Medeniyet Kültürel Araştırmalar Belleteni, İMÜ Edebiyat Fakültesi Dergisi, Sayı: 7, Cilt: 4, 2024, s. 01-17, ISSN:2792-0348, doi: 10.60051/medbel.1585638

Yapay Zekâ Ve Suç: Gelecek Açısından Hukuksal Ve Etik Tehditler

Artificial Intelligence and Crime: Legal And Ethical Threats for the Future

Buse Nur TUFAN*

ÖZ

Yapay zekâ ile suç arasındaki ilişki, giderek daha fazla önem kazanan ve henüz gelişmekte olan bir araştırma alanı olarak değerlendirilebilir. Yapay zekânın hızla gelişen teknolojisi, suç işleme yöntemlerinden suçun tespitine kadar birçok alanda etkili olmaya başlamıştır. Ancak bu alandaki literatürün sınırlı olması, yapay zekâ ile suç arasındaki ilişkinin daha derinlemesine incelenmesi gerekliliğini doğurmaktadır. Aynı zamanda, yapay zekânın suçla ilişkisi, algoritmaların kötüye kullanımı, kişisel veri ihlalleri, manipülasyonlar, gözetim teknolojileri gibi birçok farklı boyutu içermekte olup çalışmanın sınırlandırılmasını gerektirecek kadar geniş bir konuyu kapsamaktadır. Bu çalışmanın amacı, yapay zekâ kullanılarak işlenebilecek suç türlerini analiz etmek, suç önleme ve tespitinde yapay zekânın sunduğu avantajları değerlendirmek, bunun yanı sıra bu teknolojinin etik ve hukuki sonuçlarını ele alarak olası riskleri belirlemektir. Özellikle, yapay zekâ teknolojilerinin kötü niyetli kullanım potansiyeli, toplum güvenliği üzerindeki etkileri ve hukuki düzenlemelerin gerekliliği gibi konulara odaklanarak bu araştırma ile literatüre katkı sunulması amaçlanmaktadır. Sonuç olarak yapay zekânın suçla ilişkisi üzerine yapılacak araştırmalar, sadece mevcut suçları önlemek ve tespit etmek için değil, aynı zamanda toplumun gelecekteki güvenliğini sağlamak için de kritik bir öneme sahiptir. Bu çalışmanın sağladığı analizler, yapay zekânın güvenli kullanımını destekleyecek etik ve hukuki çerçevelerin oluşturulmasına katkı sunmayı hedeflemektedir. Böylelikle, yapay zekânın toplum yararına kullanılması ve suç amaçlı kullanılmasının önlenmesi için gerekli adımların atılmasına yönelik değerlendirme yapılmıştır.

Anahtar Kelimeler: Yapay Zekâ, Suç, Etik, Hukuki, Gelecek, Toplumsal

ABSTRACT

The relationship between artificial intelligence and crime is increasingly gaining importance and is considered a research area still in development. The rapidly evolving nature of AI technology has begun to influence various fields, from crime commission methods to crime detection. However, the limited literature on this topic highlights the need for a more in-depth exploration of the connection between AI and crime. Additionally, the relationship between AI and crime encompasses a wide array of issues, including algorithm misuse, personal data violations, manipulations, and surveillance technologies, making it a broad topic that requires careful scope delimitation for focused study. The purpose of this research is to analyze the types of crimes that could be committed using AI, to assess the potential advantages of AI in crime prevention and detection, and to examine the ethical and legal implications of this technology while identifying possible risks. Specifically, by focusing on the malicious potential of AI technologies, their

* Yüksek Lisans Mezunu, Bursa Teknik Üniversitesi, Sosyoloji Bölümü, busetfnn@icloud.com, (https://orcid.org/0000-0001-9686-7589).

Gönderim Tarihi: 14 Kasım 2024 – Kabul Tarihi: 14 Aralık 2024

impact on public security, and the need for legal regulations, this study aims to contribute to the literature in this field. In conclusion, research on the relationship between AI and crime is critically important not only for preventing and detecting current crimes but also for ensuring the future safety of society. The analyses provided by this study aim to support the formation of ethical and legal frameworks that ensure the safe use of AI. Thus, it evaluates the necessary steps to promote the societal benefits of AI and prevent its misuse for criminal purposes.

Keywords*: *Artificial Intelligence, Crime, Ethics, Legal, Future, Social

Extended Summary

This study aims to analyze the potential of artificial intelligence (AI) in crime prevention and detection, as well as the risks of AI-based crime and misuse, along with the ethical and legal issues it brings. The impact of AI technologies on public safety and the necessity of regulations in this field are among the core focuses of the study. The research seeks to address AI's role in crime prevention and combating crime as an area offering both opportunities and threats, as well as the subject of committing crimes through AI.

AI offers remarkable advantages in crime prevention. Particularly, through its big data analytics capabilities, it can predict criminal tendencies, identify high-risk areas and individuals, and provide critical warnings to law enforcement. This facilitates preventing crimes before they occur and allows for more efficient resource allocation. However, the risk of these powerful tools being used for illegal activities by malicious actors should not be overlooked. For instance, the creation of fake identities, conducting cyberattacks, and fraud through social engineering methods are key areas where AI can be exploited.

To mitigate these risks, the ethical and legal framework for AI's use is of great importance. Legally, existing regulations must be reviewed, and new laws specific to these technologies should be established. Ethically, raising awareness to protect individuals' privacy rights is crucial. In this context, developing and disseminating awareness programs related to personal data protection is recommended. Such educational initiatives are expected to help individuals better understand their privacy rights and prepare them against potential violation risks.

In conclusion, to balance the opportunities and risks AI offers in crime prevention and combating crime, comprehensive regulations, oversight mechanisms, and community-level awareness initiatives play a critical role. This balance will not only enhance public safety but also ensure the protection of individual rights.

Giriş

Teknolojinin hızla gelişmesi ve her alanda yaygınlaşması, bireylerin yaşamında köklü değişimlere yol açmaktadır. Bu dönüşümde önemli rol oynayan teknolojilerden biri de yapay zekâdır. Günümüzde popülerliğini artıran yapay zekâ (YZ) kavramı, bu makalenin konusunu oluşturmaktadır. YZ alanında önemli ilerlemeler kaydedilmiş olsa da araştırmalar hala başlangıç aşamasındadır. YZ araştırmacıları, bu teknolojinin gelişimine katkı sağlayacak yeni buluşlar ve yenilikler üzerinde çalışmaya devam etmektedir (Demirhan, Kılıç, & Güler, 2010). Bu teknolojiler, çeşitli cihazlar ve uygulamalar üzerinden her platformda hizmet sunmaktadır. Akıllı ev cihazları, otonom araçlar ve akıllı telefon uygulamaları YZ teknolojilerinin günlük yaşamdaki örneklerindendir (İşler & Kılıç, 2021).

YZ terimi ilk kez John McCarthy tarafından, "akıllı makineler, özellikle de zeki bilgisayar programları geliştirme bilimi ve mühendisliği" olarak tanımlanmıştır (McCarthy, 2007). "Büyük veri" ve "YZ" kavramları, günümüz dünyasında günlük yaşamın ayrılmaz bir parçası haline gelmiştir. Amazon'un kasiyersiz mağaza uygulamaları, tanınmış markaların YZ destekli satış danışmanları, YZ tabanlı avukatlar, hakimler, doktorlar, cerrahlar ve televizyon

spikerlerinin yanı sıra, yakın dönemde bir okulda ders veren YZ destekli öğretim üyesi, bu teknolojilerin toplumsal ve profesyonel alanlarda giderek daha fazla yer bulduğuna işaret etmektedir (Yücel & Adiloğlu, 2019). YZ'nin iş süreçlerini otomatikleştirerek verimliliği artırması, büyük veri analizleri sayesinde hızlı karar alması, hayatı kolaylaştırması, tekrarlayan ve riskli işleri üstlenerek iş güvenliğini artırması, zaman tasarrufu sağlaması gibi olumlu yönlerini göz ardı etmemek gerekmektedir. Ancak YZ alanında yaşanan hızlı gelişmeler birçok sorunu da beraberinde getirmektedir. Örneğin, YZ'nin suça karışma veya suç işleme gibi eylemleri gerçekleştirme olasılığı, önemli bir tehlike olarak değerlendirilmektedir. YZ, teknoloji dünyasında devrim niteliğinde değişiklikler getirirken toplumsal ve etik sorunları oluşturmaktadır. YZ sistemlerinin suç işleme ve suça karışma kapasitesini anlamak, bu teknolojilerin toplum üzerindeki etkilerini ve hukuki düzenlemeleri şekillendirmek için kritik öneme sahiptir.

Bu çalışmada, YZ aracılığıyla işlenebilecek suçların yaratabileceği hukuki ve etik sorunlar kapsamlı bir şekilde ele alınmıştır. Çalışmanın temel soruları, YZ ile işlenmiş suç örneklerinin var olup olmadığı, suç işlenmesini önlemek amacıyla YZ destekli yazılımların geliştirilip geliştirilmediği, YZ ve suçla ilgili yasal düzenlemelerin kapsamının neler olduğu üzerine yoğunlaşmaktadır. Bu amaçla, literatür derinlemesine incelenmiş ve eleştirel bir inceleme yöntemi benimsenmiştir.

Literatürde yaygın olarak ele alınan konular, YZ ile işlenen suç türleri, YZ tüzüğü ve düzenlemeleri, YZ'nin neden olduğu hukuki ve etik sorumluluklar, YZ kaynaklı suçların hukuki uygunluğu ve bu konuların İslam ve Türk hukukunda nasıl değerlendirildiği gibi başlıklar etrafında toplanmıştır.

Bu çalışmayı diğer araştırmalardan ayıran en önemli özellik, YZ'nin gelecekte suç kaynaklı hukuki ve etik sorunlar yaratma potansiyelini birlikte değerlendirmesi ve bu sorunların etkilerinin daha geniş bir perspektiften ele alınmasıdır.

Metnin ilk bölümünde kısaca YZ'nin ne olduğundan, nasıl ortaya çıktığından, kavramsal çerçevesinden bahsedilecek; ardından YZ'nin farklı türleri ve uygulama alanları ele alınacaktır. İkinci bölümde ise kısaca suç kavramından bahsedilecektir. Son bölümde ise YZ sistemlerinin suçla ilişkisinin günümüz ve gelecek açısından taşıdığı potansiyel etik ve hukuksal problemlere değinilecektir.

Bu bağlamda, YZ sistemlerinin suç işleme potansiyelini incelemek, yalnızca teknik bir analiz değil, aynı zamanda toplumsal bir sorumluluktur. Örneğin, YZ'nin kötü niyetli kişiler tarafından nasıl manipüle edilebileceği, bu teknolojilerin kullanımındaki en büyük tehditlerden biridir.

Ayrıca, YZ'nin suç öncesi, suç anı ve suç sonrası süreçlerdeki rolü, toplumun güvenliği açısından dikkate alınmalıdır. YZ tabanlı güvenlik sistemleri, suçların önlenmesine yönelik önemli bir araç olabilirken bu sistemlerin yanlış kararlar verme ihtimali de bulunmaktadır. Bu nedenle, YZ uygulamalarının etik standartlara ve hukuki çerçevelere uygun olarak geliştirilmesi gerekmektedir. Sonuç olarak YZ'nin hem fırsatlar sunan hem de riskler barındıran bir alan olduğunun altı çizilmelidir.

1. Yapay Zekâ

YZ kavramı farklı şekillerde tanımlanabilmektedir. Örneğin Pirim, YZ'yi, zekâ kavramından ayırarak tanımlamaktadır. Ayrıca, YZ'yi anlayabilmek için öncelikle bilgisayarla beyin arasındaki farklılıklar ve benzerliklerin anlaşılması gerektiğinin altını çizmektedir (Pirim, 2006, s. 86). Kaya ve Engin (2005) ise YZ'nin, insan zihninin işleyişini anlamayı ve buna benzer şekilde çalışan bilgisayar süreçlerini geliştirmeyi amaçlayan bir alan olduğunu vurgulamışlardır. YZ'nin tanımlanmasındaki çeşitlilik, büyük ölçüde YZ'nin çok disiplinli yapısından kaynaklanmaktadır. YZ'yi tanımlayan en basit çerçevede, makinelerin insan benzeri öğrenme, algılama, problem çözme ve karar verme yeteneklerini taklit etme becerisi olarak ifade

edilmektedir. Ancak, farklı alanlarda çalışan araştırmacıların ve uygulamacıların bu yetenekleri kendi ihtiyaçlarına göre yorumlamaları, farklı tanımların ve yaklaşımların ortaya çıkmasına neden olmaktadır. Örneğin, bilgisayar bilimleri perspektifinde farklı bir tanım mevcutken psikoloji veya felsefe perspektifinde farklı tanımlamalar mevcuttur.

Literatüre göre, YZ kavramının ilk kez ortaya çıkışıyla ilgili çeşitli görüşler mevcuttur. 1950'lerde Alan Turing'in "Makineler Düşünebilir mi?" sorusuyla makine öğrenimi üzerine tartışmalar başlamış ve bu süreç YZ'nin temellerinin atılmasına zemin hazırlamıştır. 1956 yılında John McCarthy, Dartmouth Konferansı'nda ilk kez "YZ" terimini kullanarak bu kavramı literatüre kazandırmıştır (Şenses Aksu, 2023). YZ'nin gelişiminde öncü olan iki önemli isim Alan Turing ve John McCarthy'dir (Arslan, 2020). Bazı kaynaklara göre ise bilgisayarın mucidi olarak bilinen Alan Turing, YZ hikayesini başlatan kişi olarak kabul edilmektedir (Larson, 2022). Slage, YZ'yi "sezgisel programlama" olarak tanımlamıştır. Benzer bir bakış açısıyla Axe, YZ'yi, yalnızca önceden tanımlanmış sorunlara çözümler sunmakla kalmayıp beklenmedik durumlarda da uygun tepkiler üretebilen zeki yazılımlar olarak görmektedir (Nabiyev, 2012). YZ insan davranışlarıyla ilgili özellikler sergilemektedir. Doğal dili işleme, problem çözme, öğrenme, uyum sağlama ve algılama gibi insan zekâsına özgü nitelikler YZ'de de gözlemlenmektedir (Tecuci, 2012). Özetle, YZ hakkında çeşitli tanımlamalar mevcuttur. Genel anlamda, bu tanımlamalar insan benzeri zekâ ve düşünme süreçlerini taklit eden teknolojiler geliştirme amacını öne çıkarmaktadır.

Bilgisayarların ve algoritmaların, genellikle insan zekâsı gerektiren öğrenme, mantık yürütme ve problem çözme gibi görevleri gerçekleştirmek amacıyla kullanılması, YZ olarak tanımlanır (Aras vd., 2021). YZ mantık ve matematik temelinde doğan bir alandır. Teknolojiyle ilişkili olan mantık türüne "Bulanık mantık" denir ve YZ alanında kullanılmaktadır. YZ'de kullanıldığı için "teknoloji mantığı" olarak da adlandırılmaktadır. İnsana benzeyen robotların, bulanık mantıktan faydalanarak en yaygın insan davranışlarını sergilemesi beklenmektedir. Aslında, YZ'nin ortaya koyduğu yeni düzen ya da düzensizlik, bulanık mantığın çok değerli yapısından kaynaklanmaktadır (Gültekin, 2021). Bu çerçevede bulanık mantık, teknolojiye adapte edilmekte ve YZ'nin gelişimine katkı sağlamaktadır. Bulanık mantık ve YZ arasındaki ilişki, özellikle belirsizlik ve karmaşık problemlerin çözümünde oldukça önemlidir. Bulanık mantık, geleneksel ikili mantığın (doğru / yanlış, 1/0) ötesine geçerek belirsiz veya kısmen doğru olan verileri de ele almaktadır. YZ, birçok durumda belirsizlikle ve muğlaklıkla başa çıkmak zorundadır. Tam da bu noktada bulanık mantık, YZ'ye esneklik kazandıran yöntem sunmaktadır.

YZ, insan zekâsı ile bir tutulmamalıdır. YZ, insanlar tarafından belirli bir kapasitede sağlanan verilerle, gerçek dünyayı matematiksel olarak modellemeye çalışır. Bunu, girdilerle ilişkili olduğu varsayılan çıktılar üzerinde çalışarak ve aralarındaki istatistiksel bağlantıları keşfederek gerçekleştirir. İnsanlar ise gözlem ve deneyim yoluyla, kişisel ya da başkalarının tecrübelerinden neden-sonuç ilişkisi kurarak zaman içinde öğrenirler. Buna karşılık, YZ bu öğrenme sürecini, istatistiksel bağlantılar kurarak aynı anda gerçekleştirme yetisine sahiptir. Bu nedenle, insanın öğrenme süreci ile YZ'nin öğrenme süreci hem benzerlikler hem de farklılıklar taşımaktadır (Abanoz Öztürk, 2024 Ara Rapor).

Chul Han (2017), insan ve makinenin "düşünme" biçimlerini şeffaflık kavramı üzerinden tartışarak bu iki düşünme biçimi arasında bir zıtlık olduğunu öne sürmüştür. Ona göre, makinenin düşünme şekli net hesaplamalara ve şeffaflığa dayanırken insanın düşünme tarzı deneyimlere ve çeşitliliğe dayanır.

> *Aslında heyecanlanma veya derin etkilenme anlamına gelen tin (Geist) kendine karşı asla şeffaf değildir. Kendine karşı şeffaflıktan bir huzursuzluk, derin bir etkilenme doğmaz. Sürekli şeffaflık talebinin temelinde, her türlü olumsuzluktan azade bir dünya ideası, hatta insan ideası yatar. Ama sadece bir makine tamamen şeffaf olabilir. Şeffaf bir iletişim, insanın yapamayacağı, ancak makinelerin becerebileceği bir iletişim olurdu.* (Chul Han, 2017, s. 104).

Özetle, insanın düşünce ve duygularında şeffaf olamayacak kadar karmaşık ve derin olduğunu, bu yüzden tam şeffaflık arayışının insana uygun olmadığını savunmaktadır. Ona göre, şeffaf ve net iletişim ancak makineler için mümkündür; insanlar ise doğaları gereği bu tür bir iletişime erişemez.

YZ, genellikle işlevsellik, yetenek ve uygulama alanlarına göre iki ana kategoriye ayrılmaktadır: dar YZ (zayıf YZ) ve geniş YZ (güçlü YZ). Dar YZ, dış müdahale ile çalışan ve belirli komutları yerine getiren, tepkisel yapıya sahip daha basit yazılımlardan oluşur. Geniş YZ ise daha gelişmiş yazılımlar kullanarak otonom bir şekilde karar verebilen ve genellikle "Bilişsel Robot" olarak bilinen daha karmaşık bir YZ türüdür (Benli & Şenel, 2020).

> *Zayıf YZ, nispeten uzunca bir süredir hayatımızda olan bir kavramdır. Amazon'un satın almış olduklarınıza ve / veya ilgilendiğiniz kategorilere göre bizlere ürün önermesi, Netflix'in daha önce izleme istatistiklerimizi gözeterek bizlere film önermesi ve öneri sistemindeki görsellerde kişiselleştirmeye gitmesi, Spotify'ın dinlediğimiz müzikleri gözeterek bize benzer müzikler önermesi uzunca bir süredir hayatımızda olan ve zayıf YZ olarak nitelendirebileceğimiz sistemlerdir.* (Binbir, Sevtap, 2021).

Tıbbi görüntüleri analiz etmek için kullanılan bir YZ, sadece belirli algoritmalarla görüntü işleyip yorum yapar; ancak bu dar kapsamın ötesine geçemez. Kendi başına öğrenerek yeni durumlara adapte olan ve insan gibi karmaşık problemleri çözme yeteneği gösteren bir robot, geniş YZ kapsamına girer. Bu YZ türü, sağlık hizmetlerinden savunma sanayine, akıllı şehir planlamasından eğitim sistemlerine kadar geniş bir yelpazede kullanılma potansiyeline sahiptir.

YZ'nin gelişimi, geçmişten aldığı unsurlar ve bu unsurları kendine entegre etmesiyle hız kazanmıştır. Günümüzde birçok alanda kullanılmakta olup gelecekte daha geniş bir kullanım alanına sahip olması planlanmaktadır. Günlük yaşamda, iş yerinde kullanılan bilgisayar tabanlı sistemlerden, ev temizliğinde kullanılan robot süpürgelere, araçlardaki navigasyon sistemlerinden bankacılık işlemlerini yöneten hesaplara kadar birçok alanda YZ sistemlerinden yararlanılmaktadır. YZ, alışveriş sitelerinden telefonlardaki arama uygulamalarına kadar geniş bir kullanım alanına sahiptir (Özgeldi, 2019). Günümüzde giderek daha önemli bir yer edinen YZ sistemleri, insanların günlük aktiviteleri ve iş rollerinin ötesinde, bakış açıları, eğlence anlayışları ve yaşam tarzları üzerinde de derin etkiler yaratmaktadır (Altun, 2019).

YZ'nin en önemli kullanım alanlarından birisi sanayidir. Sanayi devrimi, buharlı makinelerle başlamış, ardından elektrik ve otomasyon teknolojilerinin gelişimiyle ilerlemiştir. Günümüzde ise akıllı fabrikalar ve robotik üretim süreçlerini içeren Sanayi 4.0 ile devam etmektedir (Kaya, 2021). Sanayi 4.0 devriminin getirdiği faydaların en üst düzeyde kullanılması ve risklerin en aza indirilmesi, toplumsal, ekonomik ve çevresel sürdürülebilirlik açısından büyük önem taşımaktadır. Bu devrim, dünya genelinde hem endüstriyel hem de hizmet sektörlerinde robotlara olan talebi ve arzı hızla artırmaktadır (Fırat & Fırat, 2017).

YZ günümüzde, daha çok bireylerin yaşam kalitesini artırmak amacıyla kullanılmaktadır. Örneğin, arama motorları ve otomatik kelime düzelticiler, günlük yaşamın yaygın birer parçası haline gelmiştir. Ancak YZ'nin faydaları bireysel alanla sınırlı kalmamaktadır. Son bilimsel çalışmalar, YZ'nin şehir planlaması, otonom ulaşım ve akıllı tarım gibi alanlarda en verimli çözümleri sunabildiğini göstermektedir. Bu çözümlerin toplum hayatımıza tam anlamıyla entegre edilememesinin sebebi, YZ'nin bu kullanımının toplumsal düzeni köklü bir şekilde değiştirme potansiyeline sahip olmasıdır (Köroğlu, 2017). Özetle, YZ sanayiden finansa, eğitimden sağlığa, otomasyondan hizmet sektörüne kadar birçok alanda kullanılmakta ve etkisinin belirginleşmesi planlanmaktadır.

2. Suç Kavramı

Türkiye Cumhuriyeti Adalet Bakanlığı'nın resmî web sitesinde yer alan bilgilere göre, toplumsal düzenin korunması için gerekli hukuki değerlerin bilinçli ve isteyerek ihlaline, *kast* adı verilmektedir. Bu değerleri koruyan kurallara karşı özensizlik *taksir* olarak adlandırılırken bu özensizliği ifade eden insan davranışı ise *suç* olarak tanımlanmaktadır. Suç yalnızca kanunla düzenlenmektedir. Suç, Türk Ceza Kanunu'nda veya ceza hükmü içeren özel kanunlarda yer alan, hukuka aykırı ve cezai yaptırıma tabi eylemlerden oluşur. Suç, bir haksızlıktır; ancak her haksızlık suç sayılmaz (T.C. Adalet Bakanlığı, 2020). Suç, yasa tarafından cezalandırılan veya topluma zarar verdiği ya da tehlikeli olduğu yasa koyucu tarafından kabul edilen ve açıkça tanımlanan eylem ve davranışlardır (Çopur, Ulutaşdemir, & Balsak, 2015).

Suç, toplumsal bir olgudur. Suçluya ait fizyolojik ya da biyolojik özelliklerden ziyade, suç, toplumsal koşulların bir sonucudur ve her toplumda varlığını sürdürür. Bununla birlikte, toplumsal değişime paralel olarak suçun kapsamı, niteliği, suç işleme yöntemleri, suç oranları ve suçla mücadele yollarının da değiştiğini vurgulamak gerekir. Örneğin, bilişim, iletişim ve ulaşım teknolojilerinde yaşanan gelişmelerin getirdiği küreselleşme dinamikleri, siber suçlar, çevrim içi dolandırıcılık, kredi kartı ve telefon sahtekârlığı gibi yeni suç türlerinin doğmasına zemin hazırlamıştır. Aynı zamanda, geleneksel suçlar daha karmaşık şekillerde işlenebilir hale gelmiştir (Yüksel, 2019, s. 5).

Tarihsel süreç boyunca her dönemde varlığını sürdüren suç olgusu, biyolojik, psikolojik ve sosyolojik teorilerle açıklanmaya çalışılmıştır (Bingöl, 2022). *Suç* kavramını incelerken başvurulması gereken önemli konulardan birisi *suç sosyolojisi*dir. Suç sosyolojisi, suçun toplumsal boyutlarını inceleyen bir disiplin olarak karşımıza çıkmaktadır. Sosyolojik olarak açıkça ifade edildiğinde *suç*, toplumsal normların ihlal edilmesi şeklinde ortaya çıkan bir davranıştır (Bingöl, 2022).

> *Suç, bireyler, toplumlar ve kültürler arasında karmaşık bir etkileşim ağı içinde gelişen bir olgudur. Sosyoloji, suçun kökenlerini anlamak ve suçun toplumsal dinamiklerini çözümlemek adına bireylerarası, toplumsal / kültürel etkenlere odaklanarak önemli bir perspektif sunar. Bireylerarası etkenler, suçun temelini oluşturan önemli unsurlardan biridir. Bireylerin kişisel özellikleri, psikolojik durumları ve sosyal ilişkileri, suç eğilimini etkiler. Örneğin, çocukluk travmaları, aile içi şiddet ya da psikolojik sorunlar, bireyin suça yönelme olasılığını artırabilir. Bireyin içsel dünyasındaki çatışmalar ve kişisel deneyimler, suç işleme eğilimini şekillendirebilir* (Akbaş, 2024).

Suç sosyolojisi, suçun toplumsal ve kültürel kökenlerini anlamaya yönelik bir disiplin olup suçun toplumları etkileyen karmaşık bir olgu olarak farklı boyutlarını incelemeyi amaçlar (Akbaş, 2024). Suç sosyolojisinde çeşitli suç kuramları mevcuttur. Ancak bu makalede suç kuramları detaylı bir şekilde ele alınamayacak olup kısaca konuya değinmekle yetinilecektir. Tüm teoriler, belirli bir bakış açısına ve toplumsal sorunlar ile yapılar temel alınarak geliştirilmiş, kendi içinde yetersizlikler ve eksiklikler barındıran yaklaşımlardır (Güllü, 2014). "Sosyolojik Suç Teorileri"nin öncülerinden bazıları Robert Ezra Park, Emile Durkheim, Walter Reckless, Clifford Shaw, Ernest Burgess ve Frederick Thrasher'dir (Siegel, 2012). Suça sosyolojik bir bakış açısıyla yaklaşan "Sosyal Süreç Teorileri", suçlu ve sapkın davranışların bir nesilden diğerine, bir topluluktan diğerine, bir gruptan başka bir gruba ya da bireyler arasında öğrenme ve kültürel aktarım yoluyla geçtiğini savunan teorilerdir. Nötrleştirme teknikleri kuramlarına göre, bu yaklaşım, bireylerin toplumsal norm ve değerlere tamamen kayıtsız kalmamalarına rağmen neden hala suç işlediklerini açıklamaya çalışır (Bingöl, 2022).

Özetle, birden fazla suç kuramı bulunmaktadır ve suçu farklı perspektiflerden ele almaktadırlar. Modern toplumun değişen şartları ile birlikte suç kuramlarına eleştiriler getirilmiş ve genişletilmesi gerektiği literatürde sıklıkla vurgulanmıştır.

3. Hukuksal ve Etik Tehditler: Yapay Zekânın Suçta Kullanımı ve Geleceği

Metnin bu bölümünde, YZ sistemlerinin suçun önlenmesi ve suça karışması gibi konular kapsamlı bir şekilde ele alınmaktadır. Bu bağlamda, YZ'nin mevcut hukuki düzenlemelere tabi olup olmadığı derinlemesine analiz edilecek, YZ'nin suçla ilişkili kullanımı açısından etik problemlere dikkat çekilecektir. Ayrıca, mevcut yasal çerçevelerle birlikte önerilen yeni düzenlemeler değerlendirilerek bu teknolojilerin toplumsal ve hukuki etkileri üzerinde durulacaktır.

Yüz tanıma sistemleri ve otonom silah sistemlerinin kötü niyetli kişiler tarafından kullanılması durumu, askeri ve sivil alanlarda büyük riskler doğurabilecektir. Bu bağlamda, YZ'nin suçta kullanılma riski, sadece bireylerin değil, uluslararası güvenlik ve etik standartların da yeniden değerlendirilmesini gerektirmektedir. YZ'nin suçla ilişkisini düzenleyen hukuki çerçeve henüz tam anlamıyla oluşmamış olsa da çeşitli ülkeler bu konuda adımlar atmaktadır. Uluslararası düzeyde, YZ'nin suçta kullanılmasının önüne geçmek için standartlar ve düzenlemeler geliştirilmektedir. Yapay Zekâ Tüzüğü (AI Act-Tüzük)'ne göre Avrupa Konseyi tarafından belirtilen güvenli, güvenilir ve etik YZ'nin geliştirilmesinde Birliğin küresel lider olma hedefi desteklenmektedir ve Avrupa Parlamentosu tarafından özellikle talep edilen etik ilkelerin korunmasını sağlamak amaçlanmaktadır (Commission, COM (2021) 206 final, 2021/0106 (COD)). Tüzüğün ilk taslağı, yüz tanıma teknolojilerinin temel haklar ve insan haklarına yönelik oluşturabileceği kabul edilemez riskler nedeniyle bu teknolojiyi tamamen yasaklamayı öngörmektedir. Ancak, son taslakta bu yasak bir ölçüde gevşetilmiş gibi görünmektedir (Gültekin-Várkonyi, 2024 Ara Rapor). Gültekin-Várkonyi, özellikle yüz tanıma teknolojilerinin etik ve insan haklarına uygun olacak şekilde kullanımını artırmak amacıyla düzenlenmesi gerektiğinin altını sıklıkla çizmiştir. YZ'nin etik ve hukuki sorunlarını ele almak, sadece teknoloji geliştiricileri değil, aynı zamanda yasama organları ve toplumun tüm kesimleri için önemli bir görevdir. YZ sistemlerinin nasıl çalıştığını anlamak, olası riskleri ve etik sorunları minimize etmek için gereklidir. Ayrıca, YZ'nin tasarım aşamasında etik prensiplere uyulması, sistemlerin güvenliğini ve toplum üzerindeki etkilerini iyileştirebilir. Etik açıdan, YZ sistemlerinin tasarımında şeffaflık, hesap verebilirlik ve insan haklarına saygı, temel ilkeler olarak benimsenmelidir. YZ'nin suça karışmasını önlemek için algoritmalarda insan denetiminin sağlanması, eğitim ve denetim mekanizmalarının oluşturulması önem taşımaktadır.

YZ sistemlerinin suça karışmasının yanı sıra suçun önlenmesinde kritik öneme sahip olduğu vurgulanmalıdır. YZ gibi ileri teknolojik araçlar, suçları önceden tespit etme ve engelleme konusunda önemli bir etkiye sahip olabilir. YZ, suç faaliyetlerini belirleme, analiz etme ve bildirme konusundaki yetenekleriyle büyük bir potansiyele sahiptir. YZ'nin veri analizi, tahmin becerileri, sosyal medya izleme, gözetim sistemleri, ses analizi gibi yetenekler sayesinde suçu önlemesi mümkündür. Suçun önlenmesi alanında YZ'nin ihbar kapasitesi çeşitli avantajlar sunsa da bu durum bazı sınırlamalar ve hukuki sorunları da beraberinde getirir. Öncelikle, YZ'nin doğruluk oranı ile yanlış pozitif ve negatif sonuçlar üretme riski göz önünde bulundurulmalıdır. Yanlış bir ihbar, masum bireylerin haksız yere suçlanmasına, lekelenmeme hakkının ihlaline veya gizlilik haklarının zedelenmesine yol açabilir. Bu nedenle, YZ'nin kullanımı sırasında doğruluk oranının maksimum düzeye çıkarılması ve hukuki güvencelerin sağlanması büyük önem taşır (Varlı, 2023).

Örneklendirilmesi gereken konu suç tespitinde YZ araçlarının kullanılmasıdır. Örneğin, Amerika'da 2013 yılından bu yana aktif olarak kullanılan Predpol yazılımı, polis kayıtlarına erişimin yanı sıra polislerin doğru zamanda doğru yere ulaşmalarını sağlamaktadır. Bu yazılım, suçun ne zaman ve nerede işleneceğini öngörebilme kapasitesine sahiptir (Akkuş, 2019). RAND

Corporation tarafından yayınlanan rapora göre tahmine dayalı polislik yöntemleri 4 genel kategoriye ayrılmaktadır:

1. Suçları Tahmin Etme: Suçların yoğunlaşabileceği yer ve zamanları önceden belirlemeye yönelik tekniklerdir.

2. Suçluları Tahmin Etme: Gelecekte suç işleme potansiyeli olan bireyleri saptamaya çalışır.

3. Faillerin Kimliğini Tahmin Etme: Suç profilleri oluşturarak belirli suçları muhtemel faillerle eşleştirir.

4. Mağdurları Tahmin Etme: Suçun kurbanı olabilecek grupları veya bireyleri tanımlamayı amaçlar (Walter L. Perry, 2013).

Amerika'da kullanılan Predpol yazılımı ile Almanya ve İsviçre gibi bazı Avrupa ülkelerinde kullanılan Precobs yazılımı, potansiyel suç mahallini ve failleri tespit etmeye yönelik YZ araçları arasında yer almaktadır (Abanoz Öztürk, 2024 Ara Rapor). Abanoz Öztürk çalışmasında suç konusunda tasarlanan YZ araçlarını detaylı bir şekilde değerlendirmiş olup çalışma sonucunda çeşitli bulgular elde etmiştir. Çalışmanın sonucunda, suç davranışını öngörmeye yönelik YZ araçlarının, kişilerin somut bir suçu işlemesinden ziyade geçmiş verilerine dayanarak risk teşkil eden özellikleri belirleyip kişileri gruplandırdığı, böylece kolektif bir sorumluluk yarattığını belirtmiştir. Bu sistemde, bireyler topluma uyumluluklarına göre değerlendirilmekte ve benzer özellikler taşıyan diğer suç işlemiş kişilerle gruplandırılmaları, o bireylerin de suç işleme riski taşıdığı varsayımına dayandırılmaktadır. Bu durum, ceza sorumluluğunun şahsiliği ve masumiyet karinesi ilkelerine aykırı olarak değerlendirilmiştir. Ayrıca, eksik veya hatalı veriler nedeniyle algoritmaların ön yargılı ve ayrımcı sonuçlar üretebildiği bulgularına yer verilmiştir. YZ araçlarının "kara kutu" haline gelmesi halinde ise nasıl çalıştıklarının anlaşılamayacağı ve yazılımı üretenin bile açıklayamayacağı bağlantıların, adil yargılanma ilkesi ve savunma hakkı açısından sorun yaratabileceğini tespit etmiştir. YZ, suça karışma potansiyeli, suç tespiti gibi konularla ilgili etik ve hukuki sorunlarıyla birlikte gelmektedir. Bu teknolojilerin gelişimiyle, toplumsal güvenliği ve etik değerleri korumak için güçlü düzenlemeler ve standartlar oluşturulmalıdır. YZ'nin sağladığı avantajların yanı sıra, bu risklere karşı da proaktif bir yaklaşım benimsemek, daha güvenli ve adil bir toplum oluşturmanın anahtarı olabilecektir.

YZ alanında farklı uzmanlıklar ve çalışma alanları olduğundan, bu teknoloji üzerinde çalışan uzmanlar bile YZ sistemlerinin tüm işleyişine tamamen hâkim olamayabilirler. Bu, YZ'nin özellikle karmaşık ve kritik kararlar alması gereken durumlarda önemli bir denetim sorununu beraberinde getirir. Örneğin, bir YZ sistemi suç işleme potansiyeli olan bireyleri ya da durumları analiz edip ihbar etme görevini üstlendiğinde, onun yanlış karar verme ihtimali, yanlış pozitif veya yanlış negatif sonuçlar üretme riski, önemli bir endişe kaynağı haline gelir.

> *Gerçeğin hızla dijitalleşmesi, gerçeği kuran şeye teknik erişimi de hızlandırır, aynı şekilde bu erişimi gerçekleştiren dillere erişim de hızlanır ve bilgi bu yolla da üretilmiş olur. Artık zorunlu olan geçiş bu alanda gerçekleşir. Uzman ise bu alanla profesyonel olarak en yakından iştigal eden kişidir. Bilgi işleme düşüncesi, uzmana daha en başından bir mantık ve dil bahşetmiş, gerçeğin her bir vasfını formüllere dökmesini uzmanlığın hızla her alana, her şeyden önce de politikaya nüfuz etmesine yarayan araçlar sağlamıştır. Modern uzman gerçeği gündelik anlarda –veya bu anların ardışıklığında– şekillendirecek araçlara sahip olan kişidir, geleceğe dönük tercihlere açık bir perspektif içinde ise pek bir gücü yoktur.* (Balandier, 2023, s. 166-167).

İnsan uzmanlarda olduğu gibi, YZ sistemlerinin de dar uzmanlık alanlarına göre tasarlandığını varsayarsak sistem bir alana odaklandığında diğer önemli verileri göz ardı edebilir. Tıpkı bir kol uzmanının kalple ilgili bir sorunu gözden kaçırabileceği gibi, bir YZ sistemi de sadece belirli bir veri setine veya modele odaklanarak suçla ilişkili karmaşık ve çok yönlü

durumları doğru bir şekilde değerlendiremeyebilir. Bu da YZ'nin suç tespiti ve önlenmesinde hatalı ihbarlarda bulunmasına veya tehlikeli durumları göz ardı etmesine neden olabilir. Bu çerçevede, "uzman iktidarı" kavramı da önem kazanmaktadır. YZ sistemlerinin hangi suç unsurlarını tanımlayacağı ve nasıl hareket edeceği büyük ölçüde bu sistemleri geliştiren uzmanlar tarafından belirlenir. Tıpkı psikiyatride bir doktorun hastanın ruh sağlığı konusunda nihai otorite olması gibi, YZ alanında da uzmanlar sistemin hangi suçları veya suçluları "göreceğini" belirleyen bir güç ve otorite sahibidir. Bu, YZ'nin tarafsızlığını sorgulamamıza yol açar ve suçla mücadelede YZ kullanımının denetlenebilir, şeffaf ve güvenilir bir yapıya kavuşturulmasının gerekliliğini ortaya koyar.

İleri düzey YZ algoritmaları, siber saldırılar, dolandırıcılık ve kişisel verilerin çalınması gibi suçlarda etkili olabilir. Bu tür uygulamalar, YZ'nin suça karışma ihtimalini en belirgin şekilde göstermektedir. Büyüksağiş (2021) çalışmasında, kişisel verilerin YZ tarafından izinsiz depolanması, işlenmesi ve paylaşılmasının, temel haklara zarar verebileceğini ve ayrımcılığa yol açabileceğini vurgulamıştır. Yine aynı çalışmada, KVKK'nin revize edilmesi gerektiğini, ihlallerin sonuçlarının bu şekilde telafi edileceğini aynı zamanda da veri sorumlularının ve veriyi işleyenlerin, algoritmik kararları insan denetiminden geçirmeye teşvik edeceğinin altını çizmiştir. Bu şekilde, ayrımcılık riskini azaltmak amacıyla önemli kararların makine ve insan iş birliğiyle alınmasını sağlayacak hibrit bir model oluşturulmasının özendirileceğini vurgulamıştır (Büyüksağiş, 2021). Bu doğrultuda düşünüldüğünde, kişisel verilerin YZ kaynaklı ihlal edilmesi sonucunda suç işlenebilecektir. Bu durum ise özel hayatın gizliliğine tehlike teşkil edebilecek ve toplumsal düzeni bozabilecektir. Aynı zamanda hukuki ve etik problemler gündeme gelebilecektir. Özellikle, bireylerin mahremiyet ihlali, güven erozyonu, ayrımcılık riski, şeffaflık eksikliği, bilgi manipülasyonu gibi problemler örnek verilebilir.

Kişisel Verileri Koruma Kurumu tarafından hazırlanan "Yapay Zekâ Alanında Kişisel Verilerin Korunmasına Dair Tavsiyeler" adlı rapora göre, YZ'nin, bireylerin temel hak ve özgürlüklerini koruyarak kişisel verilerin korunması çerçevesinde doğru şekilde yönetilmesi gerekmektedir. Kişisel veri işleyen YZ çalışmaları, 6698 Sayılı Kişisel Verilerin Korunması Kanunu ve ikincil mevzuata uygun olmalıdır. İnsan hakları ve onurunun korunması ön planda tutulmalı, kişisel veri işlemede hukuka uygunluk, dürüstlük, ölçülülük, hesap verebilirlik ve şeffaflık ilkelerine uyulmalıdır (KVKK, 2022). Tablo 1'de dil modellerinin şeffaflık oranları yer almaktadır.

Tablo 1. Dil modelleri şeffaflık oranları

Foundation Model Transparency Index Scores by Major Dimensions of Transparency, May 2024

Source: May 2024 Foundation Model Transparency Index

Major Dimensions of Transparency	ADEPT Fuyu-8B	AI21labs Jurassic-2	Aleph Alpha Luminous	amazon Titan Text Express	Anthropic Claude 3	servicenow StarCoder	Google Gemini 1.0 Ultra	IBM Granite	Meta Llama 2	Microsoft Phi-2	Mistral AI Mistral 7B	OpenAI GPT-4	stability.ai Stable Video Diffusion	WRITER Palmyra-X	Average
Data	0%	60%	40%	0%	10%	100%	0%	60%	40%	40%	20%	20%	40%	50%	34%
Labor	0%	43%	71%	14%	14%	100%	29%	43%	29%	100%	100%	14%	100%	43%	50%
Compute	14%	86%	100%	0%	14%	100%	14%	100%	71%	57%	14%	14%	43%	86%	51%
Methods	0%	100%	100%	50%	75%	100%	75%	100%	75%	100%	100%	50%	75%	100%	79%
Model Basics	83%	100%	100%	83%	50%	100%	83%	100%	100%	100%	100%	50%	100%	100%	89%
Model Access	100%	67%	100%	67%	67%	100%	67%	67%	100%	100%	100%	67%	100%	33%	81%
Capabilities	80%	80%	100%	80%	100%	100%	80%	60%	100%	100%	100%	100%	60%	100%	89%
Risks	0%	57%	57%	43%	86%	100%	43%	71%	71%	29%	14%	57%	14%	14%	47%
Mitigations	0%	40%	20%	20%	40%	0%	40%	80%	60%	0%	60%	60%	0%	20%	31%
Distribution	57%	86%	100%	57%	86%	100%	57%	86%	71%	71%	71%	71%	86%	71%	77%
Usage Policy	40%	100%	100%	80%	100%	100%	100%	40%	40%	100%	40%	80%	60%	80%	76%
Feedback	67%	100%	67%	33%	33%	100%	67%	67%	33%	67%	67%	33%	67%	33%	60%
Impact	29%	29%	29%	0%	14%	14%	29%	0%	14%	0%	14%	14%	14%	14%	15%
Average	**36%**	**73%**	**76%**	**41%**	**53%**	**86%**	**53%**	**67%**	**62%**	**66%**	**62%**	**49%**	**58%**	**57%**	

Kaynak: Stanford University, "The Foundation Model Transparency Index", https://crfm.stanford.edu/fmti/, E.T: 26.10.2024 (The Foundation Model Transparency Index, 2024)

Tablo 1 incelendiğinde Veri (Data), Riskler (Risks) ve Etkiler (Impact) boyutlarında oranlar oldukça düşüktür. Bu durum, çoğu modelin verilerinin kaynakları veya potansiyel risk ve etkiler hakkında yeterince bilgi sunmadığını göstermektedir. Modellerin genel şeffaflık ortalaması %47 olarak görünmektedir. Bu, genel olarak iyileştirme potansiyeli olabileceğini göstermektedir. Özellikle veri, riskler ve etkiler gibi daha düşük puan alan alanlarda şeffaflık artırılabilir. Şeffaflık seviyeleri, modelin güvenliği, toplumsal etkisi ve kullanıcı tarafından nasıl kullanılabileceği konusunda önemli bilgiler sunmaktadır. Şeffaflık oranlarının düşük olduğu alanlarda, model kullanıcılarının daha fazla bilgiye ihtiyaç duyabileceği anlaşılmaktadır.

YZ sistemlerinin suça karışma potansiyeli, teknik hatalar, algoritma ön yargıları ve sistemlerin zayıf noktalarından kaynaklanabilecektir. Örneğin, bir otonom araç, yazılım hatası veya algoritma yanlılığı nedeniyle kazalara neden olabilir. Bu tür durumlar, YZ sistemlerinin sorumluluğunu ve hukuki yükümlülüklerini sorgulatmaktadır. Otonom araçların neden olduğu bir kaza veya anlaşmazlık durumunda sorumluluğun kimde olduğu problemi, ancak yasal düzenlemelerle çözülebilecektir (Bayındır, 2021). Bayındır aynı çalışmasında, araçları seviye 0 ile seviye 5 arasında değerlendirmiştir. Seviye 0 otonom sistemin olmadığı günümüzdeki birçok aracı kapsamaktadır. Seviye 1, 2, 3 ve 4 otonom sürüş sistemlerinde, araçta bir insan sürücünün bulunması gerekirken seviye 5 tam otonom bir sistem olarak tanımlanır ve sürücüye ihtiyaç duyulmamaktadır. Bu doğrultuda da ilk 4 seviyenin mevcut mevzuata uygun olduğunu belirtmiştir. Çalışma genelinde otonom araçların kaza durumlarındaki sorumluluk dağılımını ele almıştır. Araç sürücünün kontrolündeyken kaza olursa klasik olarak sürücü sorumlu tutulmaktadır. Ancak araç tam otonom durumdayken kaza meydana gelirse bu durumda araç üreticisinin sorumlu tutulabileceğini belirtmiştir. Fakat, araç üreticisinin her durumda sorumlu tutulması, teknolojinin gelişimini olumsuz etkileyebileceğinden, sorumluluğun paylaştırılması gerektiği vurgulamıştır. Bu bağlamda, zorunlu mali sigortanın kapsamının otonom araçları da içerecek şekilde genişletilmesi gerektiği ve mevzuatta değişiklik yapılmasının faydalı olabileceğini ifade etmiştir. Yan ürün üreticisinin sorumluluğuna dair bir düzenleme olmadığını ve bu konuda hukuki mevzuatın güncellenmesi gerektiğinin altını çizmiştir (Bayındır, 2021).

Çekin (2018) ise çalışmasında, gelişen teknolojilerin karmaşıklığı ve yazılımların hata riski nedeniyle üreticilerin ürün sorumluluğunun arttığını belirtmiştir. Bu sebeple, üreticilerin yeni teknolojilerle ilgili ürünlerini tanıtırken potansiyel tehlikelere de dikkat çekmelerinin önem taşıdığını vurgulamıştır. Üreticinin, otomasyon sistemini siber saldırılardan korumak için tüm önlemleri alması gerekliliğinin altını çizmiştir. Aksi takdirde, yeterli koruma sağlamayan araçların hatalı olarak değerlendirileceğini vurgulamanın yanı sıra, aracın işlevsel ve güvenli olabilmesi için dış müdahalelere karşı korunmasının zorunluluğunu belirtmiştir (Çekin, 2018). Sonuç olarak otonom araç teknolojilerinin gelişimi, hukuki sorumluluk ve yükümlülüklerin yeniden ele alınmasını gerektirmektedir. YZ sistemlerinin hataları ve ön yargıları, bu sistemlerin kazalara yol açabilme potansiyeli nedeniyle, sorumluluğun paylaşımı önem kazanmaktadır. Otonom araçların kaza durumunda üreticinin, yan üreticisinin ve ilgili tarafların sorumluluğunu düzenleyen yasal çerçevelerin oluşturulması elzemdir. Ayrıca, zorunlu mali sigorta gibi mevcut sigorta sistemlerinin otonom araçları da kapsayacak şekilde genişletilmesi, bu tür teknolojilerin güvenli bir şekilde gelişmesini destekleyecektir. Teknoloji firmalarının ürünlerinin potansiyel risklerini açıkça belirtmesi ve siber güvenlik tedbirlerini en üst düzeyde sağlaması da toplum ve birey güvenliği için kritik önemdedir.

Caldwell ve arkadaşları (2020) gerçekleştirdikleri çalışmada, yüksek endişe uyandıran suçlar, orta derecede endişe uyandıran suçlar, düşük endişe uyandıran suçlar olmak üzere üç grup şeklinde YZ ve suç ilişkisini ele almışlardır. Bu bağlamda yüksek endişe uyandıran suçlar,

sesli / görsel taklit, silah olarak kullanılan sürücüsüz araçlar, kişiye özel kimlik avı, YZ kontrollü sistemleri bozma, büyük çaplı şantaj, YZ tarafından yazılmış sahte haberler olarak sıralanmıştır. Orta derecede endişe uyandıran suçlar, *Askeri robotların kötüye kullanılması, yetersiz teknoloji ürünleri, eri zehirlenmesi, öğrenme tabanlı siber saldırılar, otonom saldırı dronları, çevrim içi tahliye, yüz tanıma sistemlerini yanıltma, piyasa saldırıları* olarak sıralanmıştır. Düşük endişe

uyandıran suçlar ise *ön yargı istismarı, hırsız botlar, YZ'yi atlatma, YZ destekli sahte yorumlar, YZ destekli takip, sahtekârlık* olarak sıralanmıştır (Caldwell, Andrews, Tanay, & Griffin, 2020). Bu suçların hukuki ve etik sonuçlarını değerlendirirken YZ kullanımıyla ortaya çıkabilecek tehditlerin bireyler, toplum ve hukuk sistemi üzerinde karmaşık etkiler yaratabileceğini söylemek mümkündür. Hukuki açıdan, yüksek endişe uyandıran suçlar kategorisindeki suçların, genellikle büyük ölçekli zarar, terör ve ciddi suç geliri sağlama potansiyeline sahip olduğu vurgulanmalıdır. Sesli / görsel taklit, YZ kontrollü sistemleri bozma gibi faaliyetler dolandırıcılık, kimlik hırsızlığı, siber saldırı suçları kapsamında değerlendirilmektedir ve ağır cezalar öngörülebilir. Silah olarak kullanılan sürücüsüz araçlar, terörizm ve kasten adam öldürme gibi suçlarla bağlantılı olacağından ulusal güvenlik yasaları kapsamında daha ağır ve hızlı yanıtlar gerektirmektedir. Bu gibi durumlar için yasaların, YZ'nin suçlarda kullanılmasını engellemeye yönelik düzenlemeler içerecek şekilde güncellenmesi önem taşımaktadır. Etik açıdan düşünüldüğünde, büyük çaplı şantaj ve kişiye özel kimlik avı gibi suçlar, bireylerin mahremiyeti ve güvenliği üzerinde derin etik kaygılar doğurabilir. YZ'nin bu tür zararlara olanak tanıyacak şekilde kötüye kullanılmasını önlemek için teknoloji geliştirenlerin ve kullanıcıların etik rehberlik ve sınırlamalarla yönlendirilmesi önem taşıyacaktır. Ayrıca YZ tarafından yazılmış sahte haberler, bilgiye erişim ve bireylerin doğru bilgilenme hakkını tehdit ederek toplumun güvenilir kaynaklara olan güvenini zedeleyebilir.

Sonuç olarak YZ'nin sınırsız potansiyeli göz önünde bulundurulduğunda daha kapsamlı bir düzenleme ve sürekli güncellenen bir hukuk sistemi gerekli olabilecektir. YZ'nin suç amacıyla kullanılması, yalnızca suç işleyenlerin değil, aynı zamanda bu teknolojileri sağlayan şirketlerin de sorumluluğuna odaklanılmasını gerektirmektedir. Etik açıdan, toplumsal fayda ve zarar dengesi önemlidir; bu nedenle hem kullanıcıların bilinçlendirilmesi hem de teknolojinin etik kullanımını destekleyen rehberler geliştirilmesi elzemdir.

Son olarak YZ sayesinde işlenen gerçek suç olaylarından bahsetmek, konunun kapsamını vurgulamak açısından önemlidir. YZ, kimlik avı, derin sahtecilik, finansal dolandırıcılık ve bilgi hırsızlığı gibi suçların daha sofistike ve inandırıcı bir şekilde işlenmesine olanak tanımaktadır. Bu tür suçlar, YZ teknolojilerinin kötüye kullanılabileceğini ve bu durumun hukuki, etik ve güvenlik açısından ciddi riskler doğurabileceğini göstermektedir. Dolayısıyla, YZ'nin sunduğu avantajların yanında, olası tehditlere karşı farkındalık ve güvenlik önlemlerinin artırılması gereklidir.

New York'ta yaşanan bir olay, YZ uygulamalarının hukuk gibi hassas alanlarda nasıl kullanılması gerektiğine dair önemli bir tartışma yaratmıştır. Davanın bir tarafının avukatları, dilekçe hazırlama sürecinde ChatGPT'yi kullanmış ve uygulamanın sunduğu bilgileri doğrulamadan, doğrudan mahkemeye sunmuştur. ChatGPT, kendisine verilen talebe yanıt olarak bazı örnek yargı kararları üretmiştir, ancak bu kararlar gerçekte mevcut değildir. Avukatlar, ChatGPT tarafından üretilen bu kararları mahkemeye sunduklarında, olayın gerçek dışı olduğu ortaya çıkmıştır.

Mahkeme, avukatların bu ihmalkâr davranışlarını dikkate alarak hem dilekçeyi hazırlayan iki avukata hem de onların çalıştığı hukuk bürosuna 5.000 dolar para cezası vermiştir. Bu olay, YZ araçlarının, özellikle güvenilirliği çok önemli olan hukuki belgelerde dikkatle ve doğrulama yapılarak kullanılması gerektiğini gösteren bir örnek olarak öne çıkmıştır. Aynı zamanda, YZ'nin sunduğu bilgilerin her zaman doğru veya geçerli olmayabileceğine dikkat çekmiştir ve bu durum, hukuki sorumluluk açısından ciddi sonuçlar ortaya koymuştur (Merken, 2023).

Hong Kong'da meydana gelen bir olayda, bir finans çalışanı, İngiltere'deki şirket merkezinde görev yapan finans müdüründen 25,6 milyon dolarlık bir transfer talebi içeren bir mesaj almıştır. İlk başta bu mesajın bir kimlik avı girişimi olabileceğinden şüphelenen çalışan, yine de emin olmak amacıyla şirketin finans müdürü ve tanıdığı diğer iş arkadaşlarıyla görüntülü görüşmeler yapmıştır. Ancak daha sonra, bu görüşmelere katılan kişilerin derin sahtecilik

teknolojisiyle oluşturulmuş sahte görüntüler olduğu anlaşılmıştır. Çalışan, durumu ancak merkez ofisle irtibata geçtikten sonra fark edebilmiştir, fakat o sırada istenen para çoktan transfer edilmiştir ve dolandırıcılık gerçekleştirilmiştir (Sheng, 2024).

Bu gibi durumların engellenmesi amacıyla belli önlemler alınması gerekmektedir. Prof. Dr. Kırık, siber korsanların kişisel verileri ele geçirmek amacıyla orijinal web sitelerinin birebir kopyalarını oluşturduğunu belirtmiştir. Bu tür "şeytani ikiz" olarak adlandırılan kopya siteler, kullanıcıları sahte sayfalara yönlendirerek veya SMS ve e-postalar yoluyla kandırarak verilerini çalmaktadır. Banka, e-ticaret ve e-devlet gibi yaygın platformların sahte versiyonlarına bilgi giren kullanıcıların, farkında olmadan tüm kişisel verilerini saldırganların eline geçirmiş olduklarını ifade etmiştir. Cihaz güvenliği için uygulama güncellemelerinin önemini vurgulayan Prof. Dr. Kırık, aynı zamanda şifre güvenliği için çift faktörlü doğrulamanın aktif edilmesi gerektiğinin altını çizmiştir. Çift faktörlü doğrulamanın, şifrenin başkalarının eline geçmesi durumunda bile SMS kodu gibi ek güvenlik katmanlarıyla koruma sağladığını da belirtmiştir (TRT, 2024). Son olarak ülkemizde, mevcut verilerin başka bir yere iletilmesi, Türk Ceza Kanunu'nun 244. maddesinin 2. fıkrası kapsamında suç teşkil etmektedir (T.C Resmi Gazete, 2004).

Bu gibi durumlara, daha katı ve yasal düzenlemelerin getirilmesi büyük önem taşımaktadır. Siber saldırılarla ilgili cezalar artırılarak caydırıcılık sağlanabilir. Kişisel verilerin korunması hakkında mevcut yasal çerçevenin genişletilmesi gerekmektedir. Bu kapsamda, veri ihlali durumlarında firmaların hızlı bildirim yapması ve sorumluluk almasının zorunlu hale getirilmesi önem taşımaktadır. Etik açıdan, bireylerin dijital güvenlik konularında bilinçlenmesi oldukça önem taşımaktadır. Kamu hizmetleri ve özel şirketler, kullanıcılarına bilgi güvenliği hakkında düzenli olarak eğitimler ve bilgilendirici kampanyalar sunabilirler. Başka bir açıdan, sosyal mühendislik saldırılarına karşı kullanıcıların nasıl davranmaları gerektiği, hangi tür bağlantılara tıklamamaları gerektiği gibi konularda kamu spotları veya ücretsiz eğitimlerin sağlanması önemlidir.

İspanya'nın Badajoz kentinde, 15 çocuk, kız çocuklarının görüntülerini sosyal medyadan almış ve YZ ile uygunsuz hale getirmişlerdir. 15 çocuk, görüntüleri manipüle etmek ve yaymakla ceza almışlardır. Badajoz Çocuk Mahkemesi, bu çocukları çocuk pornografisi ve ahlaki bütünlüğe karşı suçlardan sorumlu bulmuştur ve her birine bir yıl süreyle denetimli serbestlik cezası vermiştir. Mahkeme, bu denetimli serbestlik tedbirinin, cinsel duygusal eğitim, bilgi ve iletişim teknolojilerinin sorumlu kullanımı, eşitlik ve toplumsal cinsiyet farkındalığı gibi konularda eğitim içerikleri ile desteklendiğini vurgulamıştır (Demiroğlu, 2024). YZ teknolojilerinin kötüye kullanımını ve dijital içeriklerin manipülasyonunu engellemek için geniş kapsamlı hukuki düzenlemelerin yapılması önem taşımaktadır. Bu gibi düzenlemelerle, kişilerin izni olmadan dijital içeriklerinin değiştirilmesini ve paylaşılmasını yasaklayarak izin dışı içerik oluşturma ve paylaşmaya ciddi yaptırımlar getirilmelidir. Çocukların dijital mahremiyet hakları hakkında hem ailelere hem de çocuklara bilgilendirme yapılması, bu tür ihlallerin önlenmesine yardımcı olabilecektir. Sosyal medya şirketlerinin bu tür içerikleri tespit etme ve hızlıca kaldırma sorumluluğunu yerine getirmemesi durumunda idari para cezaları gibi yaptırımlar uygulanması önem taşımaktadır. Çocuklar ve gençler için zorunlu eğitim programları kapsamında dijital etik ve sorumlu teknoloji kullanımı gibi konulara yer verilmesi faydalı olabilecektir. Bu eğitimlerde, YZ'nin sorumlu kullanımı, dijital etik, mahremiyet ve toplumsal cinsiyet farkındalığı gibi konulara odaklanılması gerekliliği dikkat çekmiştir.

YZ ile işlenebilecek suçların geleceğine dair bazı önemli hukuki ve etik tehditler öngörülmektedir. YZ'nin hızla gelişmesi, hem yasal düzenlemeleri zorlamakta hem de toplumsal etik değerler üzerinde çeşitli tehditler oluşturmaktadır. YZ, kimlik avı ve sosyal mühendislik saldırılarını daha hedefli ve etkili hale getirebilecektir. Hukuki açıdan, bu tür kişiye özel saldırıları düzenleyen kişilerin yargılanması ve sorumlu tutulması güçleşebilecektir. Ayrıca, bu tür saldırılarda mağdurların tazminat hakkının korunması da zorlaşabilecektir. YZ'nin kendi başına karar verebildiği veya eylemlerini özerk olarak gerçekleştirebildiği durumlarda sorumluluk tartışmaları doğabilir. Bir YZ sisteminin bir suça neden olması durumunda sorumluluğun kime

ait olacağı net bir şekilde belirlenmelidir. Bu bağlamda, YZ'nin geliştirilmesinden sorumlu olan kişiler veya şirketler mi, yoksa YZ'yi kullananlar mı sorumlu tutulmalıdır? Gelecekte olası sorunları önlemek için bu soruların netleştirilmesini sağlayacak yasal düzenlemelere ihtiyaç olduğu söylenebilir.

Aydın (2023) çalışmasında, teknoloji etiğini kapsamlı bir şekilde ele almış ve bilim ile teknolojinin etik rehberliğinde ilerlemesi gerektiğini vurgulamıştır. YZ'nin insan yaşamı üzerindeki olumsuz etkilerine, doğal kaynakların tükenme riskine, artan eşitsizliklere, kişisel verilerin kötüye kullanılmasına ve mahremiyet ihlallerine dikkat çekerek bu etik sorunlara çözümler bulunmasının önemini sıkça dile getirmiştir. YZ ile kişisel verilerin izinsiz olarak toplanması, işlenmesi ve yayılması, mahremiyet hakkı üzerinde ciddi tehditler oluşturmaktadır. Mahremiyetin korunması için kişisel veri güvenliğine yönelik yasal düzenlemeler yapılmış olsa da YZ'nin gelişimiyle birlikte bu düzenlemelerin daha kapsamlı hale getirilmesi önem taşımaktadır.

YZ sistemleri, yanlış veya ön yargılı veri setleriyle beslendiğinde, toplumsal ayrımcılığı pekiştirebilecektir. Özellikle eğitim, sağlık ve istihdam, adalet gibi alanlarda eşitsizlikleri artıran kararlar verebilecektir. Bu durum etik açıdan, sosyal adalet ve eşitlik değerlerini zedeleyerek toplumsal yapıyı olumsuz etkileyebilecektir. Türkçetin (2021, s. 70), YZ ile ilgili adalet tartışmalarının büyük ölçüde algoritmik adalet etrafında şekillendiğini vurgulamıştır. YZ sistemlerinin tasarım ve uygulama süreçleri, bireylere, topluluklara veya gruplara karşı adaletsizlik yaratmamalıdır.

YZ ile oluşturulan sahte içerikler (örneğin, deepfake videolar) bireylerin itibarını zedeleyebilir. Bu tür etik ihlaller, bireylerin onurunu koruma ilkesine aykırıdır ve yanlış bilgilerin yayılmasına yol açarak toplumda yanlış yargılar oluşmasına neden olabilecektir. YZ'nin insanlarla güven ve adalet içinde çalışabilmesi, şeffaflık, sorumluluk ve hesap verebilirlik ilkelerine dayanan sağlam bir etik temel üzerine kurulmasıyla mümkün hale gelebilir (Yeşilkaya, 2022). YZ'nin insanlık yararına hizmet etmesi için her zaman insan kontrolünde olması gereklidir. Ancak, özerklik kazanan sistemlerin yanlış kararlar vermesi veya zararlı davranışlarda bulunması, etik olarak kabul edilemez sonuçlara yol açabilir.

Özetle YZ, suçun önlenmesi ve suçla mücadelede hem fırsatlar hem de riskler barındırmaktadır. Suç önleme açısından, YZ sistemleri büyük miktarda veriyi analiz ederek potansiyel suç faaliyetlerini öngörebilir, riskli bölgeleri veya bireyleri belirleyebilir ve yetkilileri zamanında uyarabilir. Bu durum, polis ve güvenlik birimlerinin suçları gerçekleşmeden önce önlem almasına olanak tanır. Ancak, YZ'nin suç amaçlı kullanım riski de göz ardı edilmemelidir. Kötü niyetli kişiler tarafından YZ, sahte kimlik üretiminden siber saldırılara veya sosyal mühendislik yöntemleriyle yapılan dolandırıcılıklara kadar çeşitli yasa dışı faaliyetlerde kullanılabilir. Bu nedenle, YZ'nin suçla mücadelede doğru ve etik bir çerçevede kullanılması için hukuki düzenlemeler ve denetim mekanizmaları önem taşımaktadır.

Sonuç

YZ'nin suç önleme ve suç işleme alanlarında sağladığı yenilikler, hem güvenlik birimleri hem de yasa koyucular açısından dikkatle ele alınması gereken bir dönüm noktasını işaret etmektedir. YZ teknolojilerinin gelişmesi, suç önleme konusunda büyük miktarda veriyi hızlı ve etkili bir şekilde analiz ederek potansiyel suç faaliyetlerini öngörme, risk altındaki bölgeleri belirleme ve gerektiğinde yetkililere uyarıda bulunma gibi işlevleriyle suçla mücadelede önemli avantajlar sunmaktadır. Bu yönüyle, YZ sistemlerinin polis güçlerine operasyonel hız ve hassasiyet kazandırdığı, böylece suçların önlenmesinde etkin bir araç haline geldiği söylenebilir. Örneğin, gelişmiş yüz tanıma sistemleri veya risk analiz algoritmaları sayesinde suç işlenme ihtimali olan bölgelerde önleyici tedbirler alınabilmekte, bu da toplum güvenliğini artırma potansiyeli taşımaktadır.

Bununla birlikte, YZ'nin kötüye kullanılması riski de göz ardı edilmemelidir. YZ teknolojileri, kötü niyetli kişilerce kötüye kullanılarak çok çeşitli yasa dışı faaliyetlerde bir araç olarak karşımıza çıkmaktadır. Örneğin, sahte kimlik ve belgeler üretmek, gelişmiş siber saldırılar düzenlemek ya da sosyal mühendislik teknikleri ile insanları yanıltarak özel bilgilere erişim sağlamak gibi farklı suç türlerinde YZ'nin sunduğu yeteneklerden faydalanılabilmektedir. Ayrıca, kişisel bilgilerin izinsiz olarak toplanması, manipülatif içeriklerin üretilmesi ve sahte haberlerin hızla yayılması gibi durumlar da YZ'nin yanlış ellerde bir tehdit haline gelebileceğini göstermektedir. Bu durum, YZ'nin yalnızca suçla mücadelede değil, suç işlenmesi bağlamında da yeni ve karmaşık zorluklar sunduğunu ortaya koymaktadır.

Bu bağlamda, YZ'nin suçla mücadelede etkili ve güvenilir bir araç olarak kullanılabilmesi için etik, güvenlik ve gizlilik konularında kapsamlı yasal düzenlemelere ihtiyaç duyulduğu sonucuna varılmıştır. YZ'nin yanlış pozitif veya yanlış negatif sonuçlar üreterek masum bireylerin haksız yere suçlanmasına veya tehlikeli durumların göz ardı edilmesine yol açma olasılığı, hukuki ve teknik denetim mekanizmalarının gerekliliğini vurgulamaktadır. Ayrıca, YZ sistemlerinin belirli bir tarafsızlıkla çalışmasını sağlamak amacıyla düzenleyici kurumlar tarafından sıkı denetimlerin yapılması elzemdir. YZ'nin suçla mücadelede etik ve etkili bir biçimde kullanılmasını sağlamak için, teknoloji geliştikçe bu alanlarda sürekli olarak güncellenen yasal çerçevelerin ve düzenlemelerin yürürlüğe girmesi önem taşımaktadır. Bu tür yasal ve etik önlemler, toplumun güvenliğini sağlamak ve YZ teknolojilerinin sorumlu bir şekilde gelişimini teşvik etmek açısından temel bir gereklilik olarak öne çıkmaktadır.

YZ'nin suça karışması konusunda etik ve hukuki sorunlar ele alındığında, mevcut yasaların geliştirilmesi gerekliliği öne çıkmaktadır. Etik açıdan ise bireylerin mahremiyetini korumak amacıyla farkındalığı artırmaya yönelik eğitim programlarının düzenlenmesi önerilmektedir. Bu eğitimlerin, bireylerin kişisel verilerinin korunması konusunda bilinçlenmelerini sağlaması ve mahremiyet haklarının ihlali riskini azaltmasına katkı sunması beklenmektedir. Özellikle okullarda zorunlu eğitim programlarının uygulanması, genç bireylerin kişisel verilerinin güvenliği ve mahremiyet hakları konusunda bilinçlenmelerine katkı sağlayacaktır. Bu tür eğitimlerin, toplumsal farkındalığı artırarak mahremiyet ihlallerinin önüne geçilmesine ve etik değerlere dayalı bir teknoloji kullanım kültürünün yerleşmesine yardımcı olması önerilmektedir.

KAYNAKLAR

Abanoz Öztürk, B. (2024 Ara Rapor). Suç Davranışını Öngören Üretken Yapay Zekâ Araçlarının Ceza Muhakemesi Hukukunun Temel İlkeleri Bağlamında Değerlendirilmesi. *Üretken Yapay Zekâ ve Hukuki Meseleler* (s. 12-31). İstanbul: İstanbul Barosu.

Akbaş, A. (2024). Suç Sosyolojisi: Türkiye'deki Hapishanelerin Mekânsal ve Zamansal Bağlamı. *Güvenlik Çalışmaları Dergisi, 26*(1), 104-131.

Akkuş, T. (2019, 10 27). *Öngörücü Polislik (Predpol)*. 10 26, 2024 tarihinde Tolga Akkuş: https://www.tolgaakkus.com/2019/10/27/ongorucu-polislik-predpol/#:~:text=Polis%20kay%C4%B1tlar%C4%B1na%20ula%C5%9Fabilen%20bu%20yaz%C4%B1l%C4%B1m,2013%20y%C4%B1l%C4%B1ndan%20beri%20aktif%20durumda. adresinden alındı

Altun, D. (2019). Sanal Gerçeklik ve Yapay Zeka. G. ed. Telli içinde, *Yapay Zeka ve Gelecek* (s. 139-157). İstanbul: Doğu Kitabevi.

Aras Bozkurt, Abdulkadir Karadeniz, David Baneres, Ana Elena Guerrero-Roldán ve M. Elena Rodríguez. (2021). Artificial Intelligence and Reflections from Educational Landscape: A Review of AI Studies in Half a Century. *Sustainability*, *13*(2), 1-16.

Arslan, K. (2020). Eğitimde Yapay Zeka ve Uygulamaları. *Batı Anadolu Eğitim Bilimleri Dergisi*, 11(1), 71-88.

Aydın, İ. (2023). Teknoloji Etiği: Teknolojinin Karanlık Yüzü Üzerine Tartışmalar. *Felsefe Dünyası Dergisi* (77-Ek), 5-37.

Balandier, G. (2023). *Sahnelenen İktidar.* (Ö. Karakaş, Dü.) İstanbul: Türkiye İş Bankası Kültür Yayınları.

Bayındır, S. (2021). Otonom Araçlarda Sözleşme Dışı Hukuki Sorumluluk Hallerinin Değerlendirilmesi. *Hukuk Fakültesi Dergisi*, 7(2), 383-410.

Benli, E., & Şenel, G. (2020). Yapay Zekâ ve Haksız Fiil Hukuku. *ASBÜ Hukuk Fakültesi Dergisi*, 2(2), 296-336.

Binbir, Sevtap. (2021). Pazarlama Çalışmalarında Yapay Zeka Kullanımı Üzerine Betimleyici Bir Çalışma. *Yeni Medya Elektronik Dergisi*, *5*(3), 314-328.

Bingöl, İ. (2022). Sosyolojik Suç Teorilerine Kuramsal Bir Yaklaşım: Sosyal Süreç Teorileri. *Bingöl Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 24, 640-652.

Büyüksağiş, E. (2021). Yapay Zeka Karşısında Kişisel Verilerin Korunması ve Revizyon İhtiyacı. *Yeditepe Üniversitesi Hukuk Fakültesi Dergisi*, 18(2), 529-541.

Caldwell, M., Andrews, J. T., Tanay, T., & Griffin, L. (2020). AI-enabled Future Crime. *Crime Science*, 1-4.

Çekin, M. S. (2018). Otonom Araçlar ve Hukuki Sorumluluk. *Türkiye Adalet Akademisi Dergisi*, 9(33), 283-301.

Chul Han, B. (2017). *Şiddetin Topolojisi.* İstanbul: Metis Yayınları.

Commission, E. (COM (2021) 206 final, 2021/0106 (COD)). *Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts.* Brussels.

Çopur, E., Ulutaşdemir, N., & Balsak, H. (2015). Çocuk ve Suç. *Uluslararası Katılımlı III. Çocuk Gelişimi ve Eğitimi Kongresi* "*Erken Müdahale*". 1. Ankara: Hacettepe University Faculty of Health Sciences Journal.

Demirhan, A., Kılıç, Y. A., & Güler, İ. (2010). Tıpta Yapay Zeka Uygulamaları. *Yoğun Bakım Dergisi*, 9(1), 31-41.

Demiroğlu, E. S. (2024, 07 10). *Yapay zekanın korkunç kullanımı! Kız çocuklarının görüntülerini kullandılar*. 11 2024 tarihinde haber7com. adresinden alındı.

Fırat, O. Z., & Fırat, S. Ü. (2017). Endüstri 4.0 Yolculuğunda Trendler ve Robotlar. *İstanbul Üniversitesi İşletme Fakültesi Dergisi*, 46(2), 211-223.

Gazete, T. R. (2004, 10 12). *Türk Ceza Kanunu*. 11 2024 tarihinde T.C Cumhurbaşkanlığı Mevzuat Bilgi Sistemi: https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=5237&MevzuatTur=1&MevzuatTertip=5 adresinden alındı.

Güllü, İ. (2014). Suç Olgusuna Teorik Ve Eleştirel Bir Yaklaşım. *KMÜ Sosyal ve Ekonomik Araştırmalar Dergisi* , 16((Özel Sayı I)), 104-107.

Gültekin, A. (2021). Klasik Mantıktan Bulanık Mantığa Yapay Zeka Serüveni. *Bingöl Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 11(22), 697- 714.

Gültekin-Várkonyi, G. (2024 Ara Rapor). Yüz Tanıma Teknolojileri ve Yapay Zekâ Tüzüğü. *Üretken Yapay Zekâ ve Hukuki Meseleler* (s. 7-11). İstanbul: İstanbul Barosu.

İşler, B., & Kılıç, M. Y. (2021). Eğitimde Yapay Zekâ Kullanımı ve Gelişimi. *Yeni Medya Elektronik Dergisi*, 5(1), 1-11.

Kaya, İ., & Engin, O. (2005). Kalite İyileştirme Sürecinde Yapay Zekâ Tekniklerinin Kullanımı. *Pamukkale Üniversitesi Mühendislik Bilimleri Dergisi*, 11(1), 103-114.

Kaya, M. (2021). Sanayi 4.0'da Yapay Zekâ ve Türkiye. *Fırat Üniversitesi. İİBF Uluslararası İktisadi ve İdari Bilimler Dergisi*, 5(2), 63-94.

Köroğlu, Y. (2017). Yapay Zeka'nın Teorik ve Pratik Sınırları. 1-10.

Larson, E. J. (2022). *Yapay Zekâ Miti: Bilgisayarlar Neden Bizim Gibi Düşünemez.* (K. Y. Us, Çev.) Fol.

McCarthy, J. (2007, 10 12). *What Is Artificial Intelligence?* 10 2024 tarihinde Computer Science Department, Stanford University: https://www-formal.stanford.edu/jmc/whatisai.pdf adresinden alındı.

Merken, S. (2023, 06 26). *New York lawyers sanctioned for using fake ChatGPT cases in legal brief*. 11 2024 tarihinde Reuters: https://www.reuters.com/legal/new-york-lawyers-sanctioned-using-fake-chatgpt-cases-legal-brief-2023-06-22/ adresinden alındı

Nabiyev, V. V. (2012). *Yapay Zeka: İnsan-Bilgisayar Etkileşimi* (Ankara b.). Seçkin Yayıncılık.

Özgeldi, M. (2019). Yapay Zeka ve İnsan Kaynakları. G. ed. Telli içinde, *Yapay Zeka ve Gelecek* (s. 198-222). İstanbul: Doğu Kitabevi.

Pirim, H. (2006). YAPAY ZEKA. *Journal of Yasar University*, 1(1), 81-93.

Sheng, E. (2024, 02 14). *Generative AI financial scammers are getting very good at duping work email*. 11 2024 tarihinde CNBC: https://www.cnbc.com/2024/02/14/gen-ai-financial-scams-are-getting-very-good-at-duping-work-email.html adresinden alındı.

Siegel, L. J. (2012). *Criminology, Wadsworth: (11. Edition).* Wadsworth Publishing.

Suç Nedir? (2020). 10 2024 tarihinde T.C. Adalet Bakanlığı Mağdur Bilgilendirme: https://magdurbilgi.adalet.gov.tr/298/Suc-Nedir#:~:text=Su%C3%A7%2C%20T%C3%BCrk%20Ceza%20Kanununda%20veya,ve%20cezai%20yapt%C4%B1r%C4%B1ma%20ba%C4%9Flanm%C4%B1%C5%9F%20eylemlerdir. adresinden alındı.

Şenses Aksu, M. (2023). Makine-İnsana ve Yapay Zeka İle Sosyal Bilim İlişkisine Dair Bir Eleştiri Denemesi. 470-483. The 17th International Scientific Research Congress -Social and Educational Sciences Asos Yayınları.

Tecuci, G. (2012). Artificial Intelligence. *WIREs Computational Statistics, 4*(2), 168-180.

The Foundation Model Transparency Index. (2024). 10 2024 tarihinde Stanford University: https://crfm.stanford.edu/fmti/May-2024/index.html adresinden alındı.

TRT. (2024, 10 25). *Suçlular dolandırıcılık yöntemlerine "yapay zekayı" da alet etti*. 11 2024 tarihinde TRTHABER: https://www.trthaber.com/haber/yasam/suclular-dolandiricilik-yontemlerine-yapay-zekayi-da-alet-etti-884392.html adresinden alındı.

Türkçetin, A. Ö. (2021). Etik Yapay Zeka Tasarımı. U. Köse içinde, *Yapay Zeka Etiği* (s. 63-81). Ankara: Nobel.

Varlı, V. (2023, 06 29). *Veri Analitiği Temelli Suç Önleme: Yapay Zekanın İhbar Rolü*. 10 2024 tarihinde EGE OLAY: https://www.egeolay.com/yazarlar/av-vefa-varli/veri-analitigi-temelli-suc-onleme-yapay-zekanin-ihbar-rolu/693/ adresinden alındı.

Walter L. Perry, B. M. (2013). *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations.* RAND Corporation.

Yapay Zekâ Alanında Kişisel Verilerin Korunmasına Dair Tavsiyeler. (2022, 05 18). 10 2024 tarihinde Kişisel Verileri Koruma Kurumu: https://www.kvkk.gov.tr/ adresinden alındı.

Yeşilkaya, N. (2022). Yapay Zekâya Dair Etik Sorunlar. *Şarkiyat İlmi Araştırmalar Dergisi*, 14(3), 949-963.

Yücel, G., & Adiloğlu, B. (2019). Dijitalleşme- Yapay Zeka ve Muhasebe Beklentiler. *Muhasebe ve Finans Tarihi Araştırmaları Dergisi , Temmuz* (17), 47-60.

Yüksel, M. (2019). Klasik Suç Kuramları. F. ed. Güllüpınar içinde, *Suç Sosyolojisi* (s. 3-31). Eskişehir: Anadolu Üniversitesi.