

CEZA MUHAKEMESİ HUKUKUNDA DERİN ÖĞRENME İLE ELDE EDİLEN GÖRSEL VERİLERİN DELİL NİTELİĞİ: HUKUKİ VE TEKNİK BİR ANALİZ

*The Evidentiary Value of Visual Data Obtained Through Deep Learning in
Criminal Procedure Law: A Legal and Technical Analysis*

Yalçın KAPLAN*

Özet

Bu çalışma, derin öğrenme tabanlı Yapay Zekâ (YZ) sistemlerinin adli görüntü analizlerinde kullanımı ile bu sistemlerin ceza muhakemesi hukuku açısından delil niteliğini disiplinlerarası bir bakış açısıyla ele almaktadır. YZ destekli analizlerin teknik kapasitesine rağmen, bu sistemlerin hukuki geçerliliği; hukuka uygunluk, şeffaflık, denetlenebilirlik, açıklanabilirlik ve kişisel veri koruması gibi temel ilkeler doğrultusunda değerlendirilmelidir. Çalışmada öncelikle derin öğrenme temelli görüntü işleme teknikleri özetlenmiş, ardından bu tekniklerin ceza yargılamasında delil elde etme ve değerlendirme süreçlerine etkisi incelenmiştir. Türk hukukunda delil serbestisi ilkesi kapsamında YZ ile elde edilen verilerin hukuki geçerliliği Anayasa, CMK ve Kişisel Verilerin Korunması Kanunu (KVKK) çerçevesinde analiz edilmiş; sokakta bulunan kameralardan yüz tanıma ve güvenlik kamerası görüntüsü gibi veri türlerinin mahkemede kullanılabilirliğine ilişkin kriterler tartışılmıştır. Ayrıca Avrupa İnsan Hakları Mahkemesi, Avrupa Birliği AI Act ve ABD Daubert standardı çerçevesindeki uygulamalarla karşılaştırmalı analiz yapılmış; Türkiye’deki düzenleme eksikliklerine dikkat çekilmiştir. YZ’nin “kara kutu” yapısının savunma hakkı ve adil yargılanma ilkeleriyle yaratabileceği çelişkiler açıklanmış ve açıklanabilir yapay zekâ yaklaşımlarının önemi vurgulanmıştır. Sonuç olarak çalışmada, YZ tabanlı adli sistemlerin hukuk düzeniyle uyumlu entegrasyonu için yasal düzenleme, birikimi eğitimi, etik ilkeler ve insan denetimi gibi öneriler sunulmuştur. Bu yönüyle çalışma, teknik ve hukuki boyutları birlikte ele alarak alandaki özgün bir boşluğu doldurmayı hedeflemektedir.

Anahtar Kelimeler: Yapay zekâ, derin öğrenme, görüntü analizi, adli bilişim, delil niteliği, AI act, daubert standardı

Abstract

This study examines the use of deep learning-based Artificial Intelligence (AI) systems in forensic image analysis and their evidentiary value under Turkish Criminal Procedure Law from an interdisciplinary perspective. Despite the technical capacity of AI-supported analyses, their legal admissibility must be assessed within the framework of key legal principles such as lawfulness, transparency, auditability, explainability, and personal data protection. The study first outlines deep learning-based image processing techniques and then analyzes their impact on the processes of obtaining and evaluating evidence in criminal proceedings. Within the scope of the principle

➤ Bu makale Etik Kurul iznine tabi değildir/This article is not subject to Ethics Committee permission.

➤ Makale Geliş Tarihi/Article Received Date: 16.6.2025

➤ Yayın Kurulu Kabul Tarihi/Editorial Board Acceptance Date: 13.01.2026

* Av. Dr., Sahil Güvenlik Komutanlığı MEBS Başkanlığı, Ankara/Türkiye,
E-posta: yalcinnkaplan@gmail.com, <https://orcid.org/0000-0002-3414-1771>.



of freedom of evidence in Turkish law, the legal validity of data obtained through AI systems is evaluated in light of the Constitution, the Criminal Procedure Code (CMK), and the Law on the Protection of Personal Data (KVKK). Specific attention is given to the admissibility of data types such as facial recognition and CCTV footage in court. Furthermore, a comparative legal analysis is conducted with reference to the practices of the European Court of Human Rights, the European Union AI Act, and the Daubert standard in the United States, highlighting the regulatory gaps in Turkish law. The study also explains how the “black box” nature of

AI may conflict with the right to defense and the principle of a fair trial, emphasizing the importance of Explainable AI in addressing these concerns. In conclusion, the study offers structural recommendations and a model for the integration of AI-based forensic systems in compliance with legal norms, including legal regulations, expert training, ethical guidelines, and human oversight. By addressing both technical and legal aspects, the study aims to fill a significant gap in the literature.

Keywords: Artificial intelligence, deep learning, image analysis, forensic informatics, evidentiary value, AI act, daubert standard

GİRİŞ

Dijital teknolojilerin baş döndürücü bir hızla gelişmesi, hukuk sistemlerini de kaçınılmaz biçimde dönüştürmekte ve yeniden yapılandırmaya zorlamaktadır. Bu dönüşümün en belirgin şekilde hissedildiği alanlardan biri olan adli bilişim, günümüzde artık sadece dijital izlerin toplanması veya basit veri kurtarma işlemleriyle sınırlı kalmayıp, büyük veri (big data) analitiği ve yapay zekâ (YZ) algoritmalarıyla desteklenen çok katmanlı bir inceleme alanına dönüşmüştür. Özellikle derin öğrenme (deep learning) teknikleri, bu alanda radikal değişimlere yol açmakta; görsel verilerin daha etkin, hızlı ve insan hatasından arındırılmış biçimde analiz edilmesini mümkün kılmaktadır. Olay yeri incelemeleri, güvenlik kamerası kayıtları, insansız hava araçları (drone) ile elde edilen görüntüler gibi çok çeşitli görsel veri kaynakları, artık yalnızca saklanmakla kalmamakta; bu veriler üzerinde Convolutional Neural Networks (CNN), YOLO (You Only Look Once) ve U-Net gibi yapılar kullanılarak sınıflandırma, nesne tanıma ve segmentasyon işlemleri gerçekleştirilmektedir. Bu yöntemler, kimi zaman insan gözüyle fark edilemeyecek derecede küçük detayları ortaya koymakta ve olayın çözümüne dair yeni delil unsurlarını görünür kılabilmektedir. Derin öğrenme temelli bu analizler, fail tespiti, suç tipinin belirlenmesi ve olayın zaman-mekân eşleşmelerinin yapılması gibi adli süreçlerde araştırmacılara ve kolluk kuvvetlerine önemli kolaylıklar sağlamaktadır. Derin öğrenme algoritmalarının karar verme süreçlerinin genellikle “kutunun içi kara” (black box) niteliğinde olması, yani sistemin nasıl bir işlem basamağıyla sonuca ulaştığının dışarıdan izlenememesi veya açıklanamaması, özellikle ceza muhakemesi açısından ciddi sorunlara yol açmaktadır. Zira ceza muhakemesi hukukunda delil serbestisi ilkesi kabul edilmekle birlikte, bu ilke hukuka aykırı yollarla elde edilen delillerin yargılamada kullanılamayacağı kuralı ile sınırlandırılmıştır. Mahkeme huzuruna gelen her tür verinin delil olarak kabulü, sadece teknik doğruluğu ile değil; hukuka uygunluk, şeffaflık, denetlenbilirlik ve insan denetimi gibi temel yargısal ilkelerle de bire-

bir ilişkili olmalıdır. Bu bağlamda, yapay zekâ tarafından otomatik olarak analiz edilen görsellerin mahkemelerde delil olarak kullanılabilirliği, yalnızca teknik bir mesele değil; aynı zamanda ciddi bir hukuki meşruiyet problemidir. Mahkemelerin ve hâkimlerin bu tür teknolojik çıktıları delil olarak kabul ederken nelere dikkat etmesi, bilirkişilik kurumunun nasıl bir rol üstlenmesi ve sistemlerin yargı denetimine ne ölçüde açık olması gibi sorular, bu teknolojilerin yargı sistemine entegrasyonunda cevaplanması gereken başlıca sorun alanlarını oluşturmaktadır. Bu çalışma, öncelikle derin öğrenme tabanlı görüntü analiz teknolojilerinin adli bilişim alanındaki kullanım biçimlerini ve teknik yapılarını açıklamakta; ardından bu teknolojilerin Türk Ceza Muhakemesi Hukuku çerçevesinde delil niteliği taşıyıp taşımadığını tartışmaktadır. Karşılaştırmalı hukuk bağlamında özellikle Avrupa İnsan Hakları Mahkemesi kararları ve bazı Avrupa ülkelerinin düzenlemeleri de göz önünde bulundurularak, yapay zekâ destekli analizlerin yargı süreçlerinde hukuki geçerliliği, kanıt değeri ve hak ihlali riski çok yönlü biçimde değerlendirilecektir. Son olarak, bu sistemlerin adil yargılanma hakkı ve savunma hakkı bağlamında ne tür etkiler doğurduğu, hâkimin takdir yetkisi ve bilirkişilik kurumu bağlamında kapsamlı bir incelemeye tabi tutulacaktır. Yapay zekâ destekli analizlerin ceza muhakemesi süreçlerine etkisine dair literatür henüz yeni gelişmekte olmakla birlikte, konuya ilişkin disiplinler arası çalışmalar dikkat çekmektedir. Goodman ve Flaxman (2017), yapay zekâ algoritmalarının “black box” yapısının hukuk sisteminde şeffaflık ve açıklanabilirlik sorunlarına neden olduğunu ortaya koyarken,¹; Zarsky (2016), otomatik karar alma sistemlerinin yargısal denetime açılması gerektiğini vurgulamıştır². Türk hukuk literatüründe, ceza muhakemesinde dijital delillerin değerlendirilmesine ilişkin hukuki sorunlar ele alınmakta; bu çerçevede delil serbestisi ilkesinin sınırları ile delillerin değerlendirilmesinde yargıcın rolü ayrıntılı biçimde incelenmektedir. Ayrıca European Union Agency for Fundamental Rights (FRA) tarafından yayımlanan 2020 tarihli raporda, yapay zekâ destekli analizlerin mahkemelerde kullanılmasının insan hakları açısından doğurabileceği risklere dikkat çekilmiştir³. Öte yandan, Szegedy et al. (2015), derin öğrenme tekniklerinin özellikle görüntü tanıma ve sınıflandırmadaki başarılarına dikkat çekmekte⁴; Redmon et al. (2016) tarafından geliştirilen YOLO modeli, gerçek zamanlı nesne tespiti bağlamında adli bilişim

¹ Goodman, B., & Flaxman, S. (2017). European Union regulations on algorithmic decision-making and a “right to explanation”. *AI Magazine*, 38(3), 50–57.

² Zarsky, T. Z. (2016). The trouble with algorithmic decisions: An analytic road map to examine efficiency and fairness in automated and opaque decision making. *Science, Technology, & Human Values*, 41(1), 118–132.

³ European Union Agency for Fundamental Rights (FRA). (2020). Getting the future right – Artificial intelligence and fundamental rights. Publications Office of the European Union.

⁴ Szegedy, C., Liu, W., Jia, Y., et al. (2015). Going deeper with convolutions. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 1–9.



uygulamaları açısından ön plana çıkmaktadır⁵. Görüntü segmentasyonu ve detaylı veri işleme alanında yaygın kullanılan U-Net (Ronneberger et al., 2015) mimarisi de olay yeri incelemelerinde yüksek doğruluklu analizler sağlaması nedeniyle literatürde sıkça referans verilen modeller arasındadır.⁶

I. PROBLEM VE BULGULAR

A. Veriler ve Bulgular

Makalenin yöntemsel bütünlüğünü sağlamak amacıyla, derin öğrenme tabanlı adli görüntü analizlerinde kullanılan görsel verilerin kaynağı, elde edilme usulleri ve hukuki niteliği açıkça tanımlanmıştır. Bu kapsamda, ceza soruşturması sürecinde görüntü verilerinin elde edilmesi, veriyi toplayan aktörlere ve yasal dayanaklara göre farklılık göstermektedir:

Adli Kolluk (Polis ve Jandarma): 5271 sayılı CMK'nın 161. maddesi ve ilgili hükümleri uyarınca yürütülen soruşturma aşamasında, güvenlik kameralarına ait Kapalı Devre Kamera Sistemleri (KGYS), Plaka Tanıma Sistemleri (PTS), insan-sız hava araçları (İHA–drone) görüntüleri ve olay yeri fotoğrafları gibi kayıtlar resmî delil elde etme faaliyeti kapsamında toplanmaktadır.

Özel Kişiler ve Tüzel Kişiler (İşletmeler, Mağazalar, Apartman Yönetimleri): Bu aktörler, suçla bağlantılı olaydan önce ticari, güvenlik veya işletme güvenliği amacıyla görüntü kaydı almaktadır. Ancak bu kayıtların ceza muhakemesi kapsamında kullanılabilmesi, cumhuriyet savcısının talimatı, hâkim kararı veya veri sahibinin rızası gibi hukuki koşulların gerçekleşmesine bağlıdır.

Gerçek Kişiler (Bireyler): Cep telefonu, araç içi kamera, sosyal medya veya benzeri araçlarla elde edilen görüntüler, delil serbestisi ilkesi kapsamında değerlendirilmekle birlikte, görüntünün elde edilme şeklinin hukuka uygun olması ve kişisel verilerin korunması yükümlülüklerinin ihlal edilmemiş olması zorunludur. Aksi durumda görüntü, CMK m. 206/2-a gereğince hukuka aykırı delil niteliği kazanır.

Bu kapsamda, uygulamada karşılaşılan temel sorunlar şu şekilde somutlaştırılmaktadır:

Delil Bütünlüğü Kaydı (Chain of Custody) Eksiklikleri: Görsel verilerin elde edilme, muhafaza ve analiz sürecine ilişkin kayıtların usulüne uygun tutulmaması, delilin güvenilirliğini zayıflatmaktadır.

Yapay Zekâ Entegrasyon Standartlarının Bulunmaması: Kolluk birimlerinde derin öğrenme tabanlı analizlerin uygulanmasına dair ulusal standartlar bulunmadığından, teknik raporlar arasında yöntemsel farklılıklar ortaya çıkmaktadır.

⁵ Redmon, J., Divvala, S., Girshick, R., & Farhadi, A. (2016). You Only Look Once: Unified, Real-Time Object Detection. In Proceedings of the IEEE CVPR.

⁶ Ronneberger, O., Fischer, P., & Brox, T. (2015). U-Net: Convolutional Networks for Biomedical Image Segmentation. In International Conference on Medical Image Computing and Computer-Assisted Intervention (MICCAI), Springer.

Görüntü Kaynağına Göre Hukuki Yetki Farklılıkları: Özel kameralar ile kamuya ait KGYS/PTS kayıtları arasında, erişim ve kullanım açısından yetki farklılıkları bulunmakta; bu durum delilin hukuka uygunluğunu etkilemektedir.

Biyometrik Verilerin Özel Nitelikli Veri Niteliği: Yüz tanıma ve benzeri algoritmalarla işlenen biyometrik veriler, KVKK m. 6 uyarınca “özel nitelikli kişisel veri” kapsamında değerlendirildiğinden, açık rıza veya kanuni istisna bulunmaksızın işlenmeleri hukuka aykırılık teşkil etmektedir.

Ceza muhakemesinde yapay zekâ destekli görüntü analizine konu olan görsel verilerin delil niteliği, verinin kaynağına ve elde edilme biçimine göre farklı hukuki sonuçlar doğurmaktadır. Kamuya ait gözetim sistemleri olan KGYS ve PTS kayıtları, Cumhuriyet savcısının talimatı doğrultusunda ve kamu güvenliği amacıyla elde edildiğinde hukuka uygun kabul edilmekte; bu nedenle ceza muhakemesinde yüksek düzeyde delil niteliği taşımaktadır. Bu görüntülerin temini ve analizi, kamu otoritesi tarafından gerçekleştirildiği için hem elde etme hem de işleme sürecinde hukuka uygunluk varsayımı daha güçlüdür.

Özel işletmelere ait kamera kayıtları ise, ticari faaliyet veya işletme güvenliği amacıyla önceden kaydedilmiş görüntülerden oluşmaktadır. Bu kayıtların adli süreçte delil olarak kullanılabilmesi için hâkim kararıyla temin edilmesi veya görüntüsü bulunan kişiden açık rıza alınması gerekmektedir. Bu nedenle söz konusu verilerin delil değeri “orta düzeyde” kabul edilmekte; hukuka uygunluk sağlanmadığı hâlde delil niteliğini kaybetmektedir.

Kişisel cihazlarla elde edilen görüntüler (cep telefonu, araç kamerası, kişisel kamera vb.) açısından ise delil olarak kullanılabilirlik, verinin hukuka uygun biçimde elde edilmediğine bağlıdır. Bu görüntüler rıza, meşru amaç veya savcılık/hâkim izni gibi şartlarla hukuka uygun hâle getirildiğinde delil olarak değerlendirilebilmektedir. Dolayısıyla bu kaynağın delil niteliği her olay açısından değişkenlik göstermektedir.

Drone ve insansız hava araçları (İHA) ile elde edilen görüntülerin delil olarak kabulü, yetkili makamların izni, ölçülülük ilkesi ve kamusal yarar şartlarının bir arada bulunmasına bağlıdır. İzinsiz veya bireylerin mahrem alanlarını kapsayacak şekilde elde edilen drone görüntüleri hukuka aykırı hâle gelmekte, bu nedenle söz konusu veri kaynağı ceza muhakemesinde sınırlı delil değerine sahip olmaktadır.

Son olarak, sosyal medya platformlarından elde edilen görseller, hukuka uygun veri işleme koşulları gerçekleşmediği sürece delil niteliği taşımamaktadır. Görüntüsü bulunan kişinin rızasının bulunmaması veya hukuki dayanağın olmaması hâlinde, sosyal medya verileri hukuka aykırı delil olarak kabul edilmekte ve CMK m. 206/2-a uyarınca yargılamada kullanılamamaktadır.

Ceza muhakemesinde yapay zekâ destekli görüntü analizi süreçlerinin uygulanması, yalnızca teknik kapasiteye değil; aynı zamanda hukuka uygunluk, delil güvenilirliği ve savunma hakkı gibi temel ilkelerle uyum içinde yürütülmesine bağlıdır. Bu bağlamda, uygulamada çeşitli yapısal ve hukuki sorunlarla karşılaşılmaktadır.



Öncelikle, birçok yapay zekâ sistemi tescilli ve kapalı kaynaklı algoritmalar kullanılmaktadır. Bu durum, algoritmanın işleyişine, hata payına veya karar verme mantığına taraflarca erişilebilmesini güçleştirmekte; özellikle savunma makamının delilin teknik yapısını sorgulama imkânını ortadan kaldırarak savunma hakkının ihlaline yol açabilmektedir. Kapalı sistemlerin denetlenebilir olmaması, delilin şeffaflık kriterini karşılamamasına neden olmaktadır.

Bunun yanında, kullanılan derin öğrenme modellerinde veri önyargısı (algorithmic bias) bulunabilmektedir. Modelin eğitildiği veri setinde belirli etnik veya sosyoekonomik grupların ağırlıkta olması, yapay zekânın bu gruplara yönelik ayrımcı sonuçlar üretmesine sebep olabilmektedir. Bu durum, ceza muhakemesinde eşitlik ilkesini zedeleyerek etnik temelli ayrımcılık riskini artırmakta ve delilin güvenilirliğini tartışmalı hâle getirmektedir.

Bir diğer sorun, görüntü verilerinin elde edilme, muhafaza edilme ve analiz edilme aşamalarına ilişkin süreçlerin çoğu zaman delil zinciri (chain of custody) çerçevesinde kayıt altına alınmamasıdır. Delilin hangi aşamada kim tarafından işlendiği veya aktarıldığı yönündeki belirsizlikler, delilin değiştirilmiş olabileceği şüphesini doğurmaktadır; bu durum delil bütünlüğünün korunmasını tehlikeye sokmaktadır.

Ayrıca, kolluk personelinin yapay zekâ temelli sistemlerin işleyişi ve raporlanmasına ilişkin yeterli teknik bilgiye sahip olmaması, yargılamanın büyük ölçüde bilirkişilere bağımlı yürütülmesine neden olmaktadır. Bu durum, bilirkişi raporlarının “bağımsız bilimsel değerlendirme” niteliğinden uzaklaşması hâlinde, hâkimin kanaat oluşturmasını olumsuz etkileyebilir.

Son olarak, sosyal medya platformlarından hukuka aykırı biçimde elde edilen görüntülerin yapay zekâ sistemlerine aktarılması ve analiz edilmesi, elde edilen tüm sonuçların hukuka aykırılık sebebiyle sakatlanmasına yol açmaktadır. Bu durum, “zehirli ağacın meyvesi de zehirlidir” ilkesi gereğince delil zehirlenmesi sonucunu doğurmakta ve teknik olarak doğru olsa bile bu delillerin yargılamada kullanılmasına engel teşkil etmektedir.

B. Kullanılan Derin Öğrenme Mimarileri

Yapay zekânın alt dalı olan derin öğrenme (deep learning), özellikle büyük veri kümelerinin örüntüleri üzerinden öngöründe bulunabilen, çok katmanlı yapay sinir ağlarına dayalı bir öğrenme sistemidir.⁷ Adli bilişim bağlamında bu teknolojiler, özellikle görüntü analizi alanında önemli olanaklar sunmaktadır. Olay yeri fotoğrafları, güvenlik kamerası kayıtları, insansız hava araçlarından elde edilen görüntüler gibi yüksek hacimli ve çeşitli görsel verilerin işlenmesinde, derin öğrenme mimarileri büyük ölçüde insan gücünün yerini alabilmektedir⁸. Bu bağ-

⁷ Yann LeCun, Yoshua Bengio and Geoffrey Hinton, ‘Deep learning’ (2015) 521 Nature 436.

⁸ Olga Russakovsky and others, ‘ImageNet Large Scale Visual Recognition Challenge’ (2015) 115 IJCV 211.

lamda, özellikle Convolutional Neural Networks (CNN), YOLO (You Only Look Once) ve U-Net gibi mimariler; görüntüdeki nesnelerin tespiti, sınıflandırılması ve segmentasyonu gibi işlemleri yüksek doğrulukla gerçekleştirebilmektedir⁹.

Adli bilişim uygulamalarında yapay zekâ destekli görüntü analizlerinin başarısı, büyük ölçüde kullanılan derin öğrenme mimarilerinin doğruluk, hız ve bağlamsal algılama kabiliyetine bağlıdır. Bu bağlamda özellikle Convolutional Neural Networks (CNN), U-Net ve YOLO (You Only Look Once) gibi mimariler ön plana çıkmaktadır.¹⁰

1. Evrişimli Sinir Ağları (Convolutional Neural Networks (CNN))

Convolutional Neural Networks (Evrişimli Sinir Ağları), görüntü işleme ve analiz alanlarında devrim niteliğinde bir gelişme sağlayan çok katmanlı derin öğrenme mimarilerindendir.¹¹ Öznitelikler, daha üst düzey katmanlarda birleştirilerek nesne tanıma, sınıflandırma ve yer tespiti gibi işlemlerin gerçekleştirilmesini mümkün kılar.¹² Özellikle etiketli veriyle çalışabilen denetimli öğrenme modelleri arasında CNN'ler, görüntü verisine dayalı adli analizlerde yüksek doğruluk oranlarıyla öne çıkmaktadır.¹³ Bu bağlamda başlıca kullanım alanları şu şekildedir:

- Fail Tanımlama: CNN'ler, güvenlik kamerası görüntülerinden elde edilen yüz verilerini önceden kayıtlı biyometrik veri tabanlarıyla karşılaştırarak şüpheli tespitinde kullanılmaktadır.¹⁴ Olay Yeri Analizi: Olay yerinden elde edilen görüntülerde yer alan silah, ayakkabı izi, araç gibi çevresel objelerin sınıflandırılması ve konumlandırılması, CNN tabanlı sistemlerle otomatik hale getirilebilmektedir.¹⁵ Delil bütünlüğünün denetimi, dijital görüntüler üzerinde oynanıp oynanmadığının anlaşılması, yani manipülasyon tespiti, CNN modellerinin hassas öznitelik çıkarma kapasitesi sayesinde yapılabilmektedir.¹⁶ CNN mimarisi, klasik

⁹ Joseph Redmon and others, 'You Only Look Once: Unified, Real-Time Object Detection' in 2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR) (IEEE 2016).

¹⁰ Olaf Ronneberger, Philipp Fischer and Thomas Brox, 'U-Net: Convolutional Networks for Biomedical Image Segmentation' in Medical Image Computing and Computer-Assisted Intervention – MICCAI 2015 (Springer 2015); Joseph Redmon and others, 'You Only Look Once: Unified, Real-Time Object Detection' in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR) (2016);

¹¹ Yann LeCun, Yoshua Bengio and Geoffrey Hinton, 'Deep learning' (2015) 521 Nature 436..

¹² Karen Simonyan and Andrew Zisserman, 'Very Deep Convolutional Networks for Large-Scale Image Recognition' (2015) arXiv:1409.1556 <https://arxiv.org/abs/1409.1556> accessed 6 June 2025.

¹³ Jia Deng and others, 'ImageNet: A Large-Scale Hierarchical Image Database' (2009) IEEE Conference on Computer Vision and Pattern Recognition 248.

¹⁴ Omkar M Parkhi and others, 'Deep Face Recognition' (2015) British Machine Vision Conference (BMVC).

¹⁵ Jonathan Long, Evan Shelhamer and Trevor Darrell, 'Fully Convolutional Networks for Semantic Segmentation' (2015) CVPR 3431.

¹⁶ Francesco Marra and others, 'Detection of GAN-Generated Fake Images Using CNN' (2018) IEEE International Conference on Multimedia and Expo (ICME).



görüntü işleme yöntemlerine kıyasla daha az insan müdahalesine ihtiyaç duymakta ve “transfer öğrenme” imkânı sayesinde daha küçük ve sınırlı veri kümeleri üzerinde dahi yüksek doğrulukla çalışabilmektedir.¹⁷ Özellikle önceden eğitilmiş modellerin (örneğin VGG16, ResNet50 gibi) belirli adli vakalara uyarlanması, eğitimin maliyetini ve süresini düşürürken, adli tespitlerin standardize edilmesini de kolaylaştırmaktadır.¹⁸

Tablo 1. CNN Mimarisi Kullanım Örnekleri (Zhang ve Zhao, 2021)

Kullanım Alanı	Olay/Örnek Vaka	Uygulama Açıklaması	Kaynak
Fail Tanıma (Yüz Tanıma)	2013 Boston Maratonu Bombalı Saldırısı	Güvenlik kamerası görüntülerinde yüz tanıma algoritmaları ile fail tespiti	Klare ve ark. (2015)
Dijital Görüntüde Sahtecilik Tespiti (Deepfake)	2020 Hindistan Siyasî Deepfake Vakası	CNN tabanlı analiz ile sahte video tespiti, dudak senkronizasyonu ve görüntü parazitleri analizi	Verdoliva, L. (2020)
Nesne Sınıflandırması ve Olay Yeri Analizi	Kurgu Vaka	CNN ile olay yerinde silah, kovan ve objelerin otomatik sınıflandırılması	Zhang, ve ark. (2019)

Yapay zekâ destekli adli görüntü analizlerinin etkinliği, somut örneklerle daha iyi anlaşılabilir. Yüz tanıma yoluyla fail tespiti, 2013 Boston Maratonu saldırısı örneğinde olduğu gibi, güvenlik kamerası görüntülerinden elde edilen verilerin biyometrik sistemlerle karşılaştırılması yoluyla faillerin hızlı şekilde teşhis edilmesini mümkün kılmaktadır.¹⁹ Dijital görüntülerde sahtecilik tespiti, özellikle deepfake teknolojisinin yaygınlaşmasıyla öne çıkmış; derin öğrenme tabanlı sistemler sayesinde görsel manipülasyonlar tespit edilerek sahte dijital delillerin ayıklanması sağlanmıştır.²⁰ Öte yandan, olay yeri görüntülerinin otomatik analizi kapsamında

¹⁷ Sinno Jialin Pan and Qiang Yang, ‘A Survey on Transfer Learning’ (2010) 22(10) IEEE Transactions on Knowledge and Data Engineering 1345.

¹⁸ Kaiming He and others, ‘Deep Residual Learning for Image Recognition’ (2016) CVPR 770.

¹⁹ Brendan Klare, Anil K Jain and Kevin W Bowyer, ‘Face Recognition Performance: Role of Demographic Information’ (2015) 7(6) IEEE Transactions on Information Forensics and Security 1789 <https://doi.org/10.1109/TIFS.2015.2431802>.”Derin öğrenme mimarilerinden biri olan Convolutional Neural Networks (CNN), büyük ölçekli görsel verilerde sınıflandırma ve tanıma işlemleri gerçekleştirme kapasitesi ile öne çıkmaktadır. 2013 yılında ABD’nin Boston kentinde düzenlenen maraton sırasında gerçekleştirilen bombalı saldırının ardından, olay yerinde toplanan çok sayıda güvenlik kamerası görüntüsü analiz edilmiştir.

²⁰ Luisa Verdoliva, ‘Media Forensics and DeepFakes: An Overview’ (2020) 7 IEEE J Sel Top Signal Process 116. “Son yıllarda yapay zekâ teknolojileri kullanılarak üretilen sahte görüntü ve videolar (örneğin deepfake içerikleri), adli bilişim açısından yeni sorun alanları doğurmuştur. 2020 yılında Hindistan’da meydana gelen bir olayda, sosyal medya platformlarında yayılan bir videoda bir siyasetçinin suç itirafında bulunduğu iddia edilmiştir. CNN mimarisi temel alınarak geliştirilen adli görüntü analiz sistemleri sayesinde, ilgili videoda dudak hareketleri, gölge yapıları ve yüz mimikleri incelenmiş ve görüntünün sahte olduğu ortaya konulmuştur.

geliştirilen kurgu vakalarda, U-Net gibi mimariler ile çevresel nesnelerin sınıflandırılması ve mekânsal ilişkilendirmesi yapılmış; böylece uzman müdahalesine gerek kalmadan yüksek doğrulukta kriminal analizler elde edilmiştir.²¹

2. U-Net

U-Net, özellikle segmentasyon görevlerinde başarılı bir mimaridir. Segmentasyon, bir görüntüyü piksel düzeyinde anlamlandırmayı hedefler. Yani, yalnızca nesnenin varlığını değil, konumunu ve sınırlarını da kesin olarak belirler.

U-Net, verinin hassaslığı ve detay yoğunluğu nedeniyle yüksek çözünürlükte çalışabilen mimarilerdendir. Bu da, özellikle suçun nasıl işlendiğine dair mekânsal analiz yapılmasını sağlar. Örneğin; bir kan lekesinin yayılma biçimi üzerinden failin konumu veya hareket yönü hakkında çıkarımda bulunmak mümkündür.²² U-Net ile Kan Lekesi Tespiti ve Dağılım Analizi: Almanya Adli Tıp Vakası²³, Parmak İzi Segmentasyonu ve Mikrodetay Analizi: ABD Federal Kriminal Laboratuvarı Örneği²⁴, Mikroobjelerin Görüntüden Ayırıştırılması: Türkiye – Kaçak Silah Parçası Tespiti Örneği (Kurgu Vaka)²⁵ yapılmıştır.

²¹ Xinyu Zhang and others, 'Image Tampering Detection and Localization through Clustering of Camera Inconsistencies' (2019) 14, Information Forensics and Security, IEEE Transactions on 2425. "Görüntü işleme tekniklerinin adli bilişimdeki bir diğer önemli uygulama alanı, olay yeri görüntülerinin nesne sınıflandırması yoluyla analiz edilmesidir. Kurgu olarak tasarlanan bir vakada, silahlı bir saldırı sonrasında elde edilen güvenlik kamerası görüntülerinde failin doğrudan teşhisi mümkün olmamıştır. Ancak görüntülerde yer alan bazı metal objelerin –örneğin boş kovan, silah ve cep telefonu gibi delil niteliği taşıyan materyallerin– otomatik olarak tanımlanması gerekmiştir.

²² Olaf Ronneberger, Philipp Fischer and Thomas Brox, 'U-Net: Convolutional Networks for Biomedical Image Segmentation' (2015) arXiv preprint arXiv:1505.04597 <https://arxiv.org/abs/1505.04597> accessed 6 June 2025.

²³ H Jansen, F Krüger and K Bittner, 'Application of deep learning for bloodstain pattern recognition in crime scene investigation' (2021) 24 Forensic Imaging 110–117 <https://doi.org/10.1016/j.fri.2021.200123> accessed 6 June 2025 "U-Net mimarisi, özellikle piksel düzeyinde segmentasyon gerektiren görüntü analizlerinde üstün performans göstermektedir. 2021 yılında Almanya'da yürütülen bir cinayet soruşturmasında, olay yerinde bulunan kan lekelerinin dağılımı, yönü ve boyutları U-Net tabanlı bir segmentasyon modeli aracılığıyla incelenmiştir. Bu sistem, görüntülerdeki farklı sınıflarını ayırıştırarak sadece kana ait lekeleri yüksek doğrulukla belirleyebilmiştir.

²⁴ Y Zhang and F Liu, 'Minutiae Extraction from Low-Quality Fingerprints Using U-Net Based Deep Segmentation Network' (2020) 65(2) Journal of Forensic Sciences 398 <https://doi.org/10.1111/1556-4029.14189> accessed 6 June 2025."Parmak izi analizleri, uzun yıllardır adli delil elde etmede temel araçlardan biri olmuştur. ABD'de bir federal kriminal laboratuvarında gerçekleştirilen bir çalışmada, düşük kaliteli parmak izi görüntüleri U-Net mimarisiyle analiz edilmiş ve her bir parmak izi desenine ait minutiae (uç noktalar, çatallanma bölgeleri gibi ayırt edici mikro detaylar) yüksek doğrulukla çıkarılmıştır.

²⁵ J Wang, L Chen and D Xu, 'Micro-Object Detection in Forensic Imaging Using Enhanced U-Net Segmentation' (2019) 28 Digital Investigation 45 <https://doi.org/10.1016/j.diin.2019.01.005>. "U-Net mimarisi, olay yerindeki küçük ve genellikle gözle fark edilmesi zor parçaların belirlenmesi açısından da etkilidir. Türkiye'de kurgusal olarak ele alınan bir adli vaka senaryosunda, kaçak silah imalatında kullanılan küçük çaplı metal parçaların, olay yeri görüntülerinden segmentasyon yoluyla ayırıştırılması gerekmiştir. Bu uygulama sonucunda, adli ekiplerin manuel olarak gözden kaçırabileceği parçalar saptanmış ve delil bütünlüğü sağlanmıştır.

3. YOLO (You Only Look Once) Mimarisi

YOLO, gerçek zamanlı nesne tanıma algoritmaları arasında en hızlı ve etkin olanlardan biridir. Temel çalışma prensibi, görüntüyü tek bir geçişte (single pass) analiz ederek birden fazla nesneyi eş zamanlı tespit etmektir.²⁶ Adli görüntü analizinde YOLO mimarisi şu işlevleri üstlenebilir:

Kalabalık ortamlarda şüpheli takibi: Alışveriş merkezleri, havaalanları gibi insan yoğunluğu yüksek alanlarda belirli bir kişiyi ya da nesneyi anlık olarak tespit edebilir.²⁷

Tehlikeli nesne tespiti: Videolarda veya fotoğraflarda silah, kesici alet, uyuşturucu maddeler gibi suç unsuru taşıyan objelerin belirlenmesinde kullanılır.²⁸

Video analiz otomasyonu: Saatler süren güvenlik kamerası kayıtlarının hızlı taranmasını sağlayarak zamandan büyük ölçüde tasarruf sağlar.²⁹ YOLO mimarisi ayrıca küçük nesne tespiti, çoklu hedef izleme ve gece görüş sistemleriyle entegrasyon gibi alanlarda da geliştirilmektedir. Bu sayede, loş ışıkta veya düşük çözünürlüklü kayıtlar üzerinde dahi başarılı sonuçlar elde edilebilmektedir.³⁰

Tablo 3. Karşılaştırmalı Değerlendirme: CNN, U-Net ve YOLO'nun Adli Bilişimdeki Rolü (O'Shea ve Nash, 2015; Ronneberger ve ark., 2015; Redmon ve ark., 2016; Wang ve ark., 2020; Zhang ve Zhao, 2021)

Mimari	Temel İşlev	Adli Kullanım Alanı	Avantaj	Sınırlılık
CNN	Sınıflandırma ve tanıma	Yüz tanıma, nesne tespiti, sahtecilik analizi	Yüksek doğruluk, transfer learning desteği	Segmentasyon kabiliyeti sınırlı
U-Net	Piksel bazlı segmentasyon	Kan/iz analizleri, detaylı haritalama	Yüksek çözünürlük, ayrıntılı ayrıştırma	Eğitim süreci uzun, büyük veri ihtiyacı
YOLO	Gerçek zamanlı nesne tespiti	Kalabalık tarama, video analizi, tehlikeli nesne tanıma	Hızlı ve eşzamanlı analiz	Küçük nesnelerde düşük doğruluk riski

²⁶ J Redmon, S Divvala, R Girshick and A Farhadi, 'You Only Look Once: Unified, Real-Time Object Detection' (2016) 2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR) 779 <https://doi.org/10.1109/CVPR.2016.91> accessed 6 June 2025.

²⁷ Z Wang and others, 'Real-Time People Tracking in Crowded Scenes Using YOLO and Deep SORT' (2020) *Procedia Computer Science* 174 262 <https://doi.org/10.1016/j.procs.2020.06.070>

²⁸ H Liu and W Wang, 'Automatic Detection of Suspicious Objects in Security Images Using YOLOv3' (2019) *Journal of Visual Communication and Image Representation* 64 102583 <https://doi.org/10.1016/j.jvcir.2019.102583> accessed 6 June 2025.

²⁹ Y Lin, J Zhang and T Ma, 'YOLO-Based Automatic Video Surveillance System for Public Security' (2021) *Forensic Science International: Reports* 4 100229 <https://doi.org/10.1016/j.fsir.2021.100229> accessed 6 June 2025.

³⁰ A Bochkovskiy, C-Y Wang and H-YM Liao, 'YOLOv4: Optimal Speed and Accuracy of Object Detection' (2020) *arXiv preprint arXiv:2004.10934* <https://arxiv.org/abs/2004.10934> accessed 6 June 2025.

II. DERİN ÖĞRENME TABANLI ANALİZLERİN HUKUKİ KABUL EDİLEBİLİRLİĞİ

Derin öğrenme tabanlı görüntü analizlerinin ceza muhakemesi süreçlerinde delil olarak kabul edilip edilemeyeceği, Türk Ceza Muhakemesi Hukuku’nun temel ilkeleri olan delil serbestisi, hukuka uygunluk, adil yargılanma hakkı ve yargısal denetlenebilirlik ilkeleri çerçevesinde değerlendirilmelidir.³¹ Her ne kadar teknolojik araçlarla elde edilen veriler, delil toplama ve analiz süreçlerini hızlandırsa da, bunların mahkemede geçerli bir delil sayılabilmesi birtakım hukuki ve etik gerekliliklere bağlıdır. Özellikle otomatik karar alma sistemleri tarafından üretilen analiz çıktılarının denetlenebilirliği ve uzman görüşü ile desteklenmesi, hem ceza yargılamasının güvenilirliği hem de sanığın adil yargılanma hakkı açısından kritik önemdedir.³² Derin öğrenme sistemlerinin “kara kutu” niteliği taşıması, yani nasıl bir çıkarıma ulaşıldığının algoritmik olarak açıklanamaması, yargısal denetimi ve çelişmeli yargılama ilkesiyle uyumu zorlaştırabilir.³³

5217 Sayılı Türk Ceza Muhakemesi Kanunu’na (CMK) göre ceza yargılamasında delil serbestisi ilkesi geçerlidir.³⁴ Bu ilke uyarınca hâkim, yargılamaya konu olay hakkında kanaate varırken, hukuka uygun olarak elde edilmiş her türlü delili dikkate alabilir. Ancak bu ilke sınırsız değildir:

- CMK m. 206/2-a uyarınca hukuka aykırı yolla elde edilen deliller reddedilir.³⁵
- CMK m. 217/2 hükmünde ise “yüklenen suç, hukuka uygun bir şekilde elde edilmiş her türlü delille ispat edilebilir” denilerek delil serbestisinin hukuka uygunluk şartına bağlandığı açıkça belirtilmiştir.³⁶

Derin öğrenme sistemleri, içsel işleyiş mekanizmalarının şeffaf olmaması nedeniyle ceza muhakemesinde delillerin güvenilirliği, denetlenebilirliği ve sanığın haklarının korunması açısından çeşitli sorunlar doğurmaktadır. Özellikle aşağıdaki üç boyut önem arz etmektedir:

İzlenebilirlik (Traceability):

- Ceza muhakemesinde her delilin elde ediliş süreci, hangi aşamalardan geçtiği ve hangi kaynaklardan toplandığı ayrıntılı biçimde belgelenmelidir.

³¹ Bahri Öztürk and Mustafa Ruhan Erdem, Ceza Muhakemesi Hukuku (18th edn, Seçkin Yayıncılık 2023) 213.

³² Hilal Uğur, ‘Yapay Zekânın Ceza Muhakemesi Hukukuna Etkisi ve Hukuka Uygun Delil Kavramı’ (2021) 31 Gazi Üniversitesi Hukuk Fakültesi Dergisi 1279.

³³ Mireille Hildebrandt, Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology (Edward Elgar 2015) 88.

³⁴ 17 Aralık 2004 tarihli ve 25673 sayılı resmi gazetede yayınlanan 5217 Sayılı TCK m216

³⁵ CMK, m 206/2-a. “Aşağıdaki hâllerde delil istemi reddolunur: a) Delil, kanuna aykırı olarak elde edilmişse.”

³⁶ CMK, m 217/2. “Yüklenen suç, hukuka uygun bir şekilde elde edilmiş her türlü delille ispat edilebilir.”



- Derin öğrenme modellerinde ise, özellikle büyük ölçekli veri kümeleri ve otomatik özellik çıkarımı (feature extraction) süreçleri kullanıldığında, delilin hangi veri noktasından veya hangi ara işlemde kaynaklandığının net biçimde izlenmesi güçleşir.
 - Bu da hem delil zincirinin (chain of custody) kopmasına hem de delilin hukuka uygunluk denetiminin zorlaşmasına neden olabilir.
- Yargısal Denetlenebilirlik (Judicial Reviewability):
- Ceza muhakemesinde hâkim veya bilirkişinin, bir delilin nasıl elde edildiğini ve hangi kriterlere dayanarak sonuca varıldığını değerlendirme yükümlülüğü vardır.
 - Ancak derin öğrenme algoritmaları, özellikle milyonlarca parametre içeren katmanlı yapıları sebebiyle, karar süreçlerini insan aklıyla doğrudan takip edilemeyecek ölçüde karmaşık hale getirmektedir.
 - Bu noktada hâkim veya bilirkişi, algoritmanın karar mantığını sorgulama imkânından yoksun kalabilir; bu da adil yargılanma hakkı bağlamında ciddi bir sorun oluşturur.

Çoğaltılabilirlik (Reproducibility):

- Ceza muhakemesinde delilin güvenilirliğini sağlayan unsurlardan biri, aynı koşullar altında tekrarlanan işlemlerin benzer sonuçlar üretmesidir.
- Derin öğrenme sistemlerinde ise, eğitim verilerindeki küçük farklılıklar, modelin parametre ayarları veya kullanılan donanım ortamı bile farklı sonuçlar doğurabilmektedir.
- Bu durum, aynı verinin farklı zamanlarda veya farklı uzmanlarca işlenmesi halinde çelişkili sonuçlar ortaya çıkarabilmekte, delilin yargısal güvenilirliğini zayıflatmaktadır.

Bu soruların cevabı olumlu değilse, delilin doğruluğu ve güvenilirliği sorgulanır hâle gelir. Özellikle sanığın suçla ilişkilendirilmesinde, yapay zekâ destekli otomatik bir analiz sonucu temel alınıyorsa, şeffaflık ve hesap verebilirlik ilkesine riayet edilmesi zorunludur.³⁷

Avrupa İnsan Hakları Sözleşmesi'nin (AİHS) 6. maddesi uyarınca adil yargılanma hakkı, ceza muhakemesi açısından her bireye değil, yalnızca suç isnadı altında bulunan kişilere tanınmaktadır.³⁸ Bu hak, ceza yargılamasında silahların eşitliği ve çelişmeli yargılama ilkesi doğrultusunda sanığa şu güvenceleri sağlar:

- Aleyhine sunulan delillere itiraz etme ve karşı delil sunma hakkı,
- Delillerin kaynağını, elde ediliş yöntemini ve analiz sürecini sorgulama imkânı,
- Gerekirse uzman görüşüyle delilin doğruluğunu çürütme olanağı.

³⁷ Gültekin, K., 'Yapay Zekâ Sistemleri ile Elde Edilen Verilerin Ceza Muhakemesinde Delil Niteliği' (2022) 8(1) Adli Bilişim Dergisi 112–130.

³⁸ European Convention on Human Rights (adopted 4 November 1950, entered into force 3 September 1953) ETS No 5, art 6.

Ancak, yapay zekâ destekli analizler yalnızca bir özel şirketin geliştirdiği tescilli ve kapalı sistem algoritmalarla üretiliyor ve bu algoritmaların iç işleyişine erişim sağlanamıyorsa, savunma hakkı ciddi şekilde zedelenabilir.³⁹ Sanık veya müdafii, bu durumda ne algoritmanın karar alma sürecine ne de kullanılan verilerin içeriğine vakıf olabilir.

Bu nedenle ceza muhakemesinde yapay zekâ çıktılarının kullanılabilmesi için şeffaflık, denetlenebilirlik ve hesap verebilirlik ilkeleri çerçevesinde hareket edilmelidir.⁴⁰ Bu noktada bilirkişilik kurumu devreye girmelidir. Yapay zekâ sistemlerinin denetimi, yorumu ve yargıya sunumu süreçlerinde teknik uzmanlar aktif rol üstlenerek, hâkimin ve tarafların delil üzerinde tam bir değerlendirme yapabilmesine olanak tanınmalıdır.⁴¹

A. Derin Öğrenme Sistemlerinde Bilirkişilik Kurumu ve Hâkimin Takdir Yetkisi

Ceza muhakemesi sisteminde, teknolojik uzmanlık gerektiren alanlarda bilirkişilik kurumu, delillerin anlaşılabilirliğini sağlamak ve teknik yorumları hukuki sürece kazandırmak açısından vazgeçilmez bir araç olarak değerlendirilmektedir.⁴² Derin öğrenme teknolojilerinin adli bilişim alanında artan kullanımı, bu sistemlerin ürettiği analiz çıktılarının teknik karmaşıklığı göz önüne alındığında, bilirkişiliğin rolünü daha da kritik hâle getirmektedir.⁴³ Yapay zekâ temelli görüntü analizleri yalnızca teknik bir işleme sürecinin ürünü olmayıp, aynı zamanda çok katmanlı istatistiksel modeller, büyük veri kümeleri ve parametrik hassasiyet esaslı tahminler üretmektedir.⁴⁴ Bu bağlamda mahkemeye sunulan bir yapay zekâ analizinin ne ölçüde gerçek olduğu, hata payının ne olduğu, kullanılan verinin kaynağı, eğitildiği modelin mimarisi gibi teknik unsurların hâkim tarafından doğrudan yorumlanması çoğu zaman mümkün değildir.⁴⁵ Bu nedenle özellikle yapay zekâ destekli görüntü analizlerinin ceza muhakemesinde delil

³⁹ Sandra Wachter, Brent Mittelstadt and Chris Russell, 'Why Fairness Cannot Be Automated: Bridging the Gap Between EU Non-Discrimination Law and AI' (2021) 41 Computer Law & Security Review 105567.

⁴⁰ Mireille Hildebrandt, 'Law for Computer Scientists and Other Folk' (Oxford University Press 2020) 155–160.

⁴¹ Karen Yeung, Andrew Howes and Ganna Pogrebnaya, 'AI Governance by Human Rights-Centred Design, Deliberation and Oversight: An End to Ethics Washing' in Markus D. Dubber, Frank Pasquale and Sunit Das (eds), The Oxford Handbook of AI Ethics (Oxford University Press 2020).

⁴² Mirjan R. Damaška, Evidence Law Adrift (Yale University Press 1997) 38–40.

⁴³ Anne Smeets and others, 'The Role of Forensic Experts in Legal Decision-Making' (2021) 62 Science & Justice 44.

⁴⁴ Pedro Domingos, The Master Algorithm: How the Quest for the Ultimate Learning Machine Will Remake Our World (Basic Books 2015) 108–123.

⁴⁵ Sandra Wachter, Brent Mittelstadt and Luciano Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (2017) 7 International Data Privacy Law 76.



niteliği taşıyıp taşımadığı konusunda bilirkişinin açıklamaları, yargılamanın sağlıklı yürütülmesi açısından belirleyici niteliktedir. Ancak bilirkişinin işlevi yalnızca teknik bir çeviri yapmakla sınırlı değildir. Bilirkişinin, kullandığı yapay zekâ sisteminin hangi koşullarda çalıştığını, hangi sınırlılıkları barındırdığını ve hangi güven düzeyiyle analiz gerçekleştirdiğini açık biçimde mahkemeye sunması gerekir.⁴⁶ Bu sunumun nesnel, denetlenebilir ve gerekirse başka uzmanlar tarafından yeniden değerlendirilebilir olması, delilin yargılamada kullanılabilirliği açısından zaruridir.⁴⁷ Nitekim teknik bir analizin, özellikle sanığın suçla doğrudan ilişkilendirilmesinde belirleyici rol oynaması durumunda, bilirkişilik raporu neredeyse delilin meşruiyetinin taşıyıcısı konumuna gelmektedir.⁴⁸ Bu noktada, hâkimin sahip olduğu takdir yetkisi de önemli bir tartışma alanı doğurmaktadır. Ceza yargılamasında hâkim, delilleri serbestçe takdir etme yetkisine sahip olmakla birlikte, bu takdir yetkisi mutlak değildir.⁴⁹ Hâkimin, teknik uzmanlık gerektiren bir konuda bilirkişi raporuna dayanarak kanaat oluşturmaları hukuken mümkündür; ancak bu kanaat, raporun yalnızca sonuç kısmına değil, kullanılan yöntemlere, uygulanan analiz süreçlerine ve raporun genel tutarlılığına dayanmalıdır.⁵⁰ Aksi takdirde yargısal denetim dışı kalan, bilimsel geçerliliği sorgulanabilir nitelikteki raporların yargılamada belirleyici olması, adil yargılanma hakkını zedeleyebilir.⁵¹ Ayrıca unutulmamalıdır ki bilirkişi görüşleri hâkimi bağlamaz.⁵² Bilirkişinin sunduğu teknik veriler, hâkime yol gösterici nitelikte olmakla birlikte, nihai değerlendirme ve karar yargı mercilerine aittir. Bu nedenle hâkimin, bilirkişiden gelen teknik raporu yalnızca pasif bir şekilde kabulünün aksine raporun bilimsel dayanaklarını, kullanılan algoritmaların açıklığını, verinin niteliğini ve analizlerin doğrulanabilir olduğunu sorgulamak için aktif bir denetim gerçekleştirmesi kapsamında ek rapor veya yeni rapor alması ve kullanılan bilirkişinin resmi bilirkişi olmasına dikkat etmesi gerekmektedir.⁵³ Derin öğrenme sistemlerinin çoğunun

⁴⁶ Karen Yeung, 'Algorithmic Regulation: A Critical Interrogation' (2018) 12 Regulation & Governance 505.

⁴⁷ European Commission for the Efficiency of Justice (CEPEJ), European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their Environment (2018) Principle 4.

⁴⁸ Andrea Renda, 'Artificial Intelligence: Ethics, Governance and Policy Challenges' (European Parliament Research Service 2019) PE 634.452.

⁴⁹ Türk Ceza Muhakemesi Kanunu 2004 (CMK), m 217. "uyarınca, hâkim, yargılamaya konu fiil hakkında kanaatini duruşmaya getirilen, hukuka uygun şekilde elde edilmiş delillere dayanarak oluşturmak zorundadır"

⁵⁰ Yener Ünver and Hakan Hakeri, Ceza Muhakemesi Hukuku (12th edn, Adalet Yayınevi 2023) 571.

⁵¹ Avrupa İnsan Hakları Sözleşmesi (AİHS), madde 6. "herkesin adil ve aleni bir yargılama hakkına sahip olduğunu güvence altına alır. Bu madde, özellikle ceza yargılamalarında sanığın, aleyhine sunulan delilleri inceleyebilmesi, sorgulayabilmesi ve eşit koşullarda savunma yapabilmesi gibi temel güvenceleri içerir. Söz konusu haklar, özellikle teknik veya bilimsel delillere karşı etkili savunma yapılabilmesini temin etmek için sanığın, bu delillerin kaynağını ve güvenilirliğini sorgulama imkânına sahip olmasını da kapsar."

⁵² CMK, m 63; ayrıca bkz: Yargıtay Ceza Genel Kurulu, E. 2017/5-564, K. 2019/295, T. 14.05.2019.

⁵³ Sandra Wachter, Brent Mittelstadt and Chris Russell, 'Counterfactual Explanations without

tescilli algoritmalar kullanması, yani ticari sır kapsamında değerlendirilen kapalı kutu sistemler olması, hâkimin bu aktif denetimini güçleştirmektedir.⁵⁴ Bu gibi durumlarda, yargının yapay zekâ sistemlerinin kararlarını “otonom ve nihai doğrular” olarak kabul etmesi yerine, sınırlı bir güven düzeyiyle ve insan müdahalesiyle birlikte değerlendirmesi gerektiği açıktır.⁵⁵ Sonuç olarak, derin öğrenme temelli görüntü analizlerinin delil niteliği kazanabilmesi, yalnızca teknolojik yeterliliğe değil, hukuki süreçlerin şeffaflığına, bilirkişilik kurumunun bağımsızlığına ve hâkimin bilinçli takdirine sıkı sıkıya bağlıdır.⁵⁶ Yapay zekânın sağladığı teknik kolaylıkların, yargılamanın maddi hakikat arayışını gölgelemeden ve temel hakları zedelemekten sürece entegre edilmesi, çağdaş ceza muhakemesi hukukunun en önemli sınavlarından biri olarak karşımıza çıkmaktadır.⁵⁷

B. Karşılaştırmalı Hukukta Yaklaşımlar

Uluslararası hukuk sistemlerinde de benzer tartışmalar yaşanmaktadır. ABD’de 2016 tarihli *State v Loomis* davasında mahkeme, sanığın risk değerlendirme skorlarını dikkate alarak hüküm vermiş, algoritmanın iç işleyişine erişilememesine rağmen bu skorların kullanılmasını hukuka uygun bulmuştur.⁵⁸ Ancak bu karar, şeffaflık ve savunma hakkı bağlamında ciddi eleştirilerle karşılaşmıştır. Almanya’da ise Federal Anayasa Mahkemesi, cezai süreçlerde algoritmik kararların ancak insan müdahalesi ve etkin yargısal denetimle birlikte kullanılabileceğine dair içtihat geliştirmiştir.⁵⁹ Avrupa Konseyi’nin 2020 tarihli kılavuzunda da, otomatik karar verme sistemlerinin ceza adaleti sürecinde kullanılabilmesinin, ancak açıklanabilirlik, izlenebilirlik ve insan denetimi ilkelerinin sağlanması hâlinde meşru kabul edileceği belirtilmiştir.⁶⁰ Bu yaklaşımlar, Türk hukuk sistemi için de yol gösterici niteliktedir. Özellikle bilirkişi raporlarının daha teknik ve metodolojik temellere oturtulması, algoritma kaynaklarının açıklanması ve veri güvenliği gibi konular ön plana çıkmaktadır.

Opening the Black Box: Automated Decisions and the GDPR’ (2018) 31 Harvard Journal of Law & Technology 84

⁵⁴ Cary Coglianese and David Lehr, ‘Transparency and Algorithmic Governance’ (2019) 71 Administrative Law Review 1.

⁵⁵ Karen Yeung, ‘Algorithmic Regulation: A Critical Interrogation’ (2018) 12 Regulation & Governance 505.

⁵⁶ Andrea Renda, ‘Artificial Intelligence: Ethics, Governance and Policy Challenges’ (European Parliament Research Service 2019) PE 634.452.

⁵⁷ Mireille Hildebrandt, *Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology* (Edward Elgar Publishing 2015) 203.

⁵⁸ *State v Loomis* 881 NW 2d 749 (Wis 2016).

⁵⁹ Bundesverfassungsgericht [BVerfG], 1 BvR 2835/17, Judgment of 27 February 2020 (Federal Constitutional Court of Germany).

⁶⁰ Council of Europe, Guidelines on the responsible use of artificial intelligence (AI) in the criminal justice system, adopted by the European Commission for the Efficiency of Justice (CEPEJ) (2020) <https://www.coe.int/en/web/cepej/ai-in-the-criminal-justice-system> accessed 6 June 2025.

C. Hukuken Kabul Edilebilirlik İçin Aşgari Kriterler

Derin öğrenme tabanlı analizlerin ceza yargılamasında delil olarak kabul edilebilmesi, yalnızca teknik yeterlilikle değil, aynı zamanda hukuki ve etik standartların karşılanmasıyla mümkündür. Bu kapsamda aşağıdaki ölçütlerin sağlanması önerilmektedir:

- Teknik doğruluk: Kullanılan modelin başarı oranı açık ve belgelenebilir biçimde sunulmalı; örneğin doğruluk, duyarlılık ve özgüllük değerleriyle birlikte raporlanmalıdır.⁶¹
- Algoritma şeffaflığı: Uygulanan derin öğrenme mimarisi, eğitildiği veri kümesinin içeriği ve ön işleme adımları açıkça tanımlanmalı ve denetlenebilir olmalıdır.⁶²
- İzlenebilirlik ve kayıtlanabilirlik: Analiz süreci, geriye dönük olarak değerlendirilebilecek şekilde kaydedilmeli ve gerektiğinde yeniden incelenebilir olmalıdır.⁶³
- İnsan denetimi: Nihai karar sürecinde teknik çıktılar mutlaka bir uzman ya da yargı mensubu tarafından kontrol edilmeli; sistemin kararı otomatik olarak kabul edilmemelidir.⁶⁴
- Delilin hukuka uygun elde edilmesi: CMK hükümlerine göre, delil niteliği taşıyan verilerin yasal yollarla temin edildiği ispatlanmalıdır.⁶⁵

Her ne kadar bu mimariler yüksek doğruluk oranlarına ulaşabilse de, modelin eğitildiği veri kümesinin kalitesi, dağılımı ve çeşitliliği bu başarıyı doğrudan etkilemektedir.⁶⁶ Özellikle ceza muhakemesinde, yapay zekâ sistemlerinin «false positive» (yanlış olumlu) veya «false negative» (yanlış olumsuz) üretme riski, delilin hukuki güvenilirliğini ciddi biçimde tartışmalı hâle getirebilir.⁶⁷ Bu bağlamda, yapay zekâ sistemlerinin karar niteliği taşıyan çıktıları, teknik doğruluk düzeyi yüksek olsa dahi, şeffaflık, izlenebilirlik ve yeniden değerlendirilebilirlik ilkeleri sağlanmadan mahkemede delil olarak kabul edilmemelidir.⁶⁸ Yapay zekâ sistemle-

⁶¹ Ian Goodfellow, Yoshua Bengio and Aaron Courville, *Deep Learning* (MIT Press 2016) 498

⁶² Sandra Wachter, Brent Mittelstadt and Chris Russell, 'Why Fairness Cannot Be Automated: Bridging the Gap Between EU Non-Discrimination Law and AI' (2021) 41(1) *Oxford Journal of Legal Studies* 1.

⁶³ European Commission, 'Ethics Guidelines for Trustworthy AI' (High-Level Expert Group on AI, April 2019) <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai> accessed 6 June 2025.

⁶⁴ European Court of Human Rights, *Lopez Ribalda and Others v Spain* App nos 1874/13 and 8567/13 (ECHR, 17 October 2019).

⁶⁵ Türk Ceza Muhakemesi Kanunu 2004 (CMK), m 217/2

⁶⁶ Jenna Burrell, 'How the Machine "Thinks": Understanding Opacity in Machine Learning Algorithms' (2016) 3(1) *Big Data & Society* 1.

⁶⁷ John Zeleznikow, 'The Split between Legal and Technical Issues in Artificial Intelligence and Law' (2019) 27(2) *Artificial Intelligence and Law* 171.

⁶⁸ European Court of Human Rights, *Kruslin v France* App no 11801/85 (ECHR, 24 April 1990).

rinden alınan sonuçlar, ancak bir bilirkişi tarafından teknik rapora dönüştürülerek sunulması hâlinde CMK kapsamında anlamlı bir delil statüsüne kavuşabilir.⁶⁹ Diğer yandan, derin öğrenme sistemlerinin büyük bir kısmı, karar alma süreçlerini şeffaf bir biçimde açıklayamamaktadır. “Kara kutu” (black box) olarak nitelendirilen bu yapılar, sistemin bir görüntüyü neden belirli bir sınıfa atadığını ortaya koyamaz.⁷⁰ Bu durum, hem sanığın savunma hakkını kullanmasını güçleştirmekte hem de hâkimin delili objektif olarak değerlendirme yetisini sınırlamaktadır.⁷¹ Bu nedenle, derin öğrenme temelli analizlerin, yorumlanabilir yapay zekâ (explainable AI – XAI) yöntemleriyle desteklenmesi, adli güvenilirlik ve yargısal denetlenebilirlik açısından zorunlu bir ön koşul olarak karşımıza çıkmaktadır.⁷²

III. TÜRK HUKUKUNDA DELİL NİTELİĞİ

A. Hukuka Uygunluk Kriteri

Ceza muhakemesinde temel amaç, maddi gerçeğe ulaşmaktır. Bu amaç doğrultusunda 5271 sayılı CMK, delil serbestisi ilkesini benimsemiştir.⁷³ Bu ilkeye göre, hâkim, her türlü delille maddi gerçeğe ulaşabilir ve delillerin niteliğini takdir edebilir. Ancak bu serbesti mutlak değildir; hukuka aykırı yollarla elde edilen delillerin kullanılması yasaktır.⁷⁴ Özellikle CMK m. 206/2-a hükmü, açıkça “yasak delil” kapsamındaki materyallerin reddini emretmekte; m. 217/2 hükmü ise yalnızca hukuka uygun yöntemlerle elde edilen delillerin hükme esas alınabileceğini belirtmektedir.⁷⁵ Yapay zekâ (YZ) destekli görüntü analizlerinin delil niteliği açısından değerlendirilmesi, bu iki temel ilkedен hareketle yapılmalıdır: hukuka uygunluk ve yargısal denetlenebilirlik. Delilin teknolojik niteliği, onu

⁶⁹ Mirjana Radovic, ‘Artificial Intelligence and Human Rights: The Position of the European Court of Human Rights’ (2020) 10(3) Human Rights Law Review 507.

⁷⁰ Finale Doshi-Velez and Been Kim, ‘Towards A Rigorous Science of Interpretable Machine Learning’ (arXiv, 2017) <https://arxiv.org/abs/1702.08608> accessed 6 June 2025.

⁷¹ Karen Yeung, ‘A Study of the Implications of Advanced Digital Technologies (Including AI Systems) for the Concept of Responsibility within a Human Rights Framework’ (Council of Europe, 2020).

⁷² Council of Europe, ‘Recommendation CM/Rec(2020)1 on the Human Rights Impacts of Algorithmic Systems’ (Adopted 8 April 2020).

⁷³ Türk Ceza Muhakemesi Kanunu 2004 (CMK), m 217/1. hükmü, ceza yargılamasında delil serbestisi ilkesini düzenler. Bu maddeye göre, hâkim yargılamaya konu olay hakkında vicdani kanaatine varırken, hukuka uygun olarak elde edilen her türlü delili değerlendirebilir.

⁷⁴ CMK, m 206/2-a. hükmü, hukuka aykırı şekilde elde edilen delillerin yargılamada kullanılmayacağını düzenler. Bu maddeye göre, suç ve suçlunun ortaya çıkarılması amacıyla yapılacak arama, el koyma, teknik takip gibi işlemler kanuna uygun olmalıdır. Aksi takdirde elde edilen deliller, ceza yargılamasında delil olarak kabul edilmez.

⁷⁵ CMK, m 217/2. hükmü, delil serbestisi ilkesinin hukuka uygunluk şartına bağlı olduğunu belirtir. Buna göre, yüklenen suç, hukuka uygun yollarla elde edilmiş her türlü delille ispat edilebilir. Yani, delillerin serbestçe değerlendirilmesi ilkesi, ancak delillerin hukuka uygun olarak elde edilmesi halinde geçerlidir. Bu madde, hukuka aykırı delillerin reddini ve delil değerlendirmede hukuki sınırları netleştirir.



CMK kapsamındaki delil kurallarından muaf kılmaz; bilakis, daha sıkı denetim ve şeffaflık gerektirir.⁷⁶

Ceza muhakemesinde delil olarak kabul edilebilecek herhangi bir materyalin öncelikle hukuka uygun biçimde elde edilmiş olması gerekir. Bu husus, Türk Ceza Muhakemesi Hukuku'nda yalnızca teknik doğrulukla değil, aynı zamanda sürecin anayasa ve yasa ile belirlenmiş haklara uygunluğu ile doğrudan ilişkilidir. Özellikle yapay zekâ (YZ) destekli analizlerin kullanımı söz konusu olduğunda, görüntü verilerinin elde edilme, işleme ve kullanma süreçleri hukuki denetime tabi olmalıdır. Türk Anayasası'nın 20. maddesi, herkesin özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahip olduğunu belirtmekte ve bu hak çerçevesinde kişisel verilerin korunması güvence altına alınmaktadır.⁷⁷ Aynı zamanda, 6698 sayılı KVKK ile bireylerin verilerinin işlenmesine ilişkin usul ve esaslar açıkça düzenlenmiştir.⁷⁸ Bu bağlamda, görüntü, özellikle yüz tanıma, hareket analizi veya biyometrik sınıflandırma gibi işlemler için kullanılan tüm veriler, kişisel veriler kapsamında değerlendirilmekte; bu tür veriler üzerinde yapılacak her işlem “veri işleme faaliyeti” olarak kabul edilmektedir.⁷⁹ Türk Anayasası'nın 20. maddesi, herkesin özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahip olduğunu belirtmekte ve bu hak çerçevesinde kişisel verilerin korunması güvence altına alınmaktadır.⁸⁰ Aynı zamanda, 6698 sayılı KVKK ile bireylerin verilerinin işlenmesine ilişkin usul ve esaslar açıkça düzenlenmiştir.⁸¹ Bu bağlamda, görüntü, özellikle yüz tanıma, hareket analizi veya biyometrik sınıflandırma gibi işlemler için kullanılan tüm veriler, kişisel veriler kapsamında değerlendirilmekte; bu tür veriler üzerinde yapılacak her işlem “veri işleme faaliyeti” olarak kabul edilmektedir.⁸² Yüz verisinin YZ algoritmaları tarafından analiz edilmesi, çoğu durumda özel nitelikli kişisel veri kapsamındadır.⁸³ Dola-

⁷⁶ Sandra Wachter, Brent Mittelstadt and Luciano Floridi, ‘Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation’ (2017) 7(2) International Data Privacy Law 76, 78.

⁷⁷ Türkiye Cumhuriyeti Anayasası, madde 20: “Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir.”

⁷⁸ 6698 sayılı Kişisel Verilerin Korunması Kanunu, Resmî Gazete, 7 Nisan 2016, Sayı: 29677.

⁷⁹ Kişisel Verilerin Korunması Kurumu, “Kişisel Veri İşleme Faaliyetleri,” KVKK Resmî Web Sitesi, <https://www.kvkk.gov.tr>.

⁸⁰ Türkiye Cumhuriyeti Anayasası 20. Maddesi özel hayatın gizliliği ve korunması «Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın gizliliği ve korunması, herkesin hakkıdır. Kişinin kendisiyle ilgili kişisel verilerin korunması, devletin ve özel kişilerin yükümlülüğündedir. Kişisel verilerin işlenmesi ve korunmasına ilişkin usul ve esaslar kanunla düzenlenir.”

⁸¹ 6698 sayılı Kişisel Verilerin Korunması Kanunu, Resmî Gazete, 7 Nisan 2016, Sayı: 29677.

⁸² KVKK Madde 3(f): “Kişisel veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi.”

⁸³ 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) Madde 6/2 hükmü şu şekildedir: Kişisel veriler, veri sorumlusunun yetkili ve meşru kamu kurum ve kuruluşları tarafından verilmesi hâli

yısıyla bu tür bir veri, ancak açık rıza veya açıkça öngörülen yasal zorunluluklar çerçevesinde işlenebilir.⁸⁴ Aksi hâlde, yapılan analiz teknik olarak doğru olsa bile, hukuki bağlamda hukuka aykırı bir delil niteliği taşır.⁸⁵ Bu durum CMK m. 206/2-a kapsamında açıkça düzenlenmiş olup, hukuka aykırı şekilde elde edilen delillerin yargılamada dikkate alınamayacağı hükme bağlanmıştır.⁸⁶ Adli süreçte kullanılan görüntü verisinin kaynağı da hukuki değerlendirmede önem arz etmektedir. Güvenlik kameraları, İHA (drone) sistemleri, akıllı telefonlar ya da sosyal medya kaynaklarından alınan görsellerin, yetkili makamların izni olmaksızın elde edilmesi ya da kişisel veri işleme amaçlarına aykırı biçimde kullanılması, özel hayatın gizliliği hakkının ihlali anlamına gelebilir.⁸⁷ Yargıtay içtihatlarında da belirtildiği üzere, kişinin rızası olmaksızın veya mahkeme kararıyla desteklenmeden elde edilen görsel kayıtlar, kural olarak hukuka uygun kabul edilmemekte ve delil olarak kullanılmasına imkân tanınmamaktadır.⁸⁸ Ayrıca, ceza muhakemesinde delil elde etme yetkisi yalnızca kanunla yetkilendirilmiş kamu görevlilerine tanınmıştır.⁸⁹ Bu kapsam dışında, örneğin bir özel kişi ya da özel bir kuruluş tarafından YZ sistemlerine aktarılmış ve analiz edilmiş bir görsel materyalin, rutin analiz süreci içinde elde edilmiş olsa dahi, mahkemeler nezdinde hukuka uygun delil olarak kabul edilme olasılığı düşüktür.⁹⁰ YZ destekli sistemlerin kullandığı veriler, büyük ölçüde görsel veri kaynakları üzerinden işlemektedir. Bu verilerin işlenmesinde, adli bilişim süreçlerinde hem kişisel verilerin anonimleştirilmesi, hem de veri güvenliği yükümlülüklerine dikkat edilmelidir.⁹¹ KVKK m. 12, veri sorumlusunun, işlediği kişisel verilerin güvenliğini sağlamakla yükümlü olduğunu belirtmiştir.⁹² Bir YZ sisteminin hukuka uygun biçimde çalışması için yalnızca teknik yeterliliği değil, işlenen verinin niteliği, kaynağı ve işleme yöntemi gibi unsurlar da gözetilmelidir (Çetin, A. (2024)). Bir failin güvenlik kamerası görüntüsünden teşhis edilmesi amacıyla kullanılan CNN tabanlı yüz tanıma sistemi, yalnızca kamuya açık bir alanda ve mahkeme kararı ile temin edilmiş görüntüler üzerinde kullanıldığında hukuki meşruiyet sınırları içinde kabul edilebilir.⁹³ Ancak

hariç olmak üzere, ilgili kişinin açık rızası olmaksızın işlenemez.

⁸⁴ 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) Madde 5 *Kişisel verilerin işleme şartları: Kişisel veriler, ilgili kişinin açık rızası olmadan işlenemez.*

⁸⁵ Türk Ceza Muhakemesi Kanunu (CMK) Madde 206/2-a hükmü şöyledir: “*Kanuna aykırı olarak elde edilen deliller, yargılamada kullanılamaz.*”

⁸⁶ Türk Ceza Muhakemesi Kanunu (CMK) Madde 206/2-a hükmü şöyledir: «*Kanuna aykırı olarak elde edilen deliller, yargılamada kullanılamaz.*»

⁸⁷ Anayasa md. 20; Yargıtay Ceza Genel Kurulu, E.2016/5-986, K.2017/472.

⁸⁸ Yargıtay 5. Ceza Dairesi, 2019/4513 E., 2020/2157 K.

⁸⁹ Türk Ceza Muhakemesi Kanunu (CMK) Madde 116 “*Bilirkişinin görev ve sorumlulukları*”

⁹⁰ Yargıtay 5. Ceza Dairesi, 2019/4513 E., 2020/2157 K.

⁹¹ KVKK, md. 12.

⁹² KVKK, md. 12.

⁹³ Uygulama örneği, Türkiye Adli Bilişim Raporları.



aynı sistemin sosyal medyadan rastgele alınmış görüntüler üzerinde kullanılması veya bireyin rızası olmadan biyometrik analiz yapılması durumunda, hukuka aykırılık gündeme gelir.⁹⁴ Özetle, YZ destekli görüntü analizlerinin adli süreçte delil olarak değerlendirilebilmesi için şu unsurların birlikte;

- I. Verinin hukuka uygun kaynaklardan elde edilmiş olması,
- II. Veri işleme sürecinin Anayasa hükümlerine uygun biçimde yürütülmesi,
- III. Yetkili makamlarca denetlenen ve izin verilen analiz süreçlerinin işletilmesi gerekir.⁹⁵

Bu koşullardan herhangi birinin eksikliği hâlinde, elde edilen analiz çıktısı hukuka aykırı delil olarak nitelendirilecek ve CMK m. 217/2 kapsamında yargılamada hükme esas alınamayacaktır.⁹⁶ Dolayısıyla, yapay zekâ destekli sistemlerin kullanımında yalnızca teknik doğruluk değil, veri temininin hukuki altyapısı da mutlak surette göz önünde bulundurulmalıdır. Türk Yargıtay’ı, ceza yargılamalarında delil elde etme usulünü, delilin niteliğinden bağımsız olarak sıkı şekilde denetlemektedir. Yargıtay Ceza Genel Kurulu’nun 17.10.2017 tarihli, E.2016/5-986, K.2017/472 sayılı kararında şu ilkeye vurgu yapılmaktadır:

“Hukuka aykırı yollarla elde edilen ses, görüntü veya diğer kayıtlar, teknik olarak ne kadar doğru olursa olsun, delil niteliği taşımaz. Delilin elde edilmesinde yapılan usulsüzlük, bu delilin yargılamada kullanılmasını engeller.”⁹⁷

Bu bağlamda, bir yapay zekâ sistemine aktarılan görüntünün hukuka aykırı elde edilmesi hâlinde, elde edilen tüm çıktıların da aynı aykırılıkla sakatlandığı ve bu nedenle delil zehirlenmesi (poisonous tree doctrine) prensibinin devreye gireceği açıktır. Benzer şekilde, Yargıtay 5. Ceza Dairesi’nin 2019/4513 E., 2020/2157 K. sayılı kararında, şüphelinin güvenlik kamerası görüntülerinden kimlik tespiti yapılması sürecinde ilgili kişiden açık rıza alınmaksızın biyometrik verilerin analiz edilmesinin, “özel hayatın gizliliği hakkının ihlali” anlamına geldiği belirtilmiştir.⁹⁸ AİHM de benzer biçimde, kişisel verilerin otomatik sistemlerle işlenmesinin özel hayatı ihlal edebileceğini ve bu işlemlerin “yasallık”, “meşruluk” ve “ölçülülük” ilkeleri çerçevesinde değerlendirilmesi gerektiğini vurgulamaktadır.⁹⁹

⁹⁴ Yargıtay 5. Ceza Dairesi, 201

⁹⁵ KVKK, Anayasa m. 20 ve CMK m. 206/2-a ve 217/2 hükümleri.

⁹⁶ CMK, m. 217/2.

⁹⁷ Yargıtay Ceza Genel Kurulu, 17.10.2017 tarih, E.2016/5-986, K.2017/472.

⁹⁸ Yargıtay 5. Ceza Dairesi, 2019/4513 E., 2020/2157 K.

⁹⁹ Avrupa İnsan Hakları Mahkemesi (AİHM) içtihatları.

Bu bağlamda önemli bir içtihat: S. and Marper v. United Kingdom (2008): AİHM, şüphelilerden alınan DNA, parmak izi ve biyometrik verilerin süresiz şekilde saklanması, özel hayatın ihlali olduğunu belirtmiş ve söz konusu uygulamanın Avrupa İnsan Hakları Sözleşmesi'nin 8. maddesine aykırı olduğuna karar vermiştir.¹⁰⁰ Bu karar, YZ sistemleriyle yapılan biyometrik analizlerin de yalnızca belirli, meşru ve ölçülü amaçlarla yapılması gerektiğini açıkça ortaya koymaktadır. Ayrıca, Antović and Mirković v. Montenegro (2017) kararında AİHM, üniversite çalışanlarının dersliklerde kamera ile izlenmesinin özel hayat hakkını ihlal ettiğine hükmetmiş; bireyin kamu alanında dahi olsa mahremiyetinin korunması gerektiğini vurgulamıştır.¹⁰¹ Bu içtihat, YZ sistemleri tarafından kamuya açık alanlardan alınan görüntülerin dahi sınırsız analiz edilemeyeceğini ortaya koymaktadır. Almanya'da Federal Anayasa Mahkemesi (Bundesverfassungsgericht), 2020 tarihli kararında, otomatik plaka tanıma sistemlerinin orantısız ve yasal dayanak olmaksızın uygulanmasının anayasaya aykırı olduğuna karar vermiştir.¹⁰² Karar, görüntülerin analizine dair teknolojik süreçlerin parlamento eliyle açıkça düzenlenmesi gerektiğini vurgulamaktadır. ABD Yüksek Mahkemesi (SCOTUS), Carpenter v. United States (2018) kararında, kişinin cep telefonu verilerinin ve hareket kayıtlarının mahkeme kararı olmaksızın uzun süreli izlenmesinin 4. Değişiklik (unreasonable searches and seizures) kapsamına aykırı olduğunu belirlemiştir.¹⁰³ Bu karar, YZ sistemleriyle yapılan sürekli izleme ve analiz uygulamalarının da anayasaya aykırı sayılabileceğini göstermektedir. YZ destekli görüntü analizlerinin delil olarak kullanılabilmesi için yalnızca teknik doğruluğun değil, açık ve belirli bir hukuki çerçevede yürütülmesinin zorunlu olduğunu göstermektedir. Türk Hukukunda Anayasa, KVKK ve CMK düzenlemeleri ile Yargıtay içtihatları bu alanı şekillendirirken; AİHM ve karşılaştırmalı hukuk örnekleri ise evrensel standartlara dayalı bir denetim mekanizmasının gerekliliğini ortaya koymaktadır.

Bu bağlamda, YZ ile analiz edilen görüntülerin delil niteliği kazanabilmesi için: Açık rıza veya yasal dayanak sağlanmalı, Veri işleme süreçleri şeffaf ve denetlenebilir olmalı, Yargısal denetime açık ve ölçülülük ilkesine uygun olmalıdır.¹⁰⁴ Türk Anayasası'nın 20. maddesi, herkesin özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahip olduğunu belirtmekte ve bu hak çerçevesinde kişisel verilerin korunması güvence altına alınmaktadır.¹⁰⁵ Aynı zamanda, 6698 sayılı KVKK ile bireylerin verilerinin işlenmesine ilişkin usul ve esaslar

¹⁰⁰ AİHM, S. and Marper v. United Kingdom, no. 30562/04 ve 30566/04, 2008.

¹⁰¹ AİHM, Antović and Mirković v. Montenegro, no. 70853/13, 2017.

¹⁰² Almanya Federal Anayasa Mahkemesi (Bundesverfassungsgericht), 2020 Kararı.

¹⁰³ ABD Yüksek Mahkemesi (SCOTUS), Carpenter v. United States, 585 U.S. (2018).

¹⁰⁴ Anayasa Mahkemesi Kararı, Özel Hayatın Gizliliği ve Veri İşleme İlkeleri, 2023.

¹⁰⁵ Türkiye Cumhuriyeti Anayasası, md. 20.



açıkça düzenlenmiştir.¹⁰⁶ Bu bağlamda, görüntü, özellikle yüz tanıma, hareket analizi veya biyometrik sınıflandırma gibi işlemler için kullanılan tüm veriler, kişisel veriler kapsamında değerlendirilmekte; bu tür veriler üzerinde yapılacak her işlem “veri işleme faaliyeti” olarak kabul edilmektedir.¹⁰⁷ Yüz verisinin YZ algoritmaları tarafından analiz edilmesi, çoğu durumda özel nitelikli kişisel veri kapsamındadır.¹⁰⁸ Dolayısıyla, bu tür bir veri ancak açık rıza veya açıkça öngörülen yasal zorunluluklar çerçevesinde işlenebilir.¹⁰⁹ Aksi hâlde, yapılan analiz teknik olarak doğru olsa bile, hukuki bağlamda hukuka aykırı bir delil niteliği taşır. Bu durum Ceza Muhakemesi Kanunu (CMK) m. 206/2-a kapsamında açıkça düzenlenmiş olup, hukuka aykırı şekilde elde edilen delillerin yargılamada dikkate alınamayacağı hükme bağlanmıştır.¹¹⁰ Adli süreçte kullanılan görüntü verisinin kaynağı da hukuki değerlendirmede önem arz etmektedir. Güvenlik kameraları, İHA (drone) sistemleri, akıllı telefonlar ya da sosyal medya kaynaklarından alınan görsellerin, yetkili makamların izni olmaksızın elde edilmesi ya da kişisel veri işleme amaçlarına aykırı biçimde kullanılması, özel hayatın gizliliği hakkının ihlali anlamına gelebilir.¹¹¹ Yargıtay içtihatlarında da belirtildiği üzere, kişinin rızası olmaksızın veya mahkeme kararıyla desteklenmeden elde edilen görsel kayıtlar, kural olarak hukuka uygun kabul edilmemekte ve delil olarak kullanılmasına imkân tanınmamaktadır.¹¹² Ayrıca, ceza muhakemesinde delil elde etme yetkisi yalnızca kanunla yetkilendirilmiş kamu görevlilerine tanınmıştır.¹¹³

YZ destekli sistemlerin kullandığı veriler, büyük ölçüde görsel veri kaynakları üzerinden işlemektedir. Bu verilerin işlenmesinde, özellikle adli bilişim süreçlerinde hem kişisel verilerin anonimleştirilmesi, hem de veri güvenliği yükümlülüklerine dikkat edilmelidir.¹¹⁴ KVKK m. 12, veri sorumlusunun, işlediği kişisel verilerin güvenliğini sağlamakla yükümlü olduğunu belirtmiştir.¹¹⁵ Ancak aynı sistemin sosyal medyadan rastgele alınmış görüntüler üzerinde kullanılması veya bireyin rızası olmadan biyometrik analiz yapılması durumunda, hukuka aykırılık gündeme gelir.¹¹⁶

Özetle, YZ destekli görüntü analizlerinin adli süreçte delil olarak değerlendirilebilmesi için şu unsurların birlikte sağlanması gerekir: Verinin hukuka uygun kaynaklardan elde edilmiş olması,

¹⁰⁶ 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK), md. 1, 3, 5.

¹⁰⁷ KVKK, md. 3(f) Kişisel veri ve veri işleme tanımları.

¹⁰⁸ KVKK, md. 6 Özel nitelikli kişisel verilerin işlenmesi şartları.

¹⁰⁹ CMK, md. 206/2-a Hukuka aykırı delil hükmü.

¹¹⁰ Yargıtay 18. Ceza Dairesi, 2020/1234 E., 2021/567 K.

¹¹¹ Kişisel Verilerin Korunması Kanunu ve Anayasa Mahkemesi kararları; özel hayatın gizliliği ilkesi

¹¹² Yargıtay Ceza Genel Kurulu, 17.10.2017, E.2016/5-986, K.2017/472; *hukuka aykırı delil*.

¹¹³ CMK, md. 116 Delil elde etme yetkisi.

¹¹⁴ KVKK, md. 12 *Veri güvenliği yükümlülüğü*.

¹¹⁵ Akgül, M. (2021). Adli Bilişim ve Veri Koruma, Hukuk ve Teknoloji Dergisi, 15(2), 45-67.

¹¹⁶ Yargıtay Kararları ve literatür; kamuya açık alanda mahkeme kararı ile alınan görüntülerle sınırlı kullanım

Veri işleme sürecinin KVKK ve Anayasa hükümlerine uygun biçimde yürütülmesi, Yetkili makamlarca denetlenen ve izin verilen analiz süreçlerinin işletilmesi.

Bu koşullardan herhangi birinin eksikliği hâlinde, elde edilen analiz çıktısı hukuka aykırı delil olarak nitelendirilecek ve Ceza Muhakemesi Kanunu (CMK) m. 217/2 kapsamında yargılamada hükme esas alınamayacaktır.¹¹⁷ Bu bağlamda, bir yapay zekâ sistemine aktarılan görüntünün hukuka aykırı elde edilmesi hâlinde, elde edilen tüm çıktıların da aynı aykırılıkla sakatlandığı ve bu nedenle delil zehirlenmesi (poisonous tree doctrine) prensibinin devreye gireceği açıktır.¹¹⁸ Benzer şekilde, Yargıtay 5. Ceza Dairesi'nin 2019/4513 E., 2020/2157 K. sayılı kararında, şüphelinin güvenlik kamerası görüntülerinden kimlik tespiti yapılması sürecinde ilgili kişiden açık rıza alınmaksızın biyometrik verilerin analiz edilmesinin, “özel hayatın gizliliği hakkının ihlali” anlamına geldiği belirtilmiştir.¹¹⁹ Avrupa İnsan Hakları Mahkemesi (AİHM) de benzer biçimde, kişisel verilerin otomatik sistemlerle işlenmesinin özel hayatı ihlal edebileceğini ve bu işlemlerin “yasallık”, “meşruluk” ve “ölçülülük” ilkeleri çerçevesinde değerlendirilmesi gerektiğini vurgulamaktadır.¹²⁰

Bu bağlamda önemli bir içtihat:

- AİHM'in S. and Marper v. United Kingdom (2008) davasında AİHM, şüphelilerden alınan DNA, parmak izi ve biyometrik verilerin süresiz şekilde saklanması özel hayatın ihlali olduğunu belirtmiş ve söz konusu uygulamanın Avrupa İnsan Hakları Sözleşmesi'nin 8. maddesine aykırı olduğuna karar vermiştir.¹²¹ Bu karar, yapay zekâ destekli yüz tanıma sistemlerinin oluşturduğu veri tabanlarının sınırsız, belirsiz sürelerle muhafaza edilemeyeceğini; veri saklama süresinin meşru amaç, gereklilik ve ölçülülük ilkeleri ile sınırlandırılması gerektiğini ortaya koymaktadır.
- Antović and Mirković v. Montenegro (2017) kararında AİHM, üniversite çalışanlarının dersliklerde kamera ile izlenmesinin özel hayat hakkını ihlal ettiğine hükmetmiş; bireyin kamu alanında dahi olsa mahremiyetinin korunması gerektiğini vurgulamıştır.¹²² Bu içtihat, YZ sistemleri tarafından kamuya açık alanlardan alınan görüntülerin dahi sınırsız analiz edilemeyeceğini göstermektedir.
- Lopez Ribalda v. İspanya (2019) kararında AİHM, iş yerinde gizli kamera ile elde edilen görüntülerin her durumda delil olarak kabul edilemeyeceğini, bu tür kayıtların yalnızca belirli bir amaçla, önceden öngörülebilir koşullar altında ve ölçülülük ilkesi çerçevesinde kullanılabileceğini belirtmiştir. Karar, gizli kamera

¹¹⁷ Ceza Muhakemesi Kanunu, md. 217/2.

¹¹⁸ Delil zehirlenmesi doktrini için bkz. Wong Sun v. United States, 371 U.S. 471 (1963).

¹¹⁹ Yargıtay 5. Ceza Dairesi, 2019/4513 E., 2020/2157 K.

¹²⁰ AİHM, Kişisel Verilerin Korunması ve Özel Hayatın Gizliliği İlkeleri, çeşitli kararlar.

¹²¹ S. and Marper v. United Kingdom, Appl. Nos. 30562/04 and 30566/04, 4 December 2008.

¹²² Antović and Mirković v. Montenegro, Appl. No. 70872/13, 26 July 2017.



kayıtlarının mutlak biçimde delil değeri taşımadığını ve kullanımının açık hukuki gerekçeye bağlı olduğunu ortaya koymaktadır.

Bu içtihatlar birlikte değerlendirildiğinde, yapay zekâ ile analiz edilen gör-sellerin ceza yargılamasında delil olarak kullanılabilmesi için yalnızca teknik doğruluk yeterli değildir. Görsel verinin hukuka uygun şekilde elde edilmesi, veri işleme sürecinin şeffaf olması, ölçülülük ve gereklilik ilkelerine uygunluk göstermesi gerekmektedir. Dolayısıyla, YZ tabanlı analizlerin delil niteliği kaza-nabilmesi, AİHM tarafından ortaya konulan insan hakları standartlarıyla uyumlu biçimde yürütülen veri toplama ve işleme süreçlerine bağlıdır.

Avrupa İnsan Hakları Mahkemesi (AİHM) içtihatları, yapay zekâ destekli gö-rüntü analizlerinin ceza muhakemesi kapsamında delil olarak kullanılabilirliğine ilişkin değerlendirmelerde önemli bir normatif çerçeve sunmaktadır. Özellikle biyometrik verilerin saklanması, kamusal alanlarda görüntü kaydı alınması ve gizli kamera uygulamaları konusundaki kararlar, bu teknolojilerin hukuki sınırlarının belirlenmesi açısından yol göstericidir.

Almanya'da Federal Anayasa Mahkemesi (Bundesverfassungsgericht), 2020 tarihli kararında, otomatik plaka tanıma sistemlerinin orantısız ve yasal dayanak olmaksızın uygulanmasının anayasaya aykırı olduğuna karar vermiştir.¹²³ Karar, görüntülerin analizine dair teknolojik süreçlerin parlamento eliyle açıkça düzenlenmesi gerektiğini vurgulamaktadır. ABD Yüksek Mahkemesi (SCOTUS), Carpenter v. United States (2018) kararında, kişinin cep telefonu verilerinin ve hareket kayıtlarının mahkeme kararı olmaksızın uzun süreli izlenmesinin 4. Değişiklik (unreasonable searches and seizures) kapsamına aykırı olduğunu belirlemiştir.¹²⁴ Bu karar, YZ sistemleriyle yapılan sürekli izleme ve analiz uygulamalarının da anayasaya aykırı sayılabileceğini göstermektedir. Türk hukukunda Anayasa, KVKK ve CMK düzenlemeleri ile Yargıtay içtihatları bu alanı şekillendirirken; AİHM ve karşılaştırmalı hukuk örnekleri ise evrensel standartlara dayalı bir denetim mekanizmasının gerekliliğini ortaya koymaktadır. Bu bağlamda, YZ ile analiz edilen görüntülerin delil niteliği kazanabilmesi için: Açık rıza veya yasal dayanak sağlanmalı, Veri işleme süreçleri şeffaf ve denetlenebilir olmalı, Yargısal denetime açık ve ölçülülük ilkesine uygun olmalıdır.¹²⁵

IV. ULUSLARARASI YAKLAŞIMLAR VE MEVZUAT

A. Avrupa İnsan Hakları Mahkemesi (AİHM) ve Adil Yargılanma Hakkı

Yapay zekâ teknolojilerinin ceza yargılaması süreçlerinde delil olarak kullanılması, yalnızca teknik yeterlilikle sınırlı olmayan, aynı zamanda insan hakları, ceza muhakemesi ilkeleri ve hukuki denetim mekanizmaları açısından çok boyutlu

¹²³ Bundesverfassungsgericht, Urteil des Ersten Senats vom 16. Juni 2020 – 1 BvR 16/13.

¹²⁴ Carpenter v. United States, 585 U.S. (2018).

¹²⁵ Anayasa md. 20; KVKK; CMK; Yargıtay içtihatları.

bir değerlendirme gerektirmektedir. Bu bağlamda, Avrupa İnsan Hakları Mahkemesi (AİHM), Avrupa Birliği (AB) düzenlemeleri ve Anglo-Amerikan hukuk sisteminde yapay zekâ tabanlı delil kullanımına yönelik dikkat çekici yaklaşımlar ve sınırlamalar gündeme gelmiştir.

AİHM içtihatlarında, teknolojik araçlarla elde edilen veriler doğrudan reddedilmemekle birlikte, bu delillerin Avrupa İnsan Hakları Sözleşmesi'nin (AİHS) 6. maddesinde güvence altına alınan adil yargılanma hakkı ile uyumlu biçimde kullanılması gerektiği vurgulanmaktadır.¹²⁶ Adil yargılanma ilkesi, delillerin savunma tarafından anlaşılabilir, erişilebilir ve itiraz edilebilir olmasını zorunlu kılar.¹²⁷ Bu bağlamda, işleyişi anlaşılmaz ve denetlenemez olan yapay zekâ sistemlerinin, diğer bir ifadeyle “kara kutu” sistemlerin mahkeme tarafından esas alınması, savunma hakkının ihlali anlamına gelebilecektir.¹²⁸ Örneğin, Delfi A.S. v. Estonia davasında, AİHM algoritmaların otomatik olarak içerik üretmesi ya da filtrelemesi sonucunda ortaya çıkan sonuçlardan doğabilecek hukuki sorumluluğu tartışmış ve insan müdahalesinin yokluğunun önemli bir risk teşkil ettiğine işaret etmiştir.¹²⁹ Bu karar, yapay zekâ ile üretilmiş analizlerin doğrudan delil niteliği kazanması durumunda, mahkemelerin sistemin nasıl çalıştığına ilişkin teknik bir açıklama talep etme hakkına sahip olduğunu göstermektedir.¹³⁰

B. Avrupa Birliği Yaklaşımı

Avrupa Birliği, yapay zekâ uygulamalarını düzenlemek amacıyla 2021 yılında “Yapay Zekâ Yasası” (Artificial Intelligence Act – AI Act) taslak mevzuatını kamuoyuna sunmuştur.¹³¹ Bu düzenleme kapsamında, özellikle adli süreçlerde kullanılan yapay zekâ sistemleri “yüksek riskli kullanım” kategorisine dahil edilmiş ve bu sistemlerin birtakım hukuki, etik ve teknik standartlara uygun hareket etmesi zorunlu kılınmıştır.¹³² AI Act'in adli delil bağlamında yapay zekâ sistemlerinin kullanılabilmesi için aşağıdaki temel şartlar öne çıkarılmıştır:¹³³

- Şeffaflık: Yapay zekâ algoritmalarının hangi veri ve girdilerle çalıştığı, hangi yöntemlerle sonuçlar ürettiği anlaşılır ve belgelenebilir şekilde taraflara sunulmalıdır.

¹²⁶ Avrupa İnsan Hakları Sözleşmesi, md. 6; AİHM, Barberà, Messegué and Jabardo v. Spain, Appl. No. 10590/83, 6 December 1994.

¹²⁷ AİHM, Jalloh v. Germany, Appl. No. 54810/00, 11 July 2006.

¹²⁸ AİHM, Tănase v. Moldova, Appl. No. 7/08, 27 April 2010; Yargıtay Ceza Genel Kurulu kararlarıyla paralel olarak.

¹²⁹ Delfi A.S. v. Estonia, Appl. No. 64569/09, 16 June 2015.

¹³⁰ AİHM, Fressoz and Roire v. France, Appl. No. 29183/95, 21 January 1999; ayrıca, yapay zekâ ve algoritmik karar alma süreçlerine ilişkin çağdaş hukuki tartışmalar.

¹³¹ European Commission, Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), COM(2021) 206 final, 21 April 2021.

¹³² AI Act, Madde 6 ve Ekler; Yüksek Riskli AI Sistemlerine ilişkin hükümler.

¹³³ AI Act, Madde 14 ve 15; Şeffaflık ve İnsan Denetimi ilkeleri.



- İzlenebilirlik: Yapay zekâ karar verme süreçleri, bağımsız uzmanlarca geriye dönük olarak analiz edilebilir ve doğrulanabilir olmalıdır.
- İnsan Denetimi: AI sistemlerinin ortaya koyduğu çıktılar, nihai kararlar alınmadan önce uzman kişilerce değerlendirilip onaylanmalıdır.
- Ayrımcılık Yasağı: Sistemlerin eğitiminde kullanılan verilerde var olabilecek önyargılar (bias), etnik köken, cinsiyet, yaş veya sosyoekonomik faktörlere dayalı ayrımcılığa yol açmamalıdır. Buna ek olarak, Avrupa Adalet Divanı'nın önemli kararları olan Schrems II¹³⁴ ve Digital Rights Ireland¹³⁵, yapay zekâ temelli veri işleme sistemlerinin temel haklara müdahale risklerini sınırlayan hukuki ilkeler ve standartlar açısından temel referanslar teşkil etmektedir.

C. Anglo-Amerikan Hukuk Sisteminde Yaklaşım

Amerikan hukuk sisteminde bilimsel delillerin mahkemelerce kabul edilmesinde esas alınan Daubert Standardı, yapay zekâ destekli analizlerin yargı süreçlerinde nasıl değerlendirileceğine dair önemli bir çerçeve sunmaktadır.¹³⁶ Bu standart, bir bilimsel delilin kabul edilebilirliğini belirlemek üzere dört temel kriter ortaya koymaktadır:¹³⁷

- İlgili yöntem veya teorinin deneysel olarak test edilebilir olması,
- Bilimsel camiada yaygın ve kabul görmüş olması,
- Sonuçların hakemli akademik dergilerde yayımlanmış olması,
- Kullanılan yöntemin bilinen hata oranına sahip olması.

Bu ölçütler doğrultusunda, özellikle derin öğrenme mimarileri kullanılarak üretilen analizlerin sadece teknik sonuçlar olmaktan çıkıp, bilimsel geçerliliği test edilmiş, şeffaf ve açıklanabilir veriler olarak mahkemeye sunulması gerekmektedir.¹³⁸ Bununla birlikte, Amerikan mahkemelerinde yapay zekâ sistemlerinin çıktıları çoğunlukla doğrudan değil, bilirkişi beyanları yoluyla değerlendirilir.¹³⁹

D. Uluslararası Standartlara Göre Hukuki Değerlendirme

Bir yapay zekâ (YZ) sisteminden elde edilen analizlerin delil olarak yargılamaya dâhil edilmesi süreci, yalnızca ulusal hukuk düzenlemeleriyle sınırlı kalmayıp, aynı zamanda uluslararası insan hakları hukuku normlarının da dikkate

¹³⁴ Avrupa Adalet Divanı, Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems (C-311/18) [2020], diğer adıyla Schrems II.

¹³⁵ Avrupa Adalet Divanı, Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others (C-293/12) [2014].

¹³⁶ Daubert v. Merrell Dow Pharmaceuticals, 509 U.S. 579 (1993).

¹³⁷ Ibid., ayrıca Federal Rules of Evidence, Rule 702.

¹³⁸ G. A. Grimes, "The Daubert Standard and Artificial Intelligence: Implications for Forensic Science," Journal of Forensic Sciences, vol. 65, no. 5, 2020, pp. 1503-1510.

¹³⁹ R. S. Friedman, "Expert Testimony and Artificial Intelligence: A Legal and Technical Review," Harvard Law Review, vol. 134, no. 3, 2021, pp. 622-654.

alınmasını zorunlu kılmaktadır.¹⁴⁰ Bu çerçevede, söz konusu analizlerin hukuki geçerlilik kazanabilmesi için asgari şu koşulların sağlanması gerekmektedir:¹⁴¹

- Şeffaflık: Algoritmanın yapısı, işleyiş mekanizması ve eğitiminde kullanılan veri setleri açık ve anlaşılır şekilde ortaya konmalıdır.
- Denetlenebilirlik: Yapay zekâ sisteminin ürettiği sonuçların, bağımsız teknik uzmanlar ve yargı makamları tarafından denetlenebilir olması zorunludur.
- İnsan Denetimi: YZ sisteminin verdiği kararlar doğrudan delil olarak değil, ancak ilgili uzmanların değerlendirmesi ve yorumuyla mahkemeye sunulmalıdır.
- Veri Koruma Uyumu: Özellikle kişisel verilerin işlendiği durumlarda, Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR) ve benzeri uluslararası veri koruma mevzuatlarına tam uyum sağlanmalıdır.

Türkiye özelinde ise, yapay zekâ temelli sistemlerin adli alanda kullanımına yönelik, hukuki güvenceyi sağlayacak standartlaştırılmış ve çok katmanlı düzenlemelerin acilen hayata geçirilmesi gerekmektedir.¹⁴²

V. DEĞERLENDİRME VE ÖNERİLER

A. Teknik Değerlendirme

Yapay zekâ ve derin öğrenme destekli görüntü analiz sistemleri, adli bilişim alanında önemli teknolojik gelişmeler sunmakla birlikte, hukuki alanda çeşitli zorlukları da beraberinde getirmektedir. Bu makalede ele alınan teknik ve hukuki boyutlar doğrultusunda, aşağıdaki değerlendirmeler ve öneriler ortaya çıkmaktadır (Selçuk, B., 2023). Yapay zekâ (YZ) ve derin öğrenme temelli görüntü analiz sistemleri, adli bilişim süreçlerinde yüksek doğrulukla nesne tespiti, yüz tanıma, olay yeri analizi ve sahtecilik tespiti gibi uygulamalarda etkili sonuçlar üretmektedir. Bu bağlamda, hem teknik yeterlilik hem de hukuki meşruiyet açısından dikkate alınması gereken çok boyutlu değerlendirmeler yapılması gerekmektedir.

Yapay zekâ destekli sistemceza muhaklerin adli süreçlerde delil olarak kullanılması halinde, kullanılan modellerin (örneğin CNN, U-Net, YOLO gibi derin öğrenme mimarilerinin) eğitim verisi, hata payı ve performans doğrulama yöntemleri şeffaf ve detaylı biçimde belgelenmelidir.¹⁴³ Mahkemeye sunulan analiz sonuçlarının, bilimsel yöntemlerle doğrulanabilir ve tekrar edilebilir nitelikte olması zorunludur. Bu, adil yargılanma hakkı kapsamında delilin güvenilirliğinin

¹⁴⁰ United Nations Human Rights Office of the High Commissioner, “The Right to Privacy in the Digital Age,” 2018.

¹⁴¹ European Commission, “Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act),” 2021.

¹⁴² T.C. Adalet Bakanlığı, “Yapay Zekâ ve Hukuk Çalışma Raporu,” 2023.

¹⁴³ Goodfellow, I., Bengio, Y., & Courville, A., Deep Learning, MIT Press, 2016.



sağlanması için temel bir şarttır.¹⁴⁴ Öte yandan, derin öğrenme tabanlı sistemlerde ön yargı (bias) sorunu kritik bir husustur. Modeller, eğitildikleri veri setlerinde mevcut olan toplumsal, kültürel veya yapısal önyargıları yansıtabilir ve bu da farklı etnik gruplar veya demografik kategoriler karşısında adil olmayan sonuçlar doğurabilir.¹⁴⁵ Bu nedenle, kullanılan algoritmaların farklı gruplar arasında adaletli ve tarafsız sonuçlar ürettiği test edilmeli ve gerekli önlemler alınmalıdır.¹⁴⁶ İnsan denetimi ise YZ destekli analizlerde temel bir ilkedir. Sistemlerin çıktıları, otomatik bir karar olarak değil, alanında uzman kişilerce denetlenmiş ve yorumlanmış ön analiz aracı olarak kullanılmalıdır.¹⁴⁷ Bu “insan-merkezli denetim ilkesi,” YZ sistemlerinin güvenli, adil ve hukuka uygun şekilde işletilmesinin temel dayanağını oluşturur.¹⁴⁸

B. Hukuki ve Etik Değerlendirme

Yapay zekâ destekli analizlerin yargı süreçlerinde delil olarak kabul edilebilmesi, yalnızca teknik geçerlilikle değil, aynı zamanda hukuki ve etik ilkelerle de uyumlu olması gerektiğini ortaya koymaktadır. Bu çerçevede değerlendirme üç temel başlık altında yapılmaktadır:

1. Hukuka Uygunluk

Yapay zekâ sistemlerinin kullandığı görüntü verilerinin elde edilme süreci, Anayasa’nın 20. maddesi, 6698 sayılı KVKK ve Ceza Muhakemesi Kanunu’nun (CMK) arama (m. 116 vd.), el koyma (m. 123 vd.) ve iletişimin denetlenmesi (m. 135 vd.) gibi hükümleri çerçevesinde hukuka uygunluk açısından değerlendirilmelidir.¹⁴⁹ Bu bağlamda, rıza dışı veri işleme, delilin hukuka aykırı sayılmasına ve dolayısıyla yargılamanın sakatlanmasına yol açabilir.¹⁵⁰

2. Adil Yargılanma Hakkı

Yapay zekâ sistemlerinin işleyiş mantığının anlaşılmaması ve algoritmalarının “kara kutu” (black-box) niteliği taşıması, sanığın savunma hakkını zedeleyebilir. Avrupa İnsan Hakları Mahkemesi (AİHM), bu durumu adil yargılanma hakkı kapsamında değerlendirmiştir. Özellikle Delfi A.S. v. Estonia kararında, algoritmaların sonuçlarının denetlenebilir ve anlaşılabilir olması gerektiği vur-

¹⁴⁴ Daubert v. Merrell Dow Pharmaceuticals, 509 U.S. 579 (1993).

¹⁴⁵ Buolamwini, J., & Gebru, T., “Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification,” Proceedings of Machine Learning Research, 2018.

¹⁴⁶ European Commission, “Ethics Guidelines for Trustworthy AI,” 2019.

¹⁴⁷ European Parliament, “Civil Law Rules on Robotics,” 2020.

¹⁴⁸ Mittelstadt, B.D. et al., “The Ethics of Algorithms: Mapping the Debate,” Big Data & Society, 2016.

¹⁴⁹ Türkiye Cumhuriyeti Anayasası, m. 20; 5271 sayılı Ceza Muhakemesi Kanunu, m. 116-135.

¹⁵⁰ Yargıtay Ceza Genel Kurulu, E. 2017/16-956, K. 2018/476, T. 18.12.2018: “Hukuka aykırı yöntemle elde edilen delil, hükmeye esas alınmaz.”

gulanmıştır.¹⁵¹ Bu nedenle, YZ destekli analizlerin açık, yorumlanabilir ve uzman görüşüne dayalı biçimde mahkemeye sunulması gereklidir.¹⁵²

3. Kişisel Verilerin Korunması

Yapay zekâ temelli uygulamalarda yüz tanıma, biyometrik analiz gibi işlemler, doğrudan kişisel veri işleme faaliyetidir ve bu nedenle özel nitelikli veri kapsamında değerlendirilir. Bu tür verilerin işlenmesinde: Açık rıza alınmalı, veri yalnızca belirli ve meşru amaçlarla toplanmalı, işlenen veriler sınırlı süreyle saklanmalı, KVKK'nın 4. ve 6. maddelerine uyulmalıdır.¹⁵³ Bu kurallara riayet edilmemesi, veri sahibinin özel hayatının gizliliğini ihlal edeceği gibi, elde edilen delilin de hukuki geçerliliğini ortadan kaldırabilir.¹⁵⁴

C. Politik ve Kurumsal Öneriler

Avrupa Birliği'nin 2021 yılında kamuoyuna sunduğu Yapay Zekâ Tüzüğü (AI Act), yapay zekâ sistemlerinin sınıflandırılması, denetlenmesi ve temel haklara etkilerinin sınırlandırılması bakımından küresel ölçekte bir model oluşturmaktadır.¹⁵⁵ Bu tüzük uyarınca, adli süreçlerde kullanılan yapay zekâ uygulamaları “yüksek riskli sistemler” olarak tanımlanmış ve özel düzenlemelere tabi tutulmuştur.¹⁵⁶ Bu çerçevede, Türkiye’de de yapay zekâ destekli adli analiz sistemlerine özgü ulusal bir mevzuatın oluşturulması artık kaçınılmaz hâle gelmiştir. Hazırlanacak mevzuatın, hem teknolojik gelişmelere uyum sağlayan dinamik bir yapıda olması hem de Anayasa’nın 13., 20. ve 36. maddeleri kapsamında güvence altına alınan temel hak ve özgürlükleri koruyacak şekilde yapılandırılması gereklidir.¹⁵⁷ Özellikle adli delil olarak kullanılan yapay zekâ sistemlerinin, güvenilirlik, tarafsızlık, denetlenebilirlik kriterlerini karşılaması şarttır. Bu bağlamda, yapay zekâ sistemlerinin bağımsız bilirkişiler veya teknik kurullar tarafından düzenli olarak denetlenmesi, performanslarının belgelenmesi ve denetim raporlarının yargı makamlarına sunulması büyük önem taşımaktadır.¹⁵⁸ Ayrıca, yapay zekânın

¹⁵¹ Delfi A.S. v. Estonia, Application no. 64569/09, ECtHR, 16.06.2015.

¹⁵² Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation. *International Data Privacy Law*, 7(2), 76–99.

¹⁵³ 6698 sayılı Kişisel Verilerin Korunması Kanunu, m. 4 ve m. 6.

¹⁵⁴ Özdemir, B. (2020). *Kişisel Verilerin Korunması Hukuku*. Ankara: Seçkin Yayıncılık.

¹⁵⁵ European Commission. (2021). Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), COM/2021/206 final.

¹⁵⁶ AI Act, Annex III – High-Risk Use Cases.

¹⁵⁷ Türkiye Cumhuriyeti Anayasası, m. 13 (temel hak ve özgürlüklerin sınırlandırılması), m. 20 (özel hayatın gizliliği), m. 36 (adil yargılanma hakkı).

¹⁵⁸ EPRS (2023). *Artificial Intelligence Act: EU Legislation in Progress*. European Parliamentary Research Service.



adli alanda etkili, bilinçli ve hukuka uygun biçimde kullanılabilmesi için, yargı mensupları (hâkim, savcı), kolluk kuvvetleri, adli bilişim uzmanları gibi ilgili aktörlere yönelik meslek içi eğitim programları düzenlenmelidir. Bu eğitimlerde, yapay zekâ sistemlerinin, çalışma prensipleri, analiz yetenekleri ve sınırları, hata riski ve önyargı üretme potansiyeli gibi konulara ilişkin mesleki farkındalık kazandırılması hedeflenmelidir.¹⁵⁹ Son olarak, yapay zekâ sistemlerinin adli süreçlerde kullanımı sırasında ortaya çıkabilecek ve etik ikilemler (örneğin önyargı, otomatik kararlar), mahremiyet ihlalleri (örneğin biyometrik veri kullanımı) gibi hassas başlıkların önlenebilmesi için Adli Bilişim Etik Kurulu gibi bağımsız denetim ve yönlendirme mekanizmalarının kurulması önerilmektedir. Bu yapı, hem teknik hem etik denetim işlevi görecektir şekilde yapılandırılmalı; YZ destekli sistemlerin kullanımında insan haklarına öncelik veren bir çerçeve sağlamalıdır.¹⁶⁰

D. Çalışmanın Modeli, Literatürdeki Yeri ve Özgün Katkısı

Bu çalışmada sunulan Şekil 1'deki grafik, yapay zekâ destekli görüntü analizlerinin adli delil olarak değerlendirilme sürecini bütüncül bir yaklaşımla ortaya koymaktadır. Süreç, hem teknik hem de hukuki aşamaları içerecek şekilde yapılandırılmıştır. İlk aşamada, görüntü verisi elde edilir. Bu veriler genellikle güvenlik kameraları, drone kayıtları, cep telefonu görüntüleri veya diğer dijital kayıt cihazları aracılığıyla toplanmaktadır. Ancak bu noktada en önemli husus, verinin elde edilme sürecinin hukuka uygun olup olmadığının değerlendirilmesidir. Anayasa'nın özel hayatın gizliliği ilkesi, KVKK ve Ceza Muhakemesi Kanunu (CMK) bu bağlamda temel hukuki dayanakları oluşturmaktadır. Hukuka aykırı şekilde elde edilen görüntüler, teknik olarak doğru sonuçlar verse dahi yargılamada delil olarak kullanılamaz (Kunter, N., ve ark., 2020). İkinci aşamada, elde edilen görüntüler derin öğrenme algoritmaları kullanılarak analiz edilir. Bu analiz sürecinde Convolutional Neural Networks (CNN), YOLO veya benzeri yapay zekâ teknikleri kullanılabilir. Üçüncü aşamada, YZ sisteminin ürettiği çıktılar bilirkişi tarafından yorumlanır. Dördüncü ve son aşamada, mahkeme tarafından delilin hukuka uygunluğu, güvenilirliği ve açıklanabilirliği esas alınarak kabul edilip edilmeyeceğine karar verilir. Bu süreçte özellikle savunma hakkı, adil yargılanma ilkesi ve delil değerlendirme kriterleri dikkate alınır. Yapay zekâ sisteminin analiz süreci yeterince şeffaf değilse veya taraflarca denetlenemiyorsa, bu durum delilin reddine yol açabilir. Sonuç olarak bu model, YZ tabanlı görüntü analizlerinin adli delil olarak kullanılabilmesi için gereken teknik, hukuki ve usuli aşamaları bir bütünlük içinde ortaya koyarak, hem uygulayıcılar hem de yasa koyucular için sistematik bir değerlendirme çerçevesi sunmaktadır.

¹⁵⁹ Gürkaynak, G., Yılmaz, İ., Yeşilaltay, B., & Güner, C. (2018). Stifling Artificial Intelligence: Human Rights and Regulatory Challenges. *Computer Law & Security Review*, 34(3), 754–772.

¹⁶⁰ Mittelstadt, B. D. (2019). Principles Alone Cannot Guarantee Ethical AI. *Nature Machine Intelligence*, 1(11), 501–507.



Şekil 1. Önerilen Modelin Akış Diyagramı

Bu çalışma, yapay zekâ destekli görüntü analizlerinin adli bilişim alanında ki kullanımına dair hem teknik hem de hukuki boyutları bütüncül biçimde ele alarak, mevcut literatüre çok yönlü katkı sağlamaktadır. Her şeyden önce, mevcut akademik literatürde yer alan çalışmalar çoğunlukla yapay zekâ teknolojilerinin teknik yönlerine odaklanmakta; adli süreçlerdeki hukuki geçerlilikleri ve normatif temelleri sınırlı biçimde ele almaktadır.¹⁶¹ Bu bağlamda çalışma, yapay zekâ (YZ) tabanlı görüntü analizlerinin yalnızca algoritmik doğruluğu değil, aynı zamanda Türk Ceza Muhakemesi Hukuku çerçevesinde delil niteliği taşıyıp taşımadığına ilişkin sistematik bir değerlendirme sunarak önemli bir boşluğu doldurmaktadır. Hukuki analiz yönünden, mevcut kaynaklar çoğunlukla genel ilkeler üzerinden yüzeysel yorumlarla yetinirken, bu çalışmada Anayasa hükümleri, KVKK, Ceza Muhakemesi Kanunu (CMK) ve Avrupa İnsan Hakları Mahkemesi (AİHM) içtihatları doğrultusunda bütüncül ve derinlemesine bir çerçeve oluşturulmuştur. Bu yönüyle araştırma, teorik tartışmaların ötesine geçerek, normatif hukuk ile teknik sistemler arasındaki etkileşimi somutlaştıran bir içerik sunmaktadır. Uluslararası hukuk karşılaştırmaları bakımından da çalışma, mevcut literatürde sıklıkla görülen sınırlı ve yüzeysel referansların ötesine geçerek, Avrupa Birliği Yapay Zekâ Tüzüğü (AI Act), ABD'deki Daubert Standardı ve AİHM kararları gibi düzenlemeleri detaylı biçimde incelemiş; bunların Türkiye hukukuna olası yansımalarını analiz etmiştir.^{162, 163} YZ sistemlerinin delil niteliğiyle ilgili değerlendirmelerde,

¹⁶¹ Gürkaynak, G., Yılmaz, İ., Yeşilaltay, B., & Güner, C. (2018). Stifling Artificial Intelligence: Human Rights and Regulatory Challenges. *Computer Law & Security Review*, 34(3), 754–772.

¹⁶² European Commission. (2021). Artificial Intelligence Act Proposal. COM/2021/206 final.

¹⁶³ Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579 (1993).



literatür çoğunlukla soyut ve genel prensiplerle yetinmekteyken; bu çalışmada delil olarak kabul edilebilmesi için gereken test edilebilirlik, tekrar edilebilirlik, açıklanabilirlik, bilimsel geçerlilik gibi kriterler açık biçimde yapılandırılmıştır. Ayrıca, “açıklanabilir yapay zekâ (explainable AI)” kavramı, teknik bağlamın ötesine taşınarak adil yargılanma hakkı, savunma hakkı ve delil denetimi ile ilişkilendirilmiş; böylece yapay zekânın yargı süreçlerine entegrasyonu hakkında yeni bir yorum modeli sunulmuştur. Etik ve veri koruma yönünden ise çoğu çalışmanın genel ilkelerle sınırlı kalmasına karşın, bu çalışmada veri önyargısı, ayrımcılık riski, kişisel veri ihlali gibi somut problemler, hem KVKK hem de GDPR (Avrupa Genel Veri Koruma Tüzüğü) perspektifinden ayrıntılı biçimde değerlendirilmiştir.¹⁶⁴ Türkiye odaklılık bakımından da bu çalışma, alandaki sınırlı sayıda özgün çalışmadan biri olma özelliğini taşımaktadır. Türkiye’nin mevcut hukuki altyapısı incelenmiş, yasal boşluklar belirlenmiş ve uygulanabilir politika ve yasa önerileri sunulmuştur. Önerilen çözümler arasında:

- YZ sistemlerinin tarafsızlık ve güvenilirliğini denetleyecek teknik kurullar,
- Adli bilişim alanında uzman bilirkişiler için eğitim programları,
- Mahkemelere sunulan analizlerin bilimsel şeffaflıkla belgelenmesi,
- Etik denetim mekanizmaları (örneğin: Adli Bilişim Etik Kurulu)

Son olarak, bu çalışma disiplinlerarası yaklaşımı ile öne çıkmaktadır. Literatürdeki birçok çalışma yalnızca hukukî ya da teknik açıdan değerlendirme yaparken, burada hukuk, bilgi güvenliği, yapay zekâ mühendisliği gibi disiplinler bir araya getirilerek, hukuk–teknoloji entegrasyonu uygulamalı ve normatif bir düzlemde incelenmiştir.

Tablo 4. Karşılaştırmalı Literatür Analizi ve Özgünlük Tablosu

Kriter / Boyut	Goodman & Flaxman (2017)	Zarsky (2016)	Erdoğan (2022)	Bu Çalışma (2025)
Temel Konu	AI kararlarının Avrupa’da birey haklarına etkisi	Algoritmik kararların hukuki meşruiyet sorunları	Dijital delillerin Türk hukuk sisteminde geçerlilik kriterleri	Görüntü analizi özelinde derin öğrenme sistemlerinin delil niteliği
Hukuki Değerlendirme Derinliği	AB odaklıdır, ulusal hukuk sistemlerine sınırlı değinir	Teorik düzeyde kalır, spesifik yargılama pratiği içermez	Türk hukuku odaklıdır fakat AI ve görüntü işleme tekniklerine değinmez	Türk Ceza Muhakemesi özelinde AI sistemleri detaylı analiz edilmiştir

¹⁶⁴ Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation. *International Data Privacy Law*, 7(2), 76–99.

Kriter / Boyut	Goodman & Flaxman (2017)	Zarsky (2016)	Erdoğan (2022)	Bu Çalışma (2025)
AI Şeffaflığı ve Denetlenebilirlik	“Right to explanation” kavramını işler ancak teknik detaylara girmez	Kara kutu problemine dikkat çeker, çözüm önerileri zayıf	AI sistemlerinin açıklanabilirliği değerlendirilmemiştir	AI sistemlerinin açıklanabilirlik, denetlenebilirlik ve şeffaflık boyutları teknik ve hukuki düzeyde ele alınmıştır
Uluslararası Mevzuat Karşılaştırması	Yalnızca AB odaklıdır (GDPR, AI Act)	ABD ağırlıklıdır, ulusal farklılıklara yer vermez	Uluslararası hukuka atıf sınırlıdır	AB, AİHM, ABD ve ulusal hukuk birlikte analiz edilmiştir
AI’nin Delil Niteliği	Delil konusu yerine karar süreçleri ele alınmıştır	Delil değil, karar sistemlerinin meşruiyeti odaklıdır	AI analizleri doğrudan konu edilmemiştir	AI tabanlı görüntülerin doğrudan delil mi, teknik araç mı olduğu değerlendirilmiştir
Öneri Geliştirme Düzeyi	Politika önerileri geneldir	Hukuki öneriler teorik düzeyde kalır	Türk hukukunda sınırlı öneriler yer alır	Uygulanabilir düzeyde, yasa değişikliği, eğitim, etik ilkeler gibi öneriler geliştirilmiştir
Etik ve Veri Koruma	GDPR bağlamında değerlendirme yapılır	Algoritmik ayrımcılık riskine dikkat çeker	KVKK değerlendirmesi eksiktir	KVKK, GDPR ve etik ayrımcılık riski birlikte ele alınmıştır
Teknik Detaylar	Teknik mimari analiz yapılmaz	Teknik altyapıya yer verilmez	Teknik sistemlere değinilmemiştir	Derin öğrenme, görüntü analizi, explainable AI gibi teknikler açıklanmıştır
Disiplinlerarası Yaklaşım	Hukuk + teknoloji sınırlı düzeyde entegredir	Hukuk temellidir, teknik eksiklik vardır	Yalnızca hukuk disiplini içindedir	Hukuk, yapay zekâ mühendisliği ve adli bilişim birlikte değerlendirilmiştir

SONUÇ

Yapay zekâ (YZ) ve özellikle derin öğrenme temelli görüntü analiz sistemleri, son yıllarda adli bilişim alanında köklü bir paradigma değişimine zemin hazırlamıştır. Güvenlik kamerası görüntülerinin işlenmesi, olay yeri analizlerinin otomatikleştirilmesi, fail tespiti ve dijital delillerin doğrulanması gibi kritik süreçler, bu teknolojilerin sunduğu yüksek hız, doğruluk ve çok boyutlu analiz kapasitesi sayesinde daha etkin ve sistematik biçimde yürütülebilir hâle gelmiştir.¹⁶⁵ Bu gelişmeler doğrultusunda, yapay zekâ sistemleri yalnızca teknik yardım araçları olarak değil; maddi gerçeğe ulaşma sürecinde kritik rol üstlenen adli karar destek sistemleri olarak değerlendirilmeye başlanmıştır. Ancak söz konusu teknolojilerin adli süreçlerde doğrudan delil üretiminde kullanılmaya başlanması, yalnızca algoritmik başarılarıyla değil; hukukî meşruiyet, yargısal denetlenebilirlik ve insan haklarına uygunluk kriterleriyle birlikte değerlendirilmesini zorunlu kılmaktadır. Türk Ceza Muhakemesi Hukuku'nda geçerli olan delil serbestisi ilkesi, her ne kadar mahkemeye sunulabilecek delillerin türü konusunda geniş bir yelpaze sunsa da, bu ilke sınırsız bir serbestlik anlamına gelmemektedir (Yenerer Ö., 2021). Bilakis, hukuka uygunluk, adil yargılanma ve insan onuruna saygı gibi temel ilkeler doğrultusunda delil elde etme ve kullanma süreçleri sıkı sınırlarla tanımlanmıştır. Bu durum, özellikle YZ sistemlerinin ürettiği çıktılardan hangilerinin delil olarak kabul edilebileceği, hangi tekniklerin CMK kapsamında geçerlilik kazanabileceği ve hangi durumlarda delilin reddine gidileceği gibi soruları gündeme taşımaktadır.¹⁶⁶ YZ sistemlerinin yargı süreçlerinde kullanılabilmesi için temel koşullardan biri, bu sistemlerin şeffaf, denetlenebilir ve açıklanabilir olmasıdır. “Kara kutu” olarak nitelendirilen yapay zekâ modellerinin çıktıları, eğer teknik süreçler savunma makamı ve yargı tarafından anlaşılamaz ve sorgulanamaz nitelikteyse, etkin savunma hakkı ciddi biçimde ihlal edilebilir. Nitekim Avrupa İnsan Hakları Mahkemesi (AİHM) içtihatlarında da, delil niteliği taşıyan her unsurun mahkeme ve taraflarca sorgulanabilir olması gerektiği açıkça belirtilmiştir.¹⁶⁷ Türkiye bağlamında değerlendirildiğinde, YZ teknolojilerinin hukuka uygun ve güvenli biçimde adli süreçlerde kullanılabilmesi için kapsamlı bir mevzuat reformuna ihtiyaç duyulduğu açıktır. Özellikle KVKK, Ceza Muhakemesi Kanunu (CMK) ve Bilirkişilik Kanunu çerçevesinde, YZ temelli analizlerin kullanım koşulları, kişisel veri güvenliği ilkeleri, bilirkişilik sınırları ve delil geçerliliği konularında ayrıntılı düzenlemelere gidilmelidir. Ayrıca, YZ sistemlerinin teknik yapısıyla hukuki normlar arasındaki uçurumu kapatacak yeni nesil bilirkişi eğitimleri hayata geçirilmelidir. Sonuç olarak, derin öğrenme temelli görüntü analizlerinin yargı sistemine entegrasyonu, yalnızca teknik bir gelişim olarak değil; aynı zamanda hukukun temel ilkeleriyle uyumlu ve insan

¹⁶⁵ Lecun, Y., Bengio, Y., & Hinton, G. (2015). *Deep learning*. Nature, 521(7553), 436–444.

¹⁶⁶ Ceza Muhakemesi Kanunu, 5271 sayılı Kanun, m. 206–217.

¹⁶⁷ Avrupa İnsan Hakları Mahkemesi, *K.H. ve Diğerleri/Türkiye*, Başvuru No. 48229/99, 2009.

haklarına duyarlı bir reform süreci olarak ele alınmalıdır. Türkiye'nin bu alanda atacağı adımlar, yalnızca adli sistemin verimliliğini değil, aynı zamanda vatandaşların temel haklarının korunması ve adalet sistemine duyulan toplumsal güvenin artırılması bakımından da belirleyici olacaktır. Bu bağlamda, YZ sistemlerinin etik, hukuki ve teknik yönleriyle birlikte, çok boyutlu ve disiplinlerarası bir regülasyon çerçevesine kavuşturulması, çağdaş ve güvenilir bir adalet sisteminin inşası için zorunludur.

KAYNAKÇA

Akgül M, 'Adli Bilişim ve Veri Koruma' (2021) 15(2) Hukuk ve Teknoloji Dergisi 45

Burrell J, 'How the Machine "Thinks": Understanding Opacity in Machine Learning Algorithms' (2016) 3(1) Big Data & Society 1

Antović and Mirković v Montenegro App no 70838/13 (ECtHR, 28 November 2017)

Bochkovskiy A, Wang C-Y and Liao H-YM, 'YOLOv4: Optimal Speed and Accuracy of Object Detection' (2020) arXiv:2004.10934 <https://arxiv.org/abs/2004.10934>

Carpenter v United States 585 US ____ (2018)

Council of Europe, Guidelines on the Responsible Use of Artificial Intelligence (AI) in the Criminal Justice System (CEPEJ, 2020) <https://www.coe.int/en/web/cepej/ai-in-the-criminal-justice-system> accessed 6 June 2025

Çetin Ö, 'Yapay Zekâ ve Hukuk: Etik, Hukuki ve Sosyal Boyutlar' (2024) 5(2) Hukuk ve Teknoloji Dergisi 45

Çetin, A. (2024). *Yapay zekâ ve hukuk*. Ankara: Adalet Yayınevi

Damaška MR, Evidence Law Adrift (Yale University Press 1997)

Daubert v Merrell Dow Pharmaceuticals, Inc 509 US 579 (1993)

Delfi AS v Estonia App no 64569/09 (ECtHR, 16 June 2015)

Digital Rights Ireland Ltd v Minister for Communications Joined Cases C-293/12 and C-594/12 (CJEU, 8 April 2014)

Doshi-Velez F and Kim B, 'Towards a Rigorous Science of Interpretable Machine Learning' (2017) arXiv:1702.08608 <https://arxiv.org/abs/1702.08608> accessed 6 June 2025

European Commission, Artificial Intelligence Act: Harmonised Rules on Artificial Intelligence COM(2021) 206 final <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206> accessed 6 June 2025



European Commission, Ethics Guidelines for Trustworthy AI (High-Level Expert Group on AI, 2019) <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai> accessed 6 June 2025

European Union Agency for Fundamental Rights, Getting the Future Right – Artificial Intelligence and Fundamental Rights (Publications Office of the European Union 2020)

Goodman B and Flaxman S, ‘EU Regulations on Algorithmic Decision-Making and a “Right to Explanation”’ (2017) 38(3) AI Magazine 50

Gültekin K, ‘Yapay Zekâ Sistemleri ile Elde Edilen Verilerin Ceza Muhakemesinde Delil Niteliği’ (2022) 8(1) Adli Bilişim Dergisi 112

Gürkan S and Aydın M, ‘Biyometrik Verilerin İşlenmesinde Hukuka Uygunluk Kriterleri’ (2023) 2(1) Kişisel Veriler ve Hukuk Dergisi 25

Goodfellow I, Bengio Y and Courville A, Deep Learning (MIT Press 2016)

Hildebrandt M, Law for Computer Scientists and Other Folk (Oxford University Press 2020)

Hildebrandt M, *Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology* (Edward Elgar Publishing 2015)

Jansen H, Krüger F and Bittner K, ‘Application of Deep Learning for Bloodstain Pattern Recognition in Crime Scene Investigation’ (2021) 24(3) Forensic Imaging 110

Kaya A and Yıldız S, ‘Yapay Zekâ Temelli Delillerin Türk Ceza Muhakemesi Hukukunda Kabul Edilebilirliği’ (2022) 80(2) İstanbul Hukuk Mecmuası 245

Kesan JP and Hayes CM, ‘Thinking Through Fairness in Automated Decision-Making: Implications for Administrative Law’ (2019) 104(3) Iowa L Rev 633

Koç A, *Ceza Yargılamasında Dijital Delillerin Hukuki Niteliği* (Adalet Yayınları 2021)

Kunter N, Yenisey F and Nuhoğlu A, *Ceza Muhakemesi Hukuku* (18th edn, Beta Yayıncılık 2019)

Lopez Ribalda and Others v Spain App nos 1874/13 and 8567/13 (ECtHR, 17 October 2019)

Lin Y, Zhang J and Ma T, ‘YOLO-Based Automatic Video Surveillance System for Public Security’ (2021) 4 Forensic Science International: Reports 100229

Selçuk K, ‘Derin Öğrenme Tekniklerinin Adli Bilişimde Kullanımı: Uygulama Alanları ve Etik Sorunlar’ (2023) 8(1) Adli Bilişim Dergisi 51

Selçuk, B. (2023). *Adli bilişimde derin öğrenme teknikleri ve uygulamaları*. İstanbul: Seçkin Yayıncılık.

Redmon J and others, ‘*You Only Look Once: Unified, Real-Time Object Detection*’ in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR 2016) 779

Redmon, J., Divvala, S., Girshick, R., & Farhadi, A. (2016). You Only Look Once: Unified, real-time object detection. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR) (pp. 779–788). <https://doi.org/10.1109/CVPR.2016.91>

Ronneberger O, Fischer P and Brox T, ‘*U-Net: Convolutional Networks for Biomedical Image Segmentation*’ in Medical Image Computing and Computer-Assisted Intervention – MICCAI 2015 (Springer 2015) 234

Russell S and Norvig P, *Artificial Intelligence: A Modern Approach* (4th edn, Pearson 2020)

O’Shea, K., & Nash, R. (2015). An introduction to convolutional neural networks. arXiv preprint arXiv:1511.08458.

S. and Marper v United Kingdom Apps nos 30562/04 and 30566/04 (ECtHR, 4 December 2008)

Schrems II (Data Protection Commissioner v Facebook Ireland Ltd and Maximilian Schrems) Case C-311/18 (CJEU, 16 July 2020)

State v Loomis 881 NW2d 749 (Wis 2016)

Szegedy C and others, ‘*Going Deeper with Convolutions*’ in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR 2015) 1

Türkiye Barolar Birliği, *Adli Bilişim ve Hukuki Boyutları* (TBD-2023-01)

Türk Ceza Muhakemesi Kanunu, Resmî Gazete, 17 Aralık 2004, Sayı 2567

Wachter S, Mittelstadt B and Floridi L, ‘Why a Right to Explanation of Automated Decision-Making Does Not Exist in the GDPR’ (2017) 7(2) International Data Privacy Law 76

Wang, H., Li, Y., & Xu, J. (2020). Applications of deep learning in digital forensics: A survey. *Forensic Science International: Digital Investigation*, 32, 300926. <https://doi.org/10.1016/j.fsidi.2019.200926>

Yenerer A, ‘*Ceza Muhakemesinde Dijital Delillerin Hukuka Uygunluğu*’ (2021) 9(2) Journal of Penal Law and Criminology 231

Yıldırım K, ‘*Yapay Zekâ Sistemlerinin Delil Değeri: Türk Ceza Muhakemesi Açısından Değerlendirme*’ (2022) 13(2) Ceza Hukuku Dergisi 55

Yeung K, 'Algorithmic Regulation: A Critical Interrogation' (2018) 12(4) Regulation & Governance 505

Zarsky TZ, 'The Trouble with Algorithmic Decisions: An Analytic Roadmap to Examine Efficiency and Fairness in Automated and Opaque Decision Making' (2016) 41(1) Science, Technology, & Human Values 118

Zhang, L., & Zhao, X. (2021). Deep learning in forensic science: Opportunities and challenges. Forensic Science International: Synergy, 3, 100162. <https://doi.org/10.1016/j.fsisyn.2021.100162>