DÜSOBED/JDUISS Düzce Üniversitesi Sosyal Bilimler Dergisi, Yıl: 12, Sayı: 2
Duzce University Journal of Social Sciences, Vol: 12, Issue: 2

Makale Türü/Article Type: Araştırma Makalesi/Research Article

DEEPFAKE UYGULAMALARININ HUKUKİ BOYUTU

İlayda ANIKAYDIN[1]

Öz

Teknolojik gelişmelerin hızla arttığı günümüzde özellikle yapay zekâ teknolojisiyle hayatlarımızda köklü değişiklikler meydana gelmiştir. Siyasetten ekonomiye, hukuktan eğitime hayatlarımızın her alanını etkileyen teknolojik gelişmeler, getirdikleri kolaylıkların yansıra birtakım sorunlara yol açmıştır. Bu gelişmelerden son yıllarda popüler hale gelen teknoloji ise deepfake kavramıdır. Çalışmada öncelikle deepfake kavramını açıklama gayretinde bulunulmuştur. Devamında ise deepfake içeriklerinin oluşturulma biçiminden söz edilmiştir. Deepfake'in oluşturduğu veya oluşturması muhtemel olan sahte haber yaratma, seçim veya borsa manipülasyonu, kişinin rıza dışı alınmış görüntüleriyle pornografik içerik üretme, siber zorbalık, sahte ses ile dolandırıcılık gibi siyasi, finansal ve suç unsuru barındıran diğer olası tehlikeleri örneklendirilerek açıklanmıştır. Söz konusu tehlikelere karşı mevcut uluslararası ve ulusal yasal düzenlemeler incelenmiştir. Sonuç olarak ise artık herkesin ulaşabildiği, hızla yaygınlaşan deepfake içeriği üretebilme erişiminin yol açtığı ya da açması öngörülen sorunlara yönelik çözüm önerilerinde bulunulmuştur.

Anahtar Kelimeler: Deepfake, Yapay Zekâ Teknolojisi, Siber Suçlar, Fikri Haklar

Abstract

In today's world, where technological developments are increasing rapidly, especially with artificial intelligence technology, fundamental changes have occurred in our lives. Technological developments that affect every aspect of our lives, from politics to economy, from law to education, have led to some problems as well as the convenience they bring. The technology that has become popular in recent years from these developments is the concept of deepfake. In the study, first of all, efforts were made to explain the concept of deepfake. In the following, the way of creating deepfake contents was mentioned. Other possible dangers such as creating fake news, election or debt manipulation, producing pornographic content with images of the person without consent, cyber bullying, fake voice fraud, etc, are explanied and examplyfied. The current international and national legal regulations have been examined against these dangers. As a result, solutions are offered for the problems that are caused or anticipated to be caused by the access to produce deepfake content, which is now accessible to everyone and is rapidly spreading.

Keywords: Deepfake, Artificial Intelligence Technology, Cybercrime, Intellectual Property

[1] İstanbul Aydın Üniversitesi Bilişim Hukuku Tezli Yüksek Lisans Öğrencisi, ilaydaanikaydin@stu.aydin.edu.tr, Orcid No: 0000-0001-9980-062X

Bu makaleye atıfta bulunmak için/Cite as: Anıkaydın, İ. (2022). Deepfake Uygulamalarının Hukuki Boyutu. *Düzce Üniversitesi Sosyal Bilimler Dergisi*, 12(2), 736-747

Makale Geliş Tarihi: 16.06.2022 Makale Kabul Tarihi: 17.11.2022 Makale Yayın Tarihi: 31.12.2022

Giriş

Dünya çapında teknolojik gelişmeler, devrim niteliğindeki bilgisayarın icadı ile hız kazanmış, dijital çağa giriş yapılmıştır. Söz konusu bu gelişmeler beraberinde ekonomik, toplumsal, hukuksal her alanda hayatlarımızda köklü değişiklikler meydana getirmiştir. Bu dijitalleşmenin bir diğer getirisi ise yapay zekâ ve robotik alanındaki gelişmelerdir. Yapay zekâ kavramı ile hayatlarımıza birçok yeni kavram girmiş olup bunlardan bir tanesi de "deepfake"dir. Deepfake Türkçe anlamı ile derin sahtenin günümüz internet kullanıcılarının sıklıkla duyduğu bir kelime olduğunu söylemek mümkündür. Öncelikle 2017 yılında Reddit platformundaki "deepfake" adındaki bir kullanıcı, Hollywood yıldızlarının yüzlerini yüz değiştirme uygulaması sayesinde porno yıldızlarının yüzüne yapıştırarak bu kavramın hayatlarımızda popüler hale gelmesine yol açmıştır. 2018 yılına gelindiğinde ise, ilgili reddit platformu kullanıcısının kullanmış olduğu benzer araçlar halka açık hale gelmiştir. İşbu araçlar vasıtasıyla oluşturulmuş ve oldukça popüler hale gelen FakeApp adlı ücretsiz uygulama çevrimiçi olarak kullanılabilir duruma gelmiştir. FakeApp, Google'ın açık kaynaklı derin öğrenme yazılımı kullanılarak geliştirilmiştir. Öyle ki, uygulama halka açık olduğu ilk iki ayında, 120.000'den fazla kez indirilmiştir (Gerstner,2020:2). FakeApp ve diğer benzer yazılımların yaygın olarak kullanılmasından kaynaklanan çok yönlü sonuçlar ve dolayısıyla problemlerin ortaya çıktığı görülmektedir. Özellikle siyasetçiler, ünlülüler hakkında sahte haber yaratma hususunda deepfake uygulamaları, epey endişe verici durumdadır. Tabi ki deepfake'in siyasi ve kültürel sonuçları önemli olsa da ve etkiledikleri alan yelpazesinde değinilmesi gereken çok sayıda husus olsa da, bu çalışmada öncelikle bu programların hukuki niteliği, mevcut/muhtemel hukuki sorunlar ve çözümleri üzerinde durulacaktır.

1. DEEPFAKE NEDİR VE NASIL ÇALIŞIR?

Deepfake içerikleri temel olarak yüz değiştirme, ifade değiştirme ve yüz yaratımı olmak üzere üç çeşit teknikle oluşturulabilmektedir. Özellikle yüz değiştirme teknolojisiyle oluşturulan deepfake içerikleri "makine öğrenimi" tekniği kullanılmak suretiyle yapay zekâ teknolojisi ile oluşturulmaktadır. Oldukça ikna edici bir deepfake içeriği 300 kadar az görüntü ile oluşturulabilmektedir. (Çolak,2021:7). Devasa veri kümeleri üzerinde çalışan algoritmalar; kaynak olarak da adlandırılabileceğimiz bir yüz ile hedef olarak adlandırılan diğer yüzü, yüz değiştirme tekniğiyle değiştirmektedir. Deepfake, var olan veri setlerinden yeni veriler üretebilen (yaratabilen) bir algoritma seti olan "*Generative Adversarial Networks'ü"* (GANlar), yani "Üretken Çekişmeli Ağları" kullanmaktadır (Baker, 2019: 6). Hangi teknik kullanılırsa kullanılsın, içerik üretme süreci genellikle çıkarma, eğitim ve oluşturma adımlarıyla gerçekleştirilmektedir. Belirtmek isteriz ki, günümüzde büyük veri setlerine ihtiyaç duyulmaksızın bir kaynağın tek bir fotoğrafı bile derin sahte içerikler oluşturmak için yeterlidir (Çolak, 2021: 12). Anlatılanlar ışığında, yukarıda bahsedilen üç tekniği açıklamakta fayda görmekteyiz. Buna göre;

1.1. Yüz Değiştirme

Yüz değiştirme, yüzü değiştirilecek olan hedef kişinin fotoğraflarının, bir diğer kişinin videosuna, video manipülasyon tekniği ile monte edilmesi işlemidir. Kısaca yüz değiştirmesi yapılacak kişinin yüzünün bulunduğu ve mümkün olduğunca yüksek kaliteli fotoğraf yahut videolardan seçilecek görüntülerin, hedef yüze yapay zekâ sistemi aracılığıyla monte edilmesi işlemidir (Berk, 2020: 1510).

1.2. İfade Değiştirme

İfade değiştirme bir kişinin yüzünün özellikleri, mimikleri, göz ve kaş ifadelerinin tekrar yaratılması anlamına gelmektedir. Burada kaynak videodan alınan yüz ifadeleri diğer kişinin yüzüne eklenmektedir. Bu işlemle birlikte esasında hedef, kişinin söylemediği bir husus hakkında

bile, kaynak videodan aldığı ifadeleri kullanarak söylemiş gibi gösterilmesidir. Bu şekliyle bu işlemin bir nevi taklit işlemi olduğunu söylemek mümkündür. (Berk,2020:1513.)

1.3. Yüz Yaratımı

Yüz yaratımı tekniğinde ise yukarıda değindiğimiz üretken çekişmeli ağlar tarafından yetkinleştirilen yazılımla iki çeşit sinir ağı yaratılmaktadır. Bu ağların, "üretken" ve "ayrıştırıcı" şeklinde iki türü mevcuttur. Bu iki ağ da birbirleriyle mücadele içerisindedir. Bu mücadelenin gayesi, daha gerçekçi ürünler ortaya çıkartmaktır. Böylelikle üretken ağı resim oluşturmaktayken, ayrıştırıcı ağ ise söz konusu resmin gerçekliği hususunda derin öğrenme (deep learning) sürecine girmektedir. Ayrıştırıcı ağ, üretken ağın ürettiği resmi yani ortaya çıkardığı neticeyi sahte olarak algılarsa; üretken ağ daha gerçekçi yani sahte olmadığını anlayacak biçimde üretmeye devam etmektedir. (Farid vd., 2019:4)

Yukarıda bahsedilen her tekniğin kendine has çalışma prensipleri bulunmaktadır. Söz konusu tekniklerden en sık kullanılan teknik ise yüz değiştirme (Face Replacement) işlemidir (Berk,2020:1515). Açıkça ifade edildiği üzere deepfake çıktıktan sonra gerekli yazılım ve yönergelerle deepfake içeriğinin neredeyse herkesin oluşturabileceği hale gelmiştir. Derin öğrenme adı altında işlem yapmakta olan yazılımlar, söz konusu yüz değiştirme işlemini çeşitli algoritmaların hesaplanmasıyla beraber oldukça basit oldukça hızlı vaziyete dönüşmüştür. (Berk,2020:1515).

2. DEEPFAKE OLUŞTURMA BİÇİMİ

Deepfake; temel olarak çıkarma, öğrenme, oluşturma olmak üzere üç işlemden meydana gelmektedir. Çıkartma işlemi hem kaynak hem de hedef video ya da fotoğraf dosyalarının yazılımın algoritmaları dolayısıyla yüzleri tanıma ve yalnızca o alanı fotoğraf biçiminde algılama yöntemidir. Söz konusu teknik neticesinde yazılım, referans kişiden aldığı verileri hedef yüze monte edilmesine olanak sağlayan bir işlemi düzenlemektedir. Bu işlemdeki derin öğrenme aşaması için referans olarak kaynak video ya da fotoğraflardan çıkartılan yüz resimleri kullanılmaktadır. Diğer bir işlem olan öğrenme ise hedef ve referans dosyadan çıkarılan fotoğraflar autoencoder işlemi (oto kodlayıcı) adı verilen "derin öğrenme" aşamasına girmektedirler (Berk,2020:1515). Bu aşamada yukarıda da bahsedildiği üzere bir tanesi referans yüz için öteki ise hedef yüz için olmak üzere iki sinir ağı kullanılmaktadır. Bu iki tür sinir ağı farksız "encoder" (kodlayıcı)'ı kullanırken, aynı zamanda iki ayrı çözücü de kullanmaktadırlar. Bu iki sinir ağı da derin öğrenme süreci otomatik kodlama işlemini, benzerlikte bir yüzün görüntüsünü, asıl sürümüne yeniden yapılandırana kadar devam etmektedir. Son kademe olarak da adlandırılan "oluşturma" işleminde, derin öğrenme evresinde yüz değiştirme işlemi, yazılımın kaynak ve hedef yüzlerin yer değişimini yapmasında kullandığı algoritmalar doğrultusunda meydana gelmektedir. Bu noktada yazılımın programlanmasının amacı derin öğrenme sürecinde kullandığı kaynak resim ya da video dosyalarından çıkardığı resimleri hedef yüze eşleştirmektir. Bu kademeye varmadan önce kaynak karakterin yüz ifadelerinin fazla olması, yüz eşleştirmesinin de seçkin bir netice vermesini sağlayacaktır (Farid vd.,2019:4).

3. DEEPFAKE VE YARATABİLECEĞİ TEHLİKELER

3.1. Deepfake ve Siyasi Tehlikeler

Deepfake'in sahte haber oluşturma, siyasi hasara neden olma ve kadınlar, azınlıklar ve savunmasız kişiler gibi belirli demografik özellikleri hedefleme dahil olmak üzere bu teknolojiyi kötüye kullanmanın ve/veya kötüye kullanmanın potansiyel tehlikeleri (Black vd., 2018: 2) mevcuttur. Öncelikle gerçek dışı haber probleminden bahsetmek gerekirse; çevrimiçi olarak yayınlanan bilgiler için merkezi bir doğruluk kontrol otoritesi yoktur ve viral medya tek bir günde

milyonlarca kez görüntülenebilmektedir. Haber döngüsüne ve medyaya olan güven, son yıllarda önemli ölçüde aşınmış durumdadır ve deepfake ile oluşturulan sahte içerikler çoğaldıkça, sorunun artması muhtemeldir. Üzerinde mutabık kalınan bir gerçek ise, ulusal ve küresel sorunlar siyasal anlamda baş gösterecektir (Dean, 2020: 21). Bunun en bilinen örneği ise Amerikalı oyuncu Jordan Peele'nin, deepfake yolu ile Amerika Birleşik Devletleri eski başkanı Barack Obama'nın ağzından "Başkan Trump tam bir ahmak" cümlesini kurdurtması ve videonun çok gerçekçi olup bu sözlerin Obama'nın ağzından çıkmış gibi görülmesi sebebiyle tüm dünyanın ilgisini çekmiştir (www.ntv.com.tr). Nitekim Amerika'da özellikle milli güvenlik, siyasi seçimlerin manipüle edilmesini önlemek ve bilgi kirliliğini engellemek gayesiyle deepfake ile ilgili kanunları çıkarıldığı görülmektedir. Söz konusu mevzuat çalışmalarında deepfake teknolojisi ile üretilmiş olan içeriklere yahut ona benzeyen yazılımlarla üretildiklerini ifade bir filigran koyulması zarureti getirilmektedir (Chipman, 2021:12). Yine Amerika'da Teksas, 1 Eylül 2019'da devlet görevi için adaylara zarar verme veya seçimleri etkileme amaçlı deepfake videoların oluşturulmasını ve dağıtımını yasaklayan ülkedeki ilk eyalet olmuştur. Teksas yasası, bir kişi seçim sürecinde Kişi, "bir adayı yaralamak veya seçim sonucunu etkilemek amacıyla", bir deepfake videosu "oluşturması" ve bu videonun "yayınlanmasına veya dağıtılmasına" neden olması için, ilçe hapishanesinde bir yıla kadar cezalandırılabilen ve 4.000 USD para cezası olan A Sınıfı bir kabahat haline getirmiştir (Chipman, 2021: 15).

3.2. Deepfake ve Finansal Tehlikeler

Deepfake'in büyük karışıklığa neden olabileceği tek sosyal alan elbette siyaset değildir. Bir deepfake'in içeriğine bağlı olarak, 2008 çöküşü gibi başka bir finansal kriz kolayca tetiklenebilir. Yanıltıcı veya yanlış haberler zaten borsada düşüşlere ve ani yükselmelere neden olmaktadır. Yanıltıcı bir deepfake içeriğinin, özellikle diğer piyasa haberleriyle bağlantılı olarak veya hisse senedi fiyatlarının zaten istikrarsız olduğu bir zamanda piyasaya sürüldüğünde, piyasadaki bu etkileri büyüteceği tamamen makuldur. Ayrıca terör örgütleri, sosyal medyayı bir işe alma aracı olarak yaygın şekilde kullanmaktadır. Mantıksal olarak, bu çabaların bir parçası olarak deepfake içeriklerini kullanarak ve üyelerini karşı oldukları ülkelere karşı daha da radikalleştirmek için malzemeler üretebileceklerdir. Deepfake içerikleri daha ikna edici ve gösterişli propagandaya izin verdiği için, karşı oldukları ülkelerin içinden üye alma yönündeki terörist çabalar da muhtemelen artacak ve takip edilmesi neredeyse imkânsız olabilecek yerleşik bir tehlike yaratacaktır (Dean, 2020: 24).

3.3. Deepfake, Dolandırıcılık, Fikri Hakların İhlali

Teknolojinin hızla gelişmesi beraberinde suçların da siber ortama taşınması durumunu ortaya getirmiştir. Böylelikle birçok suç tipinin işlenme oranı teknolojinin sağladığı kolaylıktan faydalanarak epey artmıştır. Tabi ki deepfake teknolojisi de bu hususta bazı suçların işlenmesinde kolaylık sağlamıştır. Yukarıda değinildiği gibi siber zorbalık, intikam pornosu gibi birçok suç bu yolla işlenebileceği gibi deepfake'in insanların gerçeklik algılarıyla kolaylıkla oynayabilmesi bu nedenle iradelerini de etkilemenin kolay olması sebebiyle dolandırıcılık suçu da bu teknolojiyle birlikte farklı bir boyut kazanabilecektir. Örneğin, The Wall Street Journal'ın haberine (www.wsj.com) göre; "dolandırıcılar Almanya merkezli bir şirketin CEO'sunun sesini yapay zeka tabanlı bir yazılımla taklit ederek kendi hesaplarına yüklü bir ödeme yapılmasını sağlamıştır. Bahse konu suçlular, Mart ayında, İngiltere'de faaliyet gösteren bir enerji şirketinin yöneticisini Almanya'daki patronunun sesini yapay zeka ile birebir kopyalayıp aramıştır. İngiltere'deki yönetici telefonda firmasının Almanya'daki büyük hissedarı olan şirketin CEO'sunun sesini duyduğu için hiçbir şeyden şüphelenmemiştir. Telefondaki ses, Macaristan'daki bir tedarikçiye acil olarak 243 bin dolar (yaklaşık 1,4 milyon TL) ödeme yapmasını istemiştir. Oluşan nakit açığı kısa sürede başka bir ödemeyle kapatılacaktır. Açığı kapatacak ödeme gelmemiştir. Bu arada dolandırıcılar yine Almanya'daki CEO gibi arayarak İngiltere'deki yöneticiden bir acil ödeme daha talep etmiştir. Bu

defa İngiltere'deki firma ödemeyi yapmamıştır. Sonunda Macaristan'a gönderilen paranın Meksika'ya ve başka yerlere gönderildiği anlaşılmıştır. Şirketin zararı sigorta firmalarınca karşılandı ancak yetkililer henüz dolandırıcıları yakalayamamıştır." Ses yoluyla yapılan dolandırıcılıklarla mücadele etmek için yazılım üreten Pindrop adlı bir siber güvenlik firması, 2013 senesinden bu zamana ses taklidi ile yapılan suçlarda yaklaşık %350 yükseliş olduğunu bildirmiştir (www.pindrop.com). Pindrop isimli firmaya göre her 638 telefon konuşmasından bir tanesinde yapay olarak oluşturulan ses kullanılmaktadır. Dolandırmak maksadı ile yapılan yanlış ödeme komutlarının önüne herhangi bir şekilde geçilebilse bile devamlı gelişen deepfake ile oluşturulan ses taklidi; kişilerin, firmaların hatta devletlerin gizli bilgilerinin ya da tehlikeli sırlarının ele geçirilmesine neden olabilmektedir (www.sabah.com.tr).

Bu anlatılanlar ışığında meydana gelebilecek tehlikelerden bir tanesi de fikri hakların ihlalidir. YouTube'da "Vocal Synthesis" adı verilen yalnızca deepfake ile üretilmiş içeriklerin paylaşıldığı bir kanal mevcuttur. Bu kanalda ünlü sesleri beklenmedik diyaloglarla eşleştiren videolar dikkat çekicidir: Bob Dylan, Britney Spears, Ayn Rand ve Slavoj Žižek, Sonny ve Cher ile düet yapmakta, Tucker Carlson Unabomber Manifesto'yu okumakta, Bill Clinton "Baby Got Back" şarkısını söylemekte ya da JFK Rick and Morty'i övmektedir. Vocal Synthesis'ün anonim yaratıcısı, Jay-Z'nin, Hamlet'ten "To Be or Not To Be" ve Billy Joel'in "We Didn't Start The Fire."'ı okuduğu deepfake ile oluşturulmuş iki videosu nedeniyle ilk kez YouTube'da bir telif hakkı talebi almıştır (ww.waxy.org).

3.4. Deepfake, İntikam Pornosu ve Siber Zorbalık

Çalışmanın giriş kısmında da bahsedildiği üzere, 2017 senesinde Reddit adlı internet sitesinde deepfake ile meşhur aktörlerin ve aktrislerin suratlarını pornografik video içeriklerine yerleştirmek niyetiyle kullanılmasıyla yapay zekâ destekli sahte porno üretme hususu ile çok karşılaşılır hale gelinmiştir. Daha fazla insan makine öğrenimini kullanarak sahte ünlü pornoları yaratmakta ve sonuçlar giderek daha inandırıcı hale gelmektedir. Hatta başka bir reddit kullanıcısı, bilgisayar bilimi geçmişi olmayan kullanıcıların yapay zekâ destekli sahte porno oluşturmasına izin vermek için özel olarak tasarlanmış bir uygulama bile oluşturmuştur. Bu videoları hazırlamak için ihtiyaç duyulan tüm araçlar ücretsizdir, kolayca elde edilebilir halde ve süreç boyunca acemileri yönlendiren talimatlarla birlikte sunulmaktadır (Cole,2021) Hollanda menşeili bir siber güvenlik girişimi olan Deeptrace'ce hazırlanıp 2019'un ekim ayında yayınlanan bir raporda, "tüm çevrimiçi *deepfake*lerin %96'sının pornografik" olduğu belirtilmektedir (Ajder vd., 2019:7). ABD'de Ulusal Savunma Yetki Yasası, ortaya çıkan bu alanda yasama yapmak için yoğun bir şekilde çalışmıştır. 2019'da iki eyalet, bazı deepfake'leri suç sayan kanunlar çıkarmıştır. ABD'de rıza dışı deepfake pornografinin dağıtımına cezai yaptırımlar uygulayan ilk eyalet Virginia olmuştur. 01.07.2019 tarihinde yürürlüğe giren yasa, rıza dışı "sahte içerikle oluşturulmuş" müstehcen/pornografik görüntülerin ve video içeriklerinin yayılmasını birinci sınıf kabahat olduğu hükmünü getirmiştir. Bu kabahatin cezasını bir yıla kadar hapis ve 2.500 USD para cezası olarak belirlemiştir (www.jdsupra.com).

Deepfake içerikleri yukarıda bahsedilmiş olan tehlikelerin dışında, siber zorbalık hususunda da epey tehlike oluşturmaktadır. Örneğin; Amerika'da Pennsylvania'daki isimsiz bir siber zorba, üçlü amigo kızı yerel takımı Victory Vipers'tan uzaklaştırmak amacı ile bir deepfake içeriği oluşturmuştur. Suç duyurusuna göre, bu deepfake içeriğinde genç kızları takımdan atılmalarına neden olabilecek uyuşturucu kullanırken, müstehcen görüntüler mevcuttur ve işbu görüntüler siber zorba tarafından kadronun koçuna gönderilmiştir. Aynı zamanda bu zorba, bir kıza "kendini öldürmelisin" şeklinde isimsiz mesajlar ve aramalarda bulunmuştur. Polis, zanlı olduğu iddia edilen kişinin kim olduğunu 2020 yılının sonlarında ortaya çıkarmıştır. Bucks İlçe Savcılığına göre zorba, kızı takımda olan bir Raffaela Spone adında bir annedir. Spone, "deepfake" videoları oluşturmak için Citron'un tanımladığı bazı araçları kullandığını söylemiştir. Spone'un Temmuz ayında ilk

hedefini taciz etmeye başladığı, deepfake yoluyla kızın çıplak bir videosunu oluşturduğu ve kendisini öldürmeye çağıran mesajlar gönderdiği iddia edilmiştir (Bellware, 2021). Bu hususta sosyal medya platformlarının hizmet sağlayıcıları ve çevrimiçi topluluklar da türlü stratejiler geliştirmektedir. Nitekim 2015 yılının mart ayında Twitter isimli sosyal medya platformu, izin olmaksızın cinsel görüntülerin paylaşımını yasaklamıştır (www.twitter.com). Google ise, mağdur bireyler için görüntülerinin Google aramalarından silinmesini isteyebilecek yeni bir bildiri sistemi getirmiştir. Microsoft da Google gibi, mağdurların rahatsız oldukları içeriğin Bing isimli arama motorundan, OneDrive ve Xbox Live bulut hizmetlerinden de sildirilmesini gerçekleştirebilecek benzer bir sistemi duyurmuştur (Abanoz, 2021).

4. DEEPFAKE VE OLASI AVANTAJLARI

Her ne kadar çalışmada ağırlıkla deepfake teknolojisinin tehlikeli boyutuna ve buna ilişkin hukuki çözüm önerilerine odaklanılsa da deepfake'in avantajları hususuna değinmekte fayda görmekteyiz. Buna göre; sayılabilecek avantajlar arasında, yeniden çekime gerek kalmadan bir video veya filmdeki diyaloğu değiştirebilme ve yalnızca sunucu menüsünden seçip senaryoyu girerek tüm videoları oluşturabilmenin yer aldığını söylemek mümkündür. Bunun yanı sıra 2019 yılında, İngiltere merkezli bir yardım kuruluşu, David Beckham'ın dokuz dilde sıtma karşıtı mesaj ilettiği bir video oluşturmak için derin sahte teknolojisini kullanmıştır (www.new18.com). Nitekim Moskova'daki araştırmacılar, Mona Lisa'yı hayata geçirmek için de deepfake teknolojisini kullanarak Mona Lisa'nın gözlerini, kafasını ve ağzını hareket ettirdiği bir video oluşturmuşlardır (www.bbc.com). Deepfake teknolojisi, sahte haberlere karşı mücadelede ciddi bir zorluk teşkil etse de bireysel izleyicilere özel olarak hazırlanmış sunucu liderliğindeki haber raporları oluşturmak için de kullanılmıştır. Ayrıca 2019'da dünyada meydana gelen pandeminin getirmiş olduğu sağlık hususundaki endişeler, video çekimlerinin insanlarla yapılması konusunu zorlaştırmıştır. Bu nedenler şirketler eğitimden reklama birçok video içeriğini deepfake teknolojisini kullanarak hazırlamışlardır. Deepfake gibi üretken teknolojinin bir dizi endüstriyi potansiyel olarak demokratikleştirebileceği de düşünülmektedir. Bu hususta deepfake teknolojisi, videolardan reklamlara ve filmlere kadar her şeyin ucuza yaratılmasını sağlayarak, bireylerin ve şirketlerin bu alanlara daha az yatırımla girmesine izin verebilir. Deepfake teknolojisini kullanan şirketler ve bireyler yüksek etik standartlarda çalışırlar ve teknolojinin zararlı kullanımları başarıyla önlenebilirse, bu teknoloji aslında çok şey vaat edebilecektir. Sentetik medya, diktatörlük ve baskıcı rejimlerde insan hakları aktivistlerinin ve gazetecilerin isimsiz kalmasına yardımcı olabilmektedir. Geleneksel veya sosyal medyadaki vahşetleri bildirmek için teknolojiyi kullanmak, yurttaş gazeteciler ve aktivistler için çok güçlendirici olabilmektedir. Böylelikle deepfake, mahremiyetlerini korumak için sesi ve yüzleri anonimleştirmek için kullanılabilmektedir (www.towardsdatascience.com). Deepfakes, bireylerin kendilerini ifade etmeleri için çevrimiçi olarak avatar deneyimleri oluşturmak için kullanılabilir. Kişisel dijital avatar özerklik verir ve bireylerin amaçlarını, fikirlerini ve inançlarını genişletmelerine ve aksi takdirde bazıları için zor olabilecek kendini ifade etmelerine yardımcı olabilir. Nitekim belirli fiziksel veya zihinsel engelleri olan kişiler, kendilerini çevrimiçi olarak ifade etmek için sentetik avatarlarını kullanabilmeleri mümkündür. (Danielle vd., 2019).

5. MEVCUT HUKUKİ DÜZENLEMELER VE HUKUKİ ÇÖZÜM ÖNERİLERİ

Çalışmada başlıklar halinde deepfake'in yaratabileceği birtakım hukuki, siyasi, sosyal tehlikelere değinilmiştir. Belirtmek isteriz ki deepfake içerikleriyle meydana gelebilecek tehlikeler yalnızca başlıklarda sayılanlardan ibaret değildir. Başlıklarda ayrıca yer verilmiş olması yalnızca bu problemlerin daha yaygın meydana gelmesi veya bu yönde yaygın bir öngörünün mevcut olmasıdır. Deepfake içerikleri birtakım sosyal, siyasal problemlerle birlikte birçok suç türünü de meydana çıkarmış ya da var olan suç tiplerinin işlenmesine kolaylık sağlayarak işlenmesini yaygınlaştırmıştır. Bu kapsamda deepfake ile meydana gelen hukuki problemlerde sunacağımız

çözüm yolları da çeşitlilik gösterecektir. Yukarıda anlatıldığı üzere uluslararası hukukta bu hususa ilişkin çalışmalar, bazı düzenlemeler mevcuttur. ABD'de Ulusal Savunma Yetki Yasası, ortaya çıkan bu alanda yasama yapmak için yoğun bir şekilde çalışmıştır. 2019'da iki eyalet, bazı deepfake'leri suç sayan kanunlar çıkarmıştır. Yine Amerika'da, 1 Eylül 2019'da Teksas, devlet görevi için adaylara zarar verme veya seçimleri etkileme amaçlı deepfake videoların oluşturulmasını ve dağıtımını yasaklayan ülkedeki ilk eyalet olmuştur.

Deepfake videolar kişilerin haysiyete zarar verme, kişilik hakkının ihlalinin yansıra özellikle deepfake ile oluşturulmuş pornografik içerikler, mağdurların psikolojik sağlığını derinden etkilemektedir. Lakin bu hususta kimin sorumlu olduğu hususunda problemler meydana gelmektedir. Açıkça, videoyu yayınlayan kişinin sorumlu olduğu düşünülmektedir. Nitekim, Türk mevzuatında da bu husus 5651 sayılı Kanun çerçevesinde ele alınmış ve "İçerik sağlayıcı, internet ortamında kullanıma sunduğu her türlü içerikten sorumludur." hükmolunmuştur. İçerik sağlayıcının sorumluluğu ise link vermek yahut çeşitli yollarla (retweet yapmak, beğenmek, alıntılamak) paylaşmış olduğu içerikler kapsamında ise daha farklı bir yorum getirilmektedir. Şöyle ki; 5651 sayılı Kanunun 4. maddesi bakımından içerik sağlayıcının, kural olarak paylaşmış olduğu başka bir kimseye ait İnternet sitesindeki içerikten sorumlu tutulması mümkün değildir. Fakat belirtmek gerekir ki içerik sağlayıcı, bağlantıyı veriş biçimiyle, paylaşmış olduğu içeriği açıkça benimsemişse ve paylaşma biçiminden, içerik sağlayıcının kendi İnternet sitesine bağlanan kişilerin ilgili bağlantıya ulaşmasını amaçladığı anlaşılıyorsa o içerikten ötürü de sorumlu tutulacaktır. (Taşkın,2016:182). Bununla birlikte, birçok İnternet sitesinin sunduğu anonimlik göz önüne alındığında, bu kişinin yerini belirlemek veya kimliğini belirlemek zor olabilmektedir. Bu nedenle, yer sağlayıcıyı, yani videonun barındırıldığı forum, site veya platformun peşinden koşmayı da düşünmek gerekmektedir. Amerika Birleşik Devletleri'nde, İletişim Ahlakı Yasası, kullanıcılarının eylemleri için bir hizmet sağlayıcıya bir sorumluluk kalkanı sağlamaktadır (Black vd., 2018:4). Almanya'da ise yer sağlayıcının hukuka aykırı içerikten dolayı sorumlu tutulabilmesi için teknik olarak bu yayını engelleyebilme olanağının varlığı gerekmektedir. (Cankat,2016; Erman, 2001:23). Singapur'da toplumsal ahlaki değerlere, siyasal istikrara, dini hoşgörüye ve toplum düzenine tahribat verici içerik hukuka aykırı içerik sayılmış olup bu tür içerikler nedeniyle yer sağlayıcının sorumluluğunun varlığı hüküm altına alınmıştır. (Cankat,2016:193). Benzer biçimde Türk mevzuatında da 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun mevcuttur. İlgili Kanun'un 6, 8, 8/A ve 9. Madde uyarınca; "kişilik hakkına açık saldırı niteliği taşıyan bu içeriğin çıkartılmasını içerik sağlayıcısına, buna ulaşamaması hâlinde yer sağlayıcısına başvurarak uyarı yöntemi ile içeriğin yayından çıkarılmasını isteyebileceği gibi doğrudan sulh ceza hâkimine başvurarak içerik veyahut yer sağlayıcı aracılığıyla sunulan içeriğe erişimin engellenmesini de isteyebilecektir" (Akkır, 2018). Tabi ki teknolojinin bu denli gelişmesi, deepfake içeriklerinin herkesin indirebileceği uygulamalar neticesinde çok büyük kitlelerin erişebileceği konumda olması nedeniyle bu hususta oluşabilecek hak ihlalleri de epey fazladır. Bu hususta Türk mevzuatında özel bir düzenleme mevcut olmasa da bu kişilik ihlaline karşın mağdur, Türk Medeni Kanunu'nun 24 ve 25. Maddesi uyarınca; "Önceden biliyor ise saldırı tehlikesinin önlenmesini, sürmekte olan saldırıya son verilmesini, sona ermiş olsa bile etkileri devam eden saldırının hukuka aykırılığının tespitini kendi yerleşim yerinde bulunan hâkimden isteyebilecektir."

Yukarıda anlatılanlar ışığında deepfake ile oluşabilecek suçlar kapsamında 5237 sayılı Türk Ceza Kanunu'ndaki düzenlemeleri ele aldığımızda ise; Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar" bölümünde yer alan 135. maddesinde *"kişisel verilerin kaydedilmesi suçu",* 136. maddesinde *"kişisel verilerin hukuka aykırı olarak verilmesi veya ele geçirilmesi suçu"* ve 138. maddesinde *"kişisel verileri yok etmeme"* eylemleri suç olarak düzenlenmiştir. Buna göre bir kişinin önceden yayınlanmış bir görüntüsü rızası olmaksızın deepfake teknolojisiyle manipüle ederek bir video içeriğine veya deepfake porno içeriğine yerleştirildiğinde; TCK m. 136 gereği "*kişisel verileri hukuka aykırı olarak verme veya ele geçirme suçu"* oluşabilecektir. Bir kişinin

rızası dışında deepfake teknolojisiyle manipüle ederek bir video içeriğine veya deepfake porno içeriğine yerleştirilmiş görüntüsü daha önce hiç yayınlanmamış bir görüntüsü ise; bu durumda TCK m. 134 gereği "*özel hayatın gizliliğini ihlal suçu"* oluşacaktır. Deepfake pornografisinde mağdur eğer çocuksa, TCK m. 226'da düzenlenen "*müstehcenlik suçu"* oluşabilecektir. Deepfake içeriğiyle bir kişiye hakaret edildiyse TCK m.125'de düzenlenen "hakaret suçu", tehdit ediliyorsa TCK m.106 "tehdit" suçu oluşabilecektir. Deepfake üreticisinin bu içeriği oluşturmak için başkasının görüntülerini bilişim sistemine hukuka aykırı biçimde girdiyse TCK m.243 suçu oluşabilecektir. Tüm bu anlatılanların yanısıra bir kişinin rızası bulunmaksızın gerçek bir görüntünün paylaşılması ile deepfake teknolojisi ile manipüle edilmiş gerçek dışı bir fotoğrafın paylaşılması arasında oldukça büyük bir fark bulunmaktadır. Bu nedenle yasa koyucunun, bu iki ihlal çeşidini arasındaki farkı dikkate alarak deepfake ile meydana getirelecek sahte videolar hususunda ayrı bir düzenleme getirmesi yerinde olacaktır. Kişinin rızası dışında bir pornografik içeriğin paylaşmasına ilişkin ayrı bir düzenleme olmadığı gibi bu içeriğin deepfake ile üretilmesiyle oluşması da ayrı bir düzenlemeye tabi tutulmamıştır. Lakin kanımızca her iki husus için ayrı ayrı düzenleme getirimesi yerinde olacaktır. Çünkü söz konusu eylemler mağdur üzerinde çok yıkıcı etkilere sebep olabilmektedir.

Ceza kanunlarındaki düzenlemeleri ele aldıktan sonra çalışmanın devamında deepfake'in fikri haklar bakımından yarattığı sorunlara ve çözümlerine yer verilecektir. Buna göre Aralık 2019'a ait Dünya Fikri Mülkiyet Örgütü ("WIPO") 'nün "Fikri Mülkiyet Politikası ve Yapay Zeka Hakkında Sorunlar Taslak Bildirisi" nde deepfake'in fikri haklar bakımından yarattığı sorunlara yer verilmiştir. Deepfake'i özelinde ele alınan iki soru şunlardır:

"(i) *Deepfake'ler telif hakkının konusunu oluşturan veriler esas alınarak meydana getirildiğine göre, bu deepfake'lere ilişkin telif hakkı kime ait olmalıdır?*

(ii) *Deepfake içeriğine konu olan kişilerin ücret talep etme hakkı doğacak mıdır?"*

WIPO, deepfake'in yol açabileceği başkaca sorunlara kıyasla örneğin; kişilik haklarına saldırı, özel hayatın gizliliğinin ihlali, kişisel verilerin ihlalleri vb. telif hakkı sorunun çok daha önemli olduğunu ifade etmiştir. Bu kapsamda WIPO asıl problemin "*Deepfake içerikleri telif hakkı ile koruma altına alınmalı mıdır?*" olması gerektiğini açıklamıştır. Deepfake içeriklerinin kaynak kişinin yaşamıyla ve statüsüyle tamamen alakasız bir şekilde oluşturulabileceğine değinen WIPO, bu tür içeriklerin telif hakkı ile ödüllendirilmemesi gerektiğine dikkat çekmektedir. Öte yandan WIPO mevcut soruları ise şu şekilde cevaplamıştır:

"*Deepfake onu oluşturan kişinin çalışmalarından meydan gelmektedir. Meydana gelen deepfake içeriğinde görüntüsü, sesi veya başkaca bir özelliği kullanılan kaynak kişinin hiçbir müdahalesi olmamaktadır. Verileri kullanılan kişinin meydana gelen içerikteki tek etkisi yapılan işleme onay vermekten öte değildir.*"

WIPO, deepfake'e ilişkin telif haklarının bunları oluşturan kişilere ait olması gerektiği üstünde durmaktadır. "Yaratma Gerçeği İlkesi" eser sahibi eseri meydana getiren kişidir anlamına gelen ilkedir ve WIPO'nun bu görüşü bu ilke ile de uyumludur. Görüleceği üzere deepfake içeriğine konu olan kişiler telif hakkına sahip olmadıkları ileri sürülmektedir. Bu nedenle telif hakkı deepfake'e karşı ileri sürülebilmek pek de doğru bir yol olarak gözükmemektedir. Diğer yandan deepfake'lerin sabit görüntülerin kırpılması ve algoritmik kombinasyonundan oluştuğu düşünüldüğünde Anglosakson hukuk düzeninde uygulama alanı bulan "Adil Kullanım" (Bektaş,2021) doktrini, deepfake'lere karşı telif hakkı temelli eylemlerin çoğunun önünde önemli bir engel olabilmektedir. WIPO'nun deepfake'e ilişkin verdiği örnekler de oldukça aydınlatıcıdır. Bir örneğe göre, görsel/işitsel yapımcı vefat eden bir aktöre filmde yer vermek üzere bir yapay zekâ üretir. WIPO, vefat eden kişinin yer aldığı yapay zekâ tarafından oluşturulan deepfake'e ilişkin telif haklarının yapımcıya verilebileceğini ifade etmiştir. Öte taraftan, söz konusu deepfake ticari olarak temin edilmiş bir yapay zekâ algoritması tarafından da üretilebilir. WIPO bu durumu fotoğrafçının

fotoğraf makinesini temin etmesine benzetmiştir. Şöyle ki, Fikir ve Sanat Eserleri Kanunu'na göre fotoğraf "güzel sanat eseri" olarak kabul edilmiştir. Fotoğrafçlara ilişkin telif hakkı deklanşöre basılarak, görüntünün filme yerleştirildiği an başlar ve başka hiçbir işleme gerek kalmaksızın kendiliğinden kazanılır. Bu doğrultuda, çekilen fotoğrafa ilişkin telif hakkı da makinenin sahibinde değil, fotoğrafı çeken kişide olacaktır. Dolayısıyla oluşturulan deepfake'e ilişkin telif haklarının, yapay zekayı üreten kişide değil; yapay zekayı kullanarak deepfake'i (eseri) meydana getiren kişide olduğunu söylemek mümkündür (Schmidt,2021). Bunun yanısıra rızası dışı görüntüleri deepfake içeriğinde kullanılan kişiler 5846 Sayılı Fikir ve Sanat Eserleri Kanunu'nun 84. Maddesindeki *"Bir işareti, resim veya sesi, bunları nakle yarıyan bir alet üzerine tesbit eden veya ticari maksatlarla haklı olarak çoğaltan yahut yayan kimse, aynı işaretin, resmin veya sesin 3.üncü bir kişi tarafından aynı vasıtadan faydalanılmak suretiyle çoğaltılmasını veya yayımlanmasını menedebilir. Tevacüz eden tacir olmasa bile birinci fıkra hükmüne aykırı hareket edenler hakkında haksız rekabete mütaallik hükümler uygulanır. Eser mahiyetinde olmayan her nevi fotoğraflar, benzer usullerle tesbit edilen resimler ve sinema mahsulleri hakkında da bu madde hükmü uygulanır."* hüküm uyarınca kişiye ait olan resmin kullanılması ve çoğaltılması yoluyla elde edilen bu içeriklerin yayınlanmasının men edilmesini isteyebilecektir. Bu şekilde aslında rızası olmaksızın kendi sesi veya görüntüsü kullanılmasıyla sahte içeriklere konu olan mağdur bu düzenlemeye başvurabilecektir.

SONUÇ VE TARTIŞMA

Deepfake ve ilgili teknoloji dünyası hızlı bir şekilde büyümekteyken bu teknolojiyi herkesin kullanabileceği uygulamaların ortaya çıkması, yepyeni olası suistimaller dünyasının kapılarını açmaktadır. Çalışmada da değinildiği üzere siyasetten ekonomiye, kişilerin farklı biçimde mağduriyetlerine yol açabilecek sorunlar ortaya çıkması muhtemel gözükmektedir. Bu sorunlar yapay zeka teknolojisinin gelişmesiyle elbette daha yaygın hale gelecektir. Sahte haber içerikleriyle siyasi propagandalar yapılması, seçimlerin, borsanın manipüle edilebilmesi söz konusu olacaktır. Aynı zamanda bu içeriklerle hakaret, tehdit, kişilik haklarının ihlali, dolandırıcılık gibi bir çok suç unsuru oluşabilecektir. Rahatlıkla söyleyebilmek mümkündür ki, deepfake çok sayıda hak ihlaline sebep olmaktadır ve olmaya da devam edecektir. Bu kapsamda deepfake ile yaşanabilecek hak ihlallerinin her birinin ayrı ayrı özenle değerlendirilmesi gerekmekte ve bazı hukuki ihlallere ayrıca hukuki düzenlemeler getirilmesi gerektiği önerilmektedir. Bunlardan birisi kişinin rıza dışı görüntülerinin alınarak pornografik içeriklere monte edilmek suretiyle sahte içerik üretilmesi işlemidir. Yasa koyucunun bu anlamda çalışmada yer verilen diğer ülkelerde olduğu gibi ayrı bir düzenleme getirmesi isabetli olacaktır. Bununla birlikte, yasal çözümler tek çözüm değildir. Bu nedenle, diğer pratik çözümler de kullanılmalıdır. Nitekim çalışmada değinildiği üzere deepfake kullanımın avantajlı yönleri de mevcuttur. Bu nedenle deepfake içeriklerinden kaynaklanabilecek suistimaller hukuki ve sosyal çözüm yöntemleriyle engellendikçe bu teknolojiden sanat, eğitim, sosyal anlamda birçok fayda sağlamamız mümkün olacaktır. Bu bağlamda zararlı deepfake içeriklerine yönelik alternatif çözümler arasında, zararlı deepfake videoları yasaklamak için İnternet platformlarının politikalar oluşturması ve bu tür videoları algılamak, işaretlemek ve kaldırmak için daha iyi mekanizmalar oluşturması yer almaktadır. Günümüzde teknolojilerin hızı dikkate alındığında, bu hususta ivedilikle çalışmalar yapılmalı ve gerekli düzenlemeler getirilmesi gerektiği kanaatindeyiz.

Kaynakça

Abanoz, B. (2021). Deepfake İkilemi: Sadece Eğlence mi? Tehditler ve Hukuki Tartışmalar. https://www.academia.edu/45712376/Deepfake_%C4%B0kilemi_Sadece_Eglence_mi_Tehditler_ve_Hukuki_Tart%C4%B1%C5%9Fmalar (E.T.:30.12.2022)

Akkır, Y. (2018). Bir Bilişim Suçu "Deepfake. MGC Legal. https://www.mgc.com.tr/bir- bilisim-sucu-deepfake, (E.T.: 14.11.2021)

Anadolu Ajansı (2019). Deepfake videoları demokrasileri tehdit ediyor. https://www.ntv.com.tr/teknoloji/deepfake-videolari-demokrasileri-tehdit-ediyor,7Y_WMt5iZkicDkFRKSlO8A (E.T.:16.11.2021)

Ajder, H., Patrini, G., Cavalli, F. & Cullen, L. (2019). The state of deepfakes: Landscape, threats, and impact. *Deeptrace*, 27.

Baio, A. (2020). With questionable copyright claim, Jay-Z orders deepfake audio parodies off YouTube https://waxy.org/2020/04/jay-z-orders-deepfake-audio-parodies-off-youtube/ (E.T.:30.12.2022)

Baker, J. (2019). Deepfakes Could Break The Internet. https://www.cpomagazine.com/cyber-security/deepfakes-could-break-the-internet/ (E.T.: 14.11.2021)

BBC News (2019). Mona Lisa 'brought to life' with deepfake AI https://www.bbc.com/news/technology-48395521 (E.T.:18.11.2021)

Bektaş, E. (2021). Google v Oracle; Yazılımların Telifinde Adil Kullanım (2. Bölüm). https://iprgezgini.org/category/telif-haklari/

Bellware, K. (2021). Cheer mom used deepfake nudes and threats to harrass daughter's temmates, police say. The Washington Post. https://www.washingtonpost.com/nation/2021/03/13/cheer-mom-deepfake-teammates/ (E.T.: 19.11.2021)

Berk, M.E. (2020). Dijital Çağın Yeni Tehlikesi "Deepfake". *OPUS–Uluslararası Toplum Araştırmaları Dergisi,* 16(28), 1508-1523.

Black, R., Tseng, P. & Wong, S. (2018). What can the law do about 'Deepfake'?. *McMillan Litigation and Intellectual Property Bulletin.*

Cole, S. (2021). We Are Truly Fucked: Everyone Is Making AI-Generated Fake Porn Now. https://www.vice.com/en/article/bjye8a/reddit-fake-porn-app-daisy-ridley (E.T.:19.11.2021)

Çolak, B. (2021). Legal Issues of Deepfakes. Institute for Internet and the Just Society. https://www.internetjustsociety.org/legal-issues-of-deepfakes (E.T.:18.11.2021)

Chesney, B., & Citron, D. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. *Calif. L. Rev.*, *107*, 1753.

Dean, A. (2020). Deepfakes, Pose Detection, and the Death of "Seeing is Believing" https://www.lawtechnologytoday.org/2020/08/deepfakes-pose-detection-and-the-death-of-seeing-is-believing (E.T.:18.11.2021)

Debusmann, B.J. (2021). Deepfake teknolojisi: 'İçerik üretiminin geleceği' neden bu kadar tartışma yaratıyor? https://www.bbc.com/turkce/haberler-dunya-56324776 (E.T.:14.11.2021)

Farid, H., Hwang T., Lyu S. & Zucconi A. (2019). Deepfakes and Audio-visual Disinformation, *Centre for Data Ethics and Innovation (CDEI).*

Ferraro, M.F., Chipman, J. C. & Preston, S.W. (2020). The Federal" Deepfakes" Law. *The Journal of Robotics, Artificial Intelligence & Law, 3*.

Gerstner, E. (2020). Face/off: "deepfake" face swaps and privacy laws. *Defense Counsel Journal, 87(1),* 1-14.s.2

Google, LLC v. Oracle America, 18–956 (U.S. Sup. Ct.2021) https://www.supremecourt.gov/opinions/20pdf/18-956_d18f.pdf (E.T.:17.11.2021)

Görür, S. (2021). Deepfake teknolojisi, dijital çağın yeni tehlikesi mi? - Prof. Dr. Cem Say ve Av. Gökhan Ahi ile söyleşi https://medyascope.tv/2021/03/12/deepfake-teknolojisi-dijital-cagin-yeni-tehlikesi-mi-prof- dr-cem-say-ve-av-gokhan-ahi-ile-soylesi-bu-konu-hukuktan-once-etik-konusu-tum- paydaslarin-etik-konusunda-girisimlerde-bulunm/ (E.T.:14.11.2021)

Hall, H. K. (2018). Deepfake videos: When seeing isn't believing. *Cath. UJL & Tech*, *27*, 51.

Hao, K. (2021). Deepfake porn is ruining women's lives. Now the law may finally ban it. https://www.technologyreview.com/2021/02/12/1018222/deepfake-revenge-porn-coming-ban/ (E.T.:16.11.2021)

Jaiman, A. (2020). Positive Use Cases of Synthetic Media (aka Deepfakes) https://towardsdatascience.com/positive-use-cases-of-deepfakes-49f510056387 (E.T.:18.11.2021)

Supra, J.D. (2019). First Federal Legislation on Deepfakes Signed Into Law https://www.jdsupra.com/legalnews/first-federal-legislation-on-deepfakes-42346/ (E.T.:30.12.2022)

New18 (2019). David Beckham 'Speaks' in Nine Languages, Using Deepfake Tech, in Call to End Malaria https://www.news18.com/news/buzz/david-beckham-speaks-nine-languages-using-deepfake- tech-in-call-to-end-malaria-2096187.html (E.T.:18.11.2021)

Sabah Gazetesi (2019). CEO'nun sesini yapay zekayla taklit ettiler, 1,4 milyon TL çaldılar https://www.sabah.com.tr/ekonomi/2019/09/03/ceonun-sesini-yapay-zekayla-taklit-ettiler-14- milyon-tl-caldilar (E.T.:18.11.2021)

Schmidt, N. (2019). Privacy law and resolving 'deepfakes' Online. https://iapp.org/news/a/privacy-law-and-resolving-deepfakes-online/ (E.T.:30.12.2022)

Seshadri, N. (2019). Implications of Deepfakes on Copyright Law. https://www.wipo.int/export/sites/www/about-ip/en/artificial_intelligence/conversation_ip_ai/pdf/ind_seshadri.pdf (E.T.:30.12.2022)

Taşkın, Ş.C. (2016). *İnternete Erişim Yasakları.* Birinci Baskı, Ankara: Seçkin Yayınları

Twitter (2022). Twitter Kuralları ve Hizmet Şartları ihlallerini bildirme. https://help.twitter.com/tr/rules-and-policies/twitter-report-violation, (E.T.:19.11.2021)

Yıldırım, A. & Aydınlı, C. (2019). Deepfake: An Assessment From The Perspective Of Data Protection Rules. https://www.mondaq.com/turkey/privacy-protection/863064/deepfake-an- (E.T.: 30.12.2022)

WIPO (2021). Impact of Artificial Intelligence on Intellectual Property Policy: Call for Comments. https://www.wipo.int/export/sites/www/about-ip/en/artificial_intelligence/call_for_comments/pdf/ind_lacasa.pdf (E.T.:16.11.2021)

5237 sayılı Türk Ceza Kanunu

5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun

5846 Sayılı Fikir ve Sanat Eserleri Kanun