

TEMMUZ 2026

SAYI: 4

HAKKIM VAR!

HUKUK DERGİSİ



BİLİŞİM HUKUKU

SUNUŞ

DEĞERLİ OKURLAR,

Hakkım Var! kurulduğu ilk günden bu yana bir dernek olmanın ötesinde, hukukun toplumun her kesimine ulaşabileceğine inanan bir hareket olmayı hedefledi. Bu hedef, zamanla birçok paydaşının ortak emeğiyle büyüdü. Bugün Hakkım Var'ın izlerine, etkinliklerinden ve projelerinden ayrıca; farklı şehirlerde, kurumlarda ve hukukun konuşulduğu her alanda rastlamak mümkün. Bu sahiplenme, Hakkım Var'ın en büyük kazanımlarından biri olduğu kadar aynı zamanda büyük bir ideale ilerlerken dönüp bakıldığında katedilen yolun en güçlü sağlamasıdır.

2022'den bugüne kadar hep birlikte hukukun toplumun ortak dili hâline gelmesi gerektiğine inandık ve bunun için çabaladık. Dergilerimiz, blog yazılarımız ve temas edebileceğimiz her alanda hukuk okuryazarlığını artırmayı ve toplumsal farkındalık oluşumunu desteklemeyi amaçladık. Çünkü bir hukukçu için hukuk, hiçbir zaman mesleki sınırlar içerisinde değerlendirilebilecek bir alan değildir. Hukuk; amfilerden, bürolardan, mahkeme salonlarından taşarak yaşamın her alanına temas eden ve hayatın merkezinde yer alan bir değerdir. Bu nedenle yalnızca hukuku takip eden değil, onun toplumla buluştuğu her noktada var olmaya çalışan bir anlayışı izleyerek, üniversitelerde, liselerde, sivil toplumda, dijital mecralarda ve hukukun insan hayatına temas ettiği her yerde bulunmayı amaçladık.

Hakkım Var Dergisi, belki de bilginin en nitelikli ve en doyurucu sunuluş biçimi olan yazılı eser olması ve kalıcılığıyla yarattığı birikim nedeniyle çok kıymetli. Bu nedenle dergiyi sadece bir yayın değil aynı zamanda geleceğe bırakılan bir birikim olarak görüyoruz. Bu birikimin ortaya çıkmasında emeği bulunan bütün yol arkadaşlarımızın gösterdiği özveri ise benim için çok büyük bir mutluluk ve gurur kaynağı, zira derginin her sayfasında uzun bir hazırlık sürecinin, büyük bir titizliğin ve ortak emeğin izleri bulunmaktadır. Şüphesiz ki yazarlarımızın bilgi ve birikimlerini paylaşma iradesi, yayın kurulumuzun özverili çalışmaları olmaksızın bu eser hayat bulamazdı. Bu vesileyle, dergimize emek veren tüm kıymetli yazarlarımıza, özverili yayın ekibimiz Şule Kayaoluk ve Ezgi Su Sili'ye ve katkılarıyla bu dergiyi mümkün kılan herkese en içten teşekkürlerimi ve minnettarlığımı sunuyorum.

MEHMET FATİH SELVİ
HAKKIM VAR DERNEĞİ BAŞKANI

SUNUŞ

DEĞERLİ OKUYUCU,

Uzun süren bir hazırlık sürecinin ardından yeni sayımızla karşınızda olmanın heyecanını yaşıyoruz. Bizler, hukuk dünyasındaki gelişmeleri sadece takip etmekle kalmayıp, bu gelişmelere analitik ve özgün bir perspektifle katkı sunmayı amaçlıyoruz.

Bu dergi, Hakkım Var! Derneği Fellowship Programı kapsamında yürütülen çalışmalar ile dernek üyelerimizin özverili katkılarından oluşan bir bütündür. İçinde bulunduğumuz dönem, bilginin hızla tüketilip unutulmasına değil; sindirilip, zihinsel bir olgunluğa dönüştürülmesine ihtiyaç duymaktadır. Hukuku sadece mevzuatın sınırlarına hapsetmeyip, hayatın her anına temas ederek derinlemesine incelemek ve özgün yorumlarımızla mevcut tartışmalara yeni pencereler açmak istiyoruz.

Hakkım Var Derneği olarak daha adil, barışçıl ve demokratik bir toplum için çalışmaya devam edeceğiz. Bilginin paylaştıkça çoğaldığına inanarak sizleri bu yolculukta yeni fikirler üzerinde düşünmeye davet ediyoruz. Keyifli okumalar dileriz!

ŞULE KAYAOLUK
BAŞ EDITÖR

İÇİNDEKİLER

01

The Right to Protest Under Digital Surveillance: A Constitutional Analysis of Türkiye

MUSTAFA EMRE DEMİR

Bu makale, protesto alanlarındaki yüksek teknolojiye dijital gözetimden kaynaklanan hukuki sorunları Türkiye örneği üzerinden analiz etmekte ve çeşitli çözüm önerileri sunmaktadır.

05

Dijital Yargılama Sistemlerinde Güncel Sorun: Deepfake Delillerin Dürüstlük Kuralı ve İspat Hukuku Bağlamında Değerlendirilmesi

ŞULE KAYAOLUK

Bu makale, dijitalleşen yargılama süreçlerinde mahkemelere sunulan 'Deepfake' içeriklerin, dürüstlük kuralı ve ispat hukuku çerçevesinde oluşturduğu hukuki riskleri Türk hukuku ışığında incelemektedir.

10

Avrupa Birliği Yapay Zeka Yasası

PELİN ŞENGÜN

Bu makale, yapay zekanın hızla gelişen güvenlik risklerine karşı devletlerin aldığı önlemleri incelemekte; özellikle Avrupa Birliği tarafından yürürlüğe konulan ilk kapsamlı yasal düzenlemeyi ele alarak konunun hukuki boyutunu irdelemektedir.

13

Yapay Zeka Çağında Adil Kullanım ve Hukuki Belirsizlikler

FİLİZ İŞİK

Bu makale, üretken yapay zeka modellerinin veri kullanımı ile fikri mülkiyet hukuku arasındaki çatışmayı incelemekte; 'Adil Kullanım' doktrini ışığında yaratıcılığın korunması ile teknolojik gelişim arasındaki hukuki dengeyi sorgulamaktadır.

17

Kamusal Alanda Yapay Zeka Destekli Denetim ve Siyasal İfade Özgürlüğü Üzerine Etkileri

İKLİM GÜNEŞ ATAR, FATMA RÜMEYSA TUNAY

Bu makale, kamu otoritelerinin meydanlarda yürüttüğü yapay zeka destekli gözetimin, bireylerin toplantı ve gösteri yürüyüşü hakkı ile bu hakkın ayrılmaz bir parçası olan siyasal ifade özgürlüğü üzerindeki daraltıcı etkisini incelemektedir.

Hukuk okuryazarlığını artırmayı misyon edindik. Hukuk öğrencilerinin hukukun her alanında ortaya koydukları makalelerini sizlerle paylaşmanın mutluluğunu yaşıyoruz, iyi okumalar diliyoruz...

THE RIGHT TO PROTEST UNDER DIGITAL SURVEILLANCE: A CONSTITUTIONAL ANALYSIS OF TÜRKİYE

MUSTAFA EMRE DEMİR

I. Introduction

Recent advances in digital surveillance technologies have fundamentally altered the conditions for exercising the right to protest. In Türkiye, reports regarding the use of facial recognition technologies during public demonstrations have raised serious constitutional questions regarding legality, proportionality, and the protection of the essence of fundamental rights. This article analyses the legal problems arising from high-tech digital surveillance in protest areas, using the Turkish case as an example, and offers various solutions.

II. The Right to Protest (Freedom of Peaceful Assembly) in Türkiye

a. Constitutional Framework

The right to protest in Türkiye is guaranteed by Article 34 of the Turkish Constitution (the "Constitution"): everyone has the right to hold unarmed and peaceful meetings and demonstration marches without prior permission. This right is an extension of the freedom of expression recognized in Article 26 of the Constitution.

The right to protest enables individuals to express their views collectively in public spaces. The concept of "assembly" underlies this right, aiming to protect common interests through visible actions. Often manifesting as political opposition, this right is fundamental in democratic participation by allowing citizens to challenge political authority outside of formal electoral channels. The effective exercise of this right is closely linked to accountability and pluralism within a constitutional order (Venice Commission and OSCE/ODIHR 1-2). As a result, protecting it goes beyond individual freedom of expression and emerges as a necessity for a democratic society.

b. Provisions of the Law on Meetings and Demonstrations

However, as Şirin argues, this fundamental right has been largely rendered ineffective by the strict, ambiguous, and practically prohibitive provisions of the Law on Meetings and Demonstrations (the "Law No. 2911") (7-10). As

stated above, prior permission is not required to exercise the right to protest. The notification system envisaged by the Law No. 2911 has effectively become a permission mechanism, despite the principle of "without prior permission" in the Constitution; any meeting organized without notification can be considered "unlawful" (Anayurt 119).

Moreover, since the grounds for prohibition under the law are based on unpredictable and broadly interpretable concepts such as "public order" and "general security," it opens the door to arbitrary interventions by the administration (Özenç 126). Therefore, the authorities could treat these notifications, based on these broad terms, as "permission" and ban the protests. In this context, although the exercise of the right is possible on paper, it is systematically obstructed in practice.



c. Digital Surveillance in Protests

Technological advancements and security concerns have created a new problem. It was known that CCTV cameras were used during public demonstrations, although this was controversial in terms of the exercise of rights (Abanoz Öztürk 155). In addition, media reports suggested that facial recognition systems were being used in public spaces (Gostoli; "In Turkey"). Moreover, the interior minister stated that facial recognition would be added to body cameras that record interactions between civilians and law enforcement ("Polislere"). The possibility of identifying individuals participating in protests deemed "illegal" due to lack of notification through these systems creates a deterrent and potentially punitive effect on the exercise of the right to protest.

d. Assessment of the Principle of Legality

Under Article 6 of the Personal Data Protection Law of Türkiye, facial data is classified as “special category data”. Data falling into this category may be processed with the consent of the data subject or in cases where there is a clear legal basis (Şimşek 86). It is clear that the individuals participating in the protest did not give such consent, therefore a clear legal basis must be sought. Furthermore, there is no legal basis for the use of CCTV cameras in the law enforcement laws or provincial administration laws. The administration relies on its public order function, which is a general authority of law enforcement, when carrying out this activity (Özer 155). Therefore, there is no explicit legal basis. Although Article 11 of the Law No. 2911 provides that audio and video recordings may be made during meetings and demonstrations, it does not regulate the processing of individuals' facial data and does not constitute a clear legal basis (Venice Commission and OSCE/ODIHR 66).

This situation also fails to satisfy the “quality of law” requirement developed in the jurisprudence of the European Court of Human Rights. According to this standard, interferences with fundamental rights must be accessible, foreseeable, and accompanied by adequate safeguards against arbitrariness. A general reference to public order powers, without clear limits on scope, purpose, and duration, cannot meet this threshold in a democratic society governed by the rule of law (European Court of Human Rights 15–16).

A similar concern can be observed in the jurisprudence of the Turkish Constitutional Court. The Court has consistently held the view that interference with the freedom of assembly should not impair the essence of the right and should be surrounded by strict safeguards to prevent arbitrariness. According to the Court, imposing deterrent penalties against the exercise of the right to assembly and demonstration infringes upon the essence of the right (Türkiye Barolar Birliği İnsan Hakları Merkezi 14–18). From this perspective, surveillance practices that systematically identify peaceful demonstrators without a clear and concrete legal basis raise serious constitutional concerns under Article 34 of the Constitution.

e. Criminalisation and the Destruction of the Core of the Right

Article 23 (b) of the Law No. 2911 prohibits covering the entire face or part of it and classifies it as a crime. Therefore, any material that covers the face, even masks used for medical purposes, will constitute a crime. The criminalization of covering the face and the processing of data unlawfully using FRTs when the face is uncovered renders the right to protest effectively unenforceable. That is, if the face is covered, a crime punishable by imprisonment will have been committed; if the face is uncovered, the person will be easily identified and held accountable for participating in an “unlawful” protest. This regulatory design leaves no constitutionally acceptable type of exercising the right and places individuals in a situation of unavoidable legal exposure. By structuring the exercise of the right around an automatic sanction logic, the law transforms participation in peaceful assembly into a legally hazardous act. This situation violates the prohibition on interfering with the core of the right (Gözler 210) and is, therefore, unconstitutional.

III. Proposed Legal Solutions

a. The Security Rationale Behind Surveillance

Before moving on to the solution of this legal problem, the freedom–security dilemma must be taken into account in order to understand the rationale behind the state’s increasing reliance on surveillance technologies. There are two reasons for the increasing use of camera-based surveillance: technological advancements and the emergence of a preventative policing approach (Vogiatzoglou 1–4). Türkiye's increasing security problems have contributed to the normalization of preventative security tools. Consequently, the use of digital surveillance technologies in public spaces, and especially at protests, is seen as a security requirement. While this security-oriented perspective explains the political appeal of surveillance technologies, it does not in itself resolve the constitutional requirement that any interference with fundamental rights must rest on a clear, precise, and foreseeable legal basis.

THE RIGHT TO PROTEST UNDER DIGITAL SURVEILLANCE: A CONSTITUTIONAL ANALYSIS OF TÜRKİYE

MUSTAFA EMRE DEMİR

b. Structural Reform of the Law on Meetings and Demonstrations

The solution to these problems requires a reformed approach that complies with the principle of legality. In constitutional terms, this requires a framework that is clear, accessible, and foreseeable in its effects on individuals. Primarily, the Law No. 2911 must be brought into line with Article 34 of the Constitution. The notification system should be reorganized in such a way that it does not become a permission mechanism (Kaboğlu 266). Notification should only be required to enable the state to fulfil its duty to protect (Eren 142-145).

Furthermore, the grounds for prohibiting protests should be stripped of vague language and linked to concrete criteria in line with the principle of proportionality. Proportionality also presupposes reasoned decision-making. In practice, this means the administration should be required to identify a concrete and imminent risk, consider less restrictive measures, and provide a justification capable of effective judicial review. The ban on face coverings should either be lifted or reorganized with due regard to the balance between “ends and means” and should only be applied in exceptional cases where the purpose is to conceal identity and other elements of crime are also present.



c. Regulation of Facial Recognition Technologies

The view that FRTs should be completely banned in public spaces (Gabrielli 520–21) should be evaluated in the context of Türkiye. Surveillance in protest areas is incompatible with the democratic social order not only because of the severity of the

intervention, but also because it creates a “chilling effect” that suppresses people's willingness to participate in peaceful gatherings from the outset (Venice Commission and OSCE/ODIHR 66). The chilling effect operates *ex ante*. Individuals may refrain from lawful participation because surveillance increases the perceived likelihood of identification, profiling, and later sanctions, even where no violence or disorder occurs.

Furthermore, it has been noted that this system leads to the state taking on the appearance of a “surveillance state” (Murray 147). This perception matters constitutionally because it alters the relationship between the citizen and the state. When visibility becomes a liability, the constitutional promise of participation is replaced by a logic of pre-emptive control. This concern has recently been explicitly recognised by the European Court of Human Rights. In *Glukhin v. Russia*, the Court held that the use of facial recognition technologies to identify and arrest participants in peaceful protests constituted a serious interference with Articles 8 and 10 of the Convention, emphasising its chilling effect on democratic participation. The Court underlined that deploying such highly intrusive technologies for minor administrative offences does not correspond to a pressing social need and is incompatible with a democratic society governed by the rule of law (*Glukhin v. Russia* paras. 63, 73–77).

Given the inadequacy of the legal framework in Türkiye, a complete ban on the use of FRTs in public spaces would provide the strongest guarantee for protecting the democratic function of the right to protest. At minimum, the prohibition should apply to peaceful assemblies and demonstrations as a negative protection norm. Without such a categorical boundary, safeguards risk collapsing into broad exceptions driven by security rhetoric.

Nevertheless, if the use of technology is insisted upon, a strict legal regime is essential (Gabrielli 526-529). Such a regime must be grounded in the principle of necessity. The state should demonstrate that the measure addresses a pressing social need and that less intrusive tools cannot achieve the same aim. This legal regime must clearly specify the circumstances under which the technologies may be used; it must include negative protection norms prohibiting their use in peaceful protests; and it must stipulate that their use is only possible with a court order and solely for specific and

DİJİTAL YARGILAMA SİSTEMLERİNDE GÜNCEL SORUN : DEEFAKE DELİLLERİN DÜRÜSTLÜK KURALI VE İSPAT HUKUKU BAĞLAMINDA DEĞERLENDİRİLMESİ

ŞULE KAYAOLUK

Giriş

İçinde bulunduğumuz dijital dönüşüm çağı, bilginin ve belgelerin fiziksel sınırlardan dijital mecralara taşınmasına olanak tanımış; bu durum birçok alanda olduğu gibi hukuk yargılamasında da kendini göstermiş ve "Çevrimiçi Uyuşmazlık Çözümü" (*Online Dispute Resolution - ODR*) yöntemlerinin doğmasını sağlamıştır.¹ Geleneksel alternatif uyuşmazlık çözüm yöntemleri (*Alternative Dispute Resolution-ADR*) olan müzakere, ombudsman, uzlaşma, arabuluculuk ve tahkim gibi yöntemlerin dijital platformlara entegre edilmesi, sadece bir mekan değişikliği değil; aynı zamanda hız, düşük maliyet ve usul ekonomisi ilkeleri bakımından yargılamanın verimliliğini artıran bir adımdır.² ODR, yenilikçi teknolojileri sürece bir "dördüncü taraf" olarak dahil etmekte ve "ODR platformu"³ adı verilen bu aracı mekanizmaları sürece dahil ederek uyuşmazlık çözümünde geleneksel yöntemleri teknolojiye adapte etmekte ve adalete erişimi kolaylaştırmaktadır.⁴

Günümüzde artan internet hızı, gelişmiş video konferans olanakları, çevrimiçi görüşme, belgelerin çevrimiçi paylaşımı ve bulut tabanlı veri saklama sistemleri, ODR altyapısını her geçen gün daha da ileriye taşımaktadır.⁵ Ancak teknolojinin yargılama süreçlerine sağladığı bu kitlelere erişim kolaylığı, sürdürülebilirlik ve usul ekonomisini destekleyen avantajlarının yanında daha önce karşılaşılmamış nitelikte usuli riskleri bulunmaktadır. Bu risklerin başında, Üretken Yapay Zeka (*Generative AI*) teknolojilerinin gelişmesiyle ortaya çıkan ve gerçekliğin dijital olarak manipüle edilmesine dayanan "Deepfake" içerikler gelmektedir.

¹ Ensar Lokmanoğlu ve Özlem Bora, "Dijital Dönüşüm Sürecinde Alternatif Uyuşmazlık Çözüm Yollarında Yeni Yaklaşımlar", *Business & Management Studies: An International Journal*, Cilt 12, Sayı 4 12(4), 911-927. <https://doi.org/10.15295/bmij.v12i4.2460>

² Şamil Demir, "Online Uyuşmazlık Çözümü (ODR) - Elektronik İmzalı İlam Hükümünde Anlaşmalar". *Ankara Barosu Bilişim ve Hukuk Dergisi*. 18 Ocak 2007

³ UNCITRAL ODR Teknik Notları (n 3) Bölüm V,26.

⁴ Melis Ercan, "Uyuşmazlıkların Online Çözüm Yöntemleri", Yüksek Lisans Tezi, Ankara, 2012, Cemre Çise Kadioğlu Kumtepe, Çevrimiçi Uyuşmazlık Çözümü ve Türkiye'deki Uygulamaları, On İki Levha Yayıncılık, İstanbul, 2024, s.3

⁵ Barış Mıdık, "Teknolojik Gelişmeler Işığında Hukuk Yargılamasını Yeniden Düşünmek: Otomasyondan Köklü Dönüşüme" *KOÜHFD*, 2022, Sayı: 25 / 26, s. 65

Bu çalışma, ODR yöntemlerinin sunduğu genel avantajlardan ziyade; dijitalleşen yargılama sürecinde mahkemelerde kullanılan delillerin de dijitalleşmeye başlamasıyla birlikte ortaya çıkan "Deepfake delil" sorununu merkeze almaktadır. Bu kapsamda öncelikle uyuşmazlık çözüm sistemlerinin günümüz koşullarına uyumlanmasından ve dijitalleşme ile birlikte ortaya çıkan dijital delillerden ve ardından yapay zeka aracılığıyla manipüle edilen ses, görüntü ve video kayıtlarının sonucunda ortaya çıkan *deepfake* delillerin yargılama makamlarına sunulmasının; Türk Medeni Kanunu (TMK) m. 2 ve Hukuk Muhakemeleri Kanunu (HMK) m. 29'da düzenlenen dürüstlük kuralı ile ispat hukukunun temel ilkeleri bağlamındaki etkileri incelenecektir.



Dijital Çağda İspat Hukuku ve Dijital Deliller

Hukuk kurallarının amacı hukuka uygun yollarla maddi gerçekliğe ulaşmak ve olayların aydınlatılmasını sağlamaktır. Maddi gerçekliğe ulaşma yolunda özellikle ceza yargılamasında olmak üzere en büyük ispat aracı ceza muhakemesinin yapı taşı olan delillerdir.⁶ Arapça bir kelime olan delil (kanıt, ispat vasıtası), bir şeyin varlığını, aslını, ne olduğunu ispatlamaya yarayan, yol gösteren, ipucu, iz, işaret, nişan veya alamet anlamına gelmektedir.⁷ Adalet Bakanlığı'nın Hukuk Sözlüğünde ise delil kısaca 'kanıt' olarak tanımlanmaktadır. Delillerin; hukuka uygun olarak elde edilmiş, yargılamaya konu somut olaya ilişkin, güvenilir, hayatın olağan akışına, akla, mantığa uygun (rasyonel) ve erişilebilir olması gerektiği Ceza Muhakemesi Kanunu (CMK) m. 217'de

⁶ Berkan Kurtuluş, "Dijital Deliller: Teknolojinin Deliller Üzerine Etkisi", *Hukuk ve Bilişim Dergisi*, 2022, web

⁷ Ferit Develioğlu, Osmanlıca = Türkçe Ansiklopedik Lügat, 11. Baskı, Ankara, 2013, s. 172.

DİJİTAL YARGILAMA SİSTEMLERİNDE GÜNCEL SORUN : DEEFAKE DELİLLERİN DÜRÜSTLÜK KURALI VE İSPAT HUKUKU BAĞLAMINDA DEĞERLENDİRİLMESİ

ŞULE KAYAOLUK

gerektiği Ceza Muhakemesi Kanunu (CMK) m. 217'de belirtilmektedir.⁸ Günümüzde gelişen teknolojinin sonucunda dijitalleşen yargı sistemleriyle birlikte dijital delil kavramı da ortaya çıkmıştır.

Dijital delil (elektronik delil); "Bir elektronik araç üzerinde saklanan veya bu araçlar aracılığıyla iletilen, soruşturma ve yargılama açısından hukuki değeri olan bilgi ve veriler" şeklinde tanımlanmakta, "adli bilişimle ilgili bir çalışma sırasında bilişim sistemleri ve bu kapsamdaki depolama aletleri üzerinden elde edilen adli deliller" olarak da ayrıca ifade edilmektedir.⁹ Türk Hukuk sisteminde dijital deliller CMK m. 134 ve devamı hükümlerinde düzenlenmiştir. Taşınabilen/taşınamayan bilgisayar, harddisk, flash disk, CD/DVD, hafıza kartı, akıllı telefon, kart okuyucular, dijital fotoğraf ve video kaydediciler, ses kayıt cihazları, yazıcı, faks ve fotokopi makineleri, sim kartlar dijital delillerin saklandığı alanlar olarak sayılabilir.¹⁰ Dijital mecralardan elde edilen delillerin ispat hukuku bağlamında kullanılabilmesi için akla uygunluk, gerçeklik, eksiksiz olma, inanılabilirlik, güvenilirlik, farklı kişiler tarafından incelendiğinde aynı sonuca ulaşılabilirlik gibi koşulları sağlaması gerekir.¹¹ Dijital deliller; dijital olmayan delillerin özelliklerine ek olarak belli başlı farklı özelliklere de sahiptir. Bunlar; gizli bir yapıya sahip olmaları, kopyalanabilir ve çoğaltılabilir olmaları, kolaylıkla değiştirilebilir veya yok edilebilir olmaları, uluslararası nitelikte olmaları, aidiyet tespitlerinin zor oluşu ve dinamik ve değişken yapıda olmalarıdır.¹² Dijital delillerin 'manipülasyona açık olması, değiştirilebilme kolaylığı ve sanal olmasının' hükme esas alınmasını engellemeyeceği yüksek mahkeme kararlarında vurgulanmakta ve bu noktada CMK m. 217'de düzenlenen delil serbestisine ilişkin birçok yargı kararı bulunsa da dijitalleşmenin her konuda olduğu gibi ispat hukuku bağlamında delillerin inandırıcılığı ve yargılamanın işleyişinin güvenilirliği açısından da olumsuz etkileri

bulunmaktadır.¹³ Olumsuz etkilerinden biri dijital delillerin manipüle edilmesiyle oluşan aşağıda detaylı açıklanacak olan "deepfake deliller" olarak ortaya çıkmıştır.

Deepfake Teknolojisi

Yapay zekâ kavramı ile hayatımıza birçok yeni kavram girmiş olup bu yeniliklerden biri de "deepfake" kavramıdır. İlk olarak 2017 yılında *Reddit* isimli bir sosyal medya platformunda gündeme gelmiştir.¹⁴ Deepfake teknolojisi, yapay zeka ve derin öğrenme algoritmalarını kullanarak gerçek halinden uzaklaşmış, üzerinde oynanmış ve manipüle edilmiş görüntü ve videoların oluşturulmasını sağlamaktadır. Deepfake "deep learning" (derin öğrenme) ve "fake" (sahte) kelimelerinden türetilmekte ve sahte veya manipüle edilmiş bir video, görüntü, ses kayıtlarını ifade etmektedir.¹⁵ Deepfake teknolojisinin detaylı öğrenilebilmesi açısından "yapay zekâ" (*artificial intelligence*), "makine öğrenmesi" (*machine learning*), "derin öğrenme" (*deep learning*) gibi bazı kavramların da bilinmesi önemlidir.¹⁶ Yapay zeka (*artificial intelligence*); insan zihnini model alan makinelerin; düşünme, öğrenme, karar verme gibi kompleks süreçleri yerine getirmesini mümkün kılan disiplinlerarası bilim ve teknoloji alanıdır.¹⁷ Makine öğrenimi (*machine learning*); belli kalıpları öğrenebilen ardından da öğrendiği kalıplardan doğru çıkarımlar yapabilen algoritmalarla ilgilenir. Derin öğrenme (*deep learning*); makine öğreniminin bir alt türü olmakla birlikte çok katmanlı yapay sinir ağlarının oluşturulması ile meydana gelen bir

⁸ Kurtuluş, "Dijital Deliller: Teknolojinin Deliller Üzerine Etkisi"

⁹ Gül, Ahmet. "Elektronik Delillerin Değerlendirilmesi ve Kabul ve Yargıtay Uygulamaları", Ankara, Adalet Bakanlığı Yayınları / Eğitim Dökümanları, 2021, s.3, Web

¹⁰ Gül, "Elektronik Delillerin Değerlendirilmesi ve Kabul ve Yargıtay Uygulamaları", s.3

¹¹ Ayşenur Demiral, "Dijital Delil Nedir? Ne İşe Yarar?", 2021, Web

¹² Mustafa Göksü, Hukuk Yargılamasında Elektronik Delil, Ankara, Adalet Yayınevi, 2011, s. 31-32.

GSI Team, "Hukukta Dijital Delillerin Önemi", 2025, Web

¹³ Gül, "Elektronik Delillerin Değerlendirilmesi ve Kabul ve Yargıtay Uygulamaları"

¹⁴ Fatih Arslan "Deepfake Technology: A Criminological Literature Review". *Sakarya Üniversitesi Hukuk Fakültesi Dergisi*, vol. 11, no. 1, 2023, s. 702, doi:10.56701/shd.1293642.

¹⁵ Anıl Kaymak., "Deepfake ve Yasak Cihaz veya Programlar Suçu (TCK M. 245/A)", 6. *ULUSAL ÖĞRENCİ KOLOKİYUMU Ceza Hukuku ve Bağlantılı Alanlarda Yapay Zekanın Yeri ve İşlevi*, s.32

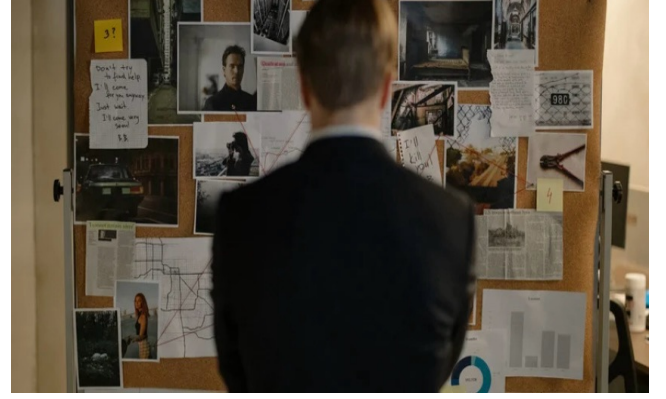
¹⁶ Nergis Belen, Nursel Yalçın, "Deepfake Teknolojisi ve Ceza Hukuku: Ses ve Görüntü Manipülasyonlarından Doğan Cezai Sorumluluk", *The Journal of International Scientific Researches*, 2025, 10(2), 203

¹⁷ Hüseyin İşcan, Ayşe Durgun Kaygısız, "Yapay Zekâ: Alt Dalları ve Uygulama Alanları", *Aksaray Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 2024, 16(4), 201-234. DOI: <https://doi.org/10.52791/aksarayıibd.1574207>

DİJİTAL YARGILAMA SİSTEMLERİNDE GÜNCEL SORUN : DEEFAKE DELİLLERİN DÜRÜSTLÜK KURALI VE İSPAT HUKUKU BAĞLAMINDA DEĞERLENDİRİLMESİ

ŞULE KAYAOLUK

öğrenme yöntemidir.¹⁸ Bu yöntem insan beynini taklit ederek büyük miktardaki verilerin daha kolay işlenebilmesini sağlar.¹⁹ Deepfake teknolojisi ile üretim yapılırken gerçek ve tüzel kişilere ait özellikle metin, ses, görüntü gibi veriler kullanılarak yüksek kaliteli ve gerçekçi ürünler oluşturulmaktadır. Gelişen deepfake teknolojisinin kullanımı hukuk, eğitim, siyaset, ticaret, eğlence gibi hayatın her alanında her geçen gün daha da yaygınlaşmaktadır.²⁰ Her teknolojik gelişmenin çift taraflı bir etkiye sahip olması gibi, deepfake teknolojisi de meşru ve olumlu amaçlara hizmet edebileceği gibi yasa dışı ve yıkıcı amaçlar için de kullanılabilir.²¹ Deepfake teknolojisinin sinema, eğitim, sanat, moda gibi alanlarda olumlu bir kullanımı varken²² özellikle siyasi propaganda, bireylerin mahremiyet haklarını ihlal etme, toplumsal cinsiyet temelli tacizleri arttırma ve sahte haberler aracılığıyla medyanın güvenilirliğine dair inancı sarsma gibi hem bireysel hem de toplumsal olumsuz sonuçları da bulunmaktadır. Deepfake teknolojisi özellikle bazı suçların işlenebilmesini kolaylaştırabilmekte, suçların işlenebilmesinde araç olarak kullanılabilmekte ve yeni suç türleri de ortaya çıkarabilmektedir.²³ Deepfake teknolojisi ile gerçekleştirilebilen bu suçlara Suç Uydurma (TCK m.271/1), Şantaj Suçu (TCK m.107/2), Kişisel Verilerin Kaydedilmesi (TCK m.135), Kişisel Verileri Hukuka Aykırı Olarak Verme, Yayma Ve Ele Geçirme (TCK m. 136), Özel Hayatın Gizliliğinin İhlali (TCK m.134/1,2) gibi suçlar örnek olarak verilebilir.²⁴



Deepfake Teknolojisinin İspat Hukuku ve Dürüstlük Kuralı Bağlamında Değerlendirilmesi

Bu teknolojinin yeni suçlar ortaya çıkarması ve bazı suçların işlenmesini kolaylaştırması gibi, suçların ispatlanmasının sağlanması bakımından da belirli olumsuz yönleri bulunmaktadır. HMK m. 27 hükmünce hukuki dinlenilme hakkının bir unsuru olarak yargılamanın taraflarına ve ilgililerine açıklama ve ispat hakkı tanınmıştır. HMK m. 189/1 hükmüne göre de davanın taraflarının Kanunda belirtilen süre ve usule uyulması koşulu ile ispat hakkına sahip oldukları düzenlenmiştir.²⁵ İspat, *bir önermenin doğruluğu hakkında kanaat verilebilmesi için bir nedenselliğin ortaya konulmasıdır*.²⁶ Yargılama hukuku bağlamında da ispat, hakim bir vakianın iddiasının gerçek olup olmadığı konusunda ikna edilmesidir.²⁷ İspat hakkı temel dayanağını, Anayasa m. 36 ve Avrupa İnsan Hakları Sözleşmesi m. 6'da düzenlenen adil yargılanma hakkından almaktadır. İspat hakkının sınırları HMK m. 189 hükmünce belirlenmiştir. Bu hüküm uyarınca hukuka aykırı olarak elde edilen deliller, vakıaların ispatında

¹⁸ Güneş Okuyucu Ergün (2023). "Machina Sapiens". *Ankara Üniversitesi Hukuk Fakültesi Dergisi*, 72 (2), s.730 <https://doi.org/10.33629/auhfd.1288894>

¹⁹ Iqbal H. Sarker, (2021). "Deep Learning: A Comprehensive Overview on Techniques, Taxonomy, Applications and Research Directions", *SN Computer Science*, 2(6), s.419

²⁰ Belen, Yalçın, "Deepfake Teknolojisi ve Ceza Hukuku: Ses ve Görüntü Manipülasyonlarından Doğan Cezai Sorumluluk", s.203

²¹ Belen, Yalçın, "Deepfake Teknolojisi ve Ceza Hukuku: Ses ve Görüntü Manipülasyonlarından Doğan Cezai Sorumluluk", s.203

²² Belen, Yalçın, "Deepfake Teknolojisi ve Ceza Hukuku: Ses ve Görüntü Manipülasyonlarından Doğan Cezai Sorumluluk", s.205

²³ Belen, Yalçın, "Deepfake Teknolojisi ve Ceza Hukuku: Ses ve Görüntü Manipülasyonlarından Doğan Cezai Sorumluluk", s.203

²⁴ Lexis Hukuk, "Yargıtay'a Göre Deepfake Teknolojisinin Cezai Boyutu", *Lexis Hukuk*, web.

²⁵ Barış Toraman, "Medeni Usul Hukukunda İspat Hakkına Dair Bazı Tespit ve Değerlendirmeler". *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi*, c. 16, Temmuz 2014, s. 1486 <https://izlik.org/JA54KW49WG>.

²⁶ Konuralp, H., İspat Kurallarının Zorlanan Sınırları, 2. Bası, Ankara: Yetkin, 2009, s. 8. Ayrıca bkz. ve karşı. Lagarde, X., *Reflexion critique sur le droit de la preuve*, Paris: L.G.D.J., 1994, no 48, s. 80, 81. Bu anlamda ispata yönelik faaliyetin, bir şeyin yahut bir kabulün gerçek veya muhtemel olduğunun gösterilmesi anlamına geldiği ifade edilebilir. Bkz. ve karşı. Mouralis, J.-L., *Preuve, 10 modes de preuve*, Rép. civ. Dalloz, 2011, no 1, s. 5; Carbonnier, J., *Droit civil, T. I*, Paris: PUF, 1962, s. 156; Planiol, M./Ripert, G., *Traité pratique de droit civil français* (2e éd.). Paris: L.G.D.J., 1954, s. 156.

²⁷ Toraman, "Medeni Usul Hukukunda İspat Hakkına Dair Bazı Tespit ve Değerlendirmeler", s.1487

DİJİTAL YARGILAMA SİSTEMLERİNDE GÜNCEL SORUN : DEEFAKE DELİLLERİN DÜRÜSTLÜK KURALI VE İSPAT HUKUKU BAĞLAMINDA DEĞERLENDİRİLMESİ

ŞULE KAYAOLUK

dikkate alınmayacak ve Kanunun belirli delillerle ispatını emredici kıldığı hususlar yalnızca o deliller ile ispat olabilecektir.²⁸ Bu hüküm hukuk muhakemeleri usulünce geçerlidir. İspat hukuku, Hukuk Muhakemeleri Usulü Kanunu'nda ve Ceza Muhakemesi Kanunu'nda birbirinden farklı olarak düzenlenmiştir. Ceza muhakemeleri kanununa göre ise delil serbestisi bulunmaktadır. Delil serbestisinden anlaşılması gereken husus; maddi gerçeği aramakta olan ceza muhakemesinde, belli hususların belli delillerle ispatının zorunlu olmadığı, ceza muhakemesinde hukuka uygun olmak koşuluyla her türlü delilin ispat unsuru olarak kullanılabileceğidir.²⁹ Ceza Muhakemesi Kanunu'nda bu husus m. 217/2 hükmünce belirtilmiştir. Dürüstlük kurallarına baktığımızda ise Türk Medeni Kanunu (TMK) m. 2 hükmünde "Herkes, haklarını kullanırken ve borçlarını yerine getirirken dürüstlük kurallarına uymak zorundadır." ifadesi belirtilmiştir.³⁰ Maddi hukukun bu temel kuralı, usul ve ispat hukuku bakımından da mutlak bir geçerliliğe sahiptir. İspat hakkı, tarafların adil yargılanma hakkının ve hukuki dinlenilme hakkının ayrılmaz bir parçası olarak anayasal koruma altında bulunsun da sınırsız bir hak değildir. İspat hakkı, dürüstlük kuralının çizdiği sınırlar dahilinde kullanılmalıdır.³¹ Dolayısıyla mahkemeyi, tarafları, yürürlükteki hukuk düzenini yanıltmaya yönelik oluşturulan dürüstlükten uzak, *deepfake* delillere dayanılması mümkün değildir. Hakkın bu şekilde *deepfake* deliller ile dürüstlük kuralına aykırı ve açıkça kötüye kullanılması halinde, söz konusu ispat faaliyeti hukuk düzeni tarafından himaye edilmeyecektir. Kanun koyucu, bu durumu TMK m.2/2'de, "Bir hakkın açıkça kötüye kullanılmasını hukuk düzeni korumaz." hükmüne yer vermek suretiyle hakkın kötüye kullanılması yasağını da maddî hukukta ayrıca ve açıkça düzenlemiştir.³²

²⁸ Toraman, "Medeni Usul Hukukunda İspat Hakkına Dair Bazı Tespit ve Değerlendirmeler", s. 1499

²⁹Doğan Gedik, "Ceza Muhakemesinde Hakim Delilleri Değerlendirme Serbestliği(CMK m.217)" *D.E.Ü. Hukuk Fakültesi Dergisi*, Prof. Dr. Durmuş TEZCAN'a Armağan, C.21, Özel S., 2019, s. 916

³⁰Ceren Demirel Mit, "Dürüst Davranma ve Doğruyu Söyleme Yükümlülüğü ile Bu Yükümlülüklere Aykırılığın Yaptırımı", *Başkent Üniversitesi Hukuk Fakültesi Dergisi*, c. 11, sy 2, Ekim 2025, ss. 342 <https://izlik.org/JA53BR93XD>.

³¹ Toraman, "Medeni Usul Hukukunda İspat Hakkına Dair Bazı Tespit ve Değerlendirmeler", s. 1499

³² Demirel Mit, "Dürüst Davranma ve Doğruyu Söyleme Yükümlülüğü ile Bu Yükümlülüklere Aykırılığın Yaptırımı", s. 342

Ayrıca HMK m. 29 hükmünde de dürüst davranma yükümlülüğü düzenlenmiştir. HMK m. 29/1'e göre dürüst davranma yükümlülüğüne uyulması tarafların iradesine bırakılmamış, bu hükme uyulmaması halinde taraflara yaptırım uygulanacağı belirtilmiştir.³³ Bu hüküm yargılamanın tüm safhalarında tarafları dürüst davranmaya zorlaması sebebiyle uyulması gereken bir yükümlülüktür.³⁴

Sonuç

Günümüzde artan dijital gelişmelerin ispat hukuku bağlamında delilleri de etkilemesi kaçınılmaz bir sonuçtur. Bu sonuç dijital delillerin değerlendirilmesi aşamasında güvenilirliğin tespitini ve teknik doğrulama denetimlerini daha önemli bir hale getirmiştir. Artık sunulan delillerin; teknolojik gelişmeler ve yapay zeka teknolojileri aracılığıyla manipüle edilmiş, üzerinde oynanmış, gerçekte olmayan bir hale getirilmiş olabileceği ispat hukuku anlamında daima göz önünde tutulmalıdır. Bu dijital gelişmeler, hukukun aradığı ölçütleri farklılaştırmamış yalnızca uygulamada daha dikkatli ve hassas olunmasını gerektirmiştir. Bir delilin varlığı için mevcut olması yetmemekte içeriğin aidiyeti, bütünlüğü, bağlamı ve üzerinde gerçeği yanıltıcı bir müdahalenin var olup olmadığı ayrıca incelenmektedir. Bu nedenle aidiyet, bütünlük, bağlam, doğrulanabilirlik ve hukuka uygun elde ediliş gibi kriterler, yapay zekâ destekli manipülasyon ihtimalinin var olduğu durumlarda daha da dikkatli değerlendirilmelidir.³⁵ Nitekim, dijital kayıtlar üzerinde değişiklik yapılabilme ihtimali nedeniyle bu tür verilerin mutlak ve kesin delil olarak kabul edilmediği; ancak diğer delillerle birlikte ispata yardımcı olabileceği yönünde yargı kararlarında da değerlendirmelere rastlanmaktadır.³⁶ Mevcut durumda, bu sorunu yeterince ele almayan ülkelerin

³³ Demirel Mit, "Dürüst Davranma ve Doğruyu Söyleme Yükümlülüğü ile Bu Yükümlülüklere Aykırılığın Yaptırımı", s. 344

³⁴ Demirel Mit, "Dürüst Davranma ve Doğruyu Söyleme Yükümlülüğü ile Bu Yükümlülüklere Aykırılığın Yaptırımı", s. 344

³⁵ Arslan, "Deepfake Technology: A Criminological Literature Review"

³⁶ Arslan, "Deepfake Technology: A Criminological Literature Review"

DIJİTAL YARGILAMA SİSTEMLERİNDE GÜNCEL SORUN : DEEFAKE DELİLLERİN DÜRÜSTLÜK KURALI VE İSPAT HUKUKU BAĞLAMINDA DEĞERLENDİRİLMESİ

SULE KAYAOLUK

hukuk sistemleri, durumdan yararlanan suçlular tarafından suistimal edilebilmektedir.³⁷

Dijital deliller, hassas yapıları gereği elde edilmesinden mahkeme önüne getirilmesine kadar geçen tüm süreçte bütünlük ve güvenilirliklerinin korunmasına ihtiyaç duyar.³⁸ Mevcut hukukumuzda elektronik veriler genel hükümlerle düzenlenmiş olsa da, yapay zekâ eliyle üretilen manipülatif içeriklerin usuli şartları henüz net olarak çizilmemiştir. Dolayısıyla yasal mevzuattaki bu boşlukların giderilmesi ve kapsamlı bir düzenleme yapılması gerekmektedir. Bu doğrultuda dijital yargılama sistemlerinin güvenilirliğini korumak ve adil yargılanma hakkını güvence altına almak adına, hukuk düzeninin hem proaktif hem de reaktif mekanizmaları bütüncül bir yaklaşımla hayata geçirmesi gerekmektedir. Bu kapsamda ilk olarak, geleneksel adli bilişim yöntemlerinin yetersiz kaldığı bu alanda "yapay zekâ destekli" çözümler üretilmelidir. Teknolojik adımların yanı sıra, usul hukukunun dinamiklerinde de köklü bir yaklaşım sergilenmeli; söz konusu verilerin hukuka uygun birer delil olarak kabul edilebilmesinde uzman bilirkişi incelemesine kritik bir rol tanınmalıdır.

KAYNAKÇA

Arslan, Fatih. "Deepfake Technology: A Criminological Literature Review". *Sakarya Üniversitesi Hukuk Fakültesi Dergisi*, cilt 11, sayı 1, 2023, s 701-20, [doi:10.56701/shd.1293642](https://doi.org/10.56701/shd.1293642).
Belen, Nergis ve Yalçın Nursel, (2025), "Deepfake Teknolojisi ve Ceza Hukuku: Ses ve Görüntü Manipülasyonlarından Doğan Cezai Sorumluluk", *The Journal of International Scientific Researches*, 10(2), 202-228.
Demir, Şamil (18 Ocak 2007). "Online Uyuşmazlık Çözümü (ODR) - Elektronik İmzalı İlam Hükümünde Anlaşmalar". *Ankara Barosu Bilişim ve Hukuk Dergisi*.
Demiral, Ayşenur, "Dijital Delil Nedir? Ne İşe Yarar?", 2021, <https://www.siberegimten.com/dijital-delil-nedir/>
Demirel Mit, Ceren. "Dürüst Davranma ve Doğruyu Söyleme Yükümlülüğü ile Bu Yükümlülüklere Aykırılığın Yaptırımı" . *Başkent Üniversitesi Hukuk Fakültesi Dergisi*, c. 11, sy 2, Ekim 2025, ss. 337-80, <https://izlik.org/IA53BR93XD>.
Develioğlu, Ferit, Osmanlıca = Türkçe Ansiklopedik Lügat, 11. Baskı, Ankara, 2013, s 172
Ercan, Melis. "Uyuşmazlıkların Online Çözüm Yöntemleri", Yüksek Lisans Tezi, Ankara, 2012

³⁷ Arslan, "Deepfake Technology: A Criminological Literature Review"

³⁸ Şenel Sarsıkoğlu, "Ceza Muhakemesinde Delil ve İspat Hukuku Açısından Elektronik Delil (E-Delil) Kavramı", *Türkiye Adalet Akademisi Dergisi*, Temmuz 2015, Sayı 22, s. 448

Ergün, G. O. (2023). "Machina Sapiens", *Ankara Üniversitesi Hukuk Fakültesi Dergisi*, 72 (2), s.717-758.
Gedik, Doğan, "Ceza Muhakemesinde Hakimin Delilleri Değerlendirme Serbestliği (CMK m.217)", *D.E.Ü. Hukuk Fakültesi Dergisi*, Prof. Dr. Durmuş TEZCAN'a Armağan, C.21, Özel S., 2019, s. 913-963
Göksü, Mustafa, "Hukuk Yargılamasında Elektronik Delil", Ankara: Adalet Yayınevi, 2011, s. 31-32.
GSI Team, Hukukta Dijital Delillerin Önemi, 2025, Web <https://www.goksusafisik.av.tr/tr/publications/2025-winter-iss-ue/hukukta-dijital-delillerin-onemi?id=1>
Gül, Ahmet. "Elektronik Delillerin Değerlendirilmesi ve Kabul ve Yargıtay Uygulamaları", Ankara, Adalet Bakanlığı Yayınları / Eğitim Dokümanları, 2021, <https://ravp.adalet.gov.tr/resimler/552/dosya/elektronik-delillerin-degerlendirilmesi-yargitay-uygulamaları-ahmet-gul28-06-202113-48.pdf>
İşcan, H. ve Dursun Kaygısız A. (2024), "Yapay Zekâ: Alt Dalları ve Uygulama Alanları", *Aksaray Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 16(4), 201-234. DOI: <https://doi.org/10.52791/aksaraviibd.1574207>
Kadioğlu Kumtepe, Cemre Çise, Çevrimiçi Uyuşmazlık Çözümü ve Türkiye'deki Uygulamaları, On İki Levha Yayıncılık, İstanbul, 2024, s.3
Kandır, Murat Osman, "Deep Fake, Yapay Zeka ve Sahte Deliller", *Hukuk ve Bilişim Dergisi* <https://hukukvebilisim.org/deep-fake-yapay-zeka-ve-sahte-deliller/>
Kaymak, Anıl. "Deepfake ve Yasak Cihaz veya Programlar Suçu (TCK M. 245/A)", 6. *ULUSAL ÖĞRENCİ KOLOKYUMU Ceza Hukuku ve Bağlantılı Alanlarda Yapay Zekanın Yeri ve İşlevi*, s.32
Konuralp, H., İspat Kurallarının Zorlanan Sınırları, 2. Bası, Ankara: Yetkin, 2009, s. 8.
Kurtuluş, Berkan. "Dijital Deliller: Teknolojinin Deliller Üzerine Etkisi", *Hukuk ve Bilişim Dergisi*, 2022, <https://hukukvebilisim.org/dijital-deliller-teknolojinin-deliller-uzerinde-etkisi/#ftn8>
Lexis Hukuk, "Yargıtay'a Göre Deepfake Teknolojisinin Cezai Boyutu", Lexis Hukuk, web <https://www.lexishukuk.com/category/blog/yargitay-a-goere-deepfake-teknolojisinin-cezai-boyutu/#deepfake>
Lokmanoğlu, Ensar ve Bora, Özlem. "Dijital Dönüşüm Sürecinde Alternatif Uyuşmazlık Çözüm Yollarında Yeni Yaklaşımlar", *Business & Management Studies: An International Journal*, Cilt 12, Sayı 4, 12(4), 911-927. <https://doi.org/10.15295/bmij.v12i4.2460>
Mıdık, Barış. "Teknolojik Gelişmeler Işığında Hukuk Yargılamasını Yeniden Düşünmek: Otomasyondan Köklü Dönüşüme" *KOÜHFD*, 2022, Sayı 25 / 26, s. 65
Sarker, I. H. (2021). "Deep Learning: A Comprehensive Overview on Techniques, Taxonomy, Applications and Research Directions", *SN Computer Science*, 2(6), 420
Sarsıkoğlu, Şenel, "Ceza Muhakemesinde Delil ve İspat Hukuku Açısından Elektronik Delil (E-Delil) Kavramı", *Türkiye Adalet Akademisi Dergisi*, Temmuz 2015, Sayı 22, ss. 427-454
Toraman, Barış. "Medeni Usul Hukukunda İspat Hakkına Dair Bazı Tespit ve Değerlendirmeler", *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi*, c. 16, Temmuz 2014, <https://izlik.org/IA54KW49WG>.
UNCITRAL ODR Teknik Notları (n 3) Bölüm V,26.

Giriş

Yapay zeka, günümüzde insan yaşamı için birçok alanda büyük devrimler yaratmakta ve hayatımızın artık her alanında bizlerle birlikte olan bir teknoloji haline gelmektedir. Birçok devlet teknoloji alanında gelişmeleri takip etmekte ve yapay zekanın önemini farkında olup bir yarış haline girmekte ve bu da teknolojinin ilerlemesini hızlandırmaktadır. Hızla gelişen teknoloji ve yapay zeka aynı zamanda birçok güvenlik problemini de beraberinde getirmektedir. Ortaya çıkan güvenlik problemlerini önlemek için devletler çeşitli düzenlemeler yapmaktadır. Ülkelerin kendi düzenlemelerinin yanında ilk kapsamlı düzenleme; Avrupa Birliği tarafından yürürlüğe girmiştir.

Yapay Zeka Kavramının Tanımı ve Tarihçesi

Yapay zeka günümüzde her alanda kullanılan ve geçmişten günümüze kadar da hızla kendini geliştiren bir teknolojidir. Yapay zekanın uluslararası tanımı veya doktrinde herhangi bir ortak kabul edilmiş tanımı yoktur. Bununla birlikte, yapay zeka için farklı tanımlamalar bulunmaktadır. Yapay zeka, Türk Dil Kurumu tarafından “Bir bilgisayarın, bilgisayar kontrolündeki bir robotun veya programlanabilir bir aygıtın insana benzer biçimde algılama, öğrenme, fikir yürütme, karar verme, sorun çözme, iletişim kurma vb. işlevleri sergileyebilme yeteneği” şeklinde tanımlanır. (TDK Yapay Zeka) Avrupa Birliği Parlamentosu tarafından ise yapay zekâ, “makinelerin akıl yürütme, öğrenme, planlama ve yaratıcılık gibi insanlara benzer davranışlar sergileme kabiliyeti” olarak tanımlanır. (Akbulut, Akbulut 467) Avrupa Komisyonu, 21 Nisan 2021’de Yapay Zekâ Üzerine Taslak Yasa (bir düzenleyici çerçeve) Önerisini yayımlamış ve 3. maddesinde yapay zekâ sistemi “EK I’de belirtilen teknik ve yaklaşımlardan bir veya birden fazlasıyla geliştirilmiş ve insan tarafından tanımlanan belirli amaçlar için, içerik, tahmin, öneri şeklinde çıktılar veya insanların etkileşimde bulundukları ortamları etkileyen kararları üretebilen yazılım” olarak tanımlamıştır. (Akbulut, Akbulut 468). Yapay zeka için makinelerin insan gibi akıl yürütme ve algısal yeteneklerine sahip, gelişmiş bilgisayar biliminin bir dalı olarak karşımıza çıktığı düşünülebilir. Yapay zekanın fikir olarak ortaya atılması günümüzden eskilere dayanmaktadır. Tarihte bilgisayarların temelini 1950’lerin başında John Von Neumann ve Alan Turing tarafından atılmış olduğu bilinmektedir. Daha sonrasında Alan Turing, Mind dergisinde yayımladığı “Makinelerin İşleyişi ve

Zeka” isimli makalesiyle daha o zaman var olmayan bir fikri ortaya atmış, makinelerin düşünüp düşünemeyeceğini tartışmış ve yapay zekanın temellerini bu makale ile atmıştır (Eriş 16).



Yapay Zeka için Atılan Hukuki Adımlar

Yapay zeka, her geçen gün gelişmesiyle ve sosyal hayatın bir parçası olmasıyla birlikte birçok problemi de beraberinde getirmektedir. Yapay zeka ve insanların menfaatleri doğrultusunda sosyal hayatı düzenleyen hukuk kurallarının yapay zekanın ortaya çıkardığı problemleri çözmek adına temel hukuk sorunlarının üzerinde durulmasını gerektirmiştir. (Kılıçarslan 368) Akla gelen sorunlardan bir tanesi de yapay zeka dolayısıyla ortaya çıkan hukuki ihlallerden kimin sorumlu olacağı yani yapay zekanın kişilik problemidir. Yapay zeka dolayısıyla ortaya çıkan problemlerden kimin sorumlu olacağı, yapay zekaya kişilik verilir verilmeyeceği tartışılmaktadır. 27 Ocak 2017’de bu tartışmalara bir cevap olarak Avrupa Parlamentosu Hukuk İşleri Komisyonu tarafından hazırlanan tavsiye niteliğindeki “Robotikler Hakkında Medeni Hukuk Kuralları Tavsiye Raporu”nda yapay zekaya kişilik statüsü atfedilmiştir. Bu raporda, otonom olarak kendi kararını alabilen yapay zekalı robotların kendi yarattıkları problemlerden sorumlu olabilmesi için Elektronik Kişilik görüşü ortaya atılmıştır. Elektronik Kişilik görüşü, mevcut hukuk sistemlerinde yer alan hukuki statülerden biri olmayıp, bu alanda tamamen yeni bir statü yaratılması gerektiğini belirtmektedir. (Darama) Bu rapor yapay zekaya kişilik verilmesini öneren ilk resmi belgedir.

AB’nin 2018 tarihli Genel Veri Koruma Yönetmeliği (GDPR), 4 Mayıs 2016’da Avrupa Birliği Resmi Gazetesi’nde yayımlanmış ve 25 Mayıs 2018’de uygulanmaya başlanmıştır. Yönetmelik, tüm Avrupa Birliği ve Avrupa Ekonomik Alanında yaşayanlar için veri koruma ve veri gizliliğine dayanan bir düzenlemedir. “Kişisel verileri işlenen kişilerin haklarını, veri işleme faaliyetinde bulunanların yükümlülüklerini, kurallara uyum sağlama

yöntemlerini ve kurallara uymayanlar hakkında uygulanacak yaptırımları öngörür. Söz konusu düzenleme veri gizliliği ve güvenliği konusunda uluslararası aktörleri ve üçüncü ülkeleri de etkileyen bir düzenlemedir.”(Avrupa Birliği Başkanlığı).

AB Komisyonu 2018’in mart ayında yapay zekâ alanındaki tartışmalara çözüm üretmek adına çalışmalara başlamıştır. Söz konusu çalışmalara başlamak adına çeşitli mesleklerdeki üyelerden oluşan bir grup kurulmuştur. 10 Nisan 2018’de Birlik üyesi devletler, yapay zekâ alanında iş birliği yapacaklarını beyan eden bir bildirgeyi imzalamışlardır. Bu adımla birlikte, yapay zekânın araştırılması ve kullanımından doğabilecek sosyal, ekonomik, etik ve hukuki nitelikteki sorunlarda ortak hareket etme iradelerini ortaya koymuşlardır. Ardından, Aralık 2018’de Avrupa Komisyonu da benzer şekilde bu yöndeki çalışmalarını sürdüreceğini duyurmuştur. Aynı dönemde Birlik tarafından Güvenilir Yapay Zekâ İçin Etik Yönergelerinin taslağı hazırlanmış ve 2019 nisan ayında Güvenilir Yapay Zekâ İçin Etik Kuralları kabul etmiştir. (Benzer 193-194)

Avrupa Komisyonu, 21 Nisan 2021 tarihinde yapay zekâyâ ilişkin kapsamlı bir düzenleme hazırlanmasına yönelik önerisini sunarak yasama sürecini resmen başlatmıştır. Bunu takiben, Avrupa Parlamentosu, Avrupa Konseyi ve Avrupa Komisyonu arasındaki görüşmeler sonucu 9 Aralık 2023 tarihinde Parlamento ile Konsey arasında geçici bir uzlaşıya varılmıştır. Yasama sürecine ilişkin gerekli onayların tamamlanmasının ardından, düzeltilmiş son metin 19 Nisan 2024 tarihinde yayımlanmıştır. Nihayetinde, 21 Mayıs 2024 tarihinde Avrupa Konseyi tarafından kabul edilen Yapay Zekâ Yasası, 12 Temmuz 2024 tarihinde Avrupa Birliği Resmî Gazetesi’nde yayımlanmış, (Dönmez 961) 1 Ağustos 2024 tarihinde yürürlüğe girmiştir. Düzenlenen hükümlerin 2030’a kadar aşamalı bir şekilde yürürlüğe girmesi planlanmıştır. Yasa, 2 Ağustos 2026 tarihi itibarıyla tüm hükümleriyle birlikte uygulanabilir olacaktır. (Avrupa Birliği Yapay Zekâ Yasası Yürürlükte) Kabul edilemez riskli yapay zeka sistemleri ile ilgili yasaklar 2 Şubat 2025 tarihine kadar; Yapay Zeka Yasası Ek III’te listelenen tüm yüksek riskli yapay zeka sistemleri ise 2 Ağustos 2026’ya kadar yürürlüğe girecektir. (Avrupa Birliği Yapay Zekâ Yasası’nın Türkiye’deki Aktörlere Yansımaları)



Yapay Zeka Yasası

Yapay Zekâ Yasası, yapay zekâ alanında dünya çapında hazırlanan ilk kapsamlı yasal düzenleme olması bakımından büyük önem taşımaktadır. Yasanın temel amacı yapay zekâ teknolojilerinin insan onuru, temel haklar ve toplumsal güven ile uyumlu bir şekilde geliştirilebilmesi ve uygulanabilmesi için gerekli çerçeveyi oluşturmaktır (Yolcu, Gülbahar 26). Yasanın dayandığı temel ilkeler; genel geçer bir düzenleme aracılığıyla iç pazarın işleyişinin geliştirilmesi, Avrupa Birliği değerlerine uygun olarak insan merkezli ve güvenilir yapay zekânın teşvik edilmesi, sağlık, güvenlik ve temel hakların korunması, yapay zekâ tabanlı mal ve hizmetlerin sınır ötesi serbest dolaşımının güvence altına alınması ve ayrıca yasada açıkça belirtilen yasaklı durumlar dışında yapay zekâ sistemlerinin geliştirilmesi, pazarlanması ve kullanımına gereksiz kısıtlamalar getirilmesinin önlenmesi olarak özetlenebilir.(Dönmez 971) Düzenlemenin hukuki dayanağını, Avrupa Birliği’ne iç pazarın işleyişini sağlamak üzere üye devletler arasında hukuk birliği tesis etme yetkisi veren hüküm oluşturmaktadır. Bu nedenle tüzük, tüm üye ülkelerde doğrudan uygulanabilir niteliktedir (Dönmez 961).Yasanın amaçlarından biri, ChatGPT gibi büyük dil modellerinin denetimden kaçmasını engellemek olduğundan yasaya “genel amaçlı yapay zekâ modeli” kavramı eklenmiştir (Dönmez 962). Genel amaçlı yapay zekâ modeli, öz denetim yöntemleriyle büyük veri setleri kullanılarak eğitilmiş olsa bile, kapsamlı bir genel kullanılabilirliğe sahip; piyasaya sunulmuş biçiminden bağımsız olarak çok sayıda farklı görevi yerine getirebilen ve çeşitli alt sistemler ile uygulamalara entegre edilebilen yapay zekâ modeli olarak tanımlanmaktadır (Yapay Zekâ Yasası m. 3) (Akbulut 469). Yapay Zekâ Yasası hem teknolojinin sunduğu fırsatlara hem de ortaya çıkardığı risklere karşılık verecek şekilde tasarlanmıştır. Bu

doğrultuda, uygulama alanı bakımından başlangıçta yapay zekâ sistemi veya yapay zekâ modeli sağlayıcıları, üreticileri, ithalatçıları, distribütörleri ve dağıtıcılarını kapsamına almaktadır (YZ Tüzüğü, m. 2/1/(a)-(g)) (Dönmez 971). Yasa, kural olarak Avrupa Birliği sınırları içerisinde gerçekleşen hak ihlallerine uygulansa da, sağlayıcıların veya dağıtıcıların Birlik içinde ya da üçüncü bir ülkede yerleşik olup olmaması uygulama alanı bakımından bir farklılık yaratmamakta, uluslararası düzeyde tüm sağlayıcılar ve dağıtıcıları da tabii tutmaktadır. Dolayısıyla, Birlik pazarına sunulan yapay zekâ sistemleri ile genel amaçlı yapay zekâ modelleri, sağlayıcı ya da dağıtıcının yerleşim yerine bakılmaksızın Tüzük hükümlerine tabi kılınacaktır. Bu şekilde yasa koyucu sınır ötesi bir yaklaşım benimsemiştir. (Turan Başara 2997) Yasa, ayrıca risk temelli bir düzenleme tekniğini benimsemiştir. Bu çerçevede bazı yapay zekâ sistemlerinin kullanımı tamamen yasaklanmış; yüksek riskli yapay zekâ sistemleri ile genel amaçlı yapay zekâ modellerinin kullanımı ise belirli koşullara bağlanmıştır. Yapay Zekâ Yasası'nın 5. maddesinde yasaklanmış uygulamalara yer verilmektedir. Yasaklanan uygulamaların başında, bireyleri manipüle ederek bilinçli karar verme yetilerini önemli ölçüde bozabilecek ve bilinçaltı teknikler kullanarak kişilerin kendilerine veya başkalarına zarar vermesine yol açabilecek yapay zekâ sistemleri gelmektedir. Bu tür uygulamaların piyasaya sürülmesi, hizmete sunulması ve kullanılması yasaktır (Dönmez 967). Ayrıca öngörülen yükümlülüklerle aykırı davranılması halinde, ihlali gerçekleştiren şirketler için idari para cezaları düzenlenmiştir. Şubat 2024'te Avrupa Komisyonu çatısı altında kurulan Avrupa Yapay Zekâ Ofisi, yasanın uygulanmasında görevli otoritedir. (Yolcu, Gülbahar 26)

SONUÇ

Yapay zeka teknolojisi sunduğu fırsat ve kolaylıkların yanında ciddi hukuki ve etik sorunları da beraberinde getirmektedir. Avrupa Birliği tarafından kabul edilen Yapay Zekâ Yasası, risk esaslı yaklaşımı ve sınır ötesi etkisiyle bu alandaki ilk kapsamlı düzenleme olarak öne çıkmaktadır. İnsan onuru, temel haklar ve toplumsal güvenin korunmasını esas alan bu yasa, yalnızca Avrupa Birliği'nde değil, küresel ölçekte de yapay zekâya ilişkin hukuki çerçevenin şekillenmesinde öncü rol oynayan bir düzenleme niteliğinde olup, gelecekte diğer ülkelerin düzenlemelerine de yön verecektir. Türkiye bakımından ise bu gelişmelerin dikkatle takip

edilmesi, hem hukuki uyum süreci hem de teknoloji politikalarının geleceği açısından stratejik bir gereklilik olarak ortaya çıkmaktadır.

KAYNAKÇA

Türk Dil Kurumu. "Yapay Zeka". 2022, [https://sozluk.gov.tr/?ara=yapay zeka](https://sozluk.gov.tr/?ara=yapay%20zeka). Erişim tarihi: 6.09.2025.

Akbulut, Berrin ve Akbulut, Mete Tuluhan, "Yapay Zekâ Yasasında Risk Kategorileri" Necmettin Erbakan Üniversitesi Hukuk Fakültesi Dergisi, sayı:1, 2025

Eriş M.H. "Yapay Zeka ve Tarihsel Gelişimi." *"Yapay Zeka Çağında Hukuk"*. İstanbul, Ankara ve İzmir Baroları Çalıştay Raporu, 2019.

Kara Kılıçarslan, Seda, "Yapay Zekanın Hukuki Statüsü Ve Hukuki Kişiliği Üzerine Tartışmalar" Yıldırım Beyazıt Hukuk Dergisi, sayı:2, 2019.

Darama, Serdar, "Yapay Zekanın Hukuki Statüsü Hakkındaki Görüşler Üzerine Değerlendirme", Özgün law, Erişim tarihi:06.09.2025

Avrupa Birliği Başkanlığı, 2023, https://www.ab.gov.tr/ab-genel-veri-koruma-tuzugu-gdpr-turkceye-cevrildi_53650.html Erişim tarihi: 06.09.2025

Benzer, Ekrem, "Yapay Zekanın Hukuki Statüsü ve Hukuki Kişiliği Üzerine Tartışmalar", Bilişim Hukuku Dergisi, sayı:1, 2025.

Dönmez, Zeynep, "Yapay Zekânın Hukuki Gelişimi ve AB Yapay Zekâ Yasası" Adalet Dergisi, sayı:74, 2025.

Özden, Sevgi Ünsal ve Çakmak Ergene, Gülnur "Avrupa Birliği Yapay Zekâ Yasası Yürürlükte" <https://www.erdem-erdem.av.tr/uploads/file/erdemerdem-avrupa-birligi-yapay-zeka-yasasi-yururlukte.pdf> Erişim tarihi: 06.09.2025.

Özden, Sevgi Ünsal "Avrupa Birliği Yapay Zekâ Yasası'nın Türkiye'deki Aktörlere Yansımaları" <https://www.erdem-erdem.av.tr/bilgi-bankasi/avrupa-birligi-yapay-zeka-yasasinin-turkiyedeki-aktorelere-yansimalari> Erişim tarihi: 06.09.2025.

Yolcu, Tuğba ve Gülbahar, Yasemin. "Avrupa Birliği Yapay Zekâ Yasası: 2018-2024 Avrupa Komisyonu Tekliflerinde Demokrasinin Yeri" Ankara Avrupa Çalışmaları Dergisi, sayı:1,2025.

Turan Başara, Gamze, "Avrupa Dijital Düzenleme Sisteminde Yapay Zeka Yasası" Ankara Üniversitesi Hukuk Fakültesi Dergisi, sayı:4, 2025.

Giriş

Fikri mülkiyet hukuku, matbaanın icadından bu yana teknolojiyle girdiği "yakalamaca" oyununda bugün, en zorlu dönemlerinden birini yaşamaktadır. Düne kadar fiziksel birer nesne olarak korunan eserler, dijital devrimle birlikte algoritmaların işlediği soyut verilere dönüşmüştür. Ancak Üretken Yapay Zeka (*Generative AI*) dönemi, hukuku sadece yeni bir telif kriziyle değil, yaratıcılığın insan tekelinden çıkması ile sonuçlanan büyük bir belirsizlikle baş başa bırakmıştır. Milyonlarca sanatçının emeğinin, herhangi bir izin alınmadan veya bedel ödenmeden devasa veri setlerine hammadde yapılması, bugün telif hukukunun en kritik emniyet subabı olan "Adil Kullanım (*Fair Use*)" doktrinini tartışmaların tam merkezine yerleştirmiştir.¹

Adil kullanım doktrini, mülkiyet haklarının korunması ile toplumsal ilerlemenin sağlanması arasındaki o kritik denge noktasını temsil etmektedir. Ancak bu doktrin, teknoloji şirketleri için sınırsız bir hukuki bağışıklık alanı sağlamamaktadır. Günümüzdeki temel tartışma, yapay zekanın veriyi sadece bir insan gibi "okuyup öğrendiği" mi, yoksa bu veriyi sistemin ticari değerini oluşturan temel bir yapı taşı olarak "tükettiği" mi noktasında kilitlenmektedir. Bu makale; adil kullanımın Anglo-Sakson ve Kıta Avrupası sistemlerindeki felsefi farklılıklarını, eser sahibinin haklarının yapay zeka karşısında nasıl kırılanaştığını ve güncel mahkeme kararları ışığında dönüştürücülük kavramını incelemektedir.



I. Fikri Mülkiyet Hukukunda Sistem Ayrımı

Adil kullanım doktrininin yapay zeka gibi karmaşık bir teknolojiye nasıl cevap verdiğini anlamak için, öncelikle bu doktrinin filizlendiği sistemlerin felsefi arka planına bakmamız gerekmektedir. Nitekim sistemler arasındaki bu felsefi fark, bir istisnanın ne kadar 'esnek' olabileceğini de doğrudan belirlemektedir. Adil kullanıma ilişkin olarak bugün dünyada temelde iki farklı hukuk sistemi bulunmakta ve bu sistemler aslında aynı kavrama oldukça farklı perspektiflerden yaklaşmaktadır. Bu felsefi ayrışmanın pratik yansımalarını daha iyi kavrayabilmek adına, doktrinin asıl şekillendiği yer olan Anglo-Sakson sisteminden başlamak konuyu temellendirmek açısından yerinde olacaktır. Anglo-Sakson sisteminin en büyük temsilcilerinden olan Amerika Birleşik Devletleri'nde hukukun temelini oluşturan bu gelenek, telif haklarını mülkiyetçi bir haktan ziyade toplumsal ilerlemeyi odağa alan faydacı (*utilitarian*) bir bakış açısıyla ele almaktadır. ABD Anayasası'ndaki ilgili maddeye baktığımızda amacın sadece yazarı zengin etmek değil, yaratıcılığı teşvik ederek toplumun bilgi hazinesini büyütmek olduğu görülmektedir.² Bu ekonomik odaklı yaklaşım, mahkemelere katı kurallar yerine her olayın kendi şartlarına göre değerlendirildiği dinamik bir alan tanımaktadır. Bu yüzden adil kullanım (*fair use*), bu sistemde sonradan eklenmiş bir istisna değil; sistemin meşruiyetini sağlayan en temel denge mekanizmalarından biri olmaktadır. Yapay zeka şirketlerinin teknolojik ilerleme ve kamu yararı argümanlarını ABD mahkemelerinde bu kadar rahat savunabilmelerinin sebebi de sistemin bu esnek yapıya sahip olmasından kaynaklanmaktadır.³ Öte yandan Türkiye'nin de dahil olduğu Kıta Avrupası geleneği ise olaya çok daha farklı bir yerden yaklaşmaktadır. Bu sistemde eser, sadece satılan bir mal değil; sanatçının kişiliğinin ve ruhunun bir yansımasıdır. Bu sistemde haklar, sadece para kazanmakla ilgili değildir; sanatçının onurunu ve eserle arasındaki manevi bağı da korumaktadır. Bu yapısal fark nedeniyle, Kıta Avrupası sistemlerinde istisnalar genel bir ilke değil, yasada sınırlı sayıda sayılan özel durumlardır.

¹ Ateş, Mustafa "Fikir ve Sanat Mahsullerinin Yapay Zekânın Eğitiminde Kullanılmasının Telif Hakları Bağlamında Değerlendirilmesi", *Ticaret ve Fikri Mülkiyet Hukuku Dergisi (TFM)*, Cilt 11, Sayı 2, 2025, s. 242.

² US Constitution, Art. I, Sec. 8, Cl. 8: "To promote the Progress of Science and useful Arts..."

³ Authors Guild, Inc. v. Google, Inc., 804 F.3d 202 (2d Cir. 2015)

Yapay zeka eğitimindeki kitlesel veri kullanımının bu sistemlerde "adil" kabul edilmesi, Anglo-Sakson geleneğine göre çok daha zordur çünkü istisnaların her zaman "dar yorumlanması" gerekir; bu da teknoloji şirketlerinin savunma alanını ciddi şekilde kısıtlamaktadır.⁴

II. Eser Sahipliği

Doktriner anlamda eser sahipliği, yaratma fiiline bağlanan bir statüdür; bu statü eserin vücut bulmasıyla kendiliğinden doğar.⁵ Ancak üretken yapay zekanın teknolojik kapasitesi, bu geleneksel mülkiyet kurgusunu daha önce tecrübe edilmemiş bir sınama ile karşı karşıya bırakmıştır. Güncel hukuki uyuşmazlıkların odak noktasını; sistemin veri işleme sürecinin teknik bir faydalanma faaliyeti mi olduğu yoksa doğrudan mülkiyet haklarına bir müdahale mi teşkil ettiği sorusu oluşturmaktadır. Bu minvalde, adil kullanım (*fair use*) denetiminin teknik safhalarına geçilmeden önce, söz konusu sürecin mali ve manevi haklar üzerindeki izdüşümlerini belirlemek; dijital çoğaltmadan üslup taklidine kadar uzanan hak iddialarını hukuki nitelikleri bakımından tasnif etmek önem arz etmektedir.

Mali hak, en basit tanımıyla eser sahibinin eserini ekonomik olarak kontrol etme yetkisidir. İşleme, çoğaltma ve yayma gibi haklar bu grubun temel taşlarıdır. Yapay zeka modelleri eğitilirken milyonlarca eserin dijitalleştirilip veri tabanlarına kaydedilmesi, aslında teknik olarak doğrudan bir "çoğaltma" işlemidir. Teknoloji dünyası bu çoğaltma işleminin aslında tam manasıyla bir çoğaltma değil ara kopyalama (*intermediate copying*) olduğunu savunmaktadır. Bazı hukukçular, bu kopyalamanın sadece sistemin içinde kaldığını ve son kullanıcıya bir "kopya" olarak sunulmadığı sürece ihlal sayılmaması gerektiğini savunmaktadır.⁶ Bu noktada, milyonlarca eserin izinsiz şekilde bir sistemin hammaddesi haline getirilmesi, eser sahibinin o eser üzerindeki ekonomik kontrolünü fiilen bitirir mi sorusu ortaya

çıkılmaktadır. Yapay zeka geliştiricileri tarafından önerilen pasif öğrenme argümanı; söz konusu telifli verilerin, aslında sistemin iktisadi değerini ve teknik kapasitesini belirleyen kurucu unsurlar olduğu gerçeğiyle temelden bir zıtlık oluşturmaktadır.

Manevi haklar ise sanatçının eseriyle olan o kişisel ve manevi bağı ifade etmektedir. Yapay zekanın belki de en çok tartışılan yönü, bir sanatçının kendine has üslubunu analiz edip saniyeler içinde o üslupta yeni içerikler üretmesidir. Telif hukuku klasik olarak "üslubu" korumamakta; sadece o üslubun somutlaşmış halini (ifadesini) korumaktadır. Ancak, yapay zekanın bir sanatçının yıllarını vererek oluşturduğu stili matematiksel bir olasılığa indirgemesi ve piyasayı bu yapay taklitlerle doldurması, olayı sadece bir mülkiyet meselesinden çıkarıp bir itibar meselesine dönüştürmektedir. Literatürde artık "üslup gaspı" olarak adlandırılan bu durum, haksız rekabet ile fikri mülkiyet arasındaki o ince çizgiyi iyice bulanıklaştırmaktadır. Sanatçının adının geçmemesi ya da eserinin bir algoritma tarafından deforme edilmesi, manevi hak ihlallerinin belki de bugün karşılaştığımız en yeni ve en zorlu biçimini oluşturmaya başlamaktadır.

III. ABD Hukukunda Adil Kullanım: Dört Faktör Testi

Amerikan Telif Hakkı Kanunu'nun 107. maddesinde bahsedilen adil kullanım ilkesi soyut yapısı dolayısıyla olay bazında değerlendirilmekte olup dünya genelinde geçerli tek bir kriteri bulunmamaktadır. Öte yandan bu kavramın yaygın olarak kullanıldığı Amerikan hukukunda telif hakkı kanunun 107. maddesinde dört adet kriter belirtilmektedir. Ancak bu kriterler değerlendirilirken mahkemelerin bu kriterleri sadece bir kontrol listesi olarak görmediği aksine her dava özelinde kriterleri ayrı ayrı değerlendirdikleri gözden kaçmamalıdır. Bu bakımdan mahkemeler tarafından yapılması beklenen analizin ilk ve en kritik basamağı dönüştürücülük olup, kullanımın "dönüştürücü" (*transformativeness*) olup olmadığı incelenmektedir. Amerikan telif hukuku pratiğinde adil kullanım doktrininin modern mimarlarından biri kabul edilen federal yargıç Pierre Leval'in teorisine göre; eğer yeni kullanım orijinal esere bambaşka bir anlam, yeni bir amaç veya farklı bir estetik mesaj katıyorsa, adil kullanım savunması güçlenmektedir.⁷

⁴ Doğan, Esmâ Muheyne "Üretken Yapay Zeka Modellerinin Eğitimde Kullanılan İçeriklerin Telif Hakkı İhlali: ABD'deki Güncel Davalar Işığında Karşılaştırmalı Bir İnceleme", *TFM*, Cilt 11, Sayı 1, 2025, s. 92.v

⁵ Tekinalp, Ünal, Fikri Mülkiyet Hukuku, 5. Baskı, Vedat Kitapçılık, İstanbul, 2012, s. 115

⁶ Mustafa Ateş, "Fikir ve Sanat Mahsullerinin Yapay Zekânın Eğitimde Kullanılmasının Telif Hakları Bağlamında Değerlendirilmesi", *Ticaret ve Fikri Mülkiyet Hukuku Dergisi (TFM)*, Cilt 11, Sayı 2, 2025, s. 241-272.

Yapay zeka şirketleri burada şu şekilde bir savunma yapmaktadır: Yapay zekanın verilerinin kullanımının aslında bir gayri ifade edici kullanım olduğunu yani bir insan gibi değil de sadece veriler arasındaki istatistiksel desenleri çözmek için kullandığını iddia etmektedir. Ancak 2023 tarihli *Warhol v. Goldsmith* kararında ABD Yüksek Mahkemesi dönüştürücülüğün sadece estetik bir fark yaratmak olmadığını; asıl bakılması gerekenin, kullanım amacının ne kadar farklılaştığı ve orijinal eserin pazarını ne kadar tehdit ettiği olduğunu vurguladı. Adil kullanıma ilişkin ikinci faktör ise eserin yaratıcılığı olup yaratıcılık şu şekilde açıklanmaktadır: Bir ressamın tablosu gibi yaratıcı eserler, teknik bir kılavuza göre hukuk tarafından çok daha sıkı korunmaktadır. Yapay zeka modelleri eğitilirken ayırt edilmeksizin her türlü sanat eserinin sisteme dahil edilmesi, bu faktörün eser sahipleri lehine ağır basmasına neden olmaktadır. Sanatçıların emeğinin yalnızca "istatistiksel ham madde" gibi görülmesi, telif hukukunun temel varlık sebebi olan yaratıcılığı koruma ilkesiyle ciddi bir çelişki yaratmaktadır. Adil kullanıma ilişkin üçüncü kriter ise eserin ne kadarının kopyalandığının ölçülmesidir. Yapay zeka eğitiminde eserin bütünüyle kopyalanması teknik bir zorunluluk gibi sunulmaktadır. Bunun yanında teknoloji devleri, bu kopyaların nihai kullanıcıya gösterilmediğini, sadece sistemin içinde 'öğrenme' amaçlı kaldığını savunmaktadır. Ancak mahkemeler artık sadece eserin yüzde kaçının kopyalandığına değil, eserin kalbi olan en can alıcı kısımlarının alınıp alınmadığına da dikkat etmeye başlamıştır.⁸ Son olarak değerlendirilen dördüncü faktör olan pazar etkisi, aslında bu analizin ekonomik kalbini oluşturmaktadır. Barton Beebe'nin 1978-2005 yılları arasındaki yüzlerce davayı kapsayan araştırması mahkemelerin her faktöre aynı önemi göstermediğini, değerlendirme yaparken her zaman birinci (amaç) ve dördüncü (pazar etkisi) faktörü daha çok önemsediklerini ortaya koymaktadır.⁹ Beebe'ye göre, mahkemeler kullanımı "dönüştürücü" bulduğunda pazar zararını bir miktar görmezden gelebilmektedir. Ancak yapay zeka çıktıları, orijinal

sanatçının potansiyel müşterilerini hedefleyip onun piyasa payını çalmaya başladığında Beebe'nin de işaret ettiği üzere adil kullanım savunması çökmeye mahkum kalmaktadır. Burada karşımıza çıkan "pazar ikamesi (*market substitution*)", adil kullanımı geçersiz kılan en keskin ve en somut kriter olarak görülmektedir.



IV. Uluslararası Denetim Mekanizması:

Adil kullanım doktrini sadece ABD iç hukukuna özgü, ucu açık bir serbestlik alanı değildir. Aksine bu doktrin, uluslararası sözleşmelerle çizilmiş çok net bir çerçeve içerisinde hareket etmek zorundadır. Berne Sözleşmesi ve TRIPS Anlaşması ile uluslararası hukuka giren "Üç Adımlı Test" bir ülkenin kendi yasasında getirdiği telif istisnalarının meşruiyetini denetlemesini sağlamaktadır. Bu test uyarınca, bir kullanımın istisna kabul edilebilmesi için şu üç basamağı da başarıyla geçmesi gerekmektedir:¹⁰

1. İstisna, yalnızca belirli ve özel durumlarda uygulanmalıdır.
2. İstisna, eserin normal kullanımına aykırı olmamalıdır.
3. İstisna, eser sahibinin meşru menfaatlerine makul olmayan düzeyde zarar vermemelidir.¹¹

Yapay zekaya ilişkin olarak milyonlarca eserin hiçbir bedel ödemediği işlenmesi hususu ise bahsi geçen bu testin ikinci basamağına tekabül etmekte ve bu noktada tartışmalara sebep olmaktadır. Günümüzde eserlerin veri setleri için lisanslanması artık başlı başına bir normal kullanım alanı, bir pazar haline gelmiş durumdadır. Teknoloji devi olan şirketler, eserleri lisanslamak yerine bu bir adil kullanımdır

⁷ Pierre N. Leval, "Toward a Fair Use Standard", *Harvard Law Review*, Vol. 103, No. 5, 1990, s. 1107

⁸ Harper & Row, *Publishers, Inc. v. Nation Enterprises*, 471 U.S. 539 (1985)

⁹ Barton Beebe, "An Empirical Study of U.S. Copyright Fair Use Opinions, 1978-2005", *University of Pennsylvania Law Review*, Vol. 156, No. 3, 2008, s. 621

¹⁰ *Berne Convention for the Protection of Literary and Artistic Works*, m. 9(2).

¹¹ Christophe Geiger, Daniel J. Gervais & Martin Senftleben, "Understanding the Three-Step Test", *International Intellectual Property*, Edward Elgar Publishing, 2015, s. 12

diyerek sistemin boşluklarından yararlanırlarsa eser sahibinin bu pazardaki en temel ekonomik beklentisini doğrudan yok etmiş olurlar. Kısacası, uluslararası hukuk perspektifinden baktığımızda, bir istisnanın meşru sayılması için bu üç adımın aynı anda karşılanması şarttır. Aksi takdirde, ilgili devletin uluslararası telif yükümlülüklerini ihlal ettiği sonucu ortaya çıkmaktadır; bu durum ise yapay zeka davalarının sadece şirketler arası bir anlaşmazlık değil, aynı zamanda uluslararası bir hukuk krizi olabileceğini gözler önüne sermektedir.

V. Güncel Yargı Kararları

ABD Yüksek Mahkemesi'nin (*Supreme Court*) 2023 yılında verdiği *Warhol v. Goldsmith* kararı, adil kullanım doktrininde son otuz yılın en önemli kırılma noktası olarak kabul edilmektedir. Karar, Andy Warhol'un bir fotoğrafçıya ait olan Prince portresini kullanarak yaptığı serigrafik çalışmaların "adil kullanım" olmadığını hükme bağlamıştır. Bu kararın yapay zeka ekosistemi için yarattığı asıl yenilik, birinci faktör olan "dönüştürücülük" analizine getirilen yeni bakış açısıdır. Mahkeme, bir kullanımın sadece estetik veya sanatsal bir farklılık yaratmasının (*transformative use*) tek başına yeterli olmadığını; asıl bakılması gerekenin kullanım amacının orijinalliyi olduğunu belirtmiştir. Eğer yeni eser, orijinal eserle aynı pazar payını hedefliyorsa ve ticari bir ikame niteliği taşıyorsa, sanatsal farklılıklar adil kullanım savunmasını kurtarmaya yetmemektedir.¹² Bu içtihat, yapay zeka şirketlerinin "biz veriyi tamamen yeni görsellere dönüştürüyoruz" şeklindeki savunmalarının önündeki en büyük hukuki engel haline gelmiştir. AI davalarında teknoloji devlerinin en çok güvendiği emsal ise 2015 yılında kesinleşen *Authors Guild v. Google* kararıdır. Google'ın milyonlarca kitabı dijitalleştirerek bir arama motoru indeksi oluşturması, mahkeme tarafından adil kullanım sayılmıştır. Mahkemenin buradaki gerekçesi, Google'ın kitapların içeriğini "okunmak için" değil, "bilgiye erişimi kolaylaştıran bir araç" olarak kullanmasıdır. Bu durum, "gayri-ifade edici kullanım" (*non-expressive use*) teorisinin temelini atmıştır¹³. Yapay zeka geliştiricileri bugün tam da bu karara sığınarak, modellerin eğitimi sürecindeki kopyalamanın Google Books örneğinde olduğu gibi

sadece teknik ve fonksiyonel bir işlem olduğunu savunmaktadır. Ancak Warhol kararı, bu fonksiyonel kullanım alanını daraltarak, AI çıktılarının ticari rekabet gücünü sorgulanır hale getirmiştir.

SONUÇ

Adil kullanım, telif hakkı tekelinin bilgi akışını tıkadığı noktalarda devreye giren yapısal bir emniyet subabıdır.¹⁴ Ancak yapay zeka çağında, sadece dönüştürücülük kriteri teknoloji şirketlerini korumaya yetmeyecektir. Geleceğin telif hukuku; yaratıcı emeği sadece bir istatistiksel veri olarak görmeyen, aksine inovasyon ile mülkiyet arasındaki o hassas denge verinin değerinin ödendiği bir lisanslama ufkuna evrilmek zorundadır. Telif hukuku, teknolojik ilerlemeyi teşvik ederken, bu ilerlemenin yakıtını sağlayan insan yaratıcılığını da feda etmemelidir. Son durumda, yapay zekanın "öğrenme" hakkı, insanın "yaratma" hakkının önüne geçtiği noktada, fikri mülkiyet hukukunun varlık sebebi ortadan kalkacaktır. Gelecekteki hukuki uyumsuzlukları azaltmanın yolu, yapay zekayı bedelsiz bir veri alanı olarak görmek yerine, eser sahiplerinin de haklarını alabildiği bir toplu lisanslama düzenini inşa etmekten, eser sahibine haklarını almasını sağlayacak standart sistemler kurmaktan geçmektedir. Adil kullanım, bir hak ihlali bahanesi değil; ancak hakkaniyetli bir bedel sistemiyle entegre edildiğinde gerçek işlevine kavuşacaktır.

KAYNAKÇA

- Andy Warhol Foundation for the Visual Arts, Inc. v. Goldsmith, 598 U.S. 508 (2023). ATEŞ, Mustafa, "Fikir ve Sanat Mahsullerinin Yapay Zekânın Eğitiminde Kullanılmasının Telif Hakları Bağlamında Değerlendirilmesi", *Ticaret ve Fikri Mülkiyet Hukuku Dergisi (TFM)*, Cilt 11, Sayı 2, 2025, s. 241-272.
- Authors Guild, Inc. v. Google, Inc., 804 F.3d 202 (2d Cir. 2015). BEEBE, Barton, "An Empirical Study of U.S. Copyright Fair Use Opinions, 1978-2005", *University of Pennsylvania Law Review*, Vol. 156, No. 3, 2008, s. 549-624.
- DOĞAN, Esma Muheyne, "Üretken Yapay Zeka Modellerinin Eğitiminde Kullanılan İçeriklerin Telif Hakkı İhlali: ABD'deki Güncel Davalar Işığında Karşılaştırmalı Bir İnceleme", *Ticaret ve Fikri Mülkiyet Hukuku Dergisi (TFM)*, Cilt 11, Sayı 1, 2025, s. 85-115.
- GEIGER, Christophe / GERVAIS, Daniel J. / SENFTLEBEN, Martin, "Understanding the Three-Step Test", *International Intellectual Property: A Handbook of Contemporary Research*, (Ed. Daniel J. Gervais), Edward Elgar Publishing, 2015.
- M. LANIER, Jaron / WEYL, E. Glen, "A Blueprint for a Better Digital Society", *Harvard Business Review*, 2018. (Veri Onuru/Data Dignit kavramı üzerine).
- LEVAL, Pierre N., "Toward a Fair Use Standard", *Harvard Law Review*, Vol. 103, No. 5, 1990, s. 1105-1136.
- Perfect 10, Inc. v. Amazon.com, Inc., 508 F.3d 1146 (9th Cir. 2007).
- Sarah Andersen et al. v. Stability AI Ltd. et al., Case No. 23-cv-00201(N.D.Cal.).
- The New York Times Company v. Microsoft Corporation, OpenAI, Inc. et al., Case No. 1:23-cv-11195 (S.D.N.Y.).

¹² Andy Warhol Foundation for the Visual Arts, Inc. v. Goldsmith, 598 U.S. 508 (2023)

¹³ Authors Guild, Inc. v. Google, Inc., 804 F.3d 202 (2d Cir. 2015).

¹⁴ Ateş, Mustafa. "Fikir ve Sanat Mahsullerinin Yapay Zekânın Eğitiminde Kullanılmasının Telif Hakları Bağlamında Değerlendirilmesi", *TFM*, 2025

KAMUSAL ALANDA YAPAY ZEKA DESTEKLİ DENETİM VE SİYASAL İFADE ÖZGÜRLÜĞÜ ÜZERİNE ETKİLERİ

Giriş

Demokratik toplumun en önemli gerekliliklerinden biri, vatandaşların kolektif iradelerini beyan ettiği, "siyasal özne" olarak varlık gösterdiği bir ortamın tesis edilmesi¹, meydanların tıpkı tarihsel süreçte siyasal ifade özgürlüğünün somutlaştığı ve iktidarın denetlendiği birer "agora" olarak işlev gördüğü gibi toplumun özgürce bir araya geldiği alanlar olmasıdır². Bu makalede, kamu otoritelerinin meydanlarda yürüttüğü yapay zeka destekli gözetimin, bireylerin **toplantı ve gösteri yürüyüşü hakkı**³ ile bu hakkın ayrılmaz bir parçası olan **siyasal ifade özgürlüğü** üzerindeki daraltıcı etkisi tartışılacaktır. Makalenin temel tezi; biyometrik teşhis teknolojilerinin, doğrudan bir müdahale veya fiziksel bir engelleme olmaksızın, bireyde "sistemlik kayıt altına alınma, dijital profillemeye ve siyasal kimliği nedeniyle cezalandırılma" korkusu yaratarak bir caydırıcı etki oluşturduğudur. Bu doğrultuda, siyasal katılımın temel ön şartı olan "anonim kalma hakkının" teknolojik araçlarla ortadan kaldırılmasının, demokratik çoğulculuğu nasıl bir otosansür sarmalına soktuğu analiz edilecektir⁴. Yapay zekanın özel hayatın gizliliğine ilişkin genel ihlalleri veya ticari amaçlı uygulamaları bu çalışmanın kapsamı dışındadır. Tartışma, yalnızca kamu otoritesinin siyasal katılım alanlarındaki dijital denetiminin, bireyin siyasal karar alma ve ifade süreçleri üzerindeki etkisi ile sınırlandırılmıştır.



¹ Anayasa Mahkemesi. *Yaman Akdeniz ve Diğerleri Başvurusu*. B. No: 2014/3986, 02 Nisan 2014, § 25.

² Habermas, Jürgen. *Kamusal Alanın Yapısal Dönüşümü*. Çeviren Tanıl Bora ve Mithat Sancar, İletişim Yayınları, 1997.

³ Anayasa Mahkemesi. *Ali Rıza Özer ve Diğerleri Başvurusu* [GK]. B. No: 2013/3924, 06 Ocak 2015, § 117.

Anayasa Mahkemesi. *Osman Erbil Başvurusu*. B. No: 2013/2394, 25 Mart 2015, § 47.

⁴ Murray, Daragh. "Yüz Tanıma ve Bildiğimiz Anlamda İnsan Haklarının Sonu mu?" *Hollanda İnsan Hakları Dergisi*, cilt 42, no. 2, 2024, ss. 147-148.

İKLİM GÜNEŞ ATAR & FATMA RÜMEYSA TÜNAY

Biyometrik Veri İşleme Süreçlerinin Teknik ve Hukuki Niteliği

Kamu otoritelerinin kamusal alanlarda kullandığı yüz tanıma teknolojilerini geleneksel güvenlik kameralarından ayıran temel fark, bu sistemlerin sadece görüntü kaydetmesi değil, kaydedilen görüntüyü saniyeler içinde analiz edilebilir ve eşleştirebilir bir "dijital kimliğe" dönüştürmesidir. Teknolojik süreçte; yüksek çözünürlüklü kameralar aracılığıyla yakalanan insan yüzü, yapay zeka algoritmaları tarafından taranarak benzersiz biyometrik koordinatlara bölünür ve geri dönülemez bir matematiksel koda (*hash*) dönüştürülür. Bu aşamadan sonra birey, meydana gelen anonim bir vatandaş değil; devletin veri tabanındaki kimlik bilgileriyle saniyeler içinde eşleşebilen dijital bir dosyadır.

Ancak bu teknolojik süreç, sanıldığı gibi hatasız veya tarafsız işleyen bir mekanizma değildir. *Electronic Frontier Foundation (EFF)* tarafından vurgulandığı üzere; "Yüz tanıma yazılımları; etnik azınlıkları, kadınları ve gençleri tanıma konusunda özellikle yetersiz kalmakta; bu grupları yanlış teşhis riskine ve orantısız baskıya maruz bırakmaktadır." Bu durum, teknolojinin teknik bir hata payından ziyade, siyasal bir denetim aracına dönüştüğünün kanıtıdır. *EFF*'nin tespitiyle bu sistemler, "tarihsel olarak adaletsiz polislik uygulamalarının hedefi olmuş toplulukların kitleler halinde gözetlenmesine hizmet etmekte; ifade özgürlüğü kapsamındaki eylemlerde bulunan kişileri hedef almak ve 'düşman' olarak algılananları dışlamak için" kullanılmaktadır⁵.

Bu verilerin toplanma ve depolanma biçimi, masum bir güvenlik önleminin ötesinde sistematik bir siyasal profillemeye altyapısı oluşturmaktadır. Yapay zeka, bir eylemcinin kimliğini tespit etme maliyetini sıfıra indirirken, toplanan biyometrik kodların merkezi sunucularda süresiz saklanması kamu otoritesine geriye dönük teşhis imkânı tanır. Verilerin neden ve nerede kullanılmak üzere toplandığı sorusunun cevabı ise doğrudan bu siyasal denetimle ilgilidir. Kamu

⁵ "Face Recognition." *Street Level Surveillance*, Electronic Frontier Foundation, 5 Eylül 2023, sfs.eff.org/technologies/face-recognition.

KAMUSAL ALANDA YAPAY ZEKA DESTEKLİ DENETİM VE SİYASAL İFADE ÖZGÜRLÜĞÜ ÜZERİNE ETKİLERİ

otoritesi, bu verileri kullanarak "muhalif", "aktivist" veya "risk grubu" gibi etiketlerle dijital bir siyasi sicil oluşturma imkanı bulur. Bu veriler; kamu personeli alımlarındaki güvenlik soruşturamalarında veya idari izin süreçlerinde bireyin karşısına görünmez bir engel olarak çıkarılmak üzere depolanmaktadır. Sonuç olarak, meydanlardaki kameralar artık sadece asayiş sağlamak için değil; her bir yüzü birer veri setine dönüştürerek kamu otoritesinin merkezi veri tabanlarında sınıflandırmaktadır.

Caydırıcı Etki ve Otosansür

Siyasal ifade özgürlüğü, sadece fiziksel engellerin yokluğuyla değil, aynı zamanda bireyin bu özgürlüğü kullanırken hissettiği psikolojik güvenlik alanıyla ölçülür. Kamu otoritelerinin meydanlarda kullandığı yapay zeka destekli yüz tanıma teknolojileri, tam da bu güvenlik alanını hedef alarak literatürde "caydırıcı etki" olarak tanımlanan bir otosansür mekanizmasını tetiklemektedir. Caydırıcı etki; bireyin yasal bir hakkını kullanmaktan, bu kullanımın doğurabileceği olası bir negatif sonuç korkusuyla vazgeçmesi halidir. Bu durumun en somut ve tehlikeli örneği, dünya çapında birçok devlet tarafından kamuda yapay zeka kullanımı açısından bir model teşkil eden **Clearview AI**⁶ yazılımıdır. *Clearview AI*, geliştirdiği yazılımla internet üzerindeki milyarlarca görüntüyü tarayıp depolayarak, saniyeler içinde eşleştirme yapabilen devasa bir "biyometrik arama motoru" oluşturmıştır. Bu yazılımın kamu otoriteleri tarafından kullanılması, birey için siyasi katılımı bir "maliyet analizi" konusuna dönüştürmektedir. Bir protestoya katılmayı düşünen vatandaş, *Clearview AI* gibi sistemlerin varlığını bildiğinde, meydana anan anonim varlığının saniyeler içinde tüm dijital geçmişiyle (sosyal medya hesapları, profesyonel özgeçmişi vb.) eşleşebileceğini fark eder. Bu durum, bireyin zihninde "*Bugün bu meydana bulunmam, yarın bir kamu mülakatında elenmem veya siyasi kimliğim nedeniyle bir yaptırımla karşılaşmama neden olur mu?*" sorusunu hayati bir kaygı haline getirir. Nitekim, *Clearview AI*'ın bu kontrolsüz veri depolama pratiği; beraberinde

⁶ Cameron, Dell. "CBP Signs Clearview AI Deal to Use Face Recognition for 'Tactical Targeting'." *Wired*, 11 Şubat 2026. Council, Jared. "Local Police Force Uses Facial Recognition to Identify Capitol Riot Suspects." *The Wall Street Journal*, 8 Ocak 2021.

İKLİM GÜNEŞ ATAR & FATMA RÜMEYSA TÜNAY

birçok hukuki davayı⁷, soruşturmayı⁸ ve ağır yaptırımları⁹ getirdiği gibi, medyanın da bu teknolojinin demokratik toplum için oluşturduğu tehlikeyi¹⁰ gözler önüne sermiştir.

Bu tür teknolojilerin yaygınlaşması, siyasi kamusal alanın fiilî kullanımını daraltma potansiyeli taşımaktadır. Nitekim çeşitli teknoloji şirketlerinin yüz tanıma sistemlerinin kullanımını sınırlandırması ve Avrupa Birliği veri koruma otoritelerinin *Clearview AI* hakkında hukuka aykırılık tespitlerinde bulunması, biyometrik gözetimin temel haklar üzerindeki etkisine ilişkin küresel düzeyde artan bir farkındalığa işaret etmektedir. Bu bağlamda, bireylerin kamusal alanda kimliklerinin tespit edilmesi ve bu verilerin ileride aleyhlerine kullanılabileceği yönündeki makul endişeleri, toplantı ve gösteri yürüyüşü hakkının kullanımını dolaylı biçimde sınırlandırabilmektedir.

Sonuç olarak, algoritmik gözetim altında şekillenen kamusal alan, farklı ve eleştirel görüşlerin serbestçe ifade edildiği bir tartışma zemini olmaktan uzaklaşarak, bireylerin potansiyel sonuçları gözeterek davranmak zorunda kaldığı daha temkinli bir ortama dönüşme riski taşımaktadır.

Siyasal İfade Özgürlüğünün Kaynakları ve Yargı Kararları Işığında Değerlendirilmesi

İfade özgürlüğü, uluslararası hukukta Birleşmiş Milletler İnsan Hakları Evrensel Beyannamesi¹¹,

⁷ "ACLU v. Clearview AI." *American Civil Liberties Union*, 9 Mayıs 2022, www.aclu.org/press-releases/aclu-v-clearview-ai-settlement-prohibits-company-selling-facial-recognition-database.

⁸ "News Release: Clearview AI's Unlawful Practices Represented Mass Surveillance of Canadians, Commissioners Say." *Office of the Privacy Commissioner of Canada*, 3 Şubat 2021, www.priv.gc.ca/en/opc-news/news-and-announcements/2021/nr-c_210203.

⁹ Lunden, Ingrid. "Clearview AI Hit with Its Largest GDPR Fine Yet as Dutch Regulator Considers Holding Execs Personally Liable." *TechCrunch*, 3 Eylül 2024, techcrunch.com/2024/09/03/clearview-ai-hit-with-its-largest-gdpr-fine-yet-as-dutch-regulator-considers-holding-execs-personally-liable/.

¹⁰ Hill, Kashmir. "The Secretive Company That Might End Privacy as We Know It." *The New York Times*, 18 Ocak 2020, www.nytimes.com/2020/01/18/technology/clearview-facial-recognition.html.

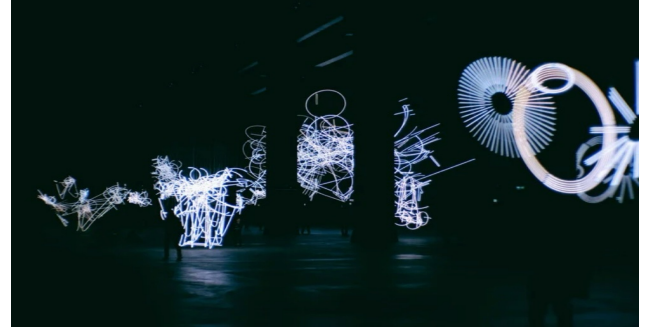
KAMUSAL ALANDA YAPAY ZEKA DESTEKLİ DENETİM VE SİYASAL İFADE ÖZGÜRLÜĞÜ ÜZERİNE ETKİLERİ

Avrupa İnsan Hakları Sözleşmesi (AİHS)¹² ve Medeni ve Siyasi Haklara İlişkin Uluslararası Sözleşme¹³ gibi temel belgelerle güvence altına alınmıştır. Bu düzenlemeler ışığında ifade özgürlüğü; her türlü araçla düşüncelerin açıklanmasını ve toplum içinde özgür bir düşünce alışverişini sağlayan, ayırım gözetmeksizin herkese tanınan temel bir haktır. Avrupa İnsan Hakları Mahkemesi içtihatları¹⁴, bu özgürlüğün demokratik bir devlette sadece tanınması değil, aynı zamanda devlet tarafından korunması ve saygı duyulması gereken bir değer olduğunu vurgulamıştır. Özellikle siyasi ifade özgürlüğü, demokratik toplumda çoğulculuğun vazgeçilmez bir şartı olarak kabul edilmiş; sarsıcı ve şok edici söylemler dahi bu koruma şemsiyesi altına alınarak devletin müdahale alanı daraltılmıştır. 1982 Anayasası'nın 26. maddesi¹⁵ de bu uluslararası standartlara uygun olarak herkesin düşüncelerini "tek başına veya toplu olarak" açıklama hakkına sahip olduğunu hüküm altına almıştır.

Ancak günümüzde, anayasal güvence altındaki bu hakkın toplu kullanımı noktasında, devletlerin "kamu güvenliği" gerekçesiyle devreye soktuğu yapay zeka destekli mekanizmalar yeni bir ihlal alanı doğurmaktadır. Bu noktada **Glukhin v. Rusya (2023)**¹⁶ kararı, teknolojik gözetimin siyasi ifade özgürlüğü üzerindeki daraltıcı etkisini tespit eden tarihi bir emsal niteliğindedir. Davaya konu olayda; barışçıl bir siyasi protesto gerçekleştiren başvurucunun, yüz tanıma sistemleri aracılığıyla teşhis edilerek cezalandırılması, AİHM tarafından hem özel hayata (m. 8) hem de ifade özgürlüğüne (m. 10) yönelik orantısız bir müdahale olarak değerlendirilmiştir. Mahkeme bu kararında, siyasi ifade özgürlüğünün sadece cezalandırılmamayı değil,

İKLİM GÜNEŞ ATAR & FATMA RÜMEYSA TÜNAY

aynı zamanda bireyin hakkını kullanırken maruz kalabileceği caydırıcı etkiden korunmasını da kapsadığını vurgulamıştır. Barışçıl bir eylemcinin yapay zeka ile anlık veya geriye dönük olarak teşhis edilmesi, demokratik bir toplumda gereklilik ve orantılılık ilkeleriyle bağdaşmamaktadır. AİHM'in tespitiyle, kamu otoritesinin elindeki bu teknolojik güç; hükümete yönelik eleştirilerin alanını genişletmek yerine, bireyler üzerinde yarattığı caydırıcı etki neticesinde siyasi katılımı minimize etmektedir.



Sonuç

Bu makalede, yüz tanıma teknolojilerinin bireylerin ifade özgürlüğünü nasıl etkilediği ve bireyler üstünde nasıl bir caydırıcı etki yarattığı ele alınmıştır. Makalede bazı devletlerin yüz tanıma teknolojisini yalnızca güvenlik için kullanmadığı; bireylerin hakları ihlal etmek amacıyla kullanıldığı vurgulanmıştır. Bu kullanımın gittikçe yaygınlaştığını ve ifade özgürlüğünün gittikçe tehlike altına girdiğini BM İnsan Hakları Konseyi yayınladığı gözetime ilişkin raporu¹⁷ ve EDPB yüz tanıma ile ilgili yayınladığı kılavuzu¹⁸ gözler önüne sermektedir. Bu yayınlarda ayrıca bu kullanımların kontrol altına alınması gerektiği de vurgulanmakta ve buna ilişkin bir çok öneri yer almaktadır.

Sonuç olarak kamunun yapay zeka destekli yüz tanıma teknolojilerin nerede, nasıl, hangi koşullar

¹¹ Birleşmiş Milletler. *İnsan Hakları Evrensel Beyannamesi*. 1948, m. 19.

¹² Avrupa Konseyi. *Avrupa İnsan Hakları Sözleşmesi*. 1950, m. 10.

¹³ Birleşmiş Milletler Genel Kurulu. *Medeni ve Siyasi Haklara İlişkin Uluslararası Sözleşme*. 1966, m. 19.

¹⁴ Avrupa İnsan Hakları Mahkemesi. *Handyside v. Birleşik Krallık*. Başvuru No: 5493/72, 07 Aralık 1976. Avrupa İnsan Hakları Mahkemesi. *Lingens v. Avusturya*. Başvuru No: 9815/82, 08/07/1986.

¹⁵ Türkiye Cumhuriyeti. *Türkiye Cumhuriyeti Anayasası*. 1982, m. 26.

¹⁶ Avrupa İnsan Hakları Mahkemesi. *Glukhin v. Rusya*. Başvuru No: 11519/20, 04 Temmuz /2023.

¹⁷ Birleşmiş Milletler, İnsan Hakları Konseyi. *Gözetim ve İnsan Hakları: Düşünce ve İfade Özgürlüğü Hakkının Teşviki ve Korunması Konusunda Özel Raportörün Raporu*. A/HRC/41/35, 28 Mayıs 2019, Özet Bölümü.

¹⁸ European Data Protection Board, *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement*, Version 2.0, adopted 26 Nisan 2023, § 35 https://www.edpb.europa.eu/news/news/2023/edpb-adopts-final-version-guidelines-facial-recognition-technology-area-law_en

KAMUSAL ALANDA YAPAY ZEKA DESTEKLİ DENETİM VE SİYASAL İFADE ÖZGÜRLÜĞÜ ÜZERİNE ETKİLERİ

altında kullanılacağı kanunla düzenlenerek öngörülebilir bir yapı kurulmalı; bu sayede bireylerin haklarına ve özgürlüklerine müdahalesi önlenememelidir. Bununla birlikte hangi verilerin toplanabileceği ve sisteme kayıt edilebileceğine ilişkin düzenlemeler de bu alan için gereklidir. Özellikle demokratik kazanımların toplumsal taleplerden ziyade idari tasarruflarla şekillendiği ve hak arama kültürünün henüz organik bir biçimde kurumsallaşmadığı bir toplumda hakların ve özgürlüklerin kanunla güvence altına alınması gerekliliği göz ardı edilemeyecek bir gerçekliktir. Bu nedenle kanunla nasıl kullanılması gerektiği düzenlenmekle birlikte insan hakların ihlalinin önlemek için AB Yapay Zeka Yasası¹⁹ kapsamındaki yasaklamalar ile sınırlı kalmayarak bu alanda caydırıcı yaptırımlar öngörülmelidir, yasaklar konulmalıdır. Yüz tanıma sistemlerinin yargı eliyle denetlenmesi gerekmektedir. Bunları, ülkelerin konuyu AB sınırları dışına taşıyarak kendi iç hukukunda düzenlemesi bireylerin ifade özgürlüğünün kullanımı üstündeki caydırıcı etki kaldırılabilir. ²⁰

KAYNAKÇA

Ada Lovelace Institute. "What Do We Talk About When We Talk About Biometrics?" 12 Temmuz 2022, www.adalovelaceinstitute.org/blog/what-talk-about-biometrics/.

Amnesty International. "Ban Dangerous Facial Recognition Technology That Amplifies Racist Policing." 26 Ocak 2021, www.amnesty.org/en/latest/press-release/2021/01/ban-dangerous-facial-recognition-technology-that-amplifies-racist-policing/.

Anayasa Mahkemesi. *Ali Rıza Özer ve Diğerleri Başvurusu [GK]*. B. No: 2013/3924, 06/01/2015.

Anayasa Mahkemesi. *Yaman Akdeniz ve Diğerleri Başvurusu*. B. No: 2014/3986, 02/04/2014.

Avrupa Birliği. *Avrupa Birliği Yapay Zeka Yasası (AI Act)*. 2024.

Avrupa İnsan Hakları Mahkemesi. *Glukhin v. Rusya*. B. No: 11519/20, 04/07/2023.

¹⁹ Avrupa Birliği. *Avrupa Birliği Yapay Zeka Yasası (AI Act)*. 2024, m. 5(e).

²⁰ Birleşmiş Milletler, İnsan Hakları Konseyi. *Gözetim ve İnsan Hakları: Düşünce ve İfade Özgürlüğü Hakkının Teşviki ve Korunması Konusunda Özel Raportörün Raporu*. A/HRC/41/35, 28 Mayıs 2019, § 66.

İKLİM GÜNEŞ ATAR & FATMA RÜMEYSA TÜNAY

Avrupa İnsan Hakları Mahkemesi. *Handyside v. Birleşik Krallık*. B. No: 5493/72, 07/12/1976.

Avrupa İnsan Hakları Mahkemesi. *Lingens v. Avusturya*. B. No: 9815/82, 08/07/1986.

Avrupa Konseyi. *Avrupa İnsan Hakları Sözleşmesi*. 1950.

Birleşmiş Milletler Genel Kurulu. *Medeni ve Siyasi Haklara İlişkin Uluslararası Sözleşme*. 1966.

Birleşmiş Milletler, İnsan Hakları Konseyi. *Gözetim ve İnsan Hakları: Düşünce ve İfade Özgürlüğü Hakkının Teşviki ve Korunması Konusunda Özel Raportörün Raporu*. A/HRC/41/35, 28 Mayıs 2019.

Birleşmiş Milletler. *İnsan Hakları Evrensel Beyannamesi*. 1948.

Cameron, Dell. "CBP Signs Clearview AI Deal to Use Face Recognition for 'Tactical Targeting'." *Wired*, 11 Şubat 2026.

Council, Jared. "Local Police Force Uses Facial Recognition to Identify Capitol Riot Suspects." *The Wall Street Journal*, 8 Ocak 2021.

Electronic Frontier Foundation. "Face Recognition." *Street Level Surveillance*, 5 Eylül 2023, sls.eff.org/technologies/face-recognition.

European Data Protection Board. *Guidelines 05/2022 on the Use of Facial Recognition Technology in the Area of Law Enforcement*. Versiyon 2.0, 26 Nisan 2023.

European Digital Rights (EDRI). "Biometric Mass Surveillance Flourishes in Germany and the Netherlands." 27 Ekim 2021, edri.org/our-work/biometric-mass-surveillance-flourishes-in-germany-and-the-netherlands/.

Habermas, Jürgen. *Kamusal Alanın Yapısal Dönüşümü*. Çeviren Tanıl Bora ve Mithat Sancar, İletişim Yayınları, 1997.

Hill, Kashmir. "The Secretive Company That Might End Privacy as We Know It." *The New York Times*, 18 Ocak 2020.

Kişisel Verileri Koruma Kurumu (KVKK). *Biyometrik Verilerin İşlenmesinde Dikkat Edilmesi Gereken Hususlara İlişkin Rehber*. 2021, www.kvkk.gov.tr/SharedFolderServer/CMSFiles/bd06f5f4-e8cc-487e-abe1-d32dc18e2d7e.pdf.

Lunden, Ingrid. "Clearview AI Hit with Its Largest GDPR Fine Yet as Dutch Regulator Considers Holding Execs Personally Liable." *TechCrunch*, 3 Eylül 2024.

Murray, Daragh. "Yüz Tanıma ve Bildiğimiz Anlamda İnsan Haklarının Sonu mu?" *Hollanda İnsan Hakları Dergisi*, cilt 42, no. 2, 2024, ss. 147-148.

Office of the Privacy Commissioner of Canada. "Clearview AI's Unlawful Practices Represented Mass Surveillance of Canadians, Commissioners Say." 3 Şubat 2021, www.priv.gc.ca/en/opc-news/news-and-announcements/2021/nr-c_210203/.

Türkiye Cumhuriyeti. *Türkiye Cumhuriyeti Anayasası*. 1982.

KÜNYE

Dergi adı: Hakkım Var! Dergisi

Yayın Tarihi: Temmuz 2026

Mahiyeti: Bilimsel

Yayın Türü: Yerel Süreli Yayın

Yayınlayan Kurum: Hakkım Var Derneği

Dergi Konuları: Hukuk

YAYIN KURULU

Şule KAYAOLUK

Ezgi Su SİLİ

İnternet Sitesi: <https://hakkimvar.com/>

Instagram: <https://www.instagram.com/hakkimvarorg/>

LinkedIn: <https://www.linkedin.com/company/hakk%C4%B1m-var/>

İletişim: info@hakkimvar.com