

Deepfake Teknolojisi ve Ceza Hukuku: Ses ve Görüntü Manipülasyonlarından Doğan Cezai Sorumluluk

Deepfake Technology and Criminal Law: Criminal Liability for Audio and Video Manipulation

Özet

Günümüz teknolojilerinin gelişmesi ile birlikte yapay zekâ ve derin öğrenme teknolojisinin öncülerinden olan "deepfake" uygulaması oldukça popüler hale gelmiştir. Deepfake "deep learning" (derin öğrenme) ve "fake" (sahte) kelimelerinden türetilmiş olup sahte veya manipüle edilmiş bir video veya ses kaydını ifade eder. Gelişen deepfake teknolojisi hukuk, eğitim, siyaset, ticaret, eğlence gibi hayatın her alanında etkili olmaktadır. Deepfake teknolojisi ile üretim yapılırken gerçek ve tüzel kişilere ait özellikle metin, ses, görüntü gibi veriler kullanılarak yüksek kaliteli ve gerçekçi ses, görüntü ve videolar oluşturulmaktadır. Bu veriler yasal olarak olumlu amaçlar için kullanılmakla beraber yasadışı ve olumsuz amaçlar için de kullanılmaktadır. Özellikle Ceza Hukuku açısından dolandırıcılık, şantaj, kişinin rıza dışı alınmış görüntüleri ile pornografik içerik üretme, yanlış bilgi yayma, sahte haber yaratma gibi durumlarda deepfake ile oluşturulmuş sahte ses ve görüntüler büyük önem taşımaktadır. Deepfake teknolojisi ile oluşturulmuş ses ve görüntülerin adli olaylara konu edilmesi, ceza hukukunda doğurduğu veya doğurabileceği sorunlar ile hangi suçlara sebebiyet verebileceği ve adli olaylara konu olmuş ses ve görüntülerin delil değeri ulusal ve uluslararası öğreti incelenerek değerlendirilecektir.

Abstract

With the development of today's technologies, the "deepfake" application, which is one of the pioneers of artificial intelligence and deep learning technology, has become very popular. Deepfake is derived from the words "deep learning" and "fake" and refers to a fake or manipulated video or audio recording. The developing deepfake technology is effective in all areas of life such as law, education, politics, trade and entertainment. While producing with deepfake technology, high quality and realistic sound, images and videos are created by using data such as text, sound and images belonging to real and legal persons. These data are legally used for positive purposes, but they are also used for illegal and negative purposes. Especially in terms of Criminal Law, fake voices and images created with deepfake are of great importance in cases such as fraud, blackmail, producing pornographic content with non-consensual images of a person, spreading false information, creating fake news. The subject matter of the audio and images created with deepfake technology to forensic events, the problems that it causes or may cause in criminal law, which crimes it may cause and the evidential value of the audio and images that have been subject to forensic events will be evaluated by examining the national and international doctrine.

Giriş

Teknolojinin gelişmesi ve yaygınlaşmasıyla beraber dijital içerik üretimi, tüketimi ve sosyal medya kullanımı artmış, dijital çağa geçilmiştir. Dijital çağın getirdiği yeniliklerden biri de yapay zekâdır. Yapay zekâ kavramı ile hayatımıza birçok yenilik girmiş olup bu yeniliklerin biri de "deepfake" kavramıdır. Deepfake kavramı "deep learning" (derin öğrenme) ve "fake" (sahte) kavramlarının birleşiminden meydana gelmiştir (Pradhan, 2020). Deepfake teknolojisi, mevcut görüntü ve videolara ses, görüntü, hareket eklenerek veya bunları manipüle etmek suretiyle derin öğrenme algoritmalarını kullanan yapay zekâ teknolojisinin bir türüdür (Kietzmann, Lee, McCarthy

Nergis Belen

Avukat, Yüksek Lisans Öğrencisi, Gazi Üniversitesi, Ankara, Türkiye, 24801002005@gazi.edu.tr
Orcid No: <https://orcid.org/0009-0007-4494-212X>

Nursel Yalçın

Doç. Dr., Gazi Üniversitesi, Ankara, Türkiye, nyalcin@gazi.edu.tr
Orcid No: <https://orcid.org/0000-0002-0393-6408>

Article Type / Makale Türü

Research Article / Araştırma Makalesi

Anahtar Kelimeler

Deepfake Teknolojisi, Yapay Zekâ, Derin Öğrenme, Ceza Hukuku, Ses ve Görüntü

Keywords

Deepfake Technology, Artificial Intelligence, Deep Learning, Criminal Law, Audio and Video

Submitted: 15 / 01 / 2025

Accepted: 31 / 05 / 2025

ve Kietzmann, 2020:136). Her teknolojinin olumlu ve olumsuz getirileri olduğu gibi deepfake teknolojisi de birtakım yenilik ve fırsatların yanında olumsuzluklar getirmektedir. Deepfake teknolojisinin sinema, eğitim, sanat, moda gibi alanlarda olumlu bir kullanımı varken özellikle siyasi propaganda, sahte haber ve pornografik içerik üretmek gibi alanlarda olumsuz bir kullanımı vardır (Westerlund:41). Deepfake teknolojisi bazı suçların işlenmesinde araç olarak da kullanılabilir. Bu gibi durumlarda karşımıza ceza hukuku çıkmaktadır. Bu çalışmada deepfake teknolojisinin tanımı yapılacak, bu teknolojinin olumlu ve olumsuz kullanım alanlarına değinilecek, deepfake ile ilgili ulusal ve uluslararası mevzuatlar incelenecek ve ülkemizdeki mevzuatlar kapsamında deepfake aracılığıyla işlenen suçlara değinilecektir. Son olarak da deepfake teknolojisinin özellikle ceza hukukunda ne denli tehlikeli olabileceği konusunda farkındalık yaratmak ve hangi önlemlerin alınabileceği hakkında bilgi sunmak adına bu çalışma ele alınmıştır.

1. Deepfake Teknolojisinin Tarihçesi ve Benzer Kavramlar

“Deepfake” terimi, “deep learning” (derin öğrenme) kavramının “deep” kısmı ve “fake” (sahte) kelimelerinin birleşmesi ile ortaya çıkmıştır (Pradhan, 2020). Deepfake teknolojisi, makine öğrenimi (machine learning) ve yapay zekâ (artificial intelligence) teknikleri kullanılarak görsel veya işitsel içerikleri birleştirmek veya üst üste bindirmek suretiyle gerçek olmayan video, ses, görüntü üreten ya da manipüle eden teknolojiyi ifade eder (Kietzmann, Lee, McCarthy ve Kietzmann, 2020:136).

Deepfake kavramı ilk olarak 2017 yılının sonlarında ‘deepfakes’ adlı bir Reddit kullanıcısının (Reddit, Amerikan sosyal haber, tartışma sitesidir. Sitedeki kullanıcılar bağlantı, fotoğraf, anket, video ve fotoğraf içeren gönderiler paylaşabilir ve diğer kullanıcılar da bu gönderileri oylayarak gönderinin ana sayfada çıkmasını sağlayabilirler.) Hollywood ünlülerinin yer aldığı pornografik videolar paylaşmasıyla ortaya çıkmıştır (Negi, Jayachandran ve Upadhyay, 2019:183). Bu olay kamuoyunun oldukça dikkatini çekmiş ve sahte içeriklerin yayılmasına yol açmıştır. Sadece aktörlerle kalmayıp şarkıcılar, politikacılar, sporcular gibi birçok ünlü isim deepfake içeriklerin hedefi haline gelmiştir (Kietzmann vd, 2020:136).

Deepfake teknolojisini incelenirken “yapay zekâ” (artificial intelligence), “makine öğrenmesi” (machine learning), “derin öğrenme” (deep learning) ve “ses klonlama” (voice cloning) kavramlarına kısaca değinmekte yarar vardır.

1.1. Yapay Zekâ (Artificial Intelligence)

Yapay zekâ artık sadece bilim kurgu eserlerinde olmayıp hayatımızın her alanında yer edinebilen hatta edinen bir kavramdır. 1956 yılına kadar yapay zekâ kavramı için İngiliz matematikçi Alan Turing tarafından ortaya atılan “makine zekâsı” kavramı kullanılmaktayken 1956 yılında Amerikalı bilgisayar bilimci John McCarthy tarafından ilk defa “yapay zekâ” terimi ortaya atılmıştır (Russell ve Norvig, 2010:17). Yapay zekâ ile ilgili birden çok tanımlama bulunmaktadır. Örneğin Kurzweil’e göre yapay zekâ “insanlar tarafından gerçekleştirildiğinde zekâ gerektiren işlevleri yerine getiren makineler yaratma sanatı”dır (Kurzweil, 1990:14). Avrupa Komisyonu’nun 2018 tarihli “Avrupa için Yapay Zekâ” başlıklı raporuna göre de yapay zekâ, “çevreleri analiz ederek ve belirli hedeflere ulaşmak için belirli dereceye kadar özerklikle harekete geçerek akıllı davranış sergileyen sistemler” olarak tanımlanmaktadır (Avrupa Birliği Komisyonu, 2018).

1.2. Makine Öğrenimi (Machine Learning)

Makine öğrenimini kısaca tanımlayacak olursak makinenin bir konuyu anlamadan önce o konuda birçok veri toplaması ve bu verilere dayanarak bir görevin nasıl yapılacağını öğrendiği süreçtir (Turan, 2016:218). Makine öğrenimi yeni şartlara uyum sağlayarak kalıpları tespit ederek tahmin yürütme üzerine kuruludur (Russell ve Norvig, 2010:2). Makine öğrenmesi literatürde yapay zekâ ile öğrenme olarak da tanımlanmaktadır (Turan, 2016:218).

1.3. Derin Öğrenme (Deep Learning)

Derin öğrenme kavramı ise makine öğrenmesinin bir alt türüdür ve çok katmanlı yapay sinir ağları oluşturularak gerçekleştirilen bir öğrenme yöntemidir (Ergün, 2023:730). Bu yöntem insan beyninin çalışmasını taklit eder ve büyük miktardaki veriler daha fazla yapay sinir ağı katmanı oluşturularak daha kolay işlenebilmektedir (Sarker, 2021:419).

1.4. Ses Klonlama (Voice Cloning)

Ses klonlama, bir bilgisayar programı kullanılarak insan sesinin yapay olarak kopyalanması şeklinde tanımlanabilir. Ses klonlama aynı zamanda ses taklidi veya ses sentezi olarak da bilinir ve bir kişinin sesini başkasının sesine benzetme amacıyla makine öğrenimi kullanılarak geliştirilen bir teknolojidir. Bu teknolojiye kişinin ses tınısı, tonlaması, ritmi, kelime ve nefesin akışı gibi ses özelliklerini analiz etmek ve onu öğrenmek için bir miktar ses verisine ihtiyaç duyulur. Bu veriler tanımlandıktan sonra ise orijinal sese çok yakın bir konuşma üretilebilir (Palmai, 2021).

2. Deepfake Teknolojisinin Kullanım Şekilleri

Deepfake uygulamasının bilinen 3 tür kullanımı mevcuttur.

2.1. Yüz Değiştirme

Yüz değiştirme, yüz yerleştirme olarak da bilinir ve yüksek kalitede bir fotoğraf veya videodan bir kişinin yüz kısmının kesilerek manipülasyon tekniği ile farklı bir yüze monte edilmesi işlemidir. Şekil 1’de görüldüğü gibi kaynak yüzden hedef yüze yapay zekâ sistemi ile resim monte edilir (Berk, 2020:1512).

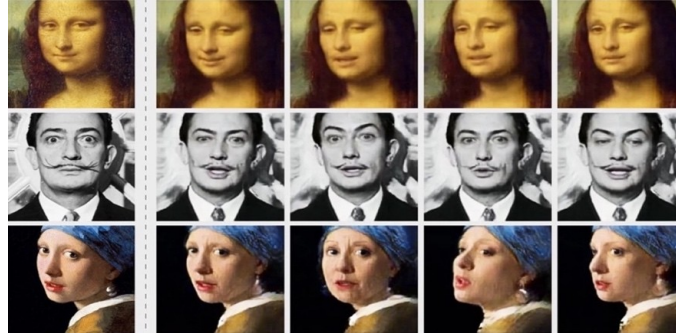


Şekil 1. Yüz Değiştirme Tekniğine Örnek Bir Görsel

Kaynak: (<https://www.technopat.net/2020/07/06/disneyden-etkileyici-yuz-degistirme-teknolojisi>)

2.2. İfade Değiştirme

Kuklacılık olarak da bilinen bu yöntem, hedef yüzün hareketlerinin, kaş, göz, ağız ifadelerinin tekrar yaratılması işlemidir. İfade değiştirme tekniğinde kaynak yüzden alınan yüz hareketleri başka bir kişinin yüz videosunun üzerine eklenir. Bu işlemde amaçlanan şey, hedef kişinin bir konu hakkında bir şeyi söylemese bile kaynak videodan aldığı ifadeleri taklit etmesiyle o şeyi söylüyormuş gibi göstermektir (Berk, 2020:1513). Şekil 2, ifade değiştirme tekniğine bir örnek olarak gösterilebilir.



Şekil 2. İfade Değiştirme Tekniğine Bir Örnek

Kaynak: (<https://www.wired.com/story/deepfakes-getting-better-theyre-easy-spot/>)

2.3. Yüz Yaratımı

Üretken Çekişmeli Ağlar (Generative Adversarial Networks) tarafından geliştirilen bu sistemde “üretken” ve “ayrıştırıcı” olmak üzere iki farklı sinir ağı ortaya çıkmaktadır. Üretken ve ayrıştırıcı ağlar birbirleri ile mücadele içerisinde. Mücadele etme amacı ise üretken ağ resim oluştururken ayrıştırıcı ağ bu resmin gerçekliği üzerinde derin öğrenme sürecine girer. Eğer üretken ağ ayrıştırıcı ağı kandırır ve resmin gerçek olduğuna inandırırsa ayrıştırıcı ağ derin öğrenme sürecine geçer. Ancak bir yanıltma söz konusu olmaz yani resmin sahte olduğunu ayrıştırıcı ağ anlarsa bu durumda üretken ağ daha gerçekçi şekilde üretime devam edecektir (Farid, Hwang, Lyu ve Zucconi, 2019:5).

Yukarıda bahsedilen her üç yöntemin kendine has çalışma prensipleri vardır. Bu teknikler arasından en çok tercih edilen yüz değiştirme (Face Replacement) işlemidir. Bilgisayarların teknik özelliklerine ve hızına göre bu işlemin uzunluğu değişmektedir. Görsel manipülasyon aslında çok eskilere dayanmaktadır. Ancak deepfake çıktıktan sonra ilgili yazılım ve yönergelerle, manipülasyon herkesin kolayca yapabileceği bir teknik haline gelmiştir. Derin öğrenme ile işlem yapan yazılımlarla yüz değiştirme işlemi çok daha kolay ve hızlı yapılabilir durumdadır (Berk, 2020:1514).

3. Deepfake Teknolojisinin Toplumsal Yaşama Etkisi

Gelişen ve erişimi kolaylaşan teknolojiyle birlikte deepfake teknolojisine ulaşmak da oldukça kolay hale gelmiştir. En basitinden hemen hemen herkesin kullandığı Instagram, SnapChat, TikTok gibi sosyal medya platformları; video, görüntü düzenleme ve yüz filtreleme araçları gibi manipülasyon seçeneklerini içermektedir. Bu da görüntü ve videoların manipülasyonlarını normalleştirmektedir (Avrupa Parlamentosu Araştırma Servisi, 2021).

Deepfake içeriklerinin kalitesi de gelişen teknolojiyle birlikte artmaktadır. Herkesin ulaşabildiği bu teknoloji günümüzde daha çok kişilerin rızası dışında alınmış pornografik görüntü ve videolarının üretilmesinde kullanılsa da eğitim, eğlence, sağlık, sanat, kültür, siyaset, ekonomi, habercilik, hukuk gibi birçok alanda kullanılmaktadır. Deepfake teknolojisi kimi alanda yararlı amaçlar için kullanılırken kimi alanda da zararlı amaçlar için kullanılmaktadır.

3.1. Deepfake Teknolojisi'nin Olumlu Etkileri

3.1.1. Eğitim Alanında Olumlu Etkileri

Deepfake teknolojisi, eğitimde çeşitli şekillerde ve aşamalarda kullanılmaktadır. Deepfake, bir eğitimcinin sıkıcı geleneksel ders anlatım yöntemlerinin dışına çıkarak çok daha ilgi çekici ve akılda kalıcı ders anlatımına olanak tanımaktadır (Citron ve Chesney, 2019:1769). Deepfake teknolojisi sayesinde ölmüş tarihi figürlerin canlandırılmış videoları üretilerek eğitim materyali olarak kullanılması, derslere olan ilgiyi artıracaktır. Aynı zamanda öğrencilerle doğrudan konuşan tarihi figürler üretmek de mümkün olacak ve bu da öğrenciler için dersi çekici hale getirebilecektir. Örneğin Samsung AI ve Skolkovo Bilim ve Teknoloji Enstitüsü'nün ortak yürüttüğü çalışma ile Albert Einstein ve Mona Lisa gibi tarihi figürler canlandırılmıştır (Feeney, 2021:5). Deepfake teknolojisi sadece öğrenciler için değil eğitimciler için de farklı yöntemler ve materyaller kullanmaları için fırsatlar sunmaktadır. Nelson Mandela veya Gandhi gibi tarihi figürlerin kendileri ve yürütmüş olduğu çalışmaları anlattığı bir video üretilip öğrencilere sunmak eğitimi çok daha ilgi çekici hale getirecektir. (Dagar ve Vishwakarma, 2022:220) Instagram'da "onlocklearning" adlı bir sayfa; aktör, siyasetçi, şarkıcı gibi ünlü insanların görüntülerini deepfake aracılığıyla kullanarak eğitim materyalleri oluşturmakta ve oldukça beğeni toplayan videolar üretmektedir. Aynı zamanda deepfake teknolojisi, tıp öğrencilerine simüle hastalar üreterek teşhis ve tedavi deneyimi sağlayabilmektedir (Aydın, 2024:70).

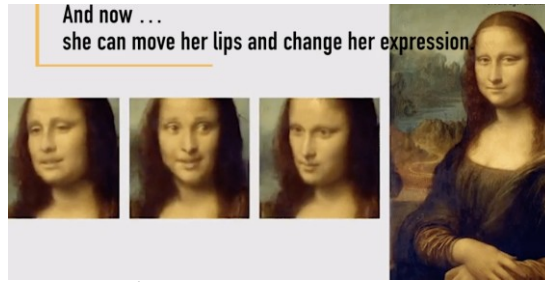
3.1.2. Sanat ve Kültür Alanındaki Olumlu Etkileri

Deepfake teknolojisi, sanat ve kültürün farklı dallarında da kullanılmaktadır. Müzelerin ziyaretçi sayısını arttırmak, izleyicileri etkilemek ve ziyaretçilere farklı deneyimler sunmak amacıyla deepfake teknolojisi kullanılmaktadır. Örneğin Florida St. Petersburg'daki Dali Müzesi'nde, bir reklam ajansı ile iş birliği yapılmış, röportajlardan elde edilen arşiv görüntüler kullanılarak 6.000'den fazla kare çekilmiş ve makine öğrenimi ile Dalí'nin vücut oranlarına sahip bir aktörün üzerinde canlandırılmıştır. Burada Dalí'nin bulunduğu kiosktaki kapı ziline basıldığında, Salvador Dali ziyaretçileriyle buluşarak onlara hayatıyla ilgili hikayeler anlatmaktadır. Sonunda da Dali, ziyaretçilere selfie çekmek isteyip istemediklerini sorup, şekil 3'te görüldüğü gibi izleyiciler çekmek isterlerse arkasını dönüp selfie çekmekte ve bu fotoğraf mesaj yolu ile ziyaretçilere iletilebilmektedir (Lee, 2019).



Şekil 3. "Dali Lives" Adlı Sergiden Bir Görüntü
Kaynak: (Wilson, 2019)

Bir başka örnek de 2019'da Moskova'daki Samsung Yapay Zekâ Laboratuvarı'ndan araştırmacılar Leonardo da Vinci'nin "Mona Lisa" veya Gustav Klimt'in "Johanna Staude Portresi" gibi tabloları konuşturmuş ve şekil 4'te görüleceği üzere gerçek insan gibi hareket ettirmiştir (Weisberger, 2019).



Şekil 4. Deepfake İle Canlandırılmış Mona Lisa Görüntüsü
Kaynak: (Weisberger, 2019)

Deepfake kullanımı portrelerle sınırlı kalmayıp konser sahnelerine kadar taşınmıştır. Şekil 5'te görülen ünlü rapçi Eminem, alter egosu olan Slim Shady'nin deepfake ile oluşturulmuş videosu ile performans sergilemiştir (Foley, 2024).



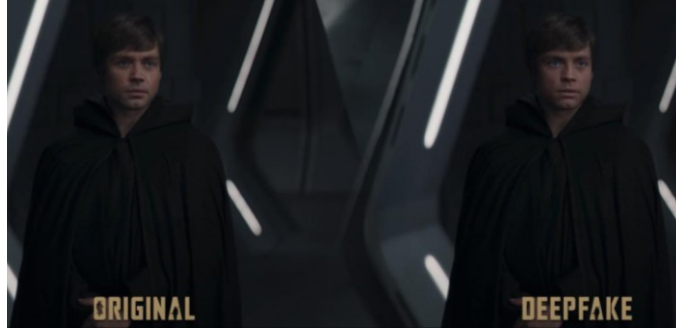
Şekil 5. Eminem'in Deepfake Slim Shady İle Birlikte Sahne Performans Görüntüsü
Kaynak: (Foley, 2024)

3.1.3. Film Endüstrisi Alanındaki Olumlu Etkileri

Film endüstrisi alanında da deepfake teknolojisinden farklı şekillerde yararlanılabilmektedir. Film sahnelerinin uzun süren çekimlerindeki hatalarda veya güncelleme gereken durumlarda sahneleri yeniden çekmek yerine deepfake teknolojisi sayesinde daha düşük maliyetle güncelleme yapılabilir hale gelmiştir. Yapımcılar deepfake sayesinde hayatını kaybetmiş aktörler için yeni filmler yapabilmekte, amatör veya eski videoların kalitelerini arttırabilmektedirler (Westerlund, 2019:41).

Örneğin The Mandalorian dizisinde Luke Skywalker karakterini canlandıran Mark Hamill'in görüntüsü ikinci sezonun finalinde dijital görsel efekt ile yeniden yaratılarak izleyicileri şaşırtmıştır. Şekil 6'da Mark Hamill'in deepfake ve orijinal görüntüleri görülmektedir. Bir kısım izleyici Luke Skywalker'ı görmekten memnun olsa da karakterin deepfake ile yapılan görüntüsü eleştiriler de almıştır. Yine YouTube platformunda içerik üretici olan Shamook adlı bir kullanıcı Mark Hamill'in

deepfake ile oluşturulmuş görüntüsünü paylaşmış ve deepfake teknolojisinin gençleştirme konusunda başarılı olduğunu göstermiştir. Bu başarısı sayesinde Lucas Film, Shamook'u görsel efekt departmanında çalışmak üzere işe almıştır (Aydın, 2024:64).

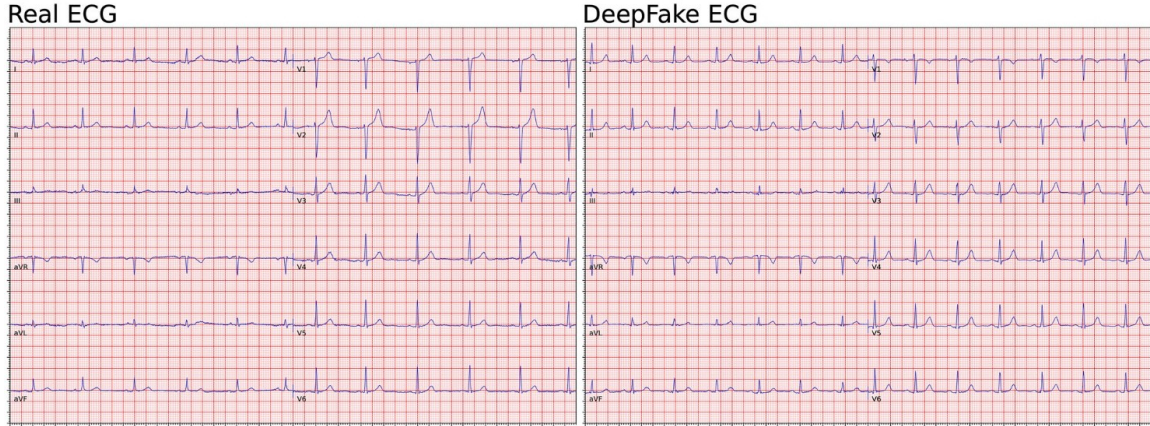


Şekil 6. Luke Skywalker'ın Orijinal ve Deepfake Görüntü Karşılaştırması
Kaynak: (Sharf, 2021)

Belgesel yapımcıları da filmlerindeki kişileri gizlemek amacıyla deepfake teknolojisi kullanmaktadırlar. 2020 yılında çekilen HBO belgeseli olan "Welcome to Chechnya"da yapımcılar, Çeçenistan'da cinsel yönelimleri sebebiyle işkenceye, ciddi yaralanmalara ve ölüme yol açabilen eşcinsel Çeçenlerin kimliklerini gizlemek için deepfake teknolojisini kullanmışlardır (Rothkopf, 2020).

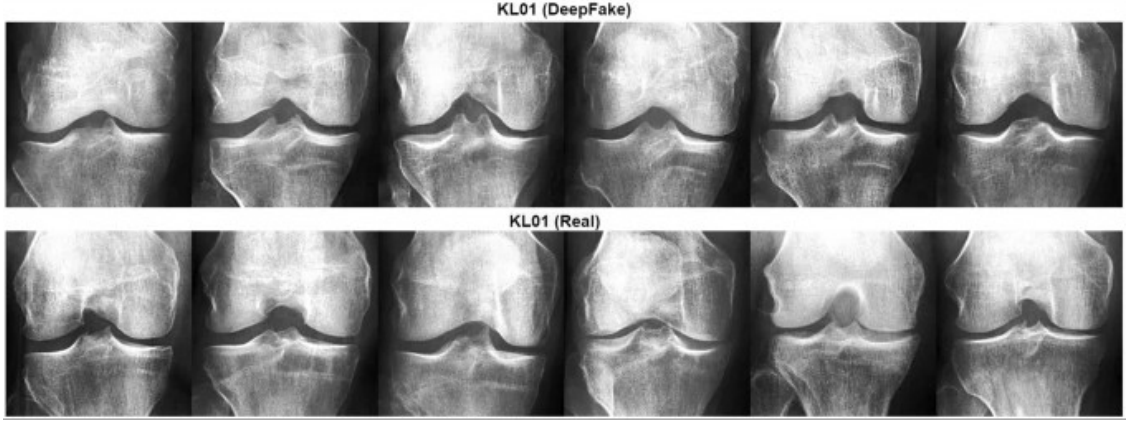
3.1.4. Sağlık Alanındaki Olumlu Etkileri

Deepfake teknolojisi, diğer alanlarda olduğu gibi sağlık alanında da kendini göstermiştir. 2021 yılında yapılan bir çalışmada derin öğrenme yöntemi kullanılarak şekil 7'de görüldüğü gibi sentetik EKG görüntüleri oluşturulmuş ve bu görüntüler gerçek EKG görüntülerle karşılaştırılmıştır. Karşılaştırma sonucunda iki görüntü arasında bazı özelliklerde benzerlikler tespit edilmiştir. Bu tespitler, tıbbi görüntüleme ve teşhiste derin öğrenmenin potansiyel bir yardımcı olabileceğini göstermektedir (Thambawita, Isaksen, Ghouse, Ahlberg, Linneberg, Hammer vd, 2021:2).



Şekil 7. Gerçek EKG ve Deepfake EKG Karşılaştırması
Kaynak: (Thambawita vd., 2021)

2022 yılında ise deepfake teknolojisinin ortopedi alanında kullanımında dair çalışma yapılmıştır. Araştırmacılar, diz eklemünde görülen 'osteoartrit' hastalığının röntgen görüntülerini üretmek için bir GAN (Generative Adversarial Network) modeli geliştirmişlerdir. Bu model hastalığın evrelerindeki (0, 1, 2, 3 ve 4 evreleri) farklılıkları saptamak için eğitilmiştir. Sonuç olarak üretilen gerçekçi röntgen görüntüleri uzmanlara sunularak anket yapılmış ve anket sonucunda uzmanların deepfake görüntülerin bazılarını, gerçek görüntülerden ayırt edemediği saptanmıştır (Prezia, Paloneva, Pölönen, Niinimäki ve Äyrämö, 2022:2). Şekil 8'de deepfake ve gerçek osteoartrit görüntülerin karşılaştırılması yapılmıştır.



Şekil 8. Deepfake Ve Gerçek Osteoartrit Görüntüleri

Kaynak: (Prezia vd., 2022)

Deepfake teknolojisi, alzheimer hastası olan kişilere gençlik yıllarını hatırlatmak ve hastalıkla mücadelede yardımcı olabilecektir (Westerlund, 2019:41). Yine aynı şekilde deepfake, bazı kanser türlerini tespit etmede, MRG (Manyetik Rezonans Görüntüleme) ile hastalık tiplerini sınıflandırmada ve X-ray’de anormalliklerin tespit edilmesinde kullanılmıştır. Tabi bu görevlerin düzgün bir şekilde yerine getirilebilmesi için çok fazla sağlık verisine ihtiyaç vardır. Burada da gizlilik ve etik gündeme gelecektir. Bu nedenle yeterli veriye ulaşmak mümkün olmamaktadır. Bu sınırı aşabilmek için de GAN modelleri, gerçeğe yakın sentetik tıbbi görüntüler üreterek örnek veri sayısını arttırmayı hedeflemektedir (Lakshmi ve Hemant, 2024:306).

Tıp bilminde yapay zekanın yaygınlaşarak kullanılacağını söylemek mümkündür. Yapay zekâ yardımıyla bazı hastalıkların teşhis ve tedavi şekillerinin belirlenmesi halen deneme ve araştırma aşamalarında (İlkılıç, 2021:122).

3.1.5. Reklam ve Pazarlama Alanındaki Olumlu Etkileri

Deepfake teknolojisinin yaratıcı içerik üretebilme yapısından reklam ve pazarlama sektörü de etkilenmiştir. Farkındalık oluşturmak, kullanıcı deneyimi paylaşmak, ürün veya hizmet tanıtmak veya bunları pazarlamak gibi konularda deepfake yaratım alanı bulmaktadır. Örneğin 2021 yılında Ziraat Bankası’nın “Sen Hep Gülümse” başlıklı reklamında deepfake teknolojisi kullanılarak Kemal Sunal oynatılmıştır. Şekil 9’da da görülen Yeşilçam’ın çok sevilen oyuncularından olan Kemal Sunal’ın videosunun oluşturulması sayesinde reklam büyük ilgi görmüştür (Aydın, 2024:63).



Şekil 9. Ziraat Bankası Kemal Sunal Reklamı

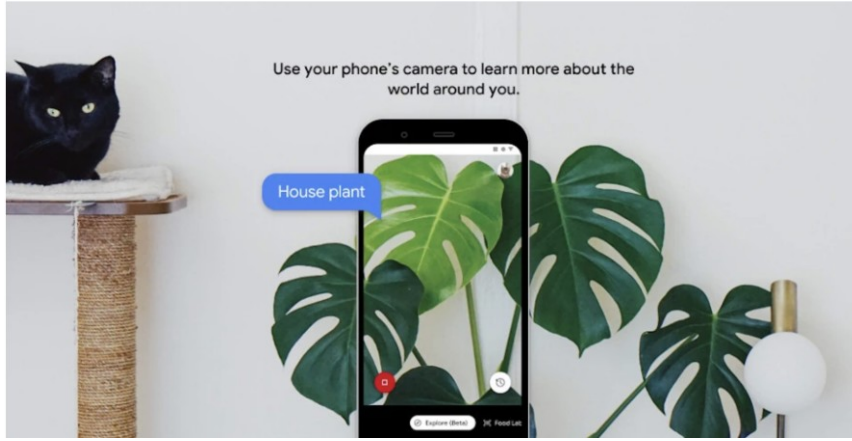
Kaynak: (<https://www.youtube.com/watch?v=fPiwmoxa0QE>)

Bir başka örnek verecek olursak ödüllü bir reklam olan “Sadece Bir Cadbury Reklamı Değil” kampanyasında ünlü aktör Shah Rukh Khan, insanları Hint işletmelerini desteklemeye davet

etmiştir. Bu reklam küçük işletmelere örnek olmuş ve ünlü aktörün deepfake ile oluşturulmuş içeriklerini kullanarak yerel işletmelerini tanıtmaya başlamışlardır (Aydın, 2024:62). Yine aynı şekilde 2019'da David Beckham'ın da yer aldığı Küresel Sıtma Farkındalık Kampanyası başlatılmıştır. Deepfake teknolojisi sayesinde David Beckham'ın dokuz dil konuşması mümkün olmuş ve çok daha düşük bir maliyetle video pazarlanmıştır (Westerlund, 2019:41).

3.1.6. Teknoloji Alanındaki Olumlu Etkileri

Deepfake'in de bir teknoloji olduğu düşünüldüğünde deepfake teknolojisinin, diğer teknolojilerin kullanılmasında ve geliştirilmesinde olumlu etkileri olduğunu söylemek mümkün olacaktır. Örneğin Google tarafından üretilen Lookout ve Microsoft tarafından üretilen Seeing AI; etrafımızdaki nesneleri, insanları tanımlamak ve bunları sesli olarak aktarmak için yapay zekadan yararlanmaktadır. Şekil 10'da görülebileceği gibi telefonun kamerasını kullanarak çevrelerindeki tüm görsel öğeleri sesli komutla algılayabilme, metin okuyabilme özellikleri vardır. Bu uygulamalara son yapılan güncellemelerle görüntüyle ilgili soru-cevap yapabilmeye özelliği getirilmiştir. Tüm bunlar özellikle görme engelli bireyler için oldukça önem taşımakta ve çevrelerini daha iyi algılayabilmelerine yardımcı olmaktadır (Jaiman, 2020). Canetroller ise bir dokunsal baston denetleyicisidir ve görme engellilerin baston etkileşimleriyle sanal dünyada gezinmelerine yardımcı olmaktadır (Zhao, Curtell, Holz, Morris, Ofek ve Wilson, 2019:2).



Şekil 10. "Lookout" Uygulamasının Reklamından Bir Görsel

Kaynak: (<https://www.xatakandroid.com/aplicaciones-android/google-lookout-aplicacion-que-ayuda-a-personas-problemas-vision-llega-espanol>)

3.2. Deepfake Teknolojisinin Olumsuz Etkileri

3.2.1. Siyasi ve Sosyal Alanda Olumsuz Etkileri

Deepfake teknolojisinin olumsuz olarak kullanıldığı alanlardan biri siyasettir. Doğrudan ve dolaylı olarak bu olumsuzluklar toplumu da olumsuz etkileyecektir. İlk olarak sahte haber probleminden bahsetmek gerekir. Sanal ortamda yayınlanan binlerce haber, bilgi vardır ve bu haberler için doğruluk kontrol sistemi bulunmamaktadır. Ayrıca bir haber medyada bir günde milyonlarca kez görüntülenebilmektedir. Sahte haber ve bilgiler yüzünden medyaya olan güven son derece azalmış durumdadır ve deepfake teknolojisinin ortaya çıkması ile bu güven ilişkisinin daha da zayıflaması muhtemeldir. Gerçek olan ise ulusal ve küresel bazda siyasal anlamda sorunların olacağıdır (Dean, 2020:21; Anıkaydın, 2022:739).

Sahte haber üretmek, yanlış bilgi yaymak; bazı insanları manipüle etmek veya toplumda kargaşa yaratmak amacıyla kullanılabilir. Deepfake teknolojisi kullanılarak oluşturulmuş videolarla siyasi liderlerin sözleri çarpıtılabilir veya yanıltıcı ifadeler eklenerek kamuoyu manipüle edilebilir (Whyte, 2020). Örneğin sahte bir video paylaşımı, yaklaşan bir füze saldırısı ya da bulaşıcı bir hastalığı duyurma gibi halkı paniğe sürükleyebilir. Yine sahte bir video ile ülkeler arası diplomatik ilişkileri bozacak, ayaklanmalara neden olacak, şiddete yol açacak kışkırtıcı içerikler üretilebilir (Citron ve Chesney, 2019:1776). Bu tarz videoların hızlı yayılması da toplumda bir çatışmaya neden olabilir. Deepfake ses kayıtları kullanılarak siyasi liderlerin söylemediği sözler söylenmiş gibi gösterilebilir, sahte telefon görüşmeleri ve sahte sesli mesajlar üretilebilir. Bu durum siyasi liderlerin

veya sahte ses kaydı üretilen kişilerin itibarını zedeleyebilir ve yanlış bilgilere dayanarak haklarında yanlış kararlar alınmasına neden olabilir (Whyte, 2020).

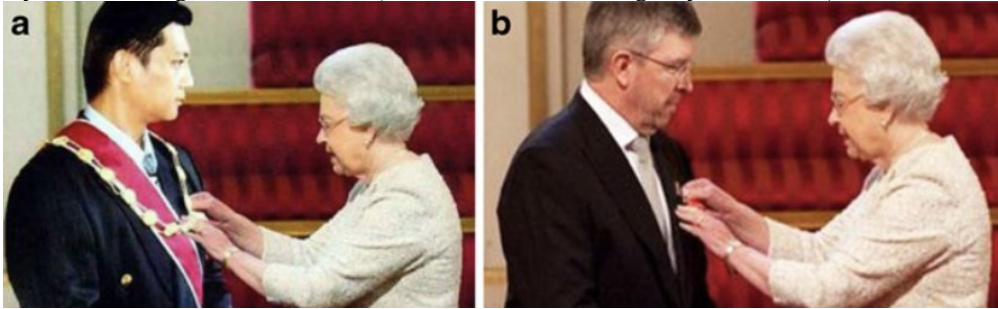
Bu durumun en bilinen örneği şekil 11’de görülen Amerikalı oyuncu Jordan Peele’nin ağzı Amerika Birleşik Devletleri’nin eski başkanı olan Barack Obama’nın üzerine yapıştırılmış ve Obama’nın ağzından “*Başkan Trump tam ve eksiksiz bir aptaldır*” cümlesi söylenmiş gibi gösterilmiştir (Mack, 2018).



Şekil 11. Barack Obama’nın, Peele’nin Ağzıyla Konuştuğu Video Görüntüsü

Kaynak: (<https://www.youtube.com/watch?v=cQ54GDm1eL0>)

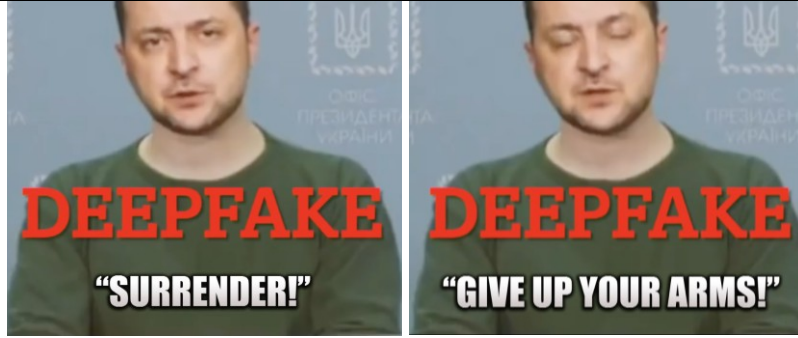
Yine bir başka örnek, Malezyalı politikacı Jeffrey Wong Su En, uluslararası yardım kuruluşu Sınır Tanımayan Doktorlar’a yaptığı katkılarından dolayı Kraliçe II. Elizabeth tarafından şövalye ilan edildiğini iddia etmiş ve şekil 12-a’da görülen Elizabeth tarafından ödüllendirildiğine dair görseli medyada yayınlamıştır. Ancak ödülle ilgili soru sorulduğunda İngiliz Yüksek Komisyonu, Bay Wong’un adının resmi şövalyelik listesinde yer almadığını ve ilgili görselin şövalyelik törenleri için benimsenen olağan protokolle uyuşmadığını belirtmiştir. En sonunda görselin Bay Wong’un popülaritesini artırmak için şekil 12-b’de görülen orijinal tören fotoğrafı ile kendi yüzünü birleştirmesiyle elde ettiği anlaşılmıştır (Redi, Taktak ve Dugelay, 2011:134).



Şekil 12. Bay Wong’un Şövalye İlan Edildiğine Dair Deepfake Görüntüsü

Kaynak: (Redi, Taktak ve Dugelay, 2011)

Aynı şekilde Ukrayna-Rusya savaşı sırasında, Ukrayna Devlet Başkanı Volodimir Zelenski’nin Rusya’ya teslim olduğunu söyleyen şekil 13’te de görülen deepfake videosu oluşturulmuştur. Ukrayna Askeri İstihbarat Teşkilatı, Rusya’nın yeni bir taktik olarak sahte video yayabileceği konusunda halkı uyarmıştır (Yapay Zekâ Çalışma Grubu, 2023:12).



Şekil 13. Volodimir Zelenski'nin Deepfake Videosundan Görüntüler

Kaynak: (<https://www.youtube.com/watch?v=enr78tJkTLE>)

Bu örneklerle bakıldığında, deepfake teknolojisinin toplum üzerinde korku yaratma, karalama kampanyası oluşturma veya insanları yanıltma gibi amaçlarla çok kolay bir şekilde kullanılabildiği görülmektedir.

3.2.2. Ekonomik Alanda Olumsuz Etkileri

Deepfake teknolojisi ile finansal piyasalar manipüle edilerek maddi kazanç sağlamak amacıyla da bu teknoloji kullanılabilir. Bir deepfake içeriğe bağlı olarak bir finansal kriz kolayca tetiklenebilir. Yanlış veya yanıltıcı haberler borsada ani düşüş ve ani yükselmelere neden olabilmektedir. Yanıltıcı bir deepfake içeriği, piyasa haberleriyle bağlantılı olarak ve hisse senedi fiyatlarının istikrarsız olduğu bir dönemde piyasaya sürülürse piyasadaki etkileri artırması olasıdır (Dean, 2022: 24). Örneğin 2019 yılında gerçekleşen bir olayda WhatsApp uygulaması üzerinden Metro Bank'ın likiditesinin tükendiğini bildiren bir mesaj gönderilmiş ve insanlar tüm para ve mücevherlerini almak için Metro Bank'a akın etmişler. Yaşanılan bu olay, payların %9'a düşmesine neden olmuştur. Bir başka örnekte, borsada işlem gören bir şirketin CEO'sunun deepfake videosu üretilerek şirkete zarar verecek açıklamalar yaptırılmış ve bu durum hisse fiyatlarının düşmesine neden olmuştur (Stupp, 2019).

3.2.3. Deepfake Teknolojisi'nin Hukuk Alanına Olumsuz Etkileri

Deepfake teknolojinin yaygın kullanımı hukuki sorunları da beraberinde getirmiştir. Deepfake içerikler oluşturulurken genelde bir kişinin yüzü veya sesi izinsiz kullanılmaktadır. Bu da kişilik haklarının, mahremiyetin ihlal edilmesi anlamına gelmektedir.

Deepfake teknolojinin kötüye kullanımı, mahkemeler açısından gerçeklik ve adalet arayışını tehdit edebilir ve adil yargılanma hakkını zedeleyebilir. Ayrıca, bu durum yargılama ilkelerini de olumsuz yönde etkileyebilir. Deepfake teknolojisi ile üretilen sahte deliller, bir kişinin yargılanmasına, hatta kişilerin işlemedikleri bir suç nedeniyle hüküm giymesine sebebiyet verebilir (Yavuz, 2022:212-213). Sahte delillerin mahkemelere sunulması ve itiraz üzerine bu delillerin tekrar tekrar incelenmesi taraflar arasında zaman ve para kaybına da sebebiyet verecektir (Çiçek ve Yalçın, 2024:35).

Örneğin Birleşik Krallık'ta görülen bir velayet davasında anne, ortak çocuklar için babaların şiddete meyilli davranışlarına maruz kaldığını ve bu nedenle çocuklar ile baba arasında bir ilişki kurulamadığını iddia ederek velayetin kendisine verilmesinin talep etmiştir. Bu iddiaları ise babaya ait olduğunu ileri süren ses kayıtlarına dayandırmıştır. Ancak babanın avukatları ses kayıtlarının deepfake teknolojisi ile oluşturulduğunu ispat etmiş ve bu kayıt mahkemece delil olarak değerlendirmeye alınmamıştır (Yavuz, 2022:213).

Teknolojinin yaygın kullanımıyla beraber internet ortamında işlenen suçlar da bir hayli yaygınlaşmıştır. Deepfake teknolojinin ortaya çıkmasıyla kişinin rıza dışı alınmış görüntüleri ile pornografik içerik üretme, dolandırıcılık, iftira, şantaj gibi birçok suç çok daha kolay işlenebilir hale gelmiştir. Meydana gelebilecek tehlikelerden biri de fikri hakların ihlal edilmesidir. Örneğin YouTube'da "Vocal Synthesis" adlı bir kanal, ünlü sesleri farklı beklenmedik diyaloglarla eşleştiren videolar üretmektedir. "Vocal Synthesis" in anonim yaratıcısı, Jay-Z'nin, deepfake ile oluşturulmuş Hamlet'in "To Be or Not To Be" ve Billy Joel'in "We Didn't Start The Fire" nı okuduğu videolar

üretmiştir ve Jay-Z de telif haklarını ihlal ettiği gerekçesiyle kaldırılmasını talep etmiştir (Attenborough, 2020).

Deepfake içerikler bunların dışında siber zorbalık konusunda da tehlike oluşturmaktadır. Örneğin Amerika'da isimsiz bir siber zorba, üçlü amigo kızı yerel takımından uzaklaştırmak için bir deepfake içerik oluşturmuştur. Suç duyurusuna göre bu içerikte; amigo kızların uyuşturucu, sigara, alkol kullandığı, müstahcen görüntüler mevcuttur ve bu görüntüler siber zorba tarafından kızların koçuna gönderilmiştir. Soruşturma sonucunda ilgili IP adresi takip edilerek zorbanın, kızı rakip takımda olan bir anne olduğu anlaşılmıştır (Bellware, 2021). Bu hususta çevrimiçi topluluklar ve sosyal medya platformları birtakım stratejiler geliştirmiştir. Örneğin X (Eskiden Twitter) platformunda izin alınmaksızın cinsel görüntülerin paylaşılması yasaklanmıştır.¹ Bu tarz içerik paylaşanların hesapları kapatılmış ve tekrar kullanıma dönebilmeleri için ilgili içerikleri silmeleri gerektiği bildirilmiştir. Aynı şekilde Google, mağdurlar için istenmeyen görüntülerin çıkarılmalarını talep edebilecekleri bir bildirim sistemi geliştirmiştir. Google gibi Microsoft da Bing arama motorundan ve OneDrive ve Xbox Live bulut hizmetlerinden mağdurların görüntülerinin kaldırılmasını sağlayabilecek bir yöntem geliştirdiğini bildirmiştir (Öztürk, 2021).

3.3. Deepfake Alanındaki Hukuki Düzenlemeler

3.3.1. Mevzuat Düzenlemeleri

Yapay Zekâ hukukunun asıl ortaya çıkışı, yapay zekânın; adalet, etik, sosyal normlar ve değerleri makul bir sınırdan tutabilmek amacıyla gerekli sınırlamaları getirirken aynı zamanda yapay zekânın büyümeye devam etmesine de olanak sağlamaktır (Mohsin, 2021:44).

Deepfake teknolojisinin kullanımının yaygınlaşmasıyla beraber teknolojinin hukuk alanında olumsuz yansımaları olmuştur. Bu olumsuzlukların önüne geçebilmek için bazı ülkelerde doğrudan deepfake teknolojisi ile ilgili yasal düzenlemeler yapılmış veya yapılmakta iken bazı ülkelerde herhangi bir düzenleme yapılmamıştır.

3.3.1.1. Türkiye

Türkiye'de yapay zekâ ile ilgili çeşitli projeler geliştirilmeye devam edilmekte ve işlevsel sistemler inşa edilmektedir. Ayrıca, bu alanda yapılan bilimsel çalışmalar da ülkemizde belirgin bir artış göstermektedir. Hukuk perspektifinden incelendiğinde ise, baroların bu alandaki birçok faaliyeti bulunmaktadır (Aksu, 2023:24-25). Ancak Türk hukukunda deepfake ile ilgili doğrudan yapılmış bir yasal düzenleme mevcut değildir. Yürürlükte olan kanunlar ilgili olduğu ölçüde uygulanabilmektedir. Deepfake kullanımı yaygınlaştıkça, herhangi bir yasal düzenleme de olmadığını göz önünde bulundurduğumuzda bazı hak ihlalleri ve bazı hukuka aykırılıklar meydana gelmektedir. Oluşturulan içeriklerin kullanım şekline göre farklı suçlar oluşabilir. Hangi durumlarda hangi suçların oluşacağı aşağıda ayrıntılı olarak incelenecektir.

3.3.1.2. Amerika Birleşik Devletleri

Türk hukukunda herhangi bir düzenleme mevcut değilken Amerika, deepfake ile ilgili ilk ve en çok düzenleme yapan ülkedir. Amerika'da hem federal düzeyde hem de federe düzeyde deepfake ile ilgili yasal düzenlemeler yapılmıştır. Deepfake teknolojisine ilişkin federal düzeydeki ilk yasa 2019'da Trump tarafından imzalanarak yasalaşmıştır (Özyiğit, 2022:498).

Virginia, ülkedeki rıza dışı alınan görüntülerle oluşturulan deepfake pornografisinin dağıtımına cezai yaptırım uygulayan ilk eyalet olmuştur. 1 Temmuz 2019'da Virginia'da yürürlüğe giren yasa ile rıza dışı sahte oluşturulmuş müstahcen görüntü ve videoların dağıtımı, 1 yıla kadar hapis ve 2.500 dolar para cezası ile cezalandırılan birinci sınıf kabahat haline getirilmiştir. Teksas ise kamu görevi için adaylara zarar vermeyi veya seçimleri etkilemeyi amaçlayan deepfake videoların oluşturulması ve dağıtılmasını yasaklayan ilk eyalet olmuştur. 1 Eylül 2019'da Teksas'ta yürürlüğe giren yasa deepfake videoyu "*kandırmak amacıyla oluşturulan, gerçekleşmeyen bir eylemi gerçekleştiren gerçek bir kişiyi tasvir eden video*" olarak tanımlar. Bu yasada bir kişinin bir adaya zarar vermek veya seçim sonucunu etkilemek amacıyla bir deepfake video oluşturması ve bu videonun bir seçimden önceki 30 gün içinde yayınlanmasına veya dağıtılmasına neden olması, kişinin 1 yıla kadar hapis

¹ Bkz. <https://help.twitter.com/tr/rules-and-policies/twitter-report-violation>

cezası ve 4.000 dolar para cezası ile cezalandırılabilmesini öngören A sınıfı kabahat olarak düzenlenmiştir (Ferraro, Chipman ve Preston, 2020:232).

Yine Kaliforniya'daki yasa bir seçimden sonraki 60 gün içinde gerçek görüntülere benzeyecek şekilde değiştirilmiş politikacıların videolarının, görüntülerinin veya seslerinin oluşturulmasını yasaklamaktadır (Briscoe, 2021).

Bu yasalar sadece sayılanlarla sınırlı olmayıp Amerika'daki birçok eyalette yasa veya yasa tasarısı çıkarılmıştır.

3.3.1.3. Çin

Çin'de de deepfake ile ilgili yasal düzenlemeler mevcuttur. Çevrimiçi Ses ve Görüntü Bilgi Hizmetlerinin Yönetimine İlişkin Hükümler (*Provisions on the Administration of Online Audio and Video Information Services*)'in 11. maddesine göre “çevrimiçi ses, görüntü bilgi sağlayıcılarının ve kullanıcılarının, aslında var olmayan ses, görüntü bilgisi yaratmak, yayınlamak veya iletmek amacıyla derin öğrenme veya sanal gerçeklik gibi yeni teknolojileri veya uygulamaları kullanmaları halinde bunu gözle görülür biçimde etiketlemeleri gerekmektedir”. Ancak aynı maddenin ikinci fıkrasında bu kuralın istisnası olarak sahte haber oluşturmak ve yaymak öngörülmüş olup bu amaçla deepfake oluşturulması yasaklanmıştır.²

Çin'de yine deepfake ile alakalı Derin Sentez İnternet Bilgisi Hizmetlerinin Yönetimine İlişkin Hükümler (*Provisions on the Administration of Deep Synthesis Internet Information Services*) yasası çıkarılmıştır. İlgili yasanın 14. maddesinde “hizmet sağlayıcılar ve teknik ekip; veri yönetimini güçlendirmeli ve veri güvenliğinin korunmasına yönelik önlemler almalı, bunların yanında verilerin kişisel veri içermesi halinde kişisel verilerin korunmasına ilişkin hükümler uygulanacak olup, ses veya yüz gibi biyometrik verilerde düzenleme yapabilmek işlevleri sağlıyorsa, kullanıcıları, bilgisi düzenlenen kişiden bu hususta rıza almaya yönlendirecektir.” denilmiştir.³ Yine aynı yasanın 17. maddesinde “hizmet sağlayıcılar; ses veya görüntü gibi biyometrik verilerde büyük değişiklikler yapıldığı takdirde görünür biçimde etiketleme yaparak halkı bu içeriklerin gerçek olmadığına dair uyarmalı, diğer teknolojilerin kullanımlarında da kullanıcıları etiket yapmaya yönlendirmeli ve onları bu konu uyarmalıdır.” demektedir. İlgili maddeden anlaşılmaktadır ki deepfake içerikler hizmet sağlayıcıların denetiminden geçerek kamuya sunulduğunda, gerekli etiketleme faaliyetleri doğrudan hizmet sağlayıcı tarafından yapılacak (Erdoğan, 2023:42) ve böylece insanlar görüntü veya videonun gerçek mi deepfake mi olduğunu anlayabilecektir.

3.3.1.4. Tayvan

Tayvan'da, 2023'e kadar deepfake teknolojisinin kullanımına dair yasal bir düzenleme yapılmamıştır. Ancak 2023'te mecliste kabul edilen Ceza Kanunları'nda yasal değişiklik öngören tasarıya göre; bir kişinin rızası olmadan cinsel içerikli görüntülerinin hazırlanması veya yetkisiz biçimde bu içeriklerin dağıtılması suç olarak düzenlenmekte olup söz konusu içeriği kâr amacıyla dağıtmak cezanın ağırlaştırılmasına yol açarken mezkûr içerikleri tehdit ya da şantaj amacıyla üretmenin ya da dağıtmanın çok daha ağır yaptırımlara tabi olduğu görülmektedir. Tasarıda içeriği üretme ve yayma kavramlarının yanı sıra içerikleri; çoğaltmak, dağıtmak, yayınlamak, iletmek, sergilemek fiilleri de suç teşkil eden fiiller olarak kabul edilmiştir. Kabul edilen tasarıya göre kişinin rızası olmadan cinsel içerikli görüntü ve video üretilmesi durumunda 3 yıla kadar, bu içeriklerin yetkisiz olarak dağıtılması durumunda ise 6 aydan 5 yıla kadar hapis cezasına çarptırılabilir. İçeriklerin kar elde etme amacıyla dağıtılması durumunda ise ceza ağırlaştırılmış ve öngörülen cezanın yarısına kadar ek bir ceza öngörülmüştür. Tayvan'da diğer bir yasa değişikliği ile dolandırıcılık faaliyetlerinde kullanılmak üzere hazırlanan deepfake içeriklerinin kullanımının da cezalandırılması öngörülmüştür.⁴

3.3.1.5. Hindistan

Hindistan'da henüz deepfake teknolojisini düzenleyen mevzuat düzenlemesi yoktur. Veri koruma ve telif hakkı yasalarına ek olarak sosyal medya platformlarının deepfake teknolojisine karşı daha sert bir duruş sergilemeye ve yapmazlarsa sorumluluklarına gidebilmek için yasanın

² Bkz. CAC, “Regulations on the Administration”, m. 11.

³ Bkz. CAC, “Provisions on the Administration of Deep Synthesis”, m. 14.

⁴ Bkz. <https://www.taipeitimes.com/News/front/archives/2023/01/08/2003792190>

sıkılaştırılması konusunda tartışmalar vardır (Nema, 2020). Hindistan'ın özelliği, mevcut yasaların ölen insanların deepfake içeriklerini oluşturma olasılığını kapsamadığı düşüncesine odaklanmasıdır. New York yasası, ölen kişinin kişilik haklarının korunmasını tanıtım hakkına yerleştirirken Hindistan'da bu durum veri koruma yasası kapsamında tartışılmaktadır. Bu bağlamda, Macaristan ve İspanya'nın gizlilik ve veri koruma yasalarındaki gibi ölen kişinin haklarının korunması için tamamlayıcı veri yasalarına atıfta bulunmaktadır (Jain, 2020).

3.3.1.6. İngiltere

Deepfake teknolojinin İngiltere'de 2019'da yaygınlaşmasının akabinde 2020 yılında mahremiyet istismarı vakalarında bir artış olmuştur. İngiltere'de yasal bağımsız bir organ olan Hukuk Komisyonu'nun 253 numaralı değerlendirme çalışmasına göre Covid-19 pandemisi nedeniyle insanların evine kapandığı dönemde mahremiyet istismarı konusunda ciddi artışlar yaşanmıştır.⁵ Değerlendirme çalışmasının giriş bölümünde İngiltere'de deepfake görüntülerin, aşağılayıcı görüntülerin ve cinsel içerikli özel görüntülerin paylaşılmasının tehdit edilmesi mevcut yasada suç olmayan zararlı davranış olduğu belirtilmiştir.⁶ Ayrıca bu çalışmada deepfake pornografisinin "mahrem görüntü istismarı" kavramına dahil olduğu belirtilmiştir.⁷ Sonuç olarak değerlendirme çalışmasında deepfake kullanılarak elde edilen rıza dışı pornografik içeriklerin suç olarak düzenlenmesi gerektiği önerilmiştir.⁸

İngiltere Hükümeti tarafından 2024'te yapılan bir basın açıklamasında, cinsel içerikli deepfake oluşturulmasını suç sayan yasa önerisi açıklanmıştır. Yeni suçun Ceza Adaleti Tasarısı (*Criminal Justice Bill*)'na bir değişiklik olarak ekleneceğini bildirilmiştir. Söz konusu tasarı henüz yasalaşmamış olup düzenlemeler Lordlar Kamarası'nda incelenmektedir (Farris, 2024).

3.3.1.7. Almanya

Almanya Federal Konseyi, deepfake ile mücadeleyle yönelik yasal düzenlemelerin yetersiz olduğunu belirterek kişisel hakları deepfake içeriklerden korumak için bir yasa tasarısı başlatmıştır. Konsey, Alman Ceza Kanunu'na "Dijital sahtecilik yoluyla kişisel hakların ihlali" başlıklı bir bölüm eklemeyi önermiştir. Bu bölümde, bilgisayar teknolojisi kullanılarak bir kişinin imajını, davranışını veya ifadelerini aldatıcı şekilde değiştirmek amacıyla içerik oluşturmak veya dağıtmak karşılığında 2 yıla kadar hapis veya para cezası öngörülmektedir. Ayrıca bu içerikleri herkese açık olarak paylaşmak veya özel konular söz konusuysa 5 yıla kadar hapis veya para cezası öngörülmüştür (Federal Konsey Yasa Tasarısı, 2024).

3.3.1.8. Avrupa Birliği

Avrupa Birliği'nde deepfake ilk olarak 2021 tarihinde Avrupa Parlamentosu Araştırma Servisi tarafından hazırlanan Deepfake ile Mücadele Raporu'nda ele alınmıştır. Bu raporda deepfake içeriklerin neden olduğu olumsuzluklar, yasal düzenleme alanındaki boşluklar ve yapılabilecek öneriler yer almaktadır (Avrupa Parlamentosu Araştırma Servisi, 2021). Avrupa Birliği'nin yapay zekaya ilişkin en kapsamlı yasal düzenlemesi olan Yapay Zekâ Tüzüğü ilk olarak 2021'de önerilmiş, 1 Ağustos 2024 tarihinde de yürürlüğe girmiştir.⁹

Yapay Zekâ Yasası'nda deepfake; "mevcut kişilere, nesnelere, yerlere, varlıklara veya olaylara benzeyen ve bir kişiye yanlış bir şekilde gerçek veya doğru görünen yapay zekâ tarafından oluşturulan veya manipüle edilmiş görüntü, ses veya video içeriği anlamına gelir." şeklinde tanımlanmıştır.¹⁰

Yapay Zekâ Yasası'nda teknoloji kullanımı yasaklanmamış ancak sistem kullanıcısı bakımından etiketleme ve nasıl oluşturulduğunu veya manipüle edildiğini şeffaflık yükümlülüğü kapsamında açıklamasını öngörmüştür. Yasada şeffaflık yükümlülüğünün kapsamı Avrupa Birliği Temel Haklar Şartı'nda güvence altına alınan ifade özgürlüğü ile bilim ve sanat özgürlüğünün kullanılması durumunda sınırlandırılmıştır. Yine aynı şekilde cezai suçları tespit etmek, önlemek, araştırmak

⁵ Bkz. Law Commission, "Intimate Image Abuse", p. 1.21.

⁶ Bkz. Law Commission, "Intimate Image Abuse", p. 1.40.

⁷ Bkz. Law Commission, "Intimate Image Abuse", p. 2.145.

⁸ Bkz. Law Commission, "Intimate Image Abuse", p. 7.156.

⁹ Bkz. https://www.ab.gov.tr/ab-yapay-zeka-yasasi-yayimlandi_53836.html

¹⁰ Bkz. "Artificial Intelligence Act" (Yapay Zeka Yasası) m. 3, p. 60.

veya kovuşturmak için kullanımın yasalarca yetkilendirildiği durumlarda da şeffaflık yükümlülüğünün kapsamı sınırlandırılmıştır.¹¹

Avrupa Birliği'nde Kasım 2022'de Dijital Hizmetler Yasası yürürlüğe girmiş olup bu yasa çevrimiçi platformlarda yasadışı içeriklerin yayılmasını sınırlandırmayı hedeflemiştir. Dijital Hizmetler Yasası'nda içerik sağlayıcılara içeriklere hangi denetleme kurallarını uyguladıklarını ve bunları uygulamak için hangi önlemleri aldıklarını şeffaf biçimde ortaya koymaları gerektiği ifade edilmiştir (Avrupa Parlamentosu Araştırma Servisi, 2021). Dijital Hizmetler Yasası kapsamında deepfake teknolojisinin kullanımının yasaya aykırı olması durumunda aracı hizmet sağlayıcısının bir önceki mali yılda elde ettiği cironun %6'sına kadar para cezasına hükmedileceği belirtilmiştir.¹²

4. Ceza Hukuku Genel Teorisi Açısından Deepfake Teknolojisi

4.1. Genel Olarak

Ceza hukuku, cezai müeyyidelerle yasaklanan suçlardan oluşan hukuk normlarının tamamını içeren bir hukuk dalıdır (Toroslu ve Toroslu, 2021:17). Ceza hukukunun temel yapı taşlarından birini oluşturan suç kavramı ise haksız, kusurlu ve cezalandırılabilir davranışı ifade etmektedir. Suç genel teorisi, bir fiilin suç teşkil edip etmediğini belirleyebilmek amacıyla, o fiilde yer alması gereken unsurları tanımlar ve inceler (Centel, Zafer ve Çakmut, 2020:213).

Suçun meydana gelebilmesi için, bir eylemin varlığı gereklidir ve bu eylem hukuka aykırı, kusurlu ve yasa da tanımlanmış olmalıdır. Buna göre de suçun unsurları öğretide çeşitli ayrımlara tabi tutulmakla beraber yasallık, maddi unsur, hukuka aykırılık ve manevi unsur olmak üzere dört başlık altında incelenebilir (Centel, Zafer ve Çakmut, 2020:217).

Yapay zekaya sahip bir makinenin de bir eyleme veya sonuca yol açmış olması mümkündür. Örneğin yapay zekâ kullanan bir makinen birini yaralaması, bir mala zarar vermesi gibi durumlarda sorumluluğun kime ait olduğu hususu gündeme gelecektir. Ceza hukukunda yer alan "hareket", "sorumluluk", "kusur" ve "isnat yeteneği" gibi kavramların yapay zekalı makineler uygulanabilirliği önemli bir tartışma konusu olmakla beraber bu kavramların yapay zekâ için de kullanılabileceğini savunanlar azımsanamayacak ölçüdedir. "Hareket", "kast", "kusur" ve "irade" gibi unsurların makineler üzerinde uygulanması sorunlu gibi görünse de makine ve insan arasındaki farklar göz önünde bulundurulduğunda bu kavramların makineler için uyarlanabileceği, içeriklerinin değiştirilebileceği veya yeni anlamlar yüklenebileceği yönünde görüşler bulunmaktadır (Kangal, 2021:44).

Ceza hukuku kapsamında sorumluluktan söz edebilmek için fail bakımından hareket ve kusur yeteneğinin olması gerekmektedir. Yapay zekanın cezai sorumluluğundan söz edebilmek için de yapay zekâ bakımından hareket ve kusur yeteneği sorununun çözülmesi gerekmektedir (Bacaksız ve Sümer, 2021:155). Bu konu çalışmamız kapsamını aştığı için daha fazla ayrıntıya yer verilmeyecektir.

4.1.1. Yasallık Unsuru

Yasallık, tipiklik veya kanunilik olarak adlandırılan unsur, fiilin ceza kanununda yazılı tanıma uygun olması olarak tanımlanmaktadır. Bir eylem, yasadaki tanıma uymuyorsa tüm suç unsurlarını taşısa dahi suç olarak kabul edilmez (Alacakaptan, 1975:29). Yasallık, fiilin ceza kanununda yer alan bir suç tanımına uygun olup olmadığının belirlenmesiyle ilgilidir ve bu belirleme yargılama sürecinde hâkim tarafından gerçekleştirilir (Zafer, 2021:232). Yapılan eylem, yalnızca yasadaki bir suç tanımına uygun olduğu takdirde cezalandırılabilir (Centel, Zafer ve Çakmut, 2020:218).

4.1.2. Maddi Unsur

Bir suçtan söz edilebilmesi için beşerî bir fiilin olması gerekmektedir (Hafızoğulları ve Özen, 2021:167) Modern ceza hukuku bakımından suç, fiilin varlığını gerektirmektedir. Ceza hukuku anlamında bir fiilin oluşabilmesi için çeşitli unsurların bulunması gerekmektedir. Bunlar; hareket, netice ve nedensellik bağıdır (Toroslu & Toroslu, 2021:133).

¹¹ Bkz. "Artificial Intelligence Act" (Yapay Zeka Yasası) p. 134.

¹² Bkz. "Digital Services Act" (Dijital Hizmetler Yasası) m. 52.

Hareket, insanın dış dünyada meydana getirdiği olumlu ya da olumsuz olabilen iradi bir davranıştır (Centel, Zafer ve Çakmut, 2020:218). Ceza hukuku bakımından önemli olan hareket kavramı, kanunun suç olarak kabul ettiği bir sonuca yol açan harekettir (Demirbaş, 2024:247). İnsanın dış dünyada ortaya çıkan iradi davranışı hareket olarak tanımlanır. Ceza hukukunda hareketin icrai olarak yapmak ve ihmali olarak yapmamak şeklinde iki görünüşü bulunmaktadır (Toroslu ve Toroslu: 2021:135).

Netice, ceza hukuku anlamındaki hareketin dış dünyada oluşturduğu değişikliktir. Ancak ceza hukuku bakımından önemli olan, hareketin oluşturduğu her değişiklik değil suçun kanunu tanımında yer alan değişikliktir (Özgenç, 2024:193). Bir suçun tanımında neticeye unsur olarak yer verilmişse suçun tamamlanabilmesi bakımından neticenin meydana gelmesi gerekir. Ancak suçun kanuni tanımında unsur olarak neticeye yer verilmemişse suçun tamamlanabilmesi için hareketin gerçekleştirilmesi yeterlidir (Koca ve Üzülmüş, 2024:128).

Nedensellik bağı, neticenin bir kişiye yüklenebilmesi için, o kişinin hareketi ile netice arasında bulunması gereken bağa denir. Nedensellik bağı uyarınca bir kişinin hareketiyle meydana gelen dış değişiklik arasında bir ilişki olmadığı durumlarda, kişi bu neticeden sorumlu tutulamaz (Toroslu ve Toroslu, 2021:149).

4.1.3. Hukuka Aykırılık

Suçun oluşması için fiilin hukuka aykırı olması gerekir. Eğer fiili hukuka uygun duruma getiren neden mevcutsa suç oluşmaz. Hukuka aykırılıktan bahsedebilmek için iki şartın meydana gelmesi gerekmektedir. Birincisi; fiilin ceza hukuku normlarına aykırılık teşkil etmesi gerekmektedir. İkincisi bu fiilin meydana getirilmesine imkân tanıyan herhangi bir kuralın bulunmaması gerekmektedir (Centel, Zafer ve Çakmut, 2020:296,297). Hukuk düzeni, belirli şartların oluşması halinde yasaklanan bir davranışa izin vermektedir. Bu durum hukuka uygunluk nedenleri olarak adlandırılan nedenlerin ortaya çıkmasına yol açmıştır. Kanunda suç olarak tanımlanan bir fiilin işlenmesi durumunda, hukuka uygunluk nedenleri varsa, toplum bakımından cezalandırılması gereken bir zarar bulunmayacağından fiil suç sayılmayacaktır (Hafızoğulları ve Özen, 2021:210-211).

Hukuka uygunluk nedenleri arasında; emrin yerine getirilmesi, meşru savunma, zorunluluk hali, hakkın kullanılması ve ilgilinin rızası, hekimlik mesleğinin icrası, sportif faaliyetler ve basın hürriyeti yer almaktadır (Hafızoğulları ve Özen, 2021:213-238).

4.1.4. Manevi Unsur

Kusurluluk olarak da ifade edilen manevi unsur, fiil ile fail arasındaki psikolojik bağı ifade etmektedir (Centel, Zafer & Çakmut, 2020:359). Hukuk sistemimize göre, bir suçun manevi unsuru, icra veya ihmali hareketinin bilinçli ve iradi bir şekilde gerçekleştirilmesini gerektirir. Bu da suçun kast ve taksir olmak üzere iki farklı biçimde meydana gelmesini sağlar (Hafızoğulları ve Özen, 2021:240).

Kast, kusurluluğun temel biçimidir ve suç meydana gelebilmesi için kastın bulunması gerekir (Centel, Zafer & Çakmut, 2020:367). Kanundaki kast tanımına bakıldığında kastın bilme ve isteme olmak üzere iki unsuru bulunduğu görülmektedir (25611 Sayılı, 12.10.2004 Tarihli Resmî Gazete'de Yayımlanan 5237 Sayılı Türk Ceza Kanunu m.21/1). Kastın bilme unsuru, suç teşkil eden fiilin fail tarafından bilinmesini ifade eder. Failin gerçekleştirdiği fiilin neticesini istemesi de kastın isteme unsurudur. Kastın gerçekleşebilmesi için bilme ve isteme unsurlarının birlikte bulunması gerekmektedir (Centel, Zafer ve Çakmut, 2020:368-371).

Taksir ise istenen bir davranış ile istenmeyen bir sonucun ortaya çıkmasından doğan sorumluluktur (Hafızoğulları & Özen, 2021:262). Türk Ceza Kanunu'na göre de taksir "dikkat ve özen yükümlülüğüne aykırılık dolayısıyla, bir davranışın suçun kanuni tanımında belirtilen neticesi öngörülmeyerek gerçekleştirilmesidir" şeklinde tanımlanmıştır (TCK m.22/2). Taksir istisnai bir nitelik taşır (Toroslu & Toroslu, 2021:233) ve taksirli bir fiilin cezalandırılabilmesi için kanunilik ilkesi gereği o fiilin kanunda ayrıca düzenlenmiş olması gerekmektedir (TCK m.22/1).

Burada Ceza Hukuku Genel Teorisi açısından suçun unsurları incelenmiş olup deepfake teknolojisi ile işlenebilecek suçlar bakımından suçun unsurları aşağıda ayrıntılı olarak incelenecektir.

4.2. Deepfake Teknolojisi Kullanılarak İşlenen veya İşlenebilecek Suçlar

Teknolojinin gelişmesi ve internetin artan kullanımıyla birlikte siber ortamda işlenen suçlar da yaygınlaşmıştır. Teknolojinin sağladığı imkanlar kullanılarak birçok suçun işlenmesi kolaylaşmıştır. Deepfake teknolojisi de bazı suçların işlenmesinde araç olarak kullanılmaktadır. Bu durumda ceza hukuku kapsamında bazı suçlar gündeme gelecektir (Kandır, 2023:152).

4.2.1. Dolandırıcılık (TCK m. 157)

Dolandırıcılık suçu, 5237 sayılı Türk Ceza Kanunu'nun 157. maddesinde düzenlenmiştir. TCK 157'ye göre; *"Hileli davranışlarla bir kimseyi aldatıp, onun veya başkasının zararına olarak, kendisine veya başkasına bir yarar sağlayan kişiye bir yıldan beş yıla kadar hapis ve beşbin güne kadar adli para cezası verilir."* (TCK m.157).

Dolandırıcılık suçunun faili herkes olabilir. Suçun mağduru da yine herkes olabilir. Suçun mağduru yani suçtan zarar gören kimse, söz konusu suç ile malvarlığı değeri azalan kimsedir. Dolandırıcılık suçunun hukuki konusu bireylerin malvarlıklarının korunmasına yönelik kamu yararadır. Dolandırıcılıkta fiil; failin bir kişiyi hileli davranışla aldatması, o kişinin veya başkasının zararına olacak şekilde kendisine veya başka bir kişi lehine yarar sağlamasıdır. Dolandırıcılık suçu kasten işlenebilen bir suçtur. Dolandırıcılık kastının, suç işlenmeden önce ya da en azından suç işleme esnasında var olması gerekir. Fiilin hukuka aykırı olması gerekmektedir. Bir kişinin hileli yollarla zarara uğratılması her durumda hukuka aykırıdır. Dolandırıcılık suçunun taksirli şekli kanunda düzenlenmediğinden bu suç taksirle işlenemez (Hafızogulları ve Özen, 2021:412-413,420).

Suçun hukuki konusu; malvarlığına ilişkin bir değer, taşınır, taşınmazlar ve hatta alacak hakkı da olabilmektedir. Deepfake içeriklerle işlenen dolandırıcılık suçlarına bakıldığında, suçluların takibini zorlaştırmak amacıyla bitcoin veya dijital para gibi alternatiflere başvurdukları gözlemlenmektedir (Öztürk, 2021:74).

TCK 158'de ise dolandırıcılık suçunun nitelikli hali düzenlenmiştir ve daha ağır ceza öngörülmüştür. Deepfake bakımından dikkate alınması gereken hüküm 158/1-(f) maddesidir. 158/1-(f)'de dolandırıcılığın, *"bilgi sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle"* işlenmesi halinde üç yıldan on yıla kadar hapis ve beşbin güne kadar adli para cezasına hükmolunacağı söylenmiştir (TCK m.158/1-f).

Dolandırıcılık suçunu deepfake içerikler bakımından ele alacak olursak, deepfake içerikler görüntü veya ses kaydı içermektedir. Fail, hileli davranışlarla bir bilgi sisteminden yararlanarak bu içeriklerle bir kimseyi aldatıp, o kimseyi yahut başkasını zarara uğratar ve kendisine ya da başkasına yarar sağlarsa ceza arttırılacaktır. Kanunun gerekçesinde ise cezanın arttırılma nedeni, bilgi sistemlerinin suçun işlenmesini kolaylaştırmasıdır (Hafızogulları ve Özen, 2021:426-427).

İnsanların sosyal medyada ve dijital platformlarda paylaştıkları veriler, deepfake teknolojisinin beslediği verilerdir. Deepfake teknolojisi de kötü niyetli kullanıcılarının dolandırıcılık amacıyla yöneldiği bir araç haline gelmiştir (Aydın, 2024:76). Örneğin Çin'de meydana gelen bir deepfake dolandırıcılığı olayında, bir deepfake kullanıcısı, mağdur Guo'nun bir arkadaşının ses ve görüntüsünü deepfake aracılığıyla yeniden oluşturarak mağdurla görüşme gerçekleştirmiştir. Görüşmede mağduru bir ihale için 4,3 milyon yuan değerinde depozito yatırması gerektiğini söylemiş ve arkadaşına inanan mağdur, parayı göndermiştir. Mağdur, arkadaşıyla buluştuğunda arkadaşının bu olaydan haberi olmadığını görmüş ve dolandırıldığını anlayıp yetkililerle irtibata geçmiştir (Hou, Tung ve Madjar, 2023).

Yine yaşanan bir olayda İngiltere merkezli bir enerji firmasının CEO'su, firmanın Alman ana şirketinin genel müdürüyle telefon görüşmesi yaptığına inanarak Macar tedarikçinin banka hesabına 220.000 € para göndermiştir. Dolandırıcı deepfake teknolojisi kullanarak genel müdürün sesini taklit etmiş ve bu şekilde telefon görüşmesi sağlamıştır. CEO; görüştüğü sesin, patronunun sesindeki Alman aksanını ve hatta patronunun tınısını taşıdığını açıklamıştır (Damiani, 2019).

Hong Kong'da meydana gelen bir olayda ise çok uluslu firmadaki bir finans çalışanı, bir video konferans görüşmesinde şirketin mali işler müdürü gibi davranmak için deepfake teknolojisini kullanan dolandırıcılara 25 milyon dolar ödemek üzere kandırılmıştır. Hong Kong polisi, firma çalışanın diğer birkaç personel üyesi olduğunu düşündüğünü ancak aslında hepsinin deepfake canlandırmaları olduğu bir video görüşmesine katılması için kandırıldığını söylemiştir. Kıdemli

başkomiser yaptığı açıklamada işçinin görüşmeye katılan diğer kişilerin meslektaşlarına benzediğini ve seslerinin de aynı olduğunu söylediğini bildirmiştir (Magramo ve Chen, 2024).

Bu örneklerle bakıldığında deepfake teknolojinin insanları dolandırmak amacıyla kullanıldığını görülmektedir.

4.2.2. Şantaj (TCK m. 107)

Şantaj suçu, 5237 sayılı Türk Ceza Kanunu'nun 107. maddesinde *"Hakkı olan veya yükümlü olduğu bir şeyi yapacağından veya yapmayacağından bahisle, bir kimseyi kanuna aykırı veya yükümlü olmadığı bir şeyi yapmaya veya yapmamaya ya da haksız çıkar sağlamaya zorlayan kişi, bir yıldan üç yıla kadar hapis ve beşbin güne kadar adli para cezası ile cezalandırılır."* şeklinde düzenlenmiştir (TCK m.107).

107. maddenin ikinci fıkrasında da *"Kendisine veya başkasına yarar sağlamak maksadıyla bir kişinin şeref veya saygınlığına zarar verecek nitelikteki hususların açıklanacağı veya isnat edileceği tehdidinde bulunulması halinde de birinci fıkraya göre cezaya hükmolunur."* denilmiştir (TCK m.107/2).

Şantaj suçu, tehdit suçunun özel bir görünümüdür. Şantaj suçunun faili ve mağduru herkes olabilir. Şantaj suçunun hukuki konusu kişilerin korkmadan, her koşulda ve her yerde özgürce hareket etme hakkını korumaya ilişkin yararadır. Şantaj suçunu oluşturan hareket, kanun gerekçesinde failin *"hakkı olan veya yükümlü olduğu bir şeyi yapacağından veya yapmayacağından bahisle başkasını zorlaması"* şeklinde ifade edilmiştir. Şantaj suçunda fiil hukuka aykırı olmalıdır (Hafızoğulları ve Özen, 2021:178, 185). TCK 107/1'de belirtilen, hakkı olan bir şeyi yapacağını söylemek, hukuka uygunluk çerçevesinde kalacağından fiil cezalandırılmayacaktır. Burada cezalandırılacak olan, karşı taradın belirli bir davranış sergilemeye veya sergilememeye ya da haksız bir kazanç elde etmeye zorlanması fiilidir (Tezcan, Erdem ve Önok, 2022:545). Şantaj suçu kasten işlenebilen bir suçtur, taksirle işlenemez (Hafızoğulları ve Özen, 2021:187).

Suçun işlenme biçimi, gerçek hususların açıklanacağı tehdidinin yanı sıra gerçek olmayan, sahte, uydurulmuş hususlarla da tehdit edilebileceği şeklinde olabilir (Tezcan, Erdem ve Önok, 2020:536). Örneğin bir kişiden, deepfake ile hazırlanmış sahte görüntülerini yok etmek için haksız bir yarar elde edilirse şantaj suçu oluşacaktır. Yine ikinci fıkrada belirtilen kişinin şeref veya saygınlığına zarar verecek nitelikteki hususlarının açıklanması suretiyle de suç işlenebilir. Bir deepfake içeriğinin gerçek olduğuna inanan bir kişiye, bu içeriklerin kullanılacağı ve bu suretle kişinin şeref veya saygınlığına zarar verecek nitelikte hususların isnat edileceği tehdidinde bulunarak haksız yarar elde edilirse şantaj suçu oluşmuş olacaktır (Yavuz, 2021:128).

4.2.3. İftira (TCK m. 267)

İftira suçu, 5237 sayılı Türk Ceza Kanunu'nun 267. maddesinde düzenlenmiştir. Bu maddede, *"Yetkili makamlara ihbar veya şikâyetle bulunarak ya da basın ve yayın yoluyla, işlemediğini bildiği halde, hakkında soruşturma ve kovuşturma başlatılmasını ya da idari bir yaptırım uygulanmasını sağlamak için bir kimseye hukuka aykırı bir fiil isnat eden kişi, bir yıldan dört yıla kadar hapis cezası ile cezalandırılır."* şeklinde düzenlenmiştir (TCK m.267).

TCK m. 267/2'de *"Fiilin maddî eser ve delillerini uydurarak iftirada bulunulması halinde, ceza yarı oranında artırılır."* şeklinde ifade edilmiştir (TCK m.267/2).

İftira suçunda mağdura suçsuz olduğu halde hukuka aykırı bir fiil isnat edilmektedir. Failin hedefi, mağdurun soruşturma veya kovuşturma geçirmesi ya da idari bir yaptırımla karşılaşmasını sağlamaktır (Yurtcan, 2019:10).

İftira suçunda fail herkes olabilmektedir. Mağdur konusunda öğretide farklı yaklaşımlar mevcuttur. Bir grup hem gerçek hem de tüzel kişilerin mağdur olabileceğini kabul ederken diğer grup mağdurların yalnızca gerçek kişi olabileceğini, tüzel kişilerin ise suçtan zarar gören konumunda olabileceğini düşünmektedir. İftira suçunun hukuki konusu, *"objektif olarak gerçek dışı olan hukuka aykırı bir fiilin isnadı"* dır. Isnat edilen fiil belirli ve açık olmalıdır (Özbek, Doğan ve Bacaksız, 2024:1176). Isnat edilen fiilin hukuka aykırı olması gerekir. Isnat edilen fiilin suç haline gelebilmesi için, failin gerçeğe aykırı bir suç duyurusunda bulunması gerekmektedir. Bu suç duyurusunun ise hukuka aykırı olup hukukla çelişmesi gerekmektedir. İftira suçu kasten işlenebilen bir suçtur. Ancak burada genel kast yeterli olmayıp özel kast aranmaktadır. Fail, suç işlemediğini bildiği bir kimse hakkında soruşturma veya kovuşturma başlatılmasını ya da idari bir yaptırım uygulanmasını sağlamak amacıyla, o kişiye hukuka aykırı bir fiil isnat etmelidir. Basının *"haber*

verme, yorum ve eleştiri yapmak hakkı" bağlamında hukuka uygunluk sınırları içinde kalan isnatları hukuka uygunluk nedeni olarak kabul edilmektedir (Ünver, 2023:106-107).

Burada deepfake ile sahte deliller oluşturulması söz konusu olabilir. Örneğin kamera kayıtlarında suçu işleyen kişinin yüzünün bir başkasıyla değiştirilerek manipüle edilmesi mümkündür. Suç işlemeyen kişi, manipüle edilmiş görüntü veya video nedeniyle soruşturma, kovuşturma geçirir veya hakkında idari yaptırım uygulanırsa iftira suçu oluşmuş olacaktır (Babayiğit, 2021:667).

4.2.4. Suç Uydurma (TCK m. 271)

Türk Ceza Kanunu'nun 271. maddesine göre "İşlenmediğini bildiği bir suçu, yetkili makamlara işlenmiş gibi ihbar eden ya da işlenmeyen bir suçun delil veya emarelerini soruşturma yapılmasını sağlayacak biçimde uyduran kimseye üç yıla kadar hapis cezası verilir" denilmiştir (TCK m.271).

Suç uydurma suçunun kanunda iki farklı işlenme şekline yer verilmiştir. Birincisi, failin işlenmediğini bildiği bir suçu işlenmiş gibi yetkili makamlara ihbar etmesidir. İkincisi ise işlenmemiş bir suçun delil ve izlerini soruşturma yapılacak şekilde uydurmaktır (Tezcan, Erdem ve Önok, 2020:1394-1395). Herkes bu suçun faili olabilir. Suç uydurma suçunun hukuki konusu, ceza hukuku bağlamında "suç"tur. Disiplin eylemi ya da kabahat uydurulması halinde suç uydurma suçu oluşmayacaktır (Özbek, Doğan ve Bacaksız, 2024:1190). Failin işlenmediğini bildiği bir suçu işlenmiş gibi yetkili makamlara ihbar etmesi veya işlenmeyen bir suçun delil ve emarelerini soruşturma yapılacak şekilde uydurması hukuka aykırı bir davranış şeklidir. Bu nedenle hukuka uygunluk nedenlerinden hiçbiri bu suç ile bağdaşmamaktadır. Suç uydurma suçu doğrudan kast ile işlenebilen bir suçtur (Hafizoğulları ve Özen, 2016:155).

Deepfake teknolojisi ile işlenmeyen bir suçu işlenmiş gibi göstermek mümkündür. Örneğin bir kamera kaydında A'nın bir hastayı tedavi etme görüntüleri varken bu videonun manipülasyonla kasten öldürme fiili işleniyormuş gibi gösterilmesi söz konusu olabilir (Babayiğit, 2021:667). A bakımından bu görüntüye dayanılarak bir soruşturma yapılırsa bu durumda video manipülasyonu yapan kişi bakımından suç uydurma suçu gündeme gelecektir.

4.2.5. Özel Hayatın Gizliliğini İhlal (TCK m. 134)

Özel hayatın gizliliğini ihlal suçu TCK'nın 134. maddesinde düzenlenmektedir. Bu maddeye göre "Kişilerin özel hayatının gizliliğini ihlal eden kimse, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır. Gizliliğin görüntü veya seslerin kayda alınması suretiyle ihlal edilmesi halinde, verilecek ceza bir kat artırılır." denilmiştir (TCK m.134).

TCK 134/2'de de "Kişilerin özel hayatına ilişkin görüntü veya sesleri hukuka aykırı olarak ifşa eden kimse iki yıldan beş yıla kadar hapis cezası ile cezalandırılır. Ifşa edilen bu verilerin basın ve yayın yoluyla yayımlanması halinde de aynı cezaya hükmolunur." şeklinde düzenleme yapılmıştır (TCK m.134/2).

Kanun özel hayatın gizliliğini ihlal etme fiilini cezalandırmaktadır. Özel hayat, kişinin kamuya kapalı olan hayatıdır. Özel hayatın gizliliğini ihlal suçunun faili ve mağduru herkes olabilir. Bu suçun hukuki konusu özel yaşamın yani mahremiyetin korunmasına yönelik kamu yararadır (Hafizoğulları ve Özen, 2021:285). Özel yaşamın gizliliğine yönelik müdahalenin herhangi bir hukuki dayanağa sahip olmaması gerekmektedir. Bu nedenle özel yaşama, ilgili kişilerin açık veya zımni rızasıyla müdahalede bulunan kimse bu suçu işlemiş sayılmaz. Bu suç genel kastla işlenebilen bir suçtur (Tezcan, Erdem ve Önok, 2022:726-727).

Özel hayatın gizliliğini ihlal suçunun da deepfake aracılığıyla işlenmesi mümkün olabilir. Özellikle de cinsel içerikli görüntülerin deepfake olarak üretilmesi ve bunların hukuka aykırı ifşa edilmesi söz konusu olabilir. Örneğin normal bir içerikten elde edilen fotoğraf ve videolar kullanılarak yüzleri görünmeyen müstehcen nitelikteki içeriklerde bu kişiler yer almış gibi manipüle edilip ifşa edilirse müstehcen görüntüde yer alan kişiler bakımından özel hayatın gizliliğini ihlal suçu oluşacaktır (Babayiğit, 2021:670-671). Ancak burada korunan veriler, kişilerin özel hayatını ilgilendiren ve yalnızca belirli kişiler tarafından erişilebilen ve kişi tarafından paylaşılmadığı sürece erişilmesi mümkün olmayan verilerdir. Bu bağlamda halkın erişimine açık bir medya paylaşımı üzerinden alınarak manipüle edilen ses ve görüntüler bakımından özel hayatın gizliliğini ihlal suçu oluşmayacaktır (Öztürk, 2021:72).

4.2.6. Kişisel Verilerin Kaydedilmesi ve Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme (TCK m. 135, 136)

Kişisel Verilerin Kaydedilmesi suçu Türk Ceza Kanunu'nun 135.maddesinde düzenlenmiştir. TCK 135'e göre "Hukuka aykırı olarak kişisel verileri kaydeden kimseye bir yıldan üç yıla kadar hapis cezası verilir." denilmiştir (TCK m.135).

6698 sayılı Kişisel Verilerin Korunması Kanunu uyarınca "kişisel veri, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi"dir (29677 Sayılı, 07.04.2016 Tarihli Resmî Gazete'de Yayımlanan 6698 Sayılı Kişisel Verilerin Korunması Kanunu m.3/1-d).

Kişisel verilerin kaydedilmesi suçunun faili ve mağduru herkes olabilir. Kanun maddesine bakıldığında kişisel verileri kaydetme fiilinin suç olarak düzenlendiği görülmektedir. Bu suçun hukuki konusu, bireylerin özel hayatlarına dair kişisel verilerinin gizliliğinin ihlal edilmesiyle ilgili yarardır. Kişisel verileri kaydetme fiili hukuka aykırı olmalıdır. Kişinin rızası veya kanun emri, bu fiili hukuka uygun hale getirmektedir. Bu suç, kastla işlenebilen bir suçtur (Hafızoğulları ve Özen, 2021:292-294).

TCK 136'da da "Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, iki yıldan dört yıla kadar hapis cezası ile cezalandırılır." şeklinde hükme bağlanmıştır. Aynı maddenin ikinci fıkrası ağırlaştırıcı neden olup "Suçun konusunun, Ceza Muhakemesi Kanununun 236'ncı maddesinin beşinci ve altıncı fıkraları uyarınca kayda alınan beyan ve görüntüler olması durumunda verilecek ceza bir kat artırılır." şeklinde ifade edilmiştir (TCK m.136/1,2).

TCK 135'te hukuka aykırı olarak kişisel verileri kaydetmek suç olarak düzenlenmişken, TCK 136'da hukuka aykırı olarak verileri yaymak, başkasına vermek ve ele geçirmek fiilleri suç olarak düzenlenmiştir.

Kişisel verileri hukuka aykırı verme veya ele geçirme suçunun faili ve mağduru herkes olabilir. Suçun hukuki konusu, kişisel verilerin korunmasına dair yarardır. Kanun, kişisel verileri ele geçirme, verme ve yayma fiilleri suç olarak düzenlemiştir. Bu fiillerin hukuka aykırı olması gerekir. Emrin yerine getirilmesi durumlarında fiil hukuka uygun olacak ve suç oluşturmayacaktır. Bu suç kast ile işlenir (Hafızoğulları ve Özen, 2021:295-297).

Deepfake içerikler kullanılırken de kişilerin sesleri, görüntüleri kullanıldığından kişisel veriler kullanılmaktadır. Örneğin yüzlerin değiştirildiği bir içerik üretilmesi için birçok veri toplanması gerekir. Elde edilen verilerin de hukuka uygun toplanması gerekmektedir. Aksi halde TCK 135 uyarınca kişisel verilerin kaydedilmesi suçu oluşacaktır (Babayiğit, 2021:667).

Kişisel Verileri Koruma Kurumu tarafından da farkındalık oluşturma amacıyla 10.01.2024 tarihinde deepfake teknolojisinin ne için kullanıldığına, kişisel veriler açısından oluşturduğu tehditlere, nasıl tespit edilebileceğine ve deepfake teknolojisine karşı kişilerin ve kurumların neler yapabileceğine ilişkin bilgilerin yer aldığı "Deepfake Bilgi Notu" yayınlanmıştır.¹³

4.2.7. Müstehcenlik (TCK m. 226)

Türk Ceza Kanunu'nun 226. maddesinde müstehcenlik suçu yer almaktadır. 226.maddenin ikinci fıkrası uyarınca "Müstehcen görüntü, yazı veya sözleri basın ve yayın yolu ile yayınlayan veya yayınlanmasına aracılık eden kişi altı aydan üç yıla kadar hapis ve beşbin güne kadar adli para cezası ile cezalandırılır." şeklinde hükme bağlanmıştır (TCK m.226/2).

Deepfake teknolojisi bakımından önemli olan husus TCK 226/2'de düzenlenen suçtur. Bu maddede müstehcen görüntü, yazı veya sözlerin basın ve yayın yoluyla yayınlanması ve yayınlanmasına aracılık edilmesi fiilleri suç olarak düzenlenmiştir. Bu suçun faili, yayıncıdır. Suçun hukuki konusu ise müstehcen görüntü, söz veya yazının yayılmasının önlenmesine dair kamusal yarardır. Bu suçun gerçekleşebilmesi için müstehcen içerikleri yayınlama veya yayınlanmasına aracılık etme fiillerinin hukuka aykırı olarak gerçekleştirilmesi gerekmektedir. Hukuka uygunluk nedenleri, müstehcenlik suçu ile bağdaşmaz. Her iki suç da kasten işlenir (Hafızoğulları ve Özen, 2021:337,339).

Deepfake teknolojisi ile yaygın olarak müstehcen olmayan içeriklerden elde edilen görüntü ve videolardan müstehcen içerik üretilmektedir. Örneğin ünlü oyuncu Emma Watson'ın

¹³ Bkz. <https://www.kvkk.gov.tr/Icerik/7807/Deepfake-Bilgi-Notu>

görüntülerinden alınan verilerin, cinsel içerikli videolardaki kişilerin kafalarıyla değiştirilerek videolar hazırlanmıştır (Tenbarge, 2023). Bu şekilde oluşturulan içeriklerin yayınlanması durumunda içerikleri yayan kişi bakımından müstehcenlik suçu oluşacaktır.

Deepfake teknolojisinin en sık kullanıldığı alan cinsel içerikli görüntü veya video oluşturulmasıdır. Daha çok ünlülerde kullanılan bu teknolojinin mağduru genelde kadınlardır. Cinsel içerikler oluşturmak için "DeepNude" adlı bir bilgisayar uygulaması geliştirilmiştir. Bu uygulama derin öğrenme algoritmalarını kullanarak normal görüntüdeki insanların üzerindeki kıyafetleri çıkararak içerik üretmektedir (Ajder, Patrini, Cavalli ve Cullen, 2019). Ekim 2020'de deepfake içerik ve tespit konusunda uzmanlaşmış olan Sensity AI firmasının bir araştırması sonucunda kadınların rızası ve bilgisi olmadan oluşturulan 100.000'den fazla cinsel içerikli görüntü üretildiği bildirilmiştir. Hatta bu araştırmaya göre reşit olmayan çocukların görüntülerine de yer verildiği belirtilmektedir. Ayrıca 2018'den bu yana oluşturulan deepfake videolarının yaklaşık %95'inin rıza dışı alınmış pornografik görüntüye dayandığı belirtilmiştir (Ray, 2020).

4.2.8. Hakaret (TCK m. 125)

Hakaret suçu Türk Ceza Kanunu'nun 125. maddesinde düzenlenmiş olup, *"Bir kimseye onur, şeref ve saygınlığını rencide edebilecek nitelikte somut bir fiil veya olgu isnat eden (...)50 veya sövmek suretiyle bir kimsenin onur, şeref ve saygınlığına saldıran kişi, üç aydan iki yıla kadar hapis veya adli para cezası ile cezalandırılır. Mağdurun gıyabında hakaretin cezalandırılabilmesi için fiilin en az üç kişiyle ihtilat ederek işlenmesi gerekir."* şeklinde ifade edilmiştir (TCK m.125).

TCK 125. maddenin ikinci fıkrasında da bu suç, *"Fiilin, mağduru muhatap alan sesli, yazılı veya görüntülü bir iletile işlenmesi halinde, yukarıdaki fıkrada belirtilen cezaya hükmolunur."* şeklinde hüküm altına alınmıştır (TCK m.125).

Hakaret suçunun faili herhangi bir gerçek kişi olabilmektedir. Tüzel kişiler hakaret suçunun faili olamazlar. Bu suçun mağduru ise herkes olabilmektedir (Tezcan, Erdem ve Önok, 2021:636-637). Kanun maddesinde, somut bir olgu veya fiil isnat etmek ya da sövme fiilleri hakaret suçunun gerçekleşmesi bakımından aranmıştır. Bu suç ile korunan hukuki değer kişinin şerefi ve sosyal saygınlığıdır. Hakaret suçu genel kast ile işlenebilen bir suçtur, özel kast aranmaz (Özbek, Doğan ve Bacaksız, 2024:511,516,525). Bir kimsenin onuruna, şerefine veya saygınlığına dokunan fiilin hukuka aykırı olması gerekmektedir. Eğer fiil; ispat hakkı, yasama dokunulmazlığı, savunma dokunulmazlığı, bir hakkın kullanılması, kanun emrini yerine getirme ve haber verme hakkı kapsamında gerçekleştirilmişse fiil hukuka uygun hale gelir ve suç oluşturmaz (Hafızoğulları ve Özen,2021:244).

Bir sesli veya görüntülü deepfake içeriğinde aslında yer almayan kişilere yer verildiğinde veya içerikte yer alsın bile farklı biçimde gösterildiğinde bu içerik kişilerin onur, şeref ve saygınlığını rencide edecek nitelikte olabilir. Örneğin toplumda saygınlığa sahip bir kişinin olan A'nın resmi kıyafetle yer aldığı görüntüsünün, sırf A'nın saygınlığına saldırmak amacıyla genel ahlak ve adaba aykırı bir kıyafet giyen B'nin görüntüsüyle manipüle edilmesi durumunda hakaret suçu oluşmuş sayılacaktır (Babayiğit, 2021:671).

4.2.9. Yasak Cihaz ve Programlar (TCK m. 245/A)

Türk Ceza Kanunu'nun 245/A maddesinde; *"Bir cihazın, bilgisayar programının, şifrenin veya sair güvenlik kodunun; münhasıran bu Bölümde yer alan suçlar ile bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçların işlenmesi için yapılması veya oluşturulması durumunda, bunları imal eden, ithal eden, sevk eden, nakleden, depolayan, kabul eden, satan, satışa arz eden, satın alan, başkalarına veren veya bulunduran kişi, bir yıldan üç yıla kadar hapis ve beşbin güne kadar adli para cezası ile cezalandırılır."* denilmiştir (TCK m.245/A).

Herkes ilgili suçun faili ve mağduru olabilir (Özbek, Doğan, Bacaksız, 2024:1058). Hangi fiillerin suç oluşturacağı kanunda sayılmıştır. Suç işlemek için oluşturulmuş programları bulundurmaya beraber bunları imal etmek, sevk etmek, nakletmek, depolamak, kabul etmek, satmak, satışa arz etmek, başkalarına vermek fiilleri de kanunda suç olarak düzenlenmiştir. Suçun hukuki konusu bir cihaz, program, şifre ya da güvenlik kodudur. (Gül, 2021:348). Suçun oluşabilmesi için ilgili fiillerin hukuka aykırı olması gerekmektedir. Kanun emrinin yerine getirilmesi ve ilgilinin rızası varsa fiiller

hukuka uygun olur ve suç oluşmaz. Bu suç kasten işlenebilir, taksirle işlenmesi mümkün değildir (Özbek, Doğan ve Bacaksız, 2024:1060-1061).

Deepfake içeriklerin üretilmesi için bu tarz içerikler oluşturmak amacıyla programlar üretilmektedir. Bunun en bilinen örneği ise DeepNude uygulamasıdır (Samuel, 2019). Örneğin dolandırıcılık suçunun bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilmesi için DeepNude uygulamasını bulundurmak, TCK 245/A'da yer alan yasak cihaz ve program bulundurma suçunu oluşturacaktır (Babayiğit, 2021:666).

4.2.10. Manevi, Mali veya Bağlantılı Haklara Tecavüz (FSEK m. 71)

Fikir ve Sanat Eserleri Kanunu'nda (FSEK) da eserlerin ihlalleriyle ilgili birtakım suçlar düzenlenmiştir. Bunlardan biri de 71.maddede düzenlenen manevi, mali veya bağlantılı haklara tecavüz suçudur. Bu maddeye göre *"Bir eseri, icrayı, fonogramı veya yapımı hak sahibi kişilerin yazılı izni olmaksızın işleyen, temsil eden, çoğaltan, değiştiren, dağıtan, her türlü işaret, ses veya görüntü nakline yarayan araçlarla umuma ileten, yayımlayan ya da hukuka aykırı olarak işlenen veya çoğaltılan eserleri satışa arz eden, satan, kiralamak veya ödünç vermek suretiyle ya da sair şekilde yayan, ticarî amaçla satın alan, ithal veya ihraç eden, kişisel kullanım amacı dışında elinde bulunduran ya da depolayan kişi hakkında bir yıldan beş yıla kadar hapis veya adli para cezasına hükmolunur."* denilmiştir (7981 Sayılı 13.12.1951 Tarihli Resmî Gazete'de Yayımlanan 5846 Sayılı Fikir ve Sanat Eserleri Kanunu m.71).

Herkes bu suçun faili olabilir. Mağdur ise Kanun bakımından koruma altına alınmış olan eser sahipleridir. Suçun konusu ise kanunda sayılan eser, icra, fonogram veya yapımdır (Bayrak, 2021:313-314). Kanun maddesi kapsamında sayılan fiillerin hukuka aykırı olarak gerçekleştirilmesi gerekmektedir. İlginin rızası hukuka uygunluk nedenidir ve rıza varsa suç oluşmayacaktır. Bu suç kasten işlenebilen bir suçtur, taksirle işlenemez (Türey, 2024:801-802)

Örneğin bir sinema filmindeki sahnenin deepfake ile değiştirilmesi mümkündür. Hatta deepfake teknolojisinin olumlu kullanımının film endüstrisinde yaygın olduğuna yukarıda değinmiştik. Ancak bu değişiklik hak sahiplerinin yazılı izni alınmadan yapılırsa FSEK 71 uyarınca suç oluşacaktır (Babayiğit, 2021:672).

4.2.11. Diğer Suçlar

Deepfake teknolojisi kullanılarak işlenen suçlar burada sayılanlarla sınırlı değildir. Yapay zeka algoritmaları kullanan teknolojiler; bireyler, çevre güvenliği, mülkiyet, kamu ve devlet çıkarlarına yönelik saldırılar gibi birçok suç için araç olarak kullanılabilir (Sukhodolov, Bychkov ve Bychkova, 2021:209). Örneğin halk arasında korku ve panik yaratmak amacıyla tehdit (TCK m. 213), suç işlemeye tahrik (TCK m. 214), suçu ve suçluyu övme (TCK m. 215), halkı kin ve düşmanlığa tahrik ve aşağılama (TCK m. 216), kanunlara uymamaya tahrik (TCK m. 217), terör propagandası (Terörle Mücadele Kanunu m. 7/2), halkı askerlikten soğutma (TCK m. 318), adil yargılamayı etkilemeye teşebbüs (TCK m.288), seçimlerde yasak propaganda (Seçimlerin Temel Hükümleri ve Seçmen Kütükleri Hakkında Kanun m. 151) gibi suçlar oluşabilmektedir (Öztürk, 2021:76; Babayiğit, 2021:675). Hatta tüm temel hakların birbiri ile bağlantılı ve bağımlı olduğu düşünüldüğünde; eğitim, hukuk, demokrasi ve sosyal alanlarda yapay zekâ teknolojilerinin kullanılması tüm insan haklarını etkileme potansiyeli taşımaktadır (Završnik, 2021:191).

Şunu da belirtmek gerekir ki tek bir fiille, bu sayılan suçlardan birden fazlasının işlenebilmesi mümkündür. Örneğin bir kişinin rıza dışı alınmış görüntüsüyle cinsel içerikli bir deepfake görüntü oluşturulup yayılması durumunda hem kişisel verileri hukuka aykırı olarak yayma hem müstehcenlik hem de özel hayatın gizliliğini ihlal suçları gündeme gelebilecektir.

Sonuç ve Değerlendirme

Teknolojinin yaygınlaşmasıyla beraber yapay zekanın kullanımı da yaygınlaşmıştır. Yapay zekâ, kuşkusuz hayatımıza büyük kolaylık ve yenilik getirmiştir. Yapay zekâ sayesinde daha hızlı sonuçlara ulaşılabilmekte, birçok yeniliğe adım atılmakta, maddi yönden tasarruf sağlanmaktadır. Deepfake teknolojisinin kullanımı da bu gelişmelerle beraber artmaktadır. Deepfake teknolojisinin olumlu kullanım alanları göz ardı edilmeyecek kadar fazladır. Müzikten sinemaya, eğitimden sanata, teknolojiye finansla hemen her alanda faydalı kullanılabilir. Bununla beraber siyaset, ulusal güvenlik, finans, psikoloji, hukuk gibi alanlarda olumsuz kullanımı da çok yaygındır.

Özellikle olumsuz kullanım durumlarında ceza hukuku karşımıza çıkmaktadır. Oluşturulan sahte içeriklerle birçok suç işlenebilmekte, insanların saygınlıkları zedelenebilmekte, medyaya duyulan güven azalmaktadır. Gerçek olmayan görüntü ve videolar, yargılama sürecini de etkilemektedir. Sahte görüntü ve videoların tespiti, adaletin sağlanmasında da kritik roller oynayabilmektedir. Bunların önüne geçebilmek için de yasal düzenlemelerin yapılmasına gereksinim duyulmaktadır. Türkiye’de deepfake teknolojisiyle alakalı bir yasal düzenleme bulunmamaktadır. Yürürlükte olan kanunlar ilgili ve yeterli olduğu ölçüde uygulanabilmektedir. Sürekli gelişen ve değişen teknolojinin gerisinde kalmayan iç hukuk düzenlemeleri yapılmalıdır. Yasal düzenlemelerin yanı sıra adli tıp uzmanlığı, bilinçlendirme çalışmaları yapılarak yargılama süreçlerinde risk en aza indirilebilir. Güvenilir kaynaklardan bilgiye ulaşmak, medya okur yazarlığını arttırmak, deepfake içeriklerin tespiti için yeni yöntemler geliştirmek gibi konulara dikkat çekilmeli ve toplum bilinçlendirilmelidir. Bu sayede dijital güvenliğin artırılması ve deepfake içeriklerin yarattığı tehditlerle mücadelede etkili stratejiler oluşturulabilir. Diğer ülke mevzuatlarında zorunlu kılınan etiketleme sistemi gibi bizim ülkemizde de deepfake içeriklerin bir etiket ile açıkça gösterilmesi de bilinçlendirme ve farkındalık arttırmaya, aynı zamanda bu teknolojinin kullanımını da kontrol altına almaya yardımcı olacaktır. Son olarak deepfake içeriklerin üretimi ve kullanımının etik sınırlarının da hukuki düzenlemelerle belirlenmesi gerekmektedir.

Kaynakça

- Abanoz, Ö. B. (2021). *Deepfake İkilemi: Sadece Eğlence mi? Tehditler ve Hukuki Tartışmalar*. Lexpera Blog. (Çevrimiçi: <https://blog.lexpera.com.tr/deepfake-ikilemi-sadece-eglenec-mi-tehditler-ve-hukuki-tartismalar/>), Erişim Tarihi: 10.12.2024.
- Abanoz, Ö. B. (2021). *Derin Sahte (Deepfake) Teknoloji Karşısında Türk Ceza Hukuku*. Yapay Zekâ Temelli Teknolojiler ve Ceza Hukuku, Yapay Zekâ Çağında Hukuk, İstanbul Barosu, s.64-81.
- Aksu, M. (2023). *Yapay Zeka ve Hukuk* (Editör: Mustafa Aksu), On İki Levha Yayıncılık, İstanbul, s.24-25.
- Alacakaptan, U. (1975). *Suçun Unsurları* (İkinci Bası). Ankara:Ankara Üniversitesi Hukuk Fakültesi Yayınları-Sevinç Matbaası.
- Anıkaydın, İ. (2022). Deepfake Uygulamalarının Hukuki Boyutu. *Düzce Üniversitesi Sosyal Bilimler Dergisi*, 12(2), s.736-747.
- Attenborough, I. (2020). *Voices, Copyrighting and Deepfakes*. [Available online at: https://ipwatchdog-com.translate.goog/2020/10/14/voices-copyrighting-deepfakes/id=126232/?_x_tr_sl=en&_x_tr_tl=tr&_x_tr_hl=tr&_x_tr_pto=wa], Retrieved on Decemeber 9, 2024.
- Aydemir, D. (2024). Görsel İletişimde Manipülasyon: Deepfake Teknolojisi ile Hazırlanan Megafon Reklamının Göstergebilimsel Analizi. *Kent Akademisi Dergisi*, 17(5), s.1902-1924.
- Aydın, S. (2024). *Derin Öğrenme Tabanlı Deepfake Algılama ve Siber Güvenlik: Toplum Algısının İncelenmesi*. Yayımlanmamış Yüksek Lisans Tezi, Haliç Üniversitesi Lisansüstü Eğitim Enstitüsü, İstanbul.
- Babayiğit, B. (2021). Deepfake’in Ceza Hukuku Bakımından Değerlendirilmesi ve De Lege Ferenda Öneriler. *Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi*, 25(4), s.655-703.
- Bacaksız, P. & Sümer, S. M. (2021). *Robotlar, Yapay Zeka ve Ceza Hukuku* (Birinci Baskı). Ankara:Adalet Yayınevi.
- Bayrak, Ö. (2021). *Fikri ve Sınai Mülkiyet ve Haksız Rekabet Suçları* (İkinci Baskı). Ankara:Seçkin Yayıncılık.
- Bellware, K. (2021). *Cheer mom used deepfake nudes and threats to harrass daughter’s temmates police say*. [Available online at: <https://www.washingtonpost.com/nation/2021/03/13/cheer-mom-deepfake-teammates/>], Retrieved on Decemeber 10, 2024.
- Berk, M. E. (2020). Dijital Çağın Yeni Tehlikesi “Deepfake. *OPUS Uluslararası Toplum Araştırmaları Dergisi*, 16(28), s.1510-1523.

- Bill to curb deepfake pornography clears legislature.* [Available online at: <https://www.taipetimes.com/News/front/archives/2023/01/08/2003792190>], Retrieved on December 11, 2024.
- Briscoe, S. (2021). *U.S. Laws Address Deepfakes.* [Available online at: <https://www.asisonline.org/security-management-magazine/latest-news/today-in-security/2021/january/U-S-Laws-Address-Deepfakes/>], Retrieved on December 11, 2024.
- Centel, N., Zafer, H. & Çakmut, Ö. (2020). *Türk Ceza Hukukuna Giriş (On Birinci Baskı)*. İstanbul:Beta Basım Yayım.
- Chesney, C. & Citron, D. (2019). Deep Fakes: A looming challenge for privacy, democracy, and national security. *California Law Review*, 107, s.1753-1820.
- Dagar, D. & Vishwakarma, D. K. (2022). A literature review and perspectives in deepfakes: generation, *International Journal of Multimedia Information Retrieval*, 3, s.219-289.
- Damiani, J. (2019). *A Voice Deepfake Was Used To Scam A CEO Out Of \$243,000.* [Available online at: <https://www.forbes.com/sites/jessedamiani/2019/09/03/a-voice-deepfake-was-used-to-scam-a-ceo-out-of-243000/>], Retrieved on December 11, 2024.
- Dean, A. (2020). *Deepfakes, Pose Detection, and the Death of "Seeing is Believing."* [Available online at: <https://www.lawtechnologytoday.org/2020/08/deepfakes-pose-detection-and-the-death-of-seeing-is-believing/>], Retrieved on December 2, 2024.
- Erdoğan, M. A. (2023). *Deepfake Teknolojisinin Hukuka Aykırı Kullanımından Doğan Hukuki ve Cezai Sorumluluk*. Yayınlanmamış Yüksek Lisans Tezi, Altınbaş Üniversitesi Lisansüstü Eğitim Enstitüsü, İstanbul.
- Ergün, G. O. (2023). *Machina Saphiens. Ankara Üniversitesi Hukuk Fakültesi Dergisi*, 72 (2), s.717-758.
- European Parliamentary Research Service. (2021). *Tackling deepfakes in European policy*, Brussels: European Parliamentary Research Service. 3.
- Farid, H., Hwang T., Lyu S. & Zucconi A. (2019). Deepfakes and Audio-visual Disinformation. *Centre for Data Ethics and Innovation*.
- Farris, L. (2024). *Government cracks down on 'deepfakes' creation.* [Available online at: <https://www.gov.uk/government/news/government-cracks-down-on-deepfakes-creation>], Retrieved on December 12, 2024.
- Federal Konsey Yasa Tasarısı, *Entwurf eines Gesetzes zum strafrechtlichen Schutz von Persönlichkeitsrechten vor Deepfakes*, [Available online at: <https://dserver.bundestag.de/btd/20/126/2012605.pdf>], Retrieved on December 12, 2024.
- Feeney, M. (2021). Deepfake Laws Risk Creating More Problems Than They Solve. *Regulatory Transparency Project of the Federalist Society*.
- Ferraro, M. F., Chipman, J. C. & Preston, S. W. (2020). The Federal "Deepfakes" Law. *The Journal of Robotics, Artificial Intelligence & Law*, 3(4), s.229-233.
- Foley, J. (2024). *25 of the best deepfake examples that terrified and amused the internet.* [Available online at: <https://www.creativebloq.com/features/deepfake-examples>], Retrieved on December 5, 2024.
- Gül, A. (2021). *Doğrudan-Dolaylı Bilişim Suçları (Üçüncü Baskı)*. Ankara:Seçkin Yayıncılık.
- Hafizoğulları, Z., Özen, M. (2016). *Türk Ceza Hukuku Özel Hükümler Millete ve Devlete Karşı Suçlar (Birinci Baskı)*. Ankara:US-A Yayıncılık.
- Hafizoğulları, Z., Özen, M. (2017). *Türk Ceza Hukuku Özel Hükümler Topluma Karşı Suçlar (Üçüncü Baskı)*. Ankara:US-A Yayıncılık.
- Hafizoğulları, Z., Özen, M. (2021). *Türk Ceza Hukuku Genel Hükümler (On Üçüncü Baskı)*. Ankara:US-A Yayıncılık.
- Hafizoğulları, Z., Özen, M. (2021). *Türk Ceza Hukuku Özel Hükümler Kişilere Karşı Suçlar (Yedinci Baskı)*. Ankara:US-A Yayıncılık.
- Hou, L.C., Tung, L. C., Madjar, K. (2023). *Police warn against scams using deepfake videos.* [Available online at: <https://www.taipetimes.com/News/taiwan/archives/2023/05/30/2003800665>], Retrieved on December 12, 2024.

- İlkılıç, İ. (2021). Tipta Yapay Zeka Kullanımında Etik Sorun Alanları. *Ceza Hukukunda Robot, Yapay Zeka ve Yeni Teknolojiler içinde* (Editör: Kayıhan İçel), Seçkin Yayıncılık, Ankara, s.121-135.
- Jaiman, A. (2020). *Positive Use Cases of Synthetic Media (aka Deepfakes)*. [Available online at: <https://towardsdatascience.com/positive-use-cases-of-deepfakes-49f510056387/>], Retrieved on December 3, 2024.
- Jain, S. (2020). *Deepfakes in India: Regulation and Privacy*. [Available online at: <https://blogs.lse.ac.uk/southasia/2020/05/21/deepfakes-in-india-regulation-and-privacy/>], Retrieved on December 12,2024.
- Kandır, M. O. (2023). Sosyal Medyanın Bilişim Suçlarına Etkisi. *Eskişehir Barosu Dergisi*, 8(1), s.152.
- Kangal, T. Z. (2021). *Yapay Zeka ve Ceza Hukuku* (Birinci Baskı), İstanbul:On İki Levha Yayıncılık.
- Kietzmann, J., Lee, L. W., MacCarthy, I. P. & Kietzmann, T. C. (2020). Deepfakes: Trick or treat?. *Business Horizons*, 63(2), s.135-146.
- Kurzweil, R. (1990). *The Age of Intelligent Machines* (First Edition). Cambridge: MIT Press.
- Lakshmi, D. & Hemanth, D. J. (2024). An Overview of Deepfake Methods in Medical Image Processing for Health Care Applications. *Design Studies and Intelligence Engineering*, 383, s.304-311.
- Lee, D. (2019). *Deepfake Salvador Dalí takes selfies with museum visitors*. [Available online at:<https://www.theverge.com/2019/5/10/18540953/salvador-dali-lives-deepfake-museum>], Retrieved on December 5, 2024.
- Mack, D. (2018). *This PSA About Fake News From Barack Obama Is Not What It Appears*. [Available online at: <https://www.buzzfeednews.com/article/davidmack/obama-fake-news-jordan-peepe-psycho-video-buzzfeed>], Retrieved on Decemeber 9, 2024.
- Magramo, K., Chen, H. (2024). *Finance worker pays out \$25 million after video call with deepfake 'chief financial officer'*. [Available online at: <https://edition.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html>], Retrieved on December 12,2024.
- Mohsin, K. (2021). Yapay Zeka Hukukunun Gerekliliği (Çev.:Ç. Karadağ). *Ceza Hukukunda Robot, Yapay Zeka ve Yeni Teknolojiler içinde* (Editör: Kayıhan İçel), Seçkin Yayıncılık, Ankara, s.41-46.
- Negi, S., Jayachandran, M. & Upadhyay, S. (2021). Deep fake : An Understanding of Fake Images and Videos. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 7(3), s.183.
- Nema, P. (2020). *Are Indian Laws Equipped To Deal With Deepfakes?*. [Available online at: <https://jils.blog/2020/07/19/are-indian-laws-equipped-to-deal-with-deepfakes/>], Retrieved on December 12,2024.
- Özyiğit, S. (2022). Karşılaştırmalı Hukuktaki Gelişmeler Işığında Deepfake Teknolojisinin Regülasyonu ve Türk Hukuku için Öneriler. *Bilişim ve Teknoloji Hukuku Yıllığı*.
- Palmi, K. (2021). *Ses klonlama teknolojisi: Kimlere yarayabilir, riskleri neler?* [Çevrimiçi: <https://www.bbc.com/turkce/haberler-dunya-57810973>], Erişim Tarihi: 01.12.2024.
- Pradhan, P. (2020). AI Deepfakes The Goose Is Cooked?, *University of Illionis Law Review*.
- Prezja, F., Paloneva, J., Pölönen, I., Niinimäki, E. & Äyrämö, S. (2022). DeepFake knee osteoarthritis X-rays from generative adversarial neural networks deceive medical experts and offer augmentation potential to automatic classification. *Scientific Reports*, 12(1) :18573. s.1-16.
- Ray, S. (2020). *Bot Generated Fake Nudes Of Over 100,000 Women Without Their Knowledge*. [Available online at:<https://www.forbes.com/sites/siladityaray/2020/10/20/bot-generated-fake-nudes-of-over-100000-women-without-their-knowledge-says-report/?sh=428694037f6b>], Retrieved on December 13, 2024.
- Redi, J., Dugelay, J. L. & Taktak, W. (2011). Digital image forensics: A booklet for beginners. *Multimedia Tools and Applications*, 51(1), s.133-162.
- Rothkopf, J. (2020). *Deepfake Technology Enters the Documentary World*. [Available online at: <https://www.nytimes.com/2020/07/01/movies/deepfakes-documentary-welcome-to-chechnya.html>], Retrieved on December 4, 2024.
- Russel, S. & Norvig, P. (2010). *Artificial Intelligence A Modern Approach* (Third Edition). England:Pearson Education.

- Samuel, S. (2019). *A guy made a deepfake app to turn photos of women into nudes. It didn't go well.* [Available online at: <https://www.vox.com/2019/6/27/18761639/ai-deepfake-deepnude-app-nude-women-porn>], Retrieved on December 13, 2024.
- Sarker, I. H. (2021). Deep Learning: A Comprehensive Overview on Techniques, Taxonomy, Applications and Research Directions. *SN Computer Science*, 2(6), 420.
- Sharf, Z. (2021). *Lucasfilm Hired the YouTuber Who Used Deepfakes to Tweak Luke Skywalker 'Mandalorian' VFX.* [Available online at: <https://www.indiewire.com/features/general/lucasfilm-hires-deepfake-youtuber-mandalorian-skywalker-vfx-1234653720/>], Retrieved on December 4, 2024.
- State of Deepfake Legislation, 2024 Annual Report.
- Stupp, C. (2019). *Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case.* [Available online at: <https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402>], Retrieved on Decemeber 9, 2024.
- Sukhodolov A. P., Bychkov A. V. & Bychkova A. M. (2021). Yapay Zeka Teknolojileri Kullanılarak İşlenen Suçlar İçin Ceza Politikası:Devlet, Sorunlar, Beklentiler. *Ceza Hukukunda Robot, Yapay Zeka ve Yeni Teknolojiler içinde* (Editör: Kayıhan İçel), Seçkin Yayıncılık, Ankara, s.207-214.
- Tenborge, K. (2023). *Hundreds of sexual deepfake ads using Emma Watson's face ran on Facebook and Instagram in the last two days.* [Available online at: <https://www.nbcnews.com/tech/social-media/emma-watson-deep-fake-scarlett-johansson-face-swap-app-rcna73624>], Retrieved on December 13, 2024.
- Tezcan, D., Erdem, M. R. & Önok, R. M. (2020). *Teorik ve Pratik Ceza Özel Hukuku* (On Sekizinci Baskı). Ankara: Seçkin Yayıncılık.
- Tezcan, D., Erdem, M. R. & Önok, R. M. (2022). *Teorik ve Pratik Ceza Özel Hukuku* (Yirminci Baskı). Ankara: Seçkin Yayıncılık.
- Thambawita, V., Isaksen, J. L., Hicks, S. A., Ghouse, J., Ahlberg, G., Linneberg, A., Hammer, H. et al. (2021). Deepfake electrocardiograms using generative adversarial networks are the beginning of the end for privacy issues in medicine. *Scientific Reports*. 11(1), s.1-8.
- Toroslu, N., Toroslu, H. (2021). *Ceza Hukuku Genel Kısım* (Yirmi Altıncı Baskı). Ankara:Savaş Yayınevi.
- Turan, M. (2016). *Bilişim Hukuku* (Sekizinci Baskı). Ankara: Seçkin Yayıncılık.
- Türay, A. (2024). *Manevi, Mali ve Bağlantılı Haklara Tecavüz Suçları* (Birinci Baskı) Ankara:Seçkin Yayıncılık.
- Ünver, Y. (2023). *İftira, Suç Uydurma, Suç Üstlenme, Yalan Tanıklık ve Bilirkişilik, Suçu İhbar Etmemek Suçları* (Yedinci Baskı). Ankara:Seçkin Yayıncılık.
- Weisberger, M. (2019). *This Animated Mona Lisa Was Created by AI, and It Is Terrifying.* [Available online at: <https://www.livescience.com/65573-mona-lisa-deepfakes.html>], Retrieved on December 5, 2024.
- Westerlund, M. (2019). The emergence of deepfake technology: a review. *Technology Innovation Management Review*. 9(11), 39-52.
- Whyte, C. (2020). Deepfake news: ai-enabled disinformation as a multi-level public policy challenge. *Journal of Cyber Policy*, 5(2), s.199-217.
- Wilson, M. (2019). *The Salvador Dalí Museum just Deepfaked Dalí.* [Available online at: <https://www.fastcompany.com/90355299/the-salvador-dali-museum-just-deepfaked-dali-see-the-video-here>], Retrieved on December 5, 2024.
- Yalçın, N. & Çiçek, H. K. (2024). Deepfake Bir Tehdit mi Fırsat mı?, *Euroasia Journal of Mathematics, Engineering, Natural & Medical Sciences*. 11(32), s.31-46.
- Yapay Zekâ Çalışma Grubu, (2023). *Yapay Zekâ ve Hukuk: Deepfake Üzerine Bir Değerlendirme.* *İstanbul Barosu Dergisi*, s.11.
- Yavuz, C. (2021). *Cinsel İçerikli Görüntülerin Rıza Dışı Paylaşımı İntikam Pornosu* (Birinci Baskı). Ankara: Seçkin Yayıncılık.
- Yavuz, C. (2022). *Deepfake (Derin Sahte)*, (Birinci Baskı). Ankara: Seçkin Yayıncılık.
- Yurtcan, E. (2019). *Yargıtay Kararları Işığında İftira Suçu* (Üçüncü Bası). Ankara:Seçkin Yayıncılık.

- Završnik, A. (2021). Yapay Zeka Hukukunun Gerekliliği (Çev.:H. Akdağ). *Ceza Hukukunda Robot, Yapay Zeka ve Yeni Teknolojiler içinde* (Editör: Kayıhan İçel), Seçkin Yayıncılık, Ankara, s.181-201.
- Zhao, Y., Cutrell, E., Holz, C., Morris, M. R., Ofek, E. & Wilson, A. D. (2019). *SeeingVR: A set of tools to make virtual reality more accessible to people with low vision*. CHI Conference on Human Factors in Computing Systems Proceedings. New York, USA.

Extended Abstract

Aim and Scope

Today, the use of deepfake technology developed using artificial intelligence and deep learning techniques has become quite widespread. This study examines the social, legal and ethical dimensions of deepfake technology. Although deepfake technology offers beneficial usage opportunities in various fields, when used as a means of committing crimes, it can cause social turmoil, undermine media trust and affect judicial processes. The positive and negative aspects of Deepfake technology are examined and its negative effects, especially in terms of criminal law, are evaluated by examining national and international doctrine. The scope of the study is not limited to technical and legal aspects, but aims to draw attention to the importance of social awareness and awareness-raising activities.

Methods

In this study, the definition, development and current usage areas of deepfake technology were examined by conducting a literature review; in addition, legal regulations were examined comparatively. The study evaluates the crimes that deepfake technology may cause. How the current legal system in Turkey deals with deepfake technology is analyzed and evaluations are made on how the deficiencies in this field can be eliminated. The analysis is supported by practical solutions such as forensic expertise and increasing media literacy, focusing on issues such as detecting deepfake content and drawing ethical boundaries. This methodological approach enables the development of effective strategies against the potential threats of deepfake technology in the legal field.

Findings

As a result of the analysis conducted in this study, it has been determined that deepfake technology has significant impacts on our lives in both positive and negative aspects. Among the positive areas of use, the creative potential and increased productivity in sectors such as cinema, education, art and music have attracted attention. However, the negative effects of the technology are more evident, especially in legal and ethical areas. Deepfake content can be associated with crimes such as the production of fake news, fraud, blackmail, violations of personal rights and the production of pornographic content. This can damage people's reputations, undermine public trust and manipulate judicial processes. Moreover, it has been observed that there are serious problems in accepting deepfake videos as forensic evidence and that existing legal regulations are insufficient in the face of this new technology.

Conclusion

Deepfake technology has many potentials, both positive and negative. It offers opportunities for creative and productive use, especially in areas such as cinema, education and art, but also poses significant threats in areas such as politics, media, law and security. This study examines the potential of deepfake content to be used as evidence in judicial processes and the legal problems that may arise from this content, and emphasizes that the current legal regulations are insufficient. The lack of a legal regulation in this field in Turkey constitutes a major deficiency in preventing deepfake-related crimes and rights violations. In order to overcome these deficiencies, it was concluded that domestic legal regulations should be renewed, forensic expertise should be increased and media literacy should be strengthened.

What needs to be done next is to develop new technologies for the detection of deepfake content, to draw ethical boundaries and to raise public awareness on this issue. In addition, legal regulations need to be updated rapidly in order to keep the production and use of deepfake content within legal boundaries. In addition, methods such as international cooperation and labeling systems can be

important steps to minimize the negative effects of deepfake technology. In conclusion, with the rapid advancement of technology, it is critical that effective strategies to protect societies and legal systems are implemented as soon as possible.