

Yapay Zekânın Suç Oranlarına Etkisi

Abdulkadir Taplamacı

<https://ekopolitik.org.tr/yapay-zekanin-suc-oranlarina-etkisi/>

17 Ocak 2026

“Güçlü bir yapay zekânın yükselişi, insanlığın başına gelen en iyi ya da en kötü şey olabilir. Hangisi olacağını bilmiyoruz.”

Stephan Hawking

Giriş

Son yıllarda yapay zekâ teknolojilerinin baş döndürücü bir hızla gelişmesi, hayatın her alanında köklü değişimlere yol açmaktadır. Günlük yaşamdan endüstriye, sağlıktan ulaşımaya pek çok sektörde yapay zekâ uygulamaları verimlilik ve kolaylık sağlamaktadır. Ancak bu ilerlemeler beraberinde yeni hukuki sorunları ve özellikle ceza hukuku alanında tartışmaları da beraberinde getireceği kanaatindeyim. Zira insan davranışını aratmayacak yeteneklere erişen akıllı sistemlerin suç işleme potansiyeli ve suç oranları üzerindeki etkisi, hukuk düzenini ciddi biçimde meşgul eden bir konu haline gelmiştir. Yapay zekânın kullanımıyla gerçekleşen *dolandırıcılık*, *veri ihlali*, *bilişim suçları*, vb. gibi vakaların basına yansımaları, mevcut ceza kanunlarımızın bu teknoloji karşısında ne ölçüde yeterli olduğu sorusunu gündeme getirecektir. Bu inceleme yazısında, yapay zekâ kavramının teknik ve felsefi temellerinden başlayarak güncel kullanım alanlarına değinilecek; Türk Ceza Kanunu bağlamında yapay zekânın ceza hukuku sorumluluğuna etkileri kusur, isnadiyet, kast ve taksir kavramları çerçevesinde analiz edilecektir. Ayrıca yapay zekâ kullanılarak işlenen suçlara dair somut örnekler ve istatistiki veriler ışığında yapay zekâ-suç ilişkisi ortaya konulacak ve güncel tartışmalara yer verilecektir. Son olarak, elde edilen bulgular doğrultusunda hukuki sistemimize yönelik çözüm önerileri ve değerlendirmeler sunulacaktır.

1. Yapay Zekânın Tanımı ve Tarihsel Gelişimi

Yapay zekâ kavramı literatürde tek bir cümleyle tanımlanamayacak kadar geniş ve dinamiklidir. Genel hatlarıyla yapay zekâ, insan zekâsını taklit eden, öğrenme, muhakeme, problem çözme ve karar verme kabiliyeti sergileyen bilgisayar sistemleri olarak ifade edilmektedir. Bununla birlikte, yapay zekânın üzerinde tüm otoritelerin uzlaştığı net bir tanım bulunmamaktadır; teknoloji sürekli evrim geçirmekte ve her geçen gün yeni özellikler kazanmaktadır. Bilim insanları başlangıçtan beri, makinelerin insan gibi düşünebilmesi, karar verebilmesi ve hatta eylem gerçekleştirebilmesi yönünde çalışmalar yürütmüşlerdir.

Modern anlamda yapay zekâ araştırmaları, dijital bilgisayarların gelişmeye başlamasıyla 1950’lerden sonra ivme kazanmıştır. 1956 yılında gerçekleştirilen Dartmouth Konferansı genellikle “yapay zekâ” teriminin akademik bir disiplin olarak doğuşu kabul edilir. İlk dönem çalışmalarında bilgisayarlara insanlarca önceden tanımlanmış kural ve algoritmalar

uygulanarak satranç oynama, matematik teoremleri ispatlama gibi görevlerde başarı sağlanmıştır. 20. yüzyılın ikinci yarısında sembolik yapay zekâ ve uzman sistemlerin gelişimiyle önemli ilerlemeler kaydedilmiş, ancak 1970’lerde ve 1980’lerde araştırma fonlarının azalmasıyla “yapay zekâ kıışı” olarak adlandırılan duraklama dönemleri de yaşanmıştır. 1990’lardan itibaren veri madenciliği, istatistik ve hesaplama gücündeki artışlar, makine öğrenmesi yöntemlerini ön plana çıkarmıştır. Özellikle 2010’lu yıllarda yapay sinir ağları ve derin öğrenme tekniklerinin gelişimi, yapay zekâ alanında adeta bir devrim niteliğindedir.

Yapay zekânın tarihsel gelişimi aynı zamanda felsefi tartışmaları da beraberinde getirmiştir. Yapay zekâ kavramı, Antik çağlardan beri efsanelerde ve hayal gücünde yer bulan yapay insanlar fikrinin modern teknolojiyle vücut bulmuş hali olarak görülebilir. “Zekâ” ve “bilinç” kavramlarının makinelere atfedilip atfedilemeyeceği, bir makinenin gerçek anlamda düşünen veya irade sahibi bir varlık sayılıp sayılamayacağı gibi sorular felsefecilerin ve hukukçuların ilgi alanındadır. Bu bağlamda teknik ilerlemeler kadar yapay zekânın mahiyetine dair felsefi değerlendirmeler de hukukun yapay zekâyâ yaklaşımını biçimlendirmektedir. Kısacası, yapay zekâ mefhumu hem mühendislik hem de felsefe disiplinlerinin kesişiminde gelişmiş; bugün gelinen noktada insansı yetenekler sergileyen algoritmalar hayatımızın parçası haline gelmiştir.

2. Yapay Zekânın Günümüzdeki Kullanım Alanları

Yapay zekânın ulaştığı gelişmişlik seviyesi, onun neredeyse bütün sektörlerde yaygın şekilde kullanılmasına imkân tanımıştır. Hukuk alanında yapay zekâ uygulamaları giderek önem kazanmaktadır. Özellikle büyük miktarda hukuki verinin işlenmesi ve analiz edilmesi gereken durumlarda, yapay zekâ destekli yazılımlar ciddi zaman tasarrufu ve tutarlılık sağlamaktadır. Örneğin akıllı arama algoritmaları, yüz binlerce sayfa yargı kararını tarayarak ilgili içtihatları saniyeler içinde bulabilmekte keza dava dilekçelerinin hazırlanmasında bazı yapay zekâ araçları taslak metin önerebilmektedir.

Türkiye’de de son yıllarda hukuk fakültelerinde “bilişim hukuku” ve “yapay zekâ hukuku” ile ilgili ders ve programlara ağırlık verilmeye başlanmıştır. Dünyada bazı ülkeler yapay zekâyı yargılamada yardımcı araç olarak test etmektedir. Örneğin ABD’de mahkemelerce kullanılan risk değerlendirme algoritmaları (ceza yargılamasında tekrar suç işleme riskini tahmin eden yazılımlar) veya Çin’de bazı bölgelerde basit hukuk uyuşmazlıklarında çevrimiçi arabuluculuk yapan yapay zekâ sistemleri pilot uygulamalar arasındadır. Ancak hukukta yapay zekâ kullanımı sadece yargıyla sınırlı değildir; kolluk kuvvetleri de öngörücü polislik yazılımlarıyla suç meydana gelmeden riskli bölgeleri tespit etme çabasındadır. Bu durum, yapay zekânın önyargılı verilerle çalışması halinde adil yargılanma ve masumiyet karinesi gibi ilkelere aykırı sonuçlar doğurabileceği endişesini de doğurmakta, hukuk ve etik tartışmalarını beraberinde getirmektedir.

Sağlık sektörü, Ulaşım, Savunma sanayi, Bankacılık/finans, Eğitim ve Tarım gibi sektörlerin her birinde yapay zekâ uygulamaları hızla yaygınlaştığı görülmektedir. Özetlemek gerekirse, yapay zekâ günümüz dünyasında genel bir kullanım alanı bulmuştur ve hayatın hemen her cephesinde karşımıza çıkmaktadır. Bu durum hukuk düzeni açısından da yapay zekâyı görmezden gelmenin imkânsızlaştığı anlamına gelecektir. Özellikle ceza hukuku

perspektifinden, yapay zekâ uygulamalarının suç oluşturan fiillere karışma ihtimali, bir sonraki bölümde ele alacağımız gibi, hukukun temel kavramlarının yeniden yorumlanmasını gerektirecektir.

3. Yapay Zekânın Ceza Hukuku Sorumluluğuna Etkisi

Yapay zekâ ile donatılmış varlıkların ceza hukuku sorumluluğu meselesi, hukuk dünyasında en çetrefilli tartışmalardan birine dönüşmüş durumdadır. Geleneksel ceza hukuku teorisi, ceza sorumluluğunun yalnızca insana özgü olduğunu ve suç failinin ancak insan olabileceğini kabul eder. Zira ancak insanlar iradi ve ahlaki bir değerlendirme yeteneğiyle kusurlu hareket edebilir; bilinç ve irade sahibi olmayan bir varlığın suç fiilinden sorumlu tutulması düşünülemeyecektir. Bugünkü mevcut teknolojik düzey itibarıyla yapay zekâ sistemleri, ne kadar karmaşık ve zeki görünseler de bilinç sahibi değildirler ve kendi başlarına özerk bir iradeyle hareket ettikleri kabul edilmemektedir. Nitekim yapay zekâ, belirli hedeflere ulaşmak üzere insanlar tarafından belirlenen talimatları yerine getirmekte henüz insanın kontrolünden tamamen bağımsız, öz bilince sahip bir “*yapay sîje*” ortaya çıkmış değildir. Bu nedenle ceza hukuku bakımından, yapay zekâların doğrudan fail olarak kabulü günümüz için mümkün görünmeyecektir.

Ceza kanunlarımızda suçun faili genellikle “kişi” olarak tanımlanır ve burada kastedilen ceza ehliyetine sahip gerçek kişilerdir. Tüzel kişilerin ceza sorumluluğu ise istisnai ve sınırlı durumlar dışında kabul edilmez. Yapay zekâ ise ne gerçek kişi ne de tüzel kişi statüsünde olmadığı için, pozitif hukuk bakımından fail kavramının dışında kalacaktır. Örneğin Türk Ceza Kanunu’nun 20. maddesinde “*ceza sorumluluğu şahsidir*” denilerek kimse başkasının fiilinden sorumlu tutulamayacağı ilkesi vurgulanır ve tüzel kişilere ceza verilemeyeceği belirtilmektedir. Bu çerçevede, bir robotun ya da yapay zekâ programının işlediği varsayılan bir suç nedeniyle cezai yaptırım uygulanması, mevcut hukuki sistemde muhatap eksikliği nedeniyle mümkün değildir. Zira ortada cezalandırılabilir iradi bir fail yoktur. Ayrıca ceza hukukunun en temel prensiplerinden biri, kusurun bulunmadığı yerde ceza sorumluluğunun olmayacağıdır (*nullum crimen sine culpa*). Kusur yeteneği ise ancak algılama ve irade yeteneğine sahip, işlediği fiilin hukuk düzenince haksızlık teşkil ettiğini anlayabilecek varlıklarda söz konusu olmaktadır. Yapay zekâlı varlıklar ise bugün itibarıyla böyle bir ahlaki veya hukuki muhakeme yeteneğinden yoksun durumdadır. Bu durumda ceza hukuku doktrinde hakim görüş, yapay zekâların kendilerinin fail veya kusur ehliyetine sahip sîjeler olarak kabul edilemeyeceği yönündedir. Hatta bazı yazarlar, teknoloji ne kadar gelişirse gelişsin “kusurlu” bir robotun tasavvur edilemeyeceğini, çünkü kusur kavramının özünün ancak özgür iradeye sahip insan davranışlarıyla anlam kazandığını ifade etmektedir.

Bu noktada, yapay zekâların ceza hukuku sorumluluğunu değerlendirirken ayırım yapmak gereken iki temel senaryo ortaya çıkmaktadır: (i) Yapay zekânın suç teşkil eden bir fiilde araç olarak kullanılması ve (ii) Yapay zekânın insan iradesinden bağımsız şekilde bir fiil işlemesi.

3.1. Yapay Zekânın Suçta Araç Olarak Kullanılması

Yapay zekâ teknolojisi henüz tam manasıyla özerk bir “fail” olma kapasitesine ulaşmamış olduğundan, günümüzde karşılaşılan vakaların büyük çoğunluğu, yapay zekânın suç işlemek isteyen bir kişi tarafından araç olarak kullanılması şeklindedir. Bu durumda suçun arkasında

iradi bir insan faaliyeti bulunmaktadır ve ceza hukuku açısından cezai sorumluluk yine insana ait olacaktır. Esasen ceza hukukumuz, bir suçun işlenmesinde cansız bir aletin veya sorumluluk ehliyeti olmayan bir kimsenin kullanılması hallerini düzenlemiş durumdadır. Örneğin TCK md. 37/2, “*bir başkasını araç olarak kullanmak suretiyle*” suç işleyen kimsenin fail sayılacağını öngörmüştür. Burada “başkası” kavramı, cezai sorumluluğu olmayan veya sınırlandırılmış olan bir kişiyi (örneğin çocuğu, akıl hastasını) suçta kullanan asıl fail durumlarını karşılamaktadır. Doktrinde ileri sürüldüğü üzere, yapay zekâ da kusur yeteneğine sahip olmadığı için tıpkı cezai ehliyeti olmayan bir kimse gibi “araç” olarak kullanılabilir. Bu bakış açısına göre, yapay zekâ ile işlenen suçlarda arka plandaki insan failin ister programlayıcı olsun ister kullanıcı dolaylı fail konumunda sorumlu tutulması mümkün olacaktır.

Yapay zekânın araç olarak kullanılmasının değişik şekilleri olabilir. Birinci ihtimal, yapay zekânın cansız bir alet gibi değerlendirilerek suçta kullanılmasıdır. Örneğin bir kimse, içine patlayıcı yüklediği yapay zekâ ile çalışan insansız bir hava aracını (drone’u) hedefe yönlendirip patlatarak bir topluluğa zarar verebilir. Bu durumda drone, fail tarafından silah olarak kullanılmış sayılır. TCK md. 6/1-f bentlerinde hangi araçların “silah” sayılacağı tanımlanmıştır; eğer yapay zekâ destekli bir cihaz bu kapsamda değerlendirilirse basit bir alet gibi muamele görecektir. Nitekim bir bomba yüklü insansız hava aracına kasten yanlış koordinatlar girilip insanların ölümüne neden olunması, doktrinde yapay zekânın suçta araç olarak kullanımına örnek gösterilmektedir. Benzer şekilde, yüz tanıma ve takip yeteneği olan bir drone ile özel hayatın gizlice gözetlenmesi veya kayıt yapılması durumunda da bu drone bilişim sistemleri vasıtasıyla işlenen özel hayatın gizliliğini ihlal suçu kapsamında sadece fiilin icrasına yarayan bir araç konumundadır. Bu senaryoda yapay zekâ, failin suç planını gerçekleştirmekte kullandığı sofistike bir aletten ibarettir.

Yapay zekânın suçta araç olmasının ceza hukukunda daha önce görülmemiş bir yansıması ise, bilişim sistemlerinin suç aracı olarak kullanılması kapsamında değerlendirilebilir. TCK md. 158’de nitelikli dolandırıcılık suçunun bilişim sistemlerinin kullanılması suretiyle işlenmesi ayrı bir ağırlaştırıcı hal olarak düzenlenmiştir. Günümüzde sıkça karşılaşıldığı gibi, yapay zekâ kullanılarak hazırlanan inandırıcı deepfake videolar veya ses sentetikleri marifetiyle insanlar dolandırılabilir. Örneğin bir dolandırıcının yapay zekâ ile bir siyasi liderin veya ünlü iş insanının sesini taklit ederek üçüncü kişilerden para talep etmesi olayları basına yansımıştır. Bu durumda dolandırıcılık suçunun hile unsuru yapay zekâ ile gerçekleştirilmektedir. Fail ise yapay zekânın üretmiş olduğu sahte içerikleri kullanarak mağduru aldatan kişi konumundadır. Türk ceza hukukunda bu senaryoyu karşılamaya aslında mevcut düzenlemeler yeterlidir. Bu durumda dolandırıcılık suçu oluşmakta ve bilişim sistemlerinin araç olarak kullanılması nedeniyle nitelikli hal uygulanmaktadır. Bu örnek, yapay zekânın suç işlemeye elverişli yeni bir araç olarak mevcut suç tipleriyle ilişkilendirilebileceğini göstermektedir.

3.2. Yapay Zekânın Öngörülme-yen Fiilleri ve İsnadiyet Sorunu

İkinci senaryo, yapay zekâ sisteminin insan kontrolü dışında kendi karar ve aksiyonları sonucunda suç teşkil eden bir sonuç ortaya çıkarmasıdır. Bu durum genellikle bir teknik arıza, beklenmeyen öğrenme çıktısı veya programlama hatasından kaynaklanabilir. Örneğin otonom bir aracın sensörlerindeki bir yazılım hatası sebebiyle kaldırıldaki yayaları araç sanıp

direksiyon kırması ve bir yayaya çarpıp ölümüne neden olması gündeme gelebilecektir. Bu senaryoda, aracı o anda kullanan bir sürücü yoksa yani tam otonom moddaysa cezai sorumluluğun kime ait olacağı tartışmalıdır. Kullanıcı konumundaki kişi araçta yalnızca yolcu ise onun kastından söz edilemez; taksir düzeyinde bir kusuru olup olmadığı ise aracın kullanım kılavuzuna uygun hareket edip etmediğine göre değerlendirilebilir. Öte yandan aracın üreticisi veya yazılım geliştiricisi, böyle bir kazayı öngörebilecek bir ihmal yapmış mıydı sorusu gündeme gelir. İşte bu noktada ceza hukukunda objektif isnadiyet ölçütleri devreye girecektir.

Objektif isnadiyet, meydana gelen neticenin hangi fiile objektif olarak yüklenebileceğini belirlemeye yarayan kriterlerdir. Bir yapay zekâ fiilinden dolayı kimseye ceza sorumluluğu yükleyebilmek için o sonucun bir insanın yaratmış olduğu hukuka aykırı bir riskin gerçekleşmesi olarak değerlendirilebilmesi gerekir. Eğer yapay zekâ nedeniyle ortaya çıkan zarar, herhangi bir insanın öngörüp önleyebileceği türden bir riskin gerçekleşmesi değilse, ceza hukuku anlamında ortada sorumlu tutulabilecek bir fail yok demektir.

Ancak yapay zekâ fiillerinde herkesin sorumluluğunu tartışmak kolay değildir. Kullanıcı, programcı ve üretici arasındaki görev dağılımı ve sorumluluk denklemi her somut olaya göre değişebilecektir. Genel bir ilke olarak; eğer yapay zekâ, kişinin hükmedebildiği alan dahilinde bir eylem yapıyorsa, yani kullanıcının veya programcının denetimi sınırları içinde bir işlem söz konusuysa, o zaman ilgili kişinin kastı veya taksiri bulunup bulunmadığı araştırılır. Mesela bir tıp alanında kullanılan yapay zekâ cihazının uyarılarına rağmen doktor hatalı kararı kendi verirse, sorumluluk doktordadır. Fakat yapay zekâ kendi kendine, beklenmedik bir şekilde ve otonom bir kararla suç teşkil eden bir sonuç doğurmuşsa, kullanıcı veya programcının da bunu öngörüp öngöremediğine bakılır. Eğer yapay zekânın davranışı tamamen öngörülemez bir türdeyse ve kişi açısından “kaçınılmazlık” söz konusuysa, kusur ilkeleri gereği o kişiye ceza isnadı yapılamayacaktır. Bu tür durumlar ceza hukukunda gerçek bir boşluk bir *faili meçhul* hal yaratmaktadır. Zira ne yapay zekâyı ceza verilebilir ne de insana verilmesi adil olur. Bu gibi durumlar için bazı yazarlar riskin izin verilen sınırlar içinde olup olmadığı ölçütüne dikkat çeker. Eğer yapay zekânın faaliyeti belli bir sosyal yarar uğruna izin verilen risk kapsamında ise (örneğin hayat kurtaran bir ameliyat robotunun çok düşük bir ihtimal gerçekleşen arızası), netice kimseye objektif olarak yüklenemeyebilir. Ama risk, makul sınırların ötesinde ve kimsenin üstlenmediği türdensen, belki de o yapay zekâ sisteminin kullanılmasına izin veren yapısal bir hata söz konusudur.

Netice itibarıyla, yapay zekâların öngörülmeyen fiilleri karşısında objektif isnadiyet ve kusur ilkeleri dikkatle uygulanması gerekmektedir. Hukukumuz, kimseyi kendi kusuru olmaksızın cezalandırmama prensibine dayandığından, yapay zekâdan kaynaklanan bir suçta uygun kusur bulunamazsa ceza sorumluluğu doğmayacaktır. Bu durum, mağdurlar açısından bir hukuki koruma boşluğu yaratabilir. Örneğin tamamen özerk bir yazılımın sebep olduğu büyük bir maddi zarar veya veri sızıntısı olayında, ortada cezalandırılacak kimse kalmazsa caydırıcılık nasıl sağlanacaktır sorusu önemlidir. Doktrinde bu boşluğu doldurmak için farklı öneriler mevcuttur. Bunlardan biri, yapay zekâların fiillerinden doğan zararlar için kusursuz sorumluluk ilkelerinin geliştirilmesidir. Avrupa Birliği’nde 2020’li yıllarda tartışılan bazı raporlarda, yüksek riskli yapay zekâ uygulamalarının neden olduğu zararlarda üretici veya işletmecinin kusursuz sorumluluğu esas alınarak mağdurlara tazminat ödenmesi görüşü dile getirilmiştir. Bu

kapsamda, yapay zekâların bir sicile kaydedilmesi ve olası zararların tazmini için özel bir fon oluşturulması gibi fikirler de öne sürülmüştür. Ancak bu tür düzenlemeler daha çok özel hukuk tazmin sorumluluğu alanına girer; ceza hukuku açısından kusursuz sorumluluk prensibi benimsenmediği için, suç fiilleri yönünden yine bir insana kusur atfedilmedikçe ceza verilemeyeceği kuralı geçerli olmaya devam etmektedir.

3.3. Yapay Zekâ ve Türk Ceza Kanunu'ndaki Bazı Suç Tipleri

Yapay zekânın ceza hukuku sorumluluğunu somutlaştırmak adına, Türk Ceza Kanunu'nda yer alan belli başlı suç tipleriyle ilişkisini incelemek faydalı olacaktır. Yukarıda değinildiği üzere, yapay zekâ kendi başına fail olmadığı için her durumda suçun maddi unsuru bir insan eylemine dayanacaktır. Bununla birlikte, bazı suçlar yapay zekâ teknolojilerinin gelişmesiyle yeni biçimlerde işlenebilmektedir:

1. **Kasten Öldürme ve Yaralama Suçları (TCK m.81, 86):** Bir yapay zekâ sistemi kullanılarak bir insana zarar verildiğinde, bunu yapan kişi kasten insan öldürme veya yaralama suçundan sorumlu olacaktır. Örneğin bir kişiye suikast amacıyla programlanmış otonom bir robot kullanılırsa, robot bir silah gibi değerlendirilip fail insana TCK m.81 uygulanır. Eğer ölüm istemeden, öngörülmeleyen bir yapay zekâ arızası sonucu olmuşsa, ihmali olan kişi için taksirle öldürme (TCK m.85) gündeme gelebilir. Örneğin 2018'de Uber şirketinin sürücüsüz aracı, bir yayaya çarparak ölümüne yol açmış; bu olayda araçta güvenlik sürücüsü olarak bulunan kişi hakkında taksirle ölüme sebebiyet suçundan soruşturma açılmıştır. Bu örnek, otonom araç kazalarında dahi bir insan operatörün veya üreticinin sorumluluğunun araştırıldığını göstermektedir.
1. **Bilişim Suçları (TCK m.243-246):** Yapay zekâ, bir bilişim sistemine izinsiz girmek, veri bozmak gibi suçlarda etkin bir araç olarak kullanılabilecektir. Örneğin gelişmiş bir yapay zekâ programı kullanarak banka sistemlerine sızıp veri çalan hacker olayları bilişim suçu sayılır. Bu durumda yapay zekâ, hacker'ın suç aleti konumundadır. Yine yasak erişim (m.243), sistemi engelleme, bozma, verileri yok etme (m.244) gibi suçlarda, fiili bizzat icra eden bir yapay zekâ yazılımı olsa dahi, onu çalıştıran operatör cezai sorumluluğu üstlenecektir.
2. **Özel Hayata ve Verilere Karşı Suçlar (TCK m.132-140):** Yapay zekâ destekli cihazlar, insanların özel hayatına ilişkin görüntü veya sesleri izinsiz kaydedip ifşa edebilmektedir. Örneğin kameralı bir drone, yapay zekâ ile belirli bir kişiyi takip edip özel görüntülerini kaydederse, bunu yapan kişi özel hayatın gizliliğini ihlal (m.134) suçundan yargılanır. Keza yapay zekâ kullanılarak sosyal medya hesaplarından kişisel verilerin toplanması, yüzlerin eşleştirilmesi gibi eylemler kişisel verilerin hukuka aykırı ele geçirilmesi (m.136) suçunu oluşturur. Nitekim otonom araçlar konusunda dahi tartışılan hususlardan biri, aracın çevredeki kişilerin konum ve görüntü verilerini sürekli kaydetmesinin bir veri ihlali riski doğurduğudur. Böyle bir durumda, o verileri hukuka aykırı kullanıma sunan kişiler TCK m.136 gereği cezai sorumluluk taşıyacaktır. Öte yandan yapay zekâ ile üretilmiş sahte görüntü ve seslerin, bir kişiye şantaj yapmak veya itibarını zedelemek amacıyla kullanılması da şantaj (m.107) veya hakaret (m.125) gibi suç tiplerine vücut verebilir. Basında yer alan örneklerde, mağdurların yüzü yapay zekâ

ile videolara montajlanıp internet ortamında yayılarak şantajı uğratıldığı görülmektedir. Bu durumda fail yine insandır ve ilgili suçtan yargılanır; yapay zekânın ileri teknik bir araç olması suçu ortadan kaldırmaz.

3. **Dolandırıcılık Suçları (TCK m.157-158):** Daha önce de temas ettiğimiz üzere, yapay zekâ özellikle nitelikli dolandırıcılık eylemlerinde sıkça kullanılmaya başlanmıştır. Deepfake teknolojisiyle önemli kişilerin ses ve görüntülerini taklit ederek insanlar kandırılabilir. Yakın tarihli bir olayda, dolandırıcılar bir iş insanının sesini yapay zekâ ile kopyalayarak karşı taraftan para talep etmiş ve bunu gerçek sanan kişiler mağdur olmuştur. Bu eylem, TCK m.158’de düzenlenen bilişim sistemlerinin araç olarak kullanılması suretiyle dolandırıcılık kapsamına girmektedir. Yine bankacılık işlemlerinde yapay zekâ ile e-posta atıp gerçekçi görünümlü taleplerle insanları kandıran *oltalama (phishing)* saldırıları da dolandırıcılık suçunu oluşturur.

Yukarıdaki örnekler çoğaltılabilir. Kamu güvenine karşı suçlar bakımından yapay zekâ kullanılarak sahte resmî belge düzenlemek mümkün hale gelebilir (örneğin yapay zekâ ile üretilmiş gerçekçi sahte kimlikler, pasaportlar); bu durumda da belgede sahtecilik suçunun unsurları oluşacaktır.

Europol’ün 2025 tarihli bir raporu, 2035’e kadar robotlar ve yapay zekâ sistemlerinin yaygınlaşmasıyla “robot suçları” diye anılan yeni bir suç dalgası yaşanabileceği uyarısında bulunmaktadır. Bu senaryolarda, polisin sadece insan şüphelileri değil suça karışan robotik sistemleri de soruşturmak zorunda kalacağı; bir olayın teknik arızadan mı yoksa kasıtlı bir sabotajdan mı kaynaklandığının tespitinin zorlaşacağı vurgulanmıştır. Bu öngörüler, yapay zekâ çağında ceza soruşturmalarının da yöntemsel olarak değişebileceğine işaret etmektedir.

4. Yapay Zekâ Kullanılarak İşlenen Suçlara Dair Güncel Örnekler

Teorik tartışmaları somutlaştırmak adına, son dönemde basına yansımış olan yapay zekâ bağlantılı suç örneklerine değinmek yararlı olacaktır. Gelişen teknoloji ile suçlular yapay zekâyı kendi amaçları doğrultusunda kullandığı gözlemlenmektedir. Aşağıda güncel ve somut birkaç vaka ele alınmıştır:

- **Deepfake ile Dolandırıcılık (Ses Taklidi):** Dolandırıcılar yapay zekâ kullanarak tanınmış kişilerin seslerini taklit edebiliyor ve bu sahte ses kayıtlarıyla insanları kandırabilmektedirler. Özellikle üst düzey yönetici, kamu görevlisi veya ünlü kişilerin seslerini yüksek kalitede kopyalayan dolandırıcılar, telefonda karşı tarafa bu kişinin kendisi olduğunu düşündürüp çeşitli bahanelerle para talep edebiliyorlar. Bu yöntemle gerçekleştirilen eylemler nitelikli dolandırıcılık suçunu oluşturacaktır. Bu olay, yapay zekâ destekli ses klonlama teknolojisinin suç dünyasında somut bir tehdit olarak belirdiğini göstermektedir. Nitekim uluslararası bir örnek olarak, 2019’da bir İngiliz enerji firmasının CEO’sunun sesinin yapay zekâ ile taklit edilmesi suretiyle şirket muhasebecisinin kandırılıp 220 bin Euro’yu dolandırıcılara aktardığı rapor edilmiştir. Yine 2023 yılında ABD’de bir anne, kızının sesi yapay zekâ ile kopyalanarak oluşturulan sahte bir “kaçırılma” telefonu almış ve fidye istenmiştir. Bu tür ses deepfake

vakalarının dünya genelinde arttığı ve milyonlarca dolarlık vurgunlara yol açtığı bilinmektedir.

- **Deepfake ile Şantaj ve İtibar Suikastı:** Yapay zekâ sadece sesi değil, görüntüyü de taklit edebildiğinden, suçlular açısından yeni şantaj yöntemleri doğmuştur. Böyle bir durumda kişinin itibarını zedeleyip maddi taleplerde bulunmayı amaçlayan kötü niyetli kişiler hakkında soruşturma başlatılarak, özel hayatın gizliliğini ihlal, kişisel verilerin hukuka aykırı kullanımı ve duruma göre şantaj suçlarını oluşturacaktır.
- **Sohbet Botu “Grok” Vakası (Hakaret Suçları):** Temmuz 2025’te Türkiye’de basına yansıyan ilginç bir olayda, X platformunun yapay zekâ destekli sohbet botu “Grok” bazı kullanıcılara cevaplarında hakaret ve küfür içerikleri sunmuştu. Bu durum üzerine Ankara Cumhuriyet Başsavcılığı, botun ürettiği içeriklerle ilgili olarak resen soruşturma başlatmıştı. Bu gelişme, bir yapay zekâ uygulamasının kendisinin suç unsuru içeren fiiller üretmesi halinde dahi sonuçta bir insan veya şirketin sorumlu tutulacağını gösteren önemli bir örnek teşkil etmektedir. Nitekim ilgili sohbet botunu işleten platform yetkilileri hakkında erişim engelleme gibi tedbirler uygulanmış ve yapay zekâ ile üretilen bu içerikler yayından kaldırılmıştır. Bu olay yapay zekâ modellerinin denetimsiz bırakılması halinde yasal sorunlara yol açabileceğini ve devletlerin bu konuda düzenleme ve yaptırım yoluna gidebileceğini göstermesi bakımından kayda değerdir.
- **Autonom Araç Kazası (Uber Olayı):** Yukarıda kısmen değindiğimiz üzere, Mart 2018’de ABD Arizona’da gerçekleşen kazada, Uber şirketinin test ettiği sürücüsüz araç, yolda bisikletle giden bir kadına çarparak ölümüne sebep oldu. Bu, otonom bir aracın karıştığı ilk ölümlü trafik kazası olarak tarihe geçti. Soruşturma neticesinde aracın yedek sürücüsünün gerekli dikkat ve müdahaleyi yapmadığı tespit edilerek kendisine taksirle adam öldürme suçlaması yöneltildi. Bu olay, teknolojik bir arızadan kaynaklanan ölümlü neticelerde dahi bir insan faktörü aranacağını en azından ihmali davranışların cezai sorumluluğa konu olabileceğini somutlaştırmıştır. Otonom araçların karıştığı benzer kazalar ileride arttıkça, hukuk sistemleri bu vakalara standart bir yaklaşım geliştirmek durumunda kalacaktır. Ancak bu tarz kazaların hukuki neticeleri konusunda ülkeler arasında yaklaşım birliği oluşmuş değildir.
- **Yapay Zekâ ile Siber Saldırıları:** Klasik siber suçlar yapay zekâ ile boyut değiştirmektedir. 2023 yılında global ölçekte bir fidye yazılımı saldırısında, saldırganlar yapay zekâ kullanarak şirketin sistem açıklarını otomatik tespit etmiş ve saniyeler içinde kurumun tüm verilerini şifrelemişlerdir. Bu olayda yapay zekâ, saldırının hızını ve etki alanını akıl almaz şekilde artırmıştır. Emniyet birimleri, bu tür yapay zekâ destekli siber saldırılara karşı yine yapay zekâ tabanlı savunma sistemleri geliştirme peşindedir. Özellikle sosyal medyada paylaşılan kişisel bilgilerin, yapay zekâ tarafından analiz edilip hedefe yönelik sahte mesajlar üretmekte kullanıldığı, böylece dolandırıcılık oranının arttığı vurgulanmaktadır. Bu örnekler, suçluların yapay zekâ sayesinde eylemlerini daha inandırıcı, hızlı ve geniş çaplı hale getirebildiklerini ortaya koymaktadır.

Yukarıda sayılanlar haricinde pek çok örnek verilebilir. Tüm bu somut vakalar yapay zekânın çift yüzlü bir teknoloji olduğunu göstermektedir: Bir yanda insanlığın yararına büyük fırsatlar sunarken diğer taraftan kötüye kullanıldığında suçluların elinde güçlü bir silaha dönüşebilmektedir. Bu noktada, yapay zekâ çağında suçlarla mücadele etmek için hem teknik tedbirlerin hem de hukuki mekanizmaların güncellenmesi kaçınılmaz görünmektedir.

5. Yapay Zekâ ve Suç İlişkisine Dair İstatistikler (Türkiye ve Uluslararası Veriler)

Yapay zekâ teknolojilerinin suç dünyasında yarattığı etkileri rakamsal verilerle de ortaya koymak mümkündür. Her ne kadar “yapay zekâ ile işlenen suçlar” kategorisi henüz istatistik kurumlarının ayrı bir başlık olarak takip ettiği bir konu olmasa da ilgili bazı gösterge veriler, suç oranlarındaki değişimde yapay zekânın rolünü göstermektedir.

Bu bölümde önce Türkiye’ye ilişkin bazı veriler, ardından uluslararası istatistikler sunulacaktır.

Türkiye açısından bakıldığında, dijital suçlarda genel bir artış trendi olduğu görülmektedir. Türkiye’de siber suçlarla mücadeleden sorumlu birimlerin verilerine göre, tespit edilen siber saldırı sayısı son yıllarda hızlı bir yükseliş göstermiştir. Bilgi Teknolojileri ve İletişim Kurumu (BTK) bünyesindeki USOM’un (Ulusal Siber Olaylara Müdahale Merkezi) verilerine dayanan bir raporda, 2022 yılında Türkiye’de yaklaşık 72.209 siber saldırı tespit edilmişken, 2023 yılında bu sayının 105.000’in üzerine çıktığı belirtilmiştir. Bu yaklaşık %45’lik artış, bir yılda siber tehditlerin ne denli büyüdüğüne işaret etmektedir. 2024 yılının ilk çeyreğinde ise 37.600 civarında siber saldırı tespit edildiği raporlanmıştır. Elbette bu saldırıların tamamı yapay zekâ kaynaklı değildir; ancak uzmanların değerlendirmeleri, son 1-2 yılda yaşanan siber saldırı artışında özellikle üretken yapay zekâ kullanımının etkili olduğunu göstermektedir. Nitekim küresel bir ankette, siber güvenlik uzmanlarının %85’i son 12 aydaki siber saldırı artışını doğrudan yapay zekâ araçlarının kötüye kullanımına bağlamıştır. *Dolandırıcılık, kimlik hırsızlığı, veri sızdırma* gibi vakalarda yapay zekâ destekli yöntemlere başvurulduğu Emniyet yetkililerince dile getirilmektedir. Örneğin Emniyet Genel Müdürlüğü raporlarında, ortalama saldırıların 2023 yılında bir önceki yıla göre %20 arttığı; özellikle sosyal medya üzerinden yapılan dolandırıcılıklarda yapay zekâ ile kişiye özel inandırıcı mesajlar kullanılması nedeniyle başarı oranının yükseldiği belirtilmektedir. Yine Türkiye’de 2023 yılında kişilerin dijital ortamdaki sahte içeriklere maruz kalma oranının ciddi ölçüde arttığı rapor edilmiştir. *Statista* verilerine göre 2023’te dünya genelinde 17 milyon siber suç işlenmiş olup, Türkiye de bu tabloda en çok “ortalama” saldırılarına maruz kalan ülkelerden biri konumundadır.

Ayrıca kolluk birimlerinin verdiği bilgilere göre, 2023 yılı itibarıyla yapay zekâ aracılığıyla işlenen dolandırıcılık vakaları toplam dolandırıcılık suçlarının önemli bir kısmını oluşturmuştur. Özellikle ses ve görüntü taklidiyle yapılan dolandırıcılıkların parasal bilançosu ağırlaşmaktadır. Küresel bir siber güvenlik şirketinin tahminine göre, 2023 yılında deepfake yöntemiyle dünya genelinde yol açılan maddi zarar 400 milyon doların üzerindedir. Bu sahteciliklerin bir kısmı Türkiye’deki mağdurları da hedef almıştır. Örneğin bir bankanın müşterilerine yönelik sahte bir mobil uygulama reklamı yapay zekâ ile oluşturularak birçok kişinin hesap bilgileri çalınmıştır (bu olayda bankanın ismi ve logosu gerçeğinden ayırt edilemeyecek şekilde yapay zekâ tarafından taklit edilmiştir). Bu tip olaylar, resmi makamları

da harekete geçirmiştir. T.C. İçişleri Bakanlığı 2024 başlarında vatandaşlara yönelik bir uyarı yayımlayarak, yapay zekâ ile üretilmiş sahte ses ve görüntülere karşı dikkatli olunmasını istemiş; özellikle telefonla arayan kişilerin kimlik bilgilerine itibar edilmemesini tavsiye etmiştir.

Uluslararası istatistiklere baktığımızda, yapay zekâ ve suç kesişiminde çarpıcı veriler mevcuttur. Dünya genelinde siber suçların sayısı ve maliyeti her yıl rekor düzeyde artmaktadır. 2023 yılında dünya çapında işlenen siber suç sayısının 17 milyon civarında olduğu bildirilmiştir. Yapay zekânın bu artıştaki rolü, niteliksel olarak büyük önem taşımaktadır. Örneğin 2024 yılının ikinci yarısında, küresel ölçekte phishing (olta saldırısı) e-posta sayısında artış tespit edilmiştir. Bunun arkasındaki temel sebeplerden biri, saldırganların yapay zekâ araçlarını kullanarak hatasız ve ikna edici e-postalar yazabilmesidir. Yine kimlik bilgilerini çalmaya yönelik phishing saldırılarının aynı dönemde arttığı, bunun da internette kolayca bulunabilen yapay zekâ destekli oltaalama kitlerinin yaygınlaşmasından kaynaklandığı rapor edilmiştir. İlginç bir veri olarak 2024 yılı itibariyle tüm phishing e-postalarının %82,6'sının bir şekilde yapay zekâ teknolojisi kullanılarak hazırlandığı belirtilmektedir. Bu oran neredeyse her 10 oltaalama e-postasından 8'inin yapay zekâ eliyle üretildiğini göstermektedir ki suçluların bu teknolojiyi ne derece benimsediğine dair çarpıcı bir göstergedir.

Bir diğer önemli istatistik alanı deepfake sahtekârlıklarıdır. Avrupa Parlamentosu'nun 2025 yılında paylaştığı verilere göre, 2023 yılında Avrupa Birliği genelinde yaklaşık 500 bin adet deepfake paylaşımı yapılmışken, 2025 yılında bu sayının 8 milyon gibi inanılmaz bir seviyeye çıkacağı öngörülmektedir. Bu, sadece iki yıl içinde deepfake içerik yayılımında %1500'ün üzerinde bir artış anlamına gelir. Finans sektörüne ilişkin bir araştırmada, 2024 itibariyle finans profesyonellerinin %53'ünün en az bir deepfake dolandırıcılık girişimiyle karşılaştığı ortaya konmuştur. Yine 2025'in ilk çeyreğinde, tüm 2024 yılı boyunca görülenlerden %19 daha fazla deepfake olayı rapor edilmiştir. Bu veriler, deepfake yönteminin geometrik biçimde yayıldığını ve suçlular için popüler bir araç haline geldiğini göstermektedir.

Ses klonlama dolandırıcılıklarına ilişkin bir anket ise, dünya genelinde her 10 yetişkinden 1'inin bir yapay zekâ ses sahtekarlığı girişimi yaşadığını; bu tuzağa düşenlerin %77'sinin para kaybına uğradığını ortaya koymuştur. Bu denli yüksek bir mağduriyet oranı, konunun ciddiyetini sayılarla desteklediği görülecektir.

Siber güvenlik ekonomisi açısından bakarsak, yapay zekânın kötüye kullanımıyla tırmanan suçların dünya ekonomisine maliyeti muazzam boyutlara ulaşmaktadır. Yapay zekâ destekli saldırılar bu mali yükün önemli bir bileşenidir; zira bir saldırganın aynı anda binlerce hedefe özelleştirilmiş saldırı yapmasına imkân tanıyan yapay zekâ araçları, suçun ölçeğini büyütmektedir. Ulusal Suç Ajansları ve Interpol gibi kuruluşlar, 2027'ye kadar suç örgütlerinin yapay zekâyı daha yoğun kullanacağı ve kolluk kuvvetlerinin yapay zekâ ile desteklenmiş suçlara karşı hazırlık yapması gerektiği yönünde raporlar yayınlamaktadır.

Türkiye özelinde resmi veriler henüz yapay zekâ bağlantılı suç istatistiklerini detaylandırmaya da yukarıda belirtilen küresel eğilimlerin ülkemize de yansıdığı aşîkârdır. Adli makamların önüne gelmeye başlayan yapay zekâ kaynaklı mağduriyet dosyaları bunun bir kanıtıdır. Ayrıca bilişim suçlarıyla ilgili genel veriler, 2020'lerden itibaren Türkiye'de soruşturma sayılarının

ciddi biçimde arttığını ortaya koymaktadır. Bu artışta yapay zekâ gibi yeni teknolojilerin kötüye kullanımının etkili olduğu değerlendirilmektedir.

Toparlamak gerekirse, istatistiksel veriler yapay zekânın suç oranları üzerindeki etkisinin giderek büyüdüğünü göstermektedir. Gerek ülkemizde gerek dünyada, suçlular yapay zekâdan yoğun şekilde faydalanmakta; bu da bazı suçların sayısında ve niteliğinde artışa yol açmaktadır. Bununla mücadele etmek için güvenlik birimleri ve yasa koyucular, stratejilerini veriye dayalı olarak güncelleme yoluna gitmesi gerekecektir.

6. Sonuç ve Değerlendirme: Hukuk Sistemine Yönelik Öneriler

Yapay zekânın suç oranlarına ve ceza hukuku sorumluluğuna etkisi üzerine yapılan bu inceleme, teknolojik gelişmeler karşısında hukuk sistemimizin bir yol ayrımında olduğunu ortaya koymaktadır. Mevcut durumda yapay zekâlar hukuken sorumlu tutulamayan araçlar konumundadır ve suçların failleri insanlar olarak kabul edilmeye devam etmektedir. Ancak yapay zekâların becerileri arttıkça ve toplumsal hayattaki rolleri derinleştikçe, ceza hukuku başta olmak üzere hukuk düzenimizin bazı kavramlarında revizyonlar yapılması gerekecektir. Aşağıda elde edilen bulgular ışığında genel bir değerlendirme yapılmakta; Doç. Dr. Ramazan Arıtürk ile birlikte yürütülen değerlendirme süreci kapsamında hukuk sistemimize yönelik bazı öneriler ortaya konulmaktadır.

- **Mevzuatın Güncellenmesi ve Açık Hükümler Konulması:** Türk Ceza Kanunu ve ilgili ceza mevzuatı, yapay zekâ çağının getirdiği yeni durumları karşılamak üzere güncellenmelidir. Özellikle TCK'nın genel hükümlerine, yapay zekâ kullanılarak suç işlenmesine dair açıklayıcı hükümler eklenebilir. Örneğin suça iştirak düzenlemelerinde (TCK md. 37-40 arası) yapay zekâ kullanımıyla ilgili bir madde fıkrası konularak, “bir fiilin icrasında yapay zekâ sistemini araç olarak kullanan kimse doğrudan fail sayılır” gibi bir ibare eklenmesi düşünülebilir. Bu aslında zaten öğreti ve içtihatla varılan sonucu kanun seviyesinde netleştirerek hukuki belirliliği artıracaktır. Ayrıca taksirli suçlar bakımından, yapay zekâ uygulamalarında gerekli özeni göstermeyen üretici veya işletmecilerin sorumluluğunu belirginleştirecek ifadeler yer alabilir. Örneğin TCK md. 22’de taksir tanımına “yapay zekâ destekli sistemlerin sevk ve idaresinde beklenen dikkat ve özen yükümlülüğüne aykırı davranmak da taksir sayılır” gibisinden bir cümle eklenebilir. Bu tarz güncellemeler, ileride karşılaşılabilecek muhtemel olaylarda yargıya kılavuzluk edecektir.
- **Özel Yasa İhtiyacı (Dijital Teknolojiler Kanunu):** Ceza Kanunu’ndaki revizyonların yanı sıra, özel bir kanun çıkarılması da gündeme gelebilir. Bu ihtiyaca cevap vermek üzere kapsamlı bir yasa hazırlanabilir. Bu kanunda yapay zekânın tanımı yapılmalı, hangi sektörlerde nasıl kullanılacağına dair temel ilkeler konmalı, hak ihlallerine karşı hızlı müdahale prosedürleri getirilmelidir. Örneğin deepfake içeriklerin çevrim içi yayılmasına karşı sulh ceza hakiminin 24 saat içinde erişim engeli kararı vermesi gibi hızlandırılmış usuller öngörülebilir. Ayrıca bu kanunla, yapay zekâ geliştiricileri ve sağlayıcıları için kayıt ve şeffaflık yükümlülükleri getirilebilir. Avrupa Birliği’nin 2024’te yürürlüğe koymayı planladığı Yapay Zekâ Yasası (AI Act) bu konuda örnek alınabilir. AI Act, yapay zekâ sistemlerini risk seviyelerine göre sınıflandırıp yüksek

riskli sistemlere sıkı denetim ve şeffaflık şartları getiriyor; deepfake gibi üretimlerde içeriğin yapay zekâ ile üretildiğine dair etiket zorunluluğu koyuyor. Türkiye de benzer şekilde yapay zekâ ürünlerinin etiketlenmesini ve denetimini zorunlu kılabilir. Bu sayede, en azından dolaşıma giren yapay içeriklerin tespiti kolaylaşacak ve kötüye kullanım bir nebze dizginlenecektir.

- **Kolluk ve Yargının Teknik Kapasitesinin Artırılması:** Yapay zekâ çağında suçla mücadele edebilmek için bizzat kolluk kuvvetlerinin ve yargı mercilerinin de yapay zekâdan yararlanması gerekecektir. Emniyet teşkilatında siber suç birimleri halihazırda var ancak daha ileri gitmek, yapay zekâ destekli analiz araçlarını devreye sokmak gerekiyor. Örneğin İzmir Emniyet Müdürlüğü bünyesinde kurulan Suç Analiz Merkezi'nde, yapay zekâ destekli yazılımlar ve görüntü inceleme sistemleriyle kentteki olaylar tüm yönleriyle ele alınmaya başlanmıştır. Bu gibi projeler ülke genelinde yaygınlaştırılmalı; polis, savcı ve hakimlere yapay zekâ farkındalığı kazandırılmalıdır. Adli teşkilat içinde *dijital delil ve yapay zekâ birimleri* oluşturulabilir. Yargıda da hâkim ve savcılara yapay zekâ konusunda hizmet içi eğitimler düzenlenmeli, adli yargılamada karşılarına gelecek bu tür meselelere hazırlıklı olmaları sağlanmalıdır.
- **Uluslararası İşbirliği ve Evrensel Standartlar:** Yapay zekâ aracılığıyla işlenen suçlar çoğu zaman sınır aşan niteliktedir. Bir deepfake video farklı ülkelerden sunucular aracılığıyla yayılabilir, fail başka bir ülkede bulunabilir. Bu nedenle uluslararası hukuk düzeyinde işbirliği şarttır. Türkiye, uluslararası inisiyatiflere aktif katılım göstermelidir. Örneğin Avrupa Konseyi Siber Suçlar Sözleşmesi'ne (Budapeşte Sözleşmesi) ek olarak yapay zekâ ile ilgili protokoller hazırlanıyorsa, bunlara taraf olmak ülkemizin faydasına olacaktır.
- **Etik ve Farkındalık Çalışmaları:** Son olarak, yapay zekâ ve suç ilişkisine dair mücadele sadece kanun ve kolluk ile sınırlı kalmaz; toplumsal farkındalık ve etik kullanım kültürü çok önemlidir. Vatandaşların yapay zekâ ile üretilen içeriklere karşı bilinçlendirilmesi gerekir. Örneğin sosyal medyada gördükleri çarpıcı bir videonun deepfake olabileceğini bilmeleri, şüpheli yaklaşımları sağlanmalıdır. Bu amaçla kamu spotları, eğitim programları düzenlenebilir.

Sonuç olarak, yapay zekânın suç oranlarına etkisi meselesi, teknolojik, hukuki ve toplumsal boyutlarıyla ele alınması gereken karmaşık bir konudur. Bu incelemede görüldüğü üzere, yapay zekâ giderek artan biçimde suç amaçlı kullanılabilen, bu da suçların sayısını ve niteliğini etkilemektedir. Ancak hukukun caydırıcılık ve düzen sağlama işlevini sürdürebilmesi için, teknolojik gelişmelere proaktif uyum göstermesi şarttır. Yapay zekâ alanında karşı karşıya olduğumuz riskler, hukuk sistemimizin gerek ceza hukuku gerekse diğer hukuk dallarında bazı reformlara gitmesini zorunlu kılmaktadır.

Son tahlilde, yapay zekâ insanlığın bir ürünüdür ve kontrolü insandadır; dolayısıyla suçla mücadelede de nihai sorumluluk biz insanlardadır. Hukuk, insan onurunu ve toplumsal düzeni koruma misyonunu teknolojik çağda da sürdürecektir. Araçları bulmak zorundadır. Bu yolda atılacak adımlar, sadece suç oranlarını düşürmekle kalmayıp yapay zekâyı duyulan güveni de pekiştirecek, bu güçlü teknolojinin barışçıl ve yararlı amaçlar için kullanımını teşvik edecektir.

Kaynakça:

1. Berrin Akbulut, “Yapay Zekâ ve Ceza Hukuku Sorumluluğu,” *Ankara Hacı Bayram Veli Hukuk Fakültesi Dergisi*, C. XXVII, S.4 (2023)
2. Hakan Aksoy, “Yapay Zekâlı Varlıklar ve Ceza Hukuku,” *International Journal of Economics, Politics, Humanities & Social Sciences*, C.4, S.1 (2021)
3. Mesut H. Caşın vd., “Yapay Zekâ ve Robotların Eylemlerinden Kaynaklanan Cezai Sorumluluk Sorunu,” *Ankara Barosu Dergisi*, 2021/1
4. “Yapay zekâ uygulaması Grok’un paylaşımları hakkında soruşturma” haberi, *Anadolu Ajansı*, 9 Temmuz 2025
5. KPMG Türkiye, “Yapay Zekâ Destekli Siber Saldırlara Bakış,” Eylül 2025 Raporu
6. Tech-Adv, “AI Cyber Attack Statistics 2025” (Çevrimiçi Blog)