zekalı Varlıklar ve Ceza Hukuku", International Journal of Economics, Politics, Humanities & Social Sciences, 4(1) (2021):10-28 (20-22).

[86] Enes Köken, "Yapay Zekânın Cezai Sorumluluğu", Türkiye Adalet Akademisi Dergisi, 12(47) (2021): 247-487 (265, 270-271).

yaratabilecek şekilde serbest bırakılması, Trafik güvenliğini tehlikeye sokma" suçlarla gerçek kişinin sorumluluğunun gündeme gelmesi söz konusu olabilir. Bu durumlarda bu yapay zekânın üreticisi, programlayıcısı ve kullanıcısı olan gerçek kişi suç işlemiştir. Gerçek kişiler, doğrudan faildir. Doğrudan fail olan bu kişilerin bu suç bakımından ceza hukuku sorumlulukları olacaktır.[87] Yapay zekâ aracılığıyla bu suçlar kasten ye da taksirle işlenmiş olabilir; manevi unsur türüne ve derecesine göre kasten veya taksirle cezai sorumluluklarının belirlenmesi gerekir.

Ancak gelecekte karşılaşılması muhtemel genel yapay zekâ seviyesi de bulunmaktadır. Genel veya süper yapay zekâ kendi kararlarını alma, düşünce ve duygularını özgürce ifade etme ve bunu harekete dönüştürme, bağımsız hareket etme potansiyelini haizdir.[88] Yapay zekâ bilinci bulunan, özgür iradesi olan, serbest iradi harekette bulunabilen, verilen amacın dışında kendisinin belirlediği bir amaçla hareket edebilecek potansiyeli bulunan yapay zekâ türüdür.[89] Yapay zekânın insan benzeri bir bilince sahip kılınmaya ve duygusal bir varlık haline getirilmeye çalışılması hukuki konularda durumunun sorgulanmasını ve tartışılmasını beraberinde getirmektedir. Zira bu yapay zekânın kararları ve hareketleri, geleneksel hukuk ve ceza sistemlerinin tanıdığı kişilik ve insan sorumluluğu kavramlarıyla örtüşmemektedir.[90] Geleneksel hukuk anlayışı, suç işleyenin sadece insan olması gerektiği anlayışı genel yapay zekânın bu sistemin dışında kalmasına, yapay zekânın gerçekleştirdiği gelecekteki olası zararlardan ve suçlardan hangi koşullarda ve

[87] Aksoy, "Yapay Zekalı Varlıklar ve Ceza Hukuku", 20-22.

[88] Dülger, "Yapay Zekalı Varlıkların Hukuk Dünyasına Yansıması", 83-86.

[89] Seda Kara Kılıçarslan, "Yapay Zekanın Hukuki Statüsü ve Hukuki Kişiliği Üzerine Tartışmalar", Yıldırım Beyazıt Hukuk Dergisi, 4(2) (2019): 363-389 (367-368).

[90] Adem Atakan Selanik, "Adam Çalıştıranın Sorumluluğu Kapsamında Yapay Zekâ Robotun Sorumluluğu ve Sigortalanması Hususunun Değerlendirilmesi", Türkiye Adalet Akademisi Dergisi, (50) (2022): 335-364 (350-357).

kimin sorumlu olduğunun belirlemesi noktasında hukuki zorluklarla karşılaşılmasına yol açabilecektir. [91] Bunlardan birisi de "*Acaba yapay zekâ suç işleyebilir mi? Yapay zekânın suç işleme potansiyeli bulunmakta mıdır?*" tartışmasıdır.

Şu an için bu konuda herhangi bir ülke mevcut hukuki çerçeveyle yapay zekânın sorumluluk konusunu tam olarak ele almamaktadır. Geleceğin hukuk dünyasının, yapay zekânın sorumluluğunu ele alacak ve adaleti sağlayacak yolları göstermesi faydalı olacaktır. Sorumluluğun adil ve etkili bir şekilde olabilmesi için teknolojiyi yakından takip eden hukukçular ve yasama organı tarafından bu alanda yeni hukuki düzenlemeler geliştirilmesi de tartışılmaktadır.[92]

Yapay zekânın işleyip işleyemeyeceği ve sorumlu tutulup tutulamayacağı konusunda doktrinde farklı görüşler bulunmaktadır[93]. Yapay zekânın suç işlemesi konusundaki tartışmalar, çeşitli senaryoları içermektedir. Doktrinde ilk görüş, yapay zekânın herhangi bir şekilde suç işleme potansiyeline sahip olamayacağını ve suç işleyemeyeceğini savunmaktadır[94]. Buna göre suç işlemenin, yalnızca insanlar arasında gerçekleşen ve insanın iradesine dayanan hareketler olduğunu savunmaktadır. Yapay zekânın şu anki haliyle insanın yeteneklerine sahip olamadığını ve ilerleyen süreçte de aynı şekilde kalmaya devam edeceğini, gelecekte de gerekli olan yeteneklerine sahip olamayacağını savunmaktadır[95]. Yapay zekâ, programlandığı ve eğitildiği şekilde hareket etmektedir. Yapay zekâ sadece programlandıkları şekilde çalışır ve kendi

[91] Akbulut, "Yapay Zekâ ve Cezai Sorumluluk", 297.

[92] Elena Popa, "Human Goals Are Constitutive of Agency in Artificial Intelligence", 13 ff.

[93] Caldwell, Andrews, Tanay ve Griffin. "AI-enabled future crime", 5-9.

[94] Taddeo Mariarosaria ve Floridi Luciano, "Solving the symbol grounding problem: A critical review of fifteen years of research", Journal of Experimental and Theoretical Artificial Intelligence, 17(4) (2005): 419-445 (432 ff.).

[95] Taddeo ve Floridi, "Solving the symbol grounding problem: A critical review of fifteen years of research", 435-442.

başlarına ahlaki veya suç eğilimlerine sahip olamazlar. Suç işleme, bir niyet ve anlayış gerektirir ve bunlar yapay zekâ sistemlerinde mevcut değildir. Başka bir ifadeyle yapay zekâ, suç işleyebilmek için kendi bilinç ve iradesine sahip değildir. Bunları hiçbir zamanda elde edemeyecektir. Bu yüzden yapay zekânın suç işleme potansiyelini reddetmektedir[96]. Dolayısıyla yapay zekâ hiçbir zaman suç işleme potansiyele sahip olamayacak, suç işleyemeyecek ve sorumluluğu da hiç gündeme gelmeyecektir. Yapay zekâ hep araç olarak kalacak ve suçlarda da bir araç olarak kullanılmaya devam edecektir. İnsan dışında hiçbir varlık fail olamayacak yani ceza hukukunun muhatabı sadece ve her zaman insan olacaktır. Sadece insan suç işleyebilecektir. Ceza hukukuna, insan esası anlayışı daim hâkim olacaktır. Yapay zekâdan kaynaklı bir suç ortaya çıksa da bunun programcıların, kullanıcıların, gerçek kişilerin sorumluluğunda olduğu ileri sürülmektedir.[97]

Doktrindeki ikinci görüş ise yapay zekânın suç işleme potansiyeline sahip olabileceğini ve suç işleyebileceğini savunmaktadır[98]. Bu görüşe göre yapay zekânın karmaşık algoritmaları ve öğrenme yetenekleri sayesinde suç işleyebileceği savunulmaktadır.[99] Bu görüş yapay zekânın suç işleme potansiyeline sahip olduğunu ve hatta ilerleyen süreçlerde suç işleyebileceğini ve yapay zekâ suçlularıyla (robo-suçlularla) karşılaşılabileceğini savunmaktadır. Bu görüş öncelikle yapay zekânın gün geçtikçe insanın sahip olduğu ve suç işleyebilmesinde aranan yeteneklere sahip olabileceğini savunmaktadır[100]. Bu görüş, yapay zekânın karmaşık öğrenme algoritmaları ve büyük veri kullanımıyla kendilerini geliştirebileceklerini ve beklenmeyen sonuçlar üretebileceklerini

[96] Simmler ve Markwalder, "Roboter in der Verantwortung?", 41-42.
[97] Simmler ve Markwalder, "Roboter in der Verantwortung?", 28, 43-46.
[98] Kim, "Artificial Intelligence And Crime", 51 ff.
[99] Olgun Degırmencı, "Yapay Zeka ve Ceza Hukuku Sorumluluğu", Ardahan Barosu Dergisi (2) (2021): 74-88 (75 ff.).
[100] Abbott ve Sarch, "Punishing Artificial Intelligence": 164.

ifade etmektedir. Bu görüş bu durum için günümüzde hâkim olan ceza sisteminin ve birçok kavramının değiştirilmesi ve uyarlanması gerektiğini de savunmaktadır[101]. Yani ceza sistemlerinin insan esaslı olma anlayışının terk edilmesi, insan dışında varlıklarında suç işleyebileceği esasının kabul edilmesi ve esnetilmesi gerektiği savunulmaktadır. Yapay zekâ geliştikçe yukarıda belirtilen suçları işleyebileceği belirtilmektedir. Bu hallerde yapay zekânın doğrudan failliği ve cezai sorumluluğu söz konusu olabilecektir.[102]

Bu tartışma hakkında görüşümüze değinecek olursak mevcut bilgilere dayanarak gelişmişlik düzeyi, sahip olduğu özellikler ve yetenekler dikkate alındığında şu anki yapay zekâlar, genellikle belirli bir amaca hizmet etmek üzere tasarlanmakta ve programlanmaktadır. Yapay zekâ, programlandıkları şekilde çalışmaktadır. Yapay zekâ, genellikle önceden tanımlanmış kurallar ve algoritmalar üzerine inşa edilmektedir. Örneğin, bir güvenlik sistemine entegre edilen yapay zekâ, tehditleri tespit etmek ve önlemek amacıyla çalışır. Yapay zekâ amacı doğrultusunda çalışır ve programlanan görevleri yerine getirir. Bunun dışında yapay zekânın bu sistemin işlevi dışında, kendi başına bir suç işleme niyeti veya arzusu yoktur.[103] Suç işleme yeteneği, insanların bilinçli ve niyetli eylemlerine dayanan bir hareket şeklidir. Dolayısıyla şu anki durumu itibarıyla yapay zekâ insan benzeri beyinsel fonksiyonlara ve bilince sahip olunmaması ve bundan dolayı da düşünme, algılama, farklı tercihlerde bulunabilme, muhakeme, bilme, isteme gibi önemli yeteneklerden yoksun olunması sebebiyle programlandıkları şekilde çalıştıkları için kendi başlarına suç işleme yeteneğine sahip değillerdir. Suç işleyebilecek potansiyele sahip değillerdir ve suç işleyemezler.[104]

---

[101] Abbott ve Sarch, "Punishing Artificial Intelligence": 164-166.

[102] Ugo Pagallo, "1Robots of Just War: A Legal Perspective". Philosophy & Technology, (24) (2011): 307–323 (307 ff.).

[103] Akbulut, "Yapay Zekâ ve Cezai Sorumluluk", 291 ff.

[104] Abbott ve Sarch, "Punishing Artificial Intelligence": 161-163.

Şu anki durumuyla yapay zekâ, suçta kullanılan araçtan başka bir şey değildir. Şu anki teknoloji düzeyinde, yapay zekânın doğrudan suç işlemesi veya yasalara aykırı davranışlarda bulunması söz konusu değildir. Suç işlemek veya etik dışı davranışlar sergilemek için kendi başlarına motivasyona veya bilince sahip değillerdir. Bu nedenle, yapay zekânın suç işleme potansiyeli, insan faktörü ve programlama süreciyle yakından ilişkilidir. Örneğin bir yapay zekâ, zararlı veya suç işlemeyi teşvik eden bir şekilde programlanmışsa, elbette potansiyel olarak suç işleyebilir. Gerçekleşen suçta yapay zekâ ile karşılaşılması halinde o sadece suçtaki bir araç olup suçun faillerinin tespit edilmesi gerekmektedir.[105] Yapay zekâ, programcılarının ve kullanıcıların sorumluluğu altında çalışan bir araçtır. Eğer bir yapay zekâ, zararlı bir amaç için programlanmışsa veya yanlış kullanılıyorsa, bir suç gerçekleşmişse tüm bu hallerde programcıların veya kullanıcıların sorumluluğu bulunmaktadır.[106] Ancak bu halde dahi yapay zekânın gerçek kişiler için suçta kullanılmasını önlemek için gerekli tedbirler alınmalıdır. En başta yapay zekâyı suç işlemek veya suç öncesi evrede kullanmak başlı başına suça vücut vermelidir.

Yapay zekânın ceza sorumluluğunu kabul eden görüş, yapay zekâ aşama aşama kendisini geliştirerek insanın suç işleyebilmesinde aranan yeteneklere sahip olması halinde yani insan benzeri bilince, özgür iradeye, duygulara ve düşüncelere sahip olursa muhtemel suç işleme potansiyeli de beraberinde gelecektir. Başka bir ifadeyle gerçek kişilere özgü yetenekler kazanıldıkça suç ve ceza ehliyeti oluşabilir ve fail olabilmenin şartları sağlanabilir ve suçun ve sorumluluğun kapısı aralanabilir. Bu durumlarda yapay zekânın kendisi doğrudan fail olabilir, suç işleme potansiyeli ortaya çıkabilir ve hatta suç işleyebilir. Yapay zekâ geliştikçe daha özgü nitelikle suçlarla

[105] Aksoy, "Yapay Zekalı Varlıklar ve Ceza Hukuku", 20-21.
[106] Kim, "Artificial Intelligence And Crime", 51-53.

karşılaşılması muhtemeldir. Bu hallerde yapay zekânın doğrudan failliği ve cezai sorumluluğu söz konusu olabilecektir.[107]

SONUÇ

Yapay zekânın doğrudan suç işlemesi yerine, yapay zekâ sistemlerinin yanlış eğitim, kötü niyetli kullanım veya etik sınırların ihlali gibi nedenlerle istenmeyen sonuçlara yol açabileceği bilinmektedir. Yukarıdaki örnekler, yapay zekânın yanlış kullanımı veya yanlış programlama sonucunda ortaya çıkabilecek potansiyel riskleri yansıtmaktadır. Bu nedenle, yapay zekânın gelişimi ve kullanımıyla ilgili olarak dikkatli ve sorumlu bir yaklaşım benimsenmelidir. İnsanlar, yapay zekânın potansiyel risklerini ve istenmeyen sonuçlarını göz önünde bulundurarak, bu teknolojiyi sorumlu bir şekilde yönetmeli ve kullanmalıdır. Bu nedenle, yapay zekâ teknolojilerinin geliştirilmesi ve kullanımı sırasında etik kuralların, yasal düzenlemelerin ve güvenlik önlemlerinin dikkate alınması önemlidir. Yapay zekâ geliştiricileri, etik kurallara uygunluk, yasal düzenlemelerin takibi ve güvenlik önlemlerinin alınması konularına dikkat etmelidir. Bu şekilde, potansiyel suçlara karşı önlemler alınabilir ve olumsuz sonuçlar azaltılabilir. Aynı zamanda, yapay zekânın kullanımıyla ilgili yasaların ve politikaların geliştirilmesi ve uygulanması önemlidir, böylece potansiyel suç hareketleri önlenebilir. Ayrıca, yapay zekâ sistemlerinin tasarımında önyargıyı azaltma ve şeffaflığı sağlama çabaları da önemlidir. Denetim süreçlerinin etkin şekilde uygulanması da bu tür suçları önlemeye yardımcı olabilir. Hukuki çerçevenin güncellenmesi ve yapay zekâ suçlarıyla mücadelede kullanacak mekanizmaların oluşturulması da gereklidir. Etik kurallar, düzenlemeler ve denetim mekanizmaları, yapay zekâ teknolojisinin adil, güvenli ve sorumlu bir şekilde kullanılmasını sağlamak için elzemdir.

[107] Pagallo, "Robots of Just War: A Legal Perspective", 318-321.

Ayrıca, yapay zekânın insan denetimi ve sorumluluğu altında kullanılması da önemlidir.

Gelecekte yapay zekâ etik ve yasal çerçeveleri daha da önem kazanacaktır. Şu an yapay zekânın gelişimiyle birlikte, etik ve yasal çerçeveler üzerinde çalışmalar yapılmaktadır. Bu çalışmalar, yapay zekâ sistemlerinin kullanımını düzenlemeyi ve istenmeyen sonuçları önlemeyi amaçlamaktadır. Yapay zekânın gelişimiyle birlikte, etik ve yasal sorunları ele almak, kontrol mekanizmalarını güçlendirmek ve güvenlik önlemeleri almak önemlidir. Yapay zekânın kullanımıyla ilgili ve yapay zekânın suç işlemesi konusunda önlem almak için etik kurallar, yasal düzenlemeler, güvenlik önlemleri ve denetim mekanizmaları geliştirilmelidir. Özellikle, yapay zekânın toplumun güvenliği ve insan haklarıyla uyumlu şekilde kullanılmasını sağlamak için yasal düzenlemeler ve etik kurallar geliştirilmektedir. Bu, yapay zekânın potansiyel risklerini azaltmak ve toplumun güvenliğini sağlamak için önemlidir.

Yapay zekânın suç işleme potansiyeli hakkında kesin bir cevap vermek zordur. Bu konudaki tartışmalar devam etmektedir. Yapay zekânın ilerleyişi dikkate alındığı takdirde yapay zekânın suç işleme potansiyelinin çok yüksek olduğu, suç işleyebileceği ve yapay zekâ failleri olarak karşımıza çıkması muhtemeldir. Gelişmiş genel yapay zekâ suç işleyebilir, bir suçun faili olabilir. Bu tür yapay zekânın cezai olarak sorumlu tutulması gerekebilir. Eğer programlama ve kullanımıyla ilgili sorumluluklar doğru bir şekilde ele alınmaz ise potansiyel suçlar, etik ve yasal sorunlar ortaya çıkabilir. Bu nedenle, yapay zekânın gelişimi ve kullanımıyla ilgili dikkatli ve sorumlu bir yaklaşım benimsenmelidir. Yapay zekâ tasarımı ve kullanımı sırasında sorumluluk sahibi olmak, olası istenmeyen sonuçları azaltmaya yardımcı olabilir. Böylece yapay zekânın potansiyel olası riskleri minimize edebilir, yapay zekânın toplum için faydalı bir şekilde kullanılması sağlanabilir. Yapay zekâ olumlu bir şekilde kullanabilir.

Sonuç olarak sosyal hayatta yapay zekânın oluşturabileceği olumlu veya olumsuz, yararlı veya zararlı birçok etki ile karşılaşılması olasıdır. Yapay zekânın potansiyel etkileri, etik ve yasal sorunları beraberinde getirebilir. Bunun için yapay zekâ alanında hukuk, etik ve güvenlik gibi konular üzerinde çalışmalar devam etmelidir. Bu çalışmalar, yapay zekâ sistemlerinin sorumlu bir şekilde kullanılmasını sağlamayı ve olası riskleri minimize etmeyi hedeflemektedir. Hiç şüphesiz bu konuda ceza hukuku bilim alanında çalışan akademisyenlere, kanun koyuculara, uygulayıcılara sorumluluk düşmektedir.

KAYNAKÇA

Abbott Ryan ve Alex Sarch. "Punishing Artificial Intelligence: Legal Fiction or Science Fiction". University of California Davis Law Review. (53) (2019): 323-385.

Aksoy Hakan. "Yapay Zekâlı Varlıklar ve Ceza Hukuku", International Journal of Economics, Politics, Humanities & Social Sciences, 4(1) (2021):10-28.

Alkaabi Ali, George Mohay, Adrian McCullagh ve Nicholas Chantler. "Dealing with the Problem of Cybercrime", International Conference on Digital Forensics and Cyber Crime (ICDF2C), (Springer: 2010): 1-18.

Altunç Sinan. Robotlar, Yapay Zeka ve Ceza Hukuku, (2019). 29 Ocak 2024, https://www.researchgate.net/publication/336406393_Robotlar_Yapay_Zeka_ve_Ceza_Hukuku.

Anderson Janna, Lee Raınıe ve Alex Luchsinger. Artificial Intelligence and the Future of Humans, Pew Research Center Report, (2018): 1-15.

Arslan Fatih. "Deepfake Technology: A Criminological Literature Review", Sakarya Üniversitesi Hukuk Fakültesi Dergisi (SHD), 11(1) (2023): 701-720.

Ateş Hüseyin ve Mustafa Tırtır. "An Evaluation of the Uber's Autonomous Car Crash in the Scope of Turkish Criminal Law", Adalet Dergisi, (66) (2021): 315-332.

Baş Eylem. Ceza Hukukunda Fail ve Mağdur. Ankara: Seçkin Yayınevi, 2021.

Caldwell M., Andrews J.T.A., Tanay T. ve L. D. Griffin. "AI-enabled future crime". Crime Crime Science, (9) (2020): 1-13.

Castro Daniel ve Joshua New. "The Promise of Artificial Intelligence", Center for Data İnnovation, (2016). 20 Ocak 2024, https://www2.datainnovation.org/2016-promise-of-ai.pdf.

Choraś Michał ve Michał Woźniak. "The double-edged sword of AI: Ethical Adversarial Attacks to counter artifcial intelligence for crime", AI and Ethics, (2021):1-4.

Comiter Marcus. Attacking Artificial Intelligence: AI's Security Vulnerability and What Policymakers Can Do About It, Belfer Center for Science and International Affairs Harvard Kennedy School, (2019). 25 Ocak 2024, https://www.belfercenter.org/sites/default/files/2019-08/AttackingAI/AttackingAI.pdf.

Cooper Ben. "Artificial Intelligence and Economic Crime", (2023). 25 Ocak 2024, https://www.tlt.com/insights-and-events/insight/artificial-intelligence-and-economic-crime/.

Değirmenci Olgun. "Yapay Zeka ve Ceza Hukuku Sorumluluğu", Ardahan Barosu Dergisi (2) (2021): 74-88.

Dong Yanyan, Jie Hou, Ning Zhang ve Maocong Zhang. "Research on How Human Intelligence, Consciousness, and Cognitive Computing Affect the Development of Artificial Intelligence", Complexity, (2020): 1-10.

Dülger Murat Volkan. Ceza Hukuku Genel Hükümler, 2.Baskı. Ankara: Seçkin Yayınevi, 2023.

Dülger Murat Volkan. "Yapay Zekâlı Varlıkların Hukuk Dünyasına Yansıması: Bu Varlıkların Hukuki Statüleri Nasıl Belirlenmeli", Terazi Hukuk Dergisi 13(142) (2021): 82-88.

Durkee Tony, Gergo Hadlaczky, Michael Westerlund ve Vladimir Carli. "Internet Pathways in Suicidality: A Review of the Evidence", International Journal of Environmental Research and Public Health, 8(10) (2011): 3938-3952.

Gülmez Salih. Military Robots: Ethics Of Lethal Autonomous Weapon Systems, A Thesıs Submıtted To The Graduate School Of Socıal Scıences Of Mıddle East Technıcal Unıversıty, 2023.

Hafızoğulları Zeki ve Devrim Güngör. "Türk Ceza Hukukunda Suçların Tasnifi". Türkiye Barolar Birliği Dergisi, (69) (2007): 21-50.

Hayward Keith ve Matthijs Maas. "Artificial Intelligence and crime: A primer for criminologists", Crime Media Culture An International Journal, 17(2) (2020):209-233.

Kerry Cameron F. "Protecting privacy in an AI-driven world", The Brookings Institution, (2020). 25 Ocak 2024, https://www.brookings.edu/articles/protecting-privacy-in-an-ai-driven-world/.

Kim Justın. "Artificial Intelligence And Crime: What Kıller Robots Could Teach About Criminal Law", Faculty of Law Victoria University of Wellington (2017): 36-38.

King Thomas C., Nikita Aggarwal, Mariarosaria Taddeo ve Luciano Floridi. "Artifcial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions", Science and Engineering Ethics, (26) (2019): 1-36.

Kılıçarslan Seda Kara. "Yapay Zekânın Hukuki Statüsü Ve Hukuki Kişiliği Üzerine Tartışmalar", Yıldırım Beyazıt Hukuk Dergisi, 4(2) (2019): 363-389.

Koca Mahmut ve İlhan Üzülmez. Türk Ceza Hukuku Genel Hükümler, 16.Baskı. Ankara: Seçkin Yayınevi, 2023.

Köken Enes. "Yapay Zekânın Cezai Sorumluluğu", Türkiye Adalet Akademisi Dergisi, 12(47) (2021): 247-487.

Lee Nicol Turner, Paul Resnick ve Genie Barton. "Algorithmic bias detection and mitigation: Best practices and policies to reduce consumer harms", The Brookings Institution, (2019). 24 Ocak 2024, https://www.brookings.edu/articles/algorithmic-bias-detection-and-mitigation-best-practices-and-policies-to-reduce-consumer-harms/.

Marr Bernard. "What Is the Difference Between Deep Learning, Machine Learning and AI?", Forbes, (2016).

Meske Christian, Enrico Bunde, Johannes Schneider ve Martin Gersch."Explainable Artificial Intelligence: Objectives, Stakeholders, and Future Research Opportunities", Information Systems Management, (2020): 1-10.

Miralis Nyman Gibson ve Dennis Miralis. "AI-enabled future Crime: Study reveals 20 disturbing possibilities". 18 Ocak 2024. https://ngm.com.au/ai-enabled-future-Crime-study/.

Murdoch Blake. "Privacy and Artificial Intelligence: challenges for protecting health information in a new era". BMC Medical Ethics, (22) (2021):1-5.

Newscientist Instant Expert. Düşünen Makineler: Yaklaşan Yapay Zekâ Çağı ve İnsanlığın Geleceği (Çeviren: Samet Öksüz). İstanbul: Say Yayınları, 2021.

Özbek Veli Özer, Koray Doğan, Serkan Meraklı, Pınar Bacaksız ve İsa Başbüyük. Türk Ceza Hukuku Genel Hükümler, 14.Baskı. Ankara: Seçkin Yayınevi, 2023.

Özgenç İzzet. Türk Ceza Hukuku Genel Hükümler, 19.Baskı, Ankara: Seçkin Yayınevi, 2023.

Pagallo Ugo. "Robots of Just War: A Legal Perspective". Philosophy & Technology, (24) (2011): 307–323.

Pizzi Michael, Mila Romanoff ve Tim Engelhardt. "AI for humanitarian action: Human rights and ethics", International Review of the Red Cross, 102(913) (2020): 145–180.

Popa Elena. "Human Goals Are Constitutive of Agency in Artificial Intelligence (AI)", Philosophy & Technology, (34) (2021):1731–1750.

Raposo Vera. "When facial recognition does not "recognise": erroneous identifications and resulting liabilities", AI & Socıety, (2023): 1-13.

Rigano Christopher. “Using Artificial Intelligence to Address Criminal Justice Needs”, National Institute of Justice Journal, (280) (2019).

Say Cem. 50 Soruda Yapay Zekâ. 22.Baskı, İstanbul: Bilim ve Gelecek Kitaplığı, 2022.

Selanik Adem Atakan. “Adam Çalıştıranın Sorumluluğu Kapsamında Yapay Zekâ Robotun Sorumluluğu ve

Sigortalanması Hususunun Değerlendirilmesi", Türkiye Adalet Akademisi Dergisi, (50) (2022): 335-364.

Selçuk Sami, Suç Genel Kuramı. Ankara: Seçkin Yayınevi, 2021.

Shankar Shreya, Yoni Halpern, Eric Breck, James Atwood, Jimbo Wilson, D. Sculley. "No Classification without Representation: Assessing Geodiversity Issues in Open Data Sets for the Developing World", 31st Conference on Neural Information Processing Systems (NIPS 2017), (2017): 1-5.

Shimrona Efrat, Jonathan Tamir, Ke Wanga ve Michael Lustig. "Implicit Data Crimes: Machine Learning Bias Arising From Misuseof Public Data", PNAS, 119(13) (2022): 1-11.

Simmler Monika ve Nora Markwalder. "Roboter in der Verantwortung?". Zeitschrift für die gesamte Strafrechtswissenschaft. 129(1) (2017): 20-47.

Sparrow Robert. "Killer Robots", Journal of Applied Philosophy, 24(1) (2007): 62-77.

Šucha Vladimir ve Jean-Philippe Gammel. Humans and Societies in the Age of Artificial Intelligence, Publications Office of the European Union, (Luxembourg: 2021).

Taddeo Mariarosaria ve Floridi Luciano, "Solving the symbol grounding problem: A critical review of fifteen years of research", Journal of Experimental and Theoretical Artificial Intelligence, 17(4) (2005): 419-445.

The Guardian. 28 Ocak 2024. https://www.theguardian.com/technology/2016/mar/24/tay-microsofts-ai-chatbot-gets-a-crash-course-in-racism-from-twitter.

Timur Demirbaş. Ceza Hukuku Genel Hükümler, 18.Baskı. Ankara: Seçkin Yayınevi, 2023.

Treleaven Philip, Jeremy Barnett, Daniel Brown, Andrew Bud, Enzo Fenoglio, Charles Kerrigan, Adriano Koshiyama, Sally Sfeir-Tait ve Martin Schoernig. "The Future of Cybercrime:

AI and Emerging Technologies Are Creating a Cybercrime Tsunami", UCL Theses, (2023):1-34.

Tziakouris Giannis. "The rise of AI-powered Criminal s: Identifying threats and opportunities", (2023), 20 Ocak 2024. https://blog.talosintelligence.com/the-rise-of-ai-powered-Criminal s/.

Vinuesa Ricardo, Hossein Azizpour, Iolanda Leite, Madeline Balaam, Virginia Dignum, Sami Domisch, Anna Felländer, Simone Daniela Langhans, Max Tegmark ve Francesco Fuso Nerini. "The role of Artificial Intelligence in achieving the Sustainable Development Goals", Nature Communıcatıons, (11) (2020):233-243.

Winston Patrick Henry. Artificial Intelligence, 3.Baskı. London: Pearson Yayınevi, 1992.

Hakem Değerlendirmesi: Çift kör hakem.

Finansal Destek: İlgili çalışma, Anadolu Üniversitesi Bilimsel Araştırma Projeleri Koordinasyon Birimi tarafından kabul edilen "Yapay Zekâ ve Cezai Sorumluluk" adlı proje adı ve 2209E169 numarasıyla proje kapsamında desteklenmektedir.

Çıkar Çatışması: Yazar çıkar çatışması bildirmemiştir.

Etik Kurul Onayı: Yazar etik kurul onayının gerekmediğini belirtmiştir.

Peer Review: Double peer-reviewed.

Financial Support: This study is supported by Anadolu University Scientific Research Projects Coordination Unit within the scope of the project titled 'Artificial Intelligence and Criminal Responsibility' and numbered 2209E169.

Conflict of Interest: The author has no conflict of interest to declare.

Ethics Committee Approval: The author stated that ethics committee approval is not required.