

DeepFake Teknolojisi ve Dezenformasyonda Kullanılabilecek Zararlı Yapısı Hakkında Araştırma ile Hukuki D zenleme Gereksinimleri

Engin DİNÇ

USMED AR-GE BAŐKANI

03.08.2021

GiriŐ

Dijital d nyanın hayatımıza girmesiyle birlikte, yalan ve algı y netimi kavramları da eŐitlilik kazanmıŐtır. Yazı, video, g rsel ve ses  zerinde yapılan deĐiŐikliklerin yanı sıra bu deĐiŐiklikleri daha gereki g stermek amacıyla yapay g r nt ler de  retilmeye baŐladı.

 lkelerin birbirlerine karŐı yaptıkları siber espionaj alıŐması neticesinde ortaya ıkan bireysel ve toplumsal kimlikler, toplumların zafiyetlerini ve bireylerin hassas noktalarını g stermektedir. Bu bilgilerin elde edilmesinden sonra istihbarat teŐkilatları, diĐer  lkeler  zerinde yıpratma operasyonlarına baŐladı. Bu alıŐmalar ok eŐitli Őekilde yapılırken; en  nemli alıŐma medya kanallarıyla dezenformasyon alıŐmasıdır. Dezenformasyon alıŐmasında ortaya atılan yalanın inandırıcılıĐının arttırılması iin yalan, Őiddetli, ok kiŐi tarafından, s rekli s ylenmektedir. Bunun da yeterli olmadığı zaman da iŐin ierisine montajlanmış belgeler, video ve ses kayıtları girmektedir. Fakat geliŐen teknoloji ile bunların sahte olduĐunun ortaya ıkması uzun s rm yor. İŐte bunun  zerine devreye bilgisayar zekası ile yapılmıŐ g r nt ler girmiŐtir. Bu makalede, DeepFake teknolojisini ve bu teknolojinin kullanılabileceĐi zararlı alanlar ile yapılması gereken hukuki alıŐmaları ele alacaĐız.

DeepFake¹

T rke karŐılıĐı Deri  Đrenme olan DeepFake, mevcut ve gerek bir g r nt de veya videoda yer alan kiŐinin yapay sinir aĐları kullanılarak baŐka bir kiŐinin g r nt s  ile deĐiŐtirilmesi ile ortaya ıkan kurgusal ve montaj bir g r nt  t r d r. Sıklıkla, otomatik kodlayıcılar ve  retken ekiŐmeli aĐlar (GAN'lar) olarak bilinen makine  Đrenme tekniklerini kullanarak mevcut medyanın kaynak medya  zerinde birleŐtirilmesi ve  st  ste konması ile

¹ Wikipedia: <https://tr.wikipedia.org/wiki/Deepfake>

üretirler.^{2 3} Deepfake ilk olarak 2017 yılında karşımıza çıktı. Amerikan sosyal medya sitesi Reddit’de, anonim bir kullanıcı bazı ünlülerin yer aldığı yetişkin içerikli videolar yayınladı. Fakat yayınlanan bu videolar, içinde yer alan ünlülere ait değildi. Bu videolar ünlülerin yüzlerinin başka bedenlere Deepfake teknolojisi ile yerleştirilmesi sonucu oluşmuştu.

Yapay Zekâ (AI⁴) olarak tanımlanan teknoloji ile yapılan DeepFake görüntülerin üretilmesi son derece kolay ve ucuzdur. Sıradan bir bilgisayar kullanıcısı veya mobil uygulama kullanıcı da bu görüntüleri üretebilir. Üretilen görüntülerin profesyonel video montaj teknikleriyle düzenlenmesi, temizlenmesi ve hassasiyetinin artırılması ile gerçekçi görüntünün elde edilme oranı daha fazla olacaktır. DeepFake özellikle iki şekilde yapılmaktadır. Bunlar; yüz değiştirme ve yüz manipülasyonudur.

Yüz Değiştirme

DeepFake teknolojisi kullanılarak bir kişinin tüm yüz hattının farklı bir kişiye nakledilmesi durumudur. Birinci kişinin yüzünün ana çerçevesi dairesel olarak alınarak ikinci kişinin yüz kısmına dairesel olarak aktarılır. Bu durumda kişinin saçları ve genelde kulakları nakil olmamakta, sadece yüz kısmı nakledilmektedir. Ayrıca uzun yüzlü bir kişinin yüzünün yuvarlak yüzlü bir kişiye aktarılmış olması durumunda yapılan montaj olduğu kolaylıkla görülebilmektedir. Aynı şekilde mimiklerinin farklı olması, ten rengindeki uyumsuzluk gibi birçok etkene dikkat edilmesi halinde videonun sahte olduğu anlamak mümkündür.

Bu teknik özellikle kişileri başka ortamlarda göstermek amacıyla kullanılmaktadır. Örneğin; dine ve ahlaka uymayan davranışlar sergileyen bir adamın yüzüne dini bir liderin yüzünün eklenmesiyle dini lider, ahlaksızca davranışlar sergiliyormuş gibi gösterilebilir. Bu teknik DeepFake’in en kolay ayırt edilebilen ve montaj olduğu anlaşılan yöntemidir. Fakat yeni bir teknoloji olması dolayısıyla inanacak insan sayısı da pek hayli fazladır.

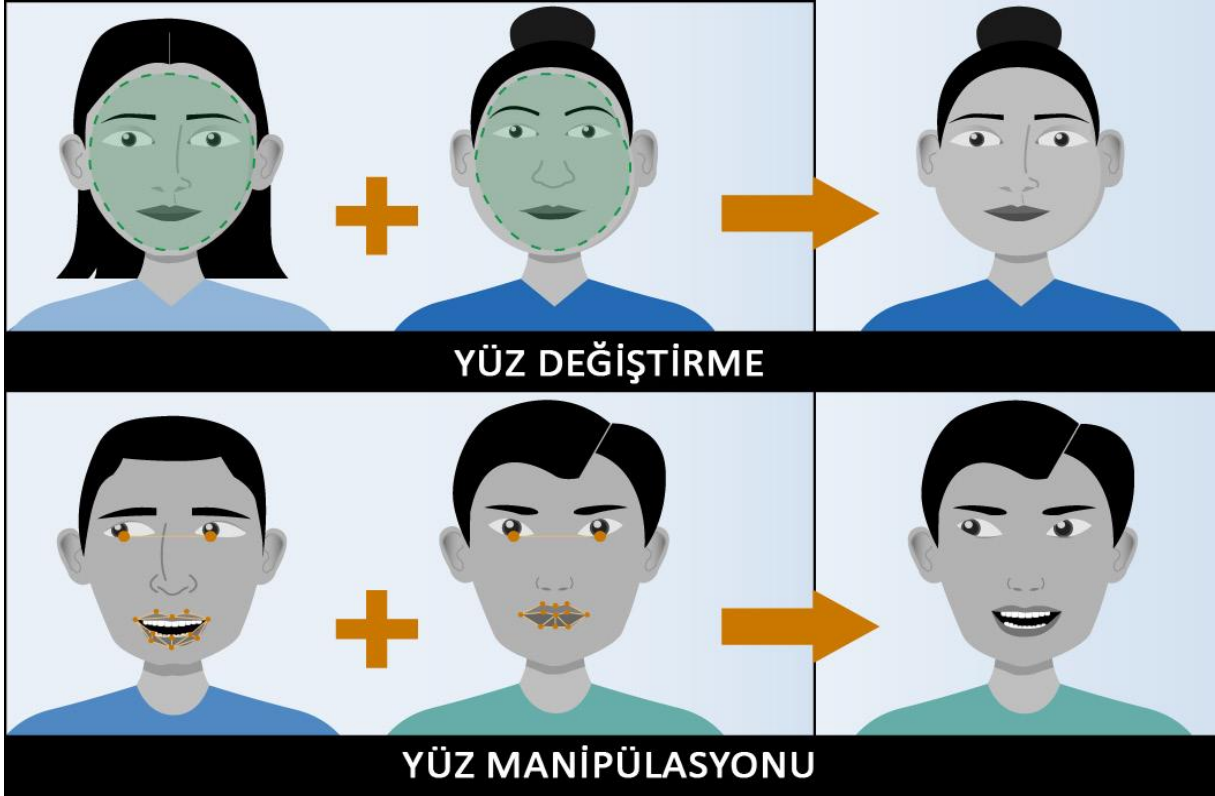
Yüz değiştirme yöntemi daha kolay ve anlaşılır olsa da günümüzde ikinci yöntem olan Yüz Manipülasyonu daha fazla kullanılmakta, DeepFake’i eğlenceli olmanın dışarısına da bu çıkartmaktadır. Öyle ki Amerika Birleşik Devletleri’nde 2016 yılında yapılan başkanlık

² Schwartz, Oscar (12 Kasım 2018). "You thought fake news was bad? Deep fakes are where truth goes to die". The Guardian (İngilizce).

³ PhD, Sven Charleer (17 Mayıs 2019). "Family fun with deepfakes. Or how I got my wife onto the Tonight Show". Medium (İngilizce).

⁴ AI: Artificial Intelligence

seimlerinde aday olan Cumhuriyeti Senatör Marco Rubio'ya gre bu teknoloji nkleer silahların modern bir eŐdeęeridir.



Yüz Manipülasyonu

Bu yöntemde de bir yüz nakli bulunmaktadır fakat burada yüzü deęiŐtirilen kurbanın kendisidir. Doęal kıyafet ve ortamındaki kiŐinin yüzü deęil, yüz ifadeleri deęiŐtirilmektedir. KiŐinin söz, ağız hareketleri, jest ve mimikleri deęiŐtirilerek söyledięinden farklı bir ifade konuŐturulabilir. Bu konuda Washington Üniversitesi'ndeki araŐtırmacılar tarafından Amerika BirleŐik Devletleri eski BaŐkanı Barack Obama'ya yapılan ve Amerika BirleŐik Devletleri BaŐkanı Donald Trump hakkında gerekte söylemedięi ifadeler ieren video rnek gsterilebilir.⁵

⁵ Kaynak: <https://www.youtube.com/watch?v=cQ54GDm1eL0>



You Won't Believe What Obama Says In This Video!

Söz konusu video da Amerika Birleşik Devletleri eski Başkanı Barack Obama'ya ait olan bir konuşma videosunun üzerine farklı bir kişinin konuşması eklenmiş, yüz ifadeleri tamamen Barack Obama'ya ait gibi gösterilmiştir. Oysa Barack Obama'yı konuşturan adamın Obama ile uzaktan yakından benzerliği de yoktur. Bu bakımdan DeepFake'i yapabilmek için kullanılan sahte görüntünün hedef kişiye benzemesi de gerekmez. Aynı durum Morgan Freeman'ın görüntüsü kullanılarak yapılan DeepFake için de geçerlidir.



Yukarıdaki görselde gördüğünüz Amerika Birleşik Devletleri oyuncularından Morgan Freeman değil, onun DeepFake ile yapılmış bir kopyası. Youtube Diep Nep kanalında yayınlanan 1:03 dakikalık bu videoda gerçekte konuşan kişi alttaki görselde fakat Deep Fake teknolojisi ile onun görüntüsü, mimikleri, ağız ve göz hareketleri tam ve gözle fark edilmeyecek şekilde Morgan Freeman'a yerleştirilmiş. Eğer söz konusu videoda iki görüntü alt alta verilip yapılanın DeepFake olduğu açıklanmamış olsaydı bunu izleyen herkesin konuşanın Morgan Freeman'ın kendisi olduğuna inanması kesindi.

Örneklerle DeepFake teknolojisinin işini yapmada ne kadar başarılı olduğunu görmemizin yanında, kötü niyetli kişilerce kullanıldığında ne kadar tehlikeli olduğunu da görmüş oluyoruz.

DeepFake İle Dezenformasyon İlişkisi

Ülkelerin iç işlerine karışmak, devlet ile vatandaş arasındaki bağları kopartmak ve siyasi emelleri gerçekleştirmek amacıyla çoğu zaman dezenformasyon çalışmalarına şahit olduk. Özellikle sosyal medya ağları üzerinden yapılan bu çalışmalarda fonlu medya kuruluşlarının ürettiği ve piyasaya sürdüğü, gerçekte uzaktan yakından ilgisi olmayan veya asıl içeriği tamamen çarpıtılmış haberler ile halk kandırılmaktadır.

Yalan içerik üretenlerin yapacağı DeepFake videoların gerçekliğinin tespit edilmesi de bir o kadar zordur. Bunun yanında yapılan diğer bir yıpratma türü de itibarsızlaştırmadır. Yalan, montaj, sahte belge gibi içeriklerle yapılan haberlerin doğrusu ortaya çıkartılıp "Montaj bu haber" denilir fakat bu süreklilik arz etmeye başlayınca, dezenformasyonu başlatanlar tarafından "Hepsi mi montaj?" denilerek itibarsızlaştırma yapılmaktadır. Bu nedenle bu tarz içerikler bir defa üretilip piyasaya sürüldüğünde ciddi, sert ve ağır yaptırımlar uygulanarak devamı kesilmelidir.

⁶ Kaynak: <https://www.youtube.com/watch?v=F4G6GNFz0O8>

Türkiye'ye Karşı Yapılan Dezenformasyon ve DeepFake

Ülkemize, Gezi Parkı olaylarıyla başlayıp artarak devam eden çok sayıda siber dezenformasyon çalışması yapılmış, yapılmaya da devam etmektedir. Bu çalışmaların en büyüğü de 1-2 Ağustos 2021 tarihlerinde Twitter ve Instagram sosyal medya ağlarında yoğun olarak görülen #HelpTurkey etiketi ile yapılandır. Türkiye'nin birçok bölgesinde çıkan orman yangınları sonucu yayılan; uçakların yetersizliği, hükümetin yeteri kadar söndürme çalışması yapmadığı yalanı Twitter ve Instagram başta olmak üzere birçok sosyal medya ağı üzerinden yayılmış, #HelpTurkey etiketi kullanılarak Birleşmiş Milletler'in Türkiye'ye yardım etmesi talep edilmiştir. Kısa bir sürede 3 milyondan fazla tweet atılmasından sonra içerikler değişmeye başlamış, Birleşmiş Milletler'in yardıma değil; ülkeye askeri müdahale için gelmesi gerektiği vurgulanmıştır.

Bu ve benzeri dezenformasyon çalışmalarında ortaya atılan yalanın güçlendirilmesi, inandırıcılığının arttırılması amacıyla DeepFake videoların da üretilmesine başlanmıştır. Bu içeriklerin üretilmesi, yayılması ve halk tarafından da gerçekliğinin teyit edilmemesi çok ağır ve yıkıcı sonuçlar doğurabilir. Neler olabileceğini örneklerle ele alalım.

Sayın Cumhurbaşkanımız Recep Tayyip Erdoğan'ın bakanları ve bürokratları ile oturduğu samimi bir ortamda; *"2023 seçimlerinden de zaferle çıktıktan sonra Anayasa değişikliği yapacağız, hilafeti ilan edecek ve hoca efendiyi de getirip elini öpüp, özür dileyip halife yapacağız"* dediği bir videonun üretilip servis edildiğini düşünelim. 2023 seçimlerini manipüle etmek isteyen, ülkemiz üzerinde karanlık emelleri olan veya siyasi otoriteyi ele almak isteyenlerin başvurabileceği bu yöntem ne kadar ses getirir? Halkımız göreceği bu videodan nasıl etkilenir, gerçek olmadığını kısa bir sürede ispat edilmemesi ne gibi sonuçları doğurur? Gerçek olmadığı ispat edilmiş olsa dahi, itibarsızlaştırma çalışmaları sonucunda yayılan bu videonun sahte olduğuna halkımız ne kadar itibar eder?

Yine aynı şekilde, bakanlardan bir tanesinin farklı bir ortamda, Sayın Cumhurbaşkanımızı kast ederek; *"Beyefendi 'seçimden sonra bir şekilde APO'yu salalım, sınır ötesi operasyon yaptığımız yerde Türkiye'ye bağlı bir Kürt Devleti kurulsun' dedi"* dediğini düşünelim.

Üretilmiş bu DeepFake içeriklerle ilgili doğrulama çalışması yapılırken, yurtdışı kaynaklı, bilindik bir doğrulama kuruluşu tarafından yapılan videonun sahte olmadığına ilişkin bir rapor yayınlanması da ne kadar yıpratıcı olur?

Dezenformasyon planlaması yapanlar sadece yalanı üretmekle, gazeteciyi satın almakla kalmıyor, güvenilir doğrulayıcıları da satın alarak teyitleri de kendi istedikleri gibi yapıyorlar. Ayrıca devletin içerisinde görev almış kişileri de tehdit, şantajla veya farklı metotlarla yalana ortak olmaya alet edebilirler. Bu bakımlardan DeepFake başta olmak üzere montaj içerikler ile ilgili yasal düzenleme yapılması mutlak gerekliliktir.

DeepFake Yasal Düzenleme Gereksinimleri

DeepFake hayatımıza 2017 yılında bir Reddit kullanıcısının paylaşımıyla girmiştir. Ocak 2019 tarihinde Amerikan Senatosu bu konuda tedbir alınması yönünde yasal çalışma yapmıştır.⁷ Birçok ülkede sahte içeriklerle yapılacak yıpratma çalışmaları yasaklanmış, ağır cezalar getirilmiştir. Ülkemizde yürürlükte olan 5237 sayılı Türk Ceza Kanunu'nda (TCK) buna ilişkin bir düzenleme yoktur. Yani ülkemizde; sahte video veya haber üretilip yayılması suç sayılmamaktadır.

Dünya Fikri Mülkiyet Örgütü (WIPO⁸) tarafından Aralık 2019 tarihinde yayınlanan “Fikri Mülkiyet Politikası ve Yapay Zekâ Sorunları Üzerine Çalışma”⁹ belgesinde DeepFake ile üretilen içeriklere yönelik sorunlara değinilmiştir. Burada en önemli vurgu ise, DeepFake mağduru olan kişinin yayınlanan videoda telif hakkı sahibi olmadığı dolayısıyla telif hakları yasasının bu durumda geçerli olamayacağıdır. Fakat yine aynı belgede Avrupa Birliği Genel Veri Koruma Yönetmeliği'nin¹⁰ 5. maddesine atıf yapılarak söz konusu DeepFake içeriğin Kişisel Verilerin Korunmasına muhalefet olacağı kabul edilebileceği bildirilmiştir.

Ülkemizde ise, DeepFake gibi içeriklerde kişinin izni olmaksızın görüntüsü kullanıldığı için 6698 sayılı Kişisel Verilerin Korunması Kanununa veya TCK'nın “Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar” bölümüne atıf yapılabilmekte ve buna ilişkin cezai işlem uygulanmaktadır. Fakat verilen cezaların da büyük çoğunluğu Hükümün Açıklanmasının Geri Bırakılması (HAGB) hükümlerine tabi olduğundan suçlu herhangi bir ceza çekmeden bu durumdan kurtulabilmektedir.

⁷ Kaynak: <https://www.congress.gov/116/bills/s2065/BILLS-116s2065rs.pdf>

⁸ WIPO: World Intellectual Property Organization

⁹ Kaynak: https://www.wipo.int/export/sites/www/about-ip/en/artificial_intelligence/call_for_comments/pdf/ind_lacasa.pdf

¹⁰ Kaynak: <https://iapp.org/resources/article/the-eu-general-data-protection-regulation/#A4>

Dünyanın birçok ülkesinde özellikle kadın ünlüler için DeepFake kullanılarak üretilen pornografik görüntüler dava konusu edilmiş, bakılan davalar Kişisel Verilerin Korunması Kanunu kapsamında ele alınmış, cezalar da bu yönde verilmiştir. Fakat DeepFake sadece kişisel veri ihlali için kullanılan bir yöntem değil, T.C. Anayasasının 26. maddesinde yer verilen “Haber alma hürriyeti” ilkesine de aykırılık barındırmaktadır.

Sonuç

Toplumun her bireyi doğru ve güvenilir haber alma hürriyetine sahiptir. Fakat DeepFake ile yapılan içeriklerin sahte olması, bu yöntemle yapılmış haberlerin gerçeği yansıtmaması kişilerin haber alma hürriyetinin de gasp edildiği anlamına gelmelidir. Bu bakımdan, basın yayın kuruluşları, internet gazeteciliği, sosyal medya haberciliği, haber doğrulama ve teyitçilik gibi kişilere haber ve bilgi veren her türlü platformda bilgilerin doğruluğu ön planda tutulmalı, kasıtlı olarak yalan haber yapanlar hakkında işlem yapılması için özel yasal çalışma yapılmalıdır.

Özellikle yurtiçinden dezenformasyona destek veren medya kuruluşlarının T.C. Anayasasının 32. maddesine yer alan “Düzeltilme ve Cevap Hakkı”ndan faydalandığı görülmektedir. Fakat bu maddenin kapsamına da sınırlandırılma getirilerek sürekli ve kasıtlı olarak yalan haber yapıp Anayasa güvencesi arkasına sığınan basın-yayın kuruluşlarına cezai işlemler uygulanmalıdır.

Yapılması gereken bu yasal çalışmada cezalar kati, sert ve ağır olmalıdır. Aksi halde yalan ve dezenformasyonun önüne geçilemeyecek, devamlılık hâsıl olacak ve dezenformasyon yapanlar tarafından itibarsızlaştırma politikası da kullanılarak istenilen kötü amaca ulaşılabacaktır.