SENTETİK MEDYANIN ADLİ TESPİTİ

Deepfake Ses ve Görüntü Delili Artık Güvenilir mi? Yapay Zekâ Üretimi İçeriğin Tespiti, Delil Değeri ve Hukuki Çerçevesi

Forensic Detection of Synthetic Media: Is Deepfake Audio and Video Evidence Still Reliable?

Derleme Makale / Review Article

Dr. Burak Olgun

burakolgun@solutionhome.net

Solution Home Bilişim Tekn. ve Dan. Hizm., İstanbul

Deepfake • Sentetik Medya • Adli Tespit • İçerik Kökeni (C2PA) • Ses Klonlama • Delil Bütünlüğü • Yapay Zekâ

ÖZET

Üretken yapay zekânın hızla olgunlaşması, gerçekten ayırt edilmesi giderek zorlaşan sentetik ses, görüntü ve video (deepfake) üretimini sıradanlaştırmıştır. Bu gelişme, ses ve görüntü kayıtlarının uzun süredir sahip olduğu 'gördüğüme ve duyduğuma inanırım' güvenini sarsmış; adli süreçte sunulan her multimedya delilinin özgünlüğünü teknik olarak sınama zorunluluğunu doğurmuştur. Bu makale, sentetik medyanın adli tespitini üç boyutta ele almaktadır: (i) deepfake üretiminin teknik temelleri ile çekişmeli üretici ağ (GAN) ve difüzyon tabanlı modellerin bıraktığı adli izler; (ii) tespit yaklaşımları -- üretim sonrası pasif analiz (fizyolojik tutarsızlıklar, sensör ve sıkıştırma artefaktları) ile üretimde imzalamaya dayalı aktif köken doğrulama (C2PA, filigran) -- ve bu yöntemlerin gerçek dünyadaki güvenilirlik sınırları; (iii) elde edilen bulguların delil değeri, delil zincirinin korunması ve Türk hukuku ile uluslararası düzenlemeler karşısındaki konumu. 2025-2026 verileri ışığında tespit doğruluğunun laboratuvardan gerçek dünyaya geçişte belirgin biçimde düştüğü gösterilmekte; deepfake kaynaklı dolandırıcılığın büyüyen ekonomik boyutu tartışılmaktadır. Türkiye bağlamında, ilgili Türk Ceza Kanunu hükümleri, KVKK rehberi, Yargıtay'ın özgünlük ve bütünlük içtihadı ve 2025 sonunda gündeme gelen yapay zekâ içeriklerine ilişkin kanun teklifi değerlendirilmektedir. Çalışma, hiçbir tespit aracının tek başına kesin sonuç vermediğini; güvenilir bir adli kanaatin ancak çok yöntemli doğrulama, köken analizi ve titiz delil yönetiminin birleşiminden doğduğunu ortaya koymaktadır.

Anahtar Kelimeler: *deepfake, sentetik medya, adli tespit, difüzyon modelleri, içerik kökeni, C2PA, ses klonlama, delil bütünlüğü, özgünlük analizi, yapay zekâ.*

ABSTRACT

The rapid maturation of generative artificial intelligence has made the production of synthetic audio, images and video (deepfakes) that are increasingly difficult to distinguish from genuine recordings a routine matter. This development has undermined the long-held trust in audiovisual records and created an obligation to technically test the authenticity of every multimedia item submitted in a forensic process. This article addresses the forensic detection of synthetic media along three axes: (i) the technical foundations of deepfake generation and the forensic traces left by generative adversarial network (GAN) and diffusion-based models; (ii) detection approaches -- passive post-hoc analysis (physiological inconsistencies, sensor and

burakolgun.com

compression artefacts) and active provenance verification based on signing at creation (C2PA, watermarking) -- and the real-world reliability limits of these methods; and (iii) the evidentiary value of the findings, the preservation of the chain of custody, and their standing under Turkish law and international regulation. Drawing on 2025-2026 data, the article shows that detection accuracy drops markedly in the transition from the laboratory to the real world, and discusses the growing economic dimension of deepfake-enabled fraud. In the Turkish context, the relevant provisions of the Turkish Penal Code, the guidance of the Personal Data Protection Authority, the authenticity-and-integrity case law of the Court of Cassation and the late-2025 draft law on artificial-intelligence content are evaluated. The study concludes that no detection tool alone yields a definitive result; a reliable forensic opinion emerges only from the combination of multi-method verification, provenance analysis and rigorous evidence management.

Keywords: *deepfake, synthetic media, forensic detection, diffusion models, content provenance, C2PA, voice cloning, evidence integrity, authenticity analysis, artificial intelligence.*

burakolgun.com

1. Giriş

Bir sesin ya da görüntünün gerçekliği, insanlık tarihinin büyük bölümünde neredeyse kendiliğinden kabul edilen bir olguydu. Bir fotoğraf, bir olayın gerçekleştiğinin; bir ses kaydı, bir kişinin o sözleri söylediğinin güçlü kanıtı sayılırdı. Üretken yapay zekânın son yıllardaki sıçraması, bu sezgisel güveni köklü biçimde sarsmıştır. Bugün, birkaç saniyelik bir ses örneğinden ikna edici bir ses klonu, birkaç fotoğraftan gerçekçi bir video üretmek, uzmanlık gerektirmeyen ve giderek ucuzlayan bir işe dönüşmüştür. 'Deepfake' olarak adlandırılan bu sentetik medya, artık yalnızca eğlence veya propaganda aracı değil; dolandırıcılıktan iftiraya, delil üretmekten delil karartmaya kadar geniş bir kötüye kullanım alanının merkezindedir.

Bu dönüşüm, adli bilişim açısından doğrudan bir meydan okuma yaratır. Ses ve görüntü kayıtları, adli süreçlerde en güçlü delil türlerinden sayılagelmiştir; oysa artık her multimedya dosyasının özgün mü yoksa üretilmiş mi olduğu, baştan sorgulanması gereken bir soru hâline gelmiştir. Sorun çift yönlüdür: Bir yandan sahte bir kayıt gerçek gibi sunulabilir; öte yandan gerçek bir kayıt, 'bu deepfake olabilir' savunmasıyla itibarsızlaştırılabilir. Literatürde 'yalancının kâr payı' (liar's dividend) olarak anılan bu ikinci risk, sentetik medyanın yalnızca sahte içerik üretmekle kalmayıp, gerçek delile duyulan güveni de aşındırdığını gösterir.

Bu tabloya teknik bir gerçek eşlik eder: Tespit, üretimin gerisinde koşmaktadır. Üretken modeller hızla gelişirken, bunları saptamak için geliştirilen araçlar çoğu zaman bir önceki neslin izlerini aramak üzere eğitilmiştir. Bağımsız değerlendirmeler, laboratuvar koşullarında yüzde doksanların üzerinde başarı gösteren tespit araçlarının, gerçek dünyadan gelen ve eğitim verisinden farklı yöntemlerle üretilmiş içerikte çok daha düşük -- kimi ölçümlerde yüzde elli-altmış düzeyine inen -- doğruluk sergilediğini ortaya koymaktadır. Bu 'genelleme açığı', adli bağlamda son derece önemlidir; çünkü gerçek bir dosyadaki içerik, tespit aracının hiç görmediği bir yöntemle üretilmiş olabilir.

Meselenin bir de büyüyen ekonomik boyutu vardır. Deepfake teknolojisi, özellikle ses klonlamaya dayalı dolandırıcılıkta patlayıcı bir artışa yol açmıştır. Sektör verilerine göre yalnızca Amerika Birleşik Devletleri'nde deepfake kaynaklı dolandırıcılık zararı 2025 yılında yaklaşık 1,1 milyar dolara ulaşmış; bu, bir önceki yılın yaklaşık üç katıdır. Yöneticileri taklit eden sahte video konferanslarla milyonlarca dolarlık transferlerin gerçekleştirildiği vakalar, sorunun soyut bir tehdit değil, somut ve ölçülebilir bir zarar olduğunu göstermektedir. Bu gelişme, sentetik medya tespitini yalnızca adli değil, aynı zamanda kurumsal güvenlik ve ekonomik bir öncelik hâline getirmiştir.

Bu makalenin temel savı, tam da bu gerilimden doğar: Sentetik medya tespiti güçlü ancak mutlak olmayan bir disiplindir ve tek bir aracın çıktısına dayanan hiçbir kanaat adli açıdan güvenilir sayılamaz. Güvenilirlik, ancak çok yöntemli doğrulamanın, köken analizinin ve titiz delil yönetiminin birleşiminden doğar. Bu yaklaşım, hem sahte içeriği ifşa etmek hem de gerçek içeriği haksız şüpheden korumak için gereklidir; zira sentetik çağda adli hatanın iki yönü de -- sahteyi gerçek saymak ve gerçeği sahte ilan etmek -- eşit derecede zarar vericidir. Makale boyunca bu denge, çözümlemenin merkezinde tutulmaktadır.

burakoguz.com

Makalenin geri kalanı şu şekilde düzenlenmiştir. İkinci bölüm sentetik medyanın teknik temellerini ve üretim yöntemlerinin adli izlerini ele alır. Üçüncü bölüm pasif ve aktif tespit yaklaşımlarını; dördüncü bölüm bu yaklaşımların güvenilirlik sınırlarını inceler. Beşinci bölüm tehdit manzarasını ve dolandırıcılık boyutunu, altıncı bölüm adli inceleme sürecini ve delil bütünlüğünü ele alır. Yedinci bölüm hukuki çerçeveyi, sekizinci bölüm Türkiye bağlamını, dokuzuncu bölüm zorlukları ve önerileri kapsar. Onuncu bölüm sonucu sunar. Çalışma boyunca herhangi bir gerçek dosyaya veya kişiye atıf yapılmamış; kamuya açık raporlar ve akademik kaynaklar temel alınarak yalnızca teknik ve hukuki farkındalık amaçlanmıştır.

2. Sentetik Medyanın Teknik Temelleri

Sentetik medyanın adli tespitini anlamak için, önce bu içeriğin nasıl üretildiğini ve hangi izleri bıraktığını kavramak gerekir. Deepfake, geniş anlamda, bir kişinin görünüşünü veya sesini yapay olarak taklit eden ya da hiç var olmayan bir gerçekliği üreten, yapay zekâ tabanlı sentetik medyayı ifade eder. Bu içeriğin üretiminde iki temel mimari öne çıkar: çekişmeli üretici ağlar ve difüzyon modelleri.

2.1. Çekişmeli Üretici Ağlar ve Difüzyon Modelleri

Uzun süre deepfake üretiminin baskın yöntemi, çekişmeli üretici ağlar (Generative Adversarial Networks -- GAN) olmuştur. Bu mimaride iki sinir ağı birbiriyle yarışır: 'üretici' (generator) sahte içerik oluşturmaya çalışırken, 'ayırt edici' (discriminator) bunun sahte olup olmadığını anlamaya çalışır. Bu çekişme, üreticiyi giderek daha gerçekçi çıktılar vermeye zorlar. GAN tabanlı yöntemler, özellikle yüz değiştirme (face swap) uygulamalarında yaygınlaşmış ve ilk kuşak deepfake içeriğinin çoğunu üretmiştir. Adli açıdan önemli olan, bu yöntemlerin belirli, tanınabilir izler -- yüz sınırlarında tutarsızlıklar, göz ve diş bölgelerinde artefaktlar, ışık ve gölge uyumsuzlukları -- bırakmasıdır.

Son yıllarda ise difüzyon modelleri (diffusion models) baskın üretim paradigması hâline gelmiştir. Bu modeller, bir görüntüyü kademeli olarak gürültüye dönüştürüp ardından bu süreci tersine çevirerek, gürültüden yepyeni ve son derece gerçekçi görüntüler üretir. Midjourney, Stable Diffusion ve video üretiminde Sora sınıfı modeller bu ailedendir. Difüzyon tabanlı içerik, GAN çıktılarından farklı bir istatistiksel imzaya sahiptir; bu da, çoğunlukla GAN verisiyle eğitilmiş tespit araçlarının difüzyon içeriği karşısında zorlanmasına yol açar. Üretim paradigmasındaki bu kayma, adli tespitin neden sürekli güncellenmesi gerektiğini açıklayan temel etkenlerden biridir.

Bu iki mimarinin ötesinde, üretim araçlarının erişilebilirliği de adli tabloyu biçimlendiren kritik bir etkendir. Bir zamanlar güçlü donanım ve teknik uzmanlık gerektiren deepfake üretimi, bugün ücretsiz mobil uygulamalar ve web hizmetleri aracılığıyla herkesin erişimine açılmıştır. Bu 'demokratikleşme', tehdidin ölçeğini niteliksel olarak değiştirmiştir: Artık karşımızda az sayıda yetenekli aktör değil, milyonlarca potansiyel üretici vardır. Adli açıdan bu, hem vaka sayısının artması hem de üretim yöntemlerinin çeşitlenmesi anlamına gelir; ki bu çeşitlilik, tek bir tespit yönteminin yetersizliğini daha da belirginleştirir.

burakorgun.com

2.2. Ses Klonlama ve Sentetik Ses

Görüntü kadar kritik bir alan da sentetik sestir. Modern ses klonlama sistemleri, bir kişinin sesinden yalnızca birkaç saniyelik bir örnek kullanarak, o kişinin söylemediği cümleleri onun sesiyle üretebilir. Sektör verilerine göre, üç saniyelik bir ses örneği, özgün konuşmacıyla yaklaşık yüzde seksen beş oranında eşleşen bir klon üretmeye yetmektedir. Sesin görüntüye kıyasla daha az sinyal içermesi ve telefon hatları gibi düşük kaliteli kanallarda daha da bozulması, sentetik sesin tespitini özellikle zorlaştırır. Nitekim ses tabanlı dolandırıcılık, deepfake kötüye kullanımının en hızlı büyüyen koludur.

Sentetik ses, adli açıdan kendine özgü izler taşır. Doğal insan konuşmasındaki nefes alma örüntüleri, ağız içi rezonanslar ve prozodik (tonlama, vurgu, ritim) tutarlılık, sentetik sistemlerde çoğu zaman kusurlu biçimde yeniden üretilir. Ayrıca üretim sürecinin kendisi, insan kulağının fark edemeyeceği ancak sinyal analiziyle saptanabilen spektral artefaktlar bırakabilir. Ne var ki üretim kalitesi arttıkça bu izler silikleşmekte; bu da ses adli analizini, sürekli yenilenmesi gereken bir yarışa dönüştürmektedir.

2.3. Üretim Yöntemlerinin Adli İzleri

Her üretim yöntemi, arkasında kendine özgü izler bırakır ve adli tespit büyük ölçüde bu izlerin okunmasına dayanır. Ancak izlerin niteliği yönteme göre değişir; bir yöntem için geliştirilen bir dedektör, başka bir yöntemin izlerini göremeyebilir. Tablo 1, başlıca üretim yöntemlerini ve bıraktıkları tipik adli izleri karşılaştırmaktadır. Bu çeşitlilik, tek bir tespit yönteminin neden yetersiz kaldığını ve çok yöntemli bir yaklaşımın neden zorunlu olduğunu açıkça ortaya koyar.

Tablo 1. Başlıca Sentetik Medya Üretim Yöntemleri ve Adli İzleri

Üretim Yöntemi	Tipik Kullanım	Bıraktığı Adli İz
GAN (yüz değiştirme)	Yüz takası, video manipülasyonu	Yüz sınırı, göz/diş artefaktı, ışık uyumsuzluğu
Difüzyon modelleri	Sıfırdan görüntü/video üretimi	Frekans imzası, doku tutarsızlığı, GAN'dan farklı
Ses klonlama	Sentetik konuşma, vishing	Prozodi kusuru, nefes/rezonans eksikliği, spektral iz
Yüz yeniden canlandırma	Dudak-ses eşleme, konuşan kafa	Fonem-vizem uyumsuzluğu, mikro-ifade eksikliği

Not. Kaynak: sentetik medya adli analizi literatürü temel alınarak derlenmiştir.

2.4. Gerçek Zamanlı Deepfake ve Canlı Yayın Tehdidi

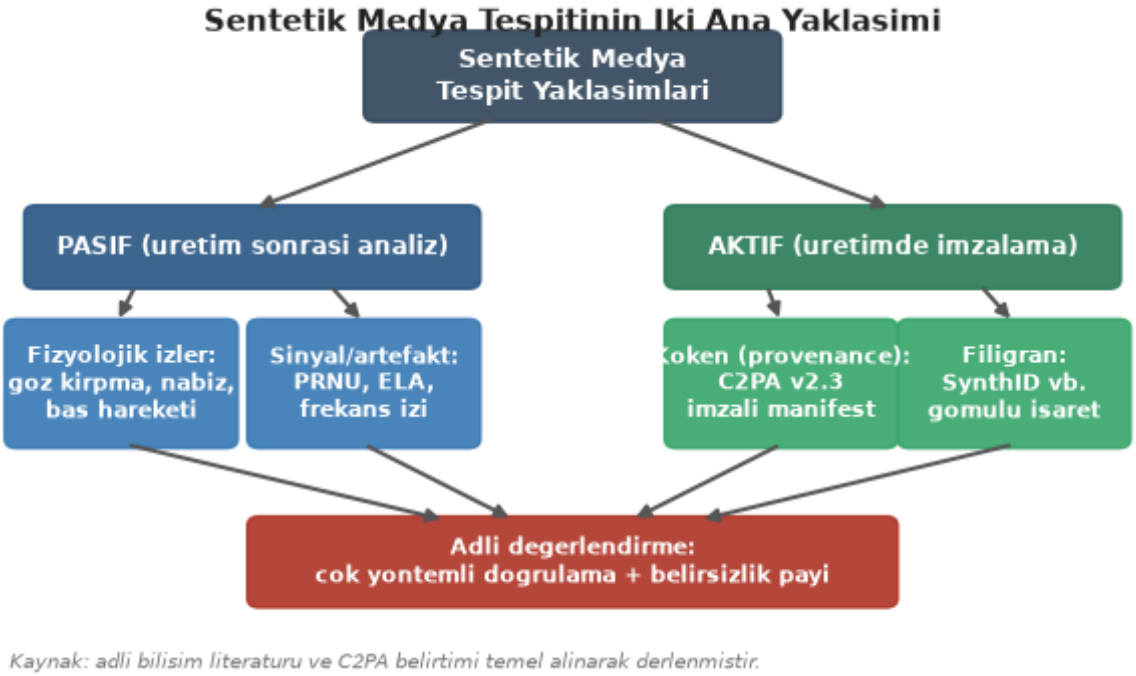
Sentetik medyanın en kaygı verici gelişmelerinden biri, üretimin gerçek zamanlıya taşınmasıdır. Erken dönem deepfake içeriği önceden hazırlanmış videolarla sınırlıyken, güncel sistemler bir görüntülü görüşme sırasında yüzü ve sesi anlık olarak değiştirebilmektedir. Bu, dolandırıcının bir üst yöneticinin yüzü ve sesiyle canlı bir toplantıya katılıp, karşı tarafın soru-cevap etkileşimine gerçek zamanlı yanıt vermesine olanak tanır. Beşinci bölümde ele alınan büyük ölçekli transfer vakaları, tam da bu canlı senaryo sayesinde bu denli ikna edici olmuştur.

Gerçek zamanlı üretim, adli tespiti iki yönden zorlaştırır. Birincisi, işlem hızı kısıtı nedeniyle bu içeriğin bazı kusurlar barındırması beklenirken, sistemler hızla iyileşerek bu

kusurları azaltmaktadır. İkincisi ve daha önemlisi, canlı bir görüşmede sonradan incelenebilecek bir 'dosya' çoğu zaman yoktur; delil, ancak görüşme kaydedildiyse elde edilebilir. Bu durum, önleyici tedbirlerin -- özellikle kritik işlemlerde canlı görüntüye değil, bağımsız kanallardan doğrulamaya dayanmanın -- neden adli tespitin önüne geçtiğini bir kez daha gösterir. Kaydı olmayan bir olayda, en gelişmiş tespit aracı bile işlevsizdir.

3. Tespit Yaklaşımları

Sentetik medya tespiti, kabaca iki ana yaklaşıma ayrılır: içeriğin üretilmesinden sonra onu analiz eden pasif yöntemler ve içeriğin üretimi sırasında ona doğrulanabilir bir imza gömen aktif yöntemler. Şekil 1, bu iki yaklaşımı ve alt dallarını göstermektedir. Olgun bir adli değerlendirme, çoğu zaman her iki yaklaşımı birlikte kullanır.



Şekil 1. Sentetik Medya Tespitinin İki Ana Yaklaşımı (2025)

3.1. Pasif Tespit: Üretim Sonrası Analiz

Pasif tespit, elde bulunan bir içeriği -- kökeni hakkında hiçbir ön bilgi olmadan -- inceleyerek sentetik olup olmadığını belirlemeye çalışır. Bu yaklaşım, adli pratikte en sık başvurulan yöntemdir; çünkü çoğu zaman incelenecek dosya, herhangi bir köken bilgisi olmadan gelir. Pasif tespit iki alt gruba ayrılabilir. Birincisi, fizyolojik ve davranışsal tutarsızlıkların analizidir: Gerçek insanlarda doğal olarak bulunan göz kırpma örüntüleri, kalp atışına bağlı ciltteki mikro renk değişimleri (fotopletismografi), doğal baş hareketleri ve konuşmada dudak biçimi ile ses arasındaki (fonem-vizem) uyum, sentetik içerikte çoğu zaman kusurludur.

İkinci alt grup, sinyal ve artefakt analizidir. Her gerçek kamera, sensöründen kaynaklanan benzersiz bir gürültü deseni (Photo Response Non-Uniformity -- PRNU) bırakır; sentetik içerikte bu sensör parmak izi ya yoktur ya da tutarsızdır. Benzer biçimde, hata düzeyi analizi

(Error Level Analysis -- ELA) sıkıştırma tutarsızlıklarını, frekans alanı incelemesi ise üretici modellerin bıraktığı periyodik izleri ortaya çıkarabilir. Bu yöntemlerin ortak zayıflığı, içeriğin yeniden sıkıştırılması, ekran görüntüsü alınması veya sosyal medyada paylaşılması gibi işlemlerle izlerin silinebilmesidir; bu da pasif tespiti kırılgan kılar.

3.2. Aktif Tespit: İçerik Kökeni ve Filigran

Aktif tespit, sorunu ters yönden ele alır: İçeriği üretildikten sonra çözmeye çalışmak yerine, üretim veya çekim anında ona doğrulanabilir bir köken bilgisi gömer. Bu alandaki en önemli girişim, İçerik Kökeni ve Gerçekliği Koalisyonu'nun (Coalition for Content Provenance and Authenticity -- C2PA) geliştirdiği standarttır. C2PA, bir medya dosyasına kriptografik olarak imzalanmış bir 'manifest' ekler; bu manifest, içeriğin hangi cihazla oluşturulduğunu, hangi yazılımlarla düzenlendiğini ve üretiminde yapay zekânın rol oynayıp oynamadığını kaydeder. Standardın Aralık 2025'te yayımlanan 2.3 sürümü, köken bilgisini canlı yayına kadar genişletmiştir.

Aktif yaklaşımın bir diğer kolu, üretici modelin çıktısına insan tarafından algılanamayan ancak makinece okunabilen bir filigran (watermark) gömmesidir. Bu sayede, sorumlu üreticilerin çıktıları kaynağında işaretlenir ve sonradan tespit edilebilir. Ancak aktif tespitin köklü bir sınırı vardır: Yalnızca beyan edilmiş kökeni doğrulayabilir; beyan edilmemiş, yani kötü niyetli bir aktörün hiç imzalamadan ürettiği içeriği saptayamaz. Dahası, bu mekanizmalar gönüllü benimsemeye dayanır ve halihazırda dolaşımdaki milyarlarca işaretsiz içeriğe karşı hiçbir koruma sağlamaz. Bu nedenle aktif ve pasif yaklaşımlar rakip değil, birbirini tamamlayıcıdır. Tablo 2 bu iki yaklaşımı karşılaştırmaktadır.

Tablo 2. Pasif ve Aktif Tespit Yaklaşımlarının Karşılaştırması

Ölçüt	Pasif Tespit	Aktif Tespit (köken/filigran)
Çalışma anı	Üretimden sonra	Üretim/çekim anında
Ön bilgi gereksinimi	Yok (her dosyaya uygulanır)	Kaynağın imzalamış olması gerekir
İşaretsiz içerik	İnceleyebilir	Koruyamaz (beyan yoksa görmez)
Temel zayıflık	Genelleme, artefakt silinmesi	Gönüllü benimseme, kapsam
Adli rol	Birincil inceleme	Doğrulama ve destekleyici kanıt

Not. Kaynak: C2PA belirtimi (2025) ve tespit literatürü temel alınarak derlenmiştir.

3.3. Yapay Zekâ Destekli Tespit ve Açıklanabilirlik

Tespit araçlarının çoğu, günümüzde bizzat derin öğrenme modellerine dayanır; yani sentetik medyayı yine yapay zekâ ile saptamaya çalışırlar. Bu modeller, büyük veri kümeleri üzerinde eğitilerek gerçek ve sahte içerik arasındaki ince istatistiksel farkları öğrenir. Yaklaşımın gücü, insan gözünün fark edemeyeceği örüntüleri yakalayabilmesidir; zayıflığı ise, bir sonuca nasıl ulaştığını çoğu zaman açıklayamamasıdır. Adli bağlamda bu 'kara kutu' niteliği ciddi bir sorundur: Bir bulgunun savunulabilmesi için, yalnızca 'model böyle dedi' demek yetmez; sonucun hangi somut kanıtlara dayandığı gösterilebilmelidir.

Bu nedenle son yıllarda açıklanabilir yapay zekâ (explainable AI) yaklaşımları önem kazanmıştır. Bu yaklaşımlar, modelin kararını hangi bölgeye veya hangi özelliğe dayandırdığını görselleştirerek, adli uzmanın sonucu değerlendirebilmesini amaçlar. Örneğin bir görüntüde

bulgu.com

modelin 'sahte' kararını yüz sınırındaki belirli artefaktlara dayandırdığının gösterilmesi, bulguyu hem daha anlaşılır hem de daha savunulabilir kılar. Yine de açıklanabilirlik, modelin genelleme açığını ortadan kaldırmaz; yalnızca uzmanın modele daha eleştirel yaklaşabilmesini sağlar. İdeal adli kullanım, otomatik aracı bir başlangıç noktası olarak alıp, insan uzmanın gerekçelendirmesiyle tamamlamaktır.

3.4. Çoklu-Modal Tespit ve Bağlam Analizi

Tek bir sinyale dayanan tespit yaklaşımlarının kırılganlığı, çoklu-modal (multi-modal) tespit fikrini öne çıkarmıştır. Bu yaklaşımda, bir içerik yalnızca tek bir açıdan değil, aynı anda birden çok boyuttan değerlendirilir: video söz konusuysa hem görüntüdeki fizyolojik tutarlılık hem sesin doğallığı hem de ses ile dudak hareketi arasındaki (fonem-vizem) uyum birlikte incelenir. Bir boyutta güçlü görünen bir sahte içerik, başka bir boyutta tutarsızlık gösterebilir; örneğin görüntüsü kusursuz bir video, ses ile dudak senkronunda küçük ama saptanabilir uyumsuzluklar barındırabilir. Bu bütünsel bakış, tek bir yöntemin atlayabileceği izleri yakalama şansını artırır.

Teknik boyutların yanında bağlam analizi de kritik bir katmandır. Bir içeriğin nereden geldiği, hangi hesap tarafından ne zaman paylaşıldığı, iddia edilen olayın diğer bağımsız kayıtlarla tutarlı olup olmadığı gibi bağlamsal sorular, çoğu zaman tek başına teknik analizden daha aydınlatıcı olabilir. Örneğin, iddia edilen bir konuşmanın yapıldığı söylenen anda kişinin başka bir yerde olduğunun bağımsız kayıtlarla gösterilmesi, teknik analizden bağımsız olarak içeriğin sahteliğine işaret edebilir. Bu nedenle olgun bir adli inceleme, teknik tespiti bağlamsal doğrulamayla birleştirir; ikisi birbirini destekler ve tek başına her birinin taşıdığı belirsizliği azaltır.

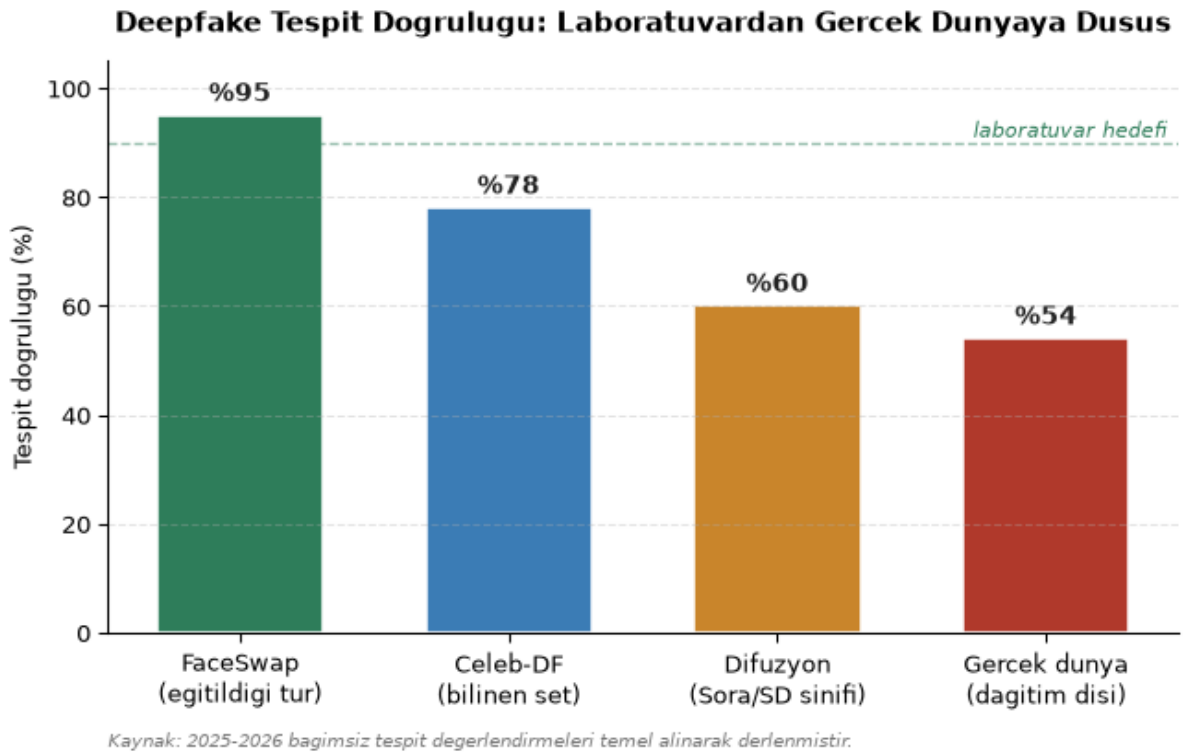
4. Tespit Güvenilirliğinin Sınırları

Sentetik medya tespitinin en kritik ve en sık göz ardı edilen yönü, güvenilirliğinin sınırlarıdır. Pazarlama söylemlerinde sıkça duyulan 'yüzde doksan dokuz doğruluk' iddiaları, adli bağlamda son derece dikkatle ele alınmalıdır; çünkü bu rakamlar genellikle laboratuvar koşullarında, aracın eğitildiği türden içerikle ölçülmüştür.

4.1. Genelleme Açığı: Laboratuvardan Gerçek Dünyaya

Tespit araçlarının en temel sorunu, genelleme yetersizliğidir. Bir araç, eğitildiği veri kümesine benzer içerikte çok yüksek başarı gösterebilir; ancak daha önce görmediği bir yöntemle üretilmiş içerikle karşılaştığında performansı çarpıcı biçimde düşer. Bağımsız değerlendirmeler, kıyaslama testlerinde yüzde doksan beş-doksan dokuz doğruluğa ulaşan araçların, gerçekçi ve dağıtım dışı verilerde yüzde elli dört-yetmiş beş düzeyine gerilediğini göstermektedir. Somut bir örnekle, yüz değiştirme içeriğinde yüzde doksan beş başarı gösteren bir motor, difüzyon tabanlı bir üreticiden gelen videoda yüzde altmış düzeyine inebilmektedir. Şekil 2 bu düşüşü görselleştirmektedir.

burakolgun.com



Şekil 2. Tespit Doğruluğunun Laboratuvardan Gerçek Dünyaya Düşüşü (2025)

Bu rakamların adli sürece yansıması doğrudandır. Bir tespit aracının 'yüzde doksan beş doğruluk' iddiası, o oranın yalnızca belirli bir üretim yöntemi ve belirli bir veri kümesi için geçerli olduğu anlamına gelir. Gerçek bir dosyada, içeriğin hangi yöntemle üretildiği çoğu zaman bilinmez; dolayısıyla aracın o dosyadaki gerçek doğruluğu, tanıtımdaki rakamdan önemli ölçüde düşük olabilir. Bu belirsizlik, tek bir aracın çıktısını kesin bir adli sonuç olarak sunmayı savunulamaz kılar. Sorumlu bir uzman, aracın hangi koşullarda hangi başarıyı gösterdiğini bilir ve bu sınırı raporuna açıkça yansıtır.

Bu genelleme açığının kökeninde, üretim ve tespit teknolojileri arasındaki asimetrik yarış yatar. Çoğu ticari dedektör, çekişmeli üretici ağlarla üretilmiş içerikle eğitilmiştir; oysa güncel sentetik medyanın önemli bölümü, temelde farklı bir süreçle çalışan difüzyon modellerinden gelmektedir. Bir yöntem için optimize edilmiş bir dedektör, diğerinin izlerini aramadığından, yeni üretim paradigmaları karşısında sistematik olarak geride kalır. Adli açıdan bunun anlamı nettir: Bir aracın 'sentetik değil' demesi, içeriğin gerçek olduğunu kanıtlamaz; yalnızca o aracın bildiği izleri bulamadığını gösterir.

4.2. Demografik Yanlılık, Açıklanabilirlik ve Yanlış Pozitifler

Genelleme açığının yanında üç sorun daha adli güvenilirliği zedeler. Birincisi demografik yanlılıktır: Araştırmalar, tespit doğruluğunun cilt tonu ve cinsiyete göre ölçülebilir biçimde değiştiğini; bazı grupların içeriğinin sistematik olarak daha yüksek hata oranıyla değerlendirildiğini göstermektedir. Bu, adil bir adli süreç açısından ciddi bir eşitlik sorunudur. İkincisi açıklanabilirlik eksikliğidir: Birçok dedektör, bir sonuca nasıl ulaştığını gerekçelendiremeyen 'kara kutu' niteliğindedir; oysa adli bir bulgunun savunulabilmesi için gerekçesinin ortaya konabilmesi gerekir.

Durakoğlu

Üçüncü sorun, yüksek yanlış pozitif oranıdır. Gerçek koşullarda, sıkıştırma, düşük çözünürlük veya alışılmadık çekim şartları, gerçek bir içeriğin sentetik olarak işaretlenmesine yol açabilir. Adli bağlamda yanlış pozitif -- gerçek bir kaydı sahte ilan etmek -- en az yanlış negatif kadar tehlikelidir; çünkü masum bir kişinin delilinin haksız yere reddedilmesine veya gerçek bir olayın inkâr edilmesine zemin hazırlar. Bu üç sorun birlikte değerlendirildiğinde, tek bir tespit aracının çıktısına dayanarak kesin bir adli kanaate varmanın neden sakıncalı olduğu açıkça görülür. Güvenilirlik, ancak birden çok bağımsız yöntemin örtüşmesiyle artar.

4.3. Rakip Saldırılar ve Karşı-Adli Teknikler

Tespit güvenilirliğini zedeleyen bir diğer etken, üreticilerin bilinçli olarak tespitten kaçınmaya çalışmasıdır. 'Rakip saldırı' (adversarial attack) olarak bilinen teknikte, sentetik içeriğe insan gözünün fark edemeyeceği ancak dedektörü yanıltacak küçük bozulmalar eklenir; böylece sahte içerik, tespit aracı tarafından 'gerçek' olarak sınıflandırılır. Benzer biçimde, içeriğin yeniden sıkıştırılması, ölçeklendirilmesi veya hafifçe bulanıklaştırılması gibi basit karşı-adli işlemler, pasif tespitin dayandığı ince artefaktları silebilir. Bu teknikler, tespit ile kaçınma arasındaki yarışın sürekli olduğunu gösterir.

Karşı-adli tekniklerin varlığı, adli değerlendirmede önemli bir alçakgönüllülük gerektirir. Bir dedektörün içeriği 'gerçek' bulması, o içeriğin gerçek olduğunu değil; ya gerçek olduğunu ya da dedektörü atlatacak biçimde işlenmiş olabileceğini gösterir. Bu nedenle olumsuz bir tespit sonucu (yani 'sahtelik bulunamadı'), asla özgünlüğün kesin kanıtı olarak sunulmamalıdır. Adli uzman, hem tespit araçlarının doğal sınırlarını hem de bilinçli kaçınma olasılığını raporunda göz önünde bulundurmalı; kesin bir aklama yerine, mevcut yöntemlerle ulaşılan güven düzeyini ifade etmelidir.

4.4. Kıyaslama Setlerinin Sınırları ve Standart İhtiyacı

Tespit araçlarının başarı iddiaları, çoğu zaman belirli kıyaslama (benchmark) veri kümeleri üzerinde ölçülür. Bu setler, alanın gelişimi için değerli olsa da, adli güvenilirliği yansıtmakta yetersiz kalabilir. Birçok kıyaslama seti, belirli üretim yöntemleriyle ve kontrollü koşullarda hazırlanmıştır; oysa gerçek bir dosyadaki içerik, farklı bir yöntemle üretilmiş, defalarca sıkıştırılmış, kırpılmış veya düşük çözünürlüklü olabilir. Bir aracın bir kıyaslama setinde yüksek puan alması, gerçek dünyadaki performansını garanti etmez. Bu uçurum, dördüncü bölümde ele alınan genelleme açığının doğrudan bir yansımasıdır.

Alanın en önemli ihtiyaçlarından biri, difüzyon tabanlı üretim de dâhil olmak üzere güncel yöntemleri kapsayan, standartlaştırılmış ve sürekli güncellenen değerlendirme çerçeveleridir. Böyle bir standart olmadan, farklı araçların iddialarını karşılaştırmak ve adli bir bağlamda hangisinin ne kadar güvenilir olduğunu belirlemek güçtür. Adli uzman açısından pratik sonuç şudur: Bir aracın tanıtımında belirtilen doğruluk oranı, o oranın hangi veri kümesinde ve hangi koşullarda ölçüldüğü bilinmeden anlamlı değildir. Raporlarda, kullanılan aracın sınırlarının ve ölçüm koşullarının belirtilmesi, bu nedenle bir dürüstlük gereğidir.

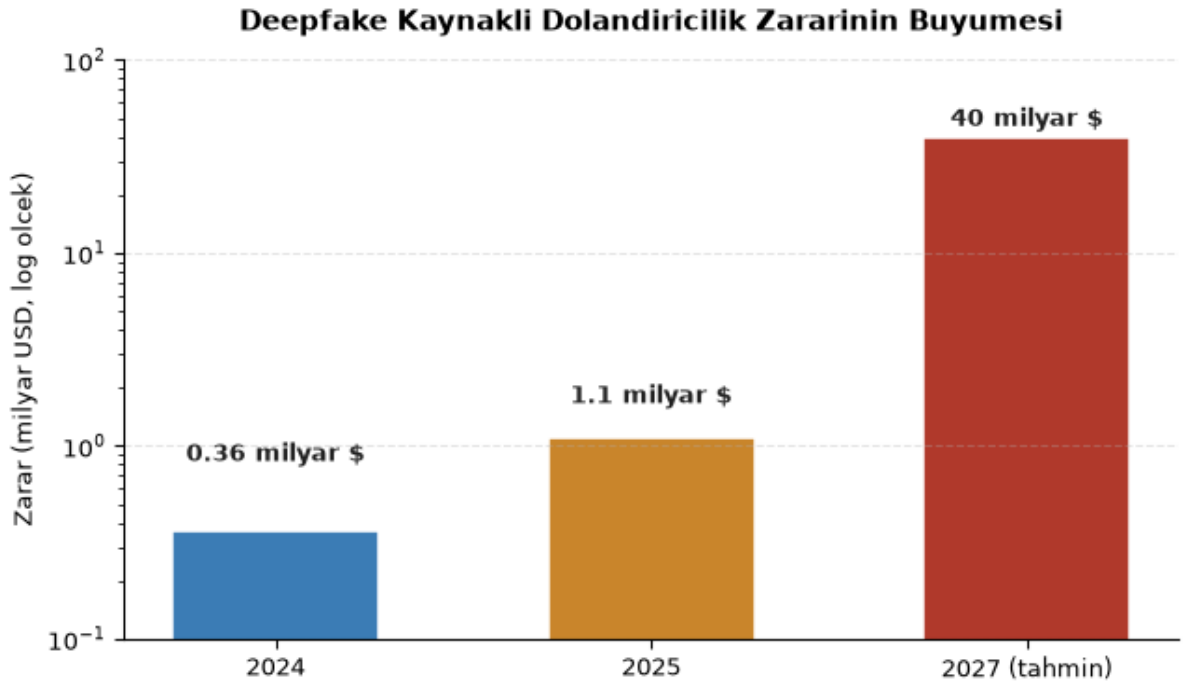
burakolgun.com

5. Tehdit Manzarası: Dolandırıcılık ve Kötüye Kullanım

Sentetik medyanın adli önemi, kötüye kullanımının ölçeğiyle doğru orantılıdır. Deepfake teknolojisi, son iki yılda özellikle ekonomik suçlarda dramatik bir araç hâline gelmiştir. Bu bölüm, tehdit manzarasının başlıca hatlarını ve büyüklüğünü ortaya koymaktadır.

En çarpıcı büyüme, ses klonlamaya dayalı dolandırıcılıkta yaşanmaktadır. Sektör verilerine göre ses klonlama saldırıları son bir yılda yaklaşık yüzde altı yüz seksen artmış; deepfake destekli sesli kimlik avı (vishing) saldırıları ise 2025'in ilk çeyreğinde bir önceki çeyreğe göre yüzde binin üzerinde bir sıçrama göstermiştir. Bu saldırılarda tipik senaryo, bir üst yöneticinin sesinin klonlanarak bir çalışandan acil para transferi talep edilmesidir. Hedeflenen kurbanların önemli bölümünün fiilen maddi kayba uğradığı bildirilmektedir; bu da yöntemin yalnızca teknik olarak değil, pratik olarak da etkili olduğunu gösterir.

Görsel deepfake'in en bilinen örneği, 2024 başında bir mühendislik firmasının Hong Kong ofisinde yaşanan vakadır: Bir çalışan, üst yöneticileri taklit eden sahte bir video konferansın ardından, toplam yaklaşık yirmi beş milyon dolarlık bir dizi transfer gerçekleştirmiştir. Bu olay, deepfake'in artık tek bir sahte görüntüyle sınırlı olmadığını; gerçek zamanlı, çok kişili ve son derece ikna edici senaryolara ulaştığını göstermesi bakımından bir dönüm noktasıdır. Şekil 3, deepfake kaynaklı dolandırıcılık zararının büyüme eğilimini özetlemektedir.



Kaynak: 2025 ABD verileri ve 2027 kuresel projeksiyonu temel alinarak derlenmistir.

Şekil 3. Deepfake Kaynaklı Dolandırıcılık Zararının Büyümesi (2025)

Giderek büyüyen bir diğer tehdit alanı, kimlik doğrulama sistemlerinin sentetik medya ile aşılmasıdır. Birçok kurum, uzaktan müşteri kabulünde (onboarding) yüz tanıma ve canlılık (liveness) denetimine dayanır; oysa gerçek zamanlı deepfake ve enjeksiyon saldırıları, bu biyometrik denetimleri atlatabilmektedir. Bu, hem sahte hesap açılışına hem de kimlik

hırsızlığına kapı aralar. Sonuç olarak sentetik medya, yalnızca içerik güvenilirliğini değil, dijital kimlik altyapısının bütününü tehdit eden bir olguya dönüşmüştür. Bu durum, canlılık denetimlerinin de sürekli güncellenmesini ve çok katmanlı doğrulamayla desteklenmesini zorunlu kılmaktadır.

Ekonomik dolandırıcılığın ötesinde, sentetik medya; iftira, şantaj, cinsel içerikli sahte görüntülerle taciz ve dezenformasyon gibi alanlarda da yoğun biçimde kötüye kullanılmaktadır. Bu kullanımların ortak paydası, mağdurun itibarını veya güvenliğini hedef almaları ve çoğu zaman hızla yayılarak geri döndürülemez zarar vermeleridir. Adli açıdan bu vakalar, hem içeriğin sentetik olduğunun teknik olarak kanıtlanmasını hem de üretici ve yayıcının tespitini gerektirir; ikisi de kendine özgü zorluklar taşır. Tehdit manzarasının bu genişliği, sentetik medya tespitini yalnızca uzmanların değil, kurumların ve bireylerin de gündemine taşımıştır.

5.1. Dezenformasyon ve Kamusal Güvenin Aşınması

Sentetik medyanın bireysel ve kurumsal zararların ötesinde bir de toplumsal boyutu vardır. Kamuya mal olmuş kişilerin ağzından hiç söylemedikleri sözlerin çıktığı sahte videolar, seçim dönemlerinde manipülasyon aracı olarak kullanılan üretilmiş görüntüler ve gerçek olayları çarpıtan sentetik içerik, kamusal tartışmanın bilgi zeminini zehirleyebilir. Bu tür içeriğin en yıkıcı etkisi, tek tek yaydığı yanlış bilgilerden çok, genel bir güvensizlik iklimi yaratmasıdır: İnsanlar her görüntüden şüphe etmeye başladığında, gerçek deliller de inandırıcılığını yitirir.

Bu olgu, beşinci bölümün başında değinilen 'yalancının kâr payı' ile doğrudan ilişkilidir. Sentetik medyanın varlığı, gerçek bir kaydı 'bu da deepfake' diyerek reddetmeyi kolaylaştırır; böylece hem sahte içerik gerçek gibi sunulabilir hem de gerçek içerik sahte ilan edilebilir. Adli açıdan bu ikili tehdit, multimedya delilinin özgünlüğünü teknik olarak belgeleme kapasitesini her zamankinden değerli kılar. Çünkü bir kaydın gerçekliğini kanıtlayabilmek, artık yalnızca sahteyi ifşa etmek kadar önemlidir; ikisi de aynı teknik titizliği gerektirir. Kamusal güvenin korunması, bu anlamda, sağlam adli doğrulama altyapısına bağımlı hâle gelmiştir.

6. Adli İnceleme Süreci ve Delil Bütünlüğü

Bir sentetik medya iddiasının adli süreçte anlam kazanması, teknik tespitin ötesinde, disiplinli bir inceleme ve delil yönetimi sürecine bağlıdır. Teknik doğruluk gereklidir ama yeterli değildir; bulgunun hukuka uygun elde edilmesi, bütünlüğünün korunması ve yeniden üretilebilir olması gerekir.

6.1. Özgünlük ve Bütünlük İncelemesi

Adli incelemenin temel amacı, incelenen kaydın özgün mü yoksa üretilmiş ya da değiştirilmiş mi olduğunu belirlemektir. Bu değerlendirme, mümkün olduğunca kaydın özgün kaynağından -- üreten cihazdan, ilk kaydedildiği dosyadan -- yola çıkmalıdır; çünkü bir kaydın üstverisi (oluşturma zamanı, cihaz bilgisi, kodlama parametreleri) ve iç yapısal tutarlılığı, özgünlüğü değerlendirmek için zengin bir zemin sunar. Ekran görüntüsü veya sosyal medyadan indirilmiş, yeniden sıkıştırılmış bir kopya, hem özgün izleri kaybettiğinden hem de manipülasyona açık olduğundan, tek başına zayıf bir inceleme nesnesidir.

burakoglu.com

Özgünlük incelemesi, çok yöntemli bir yaklaşımı gerektirir. Pasif tespit araçları, köken doğrulaması (varsa C2PA verisi), üstveri analizi, sinyal ve artefakt incelemesi ve mümkünse bağımsız kaynaklarla çapraz doğrulama, bir arada değerlendirilir. Hiçbir yöntem tek başına kesin sonuç vermediğinden, adli kanaat bu yöntemlerin örtüşmesinden -- ya da çelişmesinden -- doğar. İyi bir inceleme, yalnızca 'sentetik' veya 'gerçek' biçiminde ikili bir yargı vermez; ulaşılan sonucun güven düzeyini ve dayandığı gerekçeleri de açıkça ortaya koyar.

Özgünlük incelemesinde sık yapılan bir hata, tek bir 'deepfake tespit' aracına dosyayı yükleyip çıkan yüzdeyi sonuç olarak kabul etmektir. Bu yaklaşım, dördüncü bölümde açıklanan genelleme açığı ve yanlış pozitif riskleri nedeniyle son derece sakıncalıdır. Ticari bir aracın verdiği 'yüzde şu kadar sahte' çıktısı, o aracın eğitildiği yöntemlere ve veri kümesine bağlı, koşullu bir tahmindir; adli bir kesinlik değildir. Sorumlu bir inceleme, bu tür bir çıktıyı yalnızca bir gösterge olarak alır ve mutlaka bağımsız yöntemlerle destekler. Aksi hâlde, teknik görünümlü ama metodolojik olarak zayıf bir sonuç, adli süreci yanlış yönlendirebilir.

6.2. Delil Zinciri, Hash ve Üstveri

Dijital delilin bütünlüğü, delil zinciri (chain of custody) ile güvence altına alınır. Bir multimedya dosyasına el konulduğu andan itibaren, dosyanın kriptografik özeti (hash) alınmalı ve bu özet, dosyanın sonradan değiştirilmediğini kanıtlayan bir mühür işlevi görmelidir. İncelemenin her aşaması -- kim, ne zaman, hangi araçla, hangi işlemi yaptı -- kayıt altına alınmalı ve inceleme, bağımsız bir uzman tarafından aynı verilerle yeniden üretilebilir olmalıdır. Bu titizlik, bulgunun adli süreçte sorgulanması hâlinde ayakta kalmasını sağlar.

Üstveri, sentetik medya incelemesinde özellikle değerlidir. Bir dosyanın oluşturma ve değiştirme zaman damgaları, kullanılan cihaz ve yazılım bilgisi, kodlama parametreleri ve varsa köken manifesti, içeriğin geçmişine dair kritik ipuçları sunar. Ancak üstverinin kolayca silinebildiği veya taklit edilebildiği de unutulmamalıdır; bu nedenle üstveri, tek başına değil, içerik analiziyle birlikte ve iç tutarlılığı sınanarak değerlendirilmelidir. Üstverinin yokluğu ya da tutarsızlığı, tek başına bir 'sahtelik kanıtı' değil, daha derin incelemeyi gerektiren bir işarettir.

6.3. Bilirkişi Raporu ve Belirsizliğin İfadesi

Sentetik medya incelemesinin adli değeri, büyük ölçüde bilirkişi raporunun niteliğine bağlıdır. İyi bir rapor, kullanılan yöntemleri (hangi araç, hangi sürüm, hangi veri), elde edilen bulguları ve bunların dayanaklarını, teknik olmayan bir okuyucunun izleyebileceği bir dille ortaya koyar. En kritik nokta, belirsizliğin dürüstçe ifade edilmesidir: Tespit araçlarının hata payı, kullanılan yöntemin sınırları ve ulaşılan sonucun güven düzeyi açıkça belirtilmelidir. Olasılıksal bir değerlendirme, hiçbir zaman kesin bir tespit gibi sunulmamalıdır.

Bu dürüstlük, yalnızca etik bir gereklilik değil, aynı zamanda raporun sağlamlığının güvencesidir. Aşırı kesinlik iddia eden bir rapor, savunma tarafının aracın genelleme açığını veya yanlış pozitif oranını göstermesiyle kolayca çürütülebilir. Buna karşın, sınırlarını açıkça belirten ve sonucunu gerekçelendiren bir rapor, adli sürecin güvenle dayanabileceği bir zemin sunar. Bilirkişinin görevi, kesin bir 'sahte' ya da 'gerçek' damgası vurmak değil; mevcut yöntemlerle ulaşılabilecek en sağlam kanaati, belirsizlikleriyle birlikte ortaya koymaktır.

burakolgun.com

Tablo 4. Sentetik Medya Adli İncelemesi İçin Kontrol Listesi

Aşama	Yapılması Gereken	Amaç
1. El koyma	Özgün dosyaya ulaş, hash al	Bütünlük ve delil zinciri
2. Üstveri	Zaman damgası, cihaz, kodlama, köken	Geçmiş ve tutarlılık kontrolü
3. Pasif analiz	Fizyolojik + sinyal/artefakt inceleme	Sentetik iz arama
4. Aktif doğrulama	Varsa C2PA/filigran doğrula	Köken teyidi
5. Çapraz kontrol	Bağımsız kaynak/kayıtla karşılaştır	Özgünlüğü destekleme
6. Raporlama	Güven düzeyi + hata payı ile sun	Savunulabilir kanaat

Not. Kaynak: adli bilişim iyi uygulama ilkeleri temel alınarak derlenmiştir.

6.4. Temsilî Bir İnceleme Senaryosu

Kavramların somutlaşması için, gerçek bir dosyaya atıf yapmayan, tümüyle temsilî bir senaryo düşünelim. Bir kurum, bir üst yöneticinin talimat verdiği iddia edilen kısa bir ses kaydına dayanarak yüklü bir ödeme yaptığını, ancak yöneticinin böyle bir talimat vermediğini fark ettiğini bildirmektedir. İlk soru, kaydın özgün mü yoksa sentetik mi olduğudur. Doğru yaklaşım, öncelikle kaydın özgün kaynağına -- hangi kanaldan, hangi cihazla alındığına -- ulaşmak ve varsa üstverisini incelemektir.

İkinci aşamada çok yöntemli bir inceleme yürütülür. Sesin spektral analizi, prozodik tutarlılığı ve nefes/rezonans örüntüleri incelenir; varsa köken bilgisi doğrulanır; kaydın iletildiği kanalın üstverisi ve zaman damgaları değerlendirilir. Bu yöntemlerin her biri kısmi bir gösterge sunar; adli kanaat, bunların örtüşmesinden doğar. Örneğin, doğal nefes örüntülerinin yokluğu ile spektral bir üretim izinin bir arada bulunması, sentetik köken olasılığını güçlendirir; ancak tek bir gösterge kesin sonuç sayılmaz.

Üçüncü aşamada bulgular bir rapora dönüştürülür. Rapor, incelenen dosyayı ve özetini (hash) belgeler; kullanılan yöntemleri ve her birinin katkısını açıklar; ulaşılan sonucun güven düzeyini ve hata payını belirtir. Kritik olan, sonucun 'kesinlikle sahte' gibi mutlak bir dille değil, 'mevcut bulgular sentetik köken lehine güçlü/orta düzeyde işaret etmektedir' biçiminde, belirsizliğiyle birlikte ifade edilmesidir. Bu senaryo, makalenin ana tezini örnekler: Güvenilir sonuç, tek bir araçtan değil, çok yöntemli doğrulama ile titiz delil yönetiminin birleşiminden doğar. Senaryo tümüyle açıklayıcı amaçlıdır ve herhangi bir gerçek olayla ilişkili değildir.

6.5. Yöntem Geçerliliği ve Bilimsel Kabul

Adli bir yöntemin güvenilir sayılabilmesi için, yalnızca bir sonuç üretmesi yeterli değildir; yöntemin bilimsel olarak geçerli, sınanabilir ve bilinen bir hata oranına sahip olması beklenir. Sentetik medya tespitinde bu ölçüt özellikle önemlidir; çünkü alan hızla geliştiğinden, dün geçerli sayılan bir yöntem bugün yeni üretim teknikleri karşısında güvenilirliğini yitirebilir. Bir uzmanın kullandığı aracın veya yöntemin bilimsel literatürde sınanmış olması, hata oranının belgelenmiş olması ve bağımsız uzmanlarca tekrarlanabilmesi, bulgunun ağırlığını doğrudan etkiler.

Bu ölçüt, adli uzmana pratik bir sorumluluk yükler: Kullandığı yöntemi seçerken, onun bilimsel dayanağını ve sınırlarını bilmeli; raporunda yalnızca sonucu değil, yöntemin geçerliliğine ilişkin gerekçeleri de sunabilmelidir. Doğrulanmamış, kapalı ve hata oranı

burakolgun.com

bilinmeyen bir aracın çıktısına dayanan bir kanaat, ne kadar teknik görünürse görünsün, sağlam bir temele oturmaz. Buna karşın, bilimsel olarak kabul görmüş yöntemleri şeffaf biçimde uygulayan ve sonuçlarını belirsizlik payıyla birlikte sunan bir inceleme, adli sürecin güvenle dayanabileceği bir zemin oluşturur. Yöntem geçerliliği, bu anlamda, sentetik medya adli incelemesinin görünmeyen ama en temel güvencesidir.

7. Hukuki Çerçeve

Sentetik medyanın adli değeri, nihai olarak hukuki çerçeve içinde belirlenir. Bu bölüm, konuyu önce Türk hukuku, ardından uluslararası düzenlemeler açısından ele almaktadır.

7.1. Türk Hukuku: TCK, KVKK ve Yargıtay İçtihadı

Türk hukukunda 'deepfake' hâlihazırda tek ve doğrudan bir suç tipi olarak tanımlanmamıştır. Bunun yerine, sentetik medyanın kötüye kullanımı, içeriğin niteliğine göre Türk Ceza Kanunu'nun (TCK) çeşitli hükümleriyle ve Kişisel Verilerin Korunması Kanunu (KVKK) ile birlikte cezalandırılır. Bir deepfake içerik; hakaret, özel hayatın gizliliğini ihlal, kişisel verilerin hukuka aykırı biçimde ele geçirilmesi, müstehcenlik, iftira, nitelikli dolandırıcılık ve belgede sahtecilik gibi çok sayıda suçu aynı anda oluşturabilir. Bu hükümlerin bir arada uygulanması, tek bir fiil için ağır cezalara yol açabilir. Tablo 3, ilgili başlıca TCK hükümlerini özetlemektedir.

Tablo 3. Deepfake Kötüye Kullanımında Uygulanabilecek Başlıca TCK Hükümleri

Fiil	İlgili Hüküm	Korunan Değer
Sahte içerikle onur zedeleme	TCK m. 125 (hakaret)	Şeref ve saygınlık
Özel görüntü/ses üretme-yayma	TCK m. 134 (özel hayatın gizliliği)	Özel hayat
Kişisel veriyle sentetik içerik	TCK m. 135-136 (kişisel veri)	Veri mahremiyeti
Cinsel içerikli sahte medya	TCK m. 226 (müstehcenlik)	Genel ahlak, mağdur
Sahte isnatla suçlama	TCK m. 267 (iftira)	Adliyenin işleyişi, birey
Sahte ses/görüntüyle aldatma	TCK m. 157-158 (nitelikli dolandırıcılık)	Malvarlığı

Not. Kaynak: yürürlükteki mevzuat ve doktrindeki değerlendirmeler temel alınarak derlenmiştir. Somut nitelendirme olayın özelliğine göre değişir.

Delil hukuku boyutunda, Yargıtay'ın yerleşik içtihadı sentetik medya çağında özellikle önem kazanmaktadır. Bu içtihada göre ses, görüntü ve elektronik kayıtların delil olarak kullanılabilmesi için 'özgünlük ve bütünlük' testinden geçmeleri gerekir. Silme, ekleme, kesme veya düzenleme iddiası bulunan hiçbir dijital kaydın, uzman bilirkişi incelemesinden geçmeden hükme dayanak yapılamayacağı kabul edilmektedir. Bu ilke, deepfake tehdidi karşısında adli sürecin en önemli güvencesidir: Bir multimedya kaydının varlığı tek başına yeterli değildir; özgünlüğünün teknik olarak doğrulanması aranır.

Düzenleyici tarafta iki gelişme dikkat çekicidir. Birincisi, Kişisel Verileri Koruma Kurumu'nun 2025 sonunda yayımladığı üretken yapay zekâ ve kişisel verilerin korunmasına ilişkin rehberdir; bu rehber, deepfake, ses klonlama ve sahte görüntü üretiminin kişisel veri güvenliği açısından risklerine dikkat çekmektedir. İkincisi, 2025'in Kasım ayında yapay zekâ içeriklerine yönelik önlemler öngören bir kanun teklifinin gündeme gelmesidir. Teklif; kişilik

burak-kum.com

haklarını ihlal eden veya kamu güvenliğini tehdit eden içeriğe erişimin kısa süre içinde engellenmesini, içerik sağlayıcılar ile yapay zekâ geliştiricilerinin müşterek sorumluluğunu ve yapay zekâ ile üretilmiş içeriğin görünür biçimde etiketlenmesini öngörmektedir. Bu düzenlemeler, sentetik medyaya ilişkin hukuki çerçevenin hızla olgunlaştığını göstermektedir.

7.2. Uluslararası Çerçeve: Şeffaflık ve Köken Standartları

Uluslararası düzlemde iki eğilim öne çıkar. Birincisi, düzenleyici şeffaflık yükümlülükleridir. Avrupa Birliği'nin yapay zekâ düzenlemesi, sentetik içeriğin -- deepfake dâhil -- yapay zekâ tarafından üretildiğinin açıkça belirtilmesini ve etiketlenmesini öngörmektedir. Bu tür şeffaflık kuralları, kötü niyetli aktörleri doğrudan durdurmasa da, meşru içerik ekosisteminde köken bilgisini standart hâline getirerek adli doğrulamayı kolaylaştırır.

İkinci eğilim, teknik köken standartlarının yaygınlaşmasıdır. C2PA gibi girişimler, cihaz üreticileri, yazılım firmaları ve medya kuruluşlarının katılımıyla, içeriğin kökenini kriptografik olarak doğrulanabilir kılmayı amaçlar. Bu standartların adli değeri, gelecekte içeriğin 'nereden geldiğini' güvenilir biçimde belgeleyebilme potansiyellerinde yatar. Ancak bu yaklaşımın etkinliği, ne kadar yaygın benimsendiğine bağlıdır; gönüllülük esasına dayandığı sürece, kötü niyetli üretimin önemli bölümü kapsam dışında kalacaktır. Bu nedenle uluslararası çerçevede de, aktif köken standartları ile pasif adli tespitin birlikte yürütülmesi zorunludur.

7.3. Delil Değerlendirmesinde Uzman Görüşünün Rolü

Sentetik medya çağında, multimedya delilinin değerlendirilmesi giderek daha fazla uzman bilgisine dayanmaktadır. Bir ses veya görüntü kaydının özgünlüğü, artık çıplak gözle veya kulakla güvenilir biçimde değerlendirilemez; teknik bir inceleme gerektirir. Bu durum, bilirkişilik kurumunun adli süreçteki ağırlığını artırmaktadır. Adli makam, çoğu zaman teknik ayrıntıyı doğrudan değerlendiremeyeceğinden, uzmanın raporuna ve bu raporun anlaşılırlığına güvenmek durumundadır. Dolayısıyla uzmanın sorumluluğu yalnızca doğru bir sonuca ulaşmak değil, o sonucu teknik olmayan bir okuyucunun izleyebileceği biçimde gerekçelendirmektir.

Bu ağırlık, beraberinde bir risk de getirir. Aşırı kesinlik iddia eden veya sınırlarını gizleyen bir uzman görüşü, adli sürecin yanlış yönlenmesine yol açabilir; çünkü teknik otoritenin ağırlığı, gerçekte olduğundan daha kesin bir izlenim yaratabilir. Bu nedenle uzmanın, kullandığı yöntemin bilinen hata oranlarını, genelleme sınırlarını ve alternatif açıklamaları açıkça ortaya koyması beklenir. İyi bir uzman görüşü, tarafların ve adli makamın sorgulayabileceği, denetlenebilir bir yapıya sahiptir. Silahların eşitliği ilkesi gereği, savunma tarafının da bağımsız bir inceleme yaptırabilmesi ve raporu sınayabilmesi, adil bir değerlendirmenin vazgeçilmez bir parçasıdır.

8. Türkiye Bağlamı ve Uygulama

Türkiye, hem yüksek sosyal medya kullanımı hem de yaygın mobil bankacılık nedeniyle, sentetik medya kaynaklı tehditlere açık bir ortama sahiptir. Ses klonlamaya dayalı dolandırıcılık, sahte görüntülerle itibar saldırıları ve dezenformasyon, Türk adli makamlarının giderek daha sık karşılaştığı vaka türleridir. Bu vakalarda ortak zorluk, içeriğin sentetik olduğunun teknik olarak kanıtlanması ve failin tespitidir.

burakoguz.com

Uygulamada üç temel güçlük öne çıkar. Birincisi kapasite sorunudur: Sentetik medya incelemesi, güncel araçlara ve sürekli güncellenen uzmanlığa ihtiyaç duyar; bu kapasitenin kolluk ve adli birimlerde yaygınlaştırılması gerekir. İkincisi hız sorunudur: Sentetik içerik, saatler içinde milyonlara ulaşıp geri döndürülemez zarar verebilir; oysa tespit, engelleme ve failin belirlenmesi süreçleri daha yavaş işler. Yeni kanun teklifinde öngörülen kısa süreli erişim engelleme mekanizması, tam da bu hız asimetrisine yanıt verme çabasıdır. Üçüncüsü ise atıf sorunudur: Bir içeriği kimin ürettiğini ve yaydığını belirlemek, çoğu zaman içeriğin sentetik olduğunu kanıtlamaktan daha zordur.

Kapasite geliştirmenin yanında, kurumsal farkındalık da belirleyicidir. Ses klonlama dolandırıcılığının başarısı, çoğu zaman teknik bir açıktan değil, bir çalışanın 'patronun sesini tanıdığına' duyduğu güvenden kaynaklanır. Bu nedenle en etkili savunma katmanlarından biri, çalışanların sentetik ses ve görüntü tehdidi konusunda bilinçlendirilmesi ve kritik işlemlerde sese dayalı tek kanallı onayın kurumsal politikayla yasaklanmasıdır. Adli tespit, olay gerçekleştikten sonra devreye girer; oysa farkındalık ve süreç tasarımı, olayı en baştan önleyebilir. İki katman birbirinin yerine değil, tamamlayıcısıdır.

Bu güçlüklere karşı önerilebilecek yaklaşım, teknik ve hukuki uzmanlığın bir arada yürütüldüğü disiplinler arası bir modeldir. Bilirkişilik uygulamasında, incelemenin çok yöntemli olması, kullanılan araçların sınırlarının açıkça belirtilmesi ve sonucun güven düzeyiyle birlikte raporlanması beklenmelidir. Ayrıca, kurumların önleyici tedbirler alması -- özellikle finansal işlemlerde yalnızca sese dayalı onayı kaldırıp çok kanallı doğrulamaya geçmesi -- ses klonlama dolandırıcılığına karşı en etkili savunmadır. Adli tespit ne kadar gelişirse gelişsin, önleme her zaman tespitten daha ucuz ve daha güvenilirdir.

Uluslararası iş birliği, Türkiye bağlamının bir diğer önemli boyutudur. Sentetik içerik çoğu zaman yurt dışı platformlarda üretilip yayıldığından, hem içeriğin kaldırılması hem de failin tespiti sınır ötesi iş birliğini gerektirir. Yurt dışı hizmet sağlayıcılardan veri temini, uluslararası adli yardımlaşma süreçlerine bağlıdır ve zaman alabilir; oysa sentetik içeriğin zararı hızla büyür. Bu nedenle, platformlarla kurulacak hızlı bildirim ve kaldırma kanalları ile yeni düzenlemede öngörülen kısa süreli erişim engelleme mekanizmaları, pratik açıdan belirleyici öneme sahiptir. Ayrıca, alanında yetkin bilirkişilerin yetiştirilmesi ve sentetik medya incelemesi için ortak metodolojik standartların oluşturulması, Türkiye'nin bu tehdide kurumsal yanıtının temel taşlarıdır.

9. Zorluklar, Sınırlar ve Öneriler

Sentetik medya adli tespiti, hızla gelişen ancak sınırları dürüstçe kabul edilmesi gereken bir disiplindir. Aşağıdaki maddeler, alanın başlıca zorluklarını ve bunlara ilişkin önerileri özetlemektedir:

- **Genelleme açığını kabul et:** Hiçbir dedektör, eğitilmediği bir üretim yöntemi karşısında güvenilir değildir; tek bir araç çıktısına dayanma.
- **Çok yöntemli doğrula:** Pasif analiz, köken doğrulaması, üstveri ve çapraz kaynağı birlikte kullan; kanaat, yöntemlerin örtüşmesinden doğar.

burakolgun.com

- **Belirsizliği raporla:** Sonucun güven düzeyini, hata payını ve yöntem sınırlarını açıkça belirt; olasılığı kesinlik gibi sunma.
- **Özgün kaynağa yönel:** Ekran görüntüsü veya yeniden sıkıştırılmış kopya yerine, mümkünse üreten cihazdaki özgün dosyaya ulaş.
- **Yanlış pozitifi ciddiye al:** Gerçek bir kaydı sahte ilan etmek, en az sahteyi kaçırmak kadar zararlıdır; iki hata türünü de dengele.
- **Köken altyapısını destekle:** C2PA gibi standartların benimsenmesi, gelecekteki doğrulamayı kolaylaştırır; ancak tek başına yeterli değildir.
- **Önlemeyi önceliklendir:** Özellikle finansal onayda çok kanallı doğrulama, ses klonlama dolandırıcılığına karşı tespitten daha etkilidir.

Bu önerilerin ortak paydası, teknik yetkinliğin metodolojik şeffaflık ve hukuki titizlikle birleştirilmesidir. Sentetik medya tespiti, tek başına bir 'sihirli değnek' değildir; ancak çok yöntemli bir yaklaşım, köken analizi ve sağlam delil yönetimiyle birleştiğinde, sentetik çağda gerçekle sahteyi ayırt etmenin en güvenilir yoludur.

10. Sonuç

Üretken yapay zekâ, ses ve görüntünün 'kendiliğinden gerçek' sayıldığı çağı sona erdirmiştir. Artık her multimedya kaydı, özgünlüğü teknik olarak sınanması gereken bir iddiadır. Bu makalede gösterildiği üzere, sentetik medya tespiti güçlü ancak sınırlı bir disiplindir: Laboratuvar başarıları gerçek dünyada belirgin biçimde düşmekte, üretim yöntemleri tespit araçlarının önünde koşmakta ve hiçbir yöntem tek başına kesin sonuç vermemektedir.

Bu sınırlar, karamsarlık için değil, doğru yöntem için bir çağrıdır. Güvenilir bir adli kanaat, tek bir aracın çıktısından değil; pasif analiz, aktif köken doğrulaması, üstveri incelemesi ve çapraz kaynağın birlikte değerlendirilmesinden doğar. Delil zincirinin titizlikle korunması ve belirsizliğin dürüstçe ifade edilmesi, bu kanaatin adli süreçte ayakta kalmasının önkoşuludur. Türkiye açısından, gelişen TCK uygulaması, KVKK rehberi, Yargıtay'ın özgünlük-bütünlük içtihadı ve yeni gündeme gelen düzenlemeler, bu titiz yaklaşımı destekleyen bir hukuki zemin oluşturmaktadır.

Bu makalenin ortaya koyduğu bir diğer örüntü, üretim ile tespit arasındaki asimetridir. Yeni bir üretim yöntemi ortaya çıktığında, ona uyarlanmış tespit araçları ancak bir gecikmeyle gelir; bu arada sentetik içerik dolaşıma girer ve zarar verir. Bu asimetri, tespit odaklı bir stratejinin tek başına yeterli olamayacağını gösterir. Köken doğrulama altyapısının yaygınlaşması, kurumsal süreçlerin sentetik medyaya dayanıklı biçimde tasarlanması ve toplumsal farkındalığın artırılması, tespit araçlarının açığını kapatan tamamlayıcı katmanlardır. Sorun yalnızca teknik değil, aynı zamanda kurumsal ve toplumsal bir sorundur; çözümü de öyle olmak zorundadır.

Nihai olarak, sentetik medya çağında adaletin güvencesi, ne teknolojiye körü körüne güvenmekte ne de her kaydı peşinen reddetmektedir. Güvence, teknik gerçeği belirsizlikleriyle birlikte, hukuki çerçeveyi gözeterek ve şeffaf bir yöntemle ortaya koyabilen uzmanlıkta yatar. Üretim ile tespit arasındaki yarış sürecektir; bu yarışta belirleyici olan, statik bir araç değil,

burakolgun.com

sürekli öğrenen, sınırlarının farkında olan ve dürüstlüğü yöntemin merkezine koyan bir adli yaklaşımdır.

Kaynakça

Coalition for Content Provenance and Authenticity. (2025). *C2PA technical specification (Version 2.3)*. C2PA. https://c2pa.org/specifications/

European Union. (2024). *Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (AI Act)*. Official Journal of the European Union.

Guarnera, L., Giudice, O., & Battiato, S. (2020). DeepFake detection by analyzing convolutional traces. *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops*, 666-667. https://doi.org/10.1109/CVPRW50498.2020.00341

Korshunov, P., & Marcel, S. (2022). Improving generalization of deepfake detection with data farming and few-shot learning. *IEEE Transactions on Biometrics, Behavior, and Identity Science*, 4(3), 386-397. https://doi.org/10.1109/TBIOM.2022.3143404

Kişisel Verileri Koruma Kurumu. (2025). *Üretken yapay zekâ ve kişisel verilerin korunması rehberi*. KVKK.

Kişisel Verileri Koruma Kurumu. (2024). *Deepfake bilgi notu*. KVKK. https://www.kvkk.gov.tr/

Masood, M., Nawaz, M., Malik, K. M., Javed, A., Irtaza, A., & Malik, H. (2023). Deepfakes generation and detection: State-of-the-art, open challenges, countermeasures, and way forward. *Applied Intelligence*, 53, 3974-4026. https://doi.org/10.1007/s10489-022-03766-z

Rossler, A., Cozzolino, D., Verdoliva, L., Riess, C., Thies, J., & Niessner, M. (2019). FaceForensics++: Learning to detect manipulated facial images. *Proceedings of the IEEE/CVF International Conference on Computer Vision*, 1-11. https://doi.org/10.1109/ICCV.2019.00009

Verdoliva, L. (2020). Media forensics and deepfakes: An overview. *IEEE Journal of Selected Topics in Signal Processing*, 14(5), 910-932. https://doi.org/10.1109/JSTSP.2020.3002101

5237 sayılı Türk Ceza Kanunu. (2004). *Resmî Gazete* (Sayı: 25611). (m. 125, 134, 135-136, 157-158, 226, 267).

6698 sayılı Kişisel Verilerin Korunması Kanunu. (2016). *Resmî Gazete* (Sayı: 29677).

5271 sayılı Ceza Muhakemesi Kanunu. (2004). *Resmî Gazete* (Sayı: 25673). (m. 134, dijital delil; m. 63-67, bilirkişi).

Türkiye Büyük Millet Meclisi. (2025). *Yapay zekâ içeriklerine yönelik önlemlere ilişkin kanun teklifi* (7 Kasım 2025 tarihli teklif metni). TBMM.

National Institute of Standards and Technology. (2024). *Reducing risks posed by synthetic content* (NIST AI 100-4). U.S. Department of Commerce.

burakolgun.com

Chesney, R., & Citron, D. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. *California Law Review*, 107(6), 1753-1820.

Groh, M., Epstein, Z., Firestone, C., & Picard, R. (2022). Deepfake detection by human crowds, machines, and machine-informed crowds. *Proceedings of the National Academy of Sciences*, 119(1), e2110013119. https://doi.org/10.1073/pnas.2110013119

Farid, H. (2022). Creating, using, misusing, and detecting deep fakes. *Journal of Online Trust and Safety*, 1(4). https://doi.org/10.54501/jots.v1i4.56

Yargıtay Ceza Genel Kurulu. (2015). *Ses ve görüntü kayıtlarının delil değerine ilişkin ilkeler* (özgünlük ve bütünlük değerlendirmesi). (Karar özeti).

burakolgun.com