



International Journal of Social Sciences

ISSN:2587-2591

DOI Number:<http://dx.doi.org/10.30830/tobider.sayi.23.17>

Volume 9/3

2025 p. 272-292

RUTİN AKTİVİTE TEORİSİ (RAT) BAĞLAMINDA YAPAY ZEKÂ VE SUÇ

ARTIFICIAL INTELLIGENCE AND CRIME IN THE CONTEXT OF RAT

Ayşe Mahinur TEZCAN*

ÖZ

İnsanların tasarladığı, makinaların kullandığı bir zekâ türü olan yapay zekânın gelişimi pek çok alanda değişimlere yol açmaktadır. Bu değişimler olumlu özellikler barındırdığı gibi riskleri de beraberinde getirmektedir. Yapay zekâ ve suç ilişkisi bu riskli alan içindedir. Bu mesele iki boyutlu olarak ele alınabilir. Birinci boyutta yapay zekâ aracılığıyla işlenen ve yapay zekânın işlediği suçlar yer alırken ikinci boyutta suç takibinde yapay zekânın kolaylaştırıcı etkisi bulunmaktadır. Yapay zekâ, geleneksel suçların yöntemlerini değiştirerek ya da tamamen geleneksel suçların dışına çıkılarak suç işlemeyi kolaylaştırmakta ve suçun doğasını değiştirmektedir. Suçlunun ve mağdurun aynı zaman ve mekânı kullandığı suçlardan ziyade zamansal ve mekânsal birlikteliğin zorunlu koşul olmadığı suçlar ortaya çıkmaktadır. Bu çalışmanın amacı yapay zekâ ve suç ilişkisiyle yapay zekânın cezai sorumluluğu meselesini irdelemek ve rutin aktivite teorisinin bu suçları ne şekilde ele alabileceğini ele almaktır. Bu amaçla, çalışmada literatür taraması yöntemi kullanılmıştır. Yapay zekâ ve suç üzerine yapılan literatür çalışmasında rutin aktivite teorisinin açıklayıcılığı üzerine çalışmaların sınırlı olması ayrıca dijitalleşmenin hız kazanması ve konunun incelenmesinin erken dönemi olması nedeniyle literatüre katkı sağlamak amaçlanmaktadır.

Anahtar Kelimeler: *Yapay Zekâ, Suç, Suç Önleme ve Tahminleme, Deepfake, Rutin Aktivite Teorisi*

ABSTRACT

The development of artificial intelligence, a type of intelligence designed by humans and used by machines, is leading to changes in many areas. These changes have positive features but also bring risks. The relationship between artificial intelligence and crime is included in this risky area. This issue can be addressed in two dimensions. While the first dimension covers crimes committed through artificial intelligence and crimes committed by artificial intelligence, the second dimension includes the facilitating effect of artificial intelligence in crime pursuit. Artificial intelligence facilitates crimes by changing the methods of traditional crimes or changing the nature

* Dr., İstanbul Üniversitesi Güvenlik ve Koruma Bilimleri Meslek Yüksekokulu,
E-mail: ayseinan@istanbul.edu.tr, ORCID: 0000-0002-9202-5648, İstanbul, Türkiye.

of crime by going beyond traditional crimes. Instead of crimes where the criminal and the victim use the same time and place, crimes in which temporal and spatial coexistence is not a mandatory condition emerge. The purpose of this study is to examine the relationship between artificial intelligence and crime, specifically the issue of artificial intelligence's criminal liability, and to explore how routine activity theory might address these crimes. To this end, a literature review method was used in the study. Given the limited studies on the explanatory power of routine activity theory in the literature on artificial intelligence and crime, as well as the rapid pace of digitalization and the early stage of research on the subject, this study aims to contribute to the literature.

Keywords: *Artificial Intelligence, Crime, Crime Prevention and Prediction, Deepfake, Routine Activity Theory*

Giriş

İnsan gibi davranan ve düşünen makinalara ilişkin romanlara ve filmlere konu olan hayal, hızla ilerleyen teknolojiyle birlikte gerçekliğe dönüşmektedir. Gündelik hayat, yapay zekâ olarak adlandırmadığımız fakat sürekli kullandığımız, hayatı kolaylaştıran uygulamalarla çevrili durumdadır. Yol tarifinde kullanılan anlık yol durumunu güncelleyen haritalar ve telefonların sanal asistanları bugün akıllı telefon kullanan büyük çoğunluğun kullandığı yapay zekâ uygulamalarından bazılarıdır. Giderek artan dijitalleşme neticesinde gündelik hayat rutinleri ve alışkanlıklar dönüşüme uğramaktadır. Bu nedenlerle yapay zekâ çağında yaşadığımız söylenebilir.

Son 30 yılda dünya, geçmişte olduğundan çok daha hızlı bir şekilde değişmektedir. 20. yüzyılın ikinci yarısında askeri alanda başlayan internet kullanımı, 1990'lara kadar Amerika'da gelişmiş ve ardından birkaç yıl içinde küresel olarak yaygınlaşmıştır (Cohen-Almagor, 2011, s. 46). Türkiye'de de bu teknoloji ortaya çıkışından çok kısa bir süre sonra, 1993 yılında, ODTÜ ile Washington arasında kurulan bağlantıyla kullanılmaya başlanmıştır (Gönenç, 2003, s. 95). O dönemde internet teknoloji kullanımı sınırlı alanlarda iken bugün geline nokta internet teknolojisi hayatın her alanına yayılarak ortaya çıktığı günden bugüne mesafenin hızla açılmasına yol açmıştır.

Teknolojideki hızlı büyüme ve ilerleme internet tabanlı pek çok uygulamayı insanların kullanımına açmıştır. Başlangıçta insan zekâsı olmaksızın pek bir anlamı olmayan uygulamalar döneminden yapay zekânın ön planda olduğu bir döneme geçilmiştir. Yapay zekâ, insanların tasarladığı ve makinaların kullandığı bir zekâ olarak tanımlanmaktadır (Tai, 2020, s. 339). Russel & Norvig (2010, s. 2) yapay zekânın ne olduğuna ilişkin farklı tanımlamaları dört grupta toplamış ve bu tanımların temellerini i) insan gibi davranmak ii) insan gibi düşünmek iii) rasyonel davranmak iv) rasyonel düşünmek olarak belirlemişlerdir. Yapay zekâ genellikle, insanların problemleri çözmesine yardımcı olan ve insanların işlerini kolaylaştıran makinalar ve bilgisayarlar olarak algılanmaktadır (Tai, 2020). Bilgisayarların artık, sezgi ve kavrama özellikleri de dahil olmak üzere, birçok şeyi

insanlar kadar ya da insanlardan daha iyi yapabildiği düşünülmektedir (Russell vd., 2010). Homo sapiens ile ilişkilendirilerek yapay zekâ, machina sapiens olarak da adlandırılmaktadır (Okuyucu Ergün, 2023).

Yapay zekânın zayıf yapay zekâ, genel yapay zekâ ve güçlü yapay zekâ olarak üç çeşidi vardır (Damar vd., 2024, s. 86) Zayıf yapay zekâ dar yapay zekâ olarak da bilinmektedir ve günümüzde en yaygın kullanılan türüdür (Broadhurst vd., 2019). Makinanın zekâsının dar bir alandaki tek bir görev ya da birkaç görevle sınırlı olduğu yapay zekâ türüdür. Genel yapay zekâ ise bir makinenin dünyayı herhangi bir insan kadar anlayacağı ve çok sayıda görevi yürütebileceği zekâ türüdür (Broadhurst vd., 2019). Genel yapay zekâ halen geliştirilme aşamasındadır ve yapay zekânın genel zekâyâ ulaşmasına çok az bir süre kaldığını, gelişiminin %88'ini tamamladığını düşünen uzmanlar mevcuttur (Roitblat, 2025). Ancak halihazırda genel yapay zekâ teorik düzlemde. Güçlü yapay zekâ ise insanı aşan bir zekâyâ sahip olan türüdür (Butz, 2021). Kimileri güçlü yapay zekâyâ ulaşılabilirliğine inanırken (Butz, 2021), kimilerine göre bu ütöpik bir yaklaşımdır (Damar vd., 2024).

Yapay zekânın gelişimiyle birlikte ekonomiden iletişime, kültürden siyasete kadar hayatın pek çok alanında değişimler yaşanmaktadır. Bu değişimler olumlu özellikler barındırdığı gibi çeşitli riskleri de beraberinde getirmektedir. Bu risklerin başında suç işleme ve suça maruz kalma gelmektedir. Özellikle yapay zekâyâ aşına olunmaması, yapay zekânın sınırlarının bilinmemesi bu risklerin artmasına sebep olmaktadır. Yapay zekâ ile suç arasındaki ilişkide yapay zekâ aracılığıyla işlenen suçlar olduğu gibi yapay zekâ tarafından işlenen suçlar da mevcuttur. Diğer yanıyla, yapay zekâ suç tahminlemeleri yapabilmesi açısından suçun önlenmesinde ve takibinde de kullanılmaya çalışılmaktadır. Yapay zekâ ve suç üzerine yapılan yayınların meta analizinin yapıldığı bir çalışma 2017 yılından itibaren bu yayınlarda önemli derecede bir artış olduğunu belirtmektedir. Bu durum suç araştırmaları alanının yapay zekâyâ artan ilgisini ortaya koymaktadır. Fakat bu noktada ilgi çekici olan yapılan yayınların çoğunlukla bilgisayar bilimleri alanından olması, kriminoloji ya da suç araştırmaları alanlarından çok fazla yayının bulunmamasıdır (Campedelli, 2021, s. 511).

Yapay zekânın bir suç faili olarak ortaya çıkmasıyla birlikte yapılan çalışmalarda yapay zekânın cezai sorumluluğu meselesi önem kazanmıştır. Hallevey (2018, s. 114), yapay zekâda cezai sorumluluk meselesinin üç şekilde değerlendirilebileceğini ifade etmektedir: i) Dolaylı Failin Sorumluluğu Modeli, ii) Olası Doğal Sonuçlardan Sorumluluk Modeli ve iii) Doğrudan Sorumluluk Modeli. Yapay zekâyâ sahip varlıklara cezai sorumluluk yüklendiği takdirde karşılaşılan cezalandırma sorununun gündeme geldiğinden bahsetmektedir. Şöyle ki suç işleyen bir yapay zekâ varlığı ceza hukukunda halihazırda var olan hapis, para cezası, idam vb. cezalara çarptırmak uygulanabilir değildir. Bundan dolayı eğer ki yapay zekâ cezai sorumluluğa doğrudan sahipse ceza ayarlamaları yapılması gerektiğini belirtmektedir. Ölüm cezasının karşılığı olarak yazılımın silinmesi, hapis cezasının karşılığı olarak belirli bir süre programlandığı işi yapmaması şeklinde

ayarlamalar yapılabilir (Hallevy, 2018). Yapay zekânın cezai sorumluluğunun doğrudan olduğunun kabul edilmesi halinde dahi kullanıcı ve geliştiricilerin cezai sorumluluğu vardır. Diğer bir ifade ile yapay zekânın işlediği suçlarda sorumluluğun varlığı kabul edilse de edilmese de insanların sorumlu tutulması söz konusudur. Bu sorumluluk, kimi durumda insanların suç işleme gayesiyle yapay zekâ algoritmalarını oluşturmaktan kimi durumda da bilinçli olmayan yazılım hatalarından kaynaklanmaktadır.

Yapay zekâ ve suç üzerine Türkiye’de yayınlanan literatür incelendiğinde hukuki boyutuna ve yapay zekâ aracılığıyla işlenen suçlara ağırlık verildiği görülmektedir. Güngör (2024), yapay zekânın suç işleme potansiyelini değerlendirdiği ve ceza hukukunda bu suçların sorumluluğunu tartıştığı makalesinde, günümüzdeki yapay zekânın programlandıkları işlevleri yerine getiren ve belirli algoritmaların dışına çıkamayan yapıları itibarıyla suç işleme unsurlarını barındırmadığını ve yalnızca bir araç olduklarını belirtmektedir ve cezai sorumluluğun program geliştiricileri ve kullanıcılarda olduğunu belirtmektedir. Karabal (2023), *Yapay Zekâda Hukuk İhlalleri* başlıklı çalışmada yapay zekâyâ hukuki sorumluluğun ancak elektronik ya da tüzel kişilik verilmesi ile sağlanabileceğini ifade etmekte ve bu durumun da hukuki düzenlemelerle mümkün olabileceğinden bahsetmektedir. Fakat hukuk, felsefe ve mühendislik disiplinlerinin iş birliği yapmasıyla mümkün olabileceğini de eklemektedir. Berk (2020), dijital çağın tehlikesi olarak adlandırdığı deepfake teknolojisinin nasıl çalıştığını anlatmaktadır. Deepfake teknolojisinin özellikle saygın ve ünlü kişiler için tehdit oluşturduğunu, siyasi krizlere yol açabileceğini (siyasilerin görüntülerine söylemedikleri sözleri ekleyerek), toplum içinde kötü niyetli eski sevgililerin bu teknoloji aracılığıyla özel hayatın gizliliğini ihlal edici görüntüler oluşturabileceğini belirtmektedir. Karakoç Keskin (2025), yapay zekâ aracılığıyla oluşturulan dezenformasyonun boyutlarını incelediği nitel çalışmada, en yaygın dezenformasyon çeşidinin manipülasyon olduğunu, ikinci sırada ise uydurmanın geldiğini belirtmektedir. Dezenformasyonun çoğunlukla yabancı hesaplar tarafından dolaşıma sokulduğunu yaptığı analiz neticesinde ortaya çıkarmaktadır. Ulusoy & İlhan (2025) da 2024 ABD Başkanlık seçimlerindeki deepfake aracılığıyla gerçekleştirilen dezenformasyonu incelediği çalışmada seçim süreci boyunca sosyal medya aracılığıyla oluşturulan sahte içeriklerin çoğunun adaylara yönelik olumsuz içerikler olduğunu, küçük bir oranının (%16) olumlu olarak değerlendirilebileceğini ortaya koymaktadır. “Yeni nesil tehdit” olarak isimlendirdiği deepfake uygulamalarının gerçekliği örtecek güçte olan en büyük manipülasyon aracı olduğu ve çoğunluğunun kötü niyetli ve tehdit oluşturan yapıda olduğunu belirten Özdemir (2021), deepfake’i tespit eden uygulamaların geliştirilmesine önem verilmesi gerektiğini ve bu uygulamaların ulaşılabilirliğinin kolay olması gerektiğini ifade etmektedir. Demircan (2021) deepfake konusunda yapılan yayınlar üzerine doküman analizi yöntemi kullanarak yaptığı çalışmada deepfake uygulamalarının dolandırıcılık, itibar zedeleme, küçük düşürme ve siyasi manipülasyon aracı olarak kullanıldığını ve geleceğe ilişkin endişelerin artmasına sebep olduğu gibi gelişen teknolojinin çeşitli fırsatları da getirebileceğini belirtmektedir. Tufan (2025), suçun sosyolojik bir olgu olduğunu belirttiği çalışmada yapay zekânın sebep olduğu suçlardan ve yapay zekânın suç önlemede etkin kullanımından bahsetmekte fakat hukuki düzenlemelerin eksikliğini

vurgulamaktadır. Ayrıca yapay zekânın oluşturabileceği zararların farkına varılmasını sağlayacak eğitimlerin önemine dikkat çekmektedir. Ak (2021), yapay zekânın iç ve dış güvenlik açısından kullanılabileceğini, terörden asayişe geçmiş olaylardan hareketle geleceğe yönelik yapılacak tahminlemelerle suçların önlenmesinde kullanılırken dikkat edilmesi gereken hususun, insan hakları çerçevesinde kişisel mahremiyet, yaşam hakkının korunması ve kişisel verilerin kullanımı gibi ilkelerin gözetilmesi olduğunu belirtmektedir. Arslan (2023), deepfake teknolojisi aracılığıyla işlenebilecek dolandırıcılık, siber zorbalık, manipülasyon ve yalancı şahitlik suçlarının işlenme biçimlerini anlattıktan sonra suçlu ve mağdurların özelliklerini anlattığı kriminoloji çalışmasında, özellikle kadınların, politikacıların, ünlülerin, kamuya mal olmuş kişilerin ve iş adamlarının mağdur hedef kitesinde olduğunu belirtmektedir. Bununla birlikte suçlu karakteristiğini ortaya çıkarmak bu tür suçları işleyenlerin yaklaşık %90'ının yakalanmamış olmasından dolayı daha zor olduğunu belirtmekte fakat elde olan veriler üzerinden suçluların 15-25 yaş aralığında, asosyal ve psikolojik sıkıntıları olan ve denetimsiz ailelerden gelen kişiler olduğunu belirtmektedir.

Yapay zekâ ve suç meselesi iki boyutlu olarak ele alınabilir. Birinci boyutta yapay zekâ aracılığıyla işlenen ya da yapay zekânın işlediği suçlar yer alırken ikinci boyutta suç takibinde yapay zekânın kolaylaştırıcı etkisi bulunmaktadır. Bir başka deyişle yapay zekânın suç oluşturma potansiyeli ve suçu önleyici rolü söz konusudur. Bu çalışmanın temel amacı, Rutin Aktivite Teorisi'nin yapay zekâ suçlarına uygulanabilirliğini incelemektir. Bu bağlamda, yapay zekâ ile suç arasındaki ilişki değerlendirilerek yapay zekâ aracılığıyla işlenen suçlar ve yapay zekânın bizzat fail olduğu suçlar ele alınmaktadır. Ayrıca, yapay zekânın suç incelemelerinde ve suçu önlenmesinde nasıl kullanıldığı ile yapay zekâyâ yönelik mevcut hukuki düzenlemeler de tartışılarak, Rutin Aktivite Teorisi çerçevesinde bütüncül bir analiz yapılacaktır. Bu çalışmada literatür taraması yöntemi kullanılarak ilgili literatür incelenmiş ve değerlendirme yapılmıştır. Bu bağlamda SAGE, Google Scholar ve TR Dizin veritabanlarında yapay zekâ, suç, siber suçlar, deepfake ve rutin aktivite teorisi anahtar kelimeleri İngilizce ve Türkçe olarak taranmış, hukuk, kriminoloji, sosyoloji, medya ve psikoloji alanlarındaki yayınlar incelenmiş olup yapay zekânın teknik mühendislik boyutlarına odaklanan çalışmalar kapsam dışında bırakılmıştır. Yapay zekâ ve suç üzerine yapılan literatür çalışmasında rutin aktivite teorisinin açıklayıcılığı üzerine çalışmaların sınırlı olması ve konunun her geçen gün önem kazanması nedeniyle literatüre katkı sağlamak amaçlanmaktadır.

Yapay Zekâ Suçları ve Suç Takibinde Yapay Zekânın Kolaylaştırıcılığı

Yapay zekâ kullanımıyla birlikte geleneksel suçların ötesine geçilerek yeni suç tipleri ortaya çıkmaktadır. Bilgisayar teknolojisindeki ilerlemelere odaklanılırken ortaya çıkarabileceği olumsuz durumlar ilk etapta görmezden gelinerek tekno-iyimserlik (Hayward & Maas, 2021, s. 2) içine düşüldüğünden dolayı suç bilimi araştırmacıları için yapay zekâ suçları gizemini korumaktadır. Çünkü teknolojinin sınırları ve neleri getireceği tam olarak bilinmemektedir. Fakat eskiden düşünüldüğü gibi güllük gülistanlık olmadığı

anlaşılmıştır. Bu suçların suç bilimi için gizemini korumasının bir diğer sebebi de kriminologların yeni teknolojinin ortaya çıkaracağı problemlerin farkında olmadan kendi disiplinleri içinde kalmalarıdır (Brown, 2006, s. 225). Kriminoloji elbette ki teknoloji devrimiyle birlikte kötü niyetli yetenekli bilgisayar kullanıcılarının işlediği siber suçlara eğilmiştir. Tüm dünyada olduğu gibi Türkiye’de de siber suçlara yönelik cezai müeyyideler düzenlenmiştir. Türk Ceza Kanunu’nun 243, 244, 245 ve 246. maddeleri bilişim alanında suçlar başlığı altında yer almaktadır (Türk Ceza Kanunu, 2004). Yasada bilişim sistemine girme (md. 243), sistemi engelleme, bozma, verileri yok etme veya değiştirme (md. 244), banka veya kredi kartlarının kötüye kullanılması (md. 245), yasak cihaz ve programlar (md. 245) ile tüzel kişiler hakkında güvenlik tedbiri uygulanması (md. 246) maddeleri yer almaktadır. Bilişim suçları kapsamına giren suçlara ilişkin cezai düzenlemeler yapay zekâ suçlarının tamamını kapsamamakta ve yapay zekâ suçlarına ilişkin hukuki tartışmalar sürmektedir. Bu noktada üzerinde en fazla durulan konu yapay zekânın cezai sorumluluğu meselesidir. Bu konu daha çok yapay zekâ aracılığıyla işlenen suçlarda ve yapay zekânın işlediği suçlarda önem kazanmaktadır. Cezai sorumluluğun geliştiricide mi, uygulayıcı da mı, geliştirme için finansman sağlayanda mı yoksa herhangi bir kişiliği olmayan yapay zekâ da mı olduğu tartışılmaktadır.

Yapay Zekâ Aracılığıyla İşlenen Suçlar

Yapay zekâ, geleneksel suçların yöntemlerini değiştirerek ya da tamamen geleneksel suçların dışına çıkılarak suç işlemeyi kolaylaştırmakta ve suçun doğasını değiştirmektedir. Suçlunun ve mağdurun aynı zaman ve mekânı kullandığı suçlardan farklı olarak zamansal ve mekânsal birlikteliğin zorunlu koşul olmadığı suçlar ortaya çıkmaktadır. Uyuşturucu kaçakçılığından teröre, dolandırıcılıktan dezenformasyona ve manipülasyona, kişisel bilgilerin çalınmasından cinsel suçlara kadar pek çok suç türü yapay zekâ destekli araçlar vasıtasıyla işlenen suçlar arasında yer almaktadır. Kullanılan araçlar ve hedefler değişkenlik göstermektedir. Bu tür suçlar, toplumun her tabakasından kişilere yönelik olabildiği gibi ulusal güvenliği tehdit eden ya da kurumlara karşı işlenen suçlarda olabilir (al Qatawneh vd., 2023). Aynı zamanda yapay zekâ destekli suçlar, geleneksel suçlardan farklı olarak küresel mahiyette gerçekleştirilebilir. Dünyanın bir ucundaki bir fail diğer ucundaki kişilere yönelik suç işleyebilir. Kimi durumda suçluya ulaşmak mümkün olamazken kimi durumda suçun ispatı da mümkün olamamaktadır. Her geçen gün yenilenen teknolojinin risklerinin önceden tespiti mümkün olmaması dolayısıyla hukukta bulunan boşluklar nedeniyle fail ya da failler cezalandırılmamaktadır.

Yapay zekâ kimi durumda suçun konusu olurken kimi durumda suçun aracı olmaktadır. Suç, bilgisayarın fiziksel bileşenlerini ya da donanımını hedef aldığı anda konusu olurken bilgi sisteminin maddi olmayan bileşenleri yani yazılımı hedef alındığında araç olmaktadır (al Qatawneh vd., 2023). Eylem, yazılımın kopyalanması, silinmesi ya da değiştirilmesi şeklinde gerçekleşebilmektedir. Suçun niteliği geleneksel suçlardan farklı olarak çoğunlukla finansal suçlardır. Şiddet içeren suçlardan ziyade failin belirli niteliklere sahip

bilgisayar gibi elektronik cihazları kullanma becerisiyle ilişkili suçlar olduğundan dolayı doğası gereği daha az rahatsız edicidir (al Qatawneh vd., 2023).

Yapay zekâ aracılığıyla işlenen suçlarda en yaygın kullanılan araç deepfake teknolojisidir. Deepfake suçları yüz yaratma, yüz ve ifade değiştirme ve ses klonlama teknikleriyle kendisini göstermektedir (Anıkaydın, 2022; Arslan, 2023). Deepfake teknolojisinin sebep olduğu suçlar arasında yalan habercilik, finansal suçlar, dolandırıcılık, siyasi kirlilik, kadınlar ve azınlıklar gibi dezavantajlı gruplar aleyhine çeşitli tehlikeler yer almaktadır (Tseng, 2018). Deepfake teknolojisinin dünyada suç amaçlı ilk kullanımı 2017 yılında Reddit isimli sosyal ağda deepfake isimli kullanıcının ünlü isimlerin yüzlerinin pornografik videolara monte edilmesiyle gerçekleşmiştir (Mankoo, 2023; Özdemir, 2021). Amerikalı yönetmen Jordan Peele'nin 2018 yılında deepfake teknolojisinin manipülasyon için nasıl kullanılabileceğini göstermek amacıyla Obama'nın "Başkan Trump tam bir ahmaktır" diye başladığı bir konuşmayı "... halka açık yerlerde ben böyle şeyler söylemem... ama bir başkası söyleyebilir... Jordan Peele gibi" diye devam ettirdiği bir video yayınlamıştır (Vaccari & Chadwick, 2024). Bu, yapay zekânın siyasi manipülasyon için nasıl kullanılabileceğini gözler önüne seren ilk videodur.

Deepfake yoluyla işlenen en büyük dolandırıcılık hadiselerinden birisi 2024 yılında gerçekleşmiştir. Çokuluslu bir şirketin Hong Kong'taki finans çalışanı, şirketin İngiltere'deki finans müdüründen gelen e-postayla gizli bir ödeme yapması gerektiği yönünde bir talimat almıştır. Talimatın gizliliği ve aktarılması istenen tutarın yüksekliği nedeniyle çalışan, kimlik avı e-postası olduğu düşüncesiyle uygulamaya geçmemiştir. Ardından İngiltere'deki finans müdürünün yaptığı görüntülü video görüşmesinde diğer çalışanların görüntü ve seslerinin de olmasından dolayı talimatı uygulayarak 25,6 milyon dolar ödeyerek dolandırılmıştır. Görüntülerin ve seslerin birebir kopyalanması ve görüntülü görüşmede sadece bir kişinin olmaması finans çalışanının kandırılmasını sağlamıştır (Heather & Magramo, 2024). 2025 yılı Nisan ayında, deepfake teknolojisinin kullanıldığı bir vaka da Türkiye'de yaşanmıştır. Ankara merkezli bir yazılım şirketi bot müşteri tarafından dolandırılmıştır. Aylar süren zoom görüşmeleri ve bilgi alışverişleri sonrasında bir e-ticaret altyapısı geliştirme talebinde bulunan yazılım şirketi, 5 milyon TL karşılığında yazılımı geliştirmek üzere anlaşma imzalamış fakat projenin tesliminden sonra ödemesini alamamıştır. Zoom kayıtlarının bilişim suçları tarafından incelenmesi neticesinde deepfake teknolojisiyle toplantıların yapıldığı anlaşılmıştır (Can, 2025). 2023 yılında da Cumhurbaşkanı Recep Tayyip Erdoğan'ın sahte videosu çeşitli platformlarda yayınlanarak, bu videoda Türkiye Petrolleri'ne yatırım yapılması tavsiyesi verip vaatlerde bulunması sağlanarak dolandırıcılık yapılmaya çalışılmıştır. İletişim Başkanlığı, yaptığı açıklama ile vatandaşları uyararak; videonun, Amerikan televizyon kanalına yaptığı açıklamalardaki görüntülerin kullanılarak yapıldığı bilgisini vermiştir (İletişim Başkanlığı, 2023). TPAO'nun yürüttüğü çalışmalarla 50 bin aldatıcı reklam engellenmiş ve 450 hesap kapatılmıştır (Anadolu Ajansı, 2023). Deepfake teknolojisinin sıklıkla kullanıldığı diğer alanda siyasi çıkar sağlamak için manipülasyon ve dezenformasyon oluşturmaktır. Amerika Birleşik Devletleri'nin 2024 yılındaki başkanlık seçimleri kampanyasında bütün

adaylara yönelik olarak çok sayıda deepfake videosu, ses kaydı ve fotoğraf dolaşıma girmiştir (Ulusoy & İlhan, 2025). Yapay zekâ aracılığıyla çıkar sağlayanların, manipülasyon ve dezenformasyonun önüne geçebilmek için hukuki düzenlemelerin yapılması önem kazanmaktadır. Dezenformasyon ve manipülasyon bilgi kirliliğine sebep olarak ciddi tehditlerin oluşmasına sebep olmaktadır. Bireylerin karar verme süreçlerine müdahale edilmektedir. Bu durumun önüne geçebilmek için denetim mekanizmalarını güçlendirmek önem kazanmaktadır. Fakat burada da değişimin ve teknolojik ilerlemenin hızıyla uyumlu olacak şekilde adaptasyon ve yenilenme gerekmektedir. Yapay zekânın sebep olduğu tehditlere karşı yapay zekânın etkin kullanımıyla sürecin gerisinde kalmamak önemlidir.

Yapay Zekânın İşlediği Suçlar

Yapay zekâ suç faili olabilir mi? Eğer suç işleme kapasitesine sahipse fail olacaktır. Bu noktada mesele yapay zekânın cezai sorumluluğuna gelmektedir. Yapay zekânın suç işlemesi halinde hukuki sorumluluğunun bulunmaması önemli bir sorun teşkil etmektedir. Broadhurst vd. (2019) yapay zekâ uzmanlarının kontrolsüz ve kendisinin farkında olan bir yapay zekânın sebep olacağı tehlikelerle ilgili endişeli olduğunu fakat bu endişelerin yerinde olup olmadığının zamanla anlaşılacağını ifade etmektedir. Öte taraftan yapay zekânın suç işleme potansiyeli olduğu da düşünülmektedir (Güngör, 2024; Hallevy, 2018).

1981 yılında bir motosiklet fabrikasındaki işçinin robot tarafından yaptığı işe yönelik bir tehdit olarak algılanıp öldürülmesi hadisesi yapay zekânın işlediği ilk suç olarak kamuoyunda önemli bir yer işgal etmiş ve endişeye yol açmıştır (Hallevy, 2010). 2016 yılında Microsoft'un geliştirdiği sohbet robotu Tay, Twitter kullanıcılarıyla etkileşime girerek çok kısa bir sürede saldırgan, müstehcen ve ırkçı paylaşımlar yapmasından dolayı ilk paylaşımından 16 saat sonra kapatılmıştır (Neff & Nagy, 2016, s. 4922). Yapay zekâ sohbet robotu olan Tay'ın kullanıcılardan gelen etkileşimlerle nefret suçu işlemesi, rasyonelliği ne dereceye kadar sağlayabildiğini göstermektedir. Kullanıcılar, kendileri için eğlence malzemesi olan Tay ile yaptıkları özel sohbetlerde saldırgan ve ırkçı ifadeleri tekrarlamasını sağlayan özelliklerini harekete geçirmişlerdir. Microsoft'un araştırma başkanı Peter Lee yaptığı basın açıklamasında, güvenlik zafiyeti nedeniyle Tay'ın tutumunu önceden tahmin edemediklerini ve attığı rahatsız edici ve saldırgan tweetler için üzgün olduğunu belirtmiştir (Lee, 2016). O'Neill (2015)'in *Daily Dot* haber sitesinde kaleme aldığı haber "İsviçre'de uyuşturucu satın alan robot yakalandı" başlığıyla çıkmıştır. *The random darknet shopper* isimli sanat projesi kapsamında deep web'i keşfetmek için haftalık 100 dolarlık bitcoin bütçesiyle rastgele bir ürün satın alıp sanatçılara gönderen bir çevrimiçi alışveriş botu tasarlanmıştır. Yaptığı alışverişini sergilemişlerdir. Fakat satın aldığı ürünler içerisinde uyuşturucu hapların da bulunması sebebiyle robota ve ürünlere polis el koymuş ve üç ay sonra uyuşturucu haplar dışındaki ürünleri ve robotu serbest bırakmıştır (Kasperkevic, 2015). Sanatçılara herhangi bir ceza verilmemiştir. Bu olay, yapay zekânın yasal statüsü tartışmalarının gündeme gelmesine sebep olmuştur (Hayward & Maas, 2021).

Yapay zekânın suç işleme potansiyeli olduğunu düşünenler algoritmasındaki karmaşıklık ve öğrenme yeteneklerinin buna sebep olduğunu iddia etmektedir (Değirmenci, 2021). Ayrıca, zaman içinde robotlara irade özgürlüğünün verilebileceği dolayısıyla cezai sorumluluğu doğuracak özellikte olacakları düşünülmektedir (Akbulut, 2023). İnsanların suç davranışlarını belirleyen faktörlere ve yeteneklere, zamanla yapay zekânın da sahip olacağı iddia edilmektedir (Abbott & Sarch, 2019).

Yapay zekânın işlediği suçlar ya da işleyeceği suçlar programlama ve geliştirme süreçlerindeki hatalardan da kaynaklanabilir. Tay sohbet robotu örneğinde gelişen nefret suçunun, öngörülemeyen güvenlik zafiyeti nedeniyle olduğu geliştiricilerin kabul ettiği bir durum olmuştur. Böylesi bir yazılım hatası nedeniyle yapay zekânın işlediği suçların sorumluluğu ancak programı geliştiren ya da kullananlarda olmak durumundadır. Sorumluluğun yapay zekâda olduğu suçlar meselesi cezalandırmanın nasıl gerçekleşeceği ve cezai sorumluluğun herhangi bir kişiliği olmayan yapay zekâyâ nasıl yükleneceği tartışmasını beraberinde getirmektedir. Hallevy (2015), 17. yüzyıldan itibaren cezai sorumluluğun sadece insanlara özgü olmadığını belirtmektedir. Bu noktada, nasıl ki şirketlere tüzel kişilik verilmesiyle cezai sorumluluktan bahsedilebiliyorsa hukuki düzenlemelerle yapay zekâyâ da kişilik verilmesi gerektiği savunulmaktadır (Hallevy, 2018; Karabal, 2023). Yapay zekâ teknolojisi geliştikçe yasal çerçeve hızla değişmekte ve tartışmalar devam etmektedir (Pagallo, 2011, 2017). Yapay zekânın insan gibi düşünme ve karar verme yeteneğine sezgilerin ve duyguların da eklenme ihtimali, günümüzde etkin kullanılan değil fakat ütöpik olarak değerlendirilmesine rağmen geliştirilmeye çalışılan güçlü yapay zekâ, bilinçli suç işleme riskini beraberinde getirmekte ve öncesinde hukuki düzenlemelerin yapılmasını gerektirmektedir.

Yapay Zekâ ile Suç Takibi ve Suçun Önlenmesi

Toplumsal düzeni sağlayabilmek için devletin koyduğu hukuk kurallarına aykırı davranılması neticesinde ortaya çıkan suç türleri teknolojideki gelişmelerle birlikte çeşitlenirken bir yandan da suç önleme çalışmaları açısından olumlu sonuçlar doğurmaktadır. Yapay zekâ uygulamalarında akıllı algoritmaların kullanılması suç araştırmalarını da etkilemiştir. Makine öğrenmesi tabanlı suç analizi, veri toplama, sınıflama, tahmin etme ve görselleştirmeden oluşmaktadır (Kim vd., 2018). Yapay zekânın ve makine öğrenmesinin kullanılmasıyla birlikte suç eğilimleri ve tahminlemeleri kolaylaşmaktadır (Dakalbab vd., 2022). Suç araştırmalarının yapay zekâ uygulamaları aracılığıyla yapılabilmesini kolaylaştıran çeşitli faktörler vardır. Bunlar arasında suça ilişkin verilere ulaşılabilirliğin artması, bilgisayar bilimleri alanlarından uzmanların suç araştırmalarına ilgisinin artması, geliştirilen istatistiksel yazılımlar ve programların kolaylaştırıcılığının artması gibi faktörler yer almaktadır (Campedelli, 2021, s. 524). Öte yandan yapay zekânın adli süreçlerde kullanılması hem heyecan hem de endişe meydana getirmektedir (Bennett Moses & Chan, 2014). Ceza adaleti yaklaşımları sistemlerinde var olan eşitsizlikler başlıca endişelerdendir. Yapılan araştırmalar, ceza adalet sürecinde bireylerin sosyo-ekonomik seviyeleri, etnik kökenleri, cinsiyet gibi özelliklerinin adli

sürecin tüm aşamalarında çeşitli eşitsizlikler doğurduğunu ortaya koymaktadır (Khan, 2023, s. 27). Ayrıca, makinanın karar verme sürecinin gerçekleşebilmesi için insanlar tarafından sağlanan datanın büyük olması önemlidir. Data küçüldüğünde hata yapma ihtimali artmaktadır. Bununla birlikte bireyin biricikliği ve dolayısıyla eyleme geçiren kararlarının bireye özgü oluşu yapay zekânın yanlış karar vermesi ihtimalini doğurmaktadır. Yapay zekâ genele bakarak bir analiz yapmaktadır ve bu süreçte bu biriciklik es geçilmektedir (Broadhurst vd., 2019, s. 10).

Adli süreçlerde yapay zekâ kullanım alanları arasında suç laboratuvarı vaka yönetimi, DNA eşleştirme, metabolik profillemeye gibi adli tıp süreçleri, plaka tanıma, kapalı devre kamera gözetimi, yüz tanıma, suç haritalama ve mekânsal analiz yer almaktadır (R. A. Berk, 2021, s. 215). Suç davranışlarının önceden tahmin edilmesini sağlayan öngörücü polislik uygulamasında (Bennett Moses & Chan, 2016) yapay zekâ analizleri kullanılarak suç gerçekleşmeden önce önlenmesi hedeflenmektedir. Belirli bölgelerde ve belirli zamanlarda suç davranışlarında artışın olduğuna dair bir analiz ortaya koyulduktan sonra olası suç davranışlarının yer ve saat bilgisine dair tahminler neticesinde belirtilen bölgeye polis kuvvetlerinin gönderilmesi aracılığıyla suçun önlenmesi sağlanmaktadır (R. A. Berk, 2021, s. 216). Yapay zekâ uygulamalarından önce de bölgeden gelen ihbarlar, deneyimler ve çeşitli ipuçları kullanılarak basit haritalama yöntemiyle tahminleme yapılmaktaydı.

Yapay zekânın suçun aydınlatılmasında kullanılması suçun önlenmesinde kullanılmasından daha uzun bir geçmişe sahiptir ve daha çok rağbet görmüştür (Ak, 2021). Suçun aydınlatılması suç oranlarının artışında etkili olmuştur. Artış sayısının işlenen suçların aydınlatılmasıyla ilişkili olduğu düşünülünce bu durum olumlu olarak nitelenebilir. Fakat gelişen teknoloji ile birlikte suçların henüz işlenmeden önlenmesine yönelik faaliyetlere odaklanması beklenmektedir. Bu sebeple yapay zekânın suç önlemeye ilişkin kullanımı giderek önem kazanmaktadır.

Rutin Aktivite Teorisinin Yapay Zekâ Suçlarına Uygulanması

Kriminoloji teorileri arasında siber suçları açıklamak için uygulanan belli başlı teoriler arasında rutin aktivite teorisi, öz kontrol teorisi, feminist suç teorisi, alt kültür, gerilim teorileri bulunmaktadır. Bu teorilerden siber suçları açıklamak için en yaygın olarak kullanılanı rutin aktivite teorisidir. Yapay zekâ suçları ve siber suçların birbirine yakınlığı ve birbirini kapsayıcı yönü itibarıyla siber suçlarda uygulanan teoriler mercek altına alınmıştır. Bu çalışmada yapay zekâ suçlarını açıklamak için rutin aktivite teorisine odaklanılmıştır. Rutin aktivite teorisinin seçilme sebebi siber suçları açıklamak için en fazla kullanılan teori olmasıdır (Hasan, 2022; Holt & Bossler, 2009; Pratt vd., 2010; Yar, 2005).

Cohen & Felson (1979) tarafından ortaya koyulan rutin aktivite teorisi gündelik yaşamdaki rutin aktivitelerde meydana gelen yapısal değişikliklerin suç eyleminin oluşumuna etkisini ortaya koymaktadır. Rutin aktivite teorisine göre, suçun ortaya çıkabilmesi için üç unsur zaman ve mekânda bir araya gelebilmelidir. Bu unsurlar, motive olmuş suçlu, uygun hedef

ve yetenekli koruyucuların yokluğudur. Klasik suç teorileri suçun oluşumunu açıklarken genellikle suçlu perspektifinden bakmakta, suçlunun bulunduğu çevre ya da kişilik özelliklerinin suçun oluşumuna etkisini ortaya koymaktadır. Rutin aktivite teorisi ise suç eyleminin ortaya çıkışını açıklarken hedefi de temel unsurlar içine eklemiştir. Teorinin temel iddiası bu üç unsurdan birinin yokluğu halinde suçun ortaya çıkmayacağı üzerinedir.

Rutin aktivite teorisi, siber suçlar konusuna uygulanmakta ve açıklamalar getirmektedir (Hawdon vd., 2020; Holt & Bossler, 2009; Kigerl, 2012; Reyns, 2013). Sanal dünyada uzun süre geçirme yani gündelik rutinlerin çevrimiçinde zaman geçirme şeklinde değişmesi gibi faktörler uygun hedef unsurunu açıklamakta kullanılmaktadır (Holt & Bossler, 2009; Kigerl, 2012; Reyns, 2013). Siber suçları engellemeye yardımcı olabilecek antivirüs programlarının, ailelerin bilgisayar kullanan çocukları denetleme mekanizmalarının yokluğu ve kullanıcıların siber suçlara dair bilgi eksiklikleri rutin aktivite teorisinde yetenekli koruyucuların yokluğu unsurunun ortaya çıkmasını sağlamaktadır (Holt & Bossler, 2009; Marcum vd., 2010). Motive olmuş suçlular uygun hedef ve koruyucuların yokluğu ve eksikliği durumunda çıkar sağlamak için suç eylemine girişmektedir.

Bu açıklamaların bir kısmı yapay zekâ suçları için de geçerlidir. Rutin aktivite teorisinde suçun oluşmasını sağlayan unsurlar yapay zekâ bağlamında yeniden yorumlanabilir. *Motive olmuş kişiler*, yapay zekâyı araç olarak kullanan bireyler olduğu gibi Microsoft'un sohbet robotu Tay örneğinde olduğu gibi yapay zekânın doğrudan fail olduğu durumlar da vardır. *Uygun hedef* ise doğrudan bireyler ve kurumlar olabileceği gibi veritabanları da olabilir. *Yetenekli koruyucuların yokluğu* unsurunu, hukuki düzenlemelerin gelişen teknolojinin hızına ayak uyduramaması nedeniyle yetersiz kalması, kullanıcıların öz denetim mekanizmaları konusundaki bilgi, tecrübe ve eğitim eksiklikleri ve teknolojinin hızının ortaya çıkardığı güvenlik açıkları oluşturmaktadır. Özellikle yapay zekâ aracılığıyla suç işlemeye *motive olmuş kişiler*, *yetenekli koruyucuların yokluğu* yani adli mekanizmaların teknolojik anlamda yetersizliği dolayısıyla yakalanma korkusu olmaksızın eylemlerini gerçekleştirmektedir. Siyasiler, ünlüler, iş insanları ya da toplumun diğer üyeleri yapay zekâ aracılığıyla gerçekleştirilecek suçların boyutlarını tam olarak bilemedikleri için *uygun hedef* haline gelmektedir. Özellikle deepfake uygulaması aracılığıyla oluşturulan görüntü ve sesin gerçek olmadığını anlayabilmek için yüksek nitelikli araçlara ihtiyaç duyulmaktadır. Deepfake uygulamaları, gerçeklik algısının bozulmasına sebep olmaktadır. Duyu organları aracılığıyla edinilen deneyimlerin gerçekliği tartışmalı hale gelmektedir. Örneğin seçimlerde yapılan manipülasyonlar ve dezenformasyon rutin aktivite teorisinin üç unsurunu da karşılamaktadır. Politikacılar seçimi kazanma *motivasyonu*yla rakipleri hakkında yapay görüntü ve videolar oluşturarak *uygun hedef* olarak belirledikleri seçmenin fikirlerini etkilemek istemektedir. Yapay zekâ uygulamalarının oluşturduğu video ve görüntülerin yapay olduğunun anlaşılması ve yayıldığı kaynağın bulunması uzmanlık gerektirdiği için denetim mekanizmalarının çalışmasının çok güç olması rutin aktivite teorisinde belirtilen *yetenekli koruyucuların yokluğu* unsuru da gerçekleşmiş olmaktadır. Ayrıca yapay zekâ suçlarına ilişkin hukuki

düzenleme eksiklikleri de yetenekli koruyucuların yokluğu unsurunun oluşmasına sebep olmaktadır.

Rutin aktivite teorisindeki üç unsurdan uygun hedefin oluşması ve yetenekli koruyucuların yokluğu motive olmuş suçluların yapay zekâ aracılığıyla suç işlemesinin önünü açmaktadır. Geleneksel suçlardan farkı ise hedefin ve suçlunun zamansal ve mekânsal birlikteliğinin olmamasıdır. Cohen & Felson (1979), üç unsurun zamanda ve mekânda bir araya gelmesiyle suçun oluşacağını belirtmişlerdir. Fakat yapay zekâ suçları bağlamında bu birliktelik teorisyenlerin belirttiği gibi hedefin ve suçlunun zamanda ve mekânda birlikteliği şeklinde gerçekleşmemektedir. Yapay zekâ suçlarında mekân, dijital mekândır. Hedefin mekânı ip adresi, sosyal medya hesapları gibi dijital varlığını sürdürdüğü dijital mekândır. Suçlunun mekânı anonimdir, çeşitli teknolojileri kullanarak fiziksel mekânını gizlemek için yerinin bulunmasını sağlayacak ip adresi gibi kişisel bilgilerini anonimleştirir. Bulutlar, ağlar, veri akışının olduğu yerler suçlunun mekânıdır. Hedefe coğrafi yakınlığının anlamı yoktur. Hedefle arasında kıtalar olabilir. Zaman açısından düşünüldüğündeyse suçlu oluşturduğu algoritmalarla zamansızdır. Zamanda sürekli. Hedefin zamanını takip eder ve eylemini gerçekleştirir. Hedefin çevrimiçi olduğu saatler hedefin zamanıdır. Suçlu ile hedef bu zamanda bir araya gelmiş olur. Suçun üretildiği ve yayıldığı zamanın farklı olması da geleneksel suçlardan ayrıldığı yerlerden birisidir. Netice itibarıyla rutin aktivite teorisi yapay zekâ suçlarını açıklayabilecek niteliktedir. Anonim mekândaki motive olmuş suçlu, dijital mekânda varlığını sürdüren uygun hedefe yönelik olarak çevrimiçi zamanda yapay zekâyla oluşturulan suç unsurlarını tespit ve takip etme konusunda yetenekli koruyucuların yokluğunda suç eylemini gerçekleştirmektedir.

Sonuç

Teknolojinin gelişmesiyle birlikte ilerleyen ve ilerlemeye devam edecek olan insana benzeyen ya da insanüstü düşünme, karar verme yeteneğine sahip olan yapay zekâ uygulamaları pek çok alanda hayatı ve iş süreçlerini kolaylaştırmakta ve verimliliği artırmaktadır. Bununla birlikte yapay zekâ fırsatları olduğu kadar tehditler ve riskleri de beraberinde getirmektedir. Yapay zekâ aracılığıyla işlenen suçlar ve yapay zekânın işlediği suçlar bu risklerden bazılarıdır. Suç çeşitlerinin ve fırsatlarının çeşitlenmesi, yöntemlerinin geleneksel suçlardan ayrılmasıyla kendini gösteren yapay zekâ suçları, sınırlarının bilinmemesi ve her geçen gün teknolojinin ilerlemesi nedeniyle de araştırmacılar için gizemini korumaktadır. Bu bilinmezlik hukuki düzenlemelerin de gecikmesine sebep olmaktadır.

Yapay zekâ suçlarını açıklamak için rutin aktivite teorisinden faydalanmak mümkündür. Rutin aktivite teorisinde suçun ortaya çıkabilmesi motive olmuş suçlu, uygun hedef ve yetenekli koruyucuların yokluğu unsurları zamanda ve mekânda bir araya gelmek zorundadır. Unsurlardan birisinin yokluğu durumunda suç davranışı gerçekleşmemektedir. Yapay zekâ suçları rutin aktivite teorisine uyarlandığında, motive olmuş suçlu uygun hedefe yönelik suç davranışını yetenekli koruyucuların yokluğu durumunda

yöneltilmektedir. Yapay zekâ suçları açısından rutin aktivite teorisinin temel unsurlarından motive olmuş suçlu yapay zekâyı araç olarak kullanan bireyler ve yapay zekânın kendisi olurken, uygun hedef bireyler ve kurumlar olduğu kadar çeşitli dijital veritabanlarıdır. Hedefin, suçlunun kullandığı yapay zekâ araçlarından korunmasını sağlayacak bilgi, tecrübe ve altyapısının olmaması, suçluyu suç işlemekten caydıracak hukuki düzenlemelerin olmaması, işlediği suçun tespitinin ve takibinin yapılmasının zor olması gibi etkenler rutin aktivite teorisindeki üç unsurdan yetenekli koruyucuların yokluğuna tekabül etmektedir. Yapay zekâ suçları rutin aktivite teorisinin suçun oluşmasında gerekli olan unsurlarının biçimini değiştirirken zamansal-mekânsal birliktelik varsayımını temelden dönüştürmektedir. Zaman ve mekânda birliktelik meselesi geleneksel suçlardan farklı olarak gerçekleşmektedir. Suçlu anonim mekânda ve süresiz zamanda hedefin çevrimiçi zamanında ve dijital mekânında (ip adresi, sosyal medya sayfaları vb.) suç eylemini gerçekleştirmektedir. Fail ile mağdur arasındaki coğrafi mesafe önemini yitirmektedir. Bir diğer deyişle, yapay zekâ suçlarında zaman kesintisiz bir çevrimiçi varlık halini alırken mekân dijitalleşmektedir. Kimi durumda suçun üretildiği zaman ile mağduriyetin gerçekleştiği zaman arasında kopukluk ortaya çıkmaktadır. Bu durum rutin aktivite teorisinin yapay zekâ suçları bağlamında tartışılmasını ve klasik modelin bu bağlamda güncellenmesi gerektiğini ortaya koymaktadır.

Yapay zekâ suçları için uluslararası bir suç önleme mekanizmasının olmaması bu tür suçlarla mücadele imkânını sınırlandırmakta ve yeterli bilgi, araç ve zekâyı sahip failerin eylemlerinin cezasız kalmasına sebep olmaktadır. Üniversitelerin adli sürecin tüm aşamalarındaki bölümlerine yapay zekâ derslerinin ve anabilim dallarının eklenmesi etkin mücadele açısından önemli görünmektedir. Yapay zekâ suçlarıyla mücadele etmek üzere adli süreçte görev alan hâkimler, savcılar, polisler gibi yetkililerin teknolojik ilerlemenin getireceği yeniliklere uyum sağlayabilmeleri için düzenli eğitim programları tasarlanması gerekmektedir. Yapay zekâ suçlarının teknik takibi, ispatı ve yargılanma süreçleri teknik altyapı kadar hukuki düzenlemeleri de gerektirmektedir.

Suçun ortaya çıkmasının bağlı olduğu unsurlardan birisi, yetenekli koruyucunun yokluğu olduğuna göre koruyucuları güçlendirmek yapay zekâ suçlarını önleme çalışmalarına katkı sağlayacaktır. Şöyle ki, yetenekli koruyucuları yapay zekâ suçları bağlamında yeniden düşünecek olursak hukuki düzenlemeler ve yaptırımlar önem kazanmaktadır. En büyük problem suç takibinin yapılması ve suçlunun yakalanması meselesidir. Yapay zekânın suç işlemede kullanılırken uygulanan teknolojinin üzerine çıkacak yapıya ulaşılarak suçlu aydınlatma ve suçluyu yakalama süreçleri geliştiği takdirde ve bu teknolojinin meydana getireceği suç ve suçlulara ilişkin hukuki düzenlemeler yapıldığı takdirde yetenekli koruyucular güçlenmiş olacak ve suçun ortaya çıkmasına sebep olacak unsurlardan biri ortadan kalkacaktır. Yapay zekânın sebep olduğu tehditlere karşı yapay zekânın etkin kullanımıyla sürecin gerisinde kalmamak önemlidir. Ayrıca suç hedefi olan kişilerin yetenekli koruyucu olarak nitelendirilebilecek olan bilgisayarlarında koruma programlarının olmaması ya da güçlü şifre kullanmamaları kişisel verilerin (görüntüler, şifreler vb.) ele geçirilmesini kolaylaştırmaktadır. Kişisel veriler yapay zekâ aracılığıyla

işlenerek gerçek olmayan videolara dönüştürülmektedir. Gelişen teknolojinin ve yapay zekânın risklerine karşı toplumu bilinçlendirmek yetenekli koruyucuların etkin hale gelmesini sağlayacaktır. Bu durumda da rutin aktivite teorisinin ortaya koyduğu yetenekli koruyucuların yokluğu unsuru elimine edilerek suç davranışlarının azalması ya da önlenmesi sağlanabilecektir.

Kaynaklar

- Abbott, R., & Sarch, A. F. (2019). *Punishing Artificial Intelligence: Legal Fiction or Science Fiction* (SSRN Scholarly Paper 3327485). Social Science Research Network. <https://doi.org/10.2139/ssrn.3327485>
- Ak, T. (2021). Yapay Zekâ Teknolojileri, Güvenlik ve Kolluk Kuvvetinin Suç Önleme Faaliyetleri. *SDE Akademi*, 1(1), Article 1.
- Akbulut, B. (2023). Yapay Zeka ve Ceza Hukuku Sorumluluğu. *Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi*, 27(4), Article 4. <https://doi.org/10.34246/ahbvuhfd.1339596>
- al Qatawneh, I., Moussa, A., Haswa, M., Jaffal, Z., & Barafı, J. (2023). Artificial Intelligence Crimes. *Academic Journal of Interdisciplinary Studies*, 12(1), 143-150. <https://doi.org/10.36941/ajis-2023-0012>
- Anadolu Ajansı. (2023). *TPAO'dan sahte reklam uyarısı—Son Dakika Türkiye Haberleri* | NTV Haber. NTV. https://www.ntv.com.tr/turkiye/tpaodan-sahte-reklam-uyarisi,45NQCmFgIEKiJSQr_nC7vw
- Anıkaydın, İ. (2022). Deepfake Uygulamalarının Hukuki Boyutu. *Düzce Üniversitesi Sosyal Bilimler Dergisi*, 12(2), 736-747. <https://doi.org/10.55179/dusbed.1131728>
- Arslan, F. (2023). Deepfake Technology: A Criminological Literature Review. *Sakarya Üniversitesi Hukuk Fakültesi Dergisi*, 11(1), Article 1. <https://doi.org/10.56701/shd.1293642>

- Bennett Moses, L., & Chan, J. (2014). *Using Big Data for Legal and Law Enforcement Decisions: Testing the New Tools* (SSRN Scholarly Paper 2513564).
<https://papers.ssrn.com/abstract=2513564>
- Bennett Moses, L., & Chan, J. (2016). *Algorithmic Prediction in Policing: Assumptions, Evaluation, and Accountability* (SSRN Scholarly Paper 3742541). Social Science Research Network. <https://doi.org/10.2139/ssrn.3742541>
- Berk, M. E. (2020). Dijital Çağın Yeni Tehlikesi “Deepfake”. *OPUS Uluslararası Toplum Araştırmaları Dergisi*, 16(28), 1-1. <https://doi.org/10.26466/opus.683819>
- Berk, R. A. (2021). Artificial Intelligence, Predictive Policing, and Risk Assessment for Law Enforcement. *Annual Review of Criminology*, 4(Volume 4, 2021), 209-237.
<https://doi.org/10.1146/annurev-criminol-051520-012342>
- Broadhurst, R., Maxim, D., Brown, P., & Trivedi, H. (2019). *Artificial Intelligence and Crime: A Report for the Korean Institute of Criminology*.
- Brown, S. (2006). The criminology of hybrids: Rethinking crime and law in technosocial networks. *Theoretical Criminology*, 10(2), 223-244.
<https://doi.org/10.1177/1362480606063140>
- Butz, M. V. (2021). Towards Strong AI. *KI - Künstliche Intelligenz*, 35(1), 91-101.
<https://doi.org/10.1007/s13218-021-00705-x>
- Campedelli, G. M. (2021). Where are we? Using Scopus to map the literature at the intersection between artificial intelligence and research on crime. *Journal of Computational Social Science*, 4(2), 503-530. <https://doi.org/10.1007/s42001-020-00082-9>
- Can, M. (2025). SON DAKİKA: Yapay zeka ile milyonluk vurgun! Akıllamaz tezgah: Deepfake ile oluşturup dolandırdılar. *Sabah*.

<https://www.sabah.com.tr/galeri/yasam/son-dakika-yapay-zeka-ile-milyonluk-vurgun-akilalmaz-tezgah-deepfake-ile-olusturup-dolandirdilar>

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, 44(4), 588-608.
<https://doi.org/10.2307/2094589>

Cohen-Almagor, R. (2011). Internet History. *International Journal of Technoethics*, 2(2), 45-64.

Dakalbab, F., Abu Talib, M., Abu Waraga, O., Bou Nassif, A., Abbas, S., & Nasir, Q. (2022). Artificial intelligence & crime prediction: A systematic literature review. *Social Sciences & Humanities Open*, 6(1), 100342.
<https://doi.org/10.1016/j.ssaho.2022.100342>

Damar, M., Özen, A., Çakmak, Ü., Özoğuz, E., & Erenay, F. (2024). Super AI, Generative AI, Narrow AI and Chatbots: An Assessment of Artificial Intelligence Technologies for The Public Sector and Public Administration. *Journal of AI*, 8, 83-106.
<https://doi.org/10.61969/jai.1512906>

Değirmenci, O. (2021). Yapay Zekâ ve Ceza Hukuku Sorumluluğu. *Ardahan Barosu Dergisi, Eylül*, 74-88.

Demircan, B. (2021). “Gördüğün Her Şeye İnanma”: Derin Sahte Çalışmaları Üzerine Bir Doküman Analizi. *TRT Akademi*, 6(13), Article 13.
<https://doi.org/10.37679/trta.969162>

Gönenç, E. Ö. (2003). İnternet ve Türkiye’deki Gelişimi. *İletişim Fakültesi Dergisi*, 16, 87-98.

Güngör, M. (2024). Yapay Zekânın Suç Potansiyelinin Değerlendirilmesi. *Bilişim Hukuku Dergisi*, 6(2), 620-660. <https://doi.org/10.55009/bilisimhukukudergisi.1498256>

- Hallevy, G. (2010). The Criminal Liability of Artificial Intelligence Entities—From Science Fiction to Legal Social Control. *Akron Intellectual Property Journal*, 4, 171-199.
- Hallevy, G. (2015). *Liability for Crimes Involving Artificial Intelligence Systems*. Springer.
- Hallevy, G. (2018). Yapay Zekaya Sahip Varlıkların Cezai Sorumluluğu-Bilim Kurgudan Yasal Toplumsal Denetime (M. Fincan, Çev.). *Küresel Bakış*, 8(24), 111-142.
- Hasan, M. N. (2022). *Applicability of Routine Activity Theory: An analysis based on cybercrime in Bangladesh* (SSRN Scholarly Paper 4265385). Social Science Research Network. <https://doi.org/10.2139/ssrn.4265385>
- Hawdon, J., Parti, K., & Dearden, T. E. (2020). Cybercrime in America amid COVID-19: The Initial Results from a Natural Experiment. *American Journal of Criminal Justice: AJCJ*, 45(4), 546-562. <https://doi.org/10.1007/s12103-020-09534-4>
- Hayward, K. J., & Maas, M. M. (2021). Artificial intelligence and crime: A primer for criminologists. *Crime, Media, Culture: An International Journal*, 17(2), 209-233. <https://doi.org/10.1177/1741659020917434>
- Heather, C., & Magramo, K. (2024, Şubat 4). *Finance worker pays out \$25 million after video call with deepfake 'chief financial officer'*. CNN. <https://www.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk>
- Holt, T. J., & Bossler, A. M. (2009). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. *Deviant Behavior*, 30(1), 1-25. <https://doi.org/10.1080/01639620701876577>
- İletişim Başkanlığı. (2023). *Sahte reklam filmleri ve kısa mesaj dolandırıcılıkları hakkında açıklama* [Türkiye Cumhuriyeti Cumhurbaşkanlığı İletişim Başkanlığı]. <https://www.iletisim.gov.tr/turkce/Haberler/detay/cumhurbaskani-erdoganin-goruntulerinin-kullanildigi-sahte-reklam-filmi-hakkinda-aciklama/>

- Karabal, A. (2023). Yapay Zekada Hukuk İhlalleri. *MetaZihin: Yapay Zeka ve Zihin Felsefesi Dergisi*, 6(2), Article 2. <https://doi.org/10.51404/metazihin.1269258>
- Karakoç Keskin, E. (2025). Türkiye’de Yapay Zekânın Dezenformasyon Karnesi: Yapay Zekâ ile Üretilen Dezenformasyona İlişin Doğruluk Kontrollerinin İçerik Analizi. *TRT Akademi*, 10(23), Article 23. <https://doi.org/10.37679/trta.1557154>
- Kasperkevic, J. (2015, Nisan 22). Swiss police release robot that bought ecstasy online. *The Guardian*. <https://www.theguardian.com/world/2015/apr/22/swiss-police-release-robot-random-darknet-shopper-ecstasy-deep-web>
- Khan, C. (2023). The Future of Criminology: Exploring Emerging Trends and Challenges. *Social Science Review Archives*, 1(1), Article 1.
- Kigerl, A. (2012). Routine Activity Theory and the Determinants of High Cybercrime Countries. *Soc. Sci. Comput. Rev.*, 30(4), 470-486. <https://doi.org/10.1177/0894439311422689>
- Kim, S., Joshi, P., Kalsi, P. S., & Taheri, P. (2018). Crime Analysis Through Machine Learning. *2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, 415-420. <https://doi.org/10.1109/IEMCON.2018.8614828>
- Lee, D. (2016, Mart 25). Tay: Microsoft issues apology over racist chatbot fiasco. *BBC News*. <https://www.bbc.com/news/technology-35902104>
- Mankoo, S. S. (2023). DeepFakes- The Digital Threat in the Real World. *Gyan Management Journal*, 17(1), 71-77. <https://doi.org/10.48165/gmj.2022.17.1.8>
- Marcum, C., Higgins, G., & Ricketts, M. (2010). Potential Factors of Online Victimization of Youth: An Examination of Adolescent Online Behaviors Utilizing Routine Activity Theory. *Deviant Behavior*, 31, 381-410. <https://doi.org/10.1080/01639620903004903>

- Neff, G., & Nagy, P. (2016). Talking to Bots: Symbiotic Agency and the Case of Tay. *International Journal of Communication*, 10, 4915-4931.
- Okuyucu Ergün, G. (2023). Machina Sapiens. *Ankara Üniversitesi Hukuk Fakültesi Dergisi*, 72(2), Article 2. <https://doi.org/10.33629/auhfd.1288894>
- O'Neill, P. H. (2015). Drug-buying robot arrested in Switzerland. *daily dot*. <https://www.dailydot.com/unclick/random-darknet-shopper-seized/>
- Özdemir, Ş. (2021). Yeni Nesil Tehdit: Derin Kurgu (DeepFake). *TRT Akademi*, 6(13), Article 13. <https://doi.org/10.37679/trta.1002526>
- Pagallo, U. (2011). Robots of Just War: A Legal Perspective. *Philosophy and Technology*, 24(3), 307-323. <https://doi.org/10.1007/s13347-011-0024-9>
- Pagallo, U. (2017). AI and bad robots: The criminology of automation. İçinde *The Routledge Handbook of Technology, Crime and Justice* (ss. 643-653). <https://doi.org/10.4324/9781315743981>
- Pratt, T., Holtfreter, K., & Reisig, M. (2010). Routine Online Activity and Internet Fraud Targeting: Extending the Generality of Routine Activity Theory. *Journal of Research in Crime and Delinquency*, 47, 267-296. <https://doi.org/10.1177/0022427810365903>
- Reyns, B. (2013). Online Routines and Identity Theft Victimization Further Expanding Routine Activity Theory beyond Direct-Contact Offenses. *Journal of Research in Crime and Delinquency*, 50, 216-238. <https://doi.org/10.1177/0022427811425539>
- Roitblat, H. (2025). *Some things to know about achieving artificial general intelligence* (arXiv:2502.07828). arXiv. <https://doi.org/10.48550/arXiv.2502.07828>
- Russell, S. J., Norvig, P., & Davis, E. (2010). *Artificial intelligence: A modern approach* (3rd ed). Prentice Hall.
- Tai, M. C.-T. (2020). The impact of artificial intelligence on human society and bioethics. *Tzu Chi Medical Journal*, 32(4), 339. https://doi.org/10.4103/tcmj.tcmj_71_20

- Tseng, P. (2018). *What Can The Law Do About 'Deepfake'?* [Litigation and Intellectual Property Bulletin]. McMillan. <https://mcmillan.ca/insights/what-can-the-law-do-about-deepfake/>
- Tufan, B. N. (2025). YAPAY ZEKÂ VE SUÇ: GELECEK AÇISINDAN HUKUKSAL VE ETİK TEHDİTLER. *Medeniyet Kültürel Araştırmalar Belleteni*, 4(7), Article 7. <https://doi.org/10.60051/medbel.1585638>
- Türk Ceza Kanunu, 5237 § 10 (2004).
- Ulusoy, H., & İlhan, Ç. K. (2025). Siyasal İletişimde Yapay Zekâ Etkisi ve Deepfake (Derin Sahte) Dezenformasyonu: 2024 ABD Başkanlık Seçimleri Örneği. *TRT Akademi*, 10(23), Article 23. <https://doi.org/10.37679/trta.1563828>
- Vaccari, C., & Chadwick, A. (2024). Deepfake ve Dezenformasyon: Sentetik Siyasi Videoların Yanıltma, Belirsizlik ve Haberlere Duyulan Güven Üzerindeki Etkisini Araştırma. *Yeni Medya*, 17, Article 17.
- Yar, M. (2005). The Novelty of 'Cybercrime' An Assessment in Light of Routine Activity Theory. *European Journal of Criminology*, 2, 407-427. <https://doi.org/10.1177/147737080556056>