TAAD Yıl 17 . Sayı 66 . Nisan 2026
ISSN 1309-6826
Araştırma Makalesi/Research Article
DOI: 10.54049/taad.1861138

YAPAY ZEKÂ DESTEKLİ SOSYAL MÜHENDİSLİK SALDIRILARI: CEZA HUKUKU AÇISINDAN BİR İNCELEME

AI-Powered Social Engineering Attacks: An Analysis from the Perspective of Criminal Law

Emin GİTMEZ*

Özet

Bu çalışma, yapay zekâ teknolojilerinin sosyal mühendislik saldırılarına etkisini ceza hukuku perspektifinden incelemektedir. Yapay zekânın özellikle üretken modeller, ses klonlama, deepfake, otomatik oltalama sistemleri ve manipülatif sohbet robotları aracılığıyla geleneksel sosyal mühendisliği daha sofistike, hızlı ve tespit edilmesi güç bir hale getirdiği ortaya konulmuştur. Bu saldırılar, yalnızca bireylerin değil, kurumların, kamu düzeninin ve dijital güvenliğin bütününü tehdit eden yeni bir suç alanı yaratmaktadır. Çalışmada sosyal mühendislik kavramının tarihsel ve kavramsal gelişimi ele alınmış; yapay zekâ destekli saldırıların klasik yöntemleri nasıl dönüştürdüğü detaylı biçimde açıklanmıştır. Türk ceza hukuku yönünden, yapay zekâ destekli sosyal mühendislik saldırılarının dolandırıcılık (TCK m.157–158), özel hayatın gizliliğini ihlal (TCK m.134), kişisel verilerin hukuka aykırı kaydedilmesi ve yayılması (TCK m.135–136) ile bilişim alanındaki suçlar (TCK m.243–245) kapsamında cezalandırılabilir olduğu tespit edilmiştir. Çalışmada kurgusal bir örnek olay üzerinden bu suç tiplerinin nasıl uygulanacağı somutlaştırılmıştır. Karşılaştırmalı hukukta Avrupa Birliği'nin Yapay Zekâ Tüzüğü (AI Act), GDPR ve NIS Direktifi gibi düzenlemelerle geliştirici ve platform işletmecilerine önemli yükümlülükler getirdiği; ABD'de ise cezai sorumluluk alanında parçalı ve sınırlı bir yaklaşım bulunduğu ifade edilmiştir. Çalışma, mevcut ceza hukuku normlarının yapay zekâ destekli sosyal mühendislik saldırılarını karşılamada yetersiz kaldığını, bu nedenle Türk Ceza Hukukunda gerekli düzenlemelerin yapılması gerektiğini ortaya koymaktadır.

Anahtar Kelimeler: Yapay zekâ destekli sosyal mühendislik, TCK'da bilişim suçları, yapay zekâ ve ceza sorumluluğu

Abstract

This study examines the impact of artificial intelligence technologies on social engineering attacks from a criminal law perspective. It demonstrates that artificial intelligence, particularly through generative models, voice cloning, deepfakes, automated phishing systems, and manipulative chatbots, has made traditional social engineering more sophisticated, rapid, and difficult to detect. These attacks create a new criminal landscape that threatens not only individuals but also institutions, public order, and digital security as a whole. Under Turkish criminal law, it has been determined

- *Bu makale Etik Kurul iznine tabi değildir/This article is not subject to Ethics Committee permission.*
- *Makale Geliş Tarihi/Article Received Date: 21.1.2026*
- *Yayın Kurulu Kabul Tarihi/Editorial Board Acceptance Date: 17.4.2026*

* Dr. Öğr. Üyesi, İnönü Üniversitesi, İİBF Siyaset Bilimi ve Kamu Yönetimi Bölümü Hukuk Bilimleri Ana Bilim Dalı, Malatya/Türkiye, e-Posta: emin.gitmez@inonu.edu.tr, https://orcid.org/0000-0002-6678-2506.

that AI-enabled social engineering attacks are punishable under the following categories; fraud, violation of privacy, unlawful recording and dissemination of personal data, and cybercrimes. The study illustrates the application of these crimes through a fictional case study. In comparative law, it has been noted that the European Union imposes significant obligations on developers and platform operators through regulations such as the AI Act, GDPR, and the NIS Directive, while the US has a fragmented and limited approach to criminal liability. The study demonstrates that existing criminal law norms are insufficient to address AI-assisted social engineering attacks, and therefore, the necessary amendments must be made to Turkish Criminal Law.

Keywords: AI-powered social engineering, cybercrimes under the Turkish Penal Code, artificial intelligence and criminal liability

GİRİŞ

Sosyal mühendislik ile bir değer ifade eden her türlü bilginin saldırıya uğraması mümkündür. Günümüzde yapay zekâ teknolojilerinin hızla gelişmesi, siber güvenlik alanında hem savunma hem de saldırı yöntemlerinin dönüşmesine neden olmuştur. Bu teknolojilerin sosyal mühendislik saldırılarında kullanılması, klasik dolandırıcılık faaliyetlerini ve veri ihlali yöntemlerini ileri bir boyuta taşımıştır. Çünkü bu teknolojilerin kullanılması geleneksel olana kıyasla çok daha etkili ve tespit edilmesi zor sonuçların ortaya çıkmasına neden olmaktadır. Ses klonlama, derin sahte (deepfake) videolar, otomatik oltalama (phishing) içerikleri, rol yapma ve tersine sosyal mühendislik gibi yöntemlerle bireylerin, kurumların ve hatta devletlerin aldatılması mümkün hale gelmiştir.

İngiltere hükûmetlerinin 2024 Siber Güvenlik İhlalleri Anketi'ne[1] göre, birçok işletme ve yardım kuruluşu çok yakın zamanda siber güvenlik ihlalleri veya saldırılarıyla karşı karşıya kalmıştır. En yaygın olanı, işletmelerin %84'ünü ve yardım kuruluşlarının ise %83'ünü etkileyen kimlik avı saldırısıdır[2]. Bilgisayar korsanları taktiklerini geliştirmek için üretken yapay zekayı kullandıkça telefonla yapılan kimlik avı saldırıları (vishing) ve deepfake saldırıları artmıştır. Buna karşılık, çoğu işletme ve yardım kuruluşu, kendilerini siber tehditlere karşı korumak için geniş bir yelpazede önlemler almaya devam etmektedir. Bu bağlamda, yapay zekâ destekli sosyal mühendislik saldırıları yalnızca bireylerin değil, kamusal düzenin ve dijital güvenliğin bütününü tehdit edecek bir boyuta evrilmiştir. Bu gelişmeler, ceza hukuku bağlamında yeni suç tiplerinin ortaya çıkmasına da neden olmuştur. Bu durum ceza hukukunun sorumluluk alanlarının tartışılmasını da beraberinde getirmiştir.

---

1 7 Eylül 2023 ile 19 Ocak 2024 tarihleri arasında 2.000 İngiltere işletmesi, 1.004 İngiltere kayıtlı hayır kurumu ve 430 eğitim kurumuyla rastgele olasılıklı telefon ve çevrimiçi anket gerçekleştirilmiştir. İşletmeler ve hayır kurumlarına ait veriler, bu iki popülasyonu istatistiksel olarak temsil edecek şekilde ağırlıklandırılmıştır.

2 Maddy Ell, '2024 UK Cyber Security Breaches Survey' (*Gov.Uk*, 09 April 2024) <https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024/cyber-security-breaches-survey-2024> Erişim Tarihi 20 May 2025.

Bu çalışmada, yapay zekâ teknolojilerinin sosyal mühendislik saldırılarında nasıl kullanıldığı analiz edilmiştir. Bununla birlikte bu kullanım Türk Ceza Hukuku açısından değerlendirilmiştir. Uluslararası yaklaşımlar ve karşılaştırmalı hukuk açısından da konuya açıklık getirilmiştir. Ayrıca, mevzuattaki boşluklar, uygulamada karşılaşılan sorunlar ve çözüm önerilerine de yer verilmiştir. Sonuca binaen, mevcut ceza hukuku düzenlemelerinin, yapay zekâ destekli sosyal mühendislik saldırılarını doğrudan hedef alacak şekilde yeterli düzeyde olmadığı; bu nedenle kanun koyucunun teknoloji temelli suç tiplerini içeren özel düzenlemelere gitmesi gerektiği de ortaya konulmuştur.

I. SOSYAL MÜHENDİSLİK KAVRAMI VE EVRİMİ

Sosyal mühendislik kavramı kişileri aldatma sürecidir. Bu sebeple, sosyal mühendislik faaliyetleri anlık değildir. Bu sürecin ortaya konulması herkesçe benimsenen değerlerin kötü amacın gizlenmesi suretiyle suistimal edilmesi, istismara uğratılması yoluyla mümkün olabilmektedir. Süreç, kendi içinde karşıdaki kitleyi maniple edecek birtakım hazırlık hareketlerini içerir. Bu hazırlık faaliyetleri neticesinde kitle aldatılma sürecine girer. Kötü amaçlı kişiler aldatılma sürecinin sonunda önemli ve gizli bilgilere erişmiş olur.

A. Sosyal Mühendislik Nedir?

"Sosyal mühendis" terimi ilk kez İngiliz ekonomist John Gray'in 1842'de yayınlanan "*An Efficient Remedy for the Distress of Nations (Ulusların Sıkıntısına Etkin Bir Çare)"* adlı kitabında ortaya çıkmıştır. Toplumun hastalıklarını nasıl çözeceklerini bildiklerine inanan dönemin «siyasi ve sosyal mühendislerini», çalışmayan bir buhar makinesi için ayrı ayrı sorunu teşhis etmek üzere birbirinden habersiz çağrılan bir grup makine mühendisine benzetmiştir. Makine mühendisleri bir buhar makinesinin nasıl çalışması gerektiğini bilirler. Ve her biri ayrı ayrı çağrılsa da aynı doğru teşhise varır. Çünkü onların her biri kendi alanlarının gerektirdiği teknik donanıma fazlasıyla sahiptir ve başarılıdır. Fakat, sosyal mühendisler asla başarılı olamaz. Çünkü siyasi ve toplumsal konularda sosyal nedenler ve sonuçlar hakkında uzman bilgisine sahip olunması neredeyse imkânsızdır. Gray'a göre uygun sosyal mühendislik, toplumdaki insan davranışı hakkında uzman bilgisi gerektirir. Fakat, makine mühendislerinin aksine toplum hakkında böyle bir doğru ve toplu bilgiye erişmek mümkün değildir[3]. Siber güvenlik alanına ilişkin sosyal mühendislik kavramı ise ilk kez Eylül 1984'te yayımlanan *More on Trashing*[4] başlıklı bir makaledir. Bu makale, bir telekomünikasyon

---

[3] John Gray, *An Efficient Remedy for the Distress of Nations* (Edinburgh: William Tait 1842); Joseph M. Hatfield, Social engineering in cybersecurity: The evolution ofa concept. *Computers & Security* 73 (2018), 102–113.

[4] The Kid & Co. and The Shadow, 'More on trashing,' (1984) 1(9) 2600 Magazine: The Hacker's Quarterly <http://www.hackcanada.com/ice3/2600/2600_01-9_p50.txt> Erişim Tarihi 20 Temmuz

şirketinin çöpünün çok değerli bilgiler içerdiğini göstermiş ve çöp yoluyla bilgi toplamak için bazı özel yöntemleri tartışmıştır.

Sosyal mühendislik, bir bireyi, bir insan topluluğunu veya bir kuruluşu, belirli bir saldırganın isteğine uymaya ikna etmek için bir araç olarak sosyal etkileşimi kullanma bilimidir[5]. Sosyal mühendislik İnsanları hassas bilgileri ifşa etmeye ikna etme sanatıdır. Tipik bir sosyal mühendislik saldırısı genel olarak dört aşamada tamamlanır. Bu aşamalar ön araştırma, ilişki kurma, güven inşa etme ve bilgi edinme şeklindedir. Saldırgan önce hedefi araştırır, ardından onu etkilemek için iletişim kurar, kullanıcının güvenini kazanır ve bilgi edinme sürecine geçer[6]. Bu döngü, saldırganın hedef kişiden parola, kimlik bilgisi, finansal veri veya sistem erişimi gibi bilgiler elde etmesiyle tamamlanır. Sosyal mühendisliğin çeşitli tanımları ve bir dizi farklı sosyal mühendislik saldırısı modeli vardır.

Klasik sosyal mühendislik yöntemleri arasında "phishing" (oltalama), "pretexting" (öykü uydurma), "baiting" (tuzak veri) ve "tailgating" (fiziksel geçiş ihlali) yer alır. Oltalama tekniğinde bilgisayar korsanı kullanıcıların aldıkları mesajların meşru olduğuna inanmalarını sağlayacak şekilde bilgisayar kullanıcısına değiştirilmiş mesajlar gönderir. Bu mesajlar kullanıcıyı tuzağa çekmeyi teşvik eder nitelikte zaaflar içerir. İnsan zaafları saldırganların sosyal mühendislik saldırısı gerçekleştirmek için kullandıkları insan faktörleridir. Bu insan zaafları psikoloji, biliş, bilinç, düşünce, davranış alışkanlıkları ve sinirsel reflekslerden kaynaklanabilir. Kullanıcıların mesajdaki talimatları veya önerileri takip etmeleriyle saldırı gerçekleşmiş olur. Kimlik avının en yaygın kullanılan örnekleri e-posta ve web sitesi kimlik avıdır. Bazı kimlik avları, daha fazla kullanıcı erişimi elde etmek için kötü amaçlı yazılımlar, botlar ve truva atları kullanır. Günümüzde en sık karşılaşılan yöntemlerden bir tanesi Vishing yöntemidir. Bu yöntemle korsanlar kullanıcıların telefonlarının PIN kodlarına, tek kullanımlık parolalarına gibi gizli bilgilerine erişebilmektedir. Sıkça kullanılan Vishing örnekleri arasında da Yardım Masasında Kimlik Sahtekarlığı[7] saldırıları ve Otomatik Arama saldırıları[8] yer almaktadır.

2025.

5 Florence Sèdes and Jonathan Degrace, 'Social Engineering and Security: From Human Vulnerabilities to Malicious Threats' (2024 20th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob) Paris, October 2024).

6 Kevin D Mitnick and William L Simon, *The Art of Deception: Controlling the Human Element of Security* (Wiley Publishing 2002) 1-6.

7 Yardım masası kimlik sahtekarlığı, bir saldırganın, genellikle bir çalışan veya üst düzey yönetici gibi davranarak (kimliğine bürünerek), kurumun bilgi teknolojileri destek biriminden (help desk) hassas verilere ulaşmaya çalıştığı sosyal mühendislik yöntemidir. Wenni Syafitri *and others*, 'Social Engineering Attacks Prevention: A Systematic Literature Review' (2022) 10 IEEE Access 39325, 39327.

8 Vishing yoluyla yapılan kimlik saldırılarının önceden programlanmış sesli yanıt sistemleri veya robot çağrılar yoluyla otomatik hale getirilmiş halidir. US Cybersecurity and Infrastructure Security

B. Yapay Zekâ ile Sosyal Mühendisliğin Dönüşümü

2000'li yıllarla birlikte sosyal mühendislik kavramı çok yönlü bir evrim geçirmiştir. Teknoloji uygulamalarındaki artış ve sosyal mühendislik üzerine yapılan tartışmalar ile önemli sosyal mühendislik saldırıları konuyu ülkeler nezdinde daha görünür kılmıştır. Bununla birlikte ulus ötesi ilişkiler, sosyal psikoloji, sosyal güven, dil psikolojisi gibi duygu ve ifade içeren disiplinler sosyal mühendislik kavramını disiplinler arası konuma oturtmuştur. Siber alanda özellikle ağ teknolojilerinde meydana gelen yenilikler ve iyileştirmeler yeni siber saldırı yöntemlerinin görülmesine neden olmuştur[9]. Hatta teknoloji alanında ortaya çıkan her aldatıcı faaliyet sosyal mühendislik şemsiyesinin altına yerleştirilerek sosyal mühendisliğin kavramsal alanı genişletilmiştir.

Yapay zekâ, öncelikle veri bolluğu, geliştirilmiş algoritmalar ve donanım altyapısındaki ilerlemeler gibi temel faktörler tarafından yönlendirilen dönüştürücü bir teknoloji olarak ortaya çıkmıştır. Klasik sosyal mühendislik tekniklerini daha sofistike ve etkili hale getirerek bireylerin ve kurumların güvenliğini ciddi biçimde tehdit etmeye başlamıştır. Çünkü yapay zekanın yenilikçi ve hızlı doğası, saldırganların sosyal mühendislik saldırı yöntemlerini otomatikleştirmesini ve ölçeklendirmesi sağlamıştır. Kişi ve kurumlara yapılan saldırıların zemininin genişletilmesine neden olmuştur. Geleneksel sosyal mühendislik; insanları manipüle ederek bilgi toplamak veya sistemlere sızmak üzerine kurulu iken, yapay zekâ destekli saldırılar bu süreci otomatikleştirip gerçeklik algısını bozmaktadır. Yapay zekâ destekli sosyal mühendislik saldırılarında yapay zekanın farklı becerilere sahip türleri sıklıkla kullanılmaktadır. Bu saldırıların sonuç almasında üretken yapay zekâ diğerlerine oranla bilgisayar korsanları tarafından daha çok tercih edilmektedir. Üretken yapay zekâ, derin öğrenmeye dayalı yapay zekâ modelleri olup eğitildikleri girdi verilerine benzeyen yeni içerikler üretmek üzere tasarlanmıştır. Üretken Çelişkili Ağlar (GAN'lar) ve gerçekçi metinsel içerik üreten GPT-4 ve Palm 2 gibi Büyük Dil Modelleri (LLM'ler) bulunur sentetik görüntüler ve videolar üreten yapay zeka örnekleridir.[10]

Yapay zekanın kullanıldığı ve farklı ülkelerde gerçekleşen çok sayıda sosyal mühendislik saldırıları bulunmaktadır. Yapay zekâ destekli ses klonlama saldırısı ile bilgisayar korsanları tarafından, Alman menşeli bir enerji şirketinin CEO'sunun sesi taklit edilerek Birleşik Krallık merkezli bir enerji şirketinden 243.000 ABD doları değerinde yasadışı bir para transferini gerçekleştirilmiştir. Para transfer edildikten sonra birden çok hesap üzerinden farklı hesaplara aktarılarak takip

Agency (CISA), 'Social Engineering Attacks' <https://www.cisa.gov> Erişim Tarihi 11 Haziran 2025.

9 Zuoguang Wang, Limin Sun and Hongsong Zhu, 'Defining Social Engineering in Cybersecurity' (2020) 8 IEEE Access 85099

10 Marc Schmitt Ivan Flechais 'Digital deception: generative artificial intelligence in social engineering and phishing' (2024) 57(324) Artifical Intelligence Review 2, 8-11.

zorlaştırılmıştır[11]. Yapay zekâ destekli phishing saldırıları da sıklıkla kullanılmaktadır. 2021 yılında ABD'de Colonial Pipeline şirketine yapılan saldırıda, bir çalışan phishing e-postası üzerinden zararlı yazılımı sistemine yüklemiştir. Bu şirket Houston, Teksas'tan, New Jersey'e uzanan bir sistem içinde günlük 100 milyon galondan fazla yakıt taşıyan önemli bir boru hattını işletmekteydi. Bu siber saldırı, ABD'nin Doğu Yakası boyunca yakıt tedarikinde yaygın bir kesintiye neden olmuştur. Bu durum ülkenin en büyük akaryakıt boru hattının günlerce kapanmasına neden olmuştur[12]. Benzer şekilde gerçek Deepfake saldırı örneklerini de görmek mümkündür. Rusya'nın Ukrayna'yı işgali sırasında, Ukrayna Cumhurbaşkanı Volodimir Zelenskiy'i Ukrayna ordusuna silah bırakma çağrısı yaparken gösteren sahte bir video sosyal medyada yayılmıştır. Video, kısa sürede ifşa edilmiştir ancak geçici de olsa kafa karışıklığı yaratmıştır[13]. Barack Obama'nın deepfake videolarının ne kadar ikna edici olabileceğini göstermek için 2018 yılında konuştuğu video da bir başka örnektir[14]. Bu yönüyle Deepfake kitleleri maniple etmek amacıyla sıklıkla kullanılan bir sosyal mühendislik türüdür. Bugün itibariyle deepfake teknolojisi kolluk kuvvetleri açısından giderek büyüyen bir tehdit halini almıştır. Deepfake teknolojisi özellikle şu alanlarda suçun işlenmesini kolaylaştırmaktadır[15].

- Kişilerin internet ortamında ifşa edilmesi veya utandırılması,
- Şantaj ve dolandırıcılık faaliyetleri,
- Resmî belge sahteciliği,
- Sahte dijital kimlikler yaratılarak KYC (müşteri tanıma) protokollerinin aşılması,
- Rızaya dayanmayan müstehcen içerik yayılması,
- Çocukların istismarı,

---

11 Stupp C, 'Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case' *Wall Street Journal* (30 August 2019) <https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402> Erişim Tarihi 14 Haziran 2025.

12 Ido Kilovaty 'Cybersecuring the Pipeline' (2023) 60(3) Houston Law Review 605; Colonial Pipeline 'Media Statement Update: Colonial Pipeline System Disruption' (Colonial Pipeline, 17 May 2021) <https://www.colpipe.com/news/press-releases/media-statement-colonial-pipeline-system-disruption> Erişim Tarihi 14 Haziran 2025.

13 Marc Santora and Julian E. Barnes, 'Fake Video Shows Zelensky Telling Troops to Surrender' *The New York Times* (16 March 2022) <https://www.nytimes.com/2022/03/16/world/europe/zelensky-deepfake-video.html> Erişim Tarihi 18 Mayıs 2025

14 Olivia Solon, 'The Future Of Fake News: Don't Believe Everything You Read, See Or Hear' (*The Guardian*, 26 July 2017). <https://www.theguardian.com/technology/2017/jul/26/fake-news-obama-video-trump-face2face-doctored-content> Erişim Tarihi 18 Mayıs 2025

15 Cornelia Riehle, 'Europol Report Criminal Use of Deepfake Technology' (*Eucrim,* 9 May 2022) <https://eucrim.eu/news/europol-report-criminal-use-of-deepfake-technology/> Erişim Tarihi 18 Mayıs 2025.

- Ceza soruşturmalarında elektronik delillerin manipülasyonu,
- Finansal piyasaların manipüle edilmesi,
- Yanıltıcı bilgi yayımı ile kamuoyu etkilenmesi,
- Aşırılık yanlısı veya terörist anlatıların desteklenmesi,
- Toplumsal huzursuzluk ve politik kutuplaşmanın körüklenmesi.

Deeepfake teknolojisi suçların işlenmesini kolaylaştırmanın yanında mahkemelerde dijital delillerin güvenilirliğini doğrudan tehdit eder hâle gelmiştir. Deepfake ses, görüntü ve belgeler adli süreçlerde sunulmakta, böylece hukuki süreçlerin sağlığı ciddi biçimde tehlikeye atılmaktadır. Örneğin, Birleşik Krallık'ta bir velayet davasında, bir tarafın sunduğu ses kaydının deepfake olduğu anlaşılmış, karşı tarafın savunması kabul edilmiştir. Bu vaka, mahkemelerin artık dijital delillerin gerçekliğini sorgulamak zorunda kaldığını göstermektedir[16].

Özetle, yapay zekâ sosyal mühendisliği dönüştürmüştür. Yapay zekâ ile geleneksel sosyal mühendislik saldırıları şekil değiştirmiştir. Vishing, e-posta veya fiziksel etkileşim araçlarıyla ile ortaya konulan geleneksel sosyal mühendislik saldırıları yapay zekâ ile ses klonlama ve deepfake gibi saldırılara dönüşmüştür. Daha geniş kitleler saldırılara maruz kalmıştır. Saldırılar otomatikleştirilmiştir. Üstelik yapay zekâ destekli saldırılar içerik açısından daha gerçekçi olup bu saldırıları tespit etmek oldukça zordur. Bu tür saldırıların hedefe ulaşma süresi de geleneksel sosyal mühendislik saldırılarına oranla daha kolay ve hızlıdır.

II. CEZA HUKUKU PERSPEKTİFİNDEN SOSYAL MÜHENDİSLİK

A. Türk Ceza Kanunu'nda İlgili Hükümler

Yapay zekâ destekli sosyal mühendislik saldırıları suça konu olayın meydana gelme şekli, fail ve mağdurun durumu gibi nedenlerle Türk Ceza Kanunu'nda yer alan birden fazla suç türünü içerebilir. Bu suç türleri dolandırıcılık (Türk Ceza Kanunu madde 157-158), özel hayatın gizliliğini ihlal (Türk Ceza Kanunu madde 134), bilişim suçları (Türk Ceza Kanunu madde 243-245), kişisel verilerin hukuka aykırı olarak işlenmesi (Türk Ceza Kanunu madde 136), çocukların cinsel istismarı (Türk Ceza Kanunu madde 103), hakaret (Türk Ceza Kanunu madde 125) şeklinde görülebilir. Yapay zekâ destekli sosyal mühendislik saldırıları bu suç türlerinden dolandırıcılık, özel hayatın gizliliğini ihlali ve bilişim suçları ile doğrudan ilişkilidir.

---

16 Tania Kukreja, 'Deepfakes as a Tool for Criminal Activity' (2025) 5(4) Jus Corpus Law Journal 224; Gurjot Singh 'Offending Sentiments, A Developing Ground Limiting Free Speech' (*Live Law*, 20 June 2025) <https://www.livelaw.in/articles/offending-sentiments-developing-ground-limiting-free-speech-295364> Erişim Tarihi 20 Haziran 2025.

Konunun bundan sonraki bölümünün anlatımı aşağıda belirtilen örnek olay üzerinden kurgulanacaktır. Her ne kadar kurgu olsa da ilerleyen dönemlerde benzer çok sayıda örnek olayla karşılaşılmasının mümkün olacağı öngörülmektedir.

> *Ahmet, herkesçe bilinen başarılı bir grafik tasarımcısıdır. Türkiye'de tanınmış freelance platformlarda yıllardır çalışmaktadır. LinkedIn ve Behance*[17] *profilleri açıktır; başarılı projeleri, ödülleri ve müşteri referansları gururla sergilenmektedir. Aynı dönemde başka bir yerde, bu bilgileri kullanan R vardır. R, yapay zekâ destekli araçlarla Ahmet'in çalışmalarını çalarak, onun gibi görünen ama aslında hiç var olmayan biri adına sahte bir profil oluşturmaktadır. Üstelik yapay zekâ destekli bir ses klonlama aracını kullanarak Ahmet'in sesini birebir taklit eder. Buna ilişkin videosunu kendi profilinde paylaşarak müşteriler nezdinde daha da kabul görmesi sağlanır. R, yapay zekâ destekli bir internet sitesi üzerinden gerçekçi bir yüz fotoğrafı üretir. ChatGPT benzeri bir LLM (dil modeli) ile "15 yıllık deneyimli grafik tasarımcı" profili hazırlar. Ahmet'in Behance hesabından projeleri indirir. Birkaç sahte tasarım üretip kendi portföyüne ekler. Ahmet'in eski müşterilerinin isimlerini, yorumlarını da sahte referans olarak kopyalar. Ahmet'in seyahat ettiği ülkelerden, kullandığı yazılım araçlarına kadar tüm detayları öğrenip sahte profiline entegre eder. Böylece müşterilerle konuşurken "aynı deneyimleri yaşamış gibi" davranır. R., büyük bir Alman şirketinde çalışan içerik yöneticisi Ayşe'ye ulaşır. Ayşe, şirketin sosyal medya kampanyası için tasarımcı aramaktadır. R., yapay zekâ destekli etkileyici mesajlarla Ayşe'yi ikna eder: "Ben de geçen yıl Nemrut Dağı Ören Yerinde drone çekimleri yaptım, sizin tarzınıza çok benzer işler yaptım, paylaşabilirim" der. Elif, sahte profili kontrol eder; her şey kusursuz görünmektedir. 20.000 Türk lirasına mal olacak iş için %50 ön ödeme yapar. R., bir hafta sonra bir yapay zekâ aracıyla üretilmiş, düşük kalitede birkaç dosya gönderir. Sonrasında atılan mesajlara cevap vermez ve profili kısa süre sonra kapanır. Ayşe, parasını geri alamaz. Araştırma yaptığında projelerin bir kısmının gerçek bir tasarımcı olan Ahmet'e ait olduğunu öğrenir. Ahmet de bir süre sonra bazı projelerinin izinsiz kullanıldığını ve adına sahte profiller açıldığını fark eder.*

Yukarıdan belirtilen olay örgüsü Türk Ceza Kanunun, 134'üncü maddesi, 157 ve 158'inci maddeleri ile 243-246 maddeleri açısından değerlendirilecektir.

1. Özel hayatın Gizliliğini İhlal Suçu (Türk Ceza Kanunu Madde 134)

1982 Anayasasında özel hayatın gizliliğinin korunması kişisel verilerin korunması hakkını içermektedir. Bu anayasal yaklaşım doğrultusunda, Türk Ceza

[17] Yaratıcı tasarımlar oluşturma konusunda faaliyet gösteren bir şirket. Bkz: <https://www.behance.net>

Kanunu'nda kişisel verilere ilişkin suçlar, "Kişilere Karşı Suçlar" kısmı içinde ve "Özel hayata ve hayatın gizli alanına karşı suçlar" başlığı altında düzenlenmiştir.[18] Özel hayatın gizliliğini ihlal suçu ilk kez 2004 tarihli 5237 sayılı Türk Ceza Kanunu'nda yer almıştır. Bir önceki mülga 765 sayılı Türk Ceza Kanunu'nda bu suça dolaylı yoldan değinen özel hayatı korumaya yönelik birtakım hükümlerin yer aldığı söylenebilir[19]. Özel hayatın gizliliğini ihlal suçu, 5237 sayılı Türk Ceza Kanunu'nun 134'üncü maddesinin 1. fıkrasında düzenlenmiştir. Yasanın 134/1'inci maddesinde; *"Kişilerin özel hayatının gizliliğini ihlâl eden kimse, altı aydan iki yıla kadar hapis veya adlî para cezası ile cezalandırılır. Gizliliğin görüntü veya seslerin kayda alınması suretiyle ihlâl edilmesi hâlinde, cezanın alt sınırı bir yıldan az olamaz"* denilmektedir. Suçun tespiti açısından özel hayat kavramından kastedilenin ne olduğunun ortaya konulması gerekir. Özel hayat öğretide farklı şekillerde tanımlanmaktadır. Bu tanımlama farklılıkları kavramın kapsamının sınırlarının belirlenmesi yönüyle değişiklik göstermektedir. Ancak en basit haliyle özel hayat, kamusal alanın dışında herkesin müdahalede bulunamayacağı, yalnızca kişiye ait olan alandır. Alman hukukunda kabul edilen Üçlü Alan/Çember Teorisi ile tanımlanabilen kamusal alan, özel alan ve mahrem alanın iç içe geçtiği ve sadece kişiye üzerinde kontrol ve denetim hakkı sağlayan yaşamın bir parçasıdır[20]. Bu suç türü Kanunda düzenlenmiş olduğu bölüm başlığı altında yer alan diğer suç türlerini de kapsayan torba suç niteliğindedir. Suç açısından korunan hukuki değer kişinin sahip olduğu, üzerinde hakimiyet kurduğu, değerler açısından kişi menfaatinin ve özel hayat bilgilerinin korunmasıdır.

Suçun konusu kişinin yaşamı esas alındığında özel hayatın giz alanına girenlerin tamamı, bununla birlikte özel hayatın tamamına girenlerden ise başkasının özel bir çaba göstermeden anlayamayacağı, bilgi sahibi olamayacağı alanlardır[21]. Bu yönüyle kişinin tüm hayatının özel hayat kapsamına alınmayacağı açıktır. Özel hayatın gizliliğinin korunmasında kişinin objektif açıdan bir yararının olması aynı zamanda kişinin gizlilik beklentisinin makul bir düzeyde olması gerekir[22]. Yargıtay, vermiş olduğu güncel bir kararında özel hayatı *"kişinin sadece gözlerden uzakta, başkalarıyla paylaşmadığı, kapalı kapılar ardında, dört duvar arasında-*

---

18 Mahmut Koca, İlhan Üzülmez. 'Kişisel verilerin kaydedilmesi suçu (TCK m. 135)'. (2019), (21) Prof. Dr. Durmuş TEZCAN'a Armağan, Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, 74.

19 Sırrın masuniyeti aleyhinde cürümler (mülga Türk Ceza Kanunu, Kanun Numarası: 765, Kabul Tarihi: 01.03.1926, RG 13.03.1926. Madde 195-200)

20 Oya Araslı, 'Özel Yaşamın Gizliliği Hakkı ve T.C. Anayasasında Düzenlenişi' (Yayımlanmamış doçentlik tezi, Ankara Üniversitesi 1979), 1; Ergun Özsunay *Gerçek Kişilerin Hukuki Durumu* (5. Baskı, Der Yayınları, 1982) 127.

21 Ramazan Keklik, 'Özel Hayatın Gizliliğini İhlal Suçu' (Doktora tezi, Selçuk Üniversitesi 2011), 162.

22 Nurullah Kunter, Feridun Yenisey ve Ayşe Nuhoğlu, *Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku İkinci Kitap Hüküm Verme Görevi ve Ceza Muhakemesinin Yapısı* (17. Baskı, Beta, 2010) 69.

ki yaşantısı ve mahremiyetinden ibaret değil, herkesin bilmediği veya bilmemesi gereken, istenildiğinde başka kişilere açıklanabilen, tamamen kişiye özel hayat olaylarını ve bilgilerin tamamı" şeklinde tanımlamaktadır. Bu bağlamda Yargıtay sanığın, müşterisi olduğu erkek güzellik salonunda çalışan katılan ile salonun üst katında cinsel ilişkiye girdiği sırada cep telefonuyla gizlice çekim yaparak, katılanın cinsel mahremiyetine ilişkin görüntülerini kaydetmesi biçiminde sübut bulan eylemini özel hayatın gizliliğinin ihlali kabul etmiştir[23].

Özel hayatın gizliliğinin kapsamına kişiye ait hangi detayların girdiği konusunda bir genelleme yapılamaz. Örneğin kişinin sesi ve görüntüsünün kayda alınması her zaman her şartta bu suçun oluşması için yeterli değildir. Kişiye ait hayat olayının gizlilik gerektirip gerektirmediğinin yanında başlangıçta ilgilinin iradesinin esas alınması da suçun tespiti açısından önemlidir. Görüntü ve seslerin kayda alınmasında mağdurun rızasının olması ile bir hukuka uygunluk nedeninin söz konusu olduğu durumlarda özel hayatın gizliliğinin ihlalinden bahsedilemez. Durum bu olmakla birlikte madde hükmü esas alındığında doğrudan 134. madde kapsamına kişiye ait görüntü ve ses[24], kişiye dair ancak kişisel veri niteliğinde olmayan bilgilerin ifşa edilmesi[25], kamusal alanda meydana gelen ancak kişiler açısından özel hayata ilişkin hususları barındıran durumların[26] girdiği söylenebilir[27]. Kayda alınması suç teşkil eden eylemlerin ifşasına yönelik yaygınlaştırma hareketleri de suç kapsamı içerisinde yer alır. Bir kadının mahrem görüntülerini çeken bir kişinin bu görüntüleri internet ortamında paylaşması bu suç kapsamında cezalandırılacaktır[28]. Bu sistematik, kişisel verilerin korunmasının bağımsız bir değer olarak değil, bireyin özel hayat alanının bir parçası olarak ele alındığını göstermektedir. Başka bir ifadeyle, burada amaç verilerin kendisini korumaktan ziyade, bu verilerle bağlantılı olan bireyin mahremiyetini ve kişilik alanını gü-

---

23 Yargıtay 12. Ceza Dairesi, E 2019/1, K 2019/10579, 23.10.2019.

24 Kişinin konutunda banyo yaparken şarkı söylemesi ve sesi ile görüntüsünün kaydedilmesi.

25 Kişinin cinsel tercihini bilen birinin bunu başkalarına anlatması, yaygınlaştırması faaliyeti.

26 İki kişinin bir otobüste kendi aralarında gizlice konuşmalarının konunun tarafı olmayan yabancı bir kişi tarafından dinlenilmesi.

27 Güçlü Akyürek, 'Özel Hayatın Gizliliğini İhlal Suçu' (Doktora tezi, Galatasaray Üniversitesi 2011) sayfa 200-202.

28 Sanık ... tarafından mağdur ...'nun eşinin kullanımındaki GSM hattına gönderilen mesaj içeriklerine, mağdur ...›nun eşinin facebook hesabına gönderilen mesajların yazılı olduğu internet çıktılarına, sanığa ait bilgisayarlar ile cep telefonuna ilişkin inceleme raporlarına, soruşturma evresinde düzenlenen bilirkişi raporundaki tespitlere, mağdur ... ile mağdur ...'nun eşinin birbirleriyle uyumlu beyanlarına ve dosya kapsamına göre; sanık ...›in, mağdur ... ile birlikte olduğu esnada çektiği cinsel içerikli görüntüleri, mağdur ... ile aralarındaki arkadaşlık ilişkisi sona erdikten sonra, mağdur ...›nun başka erkeklerle de cinsel yönden birlikte olduğuna dair mesajlarla birlikte mağdur ...'nun kocası olan diğer mağdur ...'ya gönderdiği anlaşılmakla… Bkz: Yargıtay 12. Ceza Dairesi, E 2017/7920, K 2018/4602 K. 18.04.2018.

vence altına almaktır.[29] Dolayısıyla korunan hukuki değer, kişisel verilerin kendisi değil; bu veriler aracılığıyla somutlaşan bireyin özel hayat hakkıdır.

Suçun faili herhangi bir kişi olabilir. Ancak suçun görüntü ve seslerin kayda alınması suretiyle işlenmesi halinde failin en azından teknolojiyi temel düzeyde kullanabilme kabiliyetine sahip olması gerekir. Mağdur açısından da özellik gerektiren bir durum söz konusu olmayıp herhangi bir kimse suçun mağduru olabilir.[30] Mağdur akli dengesi yerinde objektif, standart normal bir insan olabileceği gibi isnad kabiliyeti olmayan akıl hastası ve yaşı küçük kişiler de olabilir. Serbest hareketli suç şeklinde düzenlenmiştir. Madde metninde suçun nasıl işleneceğine ilişkin belirlenmiş kriterler ortaya konulmadığından her türlü hareketle suçun işlenmesi mümkündür.[31] Özel hayatın gizliliğinin ihlali suçunun işlenmesi için hayatın doğal akışı içerisinde hareketin icrai olabileceği akla gelse de ihmali hareketle de bu suçun işlenmesi mümkündür.

Yukarıda belirtilen örnekte R., Ahmet'in kişisel ve mesleki geçmişine dair seyahatleri, yazılım bilgisi, müşteri ilişkileri, mesleki deneyimler ve benzeri bilgileri sistematik biçimde toplamış ve sahte profiline entegre etmiştir. Bu bilgiler Ahmet'in özel hayatına dair veriler olup, onun rızası alınmadan kullanılmıştır. Özellikle ses klonlama yoluyla Ahmet'in sesinin birebir taklit edilerek video içeriklerinde kullanılması, onun kişisel ses verisinin ifşası niteliğindedir. Bununla birlikte, video veya görsel içeriğin de kullanılmış olması fiilleri Türk Ceza Kanunun 134'üncü maddesi kapsamında açıkça cezalandırılabilecek bir fiillerdir. Sonuç itibariyle R.'nin eylemi, Ahmet'in özel hayatına dair ses ve görüntülerinin rızasız ifşası niteliğinde olup, Türk Ceza Kanunu madde134/2 kapsamında iki yıldan beş yıla kadar hapis cezası ile cezalandırılır. Bununla birlikte R'nin suç teşkil eden fiili Türk Ceza Kanunu'nun 135'inci maddesinde belirtilen kişisel verilerin kaydedilmesi yönüyle de değerlendirilebilir. R., Ahmet'in çalışma geçmişi, projeleri, müşteri listeleri, seyahatleri ve yazılım kullanımı gibi kişisel mesleki verilerini rızası olmadan toplamış ve saklamıştır. Bu eylem, verilerin izinsiz kaydı anlamına gelmektedir. Kişisel verilerin açık rıza olmaksızın kaydedilmesi, bu hüküm çerçevesinde suç teşkil etmektedir. Ayrıca R'nin hukuka aykırı eylemi Türk Ceza Kanunu'nun 136'ıncı maddesinde belirtilen verileri hukuka aykırı olarak verme veya ele geçirme suçunu da oluşturmaktadır. Çünkü R., Ahmet'e ait kişisel mesleki bilgileri yalnızca kaydetmekle kalmamış, aynı zamanda sahte profilde kamuya açık şekilde paylaşmıştır. Bu, kişisel verilerin ifşası ve üçüncü kişilere aktarılması anlamına gelmektedir. Profilin kamuya açık bir freelance platformda yer alması, verilerin alenileştirilmesini ve Ahmet gibi yeni mağdurların kandırılmasına zemin hazırlamıştır. Esasında R'nin eylemi Türk Ceza Kanunun

---

29 Elif Küzeci, Kişisel Verilerin Korunması, Ankara, 2010, s. 13.

30 İmge, *Kuzgun. Türk Ceza Hukuku Açısından Mobbing.* (On İki Levha Yayıncılık, 2020) 81.

31 Zeki, Hafızoğulları ve Muharrem Özen. "Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar". Ankara Barosu Dergisi (Temmuz 2009) 17.

137'ıncı maddesinde belirtilen "belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle suçun işlenmesi hâlinde, verilecek ceza yarı oranında artırılır" hükmüne göre nitelikli hal içermektedir. Çünkü R., özel bilgileri elde ederken dijital tasarım, yazılım ve yapay zekâ araçları gibi profesyonel araçlardan ve mesleki uzmanlıktan yararlanmıştır. Bu durum, belli bir sanat ya da mesleğin sağladığı kolaylıktan yararlanılarak kişinin suç işlediğini göstermektedir.

2. Dolandırıcılık Suçu (Türk Ceza Kanunu Madde 157-158)

Dolandırıcılık suçu Türk Ceza Kanunu'nda *"hileli davranışlarla bir kimseyi aldatıp, onun veya başkasının zararına olarak, kendisine veya başkasına bir yarar sağlama"* şeklinde tanımlanmıştır. Kanunda malvarlığına karşı suçlar başlıklı 10'uncu bölümde düzenlenmiştir. Kanunun 157. maddesinde suçun temel hali, 158. maddesinde ise dolandırıcılık suçunun nitelikli hallerine yer verilmiştir. Dolandırıcılık suçunda hukuken korunan yarar esasında malvarlığının korunması şeklinde belirse de kişinin iradesini özgürce ortaya koymasını engellediğinden hukuken mağdurun irade serbestisinin korunmak istendiği de söylenebilir[32].

Dolandırıcılık suçu Kanunda genel tanımlanmıştır. Ancak özel kanunlarda kanunun düzenlenme yaptığı alana ilişkin farklı dolandırıcılık türlerini görmek mümkündür. Örneğin piyasa, kripto varlık, sigorta ve gıda dolandırıcılığı gibi özel dolandırıcılık türleriyle günlük hayatta karşılaşılabilir. Suçun unsurları açısından bakıldığında dolandırıcılık suçunun faili herhangi bir gerçek kişi olabilir. Bu yönüyle, fail açısından özellik gerektiren bir durum söz konusu değildir. Suçun faili hileli davranış ile aldatma eyleminde bulunan kişidir[33]. Menfaatin her zaman için fail tarafından sağlanması failin kim olduğunun saptanması açısından önemsizdir. Suçun mağduru aldatma eylemine uğrayan ve malvarlığı zarar gören kişidir. Mağdur herhangi bir gerçek veya tüzel kişi olabilir. Durum bu olmakla birlikte tüzel kişilerin mağdur olamayacağını savunan bir anlayış da öğretide yer almaktadır[34]. Hareket açısından bakıldığında neticesi harekete bağlı olan bir suçtur. Suç her türlü hareketle işlenebilir ancak hareketin hileli olması ve bu eylem neticesinde bir haksız menfaatin sağlanması gerekir[35]. Burada hangi icrai hareketlerle bu eylemin yerine getirilmesinden çok hareketin aldatma amacını içerip içermediği önemlidir. Hile, bir kimsenin iradesini etkileyerek onu yanılgıya

---

32 Güçlü Akyürek, Köksal Bayraktar, Vesile Sonay Evik, Ali Kemal Yıldız, Asuman Aytekin İnceoğlu, Zeynel T Kangal, Hasan Sınar, Gülşah Bostancı Bozbayındır, Ali Hakan Evik, Sinan Altunç, Barış Erman, Eylem Aksoy Retornaz ve Pınar Memiş Kartal, Özel Ceza Hukuku Cilt IV Malvarlığına Karşı Suçlar (1. Baskı, On İki Levha Yayıncılık, 2018) 252.

33 Giuliano Marini, '*Truffa' XIX Novissimo Digesto Italiano*, (1976) 864; Mahmut Koca ve İlhan Üzülmez, *Türk Ceza Hukuku Özel Hükümler* (4. Baskı, Adalet 2017) 646.

34 Osman Yaşar, Hasan Tahsin Gökcan ve Mustafa Artuç, *Yorumlu-Uygulamalı Türk Ceza Kanunu Cilt IV* (1. Baskı, Adalet, 2010).

35 Zeki Hafızoğulları ve Muharrem Özen, *Türk Ceza Hukuku Özel Hükümler Kişilere Karşı Suçlar* (6. Baskı, US-A, 2017) 406.

düşüren her türlü davranıştır. Diğer bir ifadeyle, hileli davranış; gerçeğe aykırı bir olayın gerçekmiş gibi gösterilmesi ya da gerçek bir olayın olduğundan farklı, eksik veya hiç olmamış gibi sunulmasıdır[36]. Dolandırıcılık suçunda, netice olarak mağdurun malvarlığında bir zararın meydana gelmesi söz konusudur. Ancak, bu zarar tek başına suçun oluşumu için yeterli değildir. Suçun tamamlanması açısından, mağdurun uğradığı zararın yanı sıra failin veya üçüncü bir kişinin bu durumdan bir yarar sağlamış olması da gerekir. Dolandırıcılık suçu kasten işlenebilir. Kastın suçu meydana getiren tipik hareketlerin öncesinde veya hareketlerin yapıldığı anda bulunması gerekir. Suçun olası kastla da işlenmesi mümkündür[37].

Dolandırıcılık suçunun yapay zekâ destekli sosyal mühendislik saldırıları ile işlenmesi durumu suçun nitelikli halleri arasında sayılmıştır. Zira, Dolandırıcılık suçunun "bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle" işlenmesi, Türk Ceza Kanunu madde158/1- f'de nitelikli hal sayılmıştır. Nitelikli hallere verilen cezanın suçun temel hali esas alındığında daha yüksek olması nitelikli halin cezayı ağırlaştıran bir neden olduğu da madde metninden anlaşılmaktadır. Bilişim sistemleri ile banka ve kredi kurumlarının dolandırıcılık suçunda araç olarak kullanılmasının aynı madde metninde düzenlenmesi o günün teknolojik koşullarıyla anlaşılabilmekle birlikte günümüzde bu suçun meydana gelmesi boyutuyla aralarında doğrudan bir bağlantı söz konusu değildir[38]. Bu nedenle ayrı fıkralarda düzenlenmesi kanun yapım tekniği açısından daha yerinde olacaktır.

Dolandırıcılık suçunun tespiti açısından öncelikli olarak tamamlanması gereken husus bilişim sistemleri kavramının tanımlanmasıdır. Bilişim sistemi, bir organizasyonda karar alma, koordinasyon, kontrol, analiz ve görselleştirmeyi desteklemek için bilgi toplayan, işleyen, depolayan ve dağıtan birbiriyle ilişkili bileşenlerdir[39]. Bu tür sistemler, genel amaçlı kullanım için uygun olup, otomatik

---

36 Durmuş Tezcan, Mustafa Ruhan Erdem, Rıfat Murat Önok, *Teorik ve Pratik Ceza Özel Hukuku* (15. Baskı, Seçkin, 2017) 756; Nur Centel, Hamide Zafer, Özlem Çakmut, *Kişilere Karşı İşlenen Suçlar*, (4. Baskı, Beta, 2017) Cilt I, 502-503; Veli Özer Özbek, Koray Doğan, Pınar Bacaksız, İlker Tepe, *Türk Ceza Hukuku Özel Hükümler* (12. Baskı, Seçkin, 2017) 696.

37 Nevzat Toroslu, *Ceza Hukuku Özel Kısım* (9. Baskı, Savaş 2018) 190; Doğan Soyaslan, *Ceza Hukuku, Özel Hükümler*, (10. Baskı., Ankara, 2014) 436; Hafızoğulları ve Özen (n 29) 410.

38 Madde gerekçesi "Dolandırıcılık suçunun, bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle işlenmesi de, birinci fıkranın (f) bendinde bu suçun bir nitelikli unsuru olarak kabul edilmiştir. Bilişim sistemlerinin ya da birer güven kurumu olan banka veya kredi kurumlarının araç olarak kullanılması, dolandırıcılık suçunun işlenmesi açısından önemli bir kolaylık sağlamaktadır. Banka ve kredi kurumları açısından dikkat edilmesi gereken husus, bu kurumları temsilen, bu kurumlar adına hareket eden kişilerin başkalarını kolaylıkla aldatabilmeleridir." şeklindedir. <https://www.lexpera.com.tr/mevzuat/gerekceler/turk-ceza-kanunu-madde-gerekceleri/1> Erişim Tarihi 14 Temmuz 2025.

39 Kenneth C. Laudon and Jane P. Laudon, *Management Information Systems: Managing the Digital Firm* (16th edn, Pearson 2020).

işlem kapasitesine sahip olmaları nedeniyle bilişim sistemi olarak kabul edilir[40]. Örneğin, bir kişi internet üzerinden satılık araç ilanı verip, ilgilenen kişiden banka havalesi ya da posta çeki yoluyla kapora veya satış bedelini aldıktan sonra aracı teslim etmezse, bu durumda bilişim sisteminin dolandırıcılıkta araç olarak kullanıldığı kabul edilir ve ilgili nitelikli hâl uygulanır[41].

Yargıtay ise meydana gelen olayda bilişim sisteminin araç olarak kullanılması suretiyle dolandırıcılık suçunun işlenebilmesi için aşağıda belirtilen koşulların bir arada olmasını şart görmektedir[42]. Bu şartlar a) Sanık bilişim sisteminin birden fazla bileşenini kullanmalıdır. Bilişim sisteminin kullanılması, bilişim sistemine dahil olan bileşenlerin birkaçının kullanılmasından yahut bilişim teknolojisini barındıran bir aletin kullanılmasından ibaret olmayıp, sistemi oluşturan temel bileşenlerin kullanılmasıyla oluşur. Bu bağlamda bir haberleşme cihazı olan telefon kendisi bir bilişim sistemi değildir ama; içlerinde karmaşık bilişim sistemleri barındıran uydular, santraller, baz istasyonları gibi birçok bileşenle birlikte hizmet verir. Bu nedenle içerisinde bilgisayar veya bilişim teknolojisi bulunan akıllı cep telefonlarının haberleşmede kullanılması suretiyle işlenen dolandırıcılık suçlarında, bilişim sistemi araç olarak kullanılmış olmaz. b) Mağdur bilişim sistemine güvenerek tasarrufta bulunmalıdır. Türk Ceza Kanunu'nun 158/1-f maddesinin düzenlemesinin amacı bilişim sistemine olan güvenin ihlal edilmiş olmasıdır. Örneğin internette satış yapan internet sitelerine güvenerek alışveriş yapan mağdurlar bilişim sistemine güvendikleri için dolandırılmış olurlar. Bu durumda meydana gelen suç, bilişim sistemlerinin kullanılması suretiyle dolandırıcılık suçudur. Ancak internet sitesine verilen bir ilan neticesinde mağdurun fail ile görüşüp alışveriş yapması durumunda, mağdur faille görüşerek ikna edilmekte ve dolandırılmaktadır. Bu durumda meydana gelen suç bilişim sistemine kullanılarak dolandırıcılık suçunun işlenmesi değil dolandırıcılık suçunun temel halidir. c) Sanık mağdurla karşı karşıya gelmemelidir. Bu suçun oluşmasında mağdur ve failin doğrudan birbirileriyle doğrudan iletişime geçmemiş olması gerekir. Bir başka deyişle failin bilişim sistemini, suçun işlenmesini sağlayacak hareketlerine bir peçe olarak kullanması gerekir.

Yukarıda belirtilen örnekte de R., Ahmet'in mesleki itibarını kullanarak sahte bir kimlik ve mesleki geçmiş yaratarak Ayşe'yi bu sahte profil aracılığıyla aldatmıştır. Ayşe, 20.000 Türk lirası işin %50'sini bu sahte profile güvenerek ödemiştir. Bu durum, hileli davranışla kandırma, ön ödeme yapılması suretiyle mağdurun iradesiyle malvarlığına ilişkin bir işlem yapma, paranın geri alınamaması nedeniyle zararın doğması unsurlarıyla dolandırıcılık suçunu temel halini oluşturur. Bununla birlikte Türk Ceza Kanunu madde 158/1-f'ye göre "bilişim sistemleri-

40 Koca ve Üzülmez (n 19) 810.

41 Yargıtay Ceza Genel Kurulu, E 2012/15-1293 K 2013/11, 02.04.2013.

42 Yargıtay 23. Ceza Dairesi, E 2015/7800 K 2016/7406, 08.06.2016.

nin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle" işlenen dolandırıcılık suçu, dolandırıcılık suçunun nitelikli halidir. Bu durumda R'nin oluşturduğu sahte profil, bir freelance platform aracılığıyla dijital ortamda kurulmuştur. Ses klonlama için özel bilişim araçları kullanılmıştır. Suçun mağduru Ayşe bu bilişim sistemine güvenerek Dolandırıcı R'ye ödemede bulunmuştur. Bu nedenle, Türk Ceza Kanunu madde 158/1-f kapsamında nitelikli dolandırıcılık söz konusudur.

3. Türk Ceza Kanunu madde 243-246 (Bilişim Alanında Suçlar)

Son yıllarda bilişim alanında olağanüstü bir hızla gelişmeler yaşanmış, bilişim sistemleri hem bireylerin hem de kurumların hayatında vazgeçilmez bir yer edinmiştir. Günümüzde birçok işlem bilişim sistemleri aracılığıyla gerçekleştirilmektedir. Kişisel ve kurumsal veriler bu sistemler üzerinde işlenmekte ve saklanmaktadır. Bu durum, bilişim sistemlerinde yapılan işlemlerin ve depolanan verilerin güvenliğini sağlama gereğini ortaya çıkarmıştır. Ancak verileri siber alanda korumanın neredeyse imkânsız olması bu konuyu önemli bir sorun haline getirmiştir. Bu yönüyle artık bazı geleneksel suçlar da dahil olmak üzere, bilişim sistemlerine özgü suçlar da bu ortamda işlenmeye başlamıştır. Bu gelişmeler, bilişim sistemlerinin korunmasına yönelik özel suç düzenlemeleri yapılmasını zorunlu kılmıştır[43].

Avrupa Konseyi Siber Suç Sözleşmesi'nin 2. maddesi, sözleşmeye taraf ülkelere "Yasadışı Erişim" konusunda düzenleme yapma yükümlülüğü getirmektedir. Türkiye de bu sözleşmeye taraf olduğundan Türk Ceza Kanunu'nda bu alanda düzenleme yapma yükümlülüğü ortaya çıkmıştır. Bu kapsamda Türk Ceza Kanunu'nda "Bilişim Alanında Suçlar" bölümüne yer verilmiştir. Bu bölümde farklı yıllarda değişiklikler yapılarak *"bilişim sistemine girme" (madde 243), "sistemi engelleme, bozma, verileri yok etme veya değiştirme" (madde 244), "banka veya kredi kartlarının kötüye kullanılması" (madde 245) ve "tüzel kişiler hakkında güvenlik tedbiri uygulanması" (madde 246)* suçlarına ilişkin düzenleme yapılmıştır. Bilişim suçları açısından hukuken korunan değere ilişkin farklı görüşler ortaya konulmuştur. Bu suçla hukuken korunan değer bazı hukukçulara göre mülkiyet hakkıyla birlikte fikri mülkiyetin korunmasıdır[44]. Yargıtay kararlarında korunan hukuki değer bilişim sistemi sahibinin veya kullanıcısının maddi ve manevi çıkarları olarak belirtilmiştir[45]. Ancak bir bütünlük içinde bakıldığında mülkiyet hakkı, fikri mülkiyet hakları ile kişilik haklarının da bilişim suçları kapsamında ihlal edilebileceği öngörülmelidir.

---

43 Köksal Bayraktar, Vesile Sonay Evik, Ali Kemal Yıldız, Asuman Aytekin İnceoğlu, Zeynel T Kangal, Fulya Eroğlu, Gülşah Bostancı Bozbayındır, Ali Hakan EvikEylem Aksoy Retornaz ve Pınar Memiş Kartal, Özel Ceza Hukuku Cilt VIII Ekonomi, Sanayi ve Ticarete İlişkin Suçlar ve Bilişim Alanındaki Suçlar (1. Baskı, On İki Levha Yayıncılık, 2021) 230.

44 Veli Özer Özbek vd., (n 34) 931.

45 Yargıtay 11. Ceza Dairesi, E 2009/1616, K 2009/11328, 07.10.2009.

Bu yönüyle değerlendirildiğinde daha geniş bir perspektiften asıl korunması gereken değer bilişim sistemlerinin bütünlüğü ve güvenliğidir[46].

Yapay zekâ destekli sosyal mühendislik saldırılarında sıklıkla *"bilişim sistemine girme" (madde 243), "sistemi engelleme, bozma, verileri yok etme veya değiştirme" (madde 244) ve "banka veya kredi kartlarının kötüye kullanılması" (madde 245)* suçları görülmektedir. Türk Ceza Kanunu'na göre "*bilişim sistemine girme" (madde 243)* suçunda fail açısından özellik gerektiren bir nitelik söz konusu değildir. Bu nedenle suçun faili herkes olabilir. Bu suç türünde failin kimliğinin tespiti çok önemlidir. Zira failin yanlış tespitinden kaynaklı olarak Yargıtay tarafından bozma hükmünün verildiği kararlar mevcuttur[47]. Bilişim sistemleri aracılığıyla bütünlüğü ve güvenliği ihlal edilen zarar uğrayan kişi suçun mağdurudur. Tüzel kişiler de bu suçun mağduru olabilir[48]. Eylemin tipikliği açısından bakıldığında bilişim sistemlerine kısmen veya tamamen girmek veya orada kalmak suçun meydana gelmesi açısından yeterli görülmüştür. Serbest ve seçimlik hareketli bir suçtur. Suçun oluşması açısından orada kalmaya devam etme yönüyle sistemde ne kadar süre kalınacağına ilişkin belirlenmiş bir süre yoktur. Madde hükmünde bedeli karşılığında yararlanılabilen sistemlerde suçun işlenmesi cezayı azaltan nitelikli hal kabul edilmiştir. Hareket nedeniyle verilerin değişmesi veya silinmesi, neticesi sebebiyle suçun ağırlaşmış halidir. Bu suç kasten işlenebilir. Ancak aynı madde hükmünde 243/3 açısından failinin sisteme hukuka aykırı girmesi veya orada kalması halinde istemeyerek de olsa verileri değiştirmesi veya silinmesine sebep olabileceği öngörülebilir. Bu nedenle ilgili fıkra açısından suçun taksirle işlenmesi de mümkündür.

Bu suçun farklı görünüm şekilleri vardır. Bir işyerinde bilgi teknolojisi (IT) uzmanı olarak istihdam edilen kişinin görevinin gerektirdiği sınırları aşarak verileri silmesi, değiştirmesi, kopyalaması veya bir kişinin başkasına ait e-posta adresinin şifresini kırması, hesabına izinsiz girmesi, onun adına yazışma yapması, resimlerini kopyalaması gibi durumlarda bu suçtan bahsedilir. Yargıtay'a konu olmuş bu suç türünde örnekler görmek de mümkündür[49]. Türk Ceza Kanunun 244'üncü

---

46 Mehmet Can Karagöz, *Bilişim Sistemleri Teorisine Giriş ile Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu* (1. Baskı, On İki Levha 2020) 155.

47 Nevzat Özsoy, 'Yargıtay Kararları Işığında Doğrudan Bilişim Suçları' (2019) 1(2) Yaşar Hukuk Dergisi 295.

48 Yargıtay 8. Ceza Dairesi, E 2018/2494, K 2018/2967, 19.03.2018; Yargıtay 8. Ceza Dairesi, E 2017/22781, K 2018/560, 18.01.2018.

49 *"katılana ait .....@hotmail.com internet adresine sanık tarafından şifresinin kırılması yoluyla MSN adresine girilerek kullanılamaz hale getirildiği iddiasıyla açılan davada, sanık E.A'ya ve başka kişilere ait IP numaraları ile katılanın E-Mail hesabına giriş yapıldığının tespit edildiği, bu haliyle eylemin TCK.nun 243/1. Maddesi kapsamındaki suçu oluşturacağı, ancak katılanın girişinin 04.05.2010 tarihi itibariyle engellediğini iddia etmişse de buna ilişkin bir tespite rastlanmadığının anlaşılması karşısında; anılan tarihten şikayet tarihine kadar olan dönemde, bu adresin faal olup olmadığı, katılan tarafından kendi adresine erişim sağlanıp sağlanmadığı tespit olunmamıştır. Sanık tarafından giriş yapılıp yapılmadığı, adrese ait şifrenin değiştirilip değiştirilmediği, değiştirilmişse*

maddesi bilişim sistemine hukuka aykırı müdahaleleri suç olarak düzenlemektedir. Bu suç, bir bilişim sisteminin işleyişini engelleme, bozma, verileri yok etme, değiştirme veya erişilemez kılma gibi eylemleri kapsamaktadır. Madde, bilişim sistemlerine yönelik hukuka aykırı müdahaleleri suç sayarak öncelikle bilişim sistemlerinin güvenliği, bütünlüğü ve işlerliğini koruma amacını güder; bu kapsamda hukuken korunan yarar, dijital veri güvenliği ile sistemlerin kesintisiz ve doğru çalışmasının sağlanmasıdır[50].

Suçun faili herkes olabilir; yani bu suç, herkes tarafından işlenebilen genel bir suçtur ve faillik açısından herhangi bir özel nitelik aranmaz. Mağdur ise bilişim sisteminin sahibi, kullanıcısı ya da sistem üzerinden veri sağlayan gerçek veya tüzel kişi olabilir; bu nedenle mağdur hem birey hem kurum olabilir. Failin eylemiyle mağdurun veri bütünlüğü, mahremiyeti veya ekonomik çıkarları zarar görebilir. Bu nedenle Türk Ceza Kanunun 244'üncü maddesi, aynı zamanda kişilerin haberleşme, bilgiye erişim ve kişisel veri güvenliği haklarını da dolaylı olarak koruyan bir işlev görür[51]. Suçun oluşabilmesi için failin kastla hareket etmesi, yani bilişim sistemine yönelik eylemini bilerek ve isteyerek gerçekleştirmesi gerekir. Suçun temel şekli, sistemin çalışmasını bozmaya yönelik fiillerle oluşurken, verilerin yok edilmesi, değiştirilmesi veya erişilemez hale getirilmesi gibi durumlar daha ağır cezayı gerektiren nitelikli halleri oluşturur. Bir çalışanın, eski iş yerinden ayrıldıktan sonra hâlâ elinde bulunan erişim bilgilerini kullanarak şirketin sunucularına izinsiz giriş yapması, bazı müşterilerin verilerini silmesi ya da sistemin çalışmasını engelleyecek şekilde dosya içeriklerine zarar vermesi suça örnek verilebilir.

Türk Ceza Kanunu'nun 245'inci maddesi ise başkasına ait banka veya kredi kartlarının kötüye kullanılmasını cezalandıran bir bilişim suçudur. Suçun faili herkes olabilir[52]; mağdur ise genellikle kart sahibi ya da ilgili banka kuruluşudur. Suç, üç şekilde işlenebilir: başkasına ait kartın rızasız kullanılması (TCK 245/1), kart bilgilerinin ele geçirilerek kullanılması veya başkalarına verilmesi (TCK 245/2) ile sahte kart üretimi ve kullanımı (TCK 245/3) şeklindedir. Suçun oluşa-

hangi tarihte ve hangi IP numarası ile erişim sağlandığının ilgili internet sağlayıcısından sorulmadığı anlaşılmıştır. Bu itibarla yukarıda açıklanan yöntem izlenerek eksiklikler yerine getirilip sonucuna göre tüm deliller birlikte değerlendirilip gerektiğinde bilirkişiden de görüş alınarak sanığın hukuki durumunun takdir ve tayini gerekirken eksik araştırmaya dayanarak yazılı şekilde hüküm kurulması" bkz. Yargıtay 8. Ceza Dairesi, E 2013/10402, K 2014/11836, 07.05.2014.

50 Veli Özer Özbek vd., (n 34) 945.

51 Mehmet Emin Artuk, Ahmet Gökcen ve A. Caner Yenidünya, *Ceza Hukuku Özel Hükümler* (Yenilenmiş Gözden Geçirilmiş 15. Baskı, Adalet 2015), 880-886.

52 Bu suç tipinin işlenmesi için banka ve kredi kartları hakkında temel düzeyde bilgi sahibi olunmadı gerekir. Bilişim, banka ve kredi kartı sistemleri hakkında bilgi sahibi olmayan birinin bu suçu işlemesi mümkün olamaz. Bu nedenle doktrinde bu suç türünün profesyonel suç olarak tanımlanmasının doğru olacağını savunan bilimsel görüşler de bulunmaktadır. Bkz. Jerome E. Jackson, "Fraud Masters: Professional Credit Card Criminals and Crime, Spring" (1994) 19(1) Criminal Justice Review 24, 24.

bilmesi için failin kastla hareket etmesi ve çoğu durumda maddi yarar sağlaması gerekir. Bu durumda kart sahibinin rızası bulunmadığında hukuka aykırılık unsuru tamamlanır. Bu suçla korunan hukuki yararlar arasında mülkiyet hakkı, kişisel verilerin gizliliği, finansal güvenlik ve elektronik ödeme sistemlerine olan toplumsal güven yer alır[53]. Örneğin, failin internet üzerinden yasa dışı yollarla elde ettiği bir başkasına ait kredi kartı bilgilerini kullanarak online alışveriş yapması durumunda Türk Ceza Kanunun 245/1 ve/veya 245/2 fıkraları uyarınca fail hem başkasına ait kartı kullanmak hem de bilgi temin ederek haksız kazanç sağlamak fiilinden dolayı cezalandırılabilir.

Yukarıda belirtilen örnek olay Türk Ceza Kanunu'nda yer alan bilişim suçları üzerinden ele alındığında farklı suçların işlendiği görülmektedir. Örnek olayda Ahmet'in Behance üzerinden oluşturduğu açık profiline erişmek suç değildir. Ancak özel erişim kısıtlı içeriklere, örneğin failin gizli müşteri bilgilerine ulaşması, Ahmet'e ait eserleri tahrif ederek kendi portföyünde kullanmış veya Ahmet'in orijinal çalışmalarını kamuya sahte bağlamda sunması durumunda bilişim sistemine girme (Türk Ceza Kanunu madde 243) suçunu işlediği söylenebilir. Bu durumda sistemi engelleme, bozma, verileri yok etme veya değiştirme (Türk Ceza Kanunu madde 244) suçunu işlemiştir. Son olarak Ayşe'nin yaptığı ödeme bir online platform veya banka sistemi üzerinden gerçekleştirilmiştir. Bu bağlamda Banka veya kredi kurumlarının araç olarak kullanılması suretiyle dolandırıcılık (Türk Ceza Kanunu madde 245) suçunun işlendiği de bu kapsamda değerlendirilebilir.

B. "Aldatma" Unsurunun Genişleyen Yorumu

Klasik dolandırıcılık suçlarında "aldatma", failin mağduru bilerek ve isteyerek yanıltması olarak tanımlanır. Ancak yapay zekâ teknolojilerinin sosyal mühendislik saldırılarında aktif bir rol üstlenmeye başlaması, aldatma unsurunun sınırlarını genişletmiştir. Özellikle LLM (büyük dil modeli) tabanlı sohbet robotları, deepfake teknolojileri veya otomatikleştirilmiş e-posta üreteçleri gibi araçların, insan etkileşimi olmadan mağduru ikna etmesi durumunda, "aldatma" unsurunun nasıl oluştuğu hukuki tartışmaya açıktır. Bu çerçevede sorulması gereken temel soru şudur: Mağduru aldatma fiili, yalnızca insan fail tarafından mı gerçekleştirilmeli; yoksa insanın yönlendirmesiyle çalışan bir yapay zekâ sisteminin mağduru ikna etmesi de bu unsuru karşılar mı?

Yapay Zekâ, kullanıcı tarafından manipülatif amaçlarla programlanmış veya yönlendirilmişse, fail kullanıcıdır. Örneğin, bir kişi chatbot'u bilerek mağduru yanıltacak şekilde yönlendirirse, aldatıcı eylem onun kastına bağlanır. Burada önemli olan, failin iradesiyle hareket eden bir mekanizmanın mağduru kandırmasıdır. Failin doğrudan mağdura hitap etmemesi, fakat mağdurun davranışını

[53] İzzet Özgenç, *Türk Ceza Hukuku Genel Hükümler* (14. Baskı, Seçkin 2018) 168 vd.

yönlendiren yapay sistemin fail tarafından tasarlanmış veya yönlendirilmiş olması, dolaylı aldatma kapsamında değerlendirilebilir. Hukuken esas alınması gereken nokta, mağdurun aldatılmış olması ve bunun sonucunda bir zarar doğmasıdır; bu açıdan aldatma fiilinin mutlaka insan tarafından gerçekleştirilmiş olması zorunlu değildir. Bununla birlikte, eğer yapay zekâ sisteminin tasarımı öngörülebilir biçimde aldatıcı sonuçlar doğuruyorsa, üretici veya sağlayıcıların sorumluluğu gündeme gelebilir. Ancak bu sorumluluk ceza hukuku yerine çoğunlukla tazminat hukuku kapsamında incelenir. Sonuç olarak yapay zekâ, kendi başına bir iradeye sahip olmadığı için doğrudan fail olamaz. Ancak, yapay zekânın ürettiği aldatıcı içerik ya da manipülatif eylem, onu yönlendiren veya tasarlayan kişi ya da kurumun sorumluluğuna bağlanabilir.

Yargı pratiğinde yapay zekâ destekli sosyal mühendislik saldırıları ile ilgili yerleşmiş olan sübjektif ölçütlerden biri de mağdurun algısıdır. Mağdurun yapay bir sistemle karşı karşıya olduğunu anlamaması ve bu sistemin yönlendirmesiyle irade beyanında bulunması, aldatma unsurunu oluşturmak için yeterli sayılabilir. Bu bağlamda, failin niyeti ile mağdurun algısı birlikte değerlendirilerek, yapay sistemin bir araç olarak kullanılması dolandırıcılık suçunun manevi ve maddi unsurlarının gerçekleşmesine engel teşkil etmeyecektir. Konunun daha net anlaşılması açısından şu farazi örnek olay üzerinden konuyu netleştirelim.

> *"2025 yılında, sosyal medya üzerinden yatırım tavsiyesi verdiğini iddia eden bir yapay zekâ sohbet robotu hızla yaygınlaşır. Bu bot, «kişiye özel yatırım önerileri» sunduğunu belirtmekte ve kullanıcıların portföy bilgilerine göre yönlendirmelerde bulunmaktadır. Botun arkasında R. isimli bir şahıs vardır ve bu kişi, açık kaynak bir LLM modeli kullanarak sahte bir yatırım danışmanlığı sistemi geliştirmiştir. Sistem, kullanıcılara güvenilir bir kurumun logosunu taşıyan sahte ekran görüntüleri ve geçmişte yüksek kazanç sağladığını iddia eden kullanıcı yorumları göstererek inandırıcılığını artırmaktadır. Bu inandırıcılığı arttırma işlemleri tamamen sisteme entegre edilmiş bir üretken yapay zekâ aracılığıyla yerine getirilmektedir. Ahmet, bu sistemle iletişim kurduğunda yapay zekânın kendisine sunduğu yatırım tavsiyesine inanarak 30.000 TL tutarındaki bir meblağı sistemin yönlendirdiği kripto cüzdan adresine gönderir. Ancak bir süre sonra iletişim kesilir ve gönderilen paranın iade edilmediği anlaşılır. Soruşturma sonucunda sistemin arkasında R.'nin olduğu tespit edilir."*

Bu durumda, R.'nin doğrudan Ahmet ile iletişim kurmamış olması, aldatma unsurunu ortadan kaldırmaz. Çünkü R., mağduru yanıltmak amacıyla bir yapay sistem geliştirmiş, bu sistemin mağdurun iradesini etkileyecek şekilde davranmasını sağlamış ve böylece klasik dolandırıcılığın araçlarını yapay zekâ aracılığıyla çoğaltmıştır. Mağdurun algısında gerçek bir yatırım danışmanı izlenimi oluşmuş ve karar verme süreci bu algıya dayanmıştır. Bu nedenle, aldatma fiili mağdur

nezdinde gerçekleşmiş, failin dolaylı eylemiyle dolandırıcılık suçu oluşmuştur. Türk Ceza Kanunu'nun 158. maddesinin 1. fıkrasının (f) bendine göre: Olayda:

- Bilişim sistemi, fail tarafından yapılandırılan yapay zekâ destekli sohbet robotudur.
- Bu sistem, mağdurun aldatılmasında doğrudan araç olarak kullanılmıştır.
- Mağdurun iradesi, sistemin sunduğu sahte bilgi ve belgelerle etkilenmiş ve maddi bir zarara neden olacak şekilde yönlendirilmiştir.
- Fail, sistemin arkasında olup doğrudan iletişim kurmasa da failin iradesiyle çalışan bir mekanizma, dolaylı aldatma aracı olarak işlev görmüştür.

Bu nedenle, Türk Ceza Kanunu 158/1-f hükmü uyarınca nitelikli dolandırıcılık suçu oluşmuştur. Failin yapay sistemi kendi yararına kullanarak mağdurun malvarlığına yönelik hileli işlem gerçekleştirmesi suçun hem maddi hem manevi unsurlarını karşılamaktadır.

III. YAPAY ZEKÂNIN CEZA HUKUKU BAĞLAMINDA ROLÜ

Yapay zekâ suçun tespiti veya suça verilecek cezanın belirlenmesi konularında sıklıkla kullanılmaktadır. Ancak, yapay zekâ suç işleyebilir mi veya suçun işlenmesine aracılık edebilir mi? benzeri sorular da yakın dönemde yapay zekâ alanında yaygın karşımıza çıkmaktadır. Yapay zekânın günlük yaşamda ilk kitlesel uygulaması otonom araçların kullanımıdır. Özellikle ulaşımı önemli ölçüde etkileyecek otonom araçlara ilişkin uygulamanın ortaya çıkışı, kanunlarla yoğun bir şekilde düzenlenmesi gereken bir müdahale alanı oluşturmaktadır. Çünkü yapay zekanın ana aktör olduğu bu tür yenilikler ceza hukukunu içeren nitelikte olayın nasıl yorumlanacağını ve uygulanacağını etkileyecek sonuçlar doğuracaktır. Dahası, kişilik, zarar ve suçlama gibi geleneksel ceza hukuku kavramlarını yeniden ele almak ve bunlar üzerinde düşünmek için paha biçilmez bir fırsat ortaya koymaktadır. Çünkü bu uygulama, tanımlanan geleneksel faillik yelpazesine yeni bir faillik durumu eklemektedir. Bu noktada, yapay zekanın suç oluşturan eylemlerinden kim sorumludur veya yapay zekâ suçun işlenmesinde araç olarak kullanılmışsa faillik durumu nasıl ele alınmalıdır? konuları önemli sorunlar olarak karşımızda durmaktadır.

Öncelikle cevaplandırılması gereken soru yapay zekâ fail olabilir mi? Fail olmanın şartları nelerdir? Bir yapay zekâ aracı failliğin gerektirdiği tüm şartları sağlayabilir mi? Türk Ceza Kanunu'nun 20'nci maddesi faillik açısından temel bir kriter getirmiştir. Ceza sorumluluğunun şahsi olduğunu ve kimsenin başkasının fiilinden sorumlu olmayacağını açık, seçik ve net bir şekilde ortaya koymuştur. Madde hükmünden sadece gerçek kişilerin fail olabileceği anlaşılmaktadır. Ceza sorumluluğu tüzel kişilere uygulanmaz. Yapay zekanın insana özgü bilişsel kabiliyetler ortaya koyması hatta bazı konularda insanlardan çok daha iyi sonuçlar üretmesi tek başına onu gerçek bir hukuk öznesi konumuna ulaştırır mı? Yapay

zekanın hukuki statüsü nedir? Yapay zekanın hukuki statüsüne ilişkin iki farklı bilimsel görüş yaygın savunulmaktadır[54]. Yapay zekanın hukukun öznesi olduğunu savunanlar ile yapay zekâ hakka konu bir nesnedir görüşünü savunanlar. Faillik açısından değerlendirme yapıldığından yapay zekanın hakka konu nesne olduğu görüşü yaygın kabul edilmektedir. Gerçek kişiliğin tam ve sağ doğmak, hak ve borçlara ehil olabilme, medeni hakları kullanabilme yetisine sahip olmayı gerektirmesi yapay zekayı gerçek kişilik kavramının dışına itmektedir. Bununla birlikte, bir alternatif olarak yapay zekaya kişilik tanımlaması yapılması konusunda girişimler bulunmaktadır[55] ancak hukuk sistemlerince yapay zekanın hangi tür kişiliğe karşılık geldiği konusunda net bir hüküm bulunmamaktadır. Yapay zekâ, insan benzeri yetilere sahip olsa da insan değildir. Bu nedenle bazı yazarlar ne gerçek kişi ne de tüzel kişi olmayan, tamamen yapay zekâya özgü bir hukuki kişilik statüsü geliştirilmesini önermektedir. Bu kişilik statüsünün kapsamı ve içeriği, teknolojik gelişmelere paralel olarak zamanla şekillenecektir[56].

Ceza hukukunda fail, suçun maddi ve manevi unsurlarını gerçekleştiren kişidir. Yapay zekâ sistemlerinin ise irade, kast ve taksir yeteneği bulunmadığından cezai sorumlulukları yoktur. Çünkü, yapay zekanın bilinç ve iradesi yoktur. Hareketi başlatacak ve üzerinde egemenlik sağlayabilecek bir yapıya sahip değildir. Yapay zekâ hakkında kusur ilkesi de uygulanamaz. Ceza hukukunda kusur, failin cezalandırılabilirliği için temel bir unsurdur. Kusurun varlığı için üç temel koşul aranmaktadır: kusur yeteneği, haksızlık bilinci ve mazeret nedenlerinin yokluğu[57]. Kusur yeteneği, algılama ve irade yetisini içerir. Ancak yapay zekânın bu koşulları sağlayıp sağlayamayacağı tartışmalıdır. Dolayısıyla yapay zekâ, bir suçun faili olamaz; ancak suçun işlenmesinde kullanılan bir araç olabilir. Bu durumda, asıl odak yapay zekayı kullanan veya yönlendiren kişinin fiilidir. Yapay zekâ destekli saldırılarda failin belirlenmesinde bir takım değerlendirme kriterleri kullanılabilir. Bu kriterler failin faillik derecesinin belirlenmesi açısından önemlidir. Örneğin suçun işlenmesinde kullanılan yapay zekâ sistemini kim yönetmektedir? Suçun meydana gelmesine sebep olan hareketi başlatan kimdir? Yapay zekânın yerine getirdiği saldırı öngörülebilir bir saldırı mıdır? Kimi görüşler, kusur için irade özgürlüğünün şart olmadığını, fiilin hukuki anlam ve sonuçlarını değerlendirme yeterliliğinin yeterli olabileceğini savunur. Bu bağlamda, yapay zekâ belirli koşulları sağladığında kusur sorumluluğu yüklenebileceği ileri sürülmektedir. Bir başka deyişle yapay zekâ komutu aldıktan sonra insan müdahalesinin dışında kendisi özerk hareket edebilir. İşte böyle bir durumda eğer insan müdahalesi dı-

---

54 Berat *Çamlıca, Yapay Zekânın Ceza Sorumluluğu ve Kişilik Tartışmaları* (1. Baskı, Yetkin 2022) 52.

55 Berrin Akbulut, 'Yapay Zekâ ve Ceza Hukuku Sorumluluğu'(2023) 27(4) Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi 267.

56 ibid 287.

57 İzzet Özgenç, *Türk Ceza Hukuku Genel Hükümler* (18. Baskı, Seçkin 2022) 458-459.

şında bir durum sergiliyorsa yapay zekâ, failin sorumluluğunu sınırlandırılabilir[58]. Ayrıca, yapay zekânın oluşum aşamasında failin sahip olduğu iradenin içeriği de faillik açısından önemli olabilir. Şöyle ki yapay zekâ yazılımının özel olarak suç işlemek üzere tasarlanıp tasarlanmadığı bu noktada önemlidir. Bu tür bir durumda yapay zekâ kullanıcısının dışında yapay zekâ geliştiricisi veya yapay zekâyı kullanıcıya sağlayan kişi de "yardım eden" ya da "azmettiren" olabilir.

Sonuç itibariyle ceza hukuku, her ne kadar "fail=insan" ilkesini sürdürse de, yapay zekâ sistemlerinin rolü arttıkça yardım etme, azmettirme, dolaylı faillik ve taksirli sorumluluk gibi kavramlar genişletilerek suç dosyalarına uygulanabilir.

Durumu senaryo bazlı ele aldığımızda aşağıda belirtildiği şekilde muhtemel bir tablo ortaya çıkabilir.

Örnek Olay	**Faillik Durumu**	**Hukuki Nitelendirme**
2025 yılında, sosyal medya üzerinden yatırım tavsiyesi verdiğini iddia eden bir yapay zekâ sohbet robotu hızla yaygınlaşır. Bu bot, "kişiye özel yatırım önerileri" sunduğunu belirtmekte ve kullanıcıların portföy bilgilerine göre yönlendirmelerde bulunmaktadır. Botun arkasında R. isimli bir şahıs vardır	R örnek olayda yapay zekâ sohbet robotunu harekete geçirecek komutu veren kişi	Bu örnek olayda R doğrudan fail konumundadır.
Üretken yapay zekânın kullanıcılara güvenilir bir kurumun logosunu taşıyan sahte ekran görüntüleri ve geçmişte yüksek kazanç sağladığını iddia eden kullanıcı yorumları göstererek inandırıcılığını arttırması.	Üretken yapay zekânın belli periyodlarla sistem güncellemelerinin yapılması gerekirken ihmal ile gereklilikler yerine getirilmemişse geliştirici veya sistem yöneticisi	Bu durumda faillik durumuna göre gözetim yükümlülüğünün ihmali nedeniyle taksirle sorumluluk veya ihmali hareketle işlenen suç söz konusu olabilir.
Güvenilir bir kurumun logosunu taşıyan sahte ekran görüntüleri ve geçmişte yüksek kazanç sağladığını iddia eden kullanıcı yorumlarını üreten yapay zeka'nın bu suç potansiyeli bilinen bir platformda açık kaynak kodlu paylaştırılırsa	Üretken yapay zekâyı tasarlayan ve suç işleme konusunda kişileri yönlendiren yazılımcı veya kodu 3. kişilerle paylaşarak onların suç işlemesini kolaylaştıran dağıtıcı/aracı	Bu durumda faillik durumuna göre yardım eden, azmettirici veya dolaylı faillik tartışılabilir.

[58] Sabine Gless and Thomas Weigend 'Intelligente Agenten und das Strafrecht' (2014) 126(3) Zeitschrift für die gesamte Strafrechtswissenschaft, 561.

Örnek Olay	Faillik Durumu	Hukuki Nitelendirme
Güvenilir bir kurumun logosunu taşıyan sahte ekran görüntüleri ve geçmişte yüksek kazanç sağladığını iddia eden kullanıcı yorumlarını üreten yapay zekânın bu eyleminin tasarlama aşamasında değil de yapay zekâ sistemine virüs yükleyen bir hacker tarafından eğitilmesi ile sistemi suistimal etmesi	Bu durumda fail yapay zekâyı suç işleme konusunda eğiten Hacker	Failliğin sonradan değişmesi söz konusu olacaktır.

Sonuç olarak, Yapay zekânın ceza hukuku bakımından konumu, yalnızca "fail olabilir mi?" sorusu üzerinden ele alınamaz; aynı zamanda failin kim olduğu, sorumluluk derecesi ve kusur yeteneği gibi klasik kurumların da yeniden yorumlanmasını zorunlu kılar. Mevcut hukuk düzeninde, yapay zekânın insan benzeri bilişsel ve iradi unsurlardan yoksun olması nedeniyle doğrudan fail olarak sorumluluğu mümkün görünmemektedir. Bununla birlikte, yapay zekânın suçun işlenmesinde araç olarak kullanılması, geliştirici, kullanıcı veya üçüncü kişilerin faillik, azmettirme, yardım etme veya ihmali davranışla sorumluluk türleri altında değerlendirilmesine olanak tanımaktadır.

IV. ULUSLARARASI YAKLAŞIMLAR VE KARŞILAŞTIRMALI HUKUK

Yapay zekâ destekli sosyal mühendislik saldırılarını ceza hukuku perspektifinden ele alan uluslararası yaklaşımlar Türkiye'deki tartışma konularına benzer içerikler ortaya koymaktadır. Bu yönüyle uluslararası düzeyde ceza hukuku açısından değerlendirilen temel sorunlar şunlardır. Öncelikle, otomatik sistemleri içeren suçlarda faili tespit etmek oldukça karmaşık ve zordur. Bununla birlikte otomatik sistemlerin suçun işlenmesini kolaylaştırması, yapay zekanın aldatma, hileli davranışlarla mağduru ikna etmesi, kast ve zarar gibi unsurlar yapay zekanın kullanımıyla yeniden yorumlanmaktadır. Diğer bir tartışılan sorun ise yapay zekanın hukuki statüsüne yöneliktir. Yapay zekâ sisteminin suçta araç mı yoksa bağımsız sorumluluk sahibi özne mi sayılacağı ülkeden ülkeye farklılık göstermektedir.

Yapay zekâ destekli sosyal mühendislik saldırıları, Avrupa Birliği'nde ceza hukuku perspektifinden hem mevcut suç tipleri hem de yeni teknolojilere uyumlu düzenlemeler ışığında tartışılmaktadır. AB, yapay zekâ destekli sosyal mühendislik saldırılarına ceza düzenlemelerinde doğrudan yer vermemiştir. Ancak üye devletlerin ceza politikalarını şekillendiren çerçeve direktifler, Yapay Zekâ Tüzüğü (AI Act), Genel Veri Koruma Tüzüğü (GDPR), Ağ ve Bilgi Sistemlerinin Güvenliği Direktifi (Network and Information Systems Directive (NIS)) gibi düzenlemeler yoluyla üye ülkelerin iç hukuk sistemleri üzerinde önemli bir etki meydana

getirmektedir. Bu düzenlemeler siber suçlar, kişisel verilerin korunması, ağ ve bilgi sistemlerine yönelik saldırılar, insan haysiyetine yönelik içeriklerin üretimi (örneğin deepfake) gibi başlıklarda ortak standartlar belirlemektedir.[59]

AB Yapay Zekâ Tüzüğü (AI Act), doğrudan ceza hukukuna ilişkin bir tüzük olmamakla birlikte, suçun önlenmesi açısından geliştirici ve dağıtıcılara önemli yükümlülükler getirmektedir. Özellikle "yüksek riskli sistemler" kategorisine giren ve insan davranışını manipüle eden sistemlerin pazarlanması, AB Yapay Zekâ Tüzüğü madde 5/1-a uyarınca yasaktır[60]. Geliştirici, sistemin dolandırıcılık amacıyla kötüye kullanılmasını engelleyecek filtreleri koymak zorundadır. Platform sağlayıcısı, suç işleyen uygulamaların barındırılmasını engellemelidir. Bu tür sistemlerin geliştirilmesi, dağıtılması veya kasten kullanılmasının engellenmemesi hâlinde Geliştirici, eylemiyle suçun hazırlayıcısı veya yardımcısı olabilir. Platform sağlayıcısı, denetim yükümlülüğünü yerine getirmediği için taksirle suça iştirak hükümlerinden sorumlu tutulabilir. Sözleşmeye bağlı olmayan hukuki sorumluluk kurallarının yapay zekaya uyarlanmasına ilişkin bir "Yapay Zekâ Sorumluluk Direktifi" de bulunmaktadır[61]. Direktif şunları hedeflemektedir; iç pazarın işleyişini iyileştirmek, insan merkezli güvenilir yapay zekâ kullanımını teşvik etmek, demokrasi, hukukun üstünlüğü ve çevre koruma da dahil olmak üzere sağlık, güvenlik, temel haklar gibi unsurların yüksek düzeyde korunmasını sağlamak, Avrupa Birliği'nde yapay zekâ sistemlerinin zararlı etkilerine karşı koruma sağlamak ve inovasyonu desteklemek. Bu bağlamda, getirdiği yasaklar ve sözde yüksek riskli yapay zekâ sistemlerinin geliştirilmesi için ortaya koyduğu gereklilikler, kullanıcılar için riskleri ve zararları önlemeyi amaçlamaktadır. Yapay Zekâ Sorumluluk Direktifi, yapay zekâ sistemlerinin neden olduğu zararlara ve zarar gören kişinin medeni hukuk açısından tazmin edilmesi gerekliliğine odaklanmıştır[62]. Bu bağlamda AB Yapay Zekâ Tüzüğü ve Sorumluluk Direktifi doğrudan ceza normu koymamaktadır ancak yükümlülüklerin ihlali ulusal hukuk-

---

59 European Parliament, *Understanding cybercrime* (EPRS Briefing, 2024) <https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/760356/EPRS_BRI%282024%29760356_EN.pdf> Erişim Tarihi 25 Haziran 2025; Laura Bartoli, 'Cybersecurity and the Fight against Cybercrime: Partners or Competitors?' (2020) *European Journal of Risk Regulation* https://www.cambridge.org/core/journals/european-<journal-of-risk-regulation/article/cybersecurity-and-the-fight-against-cybercrime-partners-or-competitors/80A53F6CED87BA65B100E7A03B00DC16> Erişim Tarihi 25 Haziran 2025.

60 European Parliament and Council, 'Regulation (EU) 2024/1689 on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)' [2024] OJ L212/1. <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng> Erişim Tarihi 25 Haziran 2025.

61 European Commission, Proposal for a Regulation of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive) (COM (2022) 496 final). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0496> Erişim Tarihi 25 Haziran 2025.

62 Athina Sachoulidou 'AI Systems and Criminal Liability A Call for Action' (2024) 11(1) Oslo Law Review 1,2.

ta cezaî sonuçlar doğurabilmektedir. Sonuç olarak, AB Yapay Zekâ Tüzüğü, her ne kadar ceza sorumluluğunu doğrudan düzenlemese de suçun önlenmesine dair önemli yükümlülüklerle ceza hukukuna dolaylı etkide bulunmaktadır. Bununla birlikte AB Genel Veri Koruma Tüzüğü de yapay zekanın cezai sorumluluğunu doğrudan düzenlemez. Yapay zekâ sistemlerinin veri toplama, işleme, şeffaflık ve otomatik karar verme boyutunu sıkı biçimde sınırlayan hükümler içerir. Tüzük genel itibariyle kişisel veriye odaklıdır; Yapay Zekâ Tüzüğü ise kullanılacak teknolojinin düzeyine ve yapısına odaklanmaktadır. Ancak her iki tüzüğün hükümleri de birlikte uygulanır. Yüksek riskli bir yapay zekâ sistemi hem AB Yapay Zekâ Tüzüğünün teknik ve organizasyonel yükümlülüklerini hem de Veri Koruma Tüzüğünün veri işleme sınırlamalarını karşılamak zorundadır. Örneğin bir banka yüksek riskli bir yapay zekâ sistemi ile işe alım süreçlerini yerine getirirse hem de Genel Veri Koruma Tüzüğüne göre otomatik karar yasağı ihlali yaparsa iki düzenleme uyarınca da ayrı ayrı ceza alabilir.

2024 yılında Amerikan toplumu, sosyal mühendislik saldırıları ve diğer dolandırıcılıklar nedeniyle 12,5 milyar ABD doları kaybetmiştir[63]. Daha fazla dolandırıcı, daha kısa sürede, daha fazla dilde, daha ikna edici kimlik avı mesajları oluşturmak için üretken yapay zekayı kullandıkça bu sayı artması da mümkündür. ABD'de yapay zekânın cezai sorumluluğu konusu şu anda hukuken doğrudan tanınmış bir kavram değil, ancak doktrinde ve bazı mahkeme kararlarında dolaylı tartışmalara konu olmaktadır. Mevcut durumda yapay zekâ, ceza hukuku anlamında "kişi" sayılmadığı için kendi başına fail olarak sorumlu tutulmamaktadır. Sorumluluk, yapay zekâyı geliştiren, işleten, eğiten veya kullanan gerçek veya tüzel kişilere yüklenmektedir. Kişilerin sorumlu tutulabilmesi için savcıların kast (mens rea) veya taksir ile fiil (actus reus) unsurunu makul şüphenin ötesinde ispatlaması gerekir. Örneğin 2018 tarihinde bir Uber aracı Arizona'da bir yayaya çarparak ölümüne sebep olmuştur. Araç yarı-otonom bir araç olup operatör sürücü yola bakmadığı için "taksirle adam öldürme" suçundan hakkında dava açılmıştır[64]. ABD'de otonom araç kazalarında ceza sorumluluğu araçların otonom düzeyine göre değişebilmektedir[65]. ABD'de diğer ülke örneklerine benzer olarak meydana

---

63 Federal Trade Commission 'New FTC Data Show a Big Jump in Reported Losses to Fraud to $12.5 Billion in 2024' (Federal Trade Commission, 10 March 2025) <https://www.ftc.gov/news-events/news/press-releases/2025/03/new-ftc-data-show-big-jump-reported-losses-fraud-125-billion-2024> Erişim Tarihi 3 Temmuz 2025.

64 National Transportation Safety Board, *Highway Accident Report- Collision Between Vehicle Controlled by Developmental Automated Driving System and Pedestrian Tempe, Arizona* (NTSB, 19 November 2019) <https://www.ntsb.gov/investigations/accidentreports/reports/har1903.pdf> Erişim Tarihi 8 Ağustos 2025.

65 Ceza hukukunda sorumluluğun kime ait olduğu, otomasyon seviyesine bağlıdır; bu ayrım hukukî analizlerde kilit rol oynar. Level 0-2: Araç hâlâ sürücü odaklıdır. Sürücü, tüm sürüş ve gözetim görevlerinden sorumludur (örneğin sürücünün dikkatinden kaynaklanan "taksirle öldürme" gibi kazalarda), Level 3: Burada sistem sürüşü yapar ama "gerekirse müdahale et" yükümlülüğü sürücüde kalır. Sürücü, sistem uyarı verdiğinde reaksiyon göstermediğinde cezaî sorumlu tutulabilir. Level

gelen maddi ve manevi zarar ile ölümlerden kişiler sorumlu tutulmaktadır. Bir başka deyişle yapay zekanın cezai sorumluluğu yoktur. Bununla birlikte meydana gelen her kazadan kişiler de sorumlu tutulmamaktadır. Meydana gelen olayın somut özelliklerine göre araç operatörü ile araç üreticisi, yazılım geliştiriciler, filo işletmecileri ve hizmet sağlayıcılar ile kamusal otoritelerin sorumlu olması mümkündür. ABD'de yapay zekaya ilişkin yapılan hukuki düzenlemeler Avrupa Birliği'ne göre yetersizdir. ABD'de federal düzeyde yapay zekanın cezai sorumluluğunu düzenleyen müstakil bir düzenleme bulunmamaktadır[66]. Federal düzeyde düzenleme yaklaşımı, sektörel rehberlik, yönergeler ve başkanlık emirleriyle yürütülmektedir. Ancak eyaletler düzeyinde birtakım girişimler bulunmaktadır[67].

V. TÜRK CEZA HUKUKU AÇISINDAN BOŞLUKLAR VE DEĞERLENDİRME

Yapay zekâ destekli sosyal mühendislik saldırıları bakımından Türk Ceza Hukuku'ndaki boşluklar hem normatiflik açısından hem de pratikte söz konusu olabilmektedir. Normatifliğe ilişkin Türk Ceza Kanunu'nun suç türlerini düzenleyen ilgili madde hükümlerinde yapay zekaya yer verilmemiştir. Suça ilişkin yapay zekâ alanını düzenleyen bir müstakil madde hükmü bulunmamaktadır. Çünkü Türk Ceza Kanunu'nda yer alan suç tipleri yoruma açıktır ve suçluluğun belirlenmesi insan fail varsayımı üzerinden kurgulanmıştır. Bu nedenle Türk Ceza Kanunu'nda yapay zekâ doğrudan fail olarak tanımlanmamıştır ancak kanunda düzenlenen Malvarlığına Karşı Suçlar, Bilişim Alanında Suçlar, Özel Hayata ve Kişisel Verilere Karşı Suçlar, Kamu Güvenine Karşı Suçlar, Kamu Barışına Karşı Suçlar, Şerefe Karşı Suçlar, Terör ve Örgütlü Suçlar Kapsamında yapay zekanın araç olarak pek çok suçun işlenmesinde doğrudan veya dolaylı kullanılabilmesi mümkündür. Bununla birlikte yapay zekanın saldırıların hangi aşamasında etkili olduğu, bu etkiyi ortaya çıkaran gücün kim olduğuna bağlı olarak fail değişebilecektir. Çünkü yapay zekâ yazılımını geliştiren, yapay zekayı suç işleme konusunda eğiten, yapay zekayı belli bir suçu işlemek için kullanan veya güvenilir yapay zekayı bir sosyal mühendislik saldırısına entegre eden farklı aktörler olabilir. Türk Ceza Kanunu'nda ilgili suç türlerinde yapay zekaya atıf yapan suçun nitelikli hallerine de yer verilmemiştir.

4-5: Sistemin özerk davranması nedeniyle sürücü devreden çıkar. Bu durumda cezaî sorumluluk genellikle üretici, yazılım geliştiren veya filo işletmecisi gibi insan/tüzel kişilere yönelir. Bu sorumluluğun dayanağı ceza hukuku kapsamında *taksir*, *tehlikeye sebebiyet vermek* ya da *taksirle öldürme* olabilir. National Highway Traffic Safety Administration, 'Automated Vehicles for Safety' <https://www.nhtsa.gov/vehicle-safety/automated-vehicles-safety?> Erişim Tarihi 8 Ağustos 2025.

66 Council on Criminal Justice, 'The Implications of AI for Criminal Justice' (*CCJ*, October 2024) <https://councilоncj.org/the-implications-of-ai-for-criminal-justice/> Erişim Tarihi 12 Ağustos 2025.

67 Amanda OKeefe, 'Navigating AI Laws And Regulations Across Practice Areas' (*Thomson Reuters,* 28 Temmuz 2025) <https://legal.thomsonreuters.com/blog/navigating-ai-laws-and-regulations-across-practice-areas/> Erişim Tarihi 18 Ağustos 2025.

Yapay zekaya uygulanacak yaptırımın ne olacağı da diğer önemli bir sorun alanıdır. Türk Ceza Kanunu'nda yaptırımlar başlığı altında hapis, adli para cezası ve güvenlik tedbirlerine yer verilmiştir. Ceza insanlar tarafından uygulanır ve cezaya mahkûm edilen de insandır. Elektrik tesisatında meydana gelen bir kaçaktan dolayı zarar gören mağdura karşı sorumluluk elektrik tesisatında değil, tesisatın sorumluluğunu üstlenmiş kişidedir. Yapay zekâ açısından da aynı şeyler tekrarlanabilir. Yapay zekâ bir insan değildir, iradesi yoktur, kusur ehliyeti yoktur ve objektif isnadiyetin öznesi olamaz. Bu bakımdan yapay zekâ doğrudan cezalandırılamaz. Ancak yeni bir yasal düzenlemeyle yeni ceza türlerinin kanuna eklenmesi ve yapay zekanın failliğinin de hukuken kabul edilmesi durumunda sistemin kapatılması, lisans iptali, idari para cezası benzeri cezalar gündeme gelebilir. Türk Ceza Kanunu'nda mevcut suç türleri yapay zekâ destekli suçların tanımlanmasında yetersiz kalabilmektedir. Kanunda veri manipülasyonu, algoritmik ayrımcılık, özerk sistemlerin kötüye kullanımı şeklinde tanımlanmış yeni suç tipleri bulunmamaktadır. Suçun tespitinde mevcut suç tipleri üzerinden hareket edilerek yapay zekanın suçun oluşumundaki rolü ortaya konulmaktadır.

Türk Ceza Kanunu'nda yapay zekaya bağlı olarak yeni suç tiplerinin geliştirilmesinin gerekli olup olmadığı tartışması güncel bir konudur. Mevcut durumda yapay zekanın suçun işlenmesindeki rolü ve cezai sorumluluğuna ilişkin kanuna eklenen hüküm bulunmamaktadır. Bununla birlikte bu duruma ilişkin birtakım hukuki çözüm önerileri de ortaya konulmaktadır. Bir görüş yapay zekanın mevcut ve gelecekte yaratacağı tehlikelilik durumuna göre yeni suç tiplerinin tanımlanması gerektiğini dile getirmektedir. Karşıt görüş ise Türk Ceza Kanunu'nda tipiklik ilkesinin geçerli olduğunu, kanunun genişletici yoruma izin vermediğini, yapay zekanın etkilediği çokça suç tipinin olduğunu bu nedenle her teknolojik gelişmeyle ortaya çıkan yeni teknolojilere bağlı suç tipleri oluşturmanın sakıncalı olduğunu belirtmektedir. Bu iki görüşün aksine orta yolu benimseyenler ise bazı alanlarda özel suç tiplerinin tanımlanabileceğini ancak tamamen yeni müstakil suçlar tanımlamak yerine mevcut suç tiplerinin yapay zekâ ile işlenmesi halinde nitelikli hallerin öngörülmesinin daha yerinde olacağını savunmaktadır.

SONUÇ ve ÖNERİ

Yapay zekâ destekli sosyal mühendislik saldırıları, klasik dolandırıcılık ve bilişim suçlarından çok daha karmaşık, sınır ötesi ve tespit edilmesi güç bir yapı ortaya koymaktadır. Ses klonlama, deepfake, otomatik oltalama ve benzeri yöntemler, yalnızca bireylerin malvarlığı ve kişisel verileri üzerinde değil, aynı zamanda demokratik düzen, kamu güvenliği ve adalet sisteminin işleyişi üzerinde de ciddi tehditler doğurmaktadır. Teknoloji henüz yapay zekâ destekli yasadışı faaliyetlerin suç alanında hakimiyet kurduğu bir aşamaya ulaşmamış olsa da yapay zekâ teknolojisinin izlediği yol acil ve önleyici eylem ihtiyacını vurgulamaktadır.

Türk Ceza Kanunu'nda mevcut düzenlemeler (Türk Ceza Kanunu madde 157-158, madde 134, madde 243-245 ve diğer ilgili hükümler) belirli ölçüde yapay zekâ destekli saldırıların cezalandırılmasına imkân verse de, bu saldırıların özgün yapısı karşısında bu hükümler yetersiz kalmaktadır. Özellikle "aldatma" unsurunun genişleyen yorumu, yapay zekânın fail değil araç konumunda olduğu durumlar, kişisel verilerin sistematik olarak işlenmesi ve dijital delillerin güvenilirliği konularında ciddi boşluklar bulunmaktadır. Bu bağlamda, ceza hukukunda fail, iştirak, kusur ve kast kavramlarının yeniden yorumlanması ve yapay zekânın aracılık ettiği suçlarda özel düzenlemelerin yapılması tartışma konusudur.

Uluslararası alanda Avrupa Birliği'nin AI Act ve GDPR gibi düzenlemeleri, yapay zekâ sistemlerinin kötüye kullanımını önleme bakımından önemli örnekler sunmaktadır. Ancak bu düzenlemeler daha çok idari ve özel hukuk sorumluluğuna odaklanmakta; ceza hukuku boyutunda doğrudan ve kapsamlı bir çözüm üretmemektedir. ABD ve diğer hukuk sistemlerinde de benzer şekilde yapay zekânın bağımsız fail olarak tanınmadığı, ancak geliştirici, kullanıcı veya sağlayıcıların sorumluluğuna gidildiği görülmektedir.

Sonuç olarak, yapay zekânın ceza hukuku bağlamındaki rolü yalnızca mevcut suç tiplerine uyarlanarak çözülemeyecek kadar kapsamlıdır. Kanun koyucu "yapay zekâ destekli dolandırıcılık", "sosyal mühendislik ile işlenen suçlar" gibi özel suç tipleri ihdas edebilir. Hukuk uygulayıcıları için daha öngörülebilir ve somut normlar yaratılabilir. Böylelikle failin hangi davranışının suç oluşturduğu, hangi nitelikli hâle girdiği daha kolay belirlenebilir. Teknolojiye özgü tipik saldırı biçimleri doğrudan kanunda tanımlanarak belirlilik ilkesi güçlendirilebilir. Ancak bu yöntem aynı zamanda aşırı tipikleşme tehlikesi doğurabilir. Bu durumda teknoloji geliştikçe sürekli kanunu değiştirme ihtiyacı ortaya çıkabilir.

Türk Ceza Kanunun Genel Hükümler bölümüne yapay zekaya dair genel bir norm eklemek sorunun çözümü için yeterlidir. Bu hükmün ihdası ile

- Tüm suç tiplerine genel ve kapsayıcı bir şemsiye norm eklenmiş olur.
- Yasa koyucunun her yeni teknolojik gelişme için ayrı suç tipi ihdas etmesine gerek kalmaz.
- Türk Ceza Kanunu'nun sistematiği korunarak teknoloji odaklı nötr bir düzenleme yapılmış olur.
- Belirlilik ilkesi zarar görmeden, mevcut suç tipleriyle bağ kurularak ceza uygulaması açısından pratiklik sağlanmış olur.

Genel Hükümlere Eklenecek Çerçeve Madde Türk Ceza Kanunu madde 20'den sonrasına eklenebilir. Bu madde yapay zekanın gelişmişlik düzeyini ve suça sebep olma, araç olma durumlarını karşılama açısından yeterlidir. Ancak yapay zekâ teknolojilerindeki gelişmeye bağlı olarak madde sonradan yeniden düzenlenebilir.

> *Madde 20 – Ceza sorumluluğunun şahsiliği ve yapay zekâ sistemlerinin araç olarak kullanılması*
>
> *(1) Ceza sorumluluğu şahsidir. Kimse başkasının fiilinden dolayı sorumlu tutulamaz.*
>
> *(2) Tüzel kişiler hakkında ceza yaptırımı uygulanamaz. Ancak, suç dolayısıyla kanunda öngörülen güvenlik tedbiri niteliğindeki yaptırımlar saklıdır.*
>
> *(3) Suçun işlenmesinde yapay zekâ sistemlerinin kullanılması, failin ceza sorumluluğunu ortadan kaldırmaz.*
>
> *(4) Yapay zekâ sistemi, suçun icrasında doğrudan araç olarak kullanılmışsa, bu durumda fail; azmettirme, yardım etme veya dolaylı faillik hükümlerine göre sorumlu tutulur. Yapay zekâ sisteminin öngörülebilir şekilde suç işlemeye elverişli olarak tasarlanması veya suç işlenmesine uygun biçimde piyasaya sürülmesi hâlinde geliştirici, sağlayıcı veya dağıtıcılar hakkında ayrıca azmettirme veya yardım etme hükümleri uygulanır.*

Bu madde hükmüyle beraber bireylerin temel hak ve özgürlükleri ile kamusal güvenliğin korunması, teknolojik gelişmeler karşısında ceza hukukunun işlevini sürdürebilmesi mümkün olabilir.

KAYNAKÇA

Akbulut B, 'Yapay Zekâ ve Ceza Hukuku Sorumluluğu'(2023) 27(4) Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi 267, 319

Akyürek G, 'Özel Hayatın Gizliliğini İhlal Suçu' (Doktora tezi, Galatasaray Üniversitesi 2011)

Akyürek G, Bayraktar K, Evik VS, Yıldız AK, İnceoğlu AA, Kangal ZT, Sınar H, Bostancı Bozbayındır

G, Evik AH, Altunç S, Erman B, Aksoy Retornaz E ve Memiş Kartal P, Özel Ceza Hukuku Malvarlığına Karşı Suçlar Cilt IV (1. Baskı, On İki Levha Yayıncılık, 2018).

Araslı O, 'Özel Yaşamın Gizliliği Hakkı ve T.C. Anayasasında Düzenlenişi' (Yayımlanmamış doçentlik tezi, Ankara Üniversitesi 1979)

Artuk ME, Gökcen A ve Yenidünya AC, *Ceza Hukuku Özel Hükümler* (Yenilenmiş Gözden Geçirilmiş 15. Baskı, Adalet 2015), 880-886

Bartoli, L. 'Cybersecurity and the Fight against Cybercrime: Partners or Competitors?' (2020) *European Journal of Risk Regulation*

<https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/cybersecurity-and-the-fight-against-cybercrime-partners-or-competitors/80A53F6CED87BA65B100E7A03B00DC16> Erişim Tarihi 25 Haziran 2025

Evik AH, Aksoy Retornaz E ve Memiş Kartal P, Özel Ceza Hukuku Cilt VIII Ekonomi, Sanayi ve Ticarete İlişkin Suçlar ve Bilişim Alanındaki Suçlar (1. Baskı, On İki Levha Yayıncılık, 2021)

Centel N, Zafer H, Çakmut Ö, *Kişilere Karşı İşlenen Suçlar*, (4. Baskı, Beta, 2017) Cilt I.

Colonial Pipeline 'Media Statement Update: Colonial Pipeline System Disruption' (*Colonial Pipeline*, 17 May 2021) <https://www.colpipe.com/news/press-releases/media-statement-colonial-pipeline-system-disruption> (or) <https://perma.cc/JYV4-Q432> Erişim Tarihi 14 Haziran 2025

Council on Criminal Justice, 'The Implications of AI for Criminal Justice' (*CCJ*, October 2024) <https://councilоncj.org/the-implications-of-ai-for-criminal-justice/> Erişim Tarihi 12 August 2025

Çamlıca B, *Yapay Zekânın Ceza Sorumluluğu ve Kişilik Tartışmaları* (1. Baskı, Yetkin 2022)

Ell M, '2024 UK Cyber Security Breaches Survey' (*Gov.Uk*, 09 April 2024) <https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024/cyber-security-breaches-survey-2024> Erişim Tarihi 20 Mayıs 2025

European Parliament, *Understanding cybercrime* (EPRS Briefing, 2024) https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/760356/EPRS_BRI%282024%29760356_EN.pdf Erişim Tarihi 25 Haziran 2025

European Commission, Proposal for a Regulation of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive) (COM (2022) 496 final).

<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0496> Erişim Tarihi 25 Haziran 2025

European Parliament and Council, 'Regulation (EU) 2024/1689 on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)' [2024] OJ L212/1. <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng> Erişim Tarihi 25 Haziran 2025

Federal Trade Commission 'New FTC Data Show a Big Jump in Reported Losses to Fraud to $12.5 Billion in 2024' (*Federal Trade Commission*, 10 March 2025) <https://www.ftc.gov/news-events/news/press-releases/2025/03/new-ftc-data-show-big-jump-reported-losses-fraud-125-billion-2024> Erişim Tarihi 3 Temmuz 2025

Gless S and Weigend T, 'Intelligente Agenten und das Strafrecht' (2014) 126(3) Zeitschrift für die gesamte Strafrechtswissenschaft, 561, 591

Gray J, *An Efficient Remedy for the Distress of Nations* (William Tait, Edinburgh 1842)

Hafızoğulları Z ve Özen M, *Türk Ceza Hukuku Özel Hükümler Kişilere Karşı Suçlar* (6. Baskı, US-A, 2017) 406

Hafızoğulları, Z ve Özen M. "Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar". Ankara Barosu Dergisi, (Temmuz 2009) 9-22

Hatfield JM, 'Social Engineering in Cybersecurity: The Evolution Of A Concept'(2018) 73 Computers & Security 102, 113

Jackson JE, 'Fraud Masters: Professional Credit Card Criminals and Crime, Spring' (1994) 19(1) Criminal Justice Review 24, 55

Karagöz MC, *Bilişim Sistemleri Teorisine Giriş* İle *Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu* (1. Baskı, On İki Levha 2020)

Keklik R, 'Özel Hayatın Gizliliğini İhlal Suçu' (Doktora tezi, Selçuk Üniversitesi 2011)

Kilovaty I, 'Cybersecuring the Pipeline' (2023) 60(3) Houston Law Review 605, 651.

Koca M ve Üzülmez İ, *Türk Ceza Hukuku Özel Hükümler* (4. Baskı, Adalet 2017)

Koca M ve Üzülmez İ, 'Kişisel verilerin kaydedilmesi suçu (TCK m. 135)'. Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, Prof. Dr. Durmuş TEZCAN'a Armağan, 2019, 69-93

Kunter N, Yenisey F ve Nuhoğlu A, *Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku İkinci Kitap Hüküm Verme Görevi ve Ceza Muhakemesinin Yapısı* (17. Baskı, Beta, 2010)

Kuzgun İ. *Türk Ceza Hukuku Açısından Mobbing*. (On İki Levha Yayıncılık, 2020)

Küzeci, Elif: Kişisel Verilerin Korunması, Ankara, 2010

Laudon KC and Laudon JP, *Management Information Systems: Managing the Digital Firm* (16th edn, Pearson 2020)

Marc Santora and Julian E. Barnes, 'Fake Video Shows Zelensky Telling Troops to Surrender' *The New York Times* (16 March 2022)

<https://www.nytimes.com/2022/03/16/world/europe/zelensky-deepfake-video.html> Erişim Tarihi 14 Haziran 2025

Krotofil M ve Larsen J, 'Sociotechnical Attack Framework: Understanding the Real Impact of Cyber Attacks on Industrial Control Systems' (2017) 12 https://ics-cert.us-cert.gov Erişim Tarihi 10 Haziran 2025

Marini G, 'Truffa'(1976) XIX Novissimo Digesto Italiano, 864-888

Mitnick KD and Simon WL, *The Art of Deception: Controlling the Human Element of Security* (Wiley Publishing 2002)

National Highway Traffic Safety Administration, 'Automated Vehicles for Safety' <https://www.nhtsa.gov/vehicle-safety/automated-vehicles-safety?> Erişim Tarihi 8 Ağustos 2025

National Transportation Safety Board, *Highway Accident Report- Collision Between Vehicle Controlled by Developmental Automated Driving System and Pedestrian Tempe, Arizona* (NTSB, 19 November 2019)

<https://www.ntsb.gov/investigations/accidentreports/reports/har1903.pdf> Erişim Tarihi 8 Ağustos 2025

Toroslu N, *Ceza Hukuku Özel Kısım* (9. Baskı, Savaş 2018).

OKeefe A, 'Navigating AI Laws And Regulations Across Practice Areas' (*Thomson Reuters,* 28 July 2025) <https://legal.thomsonreuters.com/blog/navigating-ai-laws-and-regulations-across-practice-areas/> Erişim Tarihi 8 Ağustos 2025

Özbek VÖ, Doğan K, Bacaksız P ve Tepe İ, *Türk Ceza Hukuku Özel Hükümler* (Genişletilmiş ve

Güncellenmiş 12. Baskı, Seçkin 2017)

Özgenç İ, *Türk Ceza Hukuku Genel Hükümler* (14. Baskı, Seçkin 2018)

Özgenç İ, *Türk Ceza Hukuku Genel Hükümler* (18. Baskı, Seçkin 2022)

Özsoy N, 'Yargıtay Kararları Işığında Doğrudan Bilişim Suçları' (2019) 1(2) Yaşar Hukuk Dergisi 295,352

Özsunay E, *Gerçek Kişilerin Hukuki Durumu* (5. Baskı, Der Yayınları, 1982)

Riehle C, 'Europol Report Criminal Use of Deepfake Technology' (*Eucrim,* 9 May 2022) <https://eucrim.eu/news/europol-report-criminal-use-of-deepfake-technology/> Erişim Tarihi 18 Mayıs 2025

Sachoulidou A, 'AI Systems and Criminal Liability A Call for Action' (2024) 11(1) Oslo Law Review 1,10

Schmitt M and Flechais I 'Digital deception: generative artificial intelligence in social engineering and phishing' (2024) 57(324) Artifical Intelligence Review 2, 23

Sèdes F and Degrace J, 'Social Engineering and Security: From Human Vulnerabilities to Malicious Threats' (20th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Paris, October 2024)

Singh G, 'Offending Sentiments, A Developing Ground Limiting Free Speech' (Live Law, 20 June 2025) <https://www.livelaw.in/articles/offending-sentiments-developing-ground-limiting-free-speech-295364> Erişim Tarihi 20 Haziran 2025

Solon O, 'The future of fake news: don't believe everything you read, see or hear' (*The Guardian*, 26 Jul 2017) <https://www.theguardian.com/technology/2017/jul/26/fake-news-obama-video-trump-face2face-doctored-content> Erişim Tarihi 18 Mayıs 2025

Soyaslan D, *Ceza Hukuku, Özel Hükümler*, (10. Baskı., Ankara, 2014)

Stupp C, 'Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case' *Wall Street Journal* (30 August 2019) <https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402> Erişim Tarihi 14 June 2025

Syafitri W, Shukur Z, Mokhtar UA, Sulaiman R and Ibrahim MA, 'Social Engineering Attacks Prevention: A Systematic Literature Review' (2022) 10 *IEEE Access* 39325–39352

Kukreja T, 'Deepfakes as a Tool for Criminal Activity' (2025) 5(4) Jus Corpus Law Journal 224, 241

Tezcan D, Erdem MR, Önok RM, *Teorik ve Pratik Ceza Özel Hukuku* (15. Baskı, Seçkin, 2017)

The Kid & Co. and The Shadow, 'More on trashing,' (1984) 1(9) 2600 Magazine: The Hacker's Quarterly

<http://www.hackcanada.com/ice3/2600/2600_01-9_p50.txt> Erişim Tarihi 20 Temmuz 2025

US Cybersecurity and Infrastructure Security Agency (CISA), 'Social Engineering Attacks' <https://www.cisa.gov> Erişim Tarihi 11 Haziran 2025

Wang Z, Sun L and Zhu H, " Defining Social Engineering in Cybersecurity", (2020) 8 IEEE Access, 85094-85115

Yaşar O, Gökcan HT ve Artuç M, *Yorumlu-Uygulamalı Türk Ceza Kanunu Cilt IV* (1. Baskı, Adalet, 2010)