



Yapay Zekâ Tabanlı Sahte Dijital İçeriklerle (Deepfake) Görüntü ve Ses Üzerindeki Hakkın İhlali^(*)



Violation of Rights on Images and Audio with Artificial Intelligence-Based Fake Digital Content (Deepfake)

Mehmet Emin ÖZGÜL



Doçent Doktor

Pamukkale Üniversitesi Hukuk Fakültesi

Medeni Hukuk Anabilim Dalı

Anahtar Kelimeler

Yapay Zekâ,
Deepfake,
Derin Öğrenme,
Kişilik Hakkı,
5651 Sayılı Kanun.

Öz

Yapay zekâ alanında yaşanan gelişmeler, birçok hukuki sorunu da beraberinde getirmektedir. Yapay zekâdan yararlanılarak dijital içerikler üretmeye imkân veren ve sürekli gelişen yöntemlerden biri de “deepfake”tir. Mevcut fotoğraf, video gibi bir görüntünün başka bir görüntüye entegre edilerek, yeni ve oldukça gerçekçi bir içerik elde edilmesine veya bir kişinin sesinin bir konuşmaya entegre edilerek, kişilerin istenildiği gibi konuşturulmasına imkân veren bu teknolojinin faydalı ve hukuka uygun kullanım alanları olduğu gibi, zararlı ve hukuka aykırı kullanım alanları da vardır. Deepfake teknolojisinin ciddi hukuki sorunlara, konusu suç olan ya da diğer hukuka aykırı eylemlere, ulusal ya da uluslararası krizlere yol açabileceği öngörüsü, bu durumda başvurulacak hukuki çarelerin de tartışılmaya başlamasına neden olmuştur. Deepfake içerikler, hukukun birçok alanını ilgilendiren ve multidisipliner olarak ele alınması gereken bir konu olduğu için çalışmamızda farklı disiplinlerde yazılmış eserlere de başvurularak öncelikle deepfake teknolojisi tanımlanmış, görüntü ve ses üzerindeki kişilik hakkı ele alınarak hukuki sorunlardan ve çözüm yollarından bahsedilmiştir.

Keywords

Artificial Intelligence,
Deepfake,
Deep Learning,
Right of Personality,
Law No. 5651.

Abstract

Developments in the field of artificial intelligence bring along many legal issues. One of the ever-developing methods that allows the production of digital content by utilizing artificial intelligence is “deepfake”. This technology, which allows the integration of an image such as an existing photograph or video into another image to obtain new and very realistic content or the integration of a person’s voice into a speech to make people speak as desired, has beneficial and lawful areas of use as well as harmful and unlawful areas of use. The prediction that deepfake technology may lead to serious legal problems, criminal or other unlawful acts, national or international crises has led to the discussion of legal remedies to be applied in this case. Since deepfake content is an issue that concerns many areas of law and should be handled in a multidisciplinary manner, in our study, deepfake technology is first defined by referring to works written in different disciplines, and legal problems and solutions are mentioned by addressing the personality right on image and sound.

^(*) Araştırma Makalesi.
Hakem denetiminden geçmiştir.

Gönderim Tarihi: 11.06.2025, Kabul Tarihi: 09.09.2025.



GİRİŞ

Görsel ve işitsel manipülasyon ve sahte içerik üretimi nerdeyse medyanın tarihi kadar eski olsa da günümüzde *deepfake* teknolojisinin ortaya çıkması, sahte dijital içerik oluşturma ve sosyal medyada veya diğer internet ortamlarında yayma bakımından bir dönüm noktası olmuştur¹. 2000 yılı sonrasında sosyal medyanın, özellikle de sosyal paylaşım sitelerinin yaygınlaşması ve görüntülü ve/veya sesli içeriklerin paylaşıldığı platformların popüler hâle gelmesiyle, eğlence, eğitim, gezi vb. içerikli videolar da yaygınlaşmıştır². Geliştirilen yeni yazılımlar (*software*) sayesinde dijital içeriklerde yapılabilen değişiklikler, hukuka aykırı şekilde yapılan görüntü ve/veya ses manipülasyonları ve bunların denetiminde yaşanan güçlükler³, zamanla kişilik hakkı ihlalleri başta olmak üzere birçok ihlalin önünü açmıştır. Bu şekilde görüntü ve/veya ses üzerinde oynama imkânı veren yazılımlarla elde edilen içerikler hem gerçek hem de tüzel kişiler bakımından ciddi bir tehdit hâline gelmiş hatta devletlerin akıbetini dahi belirleyebilecek, önemli siyasi krizlere yol açabilecek sorunların gündeme gelmesine neden olmuştur. Yapay zekâ ve makine öğrenimindeki en son teknolojik gelişmelerle daha da güçlenen *deepfake* altyapısı, insan gözlemcilerin tespit etmesi gittikçe zorlaşan sahte içerikler oluşturmak için birçok yeni imkân sunmaktadır⁴.

İnternet ortamında yer alan video ve/veya ses içerikleri, herhangi bir metin veya fotoğraftan daha fazla ilgi çekmekte ve inandırıcılık (*believability*) kazanarak daha güvenilir bir içerik gibi algılanabilmektedir⁵. Günümüzde bu içerikler farklı teknolojiler kullanılarak yapay bir ortamda kolaylıkla üretilmektedir. Dijital taklitçilik (*digital impersonation*) giderek daha gerçekçi ve ikna edici hâle gelecek yaygınlaşmakta, çevrimiçi platformlar ve özellikle sosyal paylaşım siteleri, kullanıcılar tarafından oluşturulan *deepfake* içeriklerin hızlı ve geniş ölçüde yayılımı için aracılık etmektedir⁶.

Deepfake teknolojisi kullanılarak elde edilen tahrif edilmiş videolar ya da diğer ses ve/veya görüntü kayıtları, insanları asla yapmadıkları veya söylemedikleri şeyleri yaparken veya söylerken göstererek ciddi bir dezenformasyona yol açabilen içerikler olup⁷, sahte içeriği gerçeğinden ayırmak gün geçtikçe daha da zor bir hâle gelmektedir⁸. Gerek bu tür içerikleri üretmekte kullanılan yapay zekâ, makine öğrenmesi, derin öğrenme gibi teknolojiler gerekse yapay sinir ağları, büyük veri (*big data*), nesnelerin interneti (*internet of things*) ve bulut bilişim (*cloud computing*) teknolojileri ve bunlarla desteklenen sistemler, sosyal ve ekonomik hayatımızı büyük ölçüde etkileyen⁹, çözüme kavuşturulması gereken birçok hukuki sorunu da beraberinde getirmiştir. Sosyal medyada ve genel olarak internet ortamında yapay zekâ teknolojileri ve belli yazılımlar yoluyla görüntü ve ses üzerinde değişiklikler yapılarak elde edilen *deepfake* içeriğin yayımlanması, bu ortamlarda ciddi bir güvensizlik oluşturup, haberlere ve diğer içeriğe olan güvenin azalmasına yol açmaktadır¹⁰. Bir görüntünün ve/veya sesin diğer bir görüntü veya ses içeriğine entegre edilmesi, kişilerin yapmadıkları şeyleri yapıyor, söyleme-

¹ KIETZMANN, Jan / LEE, Linda W. / MCCARTHY Ian P. / KIETZMANN, Tim C.: “Deepfakes: Trick or treat?”, *Business Horizons*, 2020, Cilt 63, Sayı 2, s. 135.

² BERK, Mustafa Evren: “Dijital Çağın Yeni Tehlikesi ‘Deepfake’”, *OPUS Uluslararası Toplum Araştırmaları Dergisi*, 2020, Cilt 16, Sayı 28, s. 1510.

³ BERK, s. 1510.

⁴ KIETZMANN / LEE / MCCARTHY / KIETZMANN, s. 135.

⁵ KIETZMANN / LEE / MCCARTHY / KIETZMANN, s. 136; PAWELEC, Maria: “Deepfakes and Democracy (Theory): How Synthetic Audio-Visual Media for Disinformation and Hate Speech Threaten Core Democratic Functions”, *Digital Society*, 2022, Cilt 1, Sayı 19, s. 2.

⁶ NAGUMOTU, Kavyasri: “Deepfakes Are Taking Over Social Media: Can The Law Keep Up?”, *Idea: The Intellectual Property Law Review*, 2022, Cilt 62, Sayı 2, s. 102, 117 vd.

⁷ KUGLER, Matthew B. / PACE, Carly: “Deepfake Privacy: Attitudes and Regulation”, *North Western University Law Review*, 2021, Cilt 116, Sayı 3, s. 613.

⁸ KIETZMANN / LEE / MCCARTHY / KIETZMANN, s. 136.

⁹ ÇEBER, Burak: “Yeni Nesil Reklam Aracı Olarak Yapay Zekâ Uygulamaları: Reklam Filmlerinde Deepfake Teknolojilerinin Kullanımı Üzerine Nitel Bir Çalışma”, (Ed.) BECAN, Cihan: *Tüketiciyi Anlamak: Reklam Araştırmalarında Disiplinlerarası Yaklaşımlar ve Yeni Yönelimler*, Efeakademi Yayınları, İstanbul, 2023, s. 16.

¹⁰ VACCARI, Cristian / CHADWICK, Andrew: “Deepfakes and Disinformation: Exploring the Impact of Synthetic Political Video on Deception, Uncertainty, and Trust in News”, *Social Media + Society*, 2020, Cilt 6, Sayı 1, s. 1 vd.; NAGUMOTU, s. 124 vd.

dikleri sözleri söylüyor gibi göründükleri sahte içeriklerin üretilmesi hem gerçek kişileri hem de devletler ve diğer tüzel kişileri tehdit eden bir duruma dönüşebilmektedir. Gelecekte çok daha sık gündeme geleceğini düşündüğümüz bu konunun irdelenmesi hem günümüzdeki hem de geleceğe ilişkin hukuki sorunların tespit edilmesi büyük önem taşımaktadır.

I. DEEFAKE TEKNOLOJİSİNİN TANIMI, ÖZELLİKLERİ, TARİHÇESİ VE KULLANIM ALANLARI

A. Deepfake Teknolojisinin Tanımı

Deepfake, derin öğrenmedeki (*deep learning*) “derin” (*deep*) kelimesiyle “sahte” (*fake*) kelimesinin birleştirilmesi yoluyla oluşturulmuş bir kelimedir¹¹. *Deepfake*, var olan teknolojilerin kullanılması ya da geliştirilmesinden ibaret bir yöntem olarak görülebileceği gibi, bu teknolojiler kullanılarak elde edilen yeni bir teknoloji olarak da kabul edilebilir. Avrupa Birliği (AB) Yapay Zekâ Yasası’nın 2 Şubat 2025 tarihinde yürürlüğe girmiş olan “Tanımlar” başlıklı 3. maddesinde *deepfake*, “yapay zekâ tarafından oluşturulan veya manipüle edilen, mevcut kişilere, nesnelere, yerlere, varlıklara veya olaylara benzeyen ve bir kişiye yanlışlıkla gerçek veya doğru gibi görünebilen görüntü, ses veya video içeriği” olarak tanımlanmaktadır¹².

Deepfake, görüntü ve/veya ses üzerinde dijital olarak çalışılmasını, kaynak görüntünün ve/veya sesin hedef görüntü ve/veya sese yüksek gerçeklik içerecek şekilde aktarılmasını¹³, ses, görüntü ve video içeriklerinin birleştirmesini, üst üste getirilmesini ve bu şekilde üzerinde ciddi değişiklikler ve oynamalar yapılmış içerikler elde edilmesini sağlayan bir teknoloji olup, bu işlemler için yapay zekânın üretken çekişmeli (rekabetçi) ağlar [*generative adversarial networks* (GAN)¹⁴], makine öğrenmesi (*machine learning*)¹⁵ yöntemleri ve özellikle bu yöntemlerden biri olan derin öğrenme (*deep learning*)¹⁶ yönteminin yararlanılmaktadır¹⁷. *Deepfake* içerik üretmenin teknolojik ana bileşeni derin öğrenme ve yapay sinir ağları olup, bu teknikler esasen makine öğrenimi yöntemleridir¹⁸. Derin yapay sinir ağları diyebileceğimiz DNN’ler (*deep neural network*) beyindeki nöronlara benzemekte ve birbirlerine bağlı geniş bir ya-

¹¹ NGUYEN, Thanh Thi / NGUYEN, Quoc Viet Hung / NGUYEN, Dung Tien / NGUYEN, Duc Thanh / HUYNH-THE, Thien / NAHAVANDI, Saeid / NGUYEN, Thanh Tam / PHAM, Quoc-Viet / NGUYEN, Cuong M.: “Deep Learning for Deepfakes Creation and Detection: A Survey”, *Computer Vision and Image Understanding*, 2022, Cilt 223, s. 1; ÇEBER, s. 19; YAVUZ, Can: *Deepfake (Derin Sahte)-Yapay Zekâ Tarafından Üretilen Yeni Nesil Görsel-İşitsel İçerik*, Seçkin Yayıncılık, Ankara, 2022 (Deepfake), s. 35-36; MANKOO, Sandeep Singh: “DeepFakes-The Digital Threat in the Real World”, *Gyan Management Journal*, 2023, Cilt 17, Sayı 1, 2023, s. 72; METZ, Rachel: *Researchers can now use AI and a photo to make fake videos of anyone*, 2019 (<https://edition.cnn.com/2019/05/24/tech/deepfake-ai-one-photo/index.html>, ET: 02.06.2025); AKMEŞE, Başak: “The Artificial Intelligence Dimension of Digital Manipulation Deepfake Videos: The Case of the Ukrainian-Russian People”, *Contemporary Issues of Communication*, 2023, Cilt 2, Sayı 2, s. 78.

¹² *Artificial Intelligence Act* için bkz. <https://artificialintelligenceact.eu/article/3/> (ET: 06.06.2025).

¹³ KUGLER / PACE, s. 613; NGUYEN / NGUYEN / NGUYEN / NGUYEN/HUYNH-THE / NAHAVANDI / NGUYEN / PHAM / NGUYEN, s. 1; BERK, s. 1511; ARSLAN, Fatih: “Deepfake Teknolojisi: Kriminolojik Bir Literatür Taraması”, *Sakarya Üniversitesi Hukuk Fakültesi Dergisi*, 2023, Cilt 11, Sayı 1, s. 702-703.

¹⁴ Üretken çekişmeli ağlar teknolojisi Ian Goodfellow tarafından 2014 yılında geliştirilmiş bir teknolojidir. Üretken çekişmeli ağlar (GAN) orijinal video görüntülerini bir eğitim seti olarak kullanır ve iki yazılım sinir ağı arasında, her birinin diğerinin çıktısına göre gelişeceği şekilde bir rekabet oluşturur. Bu şekilde *deepfake* içeriğindeki kusurların tespit edilip, iyileştirilmesi de mümkün olur. *Deepfake* içerikler elde etmek için, var olan veri setlerinden yeni veriler üretebilen bu ağlar sıklıkla kullanılmaktadır. Bkz. KUGLER / PACE, s. 620; VACCARI / CHADWICK, s. 2-3; MANKOO, s. 73; BAKER, Jennifer: *Deepfakes Could Break the Internet*, 2019 (<https://www.cpmagazine.com/cyber-security/deepfakes-could-break-the-internet/>, ET: 01.06.2025); NAGUMOTU, s. 104; YAVUZ, *Deepfake*, s. 46 vd.

¹⁵ Ayrıntılı bilgi için bkz. ÖZDEMİR, Şebnem: “Yeni Nesil Tehdit: Derin Kurgu (DeepFake)”, *TRT Akademi Dergisi*, 2021, Cilt 6, Sayı 13, s. 906-908.

¹⁶ BERK, s. 1511; ÖZDEMİR, s. 908 vd.; ARSLAN, s. 704 vd.; METZ.

¹⁷ KIETZMANN / LEE / MCCARTHY / KIETZMANN, s. 136; ÖZDEMİR, s. 906 vd.; NGUYEN / NGUYEN / NGUYEN / NGUYEN / HUYNH-THE / NAHAVANDI / NGUYEN / PHAM / NGUYEN, s. 1 vd.; ÇEBER, s. 13, 19, 20; MANKOO, s. 72-73; PAWELEC, s. 2; NAGUMOTU, s. 104 vd.; GERSTNER, Erik: “Face/Off: ‘DeepFake’ Face Swaps and Privacy Laws”, *Defense Counsel Journal*, 2020, Cilt 87, Sayı 1, s. 2 vd.; METZ; MASCA, Mehmet Emin: *Advantages and Disadvantages of Deepfake Technology*, 2021 (<https://medium.com/geekculture/advantages-and-disadvantages-of-deepfake-technology-ccfa7c12b1ae>, ET: 02.06.2025); ÇOLAK, Betül: *Legal Issues of Deepfakes*, 2021 (<https://www.internetjustsociety.org/legal-issues-of-deepfakes>, ET: 08.06.2025); YAVUZ, *Deepfake*, s. 36 vd.; BELADA, Nurullah Enes Süheyl: “Deepfake Dezenformasyonu”, *Bilişim Hukuku Dergisi*, 2024, Sayı 1, s. 323-326.

¹⁸ KIETZMANN / LEE / MCCARTHY / KIETZMANN, s. 138.

pay zekâ kümesinden oluşmaktadır¹⁹. Beyindeki nöronlar gibi her bir birim kendi başına oldukça basit bir hesaplama yaparak ve tüm birimler birlikte bir ekran üzerindeki pikselleri görerek belirli bir kişiyi tanıma gibi karmaşık ve doğrusal olmayan işlemleri gerçekleştirebilmektedir²⁰. Bu şekilde, görüntüler ve sesler üzerinde yapılan değişikliklerle oldukça gerçekçi görüntü ve ses dosyaları oluşturulabilmekte; örneğin bir kişinin yüzü başka bir kişinin vücuduyla birleştirilerek yepyeni içerikler üretilebilmektedir²¹. Ses ve görüntü üzerinde birlikte veya ayrı ayrı çalışılması mümkündür²². *Deepfake* yoluyla yüzün değiştirilmesi, ifade ve mimiklerin değiştirilmesi ya da yüzün yeniden oluşturulması veya yüksek kalitede ses sentezi yapılarak ses taklidi yoluyla yeni bir ses içeriği edilmesi oldukça kolaydır²³. Ayrıca var olmayan bir kişinin görüntülerinin ya da sesinin oluşturulması da (*sockpuppets*) mümkündür²⁴. Günümüzde yapay zekâ uygulamaları kullanılarak oluşturulmuş ve gerçekte var olmayan kişilere ilişkin bu tür *deepfake* video içeriklerine özellikle sosyal medya platformlarında sıklıkla rastlanmaktadır. Konuşma ve ses sentezi ise *deepfake*'in nispeten yeni bir dalı olup, bir kişinin sesinin bir modelini oluşturmayı, hedef kişiyle aynı üslup, tonlama ve tempoda ses ve konuşma elde edilmesini ve bu şekilde istenilen metnin okutulmasının sağlanmasını ya da yapay zekâ sentez ürünleri kullanarak her yaştan veya cinsiyetten belirli bir hedefi taklit etmeyen anonim ses içerikleri elde edilmesini sağlar²⁵.

B. Deepfake Teknolojisinin Temel Özellikleri

Deepfake yoluyla elde edilen görüntülerin ve seslerin gerçekçi olması için kullanılan özel yazılım, temelde iki algoritma üzerinden çalışmaktadır²⁶. Bu iki algoritmanın ilki bir yüz görüntüsünü/sesi yerleştirdiği içeriği defalarca kopyalamakta, ikincisi ise en gerçekçi ve inandırıcı içeriği tespit etmek için bir kalite algılaması kullanarak eleme yapmaktadır²⁷. İkna edici bir içeriğin oluşturulması için bu şekilde elde edilen üç yüz adet görüntü üzerinde çalışılmasının dahi yeterli olduğu ifade edilmektedir²⁸. Öte yandan referans görüntü olarak sadece bir tek fotoğrafa sahip olunması *deepfake* içeriğin üretimi için yeterli olabilmekte²⁹ ancak referans görüntü sayısı arttıkça daha gerçekçi sonuçlar elde edilebilmektedir³⁰. Kaynak olarak kullanılan fotoğraf ya da kamera görüntülerindeki yüz ifadesi sayısının çokluğu *deepfake* içeriği oluştururken daha iyi, daha kaliteli sonuçlar alınmasını sağlamaktadır³¹. Aynı zamanda yüksek performanslı bir bilgisayar, güçlü grafik ekran kartları veya yüksek bilgi işlem gücüne sahip bulut işlemcilerle sahip olmak, elde edilen içeriğin, oluşturma sürecini kısaltmakta, geliştirme ve işleme sürecini kolaylaştırmakta ve taşınabilirliğini artırmaktadır³².

Politikacılar, sanatçılar, sporcular gibi kamuya mal olmuş kişilerin çevrimiçi olarak çok sayıda video ve görseli bulunduğu, bu kimseler *deepfake* içerikler üretmek için sıklıkla hedef olarak

¹⁹ KIETZMANN / LEE / MCCARTHY / KIETZMANN, s. 138.

²⁰ KIETZMANN / LEE / MCCARTHY / KIETZMANN, s. 138.

²¹ KUGLER / PACE, s. 620; YAVUZ, *Deepfake*, s. 37 vd.; AKSOY RETORNAZ, E. Eylem: *Bir Siber Taciz Biçimi: Cinsel İçerikli Görüntüleri Rızaya Aykırı Olarak İfşa Etme, Yayma, Erişilebilir Kılma veya Üretme Suçu (Revenge Porn ve Deep Fake)*, On İki Levha Yayıncılık, İstanbul, 2021, s. 99; ÖZDEMİR, s. 906 vd.; ARSLAN, s. 702-703; ÇEBER, s. 19.

²² FARID, Hany / DAVIES, Alissa / WEBB, Lynette / WOLF, Clement / HWANG Tim / ZUCCONI, Alan / LYU, Siwei: *Deepfakes and Audio-visual Disinformation*, Centre for Data Ethics and Innovation (CDEI) Snapshot Series, United Kingdom, 2019, s. 4 vd.; ARSLAN, s. 704.

²³ FARID / DAVIES / WEBB / WOLF / HWANG / ZUCCONI / LYU, s. 4 vd.; VACCARI / CHADWICK, s. 3; BERK, s. 1512 vd.; ANIKAYDIN, İlayda: "Deepfake Uygulamalarının Hukuki Boyutu", *Düzce Üniversitesi Sosyal Bilimler Dergisi*, 2022, Sayı 2, s. 737-738; ÇEBER, s. 20; YAVUZ, *Deepfake*, s. 37 vd.; ÇOLAK.

²⁴ FARID / DAVIES / WEBB / WOLF / HWANG / ZUCCONI / LYU, s. 4 vd.; MANKOO, s. 75.

²⁵ FARID / DAVIES / WEBB / WOLF / HWANG / ZUCCONI / LYU, s. 6.

²⁶ AKSOY RETORNAZ, s. 100; ÖZDEMİR, s. 906 vd.

²⁷ AKSOY RETORNAZ, s. 100; ÖZDEMİR, s. 906 vd.

²⁸ ÇOLAK; ANIKAYDIN, s. 737; AKMEŞE, s. 78.

²⁹ ÇOLAK; ANIKAYDIN, s. 737.

³⁰ NGUYEN / NGUYEN / NGUYEN / NGUYEN / HUYNH-THE / NAHAVANDI / NGUYEN / PHAM / NGUYEN, s. 1; METZ.

³¹ FARID / DAVIES / WEBB / WOLF / HWANG / ZUCCONI / LYU, s. 4-6 vd.; ANIKAYDIN, s. 738.

³² MANKOO, s. 73-74; GERSTNER, s. 3-4.

karşımıza çıkmaktadır³³. *Deepfake* içerikler için kamuya mal olmuş kişiler öncelikle akla gelen hedefler olmakla birlikte diğer kişiler de pek çok farklı gerekçeyle hedef olabilmektedir³⁴. Günümüzde yapay zekâda ve gelişmiş yapay derin sinir ağlardaki ilerlemeler, manipüle edilmiş görüntü ve videoları oluşturma sürecini kolaylaştırdığından, kişinin kimlik fotoğrafı veya kısa videosu ile şaşırtıcı derecede ikna edici bir içerik oluşturmak mümkün hâle gelmiş, hatta yalnızca hareketsiz bir görüntüyle dahi *deepfake* içerik oluşturulabildiği için, *deepfake*, yalnızca tanınmış kişiler için değil, sıradan insanlar bakımından da bir tehdit hâline gelmiştir³⁵. Nitekim *deepfake* teknolojisini kullanan bazı uygulamalar (*Zao, FaceApp, FaceSwap, ReFaceApp, FaceMagic* vb.), kolaylıkla akıllı cep telefonlarına indirilip içerik üretilmekte ya da internet üzerinden ulaşılan bazı siteler vasıtasıyla (örn. *DeepFacelab*) oldukça kolay bir şekilde her tür içerik oluşturulması mümkün olabilmektedir³⁶.

Deepfake yoluyla elde edilen içeriğin gerçeklerinden ayırt edilmesi için bazı pratik çözümlere başvurulabilmektedir. Ses-video senkronizasyon sorunları, ısıklı ses, alışılmadık ağız ve dudak hareketleri, doğal olmayan göz ya da vücut hareketleri, yüz ifadeleri, saç görünümleri, ten rengi tonları arasındaki farklılıklar, garip görünen duruşlar, gölgenin oluşturduğu açıdaki farklılıklar, düşük kaliteli ses ve/veya görüntü, duygusuz vücut gibi bazı hususlar bir ölçüt olarak değerlendirilebilmektedir³⁷. Ancak *deepfake* yoluyla elde edilen görüntü ve/veya ses içerikleri ya da video kayıtları giderek daha yüksek kalitede ve daha gerçekçi olarak üretildiği için gerçek içeriklerden ayrılması da gittikçe güçleşmektedir³⁸.

C. *Deepfake* Teknolojisinin Tarihçesi ve Kullanım Alanları

Deepfake teknolojisi oldukça yeni bir teknoloji olup, ilk olarak 2017 yılında sosyal medyada gündeme gelmiştir³⁹. *Reddit* adlı sosyal medya platformunda “*DeepFake*” rumuzlu bir kullanıcı, Hollywood yıldızları ile porno yıldızlarının yüzlerini değiştirerek oluşturduğu videonun ve *deepfake* üretiminde kullanılabilecek kodların paylaşılması ile yankı uyandırmış, ardından bu işlemin yapılmasını mümkün kılan dijital uygulamalar yaygınlaşmış, *FakeApp* vb. uygulamalar internet ortamında ücretsiz olarak elde edilebilir hâle gelmiştir⁴⁰. *FakeApp*, Google tarafından herkes tarafından kullanılabilecek şekilde açık kaynak olarak sunulduktan sonra ilk iki ayında 120.000 kereden fazla indirilmiştir⁴¹. Artık silinmiş olan “*subredditr/deepfakes*”’in o dönemde yaklaşık 90.000 üyesinin olduğu ve ağırlıklı olarak çeşitli ünlü aktörlere ait pornografik *deepfake* içerikler barındırdığı görülmüştür⁴².

³³ NGUYEN / NGUYEN / NGUYEN / NGUYEN / HUYNH-THE / NAHAVANDI / NGUYEN / PHAM / NGUYEN, s. 1; BELADA, s. 330 vd.

³⁴ FARID / DAVIES / WEBB / WOLF / HWANG / ZUCCONI / LYU, s. 10.

³⁵ KIETZMANN / LEE / MCCARTHY / KIETZMANN, s. 137; NGUYEN / NGUYEN / NGUYEN / NGUYEN / HUYNH-THE / NAHAVANDI / NGUYEN / PHAM / NGUYEN, s. 2; ayrıca bkz. <https://www.ntv.com.tr/teknoloji/deepfake-tehlikesi-buyuyor-fotograf-karesinden-video-uretmek-artik-cokkolay, gqKbDHxjG0mkVnWyaGz Bag> (ET: 02.06.2025).

³⁶ FARID / DAVIES / WEBB / WOLF / HWANG / ZUCCONI / LYU, s. 11; KUGLER / PACE, s. 621; ARSLAN, s. 704; MANKOO, s. 73; NAGUMOTU, s. 107; GERSTNER, s. 2 vd.; BELADA, s. 329; “Sosyal medya uygulamaları *Snapchat* ve *TikTok* da *deepfake* teknolojisini platformlarına entegre etmiştir. Örneğin, Aralık 2019’da *Snapchat*, kullanıcıların *deepfake* video oluşturmak için bir video ortamına kendi resimlerini eklemelerine olanak tanıyan ‘*Cameos*’ adlı yeni bir araç duyurmuştur. Ancak bu özellikler genellikle kullanıcıların *deepfake* teknolojiyle yapabileceklerini sınırlamaktadır. Örneğin, *Cameos* özelliği kullanıcıların önceden ayarlanmış sahnelerle atlamasına ve altyazıları özelleştirmesine olanak tanımakta ve bunlar genellikle eğlenceli içerikler için tasarlanmaktadır.”. Bkz. KUGLER / PACE, s. 621.

³⁷ MANKOO, s. 74; ARSLAN, s. 706; BAKER.

³⁸ PAWELEC, s. 2; ARSLAN, s. 705-706; BELADA, s. 325-329.

³⁹ KIETZMANN / LEE / MCCARTHY / KIETZMANN, s. 136; FARID / DAVIES / WEBB / WOLF / HWANG / ZUCCONI / LYU, s. 4; KUGLER / PACE, s. 620; BERK, s. 1508-1512; ARSLAN, s. 702-703; ANIKAYDIN, s. 737; NGUYEN / NGUYEN / NGUYEN / NGUYEN / HUYNH-THE / NAHAVANDI / NGUYEN / PHAM / NGUYEN, s. 1; MANKOO, s. 72, 74; NAGUMOTU, s. 106; YAVUZ, *Deepfake*, s. 37; AKMEŞE, s. 78; BELADA, s. 325; ÇOLAK.

⁴⁰ KIETZMANN / LEE / MCCARTHY / KIETZMANN, s. 136; FARID / DAVIES / WEBB / WOLF / HWANG / ZUCCONI / LYU, s. 4; ANIKAYDIN, s. 737; KUGLER / PACE, s. 620; MANKOO, s. 72, 74; NAGUMOTU, s. 106; YAVUZ, *Deepfake*, s. 37; AKMEŞE, s. 78; BELADA, s. 325.

⁴¹ GERSTNER, s. 2; ANIKAYDIN, s. 737.

⁴² NAGUMOTU, s. 106.

Deepfake yoluyla elde edilen içerikler iyiniyetli ya da kötünüyetli kullanımlara konu olabilmekte⁴³, hukuka uygun ya da aykırı farklı amaçlar için kullanılabilir. *Deepfake* kullanıcıları toplumun her kesiminden olabilmektedir. Öğretmen ve akademisyenler, araştırmacılar, kurumsal, endüstriyel profesyoneller, reklamcılar ve film şirketleri, küçük ölçekten büyük ölçeğe görsel efekt stüdyoları, amatör meraklılar ya da fanatikler, siyasi aktörler gibi pek çok kesim tarafından tercih edilebilmektedir⁴⁴. Kullanım amaçları sanat, eğitim, sağlık, elektronik ticaret, reklamcılık⁴⁵, hobi ya da eğlence olabileceği gibi, siyasi oyunlar oynama, seçimleri yönlendirme ve çeşitli manipülasyonlar yapma⁴⁶, finansal kriz çıkarma, borsada ani düşüş ya da yükselişler oluşturma⁴⁷, cinsel istismar, cinsel içerikli veya pornografik videolar hazırlama, bunları satma, paylaşma, bu yolla gelir vb. menfaatler elde etme gibi amaçlar olabilir⁴⁸. *Deepfake* yoluyla hazırlanmış içeriklerin hukuka aykırı ve/veya suç niteliğinde kullanımı alanları oldukça geniş olup, internet ortamında asılsız bilgi yayma, algı oluşturma, dezenformasyon, itibarsızlaştırma, siber tehdit ve şantaj, dolandırıcılık⁴⁹, intikam pornosu, sosyal mühendislik, casusluk ve siber saldırılar, siber zorbalık⁵⁰, sahte delil üretimi ve biyometrik tanıma sistemlerinin aldatılması⁵¹ gibi pek çok farklı eylemle karşımıza çıkabilmektedir⁵². Uygulamada kötü amaçlı kullanımlarının sayısının, büyük ölçüde olumlu kullanımların sayısını aştığı ifade edilmektedir⁵³. Bu teknolojinin yaygınlaşması ve bu konuda uzman olan ve sorumluluğun bilincinde olan kişiler dışında herkes tarafından kolaylıkla kullanılabilir olması, kötü niyetli kullanımları kolaylaştırmakta ve *deepfake*'i günümüzün ve geleceğin en büyük tehditlerinden birine dönüştürmektedir⁵⁴.

Günümüzde gelişmiş bir endüstri hâline gelmiş olan *deepfake*, aslında insanlığın yararına kullanılabilecek bir teknolojidir ve oldukça faydalı kullanım alanları bulunmaktadır⁵⁵. Örneğin, film endüstrisinde kullanılan *deepfake* teknolojisi sayesinde aynı karakter, ana karakterin gençliğini veya yaşlılığını oynayabilmekte, farklı dilleri konuşabilmekte, eğitim alanında hazırlanan bir videoda *deepfake* kullanılarak yüzlerin ve seslerin simülasyonu yoluyla daha etkin, eğlenceli ve etkileşimli içerikler hazırlanabilmektedir⁵⁶.

⁴³ BERK, s. 1518; ARSLAN, s. 702-706; NGUYEN / NGUYEN / NGUYEN / NGUYEN / HUYNH-THE / NAHAVANDI / NGUYEN / PHAM / NGUYEN, s. 2; MANKOO, s. 73; NAGUMOTU, s. 124-125.

⁴⁴ MANKOO, s. 73; NAGUMOTU, s. 124-125.

⁴⁵ Ayrıntılı bilgi için bkz. ÇEBER, s. 19 vd.

⁴⁶ *Deepfake*'in siyasi amaçlı kullanımına ilişkin ayrıntılı bilgi için bkz. AJDER, Henry / PATRINI, Giorgio / CAVALLI, Francesco / CULLEN, Laurence: "The State of Deepfakes: Landscape, Threats, and Impact", *Deeptrace*, 2019, s. 9 vd.; ayrıca bkz. VACCARI / CHADWICK, s. 1 vd.; MENESES, João Paulo: *Deepfakes and the 2020 US elections: what (did not) happen*, 2021 (https://www.researchgate.net/publication/348740568_Deepfakes_and_the_2020_US_elections_what_did_not_happen, ET: 02.06.2025), s. 2 vd.; BERK, s. 1516-1517; ÖZDEMİR, s. 910 vd.; ANIKAYDIN, s. 738-739; NAGUMOTU, s. 110 vd. *Deepfake*'in oy kullanma davranışlarına ve demokrasiye etkileri konusunda ayrıntılı bilgi için bkz. PAWELEC, s. 13 vd.

⁴⁷ ANIKAYDIN, s. 739.

⁴⁸ AJDER / PATRINI / CAVALLI / CULLEN, s. 9-11 vd.; AKSOY RETORNAZ, s. 101; YAVUZ, Can: *Cinsel İçerikli Görüntülerin Rıza Dışı Paylaşımı-İntikam Pornosu*, Seçkin Yayıncılık, Ankara, 2021 (Rıza Dışı Paylaşım), s. 18; BERK, s. 1518; ÖZDEMİR, s. 913; ARSLAN, s. 703 vd.; MANKOO, s. 73, 75; BELADA, s. 327 vd.; MASCA.

⁴⁹ Ses üzerinde oynanarak hazırlanan *deepfake* kaydıyla yapılan bir dolandırıcılık örneği için bkz. DAMIANI, Jesse: *A Voice Deepfake Was Used to Scam a CEO Out of \$243,000*, 2019 (<https://www.forbes.com/sites/jessedamiani/2019/09/03/a-voice-deepfake-was-used-to-scam-a-ceo-out-of-243000/?sh=7de31b5c2241>, ET: 07.06.2025); ARSLAN, s. 707-708; ANIKAYDIN, s. 739.

⁵⁰ ARSLAN, s. 708-709; ANIKAYDIN, s. 740.

⁵¹ YAVUZ, *Deepfake*, s. 212 vd.

⁵² AJDER / PATRINI / CAVALLI / CULLEN, s. 9-13 vd.; ÖZDEMİR, s. 913; PAWELEC, s. 2 vd.; ARSLAN, s. 703, 707; MANKOO, s. 73; YAVUZ, *Deepfake*, s. 223 vd.; ayrıca bkz. GERSTNER, s. 12; KENT, Bülent: "Alman Hukukunda Sosyal Ağlarda Yalan Haber ile Mücadele", (Ed.) KENT, Bülent / KULULAR İBRAHİM, Merve Ayşegül: *Sosyal Medya Hukuku ve Yalan Haber*, Adalet Yayınevi, Ankara, 2022, s. 12.

⁵³ NGUYEN / NGUYEN / NGUYEN / NGUYEN / HUYNH-THE / NAHAVANDI / NGUYEN / PHAM / NGUYEN, s. 2.

⁵⁴ ARSLAN, s. 705.

⁵⁵ MANKOO, s. 75; ARSLAN, s. 705; ANIKAYDIN, s. 741; ÇEBER, s. 19 vd.; NAGUMOTU, s. 124-125; YAVUZ, *Deepfake*, s. 67 vd.; REES, Geraint: *Here's How Deepfake Technology Can Actually Be a Good Thing*, 2019 (<https://www.weforum.org/agenda/2019/11/advantages-of-artificial-intelligence/>, ET: 03.06.2025); MASCA.

⁵⁶ BERK, s. 1518-1519; ARSLAN, s. 704-705; ayrıntılı bilgi için bkz. YAVUZ, *Deepfake*, s. 70 vd.; MASCA.

II. GÖRÜNTÜ VE SES ÜZERİNDEKİ KİŞİLİK HAKKI

A. Görüntü (Resim, Fotoğraf, Video vb.) Üzerindeki Kişilik Hakkı

Kişinin görüntüsü, kişilik hakkının önemli bir parçası olan bir kişilik değeri olup, bu kişilik değerinin kişiyi diğer kişilerden ayırt etme ve bu şekilde tanınmasını sağlama adına belirgin ve önemli bir işleve sahip olduğu ve aynı zamanda kişisel veri niteliği taşıdığı görülür⁵⁷. Görüntü kavramı aslında oldukça geniş bir kavram olup resim, fotoğraf, video, öz çekim, karikatür, heykel hatta kişinin bir şekilde bir ekranda ya da bir nesne üzerinde beliren görünüşü dahi görüntü kapsamında değerlendirilir⁵⁸. Görüntü üzerindeki kişilik hakkı kapsamında korunan şey esasen görüntünün üzerinde olduğu nesne değil, bizzat görüntünün kendisidir⁵⁹. Görüntü, tanınmaya elverişli şekilde bir açıklığa sahip olduğunda, bir kişilik değeri olarak korunmaya başlar⁶⁰. Kişinin görüntüsü üzerinde kolaylıkla oynanabilmesi ve gerek sosyal paylaşım sitelerinde gerekse diğer sosyal medya platformlarında sıklıkla paylaşıp, hızlı bir şekilde yayılabilmesi ona özel bir önem verilmesini haklı kılmaktadır⁶¹.

Başkasına ait bir görüntünün alınması, bir fotoğrafın çekilmesi hukuka uygun olsa dahi bu durum görüntünün özgürce paylaşılabilmesi anlamına gelmez. Görüntü sahibi yayınlanmasına, paylaşılmasına açık ya da örtülü olarak rıza vermedikçe ilgili yayın ya da paylaşım hukuka aykırı olur⁶². Kişinin sosyal medyada veya genel olarak internet ortamında rızasıyla paylaştığı veya kamuya mal olması hasebiyle haber vs. olarak paylaşılan bir görüntüsü veya video kaydından bu paylaşımının *deepfake* yoluyla işlenmesine razı olduğu sonucuna veya böyle bir işlemeyi göze alması ya da katlanması gerektiği gibi bir sonuca ulaşılamaz. Öte yandan *deepfake* yoluyla oluşturulan video kaydı, görüntüleri kullanılan kişilerin rızası alınarak oluşturulsa dahi onların rızası olmaksızın yayınlanması, internet ortamında paylaşılması hukuka aykırıdır. Somut olaya göre kişinin açık veya örtülü olarak rızası, üstün kamu yararı, kamunun haber alma özgürlüğü ve menfaati, yargı menfaati, kamu düzeni, bilime hizmet ve bilimsel amaçlı kullanım⁶³ gibi hukuka uygunluk nedenleri kişinin görüntüsüne ilişkin kişilik hakkı

⁵⁷ İMRE, Zahit: “Şahsiyet Haklarından Şahsın Özel Hayatının ve Gizliliklerinin Korunmasına İlişkin Meseleler”, *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası*, 1974, Cilt 39, Sayı 1-4, Ord. Prof. Dr. Siddık Sami Onar Hatıra Sayısı, s. 163; ÖZTAN, Bilge: *Kişiler Hukuku Gerçek Kişiler*, 11. Baskı, Yetkin Yayınları, Ankara, 2021, s. 289; OĞUZMAN, Kemal / SELİÇİ, Özer / OKTAY ÖZDEMİR, Saibe: *Kişiler Hukuku (Gerçek ve Tüzel Kişiler)*, 17. Baskı, Filiz Kitabevi, İstanbul, 2018 s. 194; ZEVKLİLER, Aydın / ERTAŞ, Şeref / HAVUTÇU, Ayşe / ACABEY, M. Beşir: *Yeni Medeni Kanun'a Göre Medeni Hukuk (Temel Bilgiler)*, 10. Baskı, Turhan Kitabevi, Ankara, 2018, s. 99; ANTALYA, O. Gökhan / TOPUZ, Murat: *Marmara Hukuk Yorumu Medeni Hukuk Giriş Temel Kavramlar Başlangıç Hükümleri Cilt I*, 4. Baskı, Seçkin Yayıncılık, Ankara, 2021, s. 165; ÖZEL, Sibel: *Uluslararası Alanda Medya ve İnternette Kişilik Hakkının Korunması*, Seçkin Yayıncılık, Ankara, 2004, s. 33; OĞUZ, Habip: *İnternet Ortamında Kişilik Haklarının İhlali ve Korunması*, Adalet Yayınevi, Ankara, 2010, s. 20; ARAS, Ümit Yaşar: *İnsan Hakları Temelinde Özel Hayat Hakkının Ulusal ve Uluslararası Alanda Uygulamaları*, Yüksek Lisans Tezi, Bahçeşehir Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2010, s. 27; YÜNLÜ, Semih: *Görüntü Üzerinde Kişilik Hakkı*, 2. Baskı, On İki Levha Yayıncılık, İstanbul, 2023 (Görüntü), s. 114 vd.; TURGUT, Cemile: *Kişilik Hakkının Bir Görünümü Olarak Unutulma Hakkı*, On İki Levha Yayıncılık, İstanbul, 2021, s. 144; ayrıca bkz. YILDIZ, Ozan Ali: “Kişinin Görüntüsü Üzerindeki Hakkın Korunması”, *Fikri Mülkiyet Hukuku Kronikleri*, 2022, Sayı 1, s. 3.

⁵⁸ OĞUZMAN / SELİÇİ / OKTAY ÖZDEMİR, s. 194; ÖZTAN, s. 289, 292; ZEVKLİLER / ERTAŞ / HAVUTÇU / ACABEY, s. 99; KILIÇOĞLU, Ahmet M.: *Medeni Hukuk Temel Kavramlar Başlangıç Hükümleri Kişiler Hukuku*, 4. Baskı, Turhan Kitabevi, Ankara, 2021, s. 309, 310; ANTALYA/TOPUZ, s. 165; AYAN, Mehmet / AYAN, Nüşen: *Kişiler Hukuku Genel Bilgiler Gerçek Kişiler Tüzel Kişiler*, 9. Baskı, Adalet Yayınevi, Ankara, 2020, s. 102; ERDOĞAN, İhsan / KESKİN, A. Dilşad: *Türk Medeni Hukuku Başlangıç Hükümleri Kişiler Hukuku*, 3. Baskı, Gazi Kitabevi, Ankara, 2020, s. 287-288; ACABEY, Mehmet Beşir: “Basın Özgürlüğü ve Bu Özgürlüğün Bir Sınırı Olarak Kişilik Hakkı”, *Yaşar Üniversitesi E-Dergisi*, 2013, Cilt 8, Özel Sayı, s. 31-32; ÖZEL, s. 33; ARAS, s. 27; TURAN BAŞARA, Gamze: *Kişiliğin İhlalinden Kaynaklanan Maddi ve Manevi Tazminat ile Haksız Kazancın İadesi*, Turhan Kitabevi, Ankara, 2018, s. 31; OĞUZ, s. 20; KAYA, Mine: “Telekomünikasyon Alanında Kişilik Haklarının Korunması”, *Ankara Barosu Dergisi*, 2010, Sayı 4, s. 283-284; AKKURT, Sinan Sami: *Sosyal Medyada Gerçekleşen İhlaller Karşısında Kişilik Hakkının Korunması*, 2. Baskı, Seçkin Yayıncılık, Ankara, 2020, s. 59; AKSOY RETORNAZ, s. 98-99; YÜNLÜ, *Görüntü*, s. 115; TURGUT, s. 144. Karikatür konusundaki değerlendirmeler için bkz. ÖZTAN, s. 292-293.

⁵⁹ ARAS, s. 27; OĞUZ, s. 20.

⁶⁰ ÖZTAN, s. 289; KILIÇOĞLU, s. 309.

⁶¹ MÜLLER TERPITZ, Ralf: “Persönlichkeitsrechtliche Aspekte der Social Media”, (Ed.) HORNUNG, Gerrit / MÜLLER TERPITZ, Ralf: *Rechtshandbuch Social Media*, 2. Baskı, Springer, Deutschland, 2021, s. 261-262; NAGUMOTU, s. 117 vd.

⁶² DURAL, Mustafa / ÖĞÜZ Tufan: *Türk Özel Hukuku Cilt II Kişiler Hukuku*, 19. Baskı, Filiz Kitabevi, İstanbul, 2018, s. 141; ÖZTAN, s. 291; SOLMECKE, Christian: *Social Media Recht-Rechtssicher in sozialen Netzwerken unterwegs*, TeleLex, 2015, s. 35; YÜNLÜ, *Görüntü*, s. 117.

⁶³ Bilimsel amaçlı kullanımlarda kişinin tanınmasına engel olan ve mümkün mertebe kimliğini gizleyici tedbirler alınması gerektiği yönünde bkz. TURAN BAŞARA, s. 34.

ihlalini kural olarak ortadan kaldırmakla birlikte⁶⁴, yapay zekâ ile üretilen sahte içerikler yani *deepfake* içerikler bakımından bu nedenlerin dikkatle ele alınması gerektiği açıktır.

1. Rıza ile *Deepfake* Görüntülerinin Paylaşımı

Kişi, görüntüsünün kullanılıp işlenmesine ve bu yolla bir *deepfake* içerik hazırlanmasına bizzat kendisi razı olmuş olabilir. Hukuken geçerli bir rıza olduğu sürece bu tür bir içerik hazırlanmasında herhangi bir sorun yoktur. Ancak bu durumda görüntünün entegre edildiği diğer bir kişiye ait olduğu tespit edilebilen bir görüntü varsa, bu görüntü sahibinin de hukuken geçerli rızasının alınması gerekir. Rıza açık ya da örtülü, ivazlı ya da ivazsız olarak verilebilir⁶⁵. *Deepfake* içerikler için alınan rızanın özellikle kişilik hakkına, hukuka, ahlaka ve adaba aykırı olmamasına dikkat edilmesi gerekir. Kişinin görüntüsü üzerindeki kişilik hakkı onun hukuki sınırlar içinde görüntüsünün başkaları tarafından kullanılmasına rıza vermesi hakkını da içermektedir. Kişi görüntüsünün ya da sesinin kullanılmasına ve işlenmesine razı olsa dahi, verdiği rızanın sınırları aşılarak bir kullanma veya işleme söz konusuysa, bu şekilde yayın veya paylaşımlarda bulunuluyorsa, bu tür eylemler kişilik hakkına ve hukuka aykırıdır⁶⁶. Bilgi ya da eğlence amaçlı olarak verilen görüntü alma ya da paylaşma izni, bu iznin sınırları aşılarak başka amaçlar için kullanıldıysa örneğin çekilen düğün fotoğrafı ya da videosu daha sonra reklam amaçlı kullanılmışsa eylem hukuka aykırıdır ve kişilik hakkının ihlali söz konusu olur⁶⁷. Aynı şekilde bu tür bir görüntünün *deepfake* yoluyla işlenerek farklı amaçlarla kullanılması, elde edilen içeriğin internet ortamında paylaşılması görüntüye ilişkin kişilik değeri yanında somut olaya göre şeref ve haysiyet, özel hayatın gizliliği gibi birçok kişilik değerini ihlal edebilir. İnternet ortamında yer alan içeriğin *deepfake* yoluyla üretildiğinin ve sahte olduğunun açıkça belirtildiği veya herkes tarafından kolayca anlaşılabilir olduğu durumda kamuoyunun bu duruma yaklaşımının ne olduğuna ilişkin yeterli veri ya da bilimsel çalışma olmamakla birlikte⁶⁸, bu tür bir içerikte kişinin rızası olmaksızın görüntüsünün ve/veya sesinin kullanılmasının, kişilik hakkının ihlal edildiği sonucuna ulaşılması için yeterli olduğu görülmektedir.

2. Kamuya Mal Olmuş Kişilerin *Deepfake* Görüntüleri

Kamuya mal olmuş kişiler, çoğunlukla *deepfake* içeriklerin öncelikli hedefleri olarak karşımıza çıkmaktadır. Kamuya mal olmuş kimselerin rızaları olmaksızın görüntülerin alınmasında, kaydında ve paylaşılmasında kural olarak üstün kamu yararı sebebiyle bir hukuka uygunluk olduğu kabul edilir. Ancak bu kimselerin de rızaları olmadan kullanılması kişilik hakkının ihlali anlamına gelebilecek görüntüleri söz konusu olabilir. Örneğin kişinin görüntüsü kamuyu ilgilendirmiyorsa, yaptığı işle, tanınıp bilindiği konuyla tamamen ilgisizse, gerçek değilse, kamunun haber alma hakkının, basın özgürlüğünün sınırlarını aşıyorsa, bu tip görüntülerin alınmasında, kaydında, basında veya internet ortamında yayınlanmasında üstün kamu yararı olduğundan bahsedilemez. *Deepfake* yoluyla oluşturulan ve bir bütün olarak ele alındığında gerçeklik taşımayan, başka görüntülerin entegre edilmesi yoluyla elde edilmiş kayıtların, örneğin ünlü bir kimsenin porno filme entegre edilmiş yüz görüntüleriyle elde edilen videoların yayın ve paylaşımı kişilik hakkını ihlal eder ve hukuka aykırıdır. Kamuya mal olmuş ünlü kişilerin görüntülerinin kaydı, yayını ve internet ortamında paylaşılması bakımından kural olarak daha ılımlı bir hukuki yaklaşım sergilense de *deepfake* ile oluşturulan bu tür içerikler bakımından durumun farklı değerlendirilmesi gerekir. Bu kimselerin ister yüzleri isterse tanınabilecekleri vücut görüntüleri kullanılarak üretilsin, *deepfake* yoluyla üretilmiş cinsel içerikler bakımından kamuya mal olmuş olmanın sonuçlarına katlanmaları beklenemez.

⁶⁴ İMRE, s. 167, 168; DURAL / ÖĞÜZ, s. 141-142; ÖZTAN, s. 292; ARAS, s. 28; TURAN BAŞARA, s. 33; YÜNLÜ, *Görüntü*, s. 208 vd.

⁶⁵ DURAL / ÖĞÜZ, s. 141; ÖZTAN, s. 292; SOLMECKE, s. 35.

⁶⁶ DURAL / ÖĞÜZ, s. 141; ÖZTAN, s. 291-292; TURAN BAŞARA, s. 32.

⁶⁷ DURAL / ÖĞÜZ, s. 141; ÖZTAN, s. 291-292. Fotoğrafçı tarafından çekilen evlilik fotoğraflarının, kişilerin bilgisi ve rızası olmaksızın işyeri vitrininde ve internet sitesinde ticari/reklam amaçlı sergilenmesinin kişilik hakkının ihlaline yol açabileceği yönünde bkz. Yargıtay, 12. CD, T. 11.04.2012, E. 2011/20872, K. 2012/9834 (YÜRTCAN, Erdener: *Yargıtay Kararları Işığında Özel Hayata Karşı Suçlar*, Adalet Yayınevi, Ankara, 2016, s. 67-69).

⁶⁸ KUGLER / PACE, s. 615.

B. Ses Üzerindeki Kişilik Hakkı

Ses, kişilik hakkının kapsamındaki kişilik değerlerinden biridir. Ses de görüntü gibi kişiye ait olduğu tespit edilebildiği ölçüde kişiliğin bir parçası olarak görülür ve bir değer olarak kişilik hakkının koruma alanına girer⁶⁹. Kişinin rızası ya da diğer hukuka uygunluk sebepleri bulunmadıkça sesin bir şekilde dinlenmesi, kaydedilmesi, elde edilen kaydın aynı şekilde veya teknik yöntemlerle işlenerek, üzerinde bazı değişiklikler yapılarak yayınlanması, internet ortamında paylaşılması bu kişilik değerini ihlal eder ve kişilik hakkına ve hukuka aykırılık teşkil eder⁷⁰. İhlalin gerçekleşmesi bakımından sesin nerde yayınlandığının, internet ortamındaki hangi sitede veya platformda paylaşıldığının bir önemi yoktur. Ancak bu husus tazminatın miktarının belirlenmesinde etkili olabilir⁷¹.

Deepfake ses içeriği herhangi bir görüntüyle bütünleşmiş şekilde oluşturulabileceği gibi yalın bir şekilde sadece ses olarak da üretilebilir. Sosyal medyada ve genel olarak internet ortamında yer alan *deepfake* içerikler çoğunlukla bir video şeklinde olup, kişinin kendi sesi veya başka bir ses bu videoya entegre edilmekte, sesin görüntüye ilişkin kişilik değeriyle birlikte ihlaline sıklıkla rastlanmaktadır. *Deepfake* yoluyla oluşturulan içerikte, kişinin videoya entegre edilen sesi, kişiye ait başka ses dosyalarından kesitler alınarak oluşturulsa da kişilik hakkı ihlal edilmiş olur. Bu ses dosyaları kişinin kamuya açık paylaşımlarından, eğer kamuya mal olmuş ünlü bir kişiye, bu kişiye ait mevcut yayınlardan elde edilmiş olabilir. Kullanılan ses ayrıca kişinin sosyal medya platformlarında sadece belli bir kişiyle veya belli bir kullanıcı grubuna yönelik yaptığı sesli paylaşımlardan, *WhatsApp*, *Telegram* vb. platformlarda yapılan sesli mesajlaşmalardan da elde edilmiş olabilir.

Ses üzerindeki kişilik hakkı ihlal edilirken, bu ihlalin, görüntü yanında diğer kişilik değerlerine ilişkin ihlaller de barındırması mümkündür. Özellikle somut olaya göre özel hayatın gizliliği ve şeref ve haysiyet gibi kişilik değerlerinin ihlal edilmesi söz konusu olabilir. Kişinin sesinin hukuken korunması aynı zamanda bir kişisel veri olmasına ve özel hayatın gizliliği kapsamında yer alabilmesine dayanır⁷². Sesin hukuka aykırı biçimde dinlenmesi, konuşmaların kayda alınması, kaydedilen sesler üzerinde teknolojik yöntemlerle değişiklikler yapılarak kişinin başta sesi olmak üzere, şeref ve haysiyetine, özel hayatının gizliliğine ya da diğer kişilik değerlerine saldırıda bulunulması, hukuka uygunluk sebepleriyle meşru kılınmadıkça, kişilik hakkı ihlaline yol açar, hukuki ve cezai yaptırımlarla karşılaşılmasına neden olur⁷³. Kişinin rızası olmaksızın kaydedilen sesi, herhangi bir teknolojik işleme tabi tutulmasa, *deepfake* vb. yöntemlerle hukuka aykırı içerikler elde etmek için kullanılsa dahi yapılan eylem, ses üzerindeki kişilik hakkı ihlaline yol açar. Aynı şekilde kişinin rızası olmaksızın sesinin kaydedilmesi, şeref ve haysiyetine saldırı veya herhangi başka bir hukuka aykırı amaçla olmasa dahi kişilik hakkının ihlal edildiği sonucunu değiştirmez⁷⁴. Sese yönelik ihlal için kaydedilen sesin, kişiyi aşağılayan, rencide eden bir şekilde kullanılmasına da lüzum yoktur. Kaydedilen sesin ticari amaçlarla, örneğin ünlü bir kimsenin sesinin reklam içeriği oluşturmak için kullanılması hâlinde yine bu kişilik değerine saldırıda bulunulmuş olur⁷⁵. Ses kaydının hukuka aykırı şekilde kaydedilmesi kişilik hakkına bir saldırı olmakla birlikte bu kayıtların yayınlanması, internet ortamında paylaşılması yoluyla

⁶⁹ OĞUZMAN / SELİÇİ / OKTAY ÖZDEMİR, s. 196; ÖZTAN, s. 293; KILIÇOĞLU, s. 312; ANTALYA, O. Gökhan: *Manevi Zararın Belirlenmesi ve Manevi Tazminatın Hesaplanması-Türk Hukukunda Manevi Tazminatın İki Aşamalı Olarak Belirlenmesine İlişkin Bir Model Önerisi*, Legal Yayıncılık, İstanbul, 2017, s. 128-129; KAYA, s. 284; TURAN BAŞARA, s. 36; AKKURT, s. 66; YÜNLÜ, *Görüntü*, s. 118-120; TURGUT, s. 144.

⁷⁰ OĞUZMAN / SELİÇİ / OKTAY ÖZDEMİR, s. 196; KILIÇOĞLU, s. 312; ANTALYA, s. 128-129; ERDOĞAN / KESKİN, s. 288; ACABEY, s. 27; KAYA, s. 284; TURAN BAŞARA, s. 63; AKKURT, s. 66-67; YÜNLÜ, *Görüntü*, s. 120.

⁷¹ ANTALYA, s. 129.

⁷² ANTALYA, s. 129; KAYA, s. 284; YÜNLÜ, *Görüntü*, s. 118-119.

⁷³ OĞUZMAN / SELİÇİ / OKTAY ÖZDEMİR, s. 196; ANTALYA, s. 129; ACABEY, s. 26-27; YÜNLÜ, *Görüntü*, s. 118-120; ayrıca bkz. Yargıtay, HGK, T. 26.11.2014, E. 2013/4-1183, K. 2014/960 (Yargıtay Karar Arama).

⁷⁴ OĞUZMAN / SELİÇİ / OKTAY ÖZDEMİR, s. 196; ACABEY, s. 27; TURAN BAŞARA, s. 36; Yargıtay, 4. HD, T. 26.10.2007, E. 13723, K. 13089 (YURTCAN, s. 11-12).

⁷⁵ KILIÇOĞLU, s. 312-313.

kamuya açık hâle getirilmesi kişilik hakkına yapılan bir diğer saldırı olarak kabul edilebilir. Yargıtay da bu tür eylemleri kişilik hakkına yapılan ikinci bir saldırı olarak kabul etmektedir⁷⁶.

III. DEEPFAKE TEKNOLOJİSİ İLE GERÇEKLEŞTİRİLEBİLEN İHLALLER VE HUKUKİ ÇÖZÜM YOLLARI

A. Genel Olarak

Deepfake, internet ortamında rahatlıkla ulaşılabilen, farklı platformlarda ücretsiz olarak sunulabilen ve herkesin kolaylıkla kullanabileceği bir teknoloji olduğu için, bu yolla görüntü ve/veya ses dosyaları oluşturmak da oldukça kolay olup, bunun için internet bağlantısı olan bilgisayar, akıllı cep telefonu vb. bir cihaza sahip olmak yeterlidir⁷⁷. Hukuka aykırı içerikler oluşturmak için gereken görüntü ve ses içeriği ya da verisi birçok farklı yoldan elde edilebilir. Kaynak veri de diyebileceğimiz bu veriler, genel olarak internet ortamından, sosyal medya platformlarından, sosyal paylaşım sitelerinde yer alan kişilerin profil fotoğraflarından veya paylaştıkları diğer fotoğraflarından ya da kamera kayıtlarından, WhatsApp, Telegram gibi platformlarda yapılan kamuya açık her tür görüntülü paylaşımlardan elde edilebilmekte ve hatta bazı platformlar sırf bu amaçla kullanılabilmektedir⁷⁸. İnternet ortamında *deepfake* videoların sayısındaki artış, *deepfake* öznelere ve genel olarak toplum üzerindeki potansiyel olumsuz etkilere dikkati çekmekte, bu konudaki çalışmalar özellikle iki noktaya; hukuka aykırılık ve doğan zararlar noktasına odaklanmaktadır⁷⁹. Hukuka aykırılığın ve zararların bir kısmı *deepfake* öznesinin özel hayatına, şeref ve haysiyetine, görüntüsü, sesine, duygusal refahına ve diğer kişilik değerlerine ilişkin iken, bir kısmı da siyasi hayata, ulusal güvenliğe ve demokratik kurumlara ilişkindir⁸⁰. Bu noktada uygulamada *deepfake* yoluyla sıklıkla gerçekleşen bazı dikkat çekici saldırıları ayrı başlıklar hâlinde inceleyip konunun ciddiyetini ortaya koyduktan sonra teknik ve hukuki sorunlara ve çözümlere değineceğiz.

B. Kamuya Mal Olmuş Kişilere Yönelik Saldırılar

Deepfake yoluyla oluşturulan hukuka aykırı içeriğin mağdurlarının özellikle kamuya mal olmuş ünlü kişiler, kadınlar başta olmak üzere kadın veya erkek mağdurlar olabildiği, *Emma Watson*, *Natalie Portman*, *Gal Gadot*, *Taylor Swift*, *Scarlett Johansson*, *Nicholas Cage*, *Barack Obama*, *Nancy Pelosi*, *Donald Trump*, *Vladimir Putin* gibi birçok kamuya mal olmuş kişinin bu mağdurlardan bazıları olduğu görülmektedir⁸¹. Ünlü kişilerin, özellikle film yıldızı, manken ya da siyasetçilerin uygunsuz içerikli videoları ya da gerçekle ilgisi olmayan konuşma veya davranışlarını içeren görüntü ve ses dosyaları oluşturularak⁸² kişilik hakkı ihlali edilmekte ve birçok farklı türde suç işlenmektedir⁸³. Kamuya mal olmuş kişilere ait bu tip içeriklerin sahte olduğu kolaylıkla ve tam bir doğrulukla tespit edilebilse bile, her zaman ve her durumda sosyal medya platformlarından kaldırılmalarının gerekip gerekmediği, bun-

⁷⁶ Yargıtay, 4. HD, T. 26.10.2007, E. 13723, K. 13089 (YURTCAN, s. 11-12); Yargıtay, 4. HD, T. 23.06.2010, E. 8119, K. 7573 (YURTCAN, s. 9-11).

⁷⁷ AKSOY RETORNAZ, s. 100.

⁷⁸ AKSOY RETORNAZ, s. 100; YAVUZ, *Rıza Dışı Paylaşım*, s. 44-45; YAVUZ, *Deepfake*, s. 194 vd.; NAGUMOTU, s. 117 vd.

⁷⁹ KUGLER / PACE, s. 623.

⁸⁰ KUGLER / PACE, s. 623.

⁸¹ YAVUZ, *Rıza Dışı Paylaşım*, s. 18; MANKOO, s. 72-76; ayrıca bkz. KUGLER / PACE, s. 626-627; ARSLAN, s. 709-710; BELADA, s. 330 vd. Yapılan analizlere göre Temmuz 2019 itibarıyla *deepfake* içeriklerin hedeflerinin büyük çoğunluğunun (%95'in üzerinde) eğlence sektörüyle ilgili olduğu görülmektedir. Hedeflerin geri kalan küçük bir yüzdesi iş dünyasından, haber medyasından ve politikadan gelmektedir. Haziran 2020 itibarıyla ise eğlence %62,7 ile hâlâ en çok hedeflenen sektör olmaya devam etmiş, moda (%21,7) ve spor (%4,4) kategorileri tüm hedeflerin toplamında %88,9'unu oluşturmuştur. Bkz. AJDER, Henry: *Deepfake Threat Intelligence: A statistics snapshot from June 2020*, 2020 (<https://perma.cc/ZHW5-53U7>, ET: 01.06.2025).

⁸² MANKOO, s. 71 vd.; BERK, s. 1512.

⁸³ Örneğin Hollanda'da yaşanan bir olayda televizyon sunucusu gazeteci bir kadının yüzü, *deepfake* yoluyla porno içeriğe entegre edilmiş, Amsterdam savcılığı, şüphelinin "sahte cinsel içerikli görüntü oluşturmak ve yaymak" suçundan yargılanacağını duyurmuştur. Habere ilişkin bkz. <https://tr.euronews.com/2023/07/30/hollanda-tv-sunucusunun-yuzuyle-deepfake-teknolojisi-kullanarak-porno-ureten-zanli-yargila> (ET: 06.06.2025).

ların dezenformasyona yol açan kötü niyetle hazırlanmış içerikler olarak mı yoksa eleştiri sınırları dahilinde kalan bir hiciv niteliğinde mi görüleceği hususu tartışmalıdır⁸⁴. Bazı sosyal medya platformları kendilerine gelen kaldırma taleplerini topluluk kurallarına aykırı olmadığı gerekçesiyle olumsuz cevaplamaktadır⁸⁵. Bu durumda yargı makamları devreye girmedikçe, söz konusu içeriklerin hukukçu olmayan ya da objektif değerlendirme yapmaktan uzak kimselerce değerlendirilmesi, esasen hukuki bir önem arz etmemektedir. Kamuya mal olmuş kişilerin, görüntü, ses, özel hayatın gizliliği, şeref ve haysiyet gibi kişilik değerlerini hiçe sayan, eleştirileri sınırlarını aşan ve üstün kamu yararı sebebiyle hukuka uygun olduğunun kabul edilmesi mümkün olmayan *deepfake* içeriklere karşı hukukten korunmaları gerektiğine şüphe yoktur. Ayrıca kamuya mal olmuş kişilerin haberleri dahi olmaksızın *deepfake* içerikli reklam videolarının hazırlanması ve özellikle sosyal medya platformlarında yayınlanarak bunlar üzerinden haksız kazanç elde edilmesi, uygulamada sıklıkla yaşanan bir durum olup, gün geçtikçe mağdurların sayısı artmaktadır. Bu durum ilerde değineceğimiz *deepfake* ile ilgili hukuki çözüm yollarının gerekliliğini bir kez daha ortaya koymaktadır.

Bu noktada ayrıca belirtmek gerekir ki *deepfake* içerikler sadece kamuya mal olmuş kişiler için tehdit olmaktan çıkmış, herkesi ilgilendiren bir tehdide dönüşmüştür. Günümüzde sosyal medya bir görüntü ve ses deposuna dönüştüğü için ünlü olmayan kişilerin dahi sosyal paylaşım sitelerinde ve diğer sosyal medya platformlarında paylaşmış oldukları sıradan bir fotoğraf, hiç ummadıkları bir şekilde bir kamera görüntüsü, bir film olarak karşılarına çıkabilmekte, örneğin cinsel içerikli bir filme gerçekçi bir şekilde işlenip, filmde oynayan kişinin o olduğuna şüphe bırakmayacak şekilde internet ortamında paylaşılabilir⁸⁶. Örneğin Telegram gruplarındaki bir uygulama yoluyla giyinik olan kadınlara ait görüntülerin çıplak hâle getirildiği ve 2019-2020 yılları arasında (Temmuz-Haziran) bu şekilde en az 104.000 kadın görüntüsünün üzerinde işlem yapılarak çıplak görüntülere dönüştürüldüğü belirlenmiştir⁸⁷. Telegram’da yer alan bu gruplara kayıtlı olanların, o dönemde (Haziran 2020) en az 45.000 kişi olduğu tahmin edilmektedir⁸⁸. Yine Temmuz 2019’dan Haziran 2020’ye kadar, internette bulunan *deepfake* videoların sayısında yüzde 330’un üzerinde bir artış olduğu görülmekte, çevrimiçi *deepfake* video sayısının 14.678’den 49.081’e yükseldiği ifade edilmektedir⁸⁹.

C. Devletler ya da Kamu Tüzel Kişilerine Yönelik Saldırıları

Deepfake yoluyla hazırlanan içerikler sadece gerçek kişileri ilgilendirmemekte, devletler ve kamu tüzel kişileri için de ciddi tehditler oluşturabilmektedir⁹⁰. Bu şekilde elde edilen ses içerikleri gizli bilgilere ulaşma, başkalarının öğrenilmesi tehlikeli olan sırları ele geçirme gibi amaçlarla kullanılabilir⁹¹, görüntü içerikleri sahte sosyal medya hesaplarında profil resmi olarak kullanılabilir ve hazırlanmış *deepfake* videolarla örgütlü siyasal manipülasyonlar yapılabilir⁹². *Deepfake* içerikler kurumların itibarını zedelemek ve diplomatik ilişkilere zarar vermek amacıyla da kullanılabilir, uygulamada bununla ilgili birçok örneğe rastlanmaktadır⁹³. Siyasi *deepfake* videoların seçimlere müdahale etme, ulusal güvenliğe zarar verme ve demokratik kurumları zayıflatma potansiyeli hakkında duyulan endişe gide-

⁸⁴ FARID / DAVIES / WEBB / WOLF / HWANG / ZUCCONI / LYU, s. 15.

⁸⁵ FARID / DAVIES / WEBB / WOLF / HWANG / ZUCCONI / LYU, s. 15.

⁸⁶ KUGLER / PACE, s. 623; YAVUZ, *Deepfake*, s. 188 vd.; AKSOY RETORNAZ, s. 101.

⁸⁷ KUGLER / PACE, s. 613; YAVUZ, *Rıza Dışı Paylaşım*, s. 45; YAVUZ, *Deepfake*, s. 195.

⁸⁸ YAVUZ, *Rıza Dışı Paylaşım*, s. 45.

⁸⁹ AJDER; KUGLER / PACE, s. 613, 620; NAGUMOTU, s. 107.

⁹⁰ Konuyla ilgili görüntülü bir haber için bkz. <https://www.trthaber.com/videolar/dijital-cagin-tehlikesi-deepfake-68267.html> (ET: 06.06.2025).

⁹¹ ANIKAYDIN, s. 740.

⁹² PAWELEC, s. 16; NAGUMOTU, s. 110 vd.; PAWELEC, s. 16-17; ayrıca bkz. BASTIAN, Matthias: *Deepfakes. China-Propaganda bei Facebook und Instagram*, 2020 (<https://the-decoder.de/deepfakes-china-propaganda-bei-facebook-und-instagram/>, ET: 02.06.2025); STONE, Jeff: *Chinese accounts blast Trump, with help from AI-generated pictures*, 2020 (<https://cyberscoop.com/graphika-spamouflage-dragon-china/>, ET: 03.06.2025); BELADA, s. 331, 332, 336.

⁹³ YAVUZ, *Deepfake*, s. 158 vd.

rek artmakta, seçimden bir gece önce sansasyonel veya manipülatif *deepfake* videoların yayınlanması, bir hükümet yetkilisinin savaş ilan ettiğini gösteren veya bir politikacı hakkındaki söylentiye doğrulayan *deepfake* videoların paylaşılması gibi senaryoların ciddiyeti sıklıkla dile getirilmektedir⁹⁴.

Deepfake yoluyla hazırlanmış ve internet ortamında yayılmış bir içerik devletler için uluslararası krizlere yol açabilecek hatta ülkelerin akıbetini belirleyebilecek kadar ciddi sonuçlar doğurabilmektedir⁹⁵. Amerika’da gittikçe artan olaylar ve sorunlar sebebiyle *derin kurgu*⁹⁶ şeklinde ifade edilen bu içerikler bir ulusal güvenlik problemi olarak kabul edilmiştir⁹⁷. Amerikan hukukunda mevcut kanunların *deepfake* videoları kapsamadığı hâller dikkate alınarak, bazı eyaletler bu konuda düzenlemeler yapmak için harekete geçmiş, 2019 yılında Kaliforniya’da pornografik *deepfake* içeriklere yönelik hukuki çözümler getiren ve seçime yakın haftalarda siyasi adayları içeren etiketsiz değiştirilmiş videoların yayılmasını yasaklayan düzenlemeler yapılmış, Virginia eyaletinde rıza dışı pornografi yasası *deepfake* videoları kapsayacak şekilde genişletilmiş, Teksas eyaletinde seçimlere giden süreçte adayların korunması sağlanmış ve *New York*’da da rıza dışı pornografi yasasını genişleten ve *deepfake*’lerin ticari kullanımlarına karşı sınırlı koruma sağlayan yeni bir kanun çıkarılmıştır⁹⁸.

Uluslararası kuruluşların da *deepfake* yoluyla hazırlanan içeriklerin yol açabileceği ciddi sorunları, gelecekteki en büyük tehditlerden biri olarak değerlendirdiği görülmektedir⁹⁹. *Deepfake* içeriklerin demokratik toplumlardaki güveni ve dolayısıyla demokrasinin kendisini yıpratılabileceği ve bu şekilde *deepfake* sebebiyle oluşan dezenformasyonun, kişilerin gördükleri ve duydukları konusunda şüphe oluşturarak, toplumsal müzakerenin olgusal temelini baltalayabileceği ve izole edilmiş, gerçek ötesi (*post real*) bir topluma sebebiyet verebileceği, aynı zamanda *deepfake* içeriklerin gerçeklere duyulan güveni tehdit ederek bilgiye dayalı güvenin azalmasına da yol açabileceği değerlendirilmektedir¹⁰⁰.

Deepfake içerikler tüzel kişi türlerinden biri olan şirketler için de ciddi tehditler oluşturabilmekte, büyük ekonomik kayıplara neden olabilmektedir. Ses üzerinden elde edilen *deepfake* içerikler yoluyla şirketler büyük zararlara uğratılabilmekte, şirket yöneticilerinin seslerine ilişkin oluşturulan içeriklerle yüklü miktarda para transferleri yaptırılabilen, farklı dolandırıcılık yöntemlerine başvurulabilmektedir¹⁰¹. Bu tür dolandırıcılıklara karşı yazılım geliştiren bir siber güvenlik firması olan *Pindrop*, 2013 yılından beri ses taklit edilerek işlenen suçlarda yaklaşık yüzde 350 artış olduğunu, her 638 telefon görüşmesinden birinde yapay ses kullanıldığını tespit etmiştir¹⁰².

D. Teknik Çözümler ve Teknik Çözümlere İlişkin Yetersizlikler

Deepfake içeriklere karşı korunmak için öncelikle paylaşımında bulunan kişilerin, fotoğraf vb. kişisel verilerini korumak konusundaki hassasiyetlerini geliştirmek ve herkese açık video ve görsellerini sınırlandırarak bizzat kendilerinin teknik önlemler almalarını sağlamak önemli bir başlangıç olarak görülmektedir¹⁰³. Bunun yanında sosyal ağ sağlayıcıların alacağı teknik önlemler, hukuka aykırı *deepfake* içeriklerin yayın ve paylaşımının önlenmesi veya durdurulması bakımından giderek etkisi artan bir çözüm olarak

⁹⁴ KUGLER / PACE, s. 626; ayrıca bkz. NAGUMOTU, s. 110 vd.; MENESES, s. 1 vd.; AKMEŞE, s. 83-84.

⁹⁵ ARSLAN, s. 703, 709; ANIKAYDIN, s. 738 vd.; BELADA, s. 336.

⁹⁶ KUGLER / PACE, s. 626 vd. Derin kurgu vakaları hakkında bkz. ÖZDEMİR, s. 910 vd.

⁹⁷ ÖZDEMİR, s. 913. Amerika’da *deepfake* ile ilgili alınan hukuki tedbirlere ilişkin bilgi için bkz. ARSLAN, s. 712-713; NAGUMOTU, s. 108 vd., 137 vd.

⁹⁸ KUGLER / PACE, s. 614; ayrıca bkz. GERSTNER, s. 11-12; BELADA, s. 338 vd.; ÇOLAK.

⁹⁹ EUROPEAN UNION AGENCY FOR LAW ENFORCEMENT COOPERATION: *Facing Reality?: Law Enforcement and the Challenge of Deepfakes, An Observatory Report from the Europol Innovation Lab*, Publications Office of the European Union, Luxembourg, 2022, s. 1-23; ARSLAN, s. 703.

¹⁰⁰ PAWELEC, s. 11-12.

¹⁰¹ NGUYEN / NGUYEN / NGUYEN / NGUYEN / HUYNH-THE / NAHAVANDI / NGUYEN / PHAM / NGUYEN, s. 2; MASCA.

¹⁰² ANIKAYDIN, s. 739.

¹⁰³ BAKER.

karşımıza çıkmaktadır. Sosyal ağ sağlayıcıların bu hususta belli algoritmalar kullanarak platformlarında paylaşılan hukuka aykırı *deepfake* içeriğini doğrudan tespit edip kaldırabilecek yapay zekâ destekli yöntemler geliştirmeye çalıştığı görülmekte, ancak bunun henüz büyük ölçüde çözülmemiş bir sorun olduğu dile getirilmektedir¹⁰⁴. Facebook'un düzenlediği bir yarışmada kazanan yarışmacının oluşturduğu algoritma ancak yüzde 65,18 doğruluk oranında yapay zekânın manipüle ettiği videoları yakalayabilmiştir¹⁰⁵. Eylül 2019'da Facebook'un halka açık olarak başlattığı bu “*Deepfake* Tespit Yarışması”nda katılımcılar, *deepfake* videoları tanımlamak için algılama sistemleri ve otonom algoritmik sistemler geliştirmeye teşvik edilmiştir¹⁰⁶. *Deepfake* yoluyla elde edilmiş ve paylaşılmış içeriğin büyük bir kısmı sosyal medya platformlarında ve özellikle sosyal paylaşım sitelerinde hızla yayılabilmekte¹⁰⁷ ve teknik olarak bunun önüne geçilmesinin hâlâ oldukça zor olduğu görülmektedir. Instagram, Facebook gibi sosyal paylaşım siteleri, uzmanlaşmış analiz şirketleri ile çalışarak tespit ettiği *deepfake* kullanılarak oluşturulmuş sahte hesapları kaldırma yoluna gitse de¹⁰⁸ bu çözümün yeterli olmadığı görülmektedir. *Deepfake* yoluyla oluşturulan hukuka aykırı içerikleri teknik olarak tespit etmenin ve denetlemenin zorlu doğası, bu içeriklerin aynı zamanda bugüne kadar var olan en sofistike yanlış bilgilendirme ve dezenformasyon aracı olarak görülmesine yol açmaktadır¹⁰⁹. Teknik imkânsızlıklar, ifade özgürlüğüne ve diğer anayasal özgürlüklere ölçüsüzce müdahale etmeksizin kötü niyetli *deepfake*'lerin oluşturulmasını durdurmaya yönelik mevzuat geliştirmeye devam edilmesini şart kılsa da teknik açıdan çözüm geliştirilmesi hukuki yönden getirilen çözümlere büyük destek sağlamaktadır¹¹⁰. Halihazırda *deepfake* içeriği evrensel olarak tespit edip engelleyecek bir sistem olmadığı için, en iyi tespiti gerçekleştiren yazılımların kullanılması ve bu yazımların geliştirilmesine destek verilmesi de büyük önem taşımaktadır¹¹¹.

E. Hukuki Sorunlar ve Çözüm Yolları

1. Kişilik Hakkı İhlaline İlişkin Hukuki Sorunlar

Mevzuatımızda *deepfake* teknolojisinin kullanımını sınırlayan ya da bu konuyla ilgili hukuki çerçeveyi belirleyen özel bir düzenleme yoktur. Ancak bu konudaki hukuki sorunlar arttıkça hukukumuzda bu tür bir ihtiyacın doğabileceği gözlemlenmektedir. Halihazırda *deepfake* ile ilgili öngörülebilir pek çok hukuki sorun söz konusudur. Kişilerin görüntüsü ve/veya sesinin haberleri dahi olmaksızın *deepfake* teknolojiyle işlenip, sosyal ağlarda veya diğer sosyal medya platformlarında, çevrimiçi sohbet platformlarında ya da internet ortamındaki herhangi bir web sitesinde paylaşılması, bu sorunların başında gelmektedir. Bu durumda hem yüzü aktarılan kimsenin hem de tanınabilir olduğu durumda vücudu kullanılan kimsenin, özel hayatının gizliliği, görüntüsü, şeref ve haysiyeti gibi kişilik değerlerinin ihlal edilebileceği görülmektedir. Bu şekilde kişilik değerlerine saldırılan kimseler kişilik hakkının ihlali bakımından mağdur sıfatı taşıdıkları gibi, ceza hukuku bağlamında oluşan suçlar bakımından da mağdur sıfatı taşıyabilmektedir¹¹².

¹⁰⁴ <https://www.theverge.com/2021/6/16/22534690/facebook-deepfake-detection-reverse-engineer-ai-model-hyperparameters> (ET: 04.06.2025); ayrıca bkz. MENESES, s. 5.

¹⁰⁵ <https://ai.facebook.com/blog/deepfake-detection-challenge-results-an-open-initiative-to-advance-ai/> (ET: 04.06. 2025).

¹⁰⁶ <https://ai.meta.com/blog/deepfake-detection-challenge-results-an-open-initiative-to-advance-ai/> (ET: 04.06.2025); NAGUMOTU, s. 108.

¹⁰⁷ PAWELEC, s. 2; NAGUMOTU, s. 117 vd.

¹⁰⁸ BASTIAN.

¹⁰⁹ MENESES, s. 9.

¹¹⁰ MENESES, s. 9.

¹¹¹ MENESES, s. 9. *Deepfake* içeriğin tespitine ilişkin geliştirilen bir yazılım hakkında bkz. <https://www.technopat.net/2023/06/08/intel-ile-deepfake-tespit-teknolojisi-fakecatcher-uzerine-konustuk/> (ET: 26/05/2025).

¹¹² AKSOY RETORNAZ, s. 101. *Deepfake* kullanılarak üretilen içerikler bakımından mağdurların çoğunlukla kadınlar olduğu yönünde bkz. AKSOY RETORNAZ, s. 101; KUGLER / PACE, s. 621. Görüntüye dayalı cinsel istismar mağdurlarının ağırlıklı olarak kadınlar olduğu yönünde bkz. BALCI, Murat / ÇAKIR, Kerim: “İnternet Ortamında ve Sosyal Ağlarda İşlenen Cinsel Suçlar”, *Anadolu Üniversitesi Hukuk Fakültesi Dergisi*, 2022, Cilt 8, Sayı 2, s. 212. Bir araştırmaya göre *deepfake* yoluyla elde edilen çevrimiçi içeriğin yüzde 96'sının pornografik ve kadınlara ait olduğu, 2019 yılı itibarıyla bu görüntülerin en az 134 milyon kişi tarafından izlendiği, en bilinen on pornografi sitesinden sekizinde bu tür içerik olduğu yönünde bkz. AJDER / PATRINI / CAVALLI / CULLEN, s. 1-7; ayrıca bkz. KUGLER / PACE, s. 613.

Kural olarak kişinin rızası alınmadıkça resmi veya karikatürü çizilemeyeceği gibi, görüntüsünün aynen ya da üzerinde değişiklikler yapılarak kaydedilmesi, kopyalanması, tahrif edilmesi, basın ve yayın organlarında yer alması, sosyal medya platformlarında ve genel olarak internet ortamında paylaşılması kişilik hakkı ihlali anlamına gelir¹¹³. Kişinin hukuken geçerli bir rızası olmadığı hâlde fotoğrafının, kamera ile kaydedilmiş görüntüsünün değiştirilmeden olduğu gibi veya kişinin tanınabileceği şekilde *Photoshop*¹¹⁴, *deepfake* vb. teknik yöntemlerle değiştirilerek kullanılması, bu şekilde cinsel içerikli görüntü kayıtları elde edilip internet ortamında paylaşılıp yayılması gibi fiiller de kişilik hakkı ihlaline yol açar¹¹⁵.

Deepfake, sahte uygunsuz cinsel içerikler üretmek için de sıklıkla kullanılan bir teknolojidir. *Deepfake* yoluyla elde edilen uygunsuz içerikte *deepfake* öznesinin sadece yüzü kullanılsa bile, öznenin kimliği yeniden tasarlanarak ve sahte olsa dahi cinsel alanına dair rıza dışı bedensel bir kurgu oluşturularak elde edilen sonucun, kişinin görüntüsü, özel hayatının gizliliği ve şeref ve haysiyeti gibi kişilik değerlerine bir saldırı teşkil ettiği görülür¹¹⁶. Pornografik içerikli *deepfake* videolarda kişi aslında yapmış gibi görüldüğü cinsel davranışta bulunmadığı için mahremiyet duygusu ciddi anlamda zedelenmektedir¹¹⁷. Söz konusu içerik, mağdurların gerçek bedenlerini tasvir etmese hatta *deepfake* bir video olduğu sahte içerik olarak etiketlenirse dahi mağdur tespit edilebildiği sürece kişilik hakkı ihlali ortadan kalkmaz. Videonun içeriğinin sahte olduğuna ilişkin uyarı yapılmış olması, kişinin rızası olmaksızın görüntüsünü, sesini kullanarak özel hayatının gizliliğini, şeref ve haysiyetini vb. kişilik değerlerini ihlal eden bir failin eylemini hukuka uygun hâle getirmek için yeterli değildir. Bu durumda ancak mağdurlara verilen zararın azalıp azalmadığı tartışılabilir¹¹⁸. Özellikle pornografik içerikli *deepfake* videolar bakımından videonun sahte olduğunun etiketlenmesinin mağdurun zararını hafifletmediği ileri sürülse de¹¹⁹ kanaatimizce somut olaya göre etiketlenmiş video ile etiketlenmemiş videonun aynı zarara yol açıp aynı sonucu doğurduğunu kabul etmek, hakkaniyete aykırı sonuçlar doğurabilir.

Deepfake yoluyla elde edilen içerik doğrudan toplumsal itibara, şeref ve haysiyetine de yönelmiş olabilir¹²⁰. Örneğin kişinin yüz görüntüsü alınarak ırkçı eylemlerde ya da söylemlerde bulunduğu, terörist bir grubu desteklediği, cinsel eylemlerde bulunduğu ya da uyuşturucu kullandığı bir içeriğe dönüştürülerek şeref ve haysiyeti ihlal edilebilir¹²¹. *Deepfake* yoluyla rıza olmaksızın hazırlanan içerik mağdurun/mağdurların başka kişilik değerlerini ihlal etmese dahi görüntü ve/veya ses üzerindeki kişilik hakkının ihlali hukuka aykırılık için yeterlidir ve bu durumda ilerde bahsedeceğimiz hukuki çözüm yollarına başvurmak mümkündür.

Kamuya mal olmuş kişilerle ilgili *deepfake* içerikler ve paylaşımlar bakımından, eleştiri sınırları dahilinde kalmak, bilimsel sanatsal nitelik arz etmek gibi koşullarla bir katlanma yükümlülüğünden bahsedilebilir. Kamuya mal olmuş kişilere yönelik eleştirel içerikler diğer kişilere ait olanlara göre

¹¹³ OĞUZMAN / SELİÇİ / OKTAY ÖZDEMİR, s. 195; DURAL / ÖĞÜZ, s. 140-141; ANTALYA, s. 128; ANTALYA / TOPUZ, s. 166; ERDOĞAN / KESKİN, s. 288; KAYA, s. 284; TURAN BAŞARA, s. 32; AKKURT, s. 60; ARAS, s. 27; TURGUT, s. 144-145; AK-YASAN BİRSEN, Gönül: *Sosyal Medyada Paylaşılan İçerik Nedeniyle Kişilik Hakkı İhlalleri*, Seçkin Yayıncılık, Ankara, 2020, s. 97; MÜLLER TERPITZ, s. 267 vd.

¹¹⁴ *Photoshop*, var olan resim, grafik veya fotoğraflar üzerinde düzenlemeler yapmaya, onları değiştirip yapılandırmaya yarayan bir tür resim editördür. Ayrıntılı bilgi için bkz. <https://ata.com.tr/blog-detay/photoshop-nedir-photoshop-nasil-kullanilir-85> (ET: 05.06.2025).

¹¹⁵ OĞUZMAN / SELİÇİ / OKTAY ÖZDEMİR, s. 195; AKİPEK, Jale / AKINTÜRK, Turgut / ATEŞ: Derya: *Türk Medeni Hukuku Başlangıç Hükümleri Kişiler Hukuku Birinci Cilt*, 18. Baskı, Beta Yayıncılık, İstanbul, 2022, s. 388; ANTALYA / TOPUZ, s. 166; KAYA, s. 284; TURAN BAŞARA, s. 32; AKKURT, s. 60; ARAS, s. 27. Bu fiiller ceza hukuku yönünden özel hayatın gizliliğini ihlal, cinsel taciz gibi farklı suçların oluşmasına da sebep olmaktadır. Bkz. AKSOY RETORNAZ, s. 98 vd., 102; BALCI / ÇAKIR, s. 208.

¹¹⁶ KUGLER / PACE, s. 624.

¹¹⁷ KUGLER / PACE, s. 624.

¹¹⁸ KUGLER / PACE, s. 625. Sahte olduğu etiketlenmiş ve etiketlenmemiş pornografik içeriğin etkileri konusunda cinsiyete göre yapılmış bir analiz için bkz. KUGLER / PACE, s. 652.

¹¹⁹ KUGLER / PACE, s. 673.

¹²⁰ KUGLER / PACE, s. 625; ayrıca bkz. YÜNLÜ, Semih: "Üretici Yapay Zekâ Kaynaklı Norm ve Kişi Bazlı Hukuki Sorumluluk", *Adalet Dergisi*, 2024, Cilt 1, Sayı 72 (Sorumluluk), s. 503, 514.

¹²¹ KUGLER / PACE, s. 625.

daha esnek bir değerlendirmeye tabi tutulur. Avrupa İnsan Hakları Mahkemesi de bireylere yönelik eleştirinin çerçevesinin, kamu görevlilerine ve siyasetçilere yönelik eleştirilere göre daha dar olduğu ve iş ilişkileri bağlamında bile olsa, saldırgan karikatürlerin veya ifadelerin kullanılmasının haklı görülmemeyeceği ve bu tür eylemlerin şeref ve haysiyeti zedeleyebileceği görüşündedir¹²². Nitekim Avrupa Birliğinde 2024 yılında kabul edilen Yapay Zekâ Yasası (*Artificial Intelligence Act*) 50. maddesinde yer alan düzenlemeye göre, *deepfake* içeriğin açıkça eleştirel sanatsal, kurgusal veya benzer bir çalışma veya programın parçası olduğu durumlarda, ifade özgürlüğü ile sanat ve bilim özgürlüğü hakkını korumak adına, içeriğin *deepfake* olduğunun belirtilerek etiketlenmesi ve bu yolla şeffaflık sağlanması zorunluluğu esnetilmektedir. Hukukumuz açısından da kamuya mal olmuş kişilerle ilgili bilimsel, sanatsal veya eleştirel içerik açısından bu tür bir yaklaşım benimsenmesi ve *deepfake* ile ilgili yapılacak hukuki düzenlemelerde bu çerçevede hareket edilmesi gerektiği görüşündeyiz. Ancak bu durumda da bir ölçülülük sağlanması gerektiği, kamuya mal olmuş kişinin yaptığı iş, tanındığı alanla ilgili olmayıp doğrudan özel hayatına veya şeref ve haysiyetine saldırı niteliğindeki *deepfake* içeriğin etiketlense dahi hukuka aykırı olacağını kabul etmek gerekir. Kamuya mal olmuş kişilerin kendilerine resim veya karikatür yoluyla yapılan eleştirilere diğer kişilere göre daha hoşgörülü yaklaşım tahammül göstermesi gerektiği kabul edilmekte ve bu çerçevede değerlendirme yapılmakla birlikte¹²³, bu tahammül ve katlanmanın sınırsız olmadığını, kamuya mal olmuş kişinin kendisine ait pornografik bir *deepfake* içeriğe, şeref ve haysiyetini ya da özel hayatının gizliliğini ölçsüz bir şekilde ihlal eden ya da reklam amacıyla üretilip haksız kazanç sağlanan içeriklere katlanmasının beklenemeyeceğini belirtmek gerekir.

2. Şeffaflık Sorunu ve Avrupa Birliği Yapay Zekâ Yasası'nda Yer Alan Düzenlemeler

Deepfake içerikler bakımından önde gelen hukuki sorunlar bir diğeri, bu içeriklerin yapay zekâ ürünü sahte içerikler olduğuna dair bir bilgilendirme, bir etiketleme yapılmaksızın doğrudan paylaşılmasıdır. İnternet ortamında *deepfake* içeriği yönetmenin önemli bir yolu, toplumun içerik konusunda bilgilendirilmesi, eğitimi ve dezenformasyona ve üzerinde oynanmış sahte içeriğe ve genel olarak çevrimiçi içeriğe karşı daha duyarlı ve eleştirel bakabilecek hâle getirilmesidir¹²⁴. Nitekim içeriğin sahte olduğunu bilmeyen, anlamayan ya da önemsemeyen kimseler, bu nedenle birçok farklı mağduriyet yaşayabilmekte, örneğin sosyal medya platformlarında sıklıkla yer aldığını gözlemlediğimiz ünlülere ait *deepfake* ürünü sahte reklam videolarına inanarak, dolandırıcılık vb. suçların mağduru olabilmektedir. Sosyal medyada ve internet ortamında paylaşılan milyonlarca *deepfake* içeriğin şeffaflık sorunu barındırdığı ve bu nedenle birçok hukuki soruna yol açtığı fark edilerek bu hususta hukuki düzenlemeler yapılmaya başlanmıştır. Örneğin dünyada en kapsamlı ilk yapay zekâ düzenlemesi olan Avrupa Birliği Yapay Zekâ Yasası'nda *deepfake* içeriklerin şeffaflık sorununu gidermeye ilişkin bazı düzenlemeler yapılmıştır. Yasa'da yapay zekâ sistemleri barındırdıkları riske göre sınıflandırılmakta, *deepfake* içerikler, sınırlı risk/şeffaflık riski içeren grupta yer almaktadır. Yasa, *deepfake* içerikler için belli şeffaflık yükümlülükleri öngörmektedir. Yasa'nın 2 Ağustos 2026 tarihinde yürürlüğe girecek olan 50. maddesi "*Belirli Yapay Zekâ Sistemlerinin Sağlayıcıları ve Dağıtıcıları İçin Şeffaflık Yükümlülükleri*" başlığını taşımakta olup, bazı *deepfake* içeriklerin yapay olarak üretildiğini yani sahte olduğunu ifşa etme zorunluluğu getirmektedir¹²⁵. Söz konusu düzenlemeye göre *deepfake* niteliğinde görüntü, ses veya video içeriği üreten veya işleyen bir yapay zekâ sisteminin dağıtımçıları, içeriğin yapay olarak üretildiğini veya işlendiğini ifşa etmek zorundadır. Bu durumun ifşası için verilen bilgiler, ilgili gerçek kişilere en geç ilk etkileşim veya maruziyet anında, açık ve ayırt edilebilir bir şekilde sağlanmalı, erişilebilirlik gerekliliklerine uygun olmalıdır. Bu yükümlülük, suçların tespiti, önlemesi, araştırma veya kovuşturması için kullanımın yasa tarafından yetkilendirildiği durumlarda geçerli değildir.

¹²² AİHM, *PS ve diğerleri/İspanya*, B. No: 28955-57-59-64/06, T. 12.09.2021 (HUDOC); ayrıca bkz. AKSOY RETORNAZ, s. 99, dn. 364.

¹²³ AKYASAN BİRSEN, s. 166-167; ayrıca bkz. AKİPEK / AKINTÜRK / ATEŞ, s. 390, 393.

¹²⁴ FARID / DAVIES / WEBB / WOLF / HWANG / ZUCCONI / LYU, s. 15; YAVUZ, *Deepfake*, s. 213 vd.

¹²⁵ *Artificial Intelligence Act* için bkz. <https://artificialintelligenceact.eu/article/50/> (ET: 26/05/2025).

İçerik, açıkça sanatsal, eleştirel, kurgusal veya benzer bir çalışmanın veya programın parçası ise şeffaflık yükümlülüğü, çalışmanın görüntülenmesini veya keyfinin çıkarılmasını engellemeyecek uygun bir şekilde söz konusu üretilen veya işlenen içeriğin varlığının ifşa edilmesiyle sınırlıdır. Yasa ayrıca yapay zekânın ürettiği bazı metinler bakımından da bilgilendirme yükümlülüğü getirmektedir. Buna göre yapay zekâ sistemi tarafından kamuoyunu kamu yararına olan konularda bilgilendirme amacıyla yayınlanan bir metni üreten veya işleyen uygulayıcılar, metnin yapay olarak üretildiğini veya işlendiğini ifşa etmelidir.

AB Yapay Zekâ Yasası 50. maddesinin gerekçesi Yasa'nın 134. Resital'inde yer almakta olup, yapay zekâ sistemi sağlayıcıları tarafından kullanılan teknik çözümlere ek olarak böyle bir düzenlemenin yapıldığı, bu şekilde *deepfake* görüntü, ses veya video içeriği oluşturmak veya işlemek için bir yapay zekâ sistemi kullanan dağıtımçılara bir şeffaflık yükümlülüğü getirildiği ifade edilmektedir¹²⁶. Sorumlu kişiler içeriğe ilişkin yapay zekâ çıktısını etiketleyerek ve yapay olduğunu, yapay olarak oluşturulduğunu belirtip, bu durumu açık, anlaşılabilir ve ayırt edilebilir bir şekilde ifşa etmelidir. Zira mevcut kişilere, nesnelere, yerlere, varlıklara veya olaylara belirgin şekilde benzeyen ve bir kişiye gerçek veya doğru gibi görünebilecek bu görüntülerin bir şeffaflık gerektirdiği açıktır. Gerekçe'ye göre şeffaflık yükümlülüğüne uyulması, yapay zekâ sisteminin veya çıktısının kullanımının, özellikle içeriğin açıkça eleştirel sanatsal, kurgusal veya benzer bir çalışma veya programın parçası olduğu durumlarda, üçüncü tarafların hakları ve özgürlükleri için uygun güvencelere tabi olarak, ifade özgürlüğü hakkını ve sanat ve bilim özgürlüğü hakkını engellemeyecek şekilde yorumlanmalıdır.

AB Yapay Zekâ Yasası'nda yer alan bu düzenlemelerde olduğu gibi hukukumuzda da şeffaflığı sağlamak adına atılacak adımlara ihtiyaç duyulduğu, her geçen gün uygulamada yaşanan olumsuzluklarla birlikte *deepfake* içerik şeffaflığını sağlamaya yönelik düzenleme yapmanın kaçınılmaz hâle geleceği gözlemlenmektedir.

3. Hukukumuzda Hukuka Aykırı *Deepfake* İçeriğe Karşı Çözüm Yolları

Hukukumuzda *deepfake* içerik sebebiyle yaşanan kişilik hakkı ihlallerinde Türk Medeni Kanunu (TMK) ve Türk Borçlar Kanunu'nda (TBK) yer alan genel hükümlere ve 5651 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun"da yer alan bazı düzenlemelere başvurulmakta, kişisel veri ihlali hâlinde ise 6698 sayılı Kişisel Verileri Koruma Kanunu 4 vd. maddelerinde yer alan hükümlere başvurulabilmektedir. TMK ve TBK'de görüntü ve ses üzerindeki kişilik hakkına yönelik özel bir düzenleme yer almamaktadır. Bu nedenle görüntünün ve sesin korunması için kişilik hakkını koruyan genel düzenlemelere başvurmak, TMK 23 vd., TBK 49 vd. ile TBK 58. maddelerinden yararlanmak mümkündür¹²⁷. Bu hükümler çerçevesinde gerek *deepfake* yoluyla gerekse başka bir şekilde görüntüsüne ya da sesine saldırıda bulunulan kişi, henüz gerçekleşmemiş saldırı için önleme davası, devam eden mevcut saldırı için saldırının durdurulması (men) davası, saldırının hukuka aykırılığının tespiti için tespit davası, haksız kazanç söz konusu ise haksız kazancın iadesi davası ve koşulları gerçekleşmişse maddi, manevi tazminat davası açabilir¹²⁸. Saldırı sosyal medyada veya genel olarak internet ortamında gerçekleşmişse 5651 sayılı Kanun'da yer alan içeriğin kaldırılması ve/veya erişimin engellenmesine ilişkin tedbirlerle başvurulması mümkündür. Ancak 5651 sayılı Kanun'un kişilik hakkının ihlali hâlinde içeriğin yayından kaldırılması ve erişimin engellenmesine ilişkin 9. maddesi Anayasa Mahkemesinin 11.10.2023 tarihli, 2020/76 Esas ve 2023/172 Karar sayılı kararı ile iptal edildiği ve hâlen yeni bir düzenleme yapılmadığı için, bu durumda ancak suç niteliğindeki bazı içerikler bakımından şartları varsa Ka-

¹²⁶ *Artificial Intelligence Act Recital 134* için bkz. <https://artificialintelligenceact.eu/recital/134/> (ET: 09.06.2025).

¹²⁷ İMRE, s. 165; ÖZTAN, s. 289-292; AYAN / AYAN, s. 117 vd.; OĞUZ, s. 145 vd.; YILDIZ, s. 3.

¹²⁸ İMRE, s. 167; ÖZTAN, s. 291-292; KAYA, s. 293 vd.; AKKURT, s. 60-61; YILDIZ, s. 3. Kişilik hakkının ihlali maddi manevi tazminat davalarına ilişkin ayrıntılı bilgi için bkz. TURAN BAŞARA, s. 103 vd. Alman hukukundaki düzenlemeler hakkında bkz. MÜLLER TERPITZ, s. 257, 267 vd.

nun'un 8. maddesindeki içerik kaldırma veya erişim engelleme tedbirlerine ya da özel hayatın gizliliğini ihlal söz konusu ise 9/A maddesindeki düzenlemeye başvurulması söz konusu olabilir. *Deepfake* içeriklerin özel hayatın gizliliğini ihlal etmesi hâlinde Kanun'un 9/A maddesine göre doğrudan Bilgi Teknolojileri ve İletişim Kurumuna (BTK) başvurarak içeriğe erişimin engellenmesi sağlanabilmektedir. Bu düzenlemeyle BTK Başkanına, erişim engelleme kararı alma ve uygulanması için Erişim Sağlayıcıları Birliği'ne gönderme yetkisi verilmekte, erişim sağlayıcılar bu tedbir talebini derhâl ve en geç dört saat içinde yerine getirmekle yükümlü tutulmaktadır. Her ne kadar idarenin bünyesinde yer alan BTK Başkanı tarafından böylesine ciddi bir karar alınsa ve uygulansa dahi, erişimin engellenmesini talep eden kişilerin, erişimin engellenmesi taleplerini, BTK'ye talepte bulundukları saatten itibaren yirmi dört saat içinde sulh ceza hâkiminin kararına sunmaları gerekmektedir. Hâkim, internet ortamında yapılan yayın içeriği nedeniyle özel hayatın gizliliğinin ihlal edilip edilmediğini değerlendirerek vereceği kararını en geç kırk sekiz saat içinde açıklayıp, doğrudan BTK'ye göndermekte, aksi durumda alınan erişimin engellenmesi tedbiri kendiliğinden kalkmaktadır. Bu düzenleme sadece özel hayatın gizliliğine ilişkin kişilik değerinin ihlali hâlinde uygulanabilmesi bakımından yetersiz ve BTK Başkanına erişim engelleme hususunda yetki verilmesi bakımlarından eleştiriye açık olsa da Kanun'un iptal edilen maddesi ile ilgili yeni bir düzenleme yapılana kadar, özel hayatın gizliliğini ihlal eden *deepfake* içerikler bakımından bu hükümden yararlanılması mümkündür.

Deepfake yoluyla hazırlanıp paylaşılan hukuka aykırı içerik için 5651 sayılı Kanun'un 4/1. maddesine göre içerik sağlayıcının sorumluluğuna¹²⁹ ve aynı zamanda koşulları varsa yer sağlayıcının ya da sosyal ağ sağlayıcının sorumluluğuna gidilmesi de mümkündür. Öncelikle içerik sağlayıcıdan ve yer sağlayıcıdan hukuka aykırı içeriği kaldırmasının istenebileceği ve bu yolun işlemesi hâlinde oldukça pratik bir çözüm sağlanabileceğini belirtmek gerekir. 5651 sayılı Kanun'un 5. maddesine göre yer sağlayıcı, yer sağladığı içeriği kontrol etmek veya hukuka aykırı bir faaliyetin söz konusu olup olmadığını araştırmakla yükümlü olmamakla birlikte, yer sağladığı hukuka aykırı içerikten usulünce haberdar edilmesi hâlinde bu içeriği yayından çıkarmakla yükümlüdür. Bu yükümlülüğe uymayan yer sağlayıcı hakkında BTK Başkanı tarafından idari para cezası yaptırımı uygulanmaktadır. 5651 sayılı Kanun'un 4/1. maddesinde içerik sağlayıcının internet ortamında sunduğu her türlü içerikten sorumlu olduğu düzenlenmekte olup, aynı maddenin ikinci fıkrasında içerik sağlayıcının bağlantı sağladığı başkasına ait içerikten kural olarak sorumlu olmadığı hususu düzenlenmektedir. Buna göre hukuka aykırı *deepfake* içeriğine erişim ya da bağlantı sağlamak (link vermek) tek başına bu bağlantıyı sağlayan kimsenin sorumluluğunu doğurmamaktadır. Ancak *deepfake* içeriğe bağlantı sağlayan kimsenin söz konusu içeriği benimsemesi ve diğer kullanıcıların bu içeriğe ulaşmasını açıkça amaçlaması hâlinde, örneğin kendisi tarafından eklenen bir yorumla, metin, ses ya da görüntü içeriğiyle mevcut içeriği desteklediği durumlarda, genel hükümler çerçevesinde sorumluluğu söz konusu olur. Bu durumda *deepfake* içeriğin olduğu gibi paylaşılması veya bu içeriğe ilişkin bağlantı (*link*) verilmesi sorumluluk doğurmamaktadır. İnternet kullanıcısı hukuka uygun herhangi bir içeriğe hukuka aykırı *deepfake* içerik ekleyerek paylaşırsa veya hukuka uygun bir *deepfake* içeriğe hukuka aykırı eklemeler, çıkarmalar veya düzenlemeler yaparak onu hukuka aykırı hâle getirdikten sonra paylaşırsa, bu eyleminden tek başına sorumlu olur.

Hukuka aykırı *deepfake* içerik çoğunlukla rastlandığı üzere eğer bir sosyal ağda yer alıyorsa bu durumda da hukukumuz bakımından başvurulabilecek bazı çözümler vardır. 5651 sayılı Kanun'un Ek 4 maddesinin üçüncü fıkrasında uyar kaldır sistemi benimsenerek Türkiye'den günlük erişimi bir milyondan fazla olan yurt içi veya yurt dışı kaynaklı sosyal ağ sağlayıcının, Kanun'un 9'uncu ve 9/A maddeleri kapsamındaki içeriklere yönelik olarak kişiler tarafından yapılacak başvurulara, başvurudan itibaren en geç kırk sekiz saat içinde olumlu ya da olumsuz cevap vermekle yükümlü olduğu, eğer olumsuz cevap verecekse gerekçeli olarak vermesi gerektiği düzenlenmiş, aynı maddenin 8. fıkrasında bu hükme uymama hâlinde sosyal ağ sağlayıcıya beş milyon Türk lirası idari para cezası öngörülmüş,

¹²⁹ YÜNLÜ, *Sorumluluk*, s. 533-534.

15. fıkrasında ise sosyal ağ sağlayıcının, başlık etiketleri ve öne çıkarılan içeriklerin uyarı yöntemiyle kaldırılması için BTK ile işbirliği içinde etkin bir başvuru mekanizması kurmakla yükümlü olduğu hükme bağlanmıştır. Ancak Kanun'un 9. maddesi genel olarak kişilik hakkına aykırı içeriğe ilişkin bir hüküm iken daha önce bahsettiğimiz üzere Anayasa Mahkemesi tarafından iptal edildiği için şu an bu hususta bir boşluk olduğu ve bu boşluğun en azından Ek 4 madde metni düzenlenilerek giderilmesi gerektiği görülmektedir. Düzenleme şimdiki hâliyle sosyal ağ sağlayıcıların sadece 9/A maddesi çerçevesindeki başvurulara cevap verme yükümlülüğü olduğu sonucunu çıkarmaya yol açtığı için bu hususta acilen bir düzenleme yapılması gerekmektedir.

Ayrıca belirtmek gerekir ki Anayasa Mahkemesi kararıyla iptal edilen 5651 sayılı Kanun'un 9. maddesinde 7253 sayılı Kanun'la 2020 yılında bir değişiklik yapılmış ve onuncu fıkrada hukuka aykırı içeriğin arama motorlarından çıkarılmasının talep edilebileceğine ilişkin bir hükme yer verilmişti¹³⁰. Hükümün on birinci fıkrasında ise bu konudaki sulh ceza hâkimi kararını süresinde yerine getirmeyen içerik, yer ve erişim sağlayıcıların sorumlularının, beş yüz günden üç bin güne kadar adli para cezası ile cezalandırılacağı şeklinde bir yaptırıma yer verilmişti. Bu hüküm kişilik hakkını ihlal eden hukuka aykırı içeriğin sadece internet adresleri ile ilişkilendirilmemesini talep etmeyi mümkün kılmakta ve unutulma hakkının bir görünümü olan arama motorlarındaki listeden çıkarılmayı (*delisting*) sağlamak-taydı. Hukuka aykırı içeriğin hâlâ internet ortamında kaldığı düşünüldüğünde, içerik kaldırma yaptırımını uygulanmadıkça bu çözümün sorunu kökten çözemeyeceği açıktı. Ancak her ne kadar arama motorlarında aratılması hâlinde sadece hukuka aykırı içerikle ilgili bir sonuç gösterilmemesini sağlasa da *deepfake* ile ilgili içeriklerin arama motorlarından kaldırılmasını sağlayan ve bu şekilde yaptırım içeren bir hükmün bulunması olumlu karşılanmalı ve yapılacak yeni düzenlemede de bu tür bir hükme yer verilmelidir.

Hukukumuzda *deepfake* teknolojisi kullanılarak hazırlanan içerik sebebiyle uygulanabilecek birtakım cezai yaptırımlar da vardır. *Deepfake* içeriğe ve somut olaya göre TCK 132-140 maddelerinde yer alan suçların oluşması mümkün olduğu gibi, hakaret, tehdit, şantaj gibi çeşitli suçların da oluşması söz konusu olabilir¹³¹. Özellikle TCK 134/2. maddesinde özel hayata ilişkin görüntü ve seslerin hukuka aykırı olarak ifşasına ilişkin bir hüküm yer almaktadır¹³². Ayrıca belirtmek gerekir ki *deepfake* videosu bir hakaret içerebileceği gibi, somut olaya göre *deepfake* yoluyla oluşturulan içeriğin başlı başına hakaret suçunu oluşturması da mümkündür¹³³. Ceza hukuku bakımından *deepfake* içeriklerle ilgili gündeme gelebilecek bir diğer suç TCK'ye sonradan eklenen bir hükümde düzenlenmektedir. 13.10.2022 tarihli ve 7418 sayılı Kanun'la Türk Ceza Kanunu'na 217/A maddesi eklenerek "Halkı yanıltıcı bilgiyi alenen yayma suçu" şeklinde bir suç düzenlenmiştir. Söz konusu düzenleme "(1) Sırf halk arasında endişe, korku veya panik yaratmak saikiyle, ülkenin iç ve dış güvenliği, kamu düzeni ve genel sağlığı ile ilgili gerçeğe aykırı bir bilgiyi, kamu barışını bozmaya elverişli şekilde alenen yayan kimse, bir yıldan üç yıla kadar hapis cezasıyla cezalandırılır. (2) Fail, suçu gerçek kimliğini gizleyerek veya bir örgütün faaliyeti çerçevesinde işlemesi hâlinde, birinci fıkraya göre verilen ceza yarı oranında artırılır." şeklindedir. *Deepfake* içerik yoluyla gerçekleştirilen hukuka aykırı eylem için somut olaya uydu-

¹³⁰ Anayasa Mahkemesi tarafından iptal edilmeden önce 5651 sayılı Kanun 9. maddesi onuncu fıkrasında yer alan düzenleme şu şekildeydi: "İnternet ortamında yapılan yayın içeriği nedeniyle kişilik hakları ihlal edilenlerin talep etmesi durumunda hâkim tarafından, başvurunun adının bu madde kapsamındaki karara konu internet adresleri ile ilişkilendirilmemesine karar verilebilir. Kararda, Birlik tarafından hangi arama motorlarına bildirim yapılacağı gösterilir." 5651 sayılı Kanun'un 9/11 maddesinde 9. maddedeki düzenlemelere uyulmaması hâlinde uygulanacak yaptırım ise şu şekilde düzenlenmekteydi: "Sulh ceza hâkiminin kararını bu maddede belirtilen şartlara uygun olarak ve süresinde yerine getirmeyen içerik, yer ve erişim sağlayıcıların sorumluları, beş yüz günden üç bin güne kadar adli para cezası ile cezalandırılır."

¹³¹ ANIKAYDIN, s. 742-743.

¹³² Ayrıntılı bilgi için bkz. YURTCAN, s. 59 vd.; AKSOY RETORNAZ, s. 84; "... Dosya kapsamına göre; katılanla aralarında önceye dayalı husumet bulunan sanığın, katılanın cinsel içerikli görüntüsünü, 02.04.2012 tarihinde, Youtube adlı video paylaşım sitesinde, '... Müdürlüğünün Sapık Teftiş Kurulu Başkanı' ibaresi altında yayımladığının iddia edildiği olayda, sanığın üzerine atılı TCK'nın 134/2. maddesindeki özel hayatın gizliliğini ihlal suçunun sübut bulduğuna ve eylemin hukuki nitelendirilmesine yönelik kabulde bir isabetsizlik görülmemiş; ...", Yargıtay, 12. CD, T. 18.05.2015, E. 2014/23405, K. 2015/8309 (Yargıtay Karar Arama).

¹³³ KUGLER / PACE, s. 629 vd.

ğu ölçüde bu suça ilişkin hükme başvurulması da mümkündür. Türk Ceza Kanunu bakımından kişinin sesinin izinsiz olarak veya gizlice kaydedilmesi ve ifşası bir suçtur. Bu durumda somut olaya bakılarak TCK 132, 133 ve 134. maddelerinde yapılan düzenlemelerde yer alan haberleşmenin gizliliğini ihlal, kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması ile özel hayatın gizliliğini ihlal suçlarına ilişkin hükümlere başvurulabilir¹³⁴.

SONUÇ

Deepfake teknolojisi, yapay zekâ teknolojisi kullanılarak görüntü ve/veya ses üzerinde değişiklikler yapılabilen, yüksek gerçeklikle ses, görüntü ve video içeriklerinin birleştirmesini ve bu şekilde yeni içerikler elde edilmesini sağlayan bir teknolojidir. *Deepfake* içerik elde edebilmek için, üretken çekimi ağırlar, derin öğrenme, makine öğrenmesi gibi yapay zekâ yöntemleri kullanılmaktadır. *Deepfake* teknolojisi kullanılarak elde edilen tahrif edilmiş videolar ya da diğer ses ve/veya görüntü kayıtları, insanları asla yapmadıkları veya söylemedikleri şeyleri yaparken veya söylerken göstererek ciddi bir dezenformasyona yol açabilen içerikler olup, sahte içeriği gerçeğinden ayırmak oldukça zor olabilmektedir. Ünlüler ya da politikacılar gibi kamuya mal olmuş kişiler, *deepfake* içeriklerin öncelikli hedefleri gibi görünmektedir. Ancak bu teknolojiye gelişim ve ulaşım kolaylığı diğer kişiler için de bir tehdit hâline gelmesine neden olmuştur. Bunun yanında *deepfake* yoluyla hazırlanan içerikler devletler ve diğer tüzel kişiler için ciddi sorunlara yol açabilmektedir.

Deepfake içeriklerin öncelikli hedefi görüntü ve ses, kişilik hakkının kapsamında olan kişilik değerleri olup, bu kişilik değerlerinin kişiyi diğer kişilerden ayırt etme ve bu şekilde tanınmasını sağlama adına belirgin ve önemli bir işleve sahip olduğu ve aynı zamanda kişisel veri niteliği taşıdıkları görülür. *Deepfake* yoluyla oluşturulan içeriklerde ses ve görüntünün birlikte ihlaline sıklıkla rastlanmaktadır. Kişinin açık veya örtülü olarak rızası, üstün kamu yararı, kamunun haber alma özgürlüğü gibi hukuka uygunluk nedenleri, kişilik hakkı ihlali kural olarak ortadan kaldırılabilmektedir. *Deepfake* yoluyla oluşturulan video kaydı, kişilerin rızası alınarak oluşturulsa dahi onların rızası olmaksızın yayınlanıp, internet ortamında paylaşılması hukuka aykırıdır. Kişi, görüntüsünün/sesinin kullanılmasına ve işlenmesine razı olsa dahi, verilen rızanın sınırları aşılarak bir kullanma veya işleme söz konusuysa, bu şekilde yayın veya paylaşımlarda bulunuluyorsa, yapılan eylemler kişilik hakkına ve hukuka aykırıdır.

Deepfake yoluyla oluşturulan hukuka aykırı içerikleri teknik olarak tespit etmek ve denetlemek oldukça zordur. Halihazırda *deepfake* içeriği tümüyle tespit edip engelleyecek teknik bir sistem yoktur. Bu konuda yapılan bilimsel çalışmalara destek verilmesi hukuki sorunların çözümü bakımından büyük önem taşımaktadır. Hukuki yaptırımlar bakımından ise dünyada *deepfake* özelinde hukuka aykırı içeriklere yönelik yaptırımlar Amerika'nın bazı eyaletlerinde görülmeye başlanmış olup giderek yaygınlaşacağı öngörülmektedir. Avrupa Birliğinde 2024 yılında çıkarılan Yapay Zekâ Yasası'nda *deepfake* içerikler için etiketleme yapılması ve bu yolla içeriğe ulaşan kişileri bilgilendirerek bir şeffaflık sağlanması adına adımlar atılmış, bilimsel, sanatsal, eleştirel içerikler gibi bazı içerikler dışında bir bilgilendirme zorunluluğu öngörülmüştür. Mevzuatımızda *deepfake* teknolojisinin kullanımını sınırlayan ya da bu konuyla ilgili hukuki çerçeveyi belirleyen özel bir düzenleme olmamakla birlikte uygulamada yaşanan sorunların artması hâlinde bu tür bir ihtiyaç doğacağı açıktır. Özellikle ceza hukuku bakımından bir takım özel düzenlemelere gidilmesi caydırıcılık bakımından etkili olabilir.

Hukukumuzda *deepfake* yoluyla sesi ve görüntüsü ya da diğer kişilik değerleri ihlal edilen kimse kişilik hakkını koruyan genel düzenlemelere başvurabilir. Bu durumda TMK 23 vd., TBK 49 vd. ile

¹³⁴ TAŞKIN, Şaban Cankat: *Bilişim Suçları*, Beta Yayıncılık, İstanbul, 2008, s. 93 vd. "... Günümüzde ulaşılan teknolojik gelişmeler nedeniyle yasa dışı yollarla kişilerin her türlü özel konuşmalarının dinlenmesi, en özel görüntülerinin izlenmesi ve kaydedilmesi olanağı vardır. Gerçekten son yıllarda kişilerin ses ve görüntülerinin gizlice kaydedilerek kişilik haklarına zarar verilmesi nedeniyle 5237 sayılı Türk Ceza Yasası'nın 132, 133 ve 134. maddelerinde haberleşmenin gizliliğinin ihlali, kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması ile özel hayatın gizliliğinin ihlal edilmesi eylemleri ayrı ayrı suç olarak düzenlenmiştir...", Yargıtay, 4. HD, T. 23.06.2010, E. 2009/8119, K. 2010/7573 (YURTCAN, s. 9-11).

TBK 58. maddelerinden yararlanmak mümkündür. Kişi bu hükümlere dayanarak önleme davası, saldırının durdurulması (men) davası, tespit davası, haksız kazancın iadesi davası ve koşulları gerçekleşmişse maddi, manevi tazminat davalarını açabilir. Ayrıca sosyal medya aracılığıyla yapılan ihlallerde koşulları bulunması hâlinde 5651 sayılı Kanun hükümlerine göre bu şekilde içerik sağlayan kimsenin yanında yer sağlayıcının veya sosyal ağ sağlayıcının da hukuki sorumlulukları söz konusu olabilir. Sosyal medyada paylaşılan içerik bakımından sosyal ağ sağlayıcının sunduğu şikayet etme, bildirimde bulunma gibi bazı teknik çözümlere başvurulup, 5651 sayılı Kanun Ek 4 maddesindeki uyar-kaldır sisteminden ve düzenlemedeki diğer hükümlerden yararlanarak bir hukuki koruma sağlanmaya çalışılabilir. Ceza hukuku bakımından *deepfake* teknolojisi kullanılarak hazırlanan içerik sebebiyle somut olaya göre TCK 132-140 maddelerinde yer alan suçların oluşması mümkün olduğu gibi, hakaret, tehdit, şantaj gibi çeşitli suçların da oluşması söz konusu olabilir. Ayrıca belirtmek gerekir ki *deepfake* içeriklerle Türk Ceza Kanunu'na 217/A maddesi eklenen “Halkı yanıltıcı bilgiyi alenen yayma suçu”nun işlenmesi de mümkündür.

Tüm hukuki çözümlere rağmen *deepfake* içeriklerin ve bu içerikleri üretenlerin tespitindeki zorluklar ile içeriklerin internet ortamındaki yayılım hızları, bizleri teknik ve hukukun birlikte yol alması gereken bir çözüme doğru götürmektedir. Özellikle toplumun bilinçlendirilerek bu içerikler konusunda farkındalık kazandırılmasının büyük önem taşıdığı, dezenformasyona ve *deepfake* içeriğe daha duyarlı ve eleştirel bakış açısı için eğitime önem verilmesinin kaçınılmaz olduğu görülmektedir.

KAYNAKÇA

- ACABEY, Mehmet Beşir: “Basın Özgürlüğü ve Bu Özgürlüğün Bir Sınırı Olarak Kişilik Hakkı”, *Yaşar Üniversitesi E-Dergisi*, 2013, Cilt 8, Özel Sayı, s. 1-54.
- AJDER, Henry / PATRINI, Giorgio / CAVALLI, Francesco / CULLEN, Laurence: “The State of Deepfakes: Landscape, Threats, and Impact”, *Deepttrace*, 2019, s. 1-20.
- AJDER, Henry: *Deepfake Threat Intelligence: A statistics snapshot from June 2020*, 2020 (<https://perma.cc/ZHW5-53U7>, ET: 01.06.2025).
- AKİPEK, Jale / AKINTÜRK, Turgut / ATEŞ: Derya: *Türk Medeni Hukuku Başlangıç Hükümleri Kişiler Hukuku Birinci Cilt*, 18. Baskı, Beta Yayıncılık, İstanbul, 2022.
- AKKURT, Sinan Sami: *Sosyal Medyada Gerçekleşen İhlaller Karşısında Kişilik Hakkının Korunması*, 2. Baskı, Seçkin Yayıncılık, Ankara, 2020.
- AKMEŞE, Başak: “The Artificial Intelligence Dimension of Digital Manipulation Deepfake Videos: The Case of the Ukrainian-Russian People”, *Contemporary Issues of Communication*, 2023, Cilt 2, Sayı 2, s. 76-85.
- AKSOY RETORNAZ, E. Eylem: *Bir Siber Taciz Biçimi: Cinsel İçerikli Görüntüleri Rızaya Aykırı Olarak İfşa Etme, Yayma, Erişilebilir Kılma veya Üretme Suçu (Revenge Porn ve Deep Fake)*, On İki Levha Yayıncılık, İstanbul, 2021.
- AKYASAN BİRSEN, Gönül: *Sosyal Medyada Paylaşılan İçerik Nedeniyle Kişilik Hakkı İhlalleri*, Seçkin Yayıncılık, Ankara, 2020.
- ANIKAYDIN, İlayda: “Deepfake Uygulamalarının Hukuki Boyutu”, *Düzce Üniversitesi Sosyal Bilimler Dergisi*, 2022, Sayı 2, s. 736-747.
- ANTALYA, O. Gökhan / TOPUZ, Murat: *Marmara Hukuk Yorumu Medeni Hukuk Giriş Temel Kavramlar Başlangıç Hükümleri Cilt I*, 4. Baskı, Seçkin Yayıncılık, Ankara, 2021.
- ANTALYA, O. Gökhan: *Manevi Zararın Belirlenmesi ve Manevi Tazminatın Hesaplanması-Türk Hukukunda Manevi Tazminatın İki Aşamalı Olarak Belirlenmesine İlişkin Bir Model Önerisi*, Legal Yayıncılık, İstanbul, 2017.
- ARAS, Ümit Yaşar: *İnsan Hakları Temelinde Özel Hayat Hakkının Ulusal ve Uluslararası Alanda Uygulamaları*, Yüksek Lisans Tezi, Bahçeşehir Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2010.
- ARSLAN, Fatih: “Deepfake Teknolojisi: Kriminolojik Bir Literatür Taraması”, *Sakarya Üniversitesi Hukuk Fakültesi Dergisi*, 2023, Cilt 11, Sayı 1, s. 701-720.
- AYAN, Mehmet / AYAN, Nurşen: *Kişiler Hukuku Genel Bilgiler Gerçek Kişiler Tüzel Kişiler*, 9. Baskı, Adalet Yayınevi, Ankara, 2020.
- BAKER, Jennifer: *Deepfakes Could Break the Internet*, 2019 (<https://www.cpomagazine.com/cyber-security/deepfakes-could-break-the-internet/>, ET: 01.06.2025).
- BALCI, Murat / ÇAKIR, Kerim: “İnternet Ortamında ve Sosyal Ağlarda İşlenen Cinsel Suçlar”, *Anadolu Üniversitesi Hukuk Fakültesi Dergisi*, 2022, Cilt 8, Sayı 2, s. 201-214.
- BASTIAN, Matthias: *Deepfakes. China-Propaganda bei Facebook und Instagram*, 2020 (<https://the-decoder.de/deepfakes-china-propaganda-bei-facebook-und-instagram/>, ET: 02.06.2025).
- BELADA, Nurullah Enes Süheyl: “Deepfake Dezenformasyonu”, *Bilişim Hukuku Dergisi*, 2024, Sayı 1, s. 321-358.
- BERK, Mustafa Evren: “Dijital Çağın Yeni Tehlikesi ‘Deepfake’”, *OPUS Uluslararası Toplum Araştırmaları Dergisi*, 2020, Cilt 16, Sayı 28, s. 1508-1523.
- ÇEBER, Burak: “Yeni Nesil Reklam Aracı Olarak Yapay Zekâ Uygulamaları: Reklam Filmlerinde Deepfake Teknolojilerinin Kullanımı Üzerine Nitel Bir Çalışma”, (Ed.) BECAN, Cihan: *Tüketiciyi Anlamak: Reklam Araştırmalarında Disiplinlerarası Yaklaşımlar ve Yeni Yönelimler*, Efeakademi Yayınları, İstanbul, 2023, s. 11-43.
- ÇOLAK, Betül: *Legal Issues of Deepfakes*, 2021 (<https://www.internetjustsociety.org/legal-issues-of-deepfakes>, ET: 08.06.2025).
- DAMIANI, Jesse: *A Voice Deepfake Was Used to Scam a CEO Out of \$243,000*, 2019 (<https://www.forbes.com/sites/jessedamiani/2019/09/03/a-voice-deepfake-was-used-to-scam-a-ceo-out-of-243000/?sh=7de31b5c2241>, ET: 07.06.2025).

- DURAL, Mustafa / ÖĞÜZ Tufan: *Türk Özel Hukuku Cilt II Kişiler Hukuku*, 19. Baskı, Filiz Kitabevi, İstanbul, 2018.
- ERDOĞAN, İhsan / KESKİN, A. Dilşad: *Türk Medeni Hukuku Başlangıç Hükümleri Kişiler Hukuku*, 3. Baskı, Gazi Kitabevi, Ankara, 2020.
- EUROPEAN UNION AGENCY FOR LAW ENFORCEMENT COOPERATION: *Facing Reality?: Law Enforcement and the Challenge of Deepfakes, An Observatory Report from the Europol Innovation Lab*, Publications Office of the European Union, Luxembourg, 2022, s. 1-23.
- FARID, Hany / DAVIES, Alissa / WEBB, Lynette / WOLF, Clement / HWANG Tim / ZUCCONI, Alan / LYU, Siwei: *Deepfakes and Audio-visual Disinformation*, Centre for Data Ethics and Innovation (CDEI) Snapshot Series, United Kingdom, 2019.
- GERSTNER, Erik: "Face/Off: 'DeepFake' Face Swaps and Privacy Laws", *Defense Counsel Journal*, 2020, Cilt 87, Sayı 1, s. 1-14.
- İMRE, Zahit: "Şahsiyet Haklarından Şahsın Özel Hayatının ve Gizliliklerinin Korunmasına İlişkin Meseleler", *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası*, 1974, Cilt 39, Sayı 1-4, Ord. Prof. Dr. Sıddık Sami Onar Hatıra Sayısı, s. 147-168.
- KAYA, Mine: "Telekomünikasyon Alanında Kişilik Haklarının Korunması", *Ankara Barosu Dergisi*, 2010, Sayı 4, s. 279-334.
- KENT, Bülent: "Alman Hukukunda Sosyal Ağlarda Yalan Haber ile Mücadele", (Ed.) KENT, Bülent / KULLAR İBRAHİM, Merve Ayşegül: *Sosyal Medya Hukuku ve Yalan Haber*, Adalet Yayınevi, Ankara, 2022, s. 9-36.
- KIETZMANN, Jan / LEE, Linda W. / MCCARTHY Ian P. / KIETZMANN, Tim C.: "Deepfakes: Trick or treat?", *Business Horizons*, 2020, Cilt 63, Sayı 2, s. 135-146.
- KILIÇOĞLU, Ahmet M.: *Medeni Hukuk Temel Kavramlar Başlangıç Hükümleri Kişiler Hukuku*, 4. Baskı, Turhan Kitabevi, Ankara, 2021.
- KUGLER, Matthew B. / PACE, Carly: "Deepfake Privacy: Attitudes and Regulation", *North Western University Law Review*, 2021, Cilt 116, Sayı 3, s. 611-680.
- MANKOO, Sandeep Singh: "DeepFakes-The Digital Threat in the Real World", *Gyan Management Journal*, 2023, Cilt 17, Sayı 1, 2023, s. 71-77.
- MASCA, Mehmet Emin: *Advantages and Disadvantages of Deepfake Technology*, 2021 (<https://medium.com/geekculture/advantages-and-disadvantages-of-deepfake-technology-ccfa7c12b1ae>, ET: 02.06.2025).
- MENESES, João Paulo: *Deepfakes and the 2020 US elections: what (did not) happen*, 2021 (https://www.researchgate.net/publication/348740568_Deepfakes_and_the_2020_US_elections_what_did_not_happen, ET: 02.06.2025).
- METZ, Rachel: *Researchers can now use AI and a photo to make fake videos of anyone*, 2019 (<https://edition.cnn.com/2019/05/24/tech/deepfake-ai-one-photo/index.html>, ET: 02.06.2025).
- MÜLLER TERPITZ, Ralf: "Persönlichkeitsrechtliche Aspekte der Social Media", (Ed.) HORNUNG, Gerrit / MÜLLER TERPITZ, Ralf: *Rechtshandbuch Social Media*, 2. Baskı, Springer, Deutschland, 2021, s. 253-304.
- NAGUMOTU, Kavyasri: "Deepfakes Are Taking Over Social Media: Can The Law Keep Up?", *Idea: The Intellectual Property Law Review*, 2022, Cilt 62, Sayı 2, s. 102-146.
- NGUYEN, Thanh Thi / NGUYEN, Quoc Viet Hung / NGUYEN, Dung Tien / NGUYEN, Duc Thanh / HUYNH-THE, Thien / NAHAVANDI, Saeid / NGUYEN, Thanh Tam / PHAM, Quoc-Viet / NGUYEN, Cuong M.: "Deep Learning for Deepfakes Creation and Detection: A Survey", *Computer Vision and Image Understanding*, 2022, Cilt 223, s. 1-19.
- OĞUZ, Habip: *İnternet Ortamında Kişilik Haklarının İhlali ve Korunması*, Adalet Yayınevi, Ankara, 2010.
- OĞUZMAN, Kemal / SELİÇİ, Özer / OKTAY ÖZDEMİR, Saibe: *Kişiler Hukuku (Gerçek ve Tüzel Kişiler)*, 17. Bası, Filiz Kitabevi, İstanbul, 2018.
- ÖZDEMİR, Şebnem: "Yeni Nesil Tehdit: Derin Kurgu (DeepFake)", *TRT Akademi Dergisi*, 2021, Cilt 6, Sayı 13, s. 904-917.
- ÖZEL, Sibel: *Uluslararası Alanda Medya ve İnternette Kişilik Hakkının Korunması*, Seçkin Yayıncılık, Ankara, 2004.

- ÖZTAN, Bilge: *Kişiler Hukuku Gerçek Kişiler*, 11. Baskı, Yetkin Yayınları, Ankara, 2021.
- PAWELEC, Maria: “Deepfakes and Democracy (Theory): How Synthetic Audio-Visual Media for Disinformation and Hate Speech Threaten Core Democratic Functions”, *Digital Society*, 2022, Cilt 1, Sayı 19, s. 1-37.
- REES, Geraint: *Here’s How Deepfake Technology Can Actually Be a Good Thing*, 2019 (<https://www.weforum.org/agenda/2019/11/advantages-of-artificial-intelligence/>, ET: 03.06.2025).
- SOLMECKE, Christian: *Social Media Recht-Rechtssicher in sozialen Netzwerken unterwegs*, TeleLex, 2015.
- STONE, Jeff: *Chinese accounts blast Trump, with help from AI-generated pictures*, 2020 (<https://cyberscoop.com/graphika-spamouflage-dragon-china/>, ET: 03.06.2025).
- TAŞKIN, Şaban Cankat: *Bilişim Suçları*, Beta Yayıncılık, İstanbul, 2008.
- TURAN BAŞARA, Gamze: *Kişiliğin İhlalinden Kaynaklanan Maddi ve Manevi Tazminat ile Haksız Kazancın İadesi*, Turhan Kitabevi, Ankara, 2018.
- TURGUT, Cemile: *Kişilik Hakkının Bir Görünümü Olarak Unutulma Hakkı*, On İki Levha Yayıncılık, İstanbul, 2021.
- VACCARI, Cristian / CHADWICK, Andrew: “Deepfakes and Disinformation: Exploring the Impact of Synthetic Political Video on Deception, Uncertainty, and Trust in News”, *Social Media + Society*, 2020, Cilt 6, Sayı 1, s. 1-13.
- YAVUZ, Can: *Cinsel İçerikli Görüntülerin Rıza Dışı Paylaşımı-İntikam Pornosu*, Seçkin Yayıncılık, Ankara, 2021 (Rıza Dışı Paylaşım).
- YAVUZ, Can: *Deepfake (Derin Sahte)-Yapay Zekâ Tarafından Üretilen Yeni Nesil Görsel-İşitsel İçerik*, Seçkin Yayıncılık, Ankara, 2022 (Deepfake).
- YILDIZ, Ozan Ali: “Kişinin Görüntüsü Üzerindeki Hakkın Korunması”, *Fikri Mülkiyet Hukuku Kronikleri*, 2022, Sayı 1, s. 1-4.
- YURTCAN, Erdener: *Yargıtay Kararları Işığında Özel Hayata Karşı Suçlar*, Adalet Yayınevi, Ankara, 2016.
- YÜNLÜ, Semih: “Üretici Yapay Zekâ Kaynaklı Norm ve Kişi Bazlı Hukuki Sorumluluk”, *Adalet Dergisi*, 2024, Cilt 1, Sayı 72, s. 501-542 (Sorumluluk).
- YÜNLÜ, Semih: *Görüntü Üzerinde Kişilik Hakkı*, 2. Baskı, On İki Levha Yayıncılık, İstanbul, 2023 (Görüntü).
- ZEVKLİLER, Aydın / ERTAŞ, Şeref / HAVUTÇU, Ayşe / ACABEY, M. Beşir: *Yeni Medeni Kanun’a Göre Medeni Hukuk (Temel Bilgiler)*, 10. Baskı, Turhan Kitabevi, Ankara, 2018.