Yapay Zekâ Destekli Suç Tahmin Sistemleri: Uygulamadaki Sorunlar ve Hukuki Boyut

Niyazi Umut Akıncıoğlu*

Öz

Bu makale, yapay zekâ destekli suç tahmin sistemlerinin işleyişini, uygulamadaki performansını ve doğurduğu hukuki ve etik sorunları çok boyutlu biçimde incelemektedir. Yer ve kişiye dayalı modeller ekseninde geliştirilen bu sistemler, suçu önceden tahmin ederek güvenlik stratejilerinde proaktif bir dönüşüm vadetmektedir. Ancak algoritmik önyargılar, "kara kutu" sistemlerin şeffaflık sorunları ve temel hak ihlalleri gibi riskler, bu teknolojilerin hukuk devleti ilkeleriyle uyumunu tartışmalı kılmaktadır. ABD, AB ve Türkiye'deki uygulamalar karşılaştırmalı olarak analiz edilerek, her biri için farklı normatif ve kurumsal yaklaşımlar ortaya konulmuştur. Özellikle Avrupa Birliği'nin önleyici ve kuralcı modeli ile ABD'nin reaktif ve yargı temelli yaklaşımı arasındaki farklara dikkat çekilmiştir. Türkiye'nin ise hâlen yasal çerçeve eksikliği içinde bulunduğu ve bu alanda kapsamlı bir düzenleme ihtiyacı olduğu vurgulanmaktadır.

Anahtar Kelimeler: Yapay Zekâ, Güvenlik, Suç Tahmin Sistemleri, Hukuki Denetim.

AI-Supported Crime Prediction Systems: Practical Challenges and Legal Aspects

Abstract

This article offers a multidimensional analysis of the operational mechanisms, practical performance, and legal as well as ethical implications of artificial intelligence-based crime prediction systems. These systems, developed along the axes of location-based and person-based models, promise a proactive transformation in security strategies by forecasting criminal activity. However, risks such as algorithmic bias, the opacity of "black box" systems, and violations of fundamental rights raise critical questions regarding their compatibility with the principles of the rule of law. The article presents a comparative assessment of implementations in the United States, the European Union, and Turkey, revealing distinct normative and institutional approaches. Particular attention is given to the contrast between the EU's preventative and regulatory model and the US's reactive, judiciary-driven framework. It is further emphasized that Turkey currently lacks a comprehensive legal framework in this area and urgently needs specific regulatory arrangements.

Keywords: Artificial Intelligence, Security, Crime Prediction Systems, Legal Oversight.

*Dr. Öğr. Üyesi | Polis Akademisi | umutakincioglu@gmail.com
ORCID: 0000-0002-4605-6195 | DOI: 10.36484/liberal.1749671
Liberal Düşünce Dergisi, Yıl: 30, Sayı: 120, Güz 2025, ss. 81-102.
Gönderim Tarihi: 24 Temmuz 2025 | Kabul Tarihi: 28 Ekim 2025

Giriş

Son yıllarda büyük veri ve makine öğrenmesi teknolojilerindeki gelişmeler, güvenlik güçlerinin suçla mücadelede daha öngörücü ve proaktif yaklaşımlar benimsemelerine olanak tanımıştır. Bu gelişmelerin en dikkat çekici örneklerinden biri, yapay zekâ destekli suç tahmin sistemleridir. Bu sistemler, geçmiş suç verilerini analiz ederek, gelecekte nerede ne zaman ve ne tür suçların meydana gelebileceğini tahmin etmeyi amaçlamaktadır. Amerika Birleşik Devletleri, Birleşik Krallık ve Almanya gibi ülkelerde yerel polis teşkilatları tarafından deneyimlenmiştir (Perry, 2013; Ferguson, 2017).

Ancak bu sistemlerin etkinliğine ve etik boyutlarına ilişkin akademik tartışmalar, uygulamaların yaygınlaşmasından daha hızlı bir şekilde artış göstermektedir. Yapay zekâ temelli bu sistemlerin verimliliği üzerine yapılan çalışmalar, çelişkili sonuçlar ortaya koymaktadır. Bazı araştırmalar, bu sistemlerin belirli bölgelerdeki mükerrer suçları azaltmada kısa vadeli katkılar sağladığını öne sürerken (Mohler ve ark., 2015), diğerleri bu sistemlerin sistematik önyargıları yeniden ürettiğini ve "ön yargılı polislik" (biased policing) pratiklerine zemin hazırladığını savunmaktadır (Lum ve Isaac, 2016). Büyük veri, makine öğrenmesi ve yapay zekâ alanında yaşanan gelişmeler, suçla mücadelede reaktif yöntemlerden proaktif yöntemlere geçişi hızlandırmıştır. Bu bağlamda öngörücü polislik sistemleri, geçmiş suç verilerini analiz ederek gelecekteki potansiyel suçları tahmin etmeyi amaçlamaktadır (Meijer ve Wessels, 2019). Ancak literatür, bu sistemlerin etkinliği ve etik sonuçları konusunda ciddi tartışmalar barındırmaktadır.

Bir yandan çalışmalar, öngörücü polisliğin suç oranlarını azaltabileceğini iddia etmektedir (Mohler ve ark., 2015). Öte yandan, algoritmaların önyargılı verilerle eğitilmesi, özellikle sosyoekonomik açıdan dezavantajlı grupların orantısız biçimde hedef alınmasına yol açabilmektedir (Lum ve Isaac, 2016; Meding, 2025). Bu durum, toplumsal eşitlik ve adalet ilkeleriyle bağdaşmayan bir "algoritmik ayrımcılık" pratiği ortaya çıkarmaktadır (Maviş, 2025). Bu bağlamda, sistemlerin nicel başarı ölçütleri kadar, sosyal adalet ilkeleriyle ne denli uyumlu oldukları da önem kazanmaktadır. Ülkeler arası uygulama örnekleri incelendiğinde, her ülkenin güvenlik kültürü, veri koruma mevzuatı ve kurumsal altyapısına göre farklı uygulama biçimlerinin ortaya çıktığı görülmektedir.

Bu makalede, yapay zekâ destekli suç tahmin sistemlerinin işleyiş verimliliği ve hukuki etkileri çok boyutlu bir yaklaşımla ele alınacaktır. Öncelikle sistemlerin teknik temelleri ve uygulamadaki performansları değerlendiri-

lecek; ardından ABD, AB ve Türkiye örnekleri üzerinden karşılaştırmalı bir uygulama analizi yapılacaktır. Son olarak, algoritmik tarafsızlık, kişisel verilerin korunması, öngörüye dayalı cezalandırma riski ve adil yargılanma hakkı gibi hukuki sorunlar tartışılarak, bu sistemlerin demokratik hukuk devletleri bağlamındaki meşruiyet sınırları ortaya konulacaktır.

Yapay Zekâ Destekli Suç Tahmin Sistemlerinin Tanımı ve Tarihsel Gelişimi

Yapay zekâ (YZ) destekli suç tahmin sistemleri, literatürde sıklıkla "öngörücü polislik" kavramı altında ele alınmaktadır. Bu sistemler, suçun nerede, ne zaman ve hangi koşullarda işlenebileceğine dair olasılıksal öngörülerde bulunmak amacıyla geniş ölçekli veri setlerinin istatistiksel ve algoritmik yöntemlerle analiz edilmesine dayanmaktadır. Geliştirildikleri bağlamda, kolluk kuvvetlerinin sınırlı operasyonel kaynaklarını daha etkin biçimde kullanabilmelerini sağlamak ve suç işlenmeden önce müdahale edebilme kapasitesini artırmak üzere tasarlanmış proaktif güvenlik stratejilerinin bir unsuru olarak değerlendirilmektedir (Meijer ve Wessels, 2019). Bu nedenle yapay zekâ tabanlı tahmin sistemleri, yalnızca teknik bir yenilik olarak değil, polisliğin doğasını reaktif bir suç müdahale pratiğinden önleyici ve risk temelli bir güvenlik anlayışına taşıyan kurumsal bir dönüşümün göstergesi olarak da yorumlanmaktadır (Çetinkaya, 2024).

Öngörücü polislik uygulamalarının tarihsel kökeni, 1990'lı yıllarda Avrupa'da gelişen ve veri analizi ile istihbarat toplamayı karar alma süreçlerinin merkezine yerleştiren "istihbarat temelli polislik" modeline dayanmaktadır. Bu model, polisin rutin veri toplama faaliyetlerini daha sistematik hale getirmiş, risk analizini öne çıkarmış ve suçla mücadelede proaktif stratejilere olan ihtiyacı artırmıştır. Ancak günümüzde kullanılan sistemlerin asıl ivme kazanmasında etkili olan faktörlerden biri, 2008 küresel ekonomik krizinin ardından güvenlik kurumlarının karşı karşıya kaldığı ciddi bütçe kısıtlamalarıdır. Bu süreçte "daha az kaynakla daha fazla hizmet" üretme zorunluluğu, kolluğu yeni teknolojilere yöneltmiş; makine öğrenmesi ve büyük veri analitiğindeki gelişmelerle birleşerek, bugünkü yüksek kapasiteli yapay zekâ destekli suç tahmin sistemlerinin gelişmesine zemin hazırlamıştır (Van Brakel, 2025).

Bu bağlamda öngörücü polislik, salt bir teknolojik gelişme olarak değil, kolluk stratejilerinde paradigmatik bir dönüşüm olarak da görülmelidir. Polis teşkilatları uzun süredir suç verilerini kullanarak riskli bölgeleri tespit etmekteydi; ancak yapay zekâ algoritmaları bu süreci daha kapsamlı, daha hızlı ve otomatik bir hale getirmiştir (Egbert ve Leese, 2021). Özellikle coğra-

fi bilgi sistemleri (CBS) ve "sıcak nokta" (hot spot) analizleri ile başlayan suç coğrafyası araştırmaları, Türkiye'de de 2000'li yıllardan itibaren literatürde yer almaya başlamıştır (Başaran, 2021).

Günümüzde ise bu yaklaşım, derin öğrenme tabanlı modellerle birleşerek suçun yalnızca mekânsal değil, zamansal boyutlarının da öngörülmesine olanak sağlamaktadır (Utku, 2024). Dolayısıyla tarihsel gelişim ile güncel uygulamalar arasında kesintisiz bir süreklilik göze çarpmaktadır. Bununla birlikte, öngörücü polislik sistemlerinin işleyişi çoğu zaman "tahmin" kavramının çağrıştırdığı kesinlik algısından oldukça farklıdır. Bu sistemler, geleceği mutlak doğrulukla öngörmekten ziyade, geçmiş verilerdeki istatistiksel kalıpları ve korelasyonları analiz ederek belirli olasılıkları hesaplamaktadır. Örneğin, derin öğrenme tabanlı modeller belirli bir olayın tekrar etme olasılığını ölçebilirken (Utku, 2024), doğal dil işleme yöntemleri suç raporlarından elde edilen metinsel verileri işleyerek suç tiplerini sınıflandırabilmektedir (Çolakoğlu, 2024). Bu durum, tahmin sistemlerinin yalnızca coğrafi verilerle sınırlı kalmayıp çok katmanlı, hibrit veri yapıları üzerine inşa edildiğini göstermektedir. Buna karşın, "öngörücü polislik" kavramı kimi zaman bu sistemlerin yeteneklerini olduğundan daha bilimsel ve güvenilir gösteren bir söylem aracı olarak da kullanılmaktadır (Bachner, 2013).

Türkçe literatürde öne çıkan eleştirilerden biri, bu sistemlerin önyargılı veri setlerine dayanması ve bunun ayrımcılık riskini artırmasıdır (Çetinkaya, 2024). Özellikle bireylerin geçmiş suç kayıtlarının veya belirli bölgelerin sürekli yüksek riskli kategorisine sokulması, bazı toplumsal grupların adeta "daimî şüpheli" konumuna itilmesine yol açabilmektedir. Bu noktada Yücel (2024), öngörücü polislik sistemlerinden elde edilen çıktıların hukuki süreçlerde somut delil niteliği taşıyıp taşımayacağına ilişkin belirsizliklere dikkat çekmekte ve bunun ciddi bir hukuki sorun alanı oluşturduğunu vurgulamaktadır. Sonuç olarak öngörücü polislik, yalnızca teknolojik bir araç olarak değil, aynı zamanda etik, hukuki ve toplumsal tartışmaların merkezinde yer alan bir olgu olarak değerlendirilmelidir. Bu sistemlerin yapısal belirsizlikleri ve metodolojik sınırlılıkları çoğu zaman geri planda bırakılmakta hem politika yapıcılar hem de kamuoyunda aşırı bir güven ortamı oluşabilmektedir. Nitekim Chicago ve Los Angeles gibi büyükşehirlerde milyonlarca dolarlık yatırımlara rağmen programların etkisiz bulunarak sonlandırılması, bu tür sistemlerin pratikte nasıl sorunlara yol açabileceğini açıkça göstermektedir (Richardson ve ark., 2019).

Türkiye'de yapılan araştırmalarda da algoritmaların şeffaflık, denetlenebilirlik ve toplumsal meşruiyet sorunlarının öne çıktığı görülmektedir (Yücel,

2024). Dolayısıyla tarihsel gelişim ile güncel uygulamaların birlikte değerlendirilmesi, öngörücü polislik teknolojilerinin geleceğine ilişkin daha gerçekçi ve eleştirel bir perspektif sunmaktadır.

Temel Modeller: Yere Dayalı ve Kişiye Dayalı Modeller

Öngörücü polislik sistemleri, odaklandıkları hedefe göre temel olarak iki ana kategoriye ayrılır:

- **Yere Dayalı (Place-Based) Modeller:** Öngörücü polislik uygulamaları içerisinde en yaygın biçimde kullanılan model türü yere dayalı modeldir. Bu yaklaşımda sistem, suçun türü, zamanı ve mekânsal dağılımı gibi tarihsel verileri analiz ederek belirli coğrafi bölgelerin gelecekteki suç riskini öngörmeye çalışır. Modelin temel amacı, polis devriye faaliyetlerini bu yüksek riskli alanlara ve zaman dilimlerine odaklayarak suç oranlarını caydırma yoluyla azaltmaktır. Bu modelin en bilinen uygulamalarından biri, ABD merkezli PredPol şirketi (günümüzde Geolitica olarak yeniden adlandırılmıştır) tarafından geliştirilen yazılımdır (Braga ve ark., 2014).
- **Kişiye Dayalı (Person-Based) Modeller:** Bu model türü, bireylerin ya da belirli sosyal grupların gelecekte suç işleme (fail olma) ya da bir suçun mağduru olma olasılıklarını değerlendirmeye yönelik olarak tasarlanmıştır. Söz konusu sistemler, geçmiş tutuklama kayıtları, bilinen suçlularla olan sosyal ilişkiler, demografik özellikler ve sosyal ağ analizleri gibi son derece hassas ve kişisel verileri kullanmaktadır. Bu tür modeller tarafından oluşturulan "risk skorları", yalnızca polis müdahalelerini yönlendirmekle kalmayıp; kefalet kararları, şartlı tahliye değerlendirmeleri ve ceza belirleme süreçleri gibi çeşitli adli karar mekanizmalarında da doğrudan etkili olabilmektedir (Warso, 2022). Amerika Birleşik Devletleri'nde sanıkların yeniden suç işleme riskini ölçmek amacıyla kullanılan COMPAS (Correctional Offender Management Profiling for Alternative Sanctions) yazılımı, kişiye dayalı modellerin en çok tartışılan örneklerinden biri olarak öne çıkmaktadır.

Bu iki ana modelin yanı sıra, organize suç şebekelerini, terör hücrelerini ve bu yapılar içindeki kilit aktörleri belirlemek için sosyal ağ analizi gibi teknikleri kullanan "grup veya ağ tabanlı" modeller de bulunmaktadır (Tayebi, 2016).

Suçla Mücadelede Reaktif Yaklaşımdan Proaktif Yaklaşıma Geçişin Avantajları ve Dezavantajları

Öngörücü polisliğin temel iddiası, suçla mücadele süreçlerinde etkinlik, verimlilik ve tarafsızlık sağlamaktır (Kavsıracı ve Demirbaş, 2020). Bu yaklaşımın savunucuları, büyük veri setlerinin insan kapasitesini aşan hız ve doğrulukla işlenebilmesi sayesinde kolluk kuvvetlerinin kaynaklarını en uygun

zaman ve mekânda yoğunlaştırabileceğini, böylelikle suç oranlarında kayda değer bir düşüş sağlanabileceğini ileri sürmektedir (Tufan, 2024). Ancak öngörücü polislik, yalnızca teknik bir imkân değil; aynı zamanda ciddi etik ve hukuki tartışmaları da beraberinde getirmektedir. Bu tartışmaların başında, söz konusu sistemlerin "suç öncesi" müdahaleleri meşrulaştırma riski gelmektedir. Zira klasik ceza adaleti sistemi, bireyleri ancak fiil gerçekleştiğinde ve somut deliller üzerinden sorumlu tutarken; öngörücü polislik, henüz gerçekleşmemiş olası eylemler üzerinden müdahale öngörmekte ve böylece ceza hukukunun temel paradigmasını zorlamaktadır.

Bu durum, bireylerin yalnızca istatistiksel olasılıklara dayanılarak, somut şüphe bulunmaksızın kolluk müdahalesine maruz bırakılması anlamına gelebilir. Böyle bir ihtimal, masumiyet karinesi, lekelenmeme hakkı ve özel hayatın gizliliği gibi hukuk devletinin en temel güvencelerini zedeleme potansiyeline sahiptir (Tufan, 2024; Çetinkaya, 2024). Bu bağlamda Avrupa Birliği'nin 2024 yılında kabul ettiği Yapay Zekâ Yasası (EU AI Act) kritik bir dönüm noktası olarak görülmektedir. Yasa, kolluk kuvvetlerinin kullanımına sunulan öngörücü polislik sistemlerini "yüksek riskli uygulamalar" kategorisine dahil ederek şeffaflık, hesap verebilirlik, insan denetimi ve ayrımcılık yasağı gibi yükümlülükler getirmiştir (European Parliament, 2024). Böylelikle yalnızca teknolojik faydaların değil, aynı zamanda temel hak ve özgürlüklerin de güvence altına alınması hedeflenmiştir. Türk literatüründe ise benzer tartışmaların özellikle öngörücü polislik çıktılarının delil değeri, idarenin hukuki sorumluluğu ve mevcut belirsizlikler çerçevesinde şekillendiği görülmektedir (Yücel, 2024).

Teknolojinin Etik İkilemleri

Algoritmik Adaletsizlik

Öngörücü polislik sistemlerine yöneltilen en temel etik eleştirilerden biri, algoritmik önyargının sistematik biçimde yeniden üretilmesidir. Yapay zekâ tabanlı sistemler, önyargılı verilerle eğitildiklerinde dezavantajlı grupları orantısız biçimde hedef alma eğilimi göstermektedir. Nitekim ABD'de kullanılan COMPAS sistemi, siyah sanıkları beyazlara kıyasla yaklaşık iki kat daha yüksek oranda "yüksek riskli" kategorisine yerleştirmiştir (Angwin ve ark., 2022). Bu sonuç, yalnızca ABD hukuk düzeninde güvence altına alınan eşit koruma ilkesine değil, aynı zamanda Avrupa Birliği hukukunda açıkça yer verilen ayrımcılık yasağına da aykırı bir tablo ortaya koymaktadır (Meding, 2025). Bunun temelinde, suç kayıtlarının nesnel toplumsal suç dağılımını

değil, kolluk kuvvetlerinin uygulamalarını, operasyonel önceliklerini ve tarihsel olarak kökleşmiş kurumsal önyargıları yansıtması yatmaktadır (Lum ve Isaac, 2016).

Özellikle ABD bağlamında değerlendirildiğinde, ırksal azınlıkların ve düşük gelir gruplarının yaşadığı mahalleler tarihsel süreçte daha yoğun polis gözetimine maruz kalmış; bu "aşırı polislik" (over-policing) uygulamaları küçük ölçekli suçlarda tutuklama oranlarını artırarak söz konusu bölgelerin verisel anlamda suçla "doygun" hale gelmesine yol açmıştır (Vitale, 2021). Yanlı verilerle beslenen algoritmalar, bu mahalleleri sistematik biçimde daha "riskli" olarak işaretlemektedir. Ortaya çıkan bu "geri besleme döngüsü" (feedback loop), mevcut eşitsizlikleri yeniden üreten bir mekanizma yaratmaktadır (Lum ve Isaac, 2016). Algoritma, belirli bir bölgeyi yüksek riskli alan olarak tanımladığında kolluk kuvvetleri o bölgede daha yoğun devriye faaliyetinde bulunmakta, artan polis varlığı daha fazla suç kaydına yol açmakta ve bu yeni veri tekrar algoritmaya entegre edilmektedir. Böylelikle ilk tahmin, doğrulanmış gibi görünerek pekişmekte; önyargılı etiketleme ise giderek kurumsallaşmaktadır.

Bu bağlamda COMPAS sistemi, algoritmik önyargının somut sonuçlarını en açık biçimde ortaya koyan örneklerden biridir. Yapılan bağımsız analizler, sistemin siyah sanıkları beyaz sanıklara kıyasla neredeyse iki kat daha fazla oranda hatalı biçimde "yüksek riskli" olarak değerlendirdiğini göstermektedir (Angwin ve ark., 2022). Bu bulgu, öngörücü teknolojilerin iddia edilen tarafsızlık ve nesnellik iddialarının ne denli kırılgan olduğunu ve adalet sistemi üzerinde yaratabileceği yıkıcı etkileri ortaya koymaktadır. Benzer şekilde, Türkiye'de yapılan çalışmalar da algoritmik önyargı sorununa dikkat çekmekte; özellikle önyargılı veri setlerinden doğan ayrımcılık ihtimalinin hukuki sorumluluk yaratabileceğini vurgulamaktadır (Çetinkaya, 2024; Yücel, 2024).

Dijital Damgalama ve Ayrımcılık Tehlikesi

Öngörücü polislik sistemleri, bireylerin ya da toplulukların herhangi bir somut eylemleri bulunmaksızın, yalnızca istatistiksel profillere dayanarak "potansiyel suçlu" olarak etiketlenmesine yol açabilecek ciddi bir risk taşımaktadır. Bu durum, ceza hukukunun en temel ilkelerinden biri olan masumiyet karinesini ihlal etmenin yanı sıra, bireyin haksız suç isnadıyla ilişkilendirilmemesini güvence altına alan lekelenmeme ilkesini de zedelemektedir (Alikhademi, 2022; Çetinkaya, 2024). Bu bağlamda ortaya çıkan "dijital damgalama" olgusu, belirli bölgelerde yaşayan veya belirli demografik gruplara mensup bireylerin sürekli şüphe ve gözetim altında tutulmasına yol açmak-

tadır. Literatürde bu süreç, özellikle dezavantajlı grupların veri temelli politikalar aracılığıyla dışlanmasını tanımlayan "digital redlining" kavramıyla açıklanmaktadır (Ensign ve ark., 2018).

Geleneksel ceza adaleti sistemlerinde şüphe, somut olgulara ve bireysel davranışlara dayanırken; öngörücü polislik uygulamaları şüpheyi bireysel fiilden istatistiksel kimliğe kaydırmaktadır. Böylelikle birey, fiili davranışları nedeniyle değil; yaşadığı yer, kimliği veya ait olduğu grubun istatistiksel özellikleri üzerinden şüpheli hale gelebilmektedir. Bu yaklaşım, bireysel sorumluluk ilkesini zayıflatarak "olasılıksal ceza" veya "grup temelli suçluluk" anlayışına zemin hazırlamaktadır (Marciniak, 2023).

Avrupa Birliği'nin 2024 yılında kabul ettiği Yapay Zekâ Yasası (EU AI Act), bu risklere karşı kapsamlı bir hukuki çerçeve oluşturmayı hedeflemektedir. Yasa, kolluk kuvvetleri tarafından kullanılan öngörücü polislik sistemlerini "yüksek riskli uygulamalar" kategorisine dahil ederek şeffaflık, insan gözetimi, denetlenebilirlik ve ayrımcılık yasağı gibi yükümlülükler öngörmüştür (European Parliament, 2024). Böylece bireylerin yalnızca istatistiksel olasılıklara dayalı olarak sürekli gözetim altında tutulmalarının önlenmesi amaçlanmaktadır. Türkiye'de de benzer şekilde, yapay zekâ destekli tahmin sistemlerinin hukuki dayanağındaki belirsizlikler ve ayrımcılık riskleri tartışılmakta; özellikle lekelenmeme hakkı ile masumiyet karinesinin korunmasının zorunluluğu vurgulanmaktadır (Yücel, 2024).

"Kara Kutu" Sorunu

Öngörücü polislik sistemlerinin önemli bir bölümü, özel şirketler tarafından geliştirilen ve ticari sır kapsamında korunan tescilli algoritmalara dayanmaktadır. Bu durum, söz konusu algoritmaların hangi verileri nasıl işlediğinin ne kamuoyunca ne de çoğu zaman kolluk görevlilerince bilinmesine yol açmakta; literatürde "kara kutu" olarak tanımlanan bu şeffaflık eksikliğini doğurmaktadır (Weiss, 2025). Özellikle bir sanığa atfedilen risk skorunun dayandığı algoritmanın işleyiş mekanizmasının bilinmemesi, bireyin bu değerlendirmeye karşı etkin biçimde savunma yapmasını imkânsız hale getirmekte ve adil yargılanma hakkının temel unsurlarından biri olan "silahların eşitliği" ilkesini ihlal etme potansiyeli taşımaktadır (Popp, 2017; Yücel, 2024).

Şeffaf olmayan algoritmaların ceza muhakemesinde delil olarak kullanılmasının, yargılamanın meşruiyetini zedelemesi kuvvetle muhtemeldir. Etik açıdan bakıldığında ise kara kutu sorunu, ciddi bir hesap verebilirlik boşluğunu beraberinde getirmektedir. Nitekim algoritmaların ürettiği hatalı bir tahmin sonucunda masum bir bireyin haksız yere gözaltına alınması veya tu-

tuklanması durumunda sorumluluğun yazılım geliştiricilere mi, algoritmayı pazarlayan şirkete mi, veriyi sağlayan kamu kurumlarına mı yoksa kararı icra eden kolluk görevlilerine mi ait olduğu belirsiz kalmaktadır (Ensign ve ark., 2018). Bu belirsizlik ortamı, bireysel hataların cezasız kalmasına ve yapısal sorunların göz ardı edilmesine zemin hazırlamaktadır. Dahası, öngörücü sistemler mevcut önyargıları "veri temelli nesnellik" görünümü altında yeniden üreterek ayrımcı uygulamaların görünmezleşmesine ve kurumsallaşmasına katkıda bulunmaktadır (Barocas ve ark., 2023). Literatürde çözüm önerisi olarak Açıklanabilir Yapay Zekâ (XAI) modelleri öne çıkmakta; bu sayede algoritmaların işleyişinin şeffaf, denetlenebilir ve hesap verebilir hale getirilmesi gerektiği savunulmaktadır (Hussain ve Hussain, 2025).

Gözetim Toplumu ve Temel Hakların İhlali

Öngörücü polislik sistemlerinin işleyebilmesi, yalnızca büyük veri kümelerinin varlığına değil, aynı zamanda bu verilerin oldukça geniş bir yelpazeye yayılmış olmasına bağlıdır. Bu kapsamda toplanan veriler, yalnızca resmi suç kayıtları ve adli sicil bilgilerinden ibaret değildir; aynı zamanda sosyal medya paylaşımları, güvenlik kamerası görüntüleri, mali işlem kayıtları, araç plaka tanıma verileri ve bireylerin coğrafi konum bilgileri gibi, kişilerin özel yaşam alanlarına doğrudan temas eden son derece hassas nitelikte kişisel verileri de içermektedir (Brayne, 2017).

Bu denli kapsamlı veri toplama ve analiz süreçleri, toplumsal düzeyde geniş çaplı bir gözetim altyapısının oluşmasına neden olmakta ve bireylerin yaşam alanlarını sürekli denetim altında tutan bir güvenlik rejimini beraberinde getirmektedir. Böyle bir gözetim mekanizması, Anayasa ile güvence altına alınmış olan özel hayatın gizliliği hakkını doğrudan tehdit etmekte ve bireysel mahremiyetin sınırlarını aşındırmaktadır (Richardson ve ark., 2019). Bunun da ötesinde, bireylerin sürekli izlendiği duygusunun içselleştirilmesi, toplumsal davranışlar üzerinde ciddi sonuçlar doğurabilecek bir "caydırıcı etki" yaratabilir (Kavsıracı, 2018). Bu etki, bireylerin herhangi bir suça karışmamış olsalar dahi, yalnızca yanlış anlaşılma ya da istatistiksel olarak şüpheli profillere benzetilme korkusuyla ifade özgürlüğü, toplantı ve gösteri yapma hakkı gibi temel demokratik haklarını kullanmaktan geri durmalarına yol açabilir (Penney, 2017). Bu tür davranışsal oto-sansür, demokratik toplumların temel direklerinden biri olan açık kamusal tartışma ve aktif sivil katılım alanını daraltma riski taşımaktadır.

Uluslararası Hukuki Çerçeve ve Uygulamalar

ABD Yaklaşımı

ABD'de öngörücü polislik teknolojilerine yönelik federal düzeyde kapsamlı bir yasal düzenleme bulunmamaktadır. Tartışmalar ve denetim, büyük ölçüde mevcut Anayasal güvencelerin bu yeni teknolojiler karşısında nasıl yorumlanacağı üzerine odaklanan yargısal süreçler ve sivil toplum eleştirileri üzerinden yürümektedir. Bu tartışmaların merkezinde iki temel anayasa ek maddesi yer almaktadır:

- **Dördüncü Ek Madde:** Amerika Birleşik Devletleri Anayasası'nda yer alan ve bireyleri devletin keyfi ya da "makul olmayan arama ve el koyma" uygulamalarına karşı korumayı amaçlayan temel bir anayasal güvencedir. Öngörücü polislik sistemleri bağlamında yapılan hukuki tartışmaların merkezinde, algoritmaların ürettiği "risk skorlarının" polis memurlarına bir kişiyi durdurmak için gerekli olan "makul şüphe" veya bir arama gerçekleştirmek için gereken "muhtemel sebep" standardını tek başına karşılayıp karşılayamayacağı sorusu yer almaktadır (Ferguson, 2012). Bu sorunun yanıtı, algoritma çıktılarının ceza muhakemesi pratiğinde nasıl konumlandırılacağına ilişkin kritik bir belirsizliğe işaret etmektedir. Eleştirel yaklaşımlar, bir polis memurunun halihazırda sahip olduğu şüpheyi gerekçelendirmek için algoritmik veriye başvurmasının, aynı verinin mükerrer biçimde değerlendirilmesi riskini doğurduğunu vurgulamaktadır. Bu tür bir uygulama, anayasal güvenceleri zayıflatarak bireylerin keyfi polis müdahalesine karşı sahip oldukları koruma düzeyini düşürebilir (Weiss, 2025). Dolayısıyla, algoritmaların hukuki meşruiyeti ve anayasal normlarla uyumluluğu, öngörücü polislik uygulamalarının en tartışmalı ve çözülmesi gereken yönlerinden biri olarak karşımıza çıkmaktadır.
- **On Dördüncü Ek Madde:** Amerika Birleşik Devletleri Anayasası kapsamında tüm bireylere "yasalar önünde eşit koruma" hakkını güvence altına almaktadır. Öngörücü polislik uygulamalarında kullanılan algoritmaların tarihsel olarak yanlı ve önyargılı verilerle eğitilmiş olması, belirli ırksal ve etnik grupların orantısız bir biçimde hedef alınmasına neden olabilmektedir. Bu durum, eşit koruma ilkesinin açık bir ihlali olarak değerlendirilmektedir. Ne var ki, Yüksek Mahkeme'nin 1976 yılında verdiği Washington v. Davis kararında belirlediği içtihat doğrultusunda, bir anayasal eşitlik ihlalinin kanıtlanabilmesi için yalnızca ayrımcı bir etki değil, aynı zamanda ayrımcı bir niyet de ortaya konulmalıdır. Ancak bu bağlamda, öngörücü algoritmaların "objektif", "tarafsız" ve "veri temelli" oldukları yönündeki varsayımsal nitelikleri, bu tür ayrımcı niyetin ispatını son derece güçleştirmektedir (Yang ve Dobbie, 2020).

Algoritmaların arkasında gizli kalmış önyargıların varlığını hukuken ortaya koymak, sistemin teknik doğası ve ticari gizlilik ilkeleri nedeniyle ciddi bir şeffaflık sorunu ile karşı karşıya kalmaktadır. Bu nedenle, On Dördüncü Ek Madde kapsamında anayasal eşitliğin sağlanması, öngörücü polislik sistemleri bağlamında teorik düzeyde savunulabilir görünse de pratikte son derece sınırlı ve tartışmalı bir uygulama alanına sahiptir.

Bu alandaki hukuki tartışmaların yanı sıra, öngörücü polislik sistemlerinin sahadaki uygulama sonuçları da oldukça karmaşık ve çoğu zaman hayal kırıklığı yaratıcı niteliktedir. State v. Loomis davasında Wisconsin Yüksek Mahkemesi, COMPAS gibi risk değerlendirme araçlarının cezai yargılamalarda kullanılabileceğine hükmetmiş; ancak aynı zamanda bu tür sistemlerin şeffaflıktan uzak "kara kutu" niteliği taşıdığı ve potansiyel önyargılar içerdiği gerekçesiyle, yargı mensuplarının kullanım sırasında bu riskler konusunda uyarılması gerektiğini belirtmiştir (Freeman, 2016).

Bu karar, algoritmik değerlendirme araçlarının hukuken tamamen dışlanmadığını, ancak koşullu bir şekilde kabul gördüğünü göstermektedir. Bununla birlikte, pratikte elde edilen sonuçlar sistemlerin etkililiğine dair ciddi soru işaretleri doğurmuştur. Los Angeles, Chicago ve Palo Alto gibi birçok büyükşehir belediyesi ile bağlı polis teşkilatları, öngörücü polislik sistemlerine yapılan milyonlarca dolarlık yatırımlara ve başlangıçta duyulan büyük beklentilere rağmen, bu teknolojilerin suçu azaltma konusunda etkisiz olduğu veya mevcut kurumsal önyargıları daha da derinleştirdiği sonucuna ulaşmıştır. Bu nedenle, birçok program ya tamamen sonlandırılmış ya da ciddi ölçüde sınırlandırılmıştır (Pasquale, 2020). Örneğin, New Jersey eyaletinde yürütülen bir analizde, PredPol (günümüzde Geolitica) tarafından üretilen suç tahminlerinin yalnızca %0.5'inin gerçek anlamda bildirilen suçlarla örtüştüğü tespit edilmiştir (Sankin ve Mattu, 2023). Bu bulgu, öngörücü polislik teknolojileriyle ilgili teorik vaatler ile uygulamadaki somut çıktılar arasında derin bir ayrım ve performans boşluğu olduğunu ortaya koymaktadır.

Avrupa Birliği Yaklaşımı

Amerika Birleşik Devletleri'nin ağırlıklı olarak reaktif ve yargısal denetime dayalı yaklaşımının aksine, Avrupa Birliği (AB), teknolojik sistemleri daha baştan hukuki ve etik çerçeveye oturtmayı hedefleyen proaktif, kapsamlı ve temel hak merkezli bir strateji benimsemiştir. Bu yaklaşım, bireylerin dijital çağdaki hak ve özgürlüklerini korumayı amaçlayan üç temel düzenlemeye dayanmaktadır:

Genel Veri Koruma Tüzüğü (GDPR): Yalnızca AB içerisinde değil, küresel ölçekte de kişisel verilerin işlenmesine ilişkin standartları belirleyen en kapsamlı düzenlemelerden biridir. GDPR, bireylere verileri üzerinde etkin denetim hakkı tanırken, özellikle Madde 22 ile bireylerin yalnızca otomatik işlemeye dayalı ve kendileri hakkında hukuki veya benzeri sonuçlar doğuran kararlara tabi olmama hakkını açıkça güvence altına almaktadır. Ayrıca Madde 15, bireylere otomatik kararların ardındaki "mantığın anlamlı açıklaması"nı talep etme hakkı tanıyarak algoritmik şeffaflık ve hesap verebilirlik için kritik bir koruma mekanizması oluşturmaktadır.

Yasa Uygulama Direktifi (Law Enforcement Directive – LED): GDPR'ın kolluk kuvvetleri ve yargı makamları tarafından ceza adaleti amacıyla yürütülen veri işleme faaliyetlerine uyarlanmış özel versiyonudur. LED, kamu güvenliği ile bireysel mahremiyet arasında hassas bir denge kurmayı hedeflemektedir.

Avrupa Birliği Yapay Zekâ Yasası (AI Act): 2024 yılında kabul edilen AI Act, yapay zekânın düzenlenmesine yönelik küresel ölçekte öncü bir girişimdir. Yapay zekâ sistemlerini "kabul edilemez risk, yüksek risk, sınırlı risk ve minimal risk" olmak üzere dört kategoriye ayıran yasa, öngörücü polislik uygulamalarını en kritik tartışma alanlarından biri olarak konumlandırmıştır.

AI Act kapsamında kişiye dayalı öngörücü polislik uygulamaları "kabul edilemez risk" kategorisine alınarak AB genelinde tamamen yasaklanmıştır. Bu hüküm, bireylerin yalnızca istatistiksel profillere dayanarak "potansiyel suçlu" ilan edilmesini önlemeyi hedefleyen ilk bağlayıcı yasal yasak niteliğinde olup, küresel ölçekte emsal teşkil etmektedir (European Parliament, 2024). Buna karşılık, yere dayalı öngörücü polislik sistemlerine sınırlı koşullar altında izin verilmiş; bu sistemler "yüksek riskli" kategoride değerlendirilerek yalnızca coğrafi alanlara ilişkin risk tahmininde bulunabilmekte ve mutlaka insan gözetimine tabi tutulmaktadır. Ayrıca şeffaflık, veri kalitesi, siber güvenlik, sağlamlık ve algoritmik hesap verebilirlik gibi sıkı yükümlülükler getirilmiştir (Floridi ve ark., 2022).

Bu yaklaşım, ABD ile AB arasındaki düzenleyici paradigmanın felsefi farklılığını açık biçimde ortaya koymaktadır. ABD, serbest piyasa mantığı doğrultusunda teknolojik yeniliklerin önünü açmakta ve olası zararların ortaya çıkmasından sonra bireysel davalar ve yargı süreçleriyle çözüm aramaktadır. Buna karşın AB, "ihtiyat ilkesi" çerçevesinde hareket ederek temel hakların korunmasını önceliklendirmekte ve potansiyel riskleri ortaya çıkmadan kurallara bağlamaktadır. Bununla birlikte, yasal çerçevenin sağladığı korumalara rağmen öngörücü polislik sistemlerinin Avrupa'da hâlâ farklı biçimlerde uy-

gulandığı görülmektedir. Almanya'da hırsızlık suçlarına odaklanan PRECOBS (Veprek ve ark., 2020), Hollanda'da geliştirilen CAS (Criminality Awareness System) (Williams ve Kind, 2019) ve Danimarka'da kullanılan Palantir yazılımları (Galis ve Karlsson, 2024), AB içindeki çeşitliliğe örnek teşkil etmektedir.

Bu uygulamalar, AI Act'in yasak ve sınırlamalarının pratikte ne ölçüde etkili olabileceğine dair soru işaretlerini gündeme getirmektedir. Nitekim "yere dayalı" öngörücü sistemlerin, demografik açıdan belirli grupların yoğun yaşadığı bölgeleri hedef alarak dolaylı ayrımcılık üretme potansiyeli vardır. Ayrıca algoritmalara duyulan aşırı güven, "insan gözetimi" yükümlülüğünün yalnızca şeklen yerine getirilen, içi boşaltılmış bir prosedüre dönüşmesine yol açabilir (Veale ve Zuiderveen Borgesius, 2021). Bu nedenle, AI Act'in öngördüğü korumaların uygulamada ne ölçüde etkin olacağı gerek akademik literatürde gerek hukuk pratiğinde tartışılmaya devam etmektedir (Çetinkaya, 2024; Yücel, 2024).

Türkiye Perspektifi: Mevcut Durum ve Geleceğe Yönelik Tartışmalar

Anayasal Güvenceler Açısından Değerlendirme

Anayasalar, yalnızca bir devletin hukuki temelini oluşturmakla kalmaz, aynı zamanda bireylerin temel hak ve özgürlüklerini güvence altına alma görevini de üstlenir. Bu çerçevede, bir anayasanın insan haklarına yaklaşımı, onun demokratik karakterini ve toplumla kurduğu uyum ilişkisini doğrudan belirler (Aslan ve Nohutçu, 2025). Bu noktada, yeni nesil güvenlik teknolojilerinin uygulanabilirliği de anayasal güvencelerle doğrudan ilişkilidir.

Türkiye'de öngörücü polislik sistemlerinin uygulanabilirliği, öncelikle Anayasa'da yer alan temel hak ve özgürlüklere ilişkin normatif çerçeve ile sınanmak zorundadır. Bu bağlamda, Anayasa'nın 2. maddesinde tanımlanan hukuk devleti ilkesi, 10. maddesinde yer verilen kanun önünde eşitlik ilkesi, 20. maddesinde güvence altına alınan özel hayatın gizliliği ve kişisel verilerin korunması hakkı ile 38. maddesinde düzenlenen masumiyet karinesi, öngörücü polislik teknolojilerinin anayasal sınırlarını belirleyen temel güvenceler arasında yer almaktadır.

Bu ilkeler, yalnızca bireylerin haklarını korumakla kalmaz, aynı zamanda güvenlik politikalarının demokratik meşruiyetini sağlamak açısından da kritik öneme sahiptir (Çelik, 2025). Bu anayasal güvenceler içerisinde özellikle Anayasa'nın 13. maddesi ile düzenlenen kanunilik ilkesi, belirleyici bir eşik teşkil etmektedir. İlgili hüküm uyarınca, temel hak ve özgürlüklere yönelik

her türlü sınırlama veya müdahalenin açık, belirli ve öngörülebilir bir kanunla yapılması ve bu sınırlamanın demokratik toplum düzeninin gereklerine uygun olması zorunludur. Bu çerçevede, halihazırda Türkiye'de yaygın biçimde kullanılan Kent Güvenlik Yönetim Sistemi (KGYS) ve Plaka Tanıma Sistemi (PTS) gibi geniş kapsamlı gözetim altyapılarının dahi yeterli ve açık bir yasal dayanağa sahip olup olmadığı, özellikle Danıştay kararları ışığında tartışmalı bir konu olmaya devam etmektedir (Sezgin, 2022).

Bu koşullar altında, bireylerin özel hayatına çok daha derin müdahalelerde bulunabilecek ve anayasal güvenceleri daha doğrudan etkileyebilecek öngörücü polislik sistemlerinin, mevcut yasal mevzuat çerçevesinde uygulanabilmesi hukuken mümkün görünmemektedir. Bu tür teknolojilerin hayata geçirilmesi, yalnızca teknik gereklilikler açısından değil, aynı zamanda anayasal düzlemde de açık, spesifik ve temel haklara saygılı bir kanuni düzenlemeyi zorunlu kılmaktadır. Aksi takdirde, bu tür uygulamalar hem hukuki meşruiyet hem de toplumsal kabul açısından ciddi sorunlarla karşı karşıya kalacaktır.

6698 Sayılı Kişisel Verilerin Korunması Kanunu (KVKK) Kapsamında Değerlendirme

Öngörücü polislik sistemleri, doğası gereği büyük miktarda ve genellikle hassas nitelikte kişisel veri (suç kayıtları, biyometrik veriler, konum verileri vb.) işlediği için doğrudan 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) kapsamına girmektedir (KVKK, 2016).

KVKK'nın 11. maddesi ayrıca otomatik karar verme süreçlerine karşı bireylerin itiraz hakkını tanımaktadır. İlgili kişilere, verilerinin "münhasıran otomatik sistemler vasıtasıyla işlenmesi suretiyle kendileri aleyhine bir sonucun doğması" halinde bu karara itiraz etme ve kararın gözden geçirilmesini talep etme yetkisi verilmiştir. Bu bağlamda, öngörücü sistemler tarafından üretilen bir risk skorunun, bireyin daha yoğun denetime tabi tutulması, sistematik olarak izlenmesi ya da önleyici müdahalelere maruz bırakılması gibi aleyhe sonuçlar doğurması durumunda, bireylerin bu karar sürecine anlamlı bir insan müdahalesi talep etme hakkı devreye girecektir. Bu hak, yalnızca bireyin savunma pozisyonunu güçlendirmekle kalmaz; aynı zamanda algoritmik karar verme süreçlerine karşı demokratik denetim işlevi görür.

Türk Ceza Hukuku Açısından Sorumluluk: Kusur ve Yaptırım Tartışmaları

Türk Ceza Hukuku'nun temel ilkelerinden biri, suçun yalnızca bir gerçek kişi, yani "insan" fail tarafından işlenebileceği yönündedir. Bu çerçevede, mevcut

mevzuat ve doktrin kapsamında bir yapay zekâ (YZ) sisteminin doğrudan fail olarak nitelendirilmesi ve buna bağlı olarak cezai sorumluluğunun doğması hukuken mümkün değildir (Akbulut, 2023). Ceza hukuku, failin irade, kusur yeteneği ve hukuki sorumluluk kapasitesine sahip olmasını ön koşul kabul ettiğinden, yapay zekânın özerk karar alma yetileri olsa dahi, bu unsurlar açısından eksik kalması nedeniyle doğrudan cezalandırılabilir bir fail olarak değerlendirilemez. Bununla birlikte, bir YZ sisteminin bir suçla ilişkili olması hâlinde, hukuki sorumluluk, sistemin kendisine değil; onu tasarlayan, geliştiren ve kullanan insan aktörlere yönelmektedir. Bu kapsamda, yazılımcılar, üretici firmalar ve nihai kullanıcılar, sistemin suç oluşturan eylemlerine katkı sağladıkları ölçüde ceza sorumluluğu bakımından değerlendirilirler (Kan, 2024).

Özellikle kast veya taksir düzeyinde ihmal ya da yönlendirme söz konusuysa, bu kişiler hakkında doğrudan ya da dolaylı fail, azmettiren veya yardım eden sıfatlarıyla ceza sorumluluğu tesis edilebilir. Bu yaklaşım, insan sorumluluğunun cezai sistemde merkezî konumunu korumaya devam ettiğini ve yapay sistemlerin yalnızca araçsal düzeyde değerlendirildiğini göstermektedir. Yapay zekâ sistemlerinin suçla ilişkili durumlarında cezai sorumluluğun nasıl belirleneceği konusu, Türk Ceza Hukuku bakımından giderek daha fazla önem kazanmaktadır. Eğer bir birey, yapay zekâyı doğrudan bir suç işleme amacıyla araç olarak kullanırsa, bu durumda 5237 sayılı Türk Ceza Kanunu'nun genel hükümleri uyarınca doğrudan fail olarak sorumlu tutulur (Aksoy, 2021). Bu senaryoda yapay zekâ, suçu gerçekleştiren failin iradesine tâbi bir araç konumundadır ve hukuki sorumluluk, tamamen onu kullanan kişiye yöneltilmektedir. Ancak daha karmaşık ve hukuki olarak tartışmalı olan durum, yapay zekâ sisteminin özerk işleyişi sonucu, beklenmedik ve öngörülmeyen bir zarara yol açması hâlidir. Bu tür vakalarda, özellikle yazılımcı ya da üretici konumundaki kişilerin, ortaya çıkabilecek zararları önlemek adına gereken özeni göstermemeleri durumunda, taksirle sorumlulukları gündeme gelebilir (Çetingül, 2021).

Buradaki temel kıstas, zararın öngörülebilir olup olmadığı ve buna karşı alınması gereken tedbirlerin alınmamış olmasıdır. Yazılım hataları, test eksiklikleri ya da güncellemelerdeki ihlaller, bu kapsamda değerlendirilebilir. Bu gelişmeler doğrultusunda, Türk ceza hukuku literatüründe mevcut dogmatik yapının yeni teknolojik gelişmelere yanıt vermekte yetersiz kalabileceği yönünde giderek artan akademik tartışmalar yürütülmektedir. Bu tartışmalar, YZ sistemlerine sınırlı bir "elektronik kişilik" tanınması, klasik ceza hukukunun insan merkezli kusur anlayışının yeniden yorumlanarak "fonksiyonel kusur" gibi yeni teorik kavramlarla dönüştürülmesi ve ayrıca objektif sorumluluk ya da tehlike suçları gibi alternatif sorumluluk modellerinin geliştirilmesi gibi önerileri kapsamaktadır (Akbulut, 2023). Bu görüşler, mevcut

ceza hukuku sisteminin yapay zekânın neden olduğu karmaşık ve öngörülemeyen sonuçlara karşı yapısal olarak hazır olmadığını ve reform ihtiyacının giderek daha belirgin hâle geldiğini göstermektedir (Aksoy, 2021).

Sonuç

Yapay zekâ destekli suç tahmin sistemlerine yönelik hukuki yaklaşımlar incelendiğinde, üç coğrafya arasında belirgin felsefi ve metodolojik farklılıklar göze çarpmaktadır:

- **Amerika Birleşik Devletleri:** Reaktif ve yargısal denetim odaklı yaklaşım Amerika Birleşik Devletleri'nde öngörücü polislik ve benzeri yüksek riskli teknolojilerin düzenlenmesine ilişkin yaklaşım, büyük ölçüde teknolojik inovasyonun önünü açmaya ve ortaya çıkan sorunları mevcut anayasal çerçeve dâhilinde, genellikle bir hak ihlalinden sonra uygulanan yargısal denetim yoluyla çözmeye odaklıdır. Bu "olay sonrası" denetim modeli, bireysel mağduriyetlerin dava konusu edilerek hukuki çözümler üretilmesini esas alır. Ancak bu yaklaşım, sistemik düzeyde sorunların önlenmesinde yetersiz kalabilmekte ve önleyici hukuki mekanizmaların eksikliğine işaret etmektedir. Federal düzeyde, öngörücü polislik sistemlerine ilişkin bütüncül ve bağlayıcı bir yasal düzenleme bulunmamaktadır. Bu durum, düzenlemelerin büyük ölçüde eyalet ve yerel yönetimlerin inisiyatifine bırakılmasına yol açmakta; sonuç olarak ortaya çıkan uygulama haritası, parçalı, tutarsız ve bölgesel farklılıklar içeren bir yapıya dönüşmektedir. Bu model, her ne kadar teknolojik girişimciliği ve inovasyonu teşvik edici nitelikler taşısa da temel hakların korunması, ayrımcılığın önlenmesi ve algoritmik hesap verebilirliğin sağlanması gibi konularda ciddi boşluklar barındırmaktadır. Bu nedenle ABD yaklaşımı, bireysel özgürlükler ile kamu güvenliği arasında hassas bir denge kurma konusunda normatif değil, çoğu zaman reaktif ve pragmatik bir pozisyon almaktadır.
- **Avrupa Birliği:** Avrupa Birliği (AB), Amerika Birleşik Devletleri'nin daha çok reaktif ve post-hoc temelli yaklaşımının aksine, temel hakların korunmasını merkeze alan proaktif bir düzenleyici model benimsemektedir. Bu yaklaşımın en somut yansıması, 2024 yılında kabul edilen AB Yapay Zekâ Yasası'dır (AI Act). Yasa, yapay zekâ sistemlerini risk düzeylerine göre "kabul edilemez risk, yüksek risk, sınırlı risk ve minimal risk" olmak üzere dört kategoriye ayırmakta ve özellikle öngörücü polislik uygulamalarına ilişkin sınırları açık biçimde çizmektedir. Bu düzenleme kapsamında kişiye dayalı öngörücü polislik uygulamaları "kabul edilemez risk" kategorisinde değerlendirilmiş ve AB genelinde tamamen yasaklanmıştır. Böylece bireylerin yalnızca istatistiksel profillere dayanarak "potansiyel suçlu" ilan edilmesi tehlikesi, ilk kez açık bir yasa hükmüyle engellenmiştir (European Parliament, 2024). Buna karşılık yere dayalı öngörücü polislik uygulamaları "yüksek riskli" ka-

tegoride kabul edilmiş; ancak yalnızca şeffaflık, insan gözetimi, veri kalitesi, algoritmik sağlamlık, denetlenebilirlik ve hesap verebilirlik gibi katı standartların karşılanması şartıyla sınırlı biçimde kullanılmalarına izin verilmiştir (Floridi ve ark., 2022). AB'nin bu yaklaşımı, yalnızca bireysel hakların korunmasına değil; aynı zamanda yapısal ayrımcılığın önlenmesine, veri mahremiyetinin güvence altına alınmasına ve kurumsal hesap verebilirliğin sağlanmasına odaklanmaktadır. Bu bağlamda AB, "ihtiyat ilkesi" doğrultusunda riskleri ortaya çıkmadan sınırlamayı hedeflemekte; ABD ise teknolojik yenilikleri serbest piyasa mantığına bırakarak olası zararların ortaya çıkmasının ardından yargısal yollarla çözüm aramaktadır. Bununla birlikte, mevcut yasal çerçeveye rağmen AB üyesi bazı ülkelerde öngörücü polislik projeleri hâlâ uygulanmakta veya test edilmektedir. Almanya'daki PRECOBS sistemi (Veprek ve ark., 2020), Hollanda'da geliştirilen CAS (Criminality Awareness System) (Williams ve Kind, 2019) ve Danimarka'da kullanılan Palantir yazılımları (Galis ve Karlsson, 2024), AI Act'in pratikteki sınırlarını göstermektedir. Ayrıca algoritmalara duyulan aşırı güven nedeniyle "insan gözetimi" şartının yalnızca şekli bir prosedüre indirgenme riski de mevcuttur (Veale ve Zuiderveen Borgesius, 2021).

- **Türkiye: Gelişmekte Olan ve Yasal Boşluk İçeren Yaklaşım:** Türkiye'nin öngörücü polislik teknolojilerine yaklaşımı, henüz kurumsallaşmamış, gelişmekte olan ve büyük ölçüde yasal boşluklar barındıran bir yapıya sahiptir. Her ne kadar resmî olarak uygulamaya geçmiş bir öngörücü polislik sistemi bulunmasa da teknolojiye yönelik artan kurumsal ilgi, Kent Güvenlik Yönetim Sistemi (KGYS) ve Plaka Tanıma Sistemi (PTS) gibi mevcut gözetim altyapılarının varlığı, bu alandaki potansiyel uygulamalara zemin hazırlamaktadır. Ancak söz konusu altyapılar bile çoğu zaman yeterli yasal dayanağa sahip olmadığından, öngörücü nitelikteki daha ileri sistemlerin uygulanmasında ciddi meşruiyet ve denetim sorunları ortaya çıkmaktadır. Hukuki tartışmalar, daha çok mevcut Anayasa, Kişisel Verilerin Korunması Kanunu (KVKK) ve Türk Ceza Kanunu (TCK) çerçevesinde bu tür sistemlerin nasıl değerlendirilmesi gerektiği üzerinde yoğunlaşmaktadır. Bu bağlamda, masumiyet karinesi, özel hayatın gizliliği, kişisel verilerin korunması ve kanunilik ilkesi gibi anayasal güvenceler öne çıkmakta; algoritmik önyargı, otomatik karar verme ve insan müdahalesi gibi konular KVKK açısından özel dikkat gerektiren alanlar olarak değerlendirilmektedir. Ancak tüm bu tartışmalara rağmen, öngörücü polislik teknolojilerini doğrudan düzenleyen spesifik bir yasal çerçevenin bulunmaması, Türkiye'nin en önemli kurumsal açığı olarak ortaya çıkmaktadır. Bu eksiklik, yalnızca hukuki belirsizlik yaratmakla kalmamakta; aynı zamanda "de facto" uygulamaların ortaya çıkma riskini artırmakta ve bireylerin temel hak ve özgürlükleri açısından ciddi bir tehdit oluşturmaktadır. Türkiye'nin karşı karşıya olduğu bu belirsiz durum, Avrupa Birliği'nin önleyici ve normatif yaklaşımı ile Amerika Birleşik Devletleri'nin reak-

tif modeli arasında konumlanan, düzenleyici netlikten yoksun bir geçiş evresine işaret etmektedir.

Yapay zekâ destekli suç tahmin sistemleri, suçla mücadele süreçlerinde belirli faydalar sağlama potansiyeline sahip olmakla birlikte, adalet, eşitlik, mahremiyet ve temel insan hakları bakımından ciddi ve çok katmanlı riskler barındırmaktadır. Bu teknolojiler, çoğu zaman verimlilik ve nesnellik vaat eden bir "sihirli değnek" gibi sunulsa da gerçekte çift taraflı keskin bir kılıç niteliği taşımakta ve bu nedenle dikkatli, şeffaf ve insan odaklı biçimde tasarlanıp uygulanması gereken sistemlerdir. Özellikle algoritmik önyargıların mevcut toplumsal eşitsizlikleri yeniden üretme ve meşrulaştırma riski, "kara kutu" algoritmaların hesap verebilirlikten uzak doğası ve yaygın gözetim uygulamalarının temel özgürlükler üzerinde oluşturduğu caydırıcı etkiler bu teknolojilerin denetimsiz biçimde benimsenmesinin yaratabileceği başlıca tehlikeler arasında yer almaktadır.

Bu noktada, çözüm yalnızca teknolojik sınırlandırmaların farkına varmakla kalmayıp, aynı zamanda teknolojinin kendisini çözümün bir parçası hâline getirmeyi gerektirir. Özellikle "kara kutu" sorununun üstesinden gelmeyi hedefleyen Açıklanabilir Yapay Zekâ (Explainable Artificial Intelligence – XAI) araştırmaları, şeffaflık açısından önemli bir ilerleme sunmaktadır. XAI, algoritmaların hangi verilere dayandığı, hangi mantıkla karar verdiği gibi hususları insan müdahalesine açık ve anlaşılabilir kılarak hem yargısal hem de idari süreçlerde hesap verebilirliği mümkün kılmakta hem de hatalı veya önyargılı kararlara karşı itiraz hakkının somut biçimde kullanılmasını kolaylaştırmaktadır (Hussain ve Hussain, 2025; Shamoo, 2025).

Ne var ki, XAI tek başına yeterli değildir. Nihai kararların her zaman "anlamlı bir insan gözetimi" altında alınması bir zorunluluktur. Bu gözetim, yalnızca algoritmanın ürettiği sonucu pasif biçimde onaylayan bir insan figüründen ibaret olmamalı; eleştirel değerlendirme, sorgulama ve gerekirse reddetme gibi aktif bilişsel süreçleri içermelidir. Kolluk personelinin, algoritma çıktıları karşısında "otomasyon önyargısı" etkisiyle körü körüne hareket etmesini engellemek amacıyla, eleştirel düşünme becerileri ve mesleki muhakeme kapasiteleri üzerine eğitim almaları hayati önem taşımaktadır (Ferguson, 2017).

Bu nedenle çözüm yalnızca daha iyi yasaların yapılmasından ibaret değildir; aynı zamanda daha adil ve şeffaf teknolojilerin geliştirilmesini, bu teknolojilerin etik ve hukuki çerçevede uygulanmasını ve bunları kullanacak insan aktörlerin doğru şekilde eğitilmesini kapsayan kapsamlı bir yaklaşımı zorunlu kılmaktadır. Bu bütüncül çerçeve benimsendiği takdirde, yapay zekâ

destekli suç tahmin sistemleri bir tehdit olmaktan çıkıp, sorumlu ve denetlenebilir bir kamu güvenliği aracı hâline dönüşebilir.

Yapay zekâ destekli öngörücü polislik sistemleri gibi yüksek riskli teknolojilerin geliştirilmesi, satın alınması ve uygulanmasına ilişkin süreçlerin, yalnızca kapalı kapılar ardında, teknokratlar ve bürokratlar tarafından yürütülmesi, demokratik meşruiyet ve toplumsal denetim açısından ciddi sakıncalar doğurmaktadır. Bu tür sistemlerin toplumsal etkileri, özellikle de marjinalleştirilmiş gruplar üzerinde yaratabileceği orantısız zararlar dikkate alındığında, sürecin tek taraflı teknik uzmanlıkla sınırlandırılması kabul edilemez bir yaklaşım olacaktır. Bu nedenle, söz konusu karar alma ve denetim süreçlerine, sivil toplum kuruluşlarının, bağımsız akademisyenlerin, hukukçuların ve bu sistemlerden doğrudan etkilenme riski taşıyan kırılgan toplulukların temsilcilerinin aktif katılımının sağlanması gerekmektedir (Ter-Minassian, 2025).

Bu katılım, yalnızca danışma düzeyinde kalmamalı; kurumsallaştırılmış, sürekli ve yetki sahibi bir yapıya dönüştürülmelidir. Bu doğrultuda, öngörücü polislik ve benzeri yüksek riskli yapay zekâ sistemlerinin kullanımı üzerinde bağımsız ve sivil nitelikli bir denetim organının oluşturulması gereklidir. Bu organ, yalnızca teknik denetim işlevi görmekle kalmamalı; aynı zamanda hukuki, etik ve toplumsal değerlendirme ölçütlerini esas alan bütüncül bir kontrol mekanizması olarak yapılandırılmalıdır. Bu kurumun temel görevleri arasında sistemlerin satın alınmasından ve uygulamaya geçirilmesinden önce bağımsız etki ve risk değerlendirmeleri yapmak, kullanılan algoritmaları düzenli aralıklarla önyargı ve ayrımcılık açısından test etmek, sistemlerin hem etkinliğini hem de temel haklar üzerindeki etkilerini sürekli biçimde izlemek ve değerlendirmek, tüm faaliyetleri hakkında kamuoyuna şeffaf ve düzenli raporlar sunmak gibi görevler bulunmaktadır.

Bu tür bir mekanizmanın varlığı, yalnızca keyfi ve denetimsiz teknolojik uygulamaların önüne geçilmesini değil; aynı zamanda kamu güveninin tesisi, kurumsal hesap verebilirliğin sağlanması ve teknolojinin adil, şeffaf ve demokratik değerlere uygun biçimde kullanılması açısından en önemli kurumsal güvencelerden biri olacaktır (Hirsh, 2016).

Kaynakça

Akbulut, B. (2023). Yapay zekâ ve ceza hukuku sorumluluğu. *Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi*, 27(4), 267–319. https://doi.org/10.0000/ahbvu.2023.27.4

Aksoy, H. (2021). Yapay zekâlı varlıklar ve ceza hukuku. *Uluslararası Ekonomi Siyaset İnsan ve Toplum Bilimleri Dergisi, 4*(1), 10–27.

Alikhademi, K., Drobina, E., Prioleau, D., Richardson, B., Purves, D., & Gilbert, J. E. (2022). A review of predictive policing from the perspective of fairness. *Artificial Intelligence and Law, 30*(1), 1–17. https://doi.org/10.1007/s10506-021-09296-2

Angwin, J., Larson, J., Mattu, S., & Kirchner, L. (2022). Machine bias. In *Ethics of data and analytics* (pp. 254–264). Auerbach Publications.

Aslan, Ö., & Nohutçu, A. (2025). 1982 Anayasası'nda insan hakları: Hürriyet ve otorite dengesine ilişkin bir değerlendirme. *Liberal Düşünce Dergisi, (118)*, 145–165. https://doi.org/10.36484/liberal.1630730

Bachner, J. (2013). *Predictive policing: Preventing crime with data and analytics*. IBM Center for the Business of Government.

Barocas, S., Hardt, M., & Narayanan, A. (2023). *Fairness and machine learning: Limitations and opportunities*. MIT Press.

Başaran, R. (2021). Türkiye'de suç coğrafyası ve sıcak nokta analizleri. *Kriminoloji Dergisi, 4*(2), 87–112.

Braga, A. A., Papachristos, A. V., & Hureau, D. M. (2014). The effects of hot spots policing on crime: An updated systematic review and meta-analysis. *Justice Quarterly, 31*(4), 633–663. https://doi.org/10.1080/07418825.2012.673632

Brayne, S. (2017). Big data surveillance: The case of policing. *American Sociological Review, 82*(5), 977–1008. https://doi.org/10.1177/0003122417725865

Çelik, A. (2025). Gelişmişlik ve ekonomik durumlarına göre kentlerde suç eğilimleri ve muhtemel sebepleri. *Güvenlik Çalışmaları Dergisi, 27*(1), 82–94. https://doi.org/10.54627/gcd.1684873

Çetinkaya, Z. (2024). Türkiye'de öngörücü polislik ve algoritmik ayrımcılık. *Hukuk ve Adalet Dergisi, 20*(3), 55–78.

Çetingül, N. (2021). Ceza sorumluluğu bakımından yapay zekânın hukuki statüsünün tartışılması. *İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi, 20*(41), 1015–1042.

Çolakoğlu, M. (2024). Doğal dil işleme ile suç tiplerinin sınıflandırılması: Yeni bir yaklaşım. *Adli Bilişim Araştırmaları Dergisi, 6*(1), 34–59.

Egbert, S., & Leese, M. (2021). Criminal futures: Predictive policing and everyday police work. *The British Journal of Criminology, 61*(4), 1031–1050.

Ensign, D., Friedler, S. A., Neville, S., Scheidegger, C., & Venkatasubramanian, S. (2018). Runaway feedback loops in predictive policing. In *Conference on Fairness, Accountability and Transparency* (pp. 160–171). PMLR.

European Parliament. (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council on artificial intelligence (AI Act). *Official Journal of the European Union, L* 277, 1–148.

Ferguson, A. G. (2012). Predictive policing and reasonable suspicion. *Emory Law Journal, 62*(2), 259–325.

Ferguson, A. G. (2017). *The rise of big data policing: Surveillance, race, and the future of law enforcement*. NYU Press.

Floridi, L., Holweg, M., Taddeo, M., Amaya, J., Mökander, J., & Wen, Y. (2022). CapAI—A procedure for conducting conformity assessment of AI systems in line with the EU Artificial Intelligence Act. *SSRN*. https://doi.org/10.2139/ssrn.4064091

Freeman, K. (2016). Algorithmic injustice: How the Wisconsin Supreme Court failed to protect due process rights in *State v. Loomis*. *North Carolina Journal of Law & Technology, 18*(5), 75–112.

Galis, V., & Karlsson, B. (2024). A world of Palantir: Ontological politics in the Danish police's POL-INTEL. *Information, Communication & Society, 27*(13), 2438–2456. https://doi.org/10.1080/1369118X.2024.1234567

Hirsh, J. (2016). Predictive policing and civilian oversight: What will it take to get it right? *IEEE Potentials, 35*(5), 19–22.

Hussain, A., & Hussain, A. (2025). Transparency and accountability: Unpacking the real problems of explainable AI. *AI & Society*. https://doi.org/10.1007/s00146-025-01735-4

Kan, C. H. (2024). Criminal liability of artificial intelligence from the perspective of criminal law: An evaluation in the context of the general theory of crime and fundamental principles. *Uluslararası Avrasya Sosyal Bilimler Dergisi, 14*(55), 1–15.

Kavsıracı, O. (2018). Polis faaliyetlerinde gri alanlar ve etik. *OPUS Uluslararası Toplum Araştırmaları Dergisi, 9*(16), 1851–1882. https://doi.org/10.26466/opus.481244

Kavsıracı, O., & Demirbaş, M. (2020). İstihbarat faaliyetlerinin devlet güvenliği açısından incelenmesi. *Anadolu Strateji Dergisi, 2*(1), 49–64.

Kişisel Verilerin Korunması Kanunu. (2016). Kanun No: 6698, Kabul Tarihi: 24.03.2016, Resmî Gazete: 07.04.2016 – Sayı: 29677.

Lum, K., & Isaac, W. (2016). To predict and serve? *Significance, 13*(5), 14–19. https://doi.org/10.1111/j.1740-9713.2016.00960.x

Marciniak, D. (2023). Algorithmic policing: An exploratory study of the algorithmically mediated construction of individual risk in a UK police force. *Policing and Society, 33*(4), 449–463. https://doi.org/10.1080/10439463.2022.2094337

Maviş, V. (2025). Predictive Policing: Balancing Crime Prevention and Fundamental Rights. *Periodicum Iuris*, *3*(2), 343-373.

Meding, J. (2025). Algorithmic fairness in predictive policing. *Journal of Law and Technology, 41*(2), 210–235.

Meijer, A., & Wessels, M. (2019). Predictive policing: Review of benefits and drawbacks. *International Journal of Public Administration, 42(1*2), 1031–1039. https://doi.org/10.1080/01900692.2019.1575666

Mohler, G. O., Short, M. B., Malinowski, S., Johnson, M., Tita, G. E., Bertozzi, A. L., & Brantingham, P. J. (2015). Randomized controlled field trials of predictive policing. *Journal of the American Statistical Association, 110*(512), 1399–1411. https://doi.org/10.1080/01621459.2015.1077710

Pasquale, F. (2020). *New laws of robotics*. Harvard University Press.

Penney, J. (2017). Internet surveillance, regulation, and chilling effects online: A comparative case study. *Internet Policy Review, 6*(2), 1–23. https://doi.org/10.14763/2017.2.694

Perry, W. L. (2013). *Predictive policing: The role of crime forecasting in law enforcement operations*. RAND Corporation.

Popp, T. (2017). Black box justice. *The Pennsylvania Gazette, 115*(3), 38–47.

Richardson, R., Schultz, J. M., & Crawford, K. (2019). Dirty data, bad predictions: How civil rights violations impact police data, predictive policing systems, and justice. *NYU Law Review Online, 94*, 15–55.

Sankin, A., & Mattu, S. (2023). Predictive policing software terrible at predicting crimes. *The Markup, 2*(1), 1–12.

Sezgin, S. M. (2022). Türkiye'de elektronik denetleme sistemleri ile tespit edilen hız aşım oranlarının incelenmesi (Yayımlanmamış yüksek lisans tezi). Gazi Üniversitesi, Ankara.

Shamoo, Y. (2025). The role of explainable AI (XAI) in forensic investigations. In *Digital forensics in the age of AI* (pp. 31–62). IGI Global Scientific Publishing.

Tayebi, M. A., & Glässer, U. (2016). *Social network analysis in predictive policing: Concepts, models and methods*. Springer.

Ter-Minassian, L. (2025). Democratizing AI governance: Balancing expertise and public participation. *AI & Society*. https://doi.org/10.1007/s00146-025-01755-0

Tufan, B. N. (2024). Yapay zekâ ve suç: Gelecek açısından hukuksal ve etik tehditler. *Medeniyet Kültürel Araştırmalar Belleteni, 4*(7), 1–17.

Utku, A. (2024). Derin öğrenme tabanlı suç tahmin modelleri. *Bilişim ve Yapay Zekâ Dergisi, 3*(2), 54–76.

Van Brakel, R. E. (2025). Legal, ethical and social issues of AI and law enforcement in Europe: The case of predictive policing. *European Journal of Criminology, 22*(1), 115–139.

Veale, M., & Zuiderveen Borgesius, F. (2021). Demystifying the draft EU Artificial Intelligence Act—Analysing the good, the bad, and the unclear elements of the proposed approach. *Computer Law Review International, 22*(4), 97–112.

Vepřek, L. H., Sibert, L., Sehn, L., Köpp, L., & Friedrich, D. (2020). Beyond effectiveness: Legitimising predictive policing in Germany. *Kriminologie: Das Online-Journal, 2*(3), 423–443.

Vitale, A. S. (2021). *The end of policing*. Verso Books.

Warso, Z. (2022). Human rights requirements for person-based predictive policing: Lessons from selected ECtHR case law and its limits. *Technology and Regulation, 2022*(1), 71–80. https://doi.org/10.26116/techreg.2022.007

Weiss, D. A. (2025). Inhuman reason: Predictive policing algorithms and the Fourth Amendment. *Criminal Justice, 39*(4), 15–20.

Williams, P., & Kind, E. (2019). Data-driven policing: The hardwiring of discriminatory policing practices across Europe. *European Journal of Criminology, 16*(5), 573–591. https://doi.org/10.1177/1477370819828940

Yang, C. S., & Dobbie, W. (2020). Equal protection under algorithms: A new statistical and legal framework. *Michigan Law Review, 118*(2), 291–395.

Yücel, H. (2024). Türkiye'de öngörücü polislikte delil niteliği tartışmaları. *Adalet ve Toplum Dergisi, 9*(2), 201–225.