DEEPFAKE'İN CEZA HUKUKU BAKIMINDAN DEĞERLENDİRİLMESİ VE DE LEGE FERENDA ÖNERİLER

Beşir BABAYİĞİT*

ÖZ

"Deepfake", eldeki verilerden derin öğrenme tekniği kullanılarak, gerçek olmamasına rağmen gerçeğe çok yakın görüntü, video ve ses biçimindeki içeriklerin üretilmesi faaliyeti ve bu faaliyet sonucu üretilen içeriklerin genel adıdır. Bu çalışmada, Türkçeye henüz çevrilmemiş bir terim olan "deepfake" kavramı ele alınmış, bu sahteciliklerin Türk ceza hukuku bakımından ortaya çıkarabileceği sorumluluk halleri incelenmiştir. Ayrıca "deepfake"in tehlikelerine karşı mücadelede diğer ülkelerde bu konuda yapılması planlanan yasal düzenlemeler ve ülkemizdeki mevcut durum ile ülkemiz bakımından yapılması gerekenler değerlendirilmiştir.

Anahtar Kelimeler: *yapay zekâ, derin öğrenme, derin sahtecilik, kişisel veri, büyük veri.*

AN EVALUATION OF DEEPFAKE IN THE CONTEXT OF CRIMINAL LAW AND DE LEGE FERENDA SUGGESTIONS

ABSTRACT

"Deepfake" is the activity of producing contents in forms of images, videos and sounds that are very realistic, although not real, using the deep learning technique, and the general name of the contents produced as a result of this activity. In this study, the concept of "deepfake", a term that has not yet been translated into Turkish, is discussed, and the liability situations that these forgeries may cause in the context of Turkish criminal law are examined. In addition, in the fight against the dangers of "deepfake", the legal regulations planned to be made in other countries, the current situation in our country and what needs to be done in terms of our country were evaluated.

Keywords: *artificial intelligence, deep learning, deep fake, personal data, big data.*

---

* **Arş. Gör.**, Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Ceza ve Ceza Muhakemesi Hukuku Anabilim Dalı/ANKARA, **e-posta:** besir.babayigit@hbv.edu.tr

ORCID : 0000-0002-3710-5792.
DOI : 10.34246/ahbvuhfd.1018877

Yayın Kuruluna Ulaştığı Tarih : 18/06/2021

Yayınlanmasının Uygun Görüldüğü Tarih: 26/10/2021

GİRİŞ

Teknolojideki gelişmeler, salt teknolojiyi değil, aynı zamanda hukuku da ilgilendiren yönleriyle yeni kavramlar ve teknikleri ortaya çıkarmaktadır. Bu gelişmelerden biri de yapay zekâ teknolojilerinden biri olan "*deepfake*"tir. Yapay zekânın getirilerinin yanında, hakların ihlali bağlamında olumsuzlukları da bulunabilmektedir. Nitekim yapay zekâ, kullanım amacına göre bilimsel ve sanatsal çalışmalar yapılmasında araç olduğu kadar suç işlenmesinde de kullanılabilmektedir[1].

Dünya, son dört yılda, "*deepfake*" kavramıyla tanışmış bulunmaktadır. Yapay zekâ içinde değerlendirilen derin öğrenme metoduyla üretilen sahte içerikler; görüntü ve ses manipülasyonu olarak karşımıza çıkan deepfake'e vücut vermektedir. Keza bu söz konusu sahte içerikler çeşitli suçların işlenmesinde bir araç olarak kullanılabilmektedir.

Günümüzde ücretsiz programlarla bile herkes tarafından kolayca deepfake içeriklerin üretilebildiği[2] göz önüne alındığında bu içeriklerin yol açabileceği tehlikelerin artacağını söyleyebiliriz. Bu tehlikelerin önemine binaen, deepfake kavramının ne olduğu, bu içeriklerle işlenebilecek suçlar ve deepfake'in tehlikelerine karşı ne şekilde mücadele edilebileceği hususları çalışmanın konusunu oluşturmaktadır. Bu çalışmayla, Türk hukuk literatüründe deepfake hususunun gündeme getirilmesi amaçlanmaktadır.

Belirtmek gerekir ki, "*deepfake*" tabiri için çalışmada Türkçe bir tabir kullanılmayacak, anlamını kaybetmemesi açısından kavram bu haliyle kullanılacaktır[3].

---

[1] Alexander P. Sukhodolov/Artur V. Bychkov/Anna M. Bychokova, "Yapay Zekâ Teknolojileri Kullanılarak İşlenen Suçlar İçin Ceza Politikası: Devlet, Sorunlar, Beklentiler" in Jocelyne Alayan (Çev.), Yener Ünver (Ed.), Karşılaştırmalı Güncel Ceza Hukuku Serisi 21, Ceza Hukukunda Robot, Yapay Zeka ve Yeni Teknolojiler, Seçkin Yayıncılık, 2021, s. 209; Eylem Aksoy Retornaz, Bir Siber Taciz Biçimi: Cinsel İçerikli Görüntüleri Rızaya Aykırı Olarak İfşa Etme, Yayma, Erişilebilir Kılma veya Üretme Suçu (Revenge Porn ve Deep Fake), On İki Levha Yayıncılık, 2021, 101.

[2] Tobias Lantwin, "Strafrechtliche Bekämpfung missbräuchlicher Deep Fakes – Geltendes Recht und möglicher Regelungsbedarf", 2020, 2, MMR-Zeitschrift für IT-Recht und Recht der Digitalisierung, s. 78; Norbert Lossau, "Deep Fake: Gefahren, Herausforderungen und Lösungswege", 2020, 382, Analysen und Argumente, Konrad-Adenauer-Stiftung, s. 3.

[3] Bazı terimlerin Türkçeye çevrilmeden kullanılması, o terimin kapsamının daralmaması bakımından tercih edilmektedir. Çalışmamızda bu sebeple yeni bir terim olan "*deepfake*"e karşılık olarak bir Türkçe tabir kullanılmayacaktır. Buna karşılık, "*deepfake*" teriminin Türkçeleştirilmesinde "*derin öğrenme teknolojisinin kullanımıyla sahte içerik oluşturma*", "*derin öğrenme teknolojisinin kullanımıyla oluşturulan sahte içerik*", "*ileri sahtecilik*", "*de-*

I. GENEL OLARAK YAPAY ZEKÂ, BÜYÜK VERİ, MAKİNE ÖĞRENMESİ VE DERİN ÖĞRENME

Çalışmanın altyapısını yapay zekâ teknolojilerinin gelişmesiyle ortaya çıkan derin öğrenme tekniği oluşturmaktadır. Bu sebeple yapay zekâ ("*artificial intelligence (AI)*"), büyük veri ("*big data*"), makine öğrenmesi ("*machine learning*") ve derin öğrenme ("*deep learning*") kavramlarına kısaca değinmek çalışmanın anlaşılması açısından önem arz etmektedir[4].

İnsanlar, bazı icatlarında tabiatı taklit etmişlerdir. Örneğin gözün çalışma mekanizmasının anlaşılmasıyla, fotoğraf makinesi icat edilmiştir. İnsan beyninin anlamlı karar verme mekanizmasının anlaşılmasıyla birlikte de insanı taklit eden makineler tasarlanmaya başlanmıştır[5]. Bu noktada, yapay zekâ, *makinelerin programlanıp insan gibi adeta "şuurlu" davranışlar gösterebilmesi* olarak tanımlanmaktadır[6]. Yapay zekâ, insan zekasının kullanım sürecinin makinelerle taklit edilmesi olarak da ifade edilmektedir[7].

Olaylar karşısındaki deneyimler aracılığıyla insanlar o durum ve benzer durumlarla ilgili görüş oluşturur, belli düşünce kalıpları geliştirir. Görüşler, o olay karşısında ne şekilde hareket edeceğimizi, yani tutumumuzu belirler.

---

rin taklit", "*derin hile*", "*derin sahtecilik*" ve "*dip düzmece*" gibi ifadeler kullanılabilir. Bu ifadeler arasından "*dip düzmece*" ve "*derin sahtecilik*" ifadelerinin kullanılmasının, "*deepfake*" teriminin kapsamına yakınlaşması ve kısa ifadeler olması sebebiyle uygun olabileceği kanaatindeyiz. Ancak bu terimin Türkçeleştirilmesinde ideal olanın, terimin bilişim alanında bir terim olması sebebiyle bilişim alanındaki ve dil alanındaki uzmanlarca Türkçeleştirilmesi olduğunu ifade etmeliyiz. Güncel bir çeviri faaliyetinde "*deepfake*" ifadesi, "*derin sahte*" olarak çevrilmiştir. Bkz. Sukhodolov/Bychkov/Bychokova, s. 209. Güncel bir başka çalışmada ise, "*deepfake*" ifadesi olabildiğince çevrilmeden kullanılsa da çalışma bağlamında yapılan açıklamalar doğrultusunda bazı yerlerde "*yüz değiş tokuşu*"na karşılık olarak kullanılmaktadır. Bkz. Aksoy Retornaz, s. 32, 99, 115, 142. "*Yüz değiş tokuşu*" ifadesinin "*faceswap*" kavramına karşılık kullanılması gerektiğini ve faceswap'ın deepfake teknolojisiyle yapılabileceklerden en yaygını olsa da deepfake'in bundan ibaret olmadığını belirtmeliyiz.

4 Belirtmek gerekir ki, bu kavramlar henüz Türk Dil Kurumu'nun (TDK) sözlüklerinde kendine yer bulamamıştır.

5 Anand Deshpande/Manish Kumar, Artificial Intelligence for Big Data, Packt, 2018, s. 8.

6 Harun Pirim, "Yapay Zeka", 2006, 1(1), Journal of Yaşar University, s. 85.

7 Sachin Ramar, Artificial Intelligence How It Changes the Future, Kendi Basımı (Independently Published), 2019, s. 7, <https://www.scribd.com/document/466365329/Artificial-Intelligence-How-It-Changes-the-Future> Erişim Tarihi 25.10.2019. Yapay zekâ ayrıca sözlükte şu şekilde tanımlanmaktadır: "*1. Bilgisayarlarda akıllı davranış simülasyonu ile uğraşan bir bilgisayar bilimleri dalı. 2. Bir makinenin akıllı insan davranışını taklit edebilme yeteneği.*" Bkz. <https://www.merriam-webster.com/dictionary/artificial%20intelligence> Erişim Tarihi 24.10.2019.

Nihayet, hareketlerimiz de ortaya bir sonuç çıkarır. Buna "*sonuçlar piramidi teorisi*" ("*the results pyramid theory*") denilmektedir[8]. Yani sonuçlar piramidi teorisine göre, tabanda deneyimler yer almakta, üstünde deneyimlere dayalı görüşler ve düşünce kalıpları, onun üstünde görüş ve düşünce kalıplarına dayalı hareketler-tutumlar ve en üstte hareketlerin sonuçları yer alır. Yapay zekâda bilgisayarın çalışma mantığı da bu şekilde gerçekleşmektedir. Veriler deneyimlere, modeller görüşlere ve çıktılar harekete-sonuçlara denk düşmektedir[9]. Burada *a posteriori*, *ampirik* bir bilgiden bahsedildiği söylenebilir. Dolayısıyla buradaki bilginin kaynağını algılar ve deneyim oluşturmaktadır. *Deepfake* bağlamında önemli olanın bu tür bir bilgi olduğunu ifade etmeliyiz.

Bir diğer kavram olan "*büyük veri*", sözlükte şu şekilde tanımlanmaktadır: "*Geleneksel veritabanı yönetimi araçları tarafından işlenemeyecek kadar büyük ve karmaşık veri birikimi*"[10]. Büyük veri terimi, eskiye nazaran ortaya çıkan verilerin artmasını ifade etmek için kullanılmaktadır. Önceden günlük 100 GB ("*gigabyte*"[11]) elektronik veri ortaya çıkarken, 2018 yılında saniyede 50.000 GB veri üretildiği ifade edilmektedir[12]. Keza 2018 yılında 33 ZB ("*zettabytes*"[13]) olan dünyadaki toplam verinin 2025 yılında 175 ZB'ta çıkacağı öngörülmektedir[14].

---

[8] Deshpande/Kumar, s. 9.

[9] Deshpande/Kumar, s. 9.

[10] <https://www.merriam-webster.com/dictionary/big%20data> Erişim Tarihi 24.10.2019.

[11] 1 gigabyte, 1024 MB'tan ("*megabytes*"), 1 megabyte, 1024 KB'tan ("*kilobytes*"), 1 kilobyte, 1024 "*bytes*"tan oluşmaktadır. Byte ise 8 adet "*bit*"ten müteşekkildir. Bit'ler, bilgisayarın en küçük verisini ifade eder. 1 gigabytes, 1,073,741,824 bytes içerir. Bkz. <https://www.merriam-webster.com/dictionary/gigabyte> Erişim Tarihi 24.10.2019; <https://www.merriam-webster.com/dictionary/megabyte> Erişim Tarihi 24.10.2019; <https://www.merriam-webster.com/dictionary/kilobyte> Erişim Tarihi 24.10.2019; <https://www.merriam-webster.com/dictionary/byte> Erişim Tarihi 24.10.2019; <https://www.merriam-webster.com/dictionary/bit> Erişim Tarihi 24.10.2019.

[12] Deshpande/Kumar, s. 14.

[13] 1 zettabyte, 1.099.511.627.776 GB'a (yaklaşık bir trilyon GB) denk düşmektedir. Bkz. <http://www.kylesconverter.com/data-storage/zettabytes-to-gigabytes> Erişim Tarihi 21.02.2021.

[14] David Reinsel/John Gantz/John Rydning, The Digitization of the World - From Edge to Core, IDC White Paper, 2018, s. 3.

Bu devasa değişim günümüzde işlenmiş ve işlenmemiş verilerin inanılmaz boyutlara ulaştığını göstermektedir. Belirtmek gerekir ki, büyük şirketler, çeşitli ürün ve uygulamalarla bu verilerin artmasına da sebep olmaktadır. Bir teknoloji şirketinin "*akıllı*" gözlüğünün veri toplaması bu bağlamda örnek olarak gösterilmektedir. Bkz. Robert Chesney/Danielle

Günümüzde ulaşılabilir büyük veriyi analiz edebilmek, veri içindeki kalıpları anlamak ve bağlamsal detaylara dayanarak sonuçta değer yaratan hızlı çözümler sunmak büyük verinin en önemli özelliği olarak ifade edilmektedir[15]. Yapay zekâ algoritmaları vasıtalarıyla bu verilerin işlenerek bunlardan anlamlı sonuçlar çıkarılması, oluşan büyük verinin kullanılmasıyla mümkün hale gelmiştir. Eldeki verinin miktarı az olduğu müddetçe araştırılan konunun içeriğine veya üretilmek istenen çıktılara yönelik sağlıklı sonuçlar almak da mümkün olmayacaktır. Dolayısıyla, deepfake medya içerikleri gerçeğe yakın biçimde üretilemeyecektir.

Büyük veriyi analiz etmek için çeşitli teknikler uygulanmaktadır. Bunlardan birisi, "*makine öğrenmesi*" olarak adlandırılmakta ve yapay zekâ ile öğrenme olarak ifade edilmektedir[16]. Daha açık ifadeyle makine öğrenmesi, makinenin bir konuyu kavramadan önce o konuyla ilgili çok fazla veri topladığı ve bu verilere dayanarak belli bir görevin nasıl gerçekleştirileceğini öğrendiği bir süreçtir[17]. Yapay zekâya sahip bir makinenin insan gibi hareket etmesi için makine öğrenmesine sahip olması beklenmektedir[18].

Keats Citron, "21st Century-Style Truth Decay: Deep Fakes and the Challenge for Privacy, Free Expression, and National Security", 2019, 78(4), Maryland Law Review, s. 890, 891. Böyle bir cihazın fonksiyonunu yerine getirebilmesi için etraftaki objelerin görüntü ve ses verilerini elde etmesi gerekmektedir. Bu da internete bağlı cihazlar vasıtasıyla sürekli olarak verilerin birikmesi ve işlenmesi anlamına gelmektedir.

[15] Deshpande/Kumar, s. 15.

[16] Metin Turan, Bilişim Hukuku, Seçkin Yayıncılık, 2016, s. 218.

[17] Ramar, s. 10. Makine öğrenmesi, sözlükte şu şekilde tanımlanmaktadır: "*Bir bilgisayarın, sürekli olarak mevcut bir istatistiksel modele dahil edilmesiyle (görüntü dosyalarının analiz edilmesinde olduğu gibi) kendi performansını iyileştirebildiği süreç.*" Bkz. <https://www.merriam-webster.com/dictionary/machine%20learning> Erişim Tarihi 24.10.2019. Makine öğrenmesine Türk araştırmacıların yaptığı bir çalışma örnek olarak verilebilir. Söz konusu çalışmada; araştırmacılar Hürriyet Gazetesi'nde yirmi yazara ait toplam yirmi bin köşe yazısını makine öğrenmesi tekniğiyle programa tanıtmış ve program ilgili yazıların ortak karakteristik özelliklerine göre hangi yazının hangi yazara ait olduğunu tespit ederek öğrendikten sonra, sisteme bu yazarlardan birinin daha önce tanıtılmamış yeni bir yazısı eklendiğinde bu yazının kime ait olduğunu yüksek bir oranla bilebilir hale gelmiştir. Araştırmacılar gelecekte, benzer teknikleri kullanarak cinsiyet ve içerik sınıflandırması üzerinde çalışmayı planladıklarını belirtmektedir. Çalışma için bkz. Mustafa Sarı/A. Murat Özbayoğlu, "Classification of Turkish Documents Using Paragraph Vector", 2018, 2018 International Conference on Artificial Intelligence and Data Processing (IDAP), s. 1-5, <https://ieeexplore.ieee.org/document/8620813> Erişim Tarihi 24.10.2019.

[18] Stuart J. Russell/Peter Norvig, Artificial Intelligence A Modern Approach, Third Edition, Pearson Publishing, 2011, s. 2.

Buna karşılık, derin öğrenme terimi sözlüklerde kendine yeni yer bulabilmektedir[19]. Bu da terimin makine öğrenmesi teriminden daha yeni olarak ortaya çıktığına bir kanıt niteliğindedir. Derin öğrenme, bilgisayarla görme ve doğal dil işleme gibi alanlarda daha karmaşık sorunları işleyen gelişmiş bir "*yapay sinir ağı*" ("*artificial neural nets*") türü olarak ifade edilmektedir[20]. Derin öğrenmedeki yazılım, bir problemin tek yönlü olarak salt çözümü için programlanmış olmak yerine, karşılıklı yönlerde tepki verecek biçimde önceki verilere dayanan deneyimlerle eğitilmektedir[21]. Tanımdan anlaşıldığı üzere derin öğrenme, makine öğrenmesinin daha karmaşık yapıdaki bir görünümüdür. Bu karmaşık yapısının daha zor becerilerin de üstesinden gelmesini sağladığını ifade edebiliriz. Derin öğrenmede makine, işlem sonucunda yaptığı çıkarımın sonucundaki hataların farkına varmakta, geri besleme ("*backpropagation*") yaparak daha sonraki hesaplamalarda bu hatayı en aza indirmektedir[22]. Deepfake içerik üretiminde ne kadar çok veriye

[19] Örneğin Marriam-Webster sözlüğünde bu terim henüz yer almamaktayken Cambridge sözlüğünde yer almaktadır. Bkz. <https://dictionary.cambridge.org/dictionary/english/deep-learning> Erişim Tarihi 14.03.2021.

[20] Agnieszka M. Walorska, "Deepfakes & Desinformation", 2020, Mai, Friedrich-Naumann-Stiftung für die Freiheit, Mai 2020, s. 9. Derin öğrenme terimi yerine yapay sinir ağları ("*artificial neural nets*") ifadesi de tercih edilebilmektedir. Bkz. Eugene Charniak, Introduction to Deep Learning, The MIT Press, 2018, s. 1; Walorska, s. 10. Deepfake içeriklerin oluşturulmasında "*üretken çatışan (çekişmeli) ağlar*" ("*generative adversarial networks-GAN*") teknolojisi kullanılmaktadır. Bkz. Anna Yamaoka-Enkerlin, "Disrupting Disinformation: Deepfakes and the Law", 2020, 22(3), New York University Journal of Legislation and Public Policy, s. 726; Matthew F. Ferraro, Deepfake Legislation: A Nationwide Survey - State and Federal Lawmakers Consider Legislation to Regulate Manipulated Media, WilmerHale, 2019, s. 3, <https://www.wilmerhale.com/-/media/files/shared_content/editorial/publications/wh_publications/client_alert_pdfs/20190925-deepfake-legislation-a-nationwide-survey.pdf> Erişim Tarihi 18.02.2021; Robert Chesney/Danielle Keats Citron, "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security", 2019, 107(6), California Law Review, s. 1760; Walorska, s. 9; Thomas C. King/Nikita Aggarwal/Manarosaria Taddeo/Luciano Floridi, "Yapay Zekâ Suçu: Öngörülebilir Tehditleri ve Çözüm Yolları Üzerine Disiplinler Arası Bir Analiz" in Hasan Dursun (Çev.), Yener Ünver (Ed.), Karşılaştırmalı Güncel Ceza Hukuku Serisi 21, Ceza Hukukunda Robot, Yapay Zeka ve Yeni Teknolojiler, Seçkin Yayıncılık, 2021, s. 262. "*Üretken çatışan (çekişmeli) ağlar*" ("*generative adversarial networks-GAN*") teknolojisinin ayrıntıları için bkz. Çetin Elmas, Yapay Zeka Uygulamaları, 5. Baskı, Seçkin Yayıncılık, 2021, s. 215; Vasif Nabiyev, Yapay Zeka, 6. Baskı, Seçkin Yayıncılık, 2021, s. 615 vd.

[21] <https://www.yourdictionary.com/deep-learning> Erişim Tarihi 24.10.2019; King/Aggarwal/Taddeo/Floridi, s. 262.

[22] <https://towardsdatascience.com/back-propagation-414ec0043d7> Erişim Tarihi 24.10.2019. Çalışma mekanizması için bkz. Elmas, s. 216, 216. Bu durum ayrıca, "*polis*" ve "*parada sahtecilik yapan kişi*" üzerinden alegori yapılarak anlatılmaktadır. Bu alegoride, "*parada sahtecilik yapan kişi*", ürettiği ürünün olabildiğince gerçekçi görünmesi için çabalar.

sahip olunursa o kadar gerçekçi bir içerik oluşturulabilecektir[23]. Sonuç olarak da büyük veri ve derin öğrenmeyle birlikte daha doğru ve kesin sonuçlar alınmaktadır. Derin öğrenmedeki işlenen bilginin, yukarıda ifade edilen sonuçlar piramidi teorisindeki bilgisayar bakımından "*deneyimsel*" bilgi olduğu görülmektedir.

II. DEEPFAKE TEKNOLOJİSİ VE DEEPFAKE İÇERİKLER

Deepfake kavramının, sözlüklerde kendine yer bulması oldukça yenidir[24]. Deepfake tabirinin, "*deep (learning)*" (derin öğrenme) ve "*fake (content)*" (sahte içerik) kelimelerinin birleştirilmesi suretiyle üretildiği belirtilmektedir[25]. Kısaca, sahte medya içeriklerinin derin öğrenme teknolojisi kullanılarak üretilmesi şeklinde tanımlanabilir[26]. Terim hem üretilen medya içerikleri hem de bu medya içeriklerinin üretilmesi işlemi için kullanılmaktadır[27].

"*Polis*" ise, bir ürünün sahteliğini tespit edebilmek yönünde kendini geliştiren kişi olarak yansıtılmaktadır. Dolayısıyla "*polis*" sahteliğin tespit edilmesi, "*parada sahtecilik yapan kişi*" ise sahteliğin tespit edilmemesi bakımından birbirleriyle rekabet halindedir. Aldatıcılık niteliği en üst derecede bir sahte paranın üretilebilmesi veya aldatıcılık niteliği en üst derecede bir sahte paranın kesin olarak tespit edilebilmesi için "*polis*" ile "*parada sahtecilik yapan kişi*"nin rekabet halinde birbirlerinin deneyimlerinden sonuç çıkarmaları gerekir. Bu rekabetten öğrenilen deneyimler sonucundaki bilgiyle birlikte sahte ürün üretilmesi tekniği gelişirken sahte ürünün tespiti tekniği, sahte ürünün tespiti tekniği gelişirken de sahte ürün üretilmesi tekniği gelişecektir. Derin öğrenme-GAN yazılımı, bu alegoriye göre aynı anda hem "*polis*" (discriminative model) hem de "*parada sahtecilik yapan kişi*" (generative model) gibi davranmaktadır. Bkz. Ian J. Goodfellow/Jean Pouget-Abadie/ Mehdi Mirza/ Bing Xu/David Warde-Farley/Sherjil Ozair/Aaron Courville/Yoshua Bengio, "Generative Adversarial Nets", 2014, arXiv:1406.2661v1, s. 1, <https://arxiv.org/pdf/1406.2661.pdf> Erişim Tarihi 14.03.2021.

[23] Tobias Lantwin, "Deep Fakes - Düstere Zeiten für den Persönlichkeitsschutz? Rechtliche Herausforderungen und Lösungsansätze", 2019, 9, MMR-Zeitschrift für IT-Recht und Recht der Digitalisierung, s. 574. Bu da üretilen içeriğin gerçekçiliğini üst seviyelere çıkarmaktadır. Bkz. Chesney/Citron, Looming Challenge, s. 1760.

[24] Bkz. <https://dictionary.cambridge.org/dictionary/english/deepfake> Erişim Tarihi 14.03.2021.

[25] Travis L. Wagner/Ashley Blewer, "'The Word Real Is No Longer Real': Deepfakes, Gender, and the Challenges of AI-Altered Video", 2019, 3(1), Open Information Science, s. 36; Lossau, s. 2; Walorska, s. 9; Yamaoka-Enkerlin, s. 726.

[26] Lantwin, Rechtliche Herausforderungen, s. 574; Aksoy Retornaz, s. 99, 100.

[27] Deepfake'in dünya üzerinde ilk olarak ortaya çıkışının, 2017 yılında "*reddit*" internet sitesi kullanıcılarından birinin cinsel nitelikteki sahte görüntüler oluşturmasıyla başladığı ifade edilmektedir. Bkz. Ronit Chawla, "Deepfakes: How a Pervert Shook the World", 2019, 4(6), International Journal of Advance Research and Development, s. 8; Lantwin, Rechtliche Herausforderungen, s. 575; Walorska, s. 14.

Deepfake'in ne olduğunun, deepfake içerikleriyle temas kurmaksızın anlatılmasında güçlük çekilebilir. Basitçe ifade etmek gerekirse, temelde, orijinal bir medya içeriğinde (fotoğraf ve video gibi) yer alan kişilerin yüzünün tamamen başka kişinin yüzüyle değiştirilmesi (A kişisinin yüzü yerine B kişinin yüzünün vücuda uyumlu hale getirilmesi)[28], orijinal içerikteki kişinin yüz ifadesinin değiştirilmesi (A'nın yüz ifadesi gülümseme iken, kızgın yüz ifadesine çevrilmesi) veya gerçekte hiç var olmayan bir insanın varmış gibi baştan oluşturulması (farazi bir C kişisinin oluşturulması) şeklinde[29] görüntü üzerinde gerçekleştirilen gerçekçi değişikliklerdir. Belirtmek gerekir ki, söz konusu değişiklikler, sadece yüz ile ilgili olmak zorunda değildir. Bir kişiyle ilişkilendirilebilecek şekilde kişinin tüm vücuduna ve vücudunun bölümlerine yönelik değişiklikler de söz konusu olabilir. Ayrıca sadece görüntü değil, bilhassa videolarda ses değişiklikleri de yapılabilmektedir. Örneğin, hiç söylenmemiş sözler, o kişi söylüyormuş gibi gerçekçi biçimde değiştirilebilmektedir[30].

III. DEEPFAKE'İN HUKUKEN ORTAYA ÇIKARABİLECEĞİ TEHLİKELER

Deepfake, kullanım amacına göre faydalı olabildiği gibi[31], sahte içeriği sebebiyle hukuki değerleri ihlal de edebilmektedir[32]. Deepfake'in ortaya çıkarabileceği tehlikelerle ilişkili başlıca hukuki değerlerin; maddi ve manevi varlığı koruma ve geliştirme hakkı (Anayasa m. 17), özel hayata ve aile hayatına saygı gösterilmesini isteme ve özel hayatın ve aile hayatının gizliliği hakkı (Anayasa m. 20/1), kişisel verilerin korunmasını isteme hakkı (Anayasa m. 20/3), düşünce ve kanaat hürriyeti ile düşünce ve kanaatleri açıklama ve yayma hakkı (Anayasa m. 25, 26), bilim ve sanat hürriyeti (Anayasa m. 27)

---

[28] King/Aggarwal/Taddeo/Floridi, s. 262; Sukhodolov/Bychkov/Bychokova, s. 209; Aksoy Retornaz, s. 99.

[29] Mustafa Evren Berk, "Dijital Çağın Yeni Tehlikesi 'Deepfake'", 2020, 16(28), Uluslararası Toplum Araştırmaları Dergisi, s. 1512, 1513; Walorska, s. 17, 18.

[30] Lantwin, Rechtliche Herausforderungen, s. 574; Walorska, s. 17; Sukhodolov/Bychkov/Bychokova, s. 209.

[31] Örneğin sinema sektöründe *deepfake* kullanımı verimli olabilmektedir. Söz gelimi, 1994'te ölen oyuncu Peter Cushing'in 2016 yılında Rogue One filminde adeta yaşıyormuş gibi filme dahil edilmesi ve oyunculuk sergiliyor gözükmesi *deepfake* sayesinde mümkün olmuştur. Bkz. <https://www.youtube.com/watch?v=cu77zS1pagk> Erişim Tarihi 10.12.2019; Chesney/Citron, Looming Challenge, s. 1770; Walorska, s. 7, 22; Yamaoka-Enkerlin, s. 734.

[32] Lantwin, Strafrechtliche Bekämpfung, s. 81; Chesney/Citron, Looming Challenge, s. 1754.

olduğunu söyleyebiliriz[33].

Nitekim bu içeriklerde kişilerin görüntüleri kullanılabilmekte ve kişilerin görüntüsü gerçeğinden ayırt edilemeyecek hale getirilebilmektedir. Örneğin, müstehcen içerikli bir videoda gerçekte yer alan kişi yerine, başka bir kişinin görüntüsü koyularak sahte videolar üretilebilmektedir[34]. Yine örneğin, bu sahte görüntüler oluşturulduktan sonra içeriğe eklenen kişinin para vermesi istenebilmekte, yoksa bu içeriğin internet sitelerinde yayımlanacağı tehdidinde bulunulabilmektedir[35]. Keza, siyasi kişiliklerin görüntü ve seslerine ilişkin verilerin internet ortamında kolayca erişilebilir olması ve bu verilerin büyük bir yekûn teşkil etmesiyle bu kişiler bakımından toplanarak analiz edilen verilerin "*büyük veri*" bağlamında değerlendirilmesi mümkündür. Dolayısıyla, deepfake içeriklerde bilhassa siyasi kişiliklerin kullanılması daha kolay ve gerçekçi olmaktadır. Bunun en meşhur örneği, Jordan Peele'nin Barack Obama'nın sesi ve görüntüsünü manipüle ederek oluşturduğu ve deepfake'in tehlikesine dikkat çektiği videosudur[36]. Bu türden videoların toplumun tamamını ve devletler arası ilişkileri etkileyebilecek düzeyde olduğu açıktır[37].

Dolayısıyla, *Deepfake*'in bireysel zararları olabildiği gibi ulusal güvenliği etkileyici yönleri de bulunmaktadır[38]. Amerika Birleşik Devletleri (ABD) Temsilciler Meclisi İstihbarat Daimî Seçim Komitesi ("*U. S.*

---

[33] Temel haklar olarak saydığımız bu değerlerin yanında, aşağıda deepfake'in kullanılmasıyla işlenebilecek suçların koruduğu hukuki değerlerin de bu kapsamda olduğunu belirtmeliyiz.

[34] Danielle Keats Citron, "Prepared Written Testimony and Statement for The Record", 2019, House Permanent Select Committee on Intelligence, s. 4, <https://docs.house.gov/meetings/IG/IG00/20190613/109620/HHRG-116-IG00-Wstate-CitronD-20190613.pdf> Erişim Tarihi 26.10.2019.

[35] Bu hususta bir örnek olay için bkz. <https://www.abc.net.au/news/2019-08-30/deepfake-revenge-porn-noelle-martin-story-of-image-based-abuse/11437774> Erişim Tarihi 26.10.2019.

[36] Bkz. <https://www.youtube.com/watch?v=cQ54GDm1eL0> Erişim Tarihi 21.02.2021.

[37] Devletler arası ilişkileri etkileyebilecek deepfake'ler bakımından kurgusal olarak şöyle bir örnek verilmektedir: "*Şimdi gerçekleşmesi muhtemel bir senaryo yazacağız. Malum ABD başkanı Trump, Twitter'dan resmi açıklamalar yapıyor ve Trump'ın da hesabından bir tweet atılsa; hem de "deepfake" kullanılarak yani yapay zeka marifetiyle sahte bir video oluşturularak... Uzmanı olmayanın sahteliğini anlayamadığı o videoda; Trump, İran'a ve Çin'e nükleer bomba atacağını bütün gerekçeleriyle Beyaz Saray'da resmi makamı olan oval ofiste anlatsa ve videonun en sonunda kırmızı bir butona bassa... Şu tweetten sonra, dünya piyasasında neler olur, hangi ülkelerde kaos başlar, dünyanın hali ne olur düşünebiliyor musunuz?*" Bkz. Ahmet Yavuz Uşaklıoğlu, Dijital Hukuk, 2. Baskı, Seçkin Yayıncılık, 2021, s. 151.

[38] Chesney/Citron, Looming Challenge, s. 1783, 1784.

House of Representatives Permanent Select Committee on Intelligence") tarafından 13.06.2019 tarihinde Yapay Zekanın Ulusal İstihbarat Sorunları, Manipüle Edilen Medya ve Deepfake'ler ("*National Intelligence Challenges of Artificial Intelligence, Manipulated Media, and Deepfakes*") başlıklı bir oturum gerçekleştirilmiştir[39]. Bu oturuma konuya hâkim kişiler ve çeşitli üniversitelerden akademisyenler katılarak fikirlerini beyan etmiş ve deepfake'in tehlikelerine karşı mücadeleye yönelik öneriler sunulmuştur. Söz konusu tespit ve önerilerden bazıları şu şekildedir[40]:

Gelişmiş yapay zekâya ve büyük veriye erişim imkânı olan ülkeler diğerlerine göre büyük avantajlara sahiptirler. Bir kez gün yüzüne çıkmış sahte bir ses, fotoğraf veya videonun sahteliğinin çürütülebilmesi oldukça zordur. Deepfake teknolojisini devletler, kitlelere yönelik çarpıtılmış içerik sunmak için kullanabilecektir. Yapay zekânın doğru kullanımını ve ses, video gibi medya içeriklerinin gerçekliğini doğrulamaya yönelik teknolojiyi ilerletmek için politikalar geliştirilmelidir. Deepfake vasıtasıyla düzenlenen iftira kampanyaları için acil müdahale planı geliştirilmelidir. Oluşturulacak genel farkındalık, sahte ses ve video içeriklerinin kötü etkilerine karşı koymada önem arz etmektedir.

Deepfake teknolojisiyle oluşturulan videolar gelecekte çokça çeşitlenebilir. Örneğin, toplumda saygın-etkin bir kişi, bir terör örgütünün gerçekleştirdiği eylemi destekleyen bir açıklama yapıyormuş gibi gösterilebilir[41]. Deepfake videolar ve sesler, seçimleri manipüle ederek demokratik sürece zarar verebilir[42]. Bu içerikte bir videonun yayılmasıyla birlikte geri dönüşü olmayan sonuçlar ortaya çıkabilecektir.

Deepfake kapsamında içerik üretilmesi ve bunların kullanılması önemli hukuki değerlerle ilişkili hak ihlallerine sebebiyet vererek toplumda katlanılamaz bir noktaya gelebilir. Dolayısıyla bu hallerde ceza hukukunun

---

[39] Bkz. <https://intelligence.house.gov/calendar/eventsingle.aspx?EventID=653> Erişim Tarihi 26.10.2019.

[40] Bkz. <https://docs.house.gov/meetings/IG/IG00/20190613/109620/HHRG-116-IG00-Wstate-WattsC-20190613.pdf> Erişim Tarihi 26.10.2019; <https://docs.house.gov/meetings/IG/IG00/20190613/109620/HHRG-116-IG00-Wstate-WattsC-20190613.pdf> Erişim Tarihi 26.10.2019.

[41] Başka örnekler için bkz. Lantwin, Rechtliche Herausforderungen, s. 575.

[42] Lantwin, Strafrechtliche Bekämpfung, s. 79; Chesney/Citron, Looming Challenge, s. 1778, 1779; Walorska, s. 7; Christoffer Waldemarsson, Disinformation, Deepfakes & Democracy, The Alliance of Democracies Foundation, 2020, s. 9, 10.

müdahalesi gündeme gelebilecektir. İlk olarak halihazırdaki mevzuat bağlamında deepfake'in ortaya çıkarabileceği ceza hukuku sorumluluğunun ele alınması gerekir. Ardından geleceğe yönelik olarak hukuki bir değerlendirme yapılacaktır.

IV. DEEPFAKE'İN ORTAYA ÇIKARABİLECEĞİ CEZA HUKUKU SORUMLULUĞU

Gelişen teknoloji ve artan internet imkânları bazı suçların internet ortamında bilişim sistemlerinin kullanılması suretiyle ve çeşitli kitle iletişim araçlarıyla işlenmesini kolaylaştırmakta ve yaygınlaştırmaktadır[43]. Deepfake içeriklerin üretilmesi için geliştirilen programların üretilmesinden başlayarak deepfake içeriklerin kullanılmasına kadar çeşitli aşamalarda farklı ceza hukuku sorumluluklarının ortaya çıkması gündeme gelebilir. Bu bağlamda, deepfake içeriklerinin üretilmesi ve kullanılması halinde en çok gündeme gelebilecek olan halihazırdaki suç tiplerine aşağıda yer verilecektir.

A. Yasak Cihaz ve Programlar

Bir bilgisayar programının bilişim suçlarının veya bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçların işlenmesi amacıyla oluşturulması, imal, ithal, sevk, nakil ve kabul edilmesi veya depolanması, satılması, satışa arz edilmesi, satın alınması, başkalarına verilmesi veya bulundurulması TCK m. 245/A'da yer alan yasak cihaz ve programlar başlıklı suça vücut vermektedir[44]. Esasen maddede ifade edilen suçların işlenmesi açısından hazırlık hareketi niteliğinde olan bu fiiller TCK'da suç olarak tanımlanmıştır[45].

Deepfake içeriklerini üretmek için, sıradan insanların da bu türden içerik oluşturabilmeleri amacıyla programlar üretilebilmektedir. Örneğin, "*DeepNude*" adlı bir program, esasen giyinik olan insanların fotoğraflardaki görüntüsünün, yapay zekâ kullanılarak çıplak hale getirilmesi için

[43] Berrin Akbulut, Bilişim Alanında Suçlar, 2. Baskı, Seçkin Yayıncılık, 2017, s. 38; Hüseyin Akarslan, Bilişim Suçları, 2. Baskı, Seçkin Yayıncılık, 2015, s. 76; Mesut Orta, Bilişim Suçları ve Elektronik Delillerin Toplanması Muhafazası Değerlendirilmesi Sunulması (Adli Bilişim), Yetkin Yayınevi, 2015, s. 92; Tunç Demircan, Bilişim Alanında Suçlar, İstanbul, Legal Yayınevi, 2016, s. 24.

[44] Mahmut Koca/İlhan Üzülmez, Türk Ceza Hukuku Özel Hükümler, 7. Baskı, Adalet Yayınevi, 2020, s. 958.

[45] Akbulut, Bilişim Alanında, s. 348; Koca/Üzülmez, Özel Hükümler, s. 959.

geliştirilmiştir[46].

Bununla birlikte yasak cihaz ve programlara ilişkin TCK m. 245/A'da yer alan suçun oluşabilmesi için, *bilişim suçlarının veya bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçların işlenmesi* ***için*** imal, ithal, sevk, nakil ve kabul edilmesi veya depolanması, satılması, satışa arz edilmesi, satın alınması, başkalarına verilmesi veya bulundurulması gerekir. Örneğin, dolandırıcılık suçunun bilişim sistemlerinin araç olarak kullanılması suretiyle işlenmesi nitelikli hali (TCK m. 158/1-f) "*bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçlar*"dan biri olduğundan, dolandırıcılık suçunun bilişim sistemlerinin araç olarak kullanılması suretiyle işlenmesi için deepfake içerik üreten bir program bulunduruyor olmak, TCK m. 245/A'da yer alan yasak program bulundurma suçunu oluşturur. Dolayısıyla, amaç unsuruna yer verilmesi sebebiyle, deepfake içeriğinin oluşturulması için üretilmiş her programın salt deepfake içerik üretiyor olmasından bahisle bu suçun oluştuğunu söylemek mümkün değildir.

B. İftira, Suç Uydurma ve Şantaj

Bilhassa basın ve yayın yoluyla ve fakat aynı zamanda yetkili makamlara ihbar veya şikâyette bulunmak suretiyle, işlemediğini bildiği halde, hakkında soruşturma ve kovuşturma başlatılmasını ya da idari bir yaptırım uygulanmasını sağlamak için bir kimseye hukuka aykırı bir fiil isnat etmek, iftira suçunu oluşturur (TCK m. 267/1). Deepfake bağlamında iftira suçunun işlenmesi, TCK'nın 267. maddesinin ikinci fıkrası bakımından söz konusu olmaktadır. Yani deepfake içeriklerin üretilmesi ve kullanılmasıyla, fiilin maddî eser ve delillerini uydurarak iftirada bulunmak söz konusu olabilmektedir[47] (TCK m. 267/2).

Dijital nitelikteki deliller bakımından da deepfake bir sorun teşkil edebilmektedir. Nitekim deepfake teknolojisinin az teknik beceriye sahip kişilerin bile gözle görülmeyen sahtecilik yaratmalarına imkân sağlamasından ötürü, dijital delillerin oluşturulmasında da deepfake teknolojisi kullanılabilir ve böylece sahte deliller oluşturulabilir[48]. Örneğin, kamera kayıtlarında kasten

---

[46] Bkz. <https://www.vice.com/en/article/kzm59x/deepnude-app-creates-fake-nudes-of-any-woman> Erişim Tarihi 22.02.2021; Aksoy Retornaz, s. 100, dn. 370.

[47] Sukhodolov/Bychkov/Bychokova, s. 210.

[48] Rebecca J. Hamilton, "New Technologies in International Criminal Investigations", 2018, 112, Proceedings of the 112th Annual Meeting, International Law in Practice, Cambridge Univesity Press, s. 131, 132. Deepfake içeriklerinin yargı mercileri önüne gelmesiyle birlikte,

öldürme suçunu işleyen A'nın yüzünün, B ile değiştirilerek videonun manipüle edilebilmesi mümkündür.

Keza suç uydurma suçu kapsamında; esasen işlenmeyen bir suçun delil veya emarelerini soruşturma yapılmasını sağlayacak biçimde uydurmak deepfake ile mümkündür (TCK m. 271/1). Örneğin, kamera kaydında hekim A'nın bir hastayı tedavi ederkenki görüntüleri yer almasına karşın, gerçekleştirdiği fiilin kasten öldürme suçunu oluşturacak biçimde videoda manipüle edilmesi söz konusu olabilir.

TCK m. 107/2'de yer alan şantaj suçunda, kendisine veya başkasına yarar sağlamak maksadıyla bir kişinin şeref veya saygınlığına zarar verecek nitelikteki hususların açıklanacağı veya isnat edileceği tehdidinde bulunulması cezalandırılmaktadır. Çalışma konusu bakımından özellik arz eden husus, suçun kişinin şeref veya saygınlığına zarar verecek nitelikteki hususların *isnat edilmesi* suretiyle de işlenebilir olmasıdır. Dolayısıyla, suçun işlenme biçimi olarak gerçek hususların açıklanacağı tehdidinin yanı sıra gerçek olmayan, uydurulmuş ama gerçekliğine inanılabilir hususların isnat edileceği tehdidinde bulunulması da bir seçimlik hareket olarak yer almaktadır[49]. Bir deepfake içeriğinin gerçekliğinin inandırıcılığı karşısında, bu içeriklerde kişinin görüntülerinin kullanılacağı ve bu suretle kişinin şeref veya saygınlığına zarar verecek nitelikteki gerçekliğine inanılabilir hususların isnat edileceği tehdidinde bulunulması bu suça vücut verecektir[50].

C. Kişisel Verilerin Kaydedilmesi ve Bu Verileri Hukuka Aykırı Verme, Yayma ve Ele Geçirme

Deepfake içeriklerin gerçeğe yakın bir biçimde üretilebilmesi için oldukça fazla verinin mevcut bulunması gerekir. Dolayısıyla, elde ne kadar çok veri mevcut bulunursa, o kadar gerçekçi sonuç alınır. Örneğin yüzlerin değiştirildiği bir medya içeriğinin üretilmesi için kişinin birçok açıdan yüzüne dair verinin toplanmış olması gerekir. Kişisel veri, kimliği belirli veya

delillerin değerlendirilmesi ve yargılama sürecine etkileri hakkında açıklamalar için bkz. Riana Pfefferkorn, "'Deepfakes' in the Courtroom", 2020, 29(2), Boston University Public Interest Law Journal, s. 245-276; Danielle C. Breen, "Silent No More: How Deepfakes Will Force Courts to Reconsider Video Admission Standards", 2021, 21(1), Journal of High Technology Law, s. 122-164.

[49] Durmuş Tezcan/Mustafa Ruhan Erdem/Murat Önok, Teorik ve Pratik Ceza Özel Hukuku, 18. Baskı, Seçkin Yayıncılık, 2020, s. 536.

[50] Can Yavuz, Cinsel İçerikli Görüntülerin Rıza Dışı Paylaşımı İntikam Pornosu, Ankara, Seçkin Yayıncılık, 2021, s. 128.

belirlenebilir gerçek kişiye ilişkin her türlü bilgi (6698 sayılı Kişisel Verilerin Korunması Kanunu-KVKK m. 3/1-d) olduğuna göre, derin öğrenme sürecine tabi tutulacak olan kişinin yüzüne, onun dış görünüşüne veya sesine özgü veriler de kişisel veridir.

Bu verinin hukuka aykırı olarak elde edilmesi kişisel verilerin kaydedilmesi (TCK m. 135) suçunu oluşturabileceği gibi, verilerin işlenmesi ve görüntülerin sunulması da kişisel verileri hukuka aykırı olarak verme, yayma veya ele geçirme (TCK m. 136) suçuna vücut verir.

Kişisel verilerin işlenmesi, "*kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem*" olarak tanımlanmaktadır[51]. Dolayısıyla deepfake içeriğin oluşturulmasında kullanılan verilerin işlenmesinin *kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla* gerçekleştirilmesi halinde, bu durum kişisel verilerin işlenmesi anlamına gelecek ve hukuka aykırı olarak kişisel verilerin kaydedilmesi, verilmesi, yayılması ve ele geçirilmesi suçları oluşacaktır[52].

Ç. Müstehcenlik

Deepfake teknolojisiyle, aslında müstehcen nitelikteki bir medya içeriğinde bulunmayan kişilerden elde edilen fotoğraf ve videolar kullanılarak müstehcen medya içeriklerinde bu kişiler yer almışlar gibi gösterilebilmektedir[53]. Örneğin, Harry Potter filmlerinde ünlenen oyuncu Emma Watson'ın cinsel nitelikte olmayan görüntülerinden veriler toplandığı, halihazırda cinsel nitelikte videolardaki kişilerin kafası yerine oyuncunun

---

[51] Kişisel Verilerin Korunması Kanunu (KVKK), m. 3/1-e.

[52] Mehmet Maden, Ceza Hukukunda Kişisel Verilerin Korunması, Adalet Yayınevi, 2021, s. 66: "*Kanaatimizce, yukarıda belirttiğimiz hususlar dikkate alınarak, TCK m. 135'te ve benzer şekilde m. 136'da, fiilin sınırlarını daha açık biçimde ortaya koyacak şekilde bir değişikliğe gidilebilir. Bu yapılmadığı takdirde dahi, içtihat yoluyla, yukarıda belirttiğimiz hususlar dikkate alınarak yapılacak bir yorumla, en azından KVKK'nın yürürlüğe girdiği tarihten itibaren gerçekleştirilen fiiller bakımından, KVKK m. 3 (1)-e kapsamına girmeyen fiillerin, TCK m. 135 ve m. 136 kapsamında da değerlendirilemeyeceği benimsenebilir.*"

[53] Aksoy Retornaz, s. 32, 100, 101.

kafası yerleştirilerek sahte içerikli videolar hazırlandığı belirtilmektedir[54]. Bu içeriklerin oluşturulmasında kullanılan kişiler çoğunlukla kadınlardır[55].

Oluşturulan cinsel nitelikteki deepfake medyanın içeriğinin yayımlanması müstehcenlik (TCK m. 226) suçuna vücut verebilecektir. Deepfake'in en sık kullanım alanının cinsel nitelikteki medya içeriklerinin oluşturulması olduğu ifade edilmektedir[56]. Nitekim Deeptrace adındaki bir girişimin, 2019 Temmuz'da yayımladığı rapora göre, internette 2019 Ocak-Temmuz döneminde, 14678 adet deepfake içerik bulunmuş ve bunların %96'sını cinsel nitelikteki (pornografik) medya oluşturmuştur[57].

Bu bağlamda, esasen ticari amaçlarla yetişkinlere yönelik olarak oluşturulan bir müstehcen içerikteki kişinin bedeni ile gerçekte o fotoğraf

---

[54] Citron, s. 4; Lossau, s. 3; Carl Öhman, "Introducing the Pervert's Dilemma: A Contribution to the Critique of Deepfake Pornography", 2021, February, Ethics and Information Technology, s. 2. Aynı şekilde oyuncu Gal Gadot için de benzer içerikler hazırlandığı ifade edilmektedir. Bkz. Wagner/Blewer, s. 37, 38; Douglas Harris, "Deepfake: False Pornography is Here and the Law Cannot Protect You", 2019, 17, Duke Law & Technology Review, s. 100, 109. Bu videoların hazırlanmasında çeşitli motivasyonlar etkili olabilmektedir. Bunlardan birisi, sırf bir kişiden *intikam* almak için oluşturulan sahte pornografik içeriklerin üretilmesi şeklindeki motivasyondur. Bkz. <https://www.abc.net.au/news/2019-08-30/deepfake-revenge-porn-noelle-martin-story-of-image-based-abuse/11437774> Erişim Tarihi 26.10.2019. Bu içerikler intikam pornosu ("*revenge porn*") olarak da tabir edilmektedir. Bkz. Dean Fido/Craig Harper/Mia Davis/Dominic Petronzi/Sophie Worrall, "Intrasexual Competition As a Predictor of Women's Judgements of Revenge Pornography Offending", 2019, PsyArXiv Preprints, s. 3, <https://psyarxiv.com/pwmqu/> Erişim Tarihi 17.02.2021; Walorska, s. 11; <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/405286/revenge-porn-factsheet.pdf> Erişim Tarihi 26.10.2019: "*İntikam pornosu, izni olmaksızın başkalarının utanç verici hale sokulması veya sıkıntıya neden olunması amacıyla, özel nitelikte cinsel materyallerin, fotoğraf veya videoların paylaşılmasıdır. Görüntülere bazen tam adları, adresleri ve sosyal medya profillerine bağlantılar da dahil olmak üzere konu hakkında kişisel bilgiler eşlik eder.*" Bu hususta ayrıntılı açıklama, tartışma ve örnekler için bkz. Yavuz, s. 11 vd.; Aksoy Retornaz, s. 27 vd.

[55] Aksoy Retornaz, s. 101.

[56] King/Aggarwal/Taddeo/Floridi, s. 262.

[57] Bkz. <https://deeptracelabs.com/mapping-the-deepfake-landscape/> Erişim Tarihi 11.11.2019. Aynı doğrultuda bkz. Matthew F. Ferraro/Louis W. Tompros, "New York's Right to Publicity and Deepfakes Law Breaks New Ground", 2021, 38(4), The Computer & Internet Lawyer, s. 2; Walorska, s. 7, 20. Eskiden iletişim mektup gibi araçlarla gerçekleştirilirken, günümüzde elektronik vasıtaların yaygınlaşmasıyla mahrem verilerin paylaşılması en çok bu yolla gerçekleştirilmektedir. Bu bağlamda, cinsel mahremiyet ve özerklik göz önüne alındığında, bu hususların hukuken özel bir tanınma ve korunmayı hak ettiği ifade edilmektedir. Bkz. Danielle Keats Citron, "Sexual Privacy", 2019, 128(7), Yale Law Journal, s. 1960. Nitekim günümüzde cinsel içeriklerin korunması özel bir ihtimam gerektirmekte ve deepfake bu ihlallerin aracı olarak kolay bir yol oluşturmaktadır. Bu konulara ilişkin bir ahlakilik tartışması için bkz. Öhman, s. 5-16.

veya videoda bulunmayan bir kişinin yüzünün deepfake teknolojisiyle birleştirilmesi halinde yine müstehcenlik suçunun oluşup oluşmayacağı bir sorun teşkil etmektedir. Nitekim fotoğraf ve videoda A kişisinin yüzü kullanılmakla birlikte, A'nın yüzü bir müstehcen içerik değildir. Ancak B'nin müstehcenlik içeren görüntüsüyle birleştirilmesi halinde, içerikteki kişinin A olduğu gibi bir yanıltma söz konusudur. Bu örnekte, A veya B eğer çocuksa, TCK m. 226/3 gereği, müstehcen görüntü, yazı veya sözleri içeren ürünlerin üretiminde çocukları, temsili çocuk görüntülerini veya çocuk gibi görünen kişileri[58] kullanmak suçu oluşur. Ancak A ve B, yetişkin ise, böyle bir ürünün salt üretilmesi müstehcenlik bağlamında suç teşkil etmemektedir. Böyle bir içeriğin çocuğa verilmesi, gösterilmesi; çocukların girebileceği veya görebileceği yerlerde ya da alenen gösterilmesi; içeriğine vakıf olunabilecek şekilde satışa veya kiraya arz edilmesi; bunların satışına mahsus alışveriş yerleri dışında, satışa arz edilmesi, satılması veya kiraya verilmesi; sair mal veya hizmet satışları yanında veya dolayısıyla bedelsiz olarak verilmesi veya dağıtılması; reklamının yapılması müstehcenlik suçunu oluşturmaya devam edecektir (TCK m. 226/3). Ancak ifade ettiğimiz üzere, her ne kadar deepfake olarak oluşturulmuş olsa da müstehcenlik suçu bağlamında medyada içeriğindeki kişilerin yetişkin olmaları halinde, salt üretilmeleri müstehcenlik suçuna vücut vermeyecektir. Bu hususta ceza hukuku bağlamında yapılması gerekenlere ilişkin değerlendirmeye aşağıda yer verilecektir.

D. Özel Hayatın Gizliliğini İhlal

Kişilerin özel hayatının gizliliğini ihlal eden ve kişilerin özel hayatına ilişkin görüntü veya sesleri hukuka aykırı olarak ifşa eden kimse cezalandırılmaktadır (TCK m. 134/1, 2). Bu fiillerin, deepfake teknolojisiyle gerçekleştirilmesi gündeme gelebilir. Bilhassa, cinsel nitelikteki görüntülerin deepfake medya içeriği olarak üretilmesi ve ifşa edilmesi mümkündür. Normalde müstehcen nitelikte bir medya içeriğinde bulunmayan kişilerden elde edilen fotoğraf ve videolar kullanılarak müstehcen nitelikteki medya içeriklerinde bu kişiler yer almışlar gibi gösterilmesi halinde, yüzü yer almamakla birlikte vücudu yer alan kişiler bakımından bunların ifşa edilmesi halinde, kişilerin özel hayatına ilişkin görüntü veya seslerini hukuka aykırı

[58] Deepfake teknolojisi, bilhassa "*deepweb-darknet*"te çocukların müstehcen içeriklerde kullanılması ve bunların yayılması bakımından da tehlike oluşturmaktadır. Bu hususta bir değerlendirme için bkz. Sandra Wittmer/Martin Steinebach, "Computergenerierte Kinderpornografie zu Ermittlungszwecken im Darknet", 2019, 10, MMR-Zeitschrift für IT-Recht und Recht der Digitalisierung, s. 650-653.

olarak ifşa etme suçu oluşur (TCK m. 134/2). Ancak bu halde, yüzüne yer verilen kişi bakımından bu suç oluşmamaktadır. Nitekim fotoğraf ve videoda A kişisinin yüzü kullanılmakla birlikte, A'nın yüzü "*özel hayatına ilişkin*" bir içerik değildir. Ancak B'nin müstehcenlik içeren görüntüsüyle birleştirilmesi halinde, medya içeriğindeki kişinin A olduğu gibi bir yanıltma söz konusu olmaktadır. A'nın maruz kaldığı mağduriyete karşılık olarak özel hayatın gizliliğini ihlal suçu bir koruma sağlamamaktadır[59].

E. Hakaret

Bir kimsenin onur, şeref ve saygınlığını rencide edebilecek nitelikte somut bir fiil veya olgu isnat etmek veya sövmek suretiyle bir kimsenin onur, şeref ve saygınlığına saldırmak hakaret suçunu oluşturmaktadır (TCK m. 125/1). Bu suçun, mağduru muhatap alan sesli, yazılı veya görüntülü bir iletiyle işlenmesi de mümkündür (TCK m. 125/2). Deepfake içeriklerinde aslında yer almayan kişilere yer verildiğinde veya yer aldığı durumdan farklı biçimde gösterildiğinde, söz konusu sesli ve/veya görüntülü medya içeriği o kişilerin onur, şeref ve saygınlığını rencide edici nitelikte olabilir. Örneğin, toplumda saygın bir kişiliğe sahip olan A bir fotoğrafta resmî kıyafetle yer almaktayken, genel ahlak ve adaba aykırı bir kıyafet giyen B'nin fotoğrafıyla kendi fotoğrafı manipüle edilerek, sırf A'nın saygınlığına saldırmak amacıyla B'nin kıyafetleri içinde ve bulunduğu konumda gerçekçi biçimde gösterilebilir. Bu halde, deepfake içeriklerinin üretilmesi ve kullanılması hakaret suçunu oluşturur.

[59] *Aksoy Retornaz*, manipüle edilen medya içeriğinin ticari amaçlarla yetişkinlere yönelik olarak oluşturulan bir müstehcen içerik olması hususuna değinmeksizin buradaki örnekle benzer açıklamalarından sonra, doktrinde sadece yüzü görünen kişinin mağdur olduğunun kabul edildiğini aktarmakla birlikte, yüzü yer almayan kişinin vücudunun tanınabilir olduğu durumlarda o kişinin de özel hayatın gizliliğinin ihlal edildiğinden bahsetmenin mümkün olduğunu belirtmektedir. Bkz. Aksoy Retornaz, s. 101. Manipüle edilen medya içeriğinin ticari amaçlarla yetişkinlere yönelik olarak oluşturulan bir müstehcen içerik olmaması halinde, yüzüne yer verilmeyen kişi için savunulan görüşe katılmaktayız. Ancak hem müstehcenlik suçu hem de özel hayatın gizliliğini ihlal suçu bakımından yaptığımız açıklamalar bağlamında yüzü kullanılan kişinin hangi suçtan mağdur olduğu kısmı belirtilmemektedir. Yazar, bu şekilde oluşturulan görüntülerin, TCK'da "*özel hayata ve hayatın gizli alanına karşı suçlar*" arasında ayrı bir suç olarak düzenlenmesini önerdiği "*siber alanda cinsel içerikli görüntüleri rızaya aykırı olarak ifşa etme, yayma, erişilebilir kılma veya üretme suçu*"nun (Aksoy Retornaz, s. 85) konusunu oluşturduğunu ifade etmektedir. Bkz. Aksoy Retornaz, s. 102, 115. Bu açıklamalar birlikte değerlendirildiğinde, eğer söz konusu suç ihdas edilirse, yüzü kullanılan kişinin ihdas edilecek suçta mağdur olacağını ifade edebiliriz.

F. Fikir ve Sanat Eserleriyle İlgili Manevi, Mali veya Bağlantılı Hakların İhlali Suretiyle İşlenen Suçlar

Fikir ve sanat eserleriyle ilgili manevi, mali veya bağlantılı hakların ihlali suretiyle işlenen suçlar, 5846 sayılı Fikir ve Sanat Eserleri Kanunu (FSEK) m. 71'de düzenlenmektedir. Söz gelimi, *sahibinin hususiyetini taşıyan ve ilim ve edebiyat, musiki, güzel sanatlar veya sinema eserleri olarak sayılan her nevi fikir ve sanat mahsullerinden* (FSEK m. 1/B-a) bir eseri, icrayı, fonogramı veya yapımı, hak sahibi kişilerin yazılı izni olmaksızın değiştirmek bu suçu oluşturmaktadır (FSEK m. 71/1-1). Örneğin, bir sinema filmindeki sahnenin deepfake teknolojisiyle değiştirilmesi mümkündür. Bu değişikliğin hak sahibi kişilerin yazılı izni olmaksızın yapılması halinde bu suç oluşacaktır.

G. Dolandırıcılık

Deepfake içeriklerin yanıltıcılığı, kişilerin dolandırılması amacına hizmet edebilir[60]. Bu bağlamda, dolandırıcılık suçunun bilişim sistemlerinin araç olarak kullanılması suretiyle işlenmesi nitelikli hali (TCK m. 158/1-f) irdelenmelidir.

"*Bilgisayar*" tabirinden daha geniş bir kapsamı ihtiva eden "*bilişim sistemi*" tabiri[61], TCK m. 243'te düzenlenen "*bilişim sistemine girme*" suçu bağlamında söz konusu maddenin gerekçesinde tanımlanmaktadır: "*Bilişim sisteminden maksat, verileri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tâbi tutma olanağını veren manyetik sistemlerdir.*" Bu doğrultuda, dolandırıcılık suçunun bilişim sistemlerinin araç olarak kullanılması bağlamında bilişim sisteminin, "*bilgileri otomatik olarak işleme tabi tutan manyetik sistem*" olarak ifade edildiği görülmektedir[62]. Buna karşılık, bilişim sistemlerinde manyetik sistemlerin yanında elektronik ve optik sistemlerin de kullanılmasından bahisle gerekçedeki ifade eleştirilmiştir[63].

Bilişim sistemlerinin araç olarak kullanılması suretiyle dolandırıcılık suçunun işlenmesi için, bilişim sisteminin, aldatıcılığın bir unsuru olması ve aldatıcılığı kuvvetlendirici bir araç olarak kullanılması, böylece muhatabın

---

60 Lantwin, Strafrechtliche Bekämpfung, s. 79.

61 Bu hususta açıklamalar için bkz. Murat Volkan Dülger, Bilişim Suçları ve İnternet İletişim Hukuku, 8. Baskı, Seçkin Yayıncılık, 2020, s. 66-69.

62 Bkz. Koca/Üzülmez, Özel Hükümler, s. 749.

63 Bkz. Akbulut, Bilişim Alanında, s. 110.

daha kolay aldatılabilmesi gerekir[64].

Bu bağlamda, deepfake içeriklerin, yani deepfake teknolojisinin kullanılmasıyla ortaya çıkarılan ses, görüntü ve videoların kendisinin bir bilişim sistemi olmadığını belirtmeliyiz. Ancak bu içeriklerin üretilmesi, sadece bilişim sistemlerinin kullanılmasıyla mümkündür. Keza bu içeriklerin muhataba ulaştırılabilmesi ve aldatıcılığından faydalanılabilmesi de çoğunlukla bir bilişim sistemi aracılığıyla mümkün olmaktadır. Bu sebeple dolandırıcılık suçunun işlenmesinde; (I) bu içeriklerin üretilmesi amacıyla kullanılan bilişim sisteminin dolandırıcılık suçunda araç olarak kullanılması, (II) bu içeriklerin üretilmesi amacıyla kullanılan bilişim sisteminin değil, fakat bu içerikleri muhataba ulaştırmak ve aldatıcılığı artırmak için bir bilişim sisteminin kullanılması ve (III) bir bilişim sistemi aracı kılınmaksızın deepfake içeriklerinin kullanılmasının ayrı ayrı değerlendirilmesi gerekir:

I. Eğer deepfake içeriklerinin üretilmesi amacıyla kullanılan bilişim sistemi, dolandırıcılık suçunun işlenmesinde araç olarak kullanılıyorsa, bilişim sistemlerinin araç olarak kullanılması suretiyle dolandırıcılık suçunun işlendiği kabul edilmelidir (TCK m. 158/1-f). Bu hususta bir somut örneğe aşığa yer verilecektir.

II. Deepfake içeriklerinin muhataba ulaştırılması ve aldatıcılık etkisinin gösterebilmesi için başka bir bilişim sisteminin kullanıldığı durumlarda da bilişim sistemlerinin araç olarak kullanılması suretiyle dolandırıcılık suçunun işlendiği kabul edilmelidir (TCK m. 158/1-f). Yani deepfake içerikleri bir bilişim sisteminde üretilmiş ve fakat başka bir bilişim sistemi araç olarak kullanılarak dolandırıcılık suçu işlenmiş olabilir. Örneğin, A, kendi ev bilgisayarında deepfake içerik üretiyor ve bu içeriği X internet sitesine yüklemek suretiyle internet sitesini (bu bilişim sistemini) dolandırıcılık suçunun işlenmesinde araç olarak kullanıyor olabilir.

III. Bir bilişim sistemi aracı kılınmadan deepfake içerikler kullanılarak muhatap aldatılmışsa, bilişim sistemlerinin araç olarak kullanılması suretiyle dolandırıcılık suçunun işlendiğinden bahsedilemez. Örneğin, bir fotoğraf, bilişim sistemi kullanılarak deepfake teknolojisiyle manipüle edilerek ona aldatıcılık özelliği kazandırılmış olabilir. Ancak bu fotoğraf, fizikî bir kâğıda basılarak muhataba sunulmuş ve kişi aldatılmış olabilir. Bu durumda, sırf söz konusu fotoğrafın üretilmesinde bilişim sistemlerinin kullanılmış olması,

[64] Bkz. Dülger, Bilişim Suçları, s. 521.

dolandırıcılık suçunun bilişim sistemlerinin araç olarak kullanılması suretiyle işlendiği anlamına gelmemektedir. Bu örnekte, somut olayda başka bir nitelikli hal söz konusu değilse, dolandırıcılık suçunun temel halinden (TCK m. 157/1) sorumluluk söz konusudur.

Deepfake içerik üretme ve kullanmayla ilgili olarak, deepfake içeriklerinin üretilmesi amacıyla kullanılan bilişim sisteminin dolandırıcılık suçunun işlenmesinde araç olarak kullanıldığı bir olay Mart 2019'da yaşanmıştır[65]. Olayda, fail, bir enerji firmasının ana şirketinin başındaki yöneticiymiş gibi alt şirketin yetkilisiyle telefonla konuşur. Fail, görüşme esnasında sesinin şirketin başındaki yöneticiymiş gibi çıkması için yapay zekâ teknolojisini kullanır. Dolayısıyla telefonun karşısındaki kişi, konuştuğu kişinin kendi patronu olduğunu düşünür. Fail, 220.000 Euro'nun belirttiği hesaba acilen aktarılmasını talep eder. Aldatılan yönetici ise bu talebi yerine getirir. Bu olayda, yapay zekânın kullanımıyla bir deepfake içerik üretimi ve içeriğin üretilmesiyle birlikte o anda kullanımı söz konusudur. Söz konusu deepfake içeriğinin gerçekçiliğiyle birlikte aldatıcılığı oldukça artmaktadır. Deepfake teknolojisinde anlık olarak görüntülerin manipüle edilebilmesiyle birlikte, bu olaya benzer biçimde, uzaktan görüntülü konuşma gerçekleştirilmesi suretiyle de dolandırıcılık suçunun işlenmesi gündeme gelecektir. Bu durumlarda, bilişim sistemlerinin araç olarak kullanılması suretiyle dolandırıcılık suçunun işlenmesi söz konusu olur (TCK m. 158/1-f).

Ğ. Seçimlerde Yasak Propaganda

298 sayılı Seçimlerin Temel Hükümleri ve Seçmen Kütükleri Hakkında Kanun m. 151'e göre; *oy verme gününden önceki günün saat 18.00'inden sonra ve oy verme gününde* umumi veya umuma açık yerlerde seçim propagandası için toplantı veya propaganda yapmak veya bu maksatla yayınlarda bulunmak veya *ne suretle olursa olsun seçimin düzenini bozabilecek veya oy vermenin tam bir serbestlikle yapılmasına tesir edebilecek mahiyette söz, yazı veya sair suretlerle propaganda yapmak* veya *asılsız şayialar çıkarmak* cezalandırılmaktadır.

Hükümde yer alan, "*oy verme gününden önceki günün saat 18.00'inden sonra ve oy verme gününde*" ifadesinin, sadece "*umumi veya umuma açık*

[65] Söz konusu olay, telefonla Almanya'dan arıyormuş görüntüsü verilerek İngiltere'den aramak suretiyle ve paranın Macaristan'a ve oradan Meksika'ya aktarılması şeklinde birden fazla ülkeyi ilgilendiren biçimde yaşanmıştır. Ayrıntıları için bkz. <https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402> Erişim Tarihi 12.03.2021; Walorska, s. 20.

yerlerde seçim propagandası için toplantı veya propaganda yapmak veya bu maksatla yayınlarda bulunmak" bakımından mı geçerli olduğu, yoksa aynı zamanda "*ne suretle olursa olsun seçimin düzenini bozabilecek veya oy vermenin tam bir serbestlikle yapılmasına tesir edebilecek mahiyette söz, yazı veya sair suretlerle propaganda yapmak* veya *asılsız şayialar çıkarmak*" fiillerini de mi kapsadığı metinden anlaşılamamaktadır.

Deepfake içerikleriyle siyasal güvenliğin tehlikeye atılması ve seçimlerin haksız yönlendirilmeleri söz konusu olabilir[66]. Deepfake içerik üretmek-kullanmak suretiyle seçimi etkilemeye çalışmak amacıyla gerçekleştirilen davranış, "*ne suretle olursa olsun seçimin düzenini bozabilecek veya oy vermenin tam bir serbestlikle yapılmasına tesir edebilecek mahiyette söz, yazı veya sair suretlerle propaganda yapmak* veya *asılsız şayialar çıkarmak*" niteliğinde olacağından, eğer davranışın "*oy verme gününden önceki günün saat 18.00'inden sonra ve oy verme gününde*" gerçekleştirilmesi şartı bu fiil bakımından geçerli değilse, bu düzenlemenin deepfake içeriklerinin üretilmesi-kullanılması suretiyle seçimi manipüle etmek bakımından genel mahiyette bir düzenleme olduğu söylenebilir. Aksi halde, deepfake içeriklerinin üretilmesi-kullanılması suretiyle seçimi manipüle etmek bakımından bu hüküm etkili bir koruma sağlamamaktadır.

H. Diğer Suçlar

Deepfake teknolojisiyle üretilen içeriklerin kullanım şekline göre başka suçlar da gündeme gelebilir. Bilhassa beyanda bulunma suretiyle işlenebilen suçların gündeme geleceğini belirtmeliyiz. Bunlardan bazılarını; 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), suç işlemek amacıyla örgüt kurma (propaganda) (TCK m. 220/8), halkı askerlikten soğutma (TCK m. 318), terör propagandası (Terörler Mücadele Kanunu-TMK m. 7/2) suçları şeklinde sayabiliriz.

I. Deepfake İçeriklerin Üretilmesi ve Kullanılması Suretiyle İşlenen Suçlarda Suçun İşlendiği Yerin Tespiti Sorunu

Ceza kanunlarının yer bakımından uygulanması suçun işlendiği yere göre belirlenmekle birlikte özellikle suçun bilişim sistemleri aracılığıyla işlenmesi

[66] Kamshad Mohsin, "Yapay Zekânın Düzenlenmesi ve Yapay Zekâ Suçları" in Jülide Yaşar (Çev.), Yener Ünver (Ed.), Karşılaştırmalı Güncel Ceza Hukuku Serisi 21, Ceza Hukukunda Robot, Yapay Zeka ve Yeni Teknolojiler, Seçkin Yayıncılık, 2021, s. 231.

halinde suçun işlendiği yerin tespitine dair farklı görüşler bulunmaktadır.

Bu hususta bir görüşe göre, internet ortamında yapılan yayın yoluyla işlenen suçlarda internet ortamındaki içeriğe ulaşılabilen her yerde suç işlenmektedir[67]. Diğer görüş, suç teşkil eden içeriğin Türkiye'de bir yer sağlayıcıya veya bilgisayara yüklenmesi halinde suçun Türkiye'de işlendiğini belirtmektedir[68]. Bir başka görüş ise, içerik sağlayıcının bulunduğu yer ile yer sağlayıcının yer sağlama hizmetini sunduğu yerin suçun işlendiği yer olduğunu kabul etmektedir[69]. Kanaatimizce internetin hemen her ülkede ulaşılabilir olması sebebiyle, internet ortamında yapılan yayın yoluyla işlenen suçlarda internet ortamındaki içeriğe ulaşılabilen her yerde suçun işlendiğini kabul etmek bütün bu ülkelerin ceza kanunlarının uygulanabilmesi sorununu doğuracaktır. Bu sebeple, bilişim sistemleri aracılığıyla işlenen suçlarda içerik sağlayıcının bulunduğu yer ile yer sağlayıcının yer sağlama hizmetini sunduğu yeri suçun işlendiği yer olarak kabul etmek gerekir[70].

Deepfake içeriklerinin yoğun bilişim sistemi faaliyetini gerektirmesi sebebiyle, deepfake içerikleriyle işlenen suçlarda suçun işlendiği yer sorunu, bu içeriklerin yayılmasının "*deep web*"[71] ağına dahil yer ve içerik sağlayıcılarca

---

[67] Kayıhan İçel, Ceza Hukuku Genel Hükümler, Yenilenmiş Bası, Beta Yayıncılık, 2016, s. 161; İzzet Özgenç, Türk Ceza Hukuku Genel Hükümler, 16. Bası, Seçkin Yayıncılık, 2020, s. 1010, dn. 3; M. Emin Artuk/Ahmet Gökcen/M. Emin Alşahin/Kerim Çakır, Ceza Hukuku Genel Hükümler, 11. Baskı, Adalet Yayınevi, 2017, s. 1022; Hasan Sınar, "İnternetin Ortaya Çıkardığı Hukuki Sorunlara Bir Ceza Hukuku Yaklaşımı", 2001, 17(1-2), Milletlerarası Hukuk ve Milletlerarası Özel Hukuk Bülteni, s. 370.

[68] Durmuş Tezcan/Mustafa Ruhan Erdem/Murat Önok, Uluslararası Ceza Hukuku, 4. Baskı, Seçkin Yayıncılık, 2017, s. 100; Demirbaş, Timur, Ceza Hukuku Genel Hükümler, 11. Baskı, Seçkin Yayıncılık, 2016, s. 151.

[69] Berrin Akbulut, Ceza Hukuku Genel Hükümler, 4. Baskı, Adalet Yayınevi, 2017, s. 136; Veli Özer Özbek/ Koray Doğan/Pınar Bacaksız/İlker Tepe, Türk Ceza Hukuku Genel Hükümler, 7. Baskı, Seçkin Yayıncılık, 2016, s. 153; Veli Özer Özbek, "İnternet Kullanımında Ortaya Çıkabilecek Bazı Ceza Hukuku Sorunları", 2002, 4(1), Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, s. 127, 128.

[70] Beşir Babayiğit, Kumar Oynanması İçin Yer ve İmkân Sağlama Suçu, Adalet Yayınevi, 2021, s. 229. Kural olarak bu şekilde ifade etmekle birlikte, işlenen her suç bakımından fiilin kısmen veya tamamen işlendiği yer ile neticenin gerçekleştiği yer değerlendirmesinin yapılması gerekir (TCK m. 8/1). Bu suçlarda, internet ortamında gerçekleştirilen bir yayının, yayının yapıldığı ülke dışındaki bir ülkede sonuç doğurmuş sayılması için, yani neticenin diğer ülkede gerçekleştiğinin kabul edilmesi için, söz konusu yayının doğrudan o ülkeye yönelik yapıldığını gösteren somut bağlantı noktalarının bulunmasının gerektiği ifade edilmektedir. Bkz. İzzet Erdem Külçür, Ceza Hukukunda Yer Bakımından Uygulama, On İki Levha Yayıncılık, 2017, s. 210

[71] Deep web, günlük olarak kullanılan ve internete erişimi olan herkesin girebildiği internet

gerçekleştirilmesi söz konusu olduğunda daha çok gündeme gelecek, muhakeme sürecinde içeriğin nerede bulunduğu ve nereden yayıldığının tespiti de zorlaşacaktır[72].

V. ÜLKELERİN DEEPFAKE'İN TEHLİKELERİNE KARŞI MÜCADELE YÖNTEMLERİ

Deepfake'in tehlikelerine karşı mücadele çok yönlü bir süreci ifade etmektedir. Hak ihlalleri sebebiyle hukuki mücadele yöntemleri kullanılmak istenmekle birlikte, deepfake'in esasen teknolojik bir olgu olması sebebiyle yine teknoloji vasıtasıyla bir mücadelenin yürütülmesi söz konusu olmaktadır. Ceza hukuku yaptırımlarının son çare olma özelliği göz önünde bulundurulduğunda deepfake'in tehlikelerine karşı teknolojik mücadeleye öncelikle başvurulması gerektiğini ifade edebiliriz[73]. Bu sebeple, ilk olarak bu hususa kısaca yer vermekte fayda görmekteyiz. Ardından deepfake'in tehlikelerine karşı hukuki mücadele ele alınacaktır.

---

ağından farklı olarak, Invisible Internet Project (I2P) ve The Onion Router (TOR) gibi protokol ve araçlarla erişimin mümkün olduğu internet ağını ifade etmektedir. TOR ağına bağlanmak suretiyle erişilebilir olan "*.onion*" uzantılı bu internet siteleri, klasik arama motorlarında indekslenmediği için buralara ulaşmak teknik bilgi gerektirmekte ve ulaşım zorlukları çıkarmaktadır. Keza içerik sağlayıcılar kişisel bilgisayarlarını bu internet sitelerinin oluşturulmasında yer sağlama amacıyla kullanabildiklerinden, bilgisayarların kapalı olması halinde siteye erişim de söz konusu olamamaktadır. Ayrıca bu ağda, gerçek kişiler üzerinden ağa bağlanma söz konusu olduğundan internete bağlanarak bir internet sitesine erişen kişinin hangi IP adresine sahip olduğunu bilmek neredeyse imkânsız hale gelmektedir. Bu hususta bir inceleme için bkz. Göktuğ Sönmez/Emine Çelik, "Anonimlik ile İllegalite Arasında: Deep Web, Dark Web ve Devlet Dışı Silahlı Aktörlerin Uluslararası Siber Faaliyetleri", 2020, 22(1), Güvenlik Çalışmaları Dergisi, s. 66-88.

[72] Bilişim sistemleriyle işlenen suçların genel mahiyeti olarak bu suçların soruşturulması, failin tespiti ve suçun ispatı gibi hususların zorluk arz ettiği kabul edilmektedir. Bkz. Mehmet Bedii Kaya, Teknik ve Hukuki Boyutlarıyla İnternete Erişimin Engellenmesi, On İki Levha Yayıncılık, 2010, s. 36, 44, 81; Dülger, Bilişim Suçları, s. 103, 646; Emre İkbal Açıkgöz, Bilişim Sistemi Aracılığıyla Haksız Yarar Sağlama Suçu, Adalet Yayınevi, 2020, s. 36. Bu sorun, uluslararası adli yardımlaşma ve suçluların iadesi prosedürleri çerçevesinde çözüme kavuşturulmaya çalışılacaktır. Ancak deepfake içerikleriyle işlenen suçlarda bu sorunun özünü teşkil eden husus teknik ve teknolojik olup sorunun çözümü uzmanlık gerektirmekte ve bilirkişi incelemesi önem kazanmaktadır. Nitekim söz konusu içeriklerin nerede bulunduğu ve yayına sunulduğunun tespiti bilişim sistemlerine yönelik incelemelerle ortaya çıkabilir.

[73] Lantwin, Rechtliche Herausforderungen, s. 577. Keza deepfake'in tehlikelerine karşı mücadelenin yalnızca ceza hukuku yoluyla yürütülemeyeceği, ceza hukukunun teknik tespit yöntemlerine ve sosyal bilinçlenmeye ek olarak başvurulabilecek araçlardan sadece biri olduğu ifade edilmektedir. Bkz. Lantwin, Strafrechtliche Bekämpfung, s. 82.

A. Teknolojik Mücadele

Deepfake'in tehlikeleriyle mücadelenin hukuki, eğitimsel[74] ve teknolojik[75] olarak yapılması gerektiği ifade edilmektedir[76]. Deepfake içeriklerle hukuken mücadele edilmesi önemli olmakla birlikte[77], bunun tek başına yetersiz olacağı da açıktır[78]. Nitekim aşağıda ele alınacağı üzere, bu konuda hukuki düzenlemeler yapılmaya çalışılmaktadır. Diğer yandan, mücadelenin teknolojik açıdan da yapılması gerekir.

Deepfake teknolojisi geliştikçe bu teknolojiyle üretilen içeriğin tespitine yönelik teknoloji de gelişmektedir. Bu kapsamda örneğin, yüz ifadeleriyle

---

[74] "*Eğitim*" alanı, eğitimcilerin uzmanlık alanı olmakla birlikte, genel anlamda eğitimsel mücadeleyi, başta eğitim-öğretimin her kademesinde yapay zekâ teknolojilerine ilişkin bilgilerin öğrencilere verilmesi ve bunun dışında da diğer kamusal ve özel eğitim alanlarında bu hususta toplumun bilinçlendirilmesi şeklinde ifade edebiliriz. Söz gelimi, yapay zekâ ve deepfake hususunda bilgilendirici kamu spotları oluşturulabilir.

[75] Çalışmanın kapsamını aşması sebebiyle teknolojik mücadele yöntemlerine ayrıntılı olarak yer verilmeyecek olup çalışmayı tamamlayıcı mahiyette olması amacıyla başlıca bazı teknolojik mücadele yöntemlerine yer verilmekle yetinilecektir. Her ne kadar teknolojik mücadelenin ceza muhakemesini ilgilendiren yönleri bulunuyor olsa da bu hususun başka bir çalışmanın konusunu oluşturması daha isabetli olacaktır. Deepfake içeriklerinin yargı mercileri önüne gelmesiyle birlikte, delillerin değerlendirilmesi ve yargılama sürecine etkileri hakkında açıklamalar için bkz. Pfefferkorn, Deepfakes in the Courtroom, s. 245-276; Breen, How Deepfakes Will Force Courts to Reconsider Video Admission Standards, s. 122-164.

[76] Ayrıntıları için bkz. Alexa Koenig, "'Half the Truth is Often a Great Lie': Deep Fakes, Open Source Information, and International Criminal Law", 2019, 113, American Journal of International Law, s. 253-255. Deepfake'in tehlikelerine karşı mücadelede ayrıca şu yöntemlerin kullanılması önerilmektedir: medya okuryazarlığının teşvik edilmesi, meşru gazeteciliğin öneminin kavranması, gerçekleri denetleyen kuruluşların oluşturulması, deepfake içerikleri saptamak için ileri teknoloji kullanılması, açık ve şeffaf politikalar oluşturan internet şirketlerinin varlığı, sahte haberleri önlemek için raporlama prosedürleri ve yanlış bilgi ve dezenformasyonun yayılmasına sebep olan finansal teşvikleri azaltan algoritmalardan yararlanılması. Bkz. Holly Kathleen Hall, "Deepfake Videos: When Seeing Isn't Believing", 2018, 27(1), Catholic University Journal of Law and Technology, s. 75, 76.

[77] Deepfake gibi sahteliklerin önlenmesi için mevzuatın hızla gelişen teknolojiye göre güncellenmesi gerektiği ifade edilmektedir. Bkz. Ashu M. G. Solo, "Combating Online Defamation and Doxing in the United States", 2019, The 20th International Conference on Internet Computing and Internet of Things, s. 75, 76, <https://www.researchgate.net/publication/334604707_Combating_Online_Defamation_and_Doxing_in_the_United_States/link/5d35856ba6fdcc370a5495c3/download> Erişim Tarihi 24.10.2019; Rebecca A. Delfino, "Pornographic Deepfakes: The Case for Federal Criminalization of Revenge Porn's Next Tragic Act", 2019, 88(3), Fordham Law Review, s. 903, 904.

[78] Marc Jonathan Blitz, "Lies, Line Drawing, and (Deep) Fake News", 2018, 71(1), Oklahoma Law Review, Symposium: Falsehoods, Fake News, and the First Amendment, s. 116; Lantwin, Rechtliche Herausforderungen, s. 577.

baş hareketleri arasındaki korelasyonun, bir insanı diğer insanlardan ayırmada olduğu gibi, gerçek videoları deepfake videolardan ayırmak için kullanılabileceği ifade edilmekte ve bunun yöntemleri açıklanmaya çalışılmaktadır[79]. Yöntemlerden biri de dijital filigran uygulamasıdır[80]. Herhangi bir cihazda bir fotoğraf veya video çekildiğinde, ne zaman çekildiğini belirten dijital filigranla bu fotoğraf veya video otomatik olarak etiketlenebilmektedir. Böylece söz konusu içeriğin deepfake medya içeriği olup olmadığı anlaşılabilmektedir[81].

Ayrıca belirtmek gerekir ki, özellikle sahte içerikle üretilen siyasi konuşmaların sebebi olarak, statükonun baskıcı tutumu ve azınlık konumunda

---

[79] Bu ve benzer teknik tespit yöntemleri için bkz. Shruti Agarwal/Hany Farid/Yuming Gu/ Mingming He/ Koki Nagano/Hao Li, "Protecting World Leaders Against Deep Fakes", 2019, The IEEE Conference on Computer Vision and Pattern Recognition (CVPR) Workshops 2019, s. 38-45, <https://openaccess.thecvf.com/content_CVPRW_2019/papers/Media%20Forensics/Agarwal_Protecting_World_Leaders_Against_Deep_Fakes_CVPRW_2019_paper.pdf> Erişim Tarihi 24.10.2019. Aynı amaçla ortaya koyulan çalışmalar için bkz. Umut Aybars Ciftci/ İlke Demir/Lijun Yin, "FakeCatcher: Detection of Synthetic Portrait Videos using Biological Signals", 2019, arXiv:1901.02212, s. 1-14, <https://arxiv.org/pdf/1901.02212v2.pdf> Erişim Tarihi 24.10.2019; Luciano Floridi, "Artificial Intelligence, Deepfakes and a Future of Ectypes", 2018, 31(3), Philosophy & Technology, s. 317-321; David Güera/ Edward J. Delp, "Deepfake Video Detection Using Recurrent Neural Networks", 2018, 5th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS), s. 1-6, <https://ieeexplore.ieee.org/document/8639163> Erişim Tarihi 24.10.2019; Haya R. Hasan/Khaled Salah, "Combating Deepfake Videos Using Blockchain and Smart Contracts", 2019, 7, IEEE Access, s. 41596-41606, <https://ieeexplore.ieee.org/document/8668407> Erişim Tarihi 24.10.2019; Marissa Koopman/Andrea Macarulla Rodriguez/Zeno Geradts, "Detection of Deepfake Video Manipulation", 2018, The 20th Irish Machine Vision and Image Processing Conference, IMVIP 2018, s. 133-136, <https://www.researchgate.net/publication/329814168_Detection_of_Deepfake_Video_Manipulation/link/5c1bdf7da6fdccfc705da03e/download> Erişim Tarihi 25.10.2019; Pavel Korshunov/Sebastien Marcel, "Vulnerability Assessment and Detection of Deepfake Videos", 2019, Idiap Publications, The Idiap Research Institute, s. 1-6, <http://publications.idiap.ch/downloads/papers/2019/Korshunov_ICB_2019.pdf> Erişim Tarihi 24.10.2019; Yuezun Li/Siwei Lyu, "Exposing DeepFake Videos By Detecting Face Warping Artifacts", 2019, arXiv:1811.00656v3, s. 46-52, <https://arxiv.org/abs/1811.00656> Erişim Tarihi 24.10.2019; Thanh Thi Nguyen/Cuong M. Nguyen/Dung Tien Nguyen/Duc Thanh Nguyen/Saeid Nahavandi, "Deep Learning for Deepfakes Creation and Detection", 2019, arXiv:1909.11573, s. 1-16, <https://arxiv.org/abs/1909.11573> Erişim Tarihi 24.10.2019; Ekraam Sabir/Jiaxin Cheng/Ayush Jaiswal/Wael AbdAlmageed/Iacopo Masi/Prem Natarajan, "Recurrent Convolutional Strategies for Face Manipulation Detection in Videos", 2019, arXiv:1905.00582v3, s. 80-87, <https://arxiv.org/abs/1905.00582v3> Erişim Tarihi 24.10.2019.

[80] Lossau, s. 3.

[81] Bkz. <https://jsis.washington.edu/news/deep-fakes-fake-news-and-what-comes-next/> Erişim Tarihi 12.12.2019; Lossau, s. 3.

olanlara özgürce konuşma ortamının sağlanmaması gösterilmektedir. Bu da deepfake içeriklerin ortaya çıkmasında bir etken olarak görülmekte ve ifade özgürlüğünün siyasi deepfake içeriklerin oluşturulmasını azaltacağı savunulmaktadır[82].

B. Hukuki Mücadele

Deepfake, ülkelerin suç siyaseti bağlamında ele alınması gereken bir olgu halini almaya başlamıştır. Bu çalışmada, deepfake'in tehlikelerine karşı hukuki mücadelede temel olarak ABD'deki hukuki gelişmeler ele alınacaktır. Zira ABD'de bu konuda somut hukuki adımlar atılmış ve atılmaya devam etmektedir[83]. Avrupa Birliği (AB) müktesebatı bakımından ise, Yapay Zekâ ve Robotik Üzerine Kapsamlı Bir Avrupa Sanayi Politikası Hakkında 12 Şubat 2019 Tarihli Avrupa Parlamentosu Kararı ile yapay zekâya ilişkin 21.04.2021 tarihli regülasyon teklif belgesine değinilecektir.

1. Amerika Birleşik Devletleri'nde Deepfake'in Tehlikelerine Karşı Hukuki Mücadele

Dünyada deepfake'in tehlikelerine karşı hukuki mücadelede başı çeken ülke ABD olmuştur[84]. Bu bağlamda ilk olarak Virginia'da bazı

---

[82] Bkz. Mary Anne Franks/Ari Ezra Waldman, "Sex, Lies, and Videotape: Deep Fakes and Free Speech Delusions", 2019, 78(4), Maryland Law Review, s. 897, 898.

[83] Diğer ülkelerde henüz deepfake özelinde hukuki düzenlemelere yer verilmediği görülmektedir. Örneğin İngiltere, Almanya, Fransa ve Kanada'da deepfake'ten kaynaklanan hak ihlallerinde hukuki yaptırımlar bakımından mevcut hükümler çerçevesinde hareket edildiği, henüz deepfake'e yönelik ayrı bir düzenleme getirilmediği belirtilmektedir. Çin'de, deepfake içeriklerin engellenmesi için çalışmaların yürütüldüğü ifade edilmektedir. Bu değerlendirmeler için bkz. Lantwin, Rechtliche Herausforderungen, s. 576; Lantwin, Strafrechtliche Bekämpfung, s. 78-82; Walorska, s. 28; Waldemarsson, s. 15-20; Penelope Thornton/ Patrick Fromlowitz/Aissatou Sylla/Rachel Fleeson/Margaret K. Pennisi, "Deepfakes: An EU and U.S. Perspective", 2020, Spring/Summer, Hogan Lovells-Global Media Technology and Communications Quarterly (GMCQ), s. 31, 32; Penelope Thornton/ Aissatou Sylla/Patrick Fromlowitz, "The War against Deepfakes", 2020, Managing Intellectual Property, 285, s. 29-30; <https://www.reuters.com/article/us-china-technology/china-seeks-to-root-out-fake-news-and-deepfakes-with-new-online-content-rules-idUSKBN1Y30VU> Erişim Tarihi 30.11.2019; B. J. Siekierski, Deep Fakes: What Can Be Done About Synthetic Audio and Video?, Brief Series Publication No. 2019-11-e, Canada, Library of Parliament, 2019, s. 2, 3; <https://www.berliner-zeitung.de/zukunft-technologie/deepfake-technologien-china-verbietet-mit-kuenstlicher-intelligenz-kreierte-fake-news-li.2380> Erişim Tarihi 12.03.2021.

[84] Burada deepfake için özel olarak getirilen veya getirilecek olan düzenlemelere yer verilecek olup bu hükümler dışındaki mevcut hükümler çerçevesinde ABD mevzuatına göre deepfake'in değerlendirmesi için bkz. Delfino, s. 904 vd.

deepfake içeriklerin hukuka aykırı olarak satılması ve yayılması suç haline[85] getirilmiştir. Bu suç; "*Code of Virginia*"da suçların düzenlendiği bölümde ahlaka ilişkin suçlar arasında yer alan müstehcenlik suçlarından biri olarak düzenlenen "*hukuka aykırı olarak başkasının görüntüsünü satmak veya yaymak*"[86] suçudur. "*Hukuka aykırı olarak başkasının görüntüsünü satmak veya yaymak*" suçunda, kişilerin sahte olmayan müstehcen görüntülerinin tehdit veya taciz etmek için satılması veya yayılması cezalandırılmaktaydı. 18 Mart 2019 tarihli değişiklikle suç tanımına bir cümle ve fıkra eklenmiştir[87]. Söz konusu ekleme ile birlikte, kişilerin müstehcen nitelikteki sahte olarak oluşturulan görüntüleri de suçun konusunu oluşturmaktadır.

Deepfake'in seçimleri etkileme tehlikesine karşı mücadelede ilk hukuki düzenleme[88] ise Teksas'ta 1 Eylül 2019'da yürürlüğe girmiştir. Teksas 751 sayılı kanun tasarısının kabulüyle birlikte, Teksas Seçim Kanunu'nun[89] 255.004 numaralı maddesi değiştirilmiştir[90]. Söz konusu değişiklikle birlikte, seçime katılan adaylara zarar vermek veya seçimin sonucunu etkilemek amacıyla; deepfake video oluşturmak veya seçimi takip eden 30 gün içinde bu nitelikteki deepfake videonun yayınlanması ya da dağıtılmasına sebep olmak suç haline getirilmiştir[91]. Madde bağlamında "*deep fake video*" tabiri,

---

[85] Hafif ve ağır suç (misdemeanor-felony) ayrımına girilmeksizin söz konusu davranışların ceza hukuku yaptırımına tabi tutulmaları ve karşılığında hapis cezası öngörülmeleri sebebiyle çalışmada bunlar "*suç*" olarak ifade edilecektir.

[86] Code of Virginia, § 18.2-386.2. Bkz. <https://law.lis.virginia.gov/vacode/title18.2/chapter8/section18.2-386.2/> Erişim Tarihi 12.03.2021. Bu suç, "*Class 1 misdemeanor*" olarak sınıflandırılmaktadır. Code of Virginia'ya göre "*Class 1 misdemeanor*" olarak sınıflandırılan haksızlıkların yaptırımı, "*on iki aydan fazla olmayan hapis cezası ve 2,500 dolardan fazla olmayan para cezası, bunlardan biri veya her ikisi*"dir. Bkz. <https://law.lis.virginia.gov/vacode/title18.2/chapter1/section18.2-11/> Erişim Tarihi 12.03.2021.

[87] Değişiklik tasarısı metni için bkz. <https://lis.virginia.gov/cgi-bin/legp604.exe?191+ful+CHAP0490> Erişim Tarihi 13.03.2021. Hüküm, 1 Temmuz 2019'da yürürlüğe girmiştir. Bkz. Ferraro, s. 15. Söz konusu düzenlemeyi yapmaya iten olaya, yukarıda bahsettiğimiz "*DeepNude*" adlı programın sebep olduğu belirtilmektedir. Virginia'da öncelikle bu program yasaklanmış ve ardından deepfake'in tehlikelerine karşı mücadele etmek amacıyla düzenleme yapmak yoluna gidilmiştir. Bkz. Ferraro, s. 15.

[88] Ferraro, s. 14.

[89] "*Election Code*", bkz. <https://statutes.capitol.texas.gov/?link=EL> Erişim Tarihi 13.03.2021.

[90] Bkz. <https://capitol.texas.gov/tlodocs/86R/billtext/html/SB00751F.htm> Erişim Tarihi 13.03.2021; <https://statutes.capitol.texas.gov/Docs/EL/htm/EL.2.htm#2.055> Erişim Tarihi 13.03.2021.

[91] Teksas Seçim Kanunu, 255.004.d; Sukhodolov/Bychkov/Bychokova, s. 210. Bu suç, "*Class A misdemeanor*" olarak sınıflandırılmaktadır. Teksas Ceza Kanunu'na göre "*Class*

bir kişinin aslında gerçekleştirmediği bir davranışı gerçekleştiriyormuş gibi gösteren ve aldatma amacıyla oluşturulan videoları ifade etmektedir[92].

Deepfake içeriklerin oluşturulmasına yönelik suç ihdasına ilişkin olarak Massachusetts'te 22.01.2019 tarihinde H.3366 sayılı kanun tasarısı sunulmuştur[93]. Söz konusu suç tanımına göre; dağıtmak amacıyla deepfake içerikleri oluşturmak veya görsel-işitsel bir kaydın deepfake içerik olduğu bilinmesine rağmen bir suçun işlenmesini ya da haksız bir davranışın gerçekleştirilmesini kolaylaştırmak amacıyla bunları dağıtmak cezalandırılacaktır[94]. Madde bağlamında "*görsel-işitsel kayıt*" tabiri; elektronik formattaki her türlü işitsel veya görsel medya içeriği ve her türlü fotoğrafı, sinema filmini, video kaydını, elektronik görüntüyü veya ses kaydını ifade etmektedir. Madde bağlamında "*deep fake*" tabiri ise; makul bir gözlemciye göre içeriğinin bir kişinin gerçek konuşması veya davranışıymış gibi algılanacak şekilde sahte olarak oluşturulmuş veya değiştirilmiş görsel-işitsel kayıtları ifade etmektedir[95].

Kaliforniya'da da deepfake'in tehlikelerine karşı hukuki düzenleme yapılması hususunda adımlar atılmaktadır. 29.02.2019 yayın tarihli ve 1280 sayılı, 10.04.2019 yayın tarihli ve 730 sayılı kanun tasarılarıyla[96] birlikte, deepfake içerikleri başkalarına dağıtmak, sergilemek veya başkalarıyla değiş tokuş yapmak veya deepfake içerikleri başkalarına dağıtmayı, sergilemeyi veya başkalarıyla değiş tokuş etmeyi teklif etmek suç olarak tanımlanacaktır[97]. Ayrıca, seçime katılan adayların itibarını zedelemek veya bir seçmeni

A misdemeanor" olarak sınıflandırılan haksızlıkların yaptırımı, "*4,000 doları aşmayan bir para cezası veya bir yılı geçmemek üzere hapis cezası ya da hem para cezası hem de hapis cezası*"dır. Bkz. < https://statutes.capitol.texas.gov/Docs/PE/htm/PE.12.htm#12.02> Erişim Tarihi 13.03.2021.

92 Teksas Seçim Kanunu, 255.004.e.

93 Söz konusu tasarı henüz kanunlaşmamıştır. Bkz. <https://malegislature.gov/Bills/191/H3366> Erişim Tarihi 31.05.2021.

94 H.3366 sayılı tasarı vasıtasıyla ihdas edilecek General Laws, 266, 37E 1/2. (b) numaralı maddesi. Suçun yaptırımı, "*5.000 dolardan fazla olmayan para cezası veya iki buçuk yıldan fazla olmayan hapis veya bu tür para cezası ve hapis cezası*"dır.

95 H.3366 sayılı tasarı vasıtasıyla ihdas edilecek General Laws, 266, 37E 1/2. (a) numaralı maddesi.

96 Bkz.<https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB1280> Erişim Tarihi 31.05.2021; <https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB730> Erişim Tarihi 31.05.2021.

97 1280 sayılı kanun tasarıyla Kaliforniya "*Penal Code*"a eklenmesi teklif edilen 644. madde.

aday lehine veya aleyhine oy vermesi için kandırmak amacıyla deepfake içeriklerinin kullanılması yasaklanacaktır[98].

Deepfake hususunda geniş kapsamlı[99] kanun tasarısı ise, "*United States Code*"a yönelik olarak "*İnsanların Sömürü Öznesi Yapılmasından Kişilerin Sorumlu Tutulması Bağlamında Sahte Görünümlerden Korunması Kanunu*"[100] adıyla 12.06.2019 tarihinde sunulan kanun tasarısıdır[101].

Kanunun kısa adı "*DEEP FAKES Accountability Act*" (DAA) şeklindedir (DAA m. 1). Kanunun amacı, deepfake teknolojisi kullanılarak ortaya çıkan dezenformasyonun yayılmasıyla mücadele etmektir.

Tasarıda yer alan tanıma[102] göre deepfake; *esasen görüntü veya sesteki bir konuşma ya da davranışı gerçekleştirmeyen bir kişinin, o konuşmayı yapıyor ya da davranışı gerçekleştiriyormuş gibi gösterilen* veya *bir kişinin başkasının fiziksel ya da sözlü olarak kimliğine bürünme kabiliyetinden ziyade teknik araçların kullanılması suretiyle o kişinin fiziksel ya da sözlü olarak kimliğine bürünerek üretilen; her türlü video kaydı, sinema filmi, ses kaydı, bir konuşmanın teknolojik temsili, elektronik görüntü, fotoğraf ve benzerleridir.*

Tasarı ile "*ileri teknolojiyle oluşturulan sahte kişilik kaydı*" suçu ihdas edilmek istenmektedir[103]. Bu suçla birlikte; kişiyi küçük düşürmek veya

---

98 730 sayılı kanun tasarıyla değiştirilecek Kaliforniya "*Elections Code*"'un 20010. maddesi.

99 Kanun tasarısının, deepfake hususunda en geniş kapsamlı kanun tasarısı olduğu belirtilmektedir. Bu tasarıyla, kişinin rızasına aykırı olarak müstehcen içerik oluşturmaktan seçimler ile kamu politikası tartışmalarına müdahale etmeye, şiddeti teşvik etmekten mali dolandırıcılık ve kimlik hırsızlığına kadar deepfake içeriklerin ortaya çıkarabileceği her türlü zararlara karşı koruma sağlamanın amaçlandığı ifade edilmektedir. Bkz. Ferraro, s. 7, 8.

100 "*Defending Each and Every Person from False Appearances by Keeping Exploitation Subject to Accountability Act of 2019*".

101 Kanun tasarısının metni için bkz. <https://www.congress.gov/bill/116th-congress/house-bill/3230/text> Erişim Tarihi 07.12.2019. Söz konusu kanun tasarısı, 28.06.2019 tarihinde Suç, Terörizm ve İç Güvenlik Alt Komitesi'ne sevk edilmiş ve henüz kanunlaşmamıştır. Kanunlaşma süreci, tasarının "*Introduced, Passed House, Passed Senate, To President, Became Law*" aşamalarından geçmesiyle son bulmaktadır. Tasarı şu anda "*Introduced*" aşamasındadır. Bkz. <https://www.congress.gov/bill/116th-congress/house-bill/3230/all-actions?overview=closed#tabs> Erişim Tarihi 31.05.2021; <https://www.congress.gov/bill/116th-congress/house-bill/3230> Erişim Tarihi 31.05.2021.

102 DAA, 5. Bölüm'de yer verilen ve United States Code'da 1041/n-3 maddesi olarak düzenlenecek hükümde yer almaktadır.

103 Kanun tasarısının 2. maddesi vasıtasıyla United States Code, Bölüm 18, Ceza ve Ceza Muhakemesi, Suçlar, Sahtecilik ve Yanlış Bildirimler bölümüne 1041. madde olarak

başka şekilde taciz etmek amacıyla oluşturulan görsel nitelikteki sahte kişilik kayıtlarında kişiyi cinsel eylemlere ya da çıplaklık hallerine karışmış gibi göstermek; şiddete veya fiziksel zarara neden olmak, silahlı veya diplomatik çatışmayı kışkırtmak veya resmi bir yargılamaya müdahale etmek; bir ulusal kamu politikasının tartışılmasını etkilemek ve bir seçime müdahale etmek; dolandırıcılık suçlarının işlenmesinde sahte kişilik kaydı kullanmak hallerinde beş yıla kadar hapis cezası öngörülmektedir.

Tasarıda, bu suçun kapsamının dışında olarak; bu tür bir kaydın üretilmesi sürecinde deepfake teknolojisinin kullanılması halinde nihai olarak dağıtılan kaydın meşru olması; sanatçılar gibi kişilerin görüntülerini veya ses kayıtlarını içeren ve büyük ölçüde dijital olarak değiştirilmemiş kayıtların söz konusu olması; sinema filmi, televizyon, müzik veya benzeri prodüksiyonların düzenlenmesiyle bağlantılı olarak oluşturulan veya orijinal içeriği bu Kanun'un yürürlüğe girmesinden önce oluşturulmuş olmakla birlikte içinde görünen kişinin rıza gösterdiği şekilde üretilmiş görüntülerin olması; bir kişinin makul düzeyde oluşturulan parodi şovları veya yayınları, tarihi canlandırmalar veya kurgusal radyo, televizyon veya sinema filmi gibi içeriklerde bu kişinin gerçekliğini sahte materyallerle haksızlaştırmayacak şekilde oluşturulması; bir kamu görevlisi tarafından veya onun yetkisi altındaki kişi tarafından, kamu güvenliği veya ulusal güvenlik önlemleri kapsamında yapılan üretimlerden olması hallerinde deepfake içeriklerin üretilmesi ve kullanılmasına imkân tanınmak istenmektedir.

Deepfake'in tehlikelerine karşı mücadele için birimlerin oluşturulması da kanun tasarısıyla sunulmaktadır. Kanun tasarısının 7. maddesinde; deepfake'in tespiti için Bilim ve Teknoloji Direktörlüğü bünyesinde "*Deepfake Görev Gücü*"[104] adında bir görev gücünün kurulması öngörülmektedir. Keza,

eklenmesi teklif edilmiştir. Halihazırda ilgili bölümde en son 1040. madde bulunmaktadır. Bkz. <https://uscode.house.gov/browse/prelim@title18/part1/chapter47&edition=prelim> Erişim Tarihi 31.05.2021. Ayrıca söz konusu kanun tasarısının 5. bölümünde yer alan değişiklikle, "*kimlik belgeleri, kimlik doğrulama özellikleri ve bilgilerle bağlantılı olarak sahtekarlık ve ilgili faaliyetler*" suçuna birtakım eklemelerin yapılması öngörülmektedir. Buna göre; a bendinde, 1, 4 ve 5. paragraftaki "*veya sahte bir kimlik belgesi*" ifadesinin, "s*ahte bir kimlik belgesi veya sahte bir görsel-işitsel kimlik kaydı*" olarak değiştirilmesi; b bendinde, "*veya sahte bir kimlik belgesi*" ifadesinin, "*sahte bir kimlik belgesi, sahte görsel-işitsel kimlik kaydı*" olarak değiştirilmesi; c bendinde, "*bir belge*" ifadesinden sonra "*veya sahte görsel-işitsel kimlik kaydı*" ifadesinin eklenmesi teklif edilmektedir. Söz konusu suçun halihazırdaki hali için bkz. <https://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title18-section1028&num=0&edition=prelim> Erişim Tarihi 31.05.2021.

[104] "*Deep Fakes Task Force*".

8. maddeye göre; bu görev gücünün başındaki kişi olarak İç Güvenlik sekreterinin, yılda en az bir kere gizli oturumda brifing vermesi gerekmektedir. Brifingde yabancı devletler tarafından ABD'nin iç işlerine ve seçimlerine etki etmeye yönelik deepfake içerikler ele alınacaktır.

Görüldüğü üzere, deepfake'in tehlikeleriyle mücadele kapsamında ABD'de birimler kurulmakta, deepfake'e özel olarak münferit suç tanımları ve ilgili mevcut suçlara eklemeler yapılmaktadır. Böylece sosyal düzeni bozucu nitelikte olan deepfake içeriklerle mücadele, hukuk zeminine taşınmakta ve deepfake içeriklerinin üretilmesi suretiyle ihlal edilebilecek hukuki değerlerin korunması amacıyla etkin bir mücadele yürütülmeye çalışılmaktadır.

2. Avrupa Birliği Müktesebatında Deepfake'in Tehlikelerine Karşı Hukuki Mücadele

Avrupa Birliği (AB) müktesebatında, ceza hukukunu ilgilendirecek biçimde doğrudan deepfake'e ilişkin hüküm içeren hukuki metin Yapay Zekâ ve Robotik Üzerine Kapsamlı Bir Avrupa Sanayi Politikası Hakkında 12 Şubat 2019 Tarihli Avrupa Parlamentosu Kararı'dır[105].

Bu Karar, *yapay zekâ destekli uygulamaları ve işletmeleri artırmak için* bir grup yapay zekâ uzmanı olan yapay zekâ ittifakı içindeki paydaşlarla iş birliği içinde *taslak yapay zekâ yönergeleri* geliştirerek yapay zekâya bir Avrupa yaklaşımı önermeyi taahhüt etmek amacıyla alınmıştır[106]. Karar'ın alınmasında etkili olan hususlar sayılırken[107] bunlardan biri olarak, AB'nin diğer ülkeler, özellikle ABD ve Çin tarafından yapılan büyük yatırımlarla rekabet edebilmesi için Avrupa düzeyinde koordineli bir yaklaşıma acilen ihtiyaç duyulması gösterilmektedir[108].

Yapay zekânın kötü niyetli kullanımının dijital güvenliği, kamu güvenliğini ve genel olarak kişilerin kendi kaderini tayin hakkını tehdit edebileceği ifade edilmektedir. Ayrıca yapay zekânın kötü niyetli bir şekilde kullanılmasının demokrasi ve temel haklar için bir risk oluşturabileceği de

[105] "*European Parliament resolution of 12 February 2019 on a comprehensive European industrial policy on artificial intelligence and robotics (2018/2088(INI))*". Karar metni için bkz. <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52019IP0081&qid=1613925410572&from=EN> Erişim Tarihi 21.02.2021.

[106] Karar, par. J.

[107] Karar, par. A-I.

[108] Karar, par. I.

vurgulanmaktadır[109].

Karar'da, Komisyon, kişiselleştirilmiş içerik veya haber beslemelerinin, olumsuz sonuçlara yol açabilecek biçimde gerçeklik algısının çarpıtılmasına yol açtığı zaman, (örneğin, seçim sonuçları veya göç gibi sosyal olgularla ilgili çarpık algıların oluşturulması gibi) *algı manipülasyonu uygulamalarını cezalandıran* bir çerçeve önermeye çağrılmaktadır[110]. Bu türden yapay zekâ uygulamalarının tespitine yarayacak uygulamaların geliştirilmesi gerektiği ifade edilmektedir[111]. Yüz ve ses tanıma dahil olmak üzere yapay zekâ uygulamalarının sosyal istikrarı korumak için "*gözetleme*" programlarında Çin'deki "*sosyal kredi sistemi*"ndeki[112] gibi kullanımlarının, Avrupa değerleri ve normlarıyla doğası gereği çelişkili olduğu vurgulanmaktadır[113].

Böylece Avrupa'da, gerçeklik algısının çarpıtılmasına sebep olan deepfake içerikleri bağlamında, seçim manipülasyonu gibi hallerde, *algı manipülasyonu uygulamalarını cezalandıran* bir hukuki düzenleme yapılması yönünde yol alınmaya çalışıldığı görülmektedir.

Keza Karar'da "*algoritmaların şeffaflığı, eğilimi ve açıklanabilirliği*" başlıklı 5.4. maddesinde, Komisyon, deepfake materyal veya sentetik videolar veya gerçekçi olarak yapılmış diğer sentetik videolar üreten herkesin, bunların orijinal olmadıklarını açıkça belirtmesini sağlamaya çağrılmaktadır[114].

Bu çalışmalar kapsamında, Avrupa Parlamentosu ve Avrupa Konseyi yapay zekâya ilişkin 21.04.2021 tarihli bir regülasyon teklif belgesi

[109] Karar, m. 1.2.9.

[110] Karar, m. 1.2.10.

[111] Karar, m. 1.2.11.

[112] Sosyal kredi sistemi (*social credit system*), kameralardan bireylerin davranışlarının taranması suretiyle elde edilen büyük verinin işlenmesi suretiyle kişilerin kredilenmesini (notlandırılmasını) sağlayan ve böylece kişiler hakkında kara liste oluşturulabilen bir sistemdir. Ayrıntıları için bkz. Nir Kshetri, "China's Social Credit System: Data, Algorithms and Implications", 2020, March/April, IT Professional, s. 14-18.

[113] Karar, m. 1.2.12.

[114] Karar, m. 5.4.178.

oluşturmuştur[115]. Bu belge ile yürürlüğe girecek "*Yapay Zekâ Kanunu*"[116] için yapay zekâ hususunda uyumlaştırılmış kuralları belirleyen bir regülasyon ortaya koyulmak istenmektedir[117]. Bu bağlamda, tüm yapay zekâ sistemlerinin temel hakları koruyan mevcut mevzuatın güvenliğini ve bunlara saygı gösterilmesini sağlaması amacıyla, bu sistemlerin sağlayıcılarına ve kullanıcılarına öngörülebilir, orantılı ve net yükümlülüklerin yükleneceği belirtilmektedir. Keza bazı yapay zekâ sistemleri ve özellikle sohbet robotları ("*chatbots*") ile deepfake'lerin kullanımları bakımından sadece "*asgari şeffaflık yükümlülükleri*"nin[118] getirilmesi önerilmektedir[119].

Teklif'in yapay zekâ sistemleri için şeffaflık yükümlülüklerini düzenleyen maddesinde[120] yapay zekâ sistemlerinin, oluşturdukları belirli manipülasyon

---

[115] "*Proposal for a Regulation Of The European Parliament And Of The Council Laying Down Harmonised Rules On Artificial Intelligence (Artificial Intelligence Act) And Amending Certain Union Legislative Acts*" başlıklı belge için bkz. <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0206&qid=1622473802812&from=EN> Erişim Tarihi 31.05.2021.

[116] "*Artificial Intelligence Act*".

[117] Teklif'in Açıklayıcı Notu, par. 1.1./1.

[118] "*Minimum transparency obligations*". Burada ifade edilen, şeffaflığın sağlanmasına yönelik alt sınırların belirlenmesi olup o alt sınırların seviyesinden daha aşağı bir şeffaflık yükümlülüğüne izin verilmemesi ifade edilmektedir. Dolayısıyla, ifadede şeffaflığın olabildiğince az olduğu kastedilmemekte, esasen asgari bir şeffaflığın sağlanması gerektiğine vurgu yapılmaktadır.

[119] Teklif'in Açıklayıcı Notu, par. 1.1./9.

[120] Teklif, m. 52, "*Transparency obligations for certain AI systems*". Maddenin tarafımızca yapılan çevirisi şu şekildedir: "*1. (Yapay zekâ sistemi) sağlayıcıları, gerçek kişilerle etkileşime girmesi amaçlanan yapay zekâ sistemlerinin, koşulları ve kullanımının bağlamından açıkça anlaşılmadığı sürece, gerçek kişilerin bir yapay zekâ sistemi ile etkileşimde bulundukları konusunda bilgilendirilecekleri şekilde tasarlanmasını ve geliştirilmesini sağlayacaktır. Bu yükümlülük, bu sistemler halkın bir suçu bildirmesini mümkün kılması için mevcut olmadığı sürece, suçları tespit etmek, önlemek, soruşturmak ve kovuşturmak için kanunen yetkilendirilmiş yapay zekâ sistemleri için geçerli değildir.*

2. Duygu tanıma sistemi veya biyometrik sınıflandırma sistemi kullanıcıları, sistemin işleyişi hakkında bu sisteme maruz kalan gerçek kişileri bilgilendirecektir. Bu yükümlülük, suçları tespit etmek, önlemek ve soruşturmak için yasaların izin verdiği biyometrik kategorizasyon için kullanılan yapay zekâ sistemlerine uygulanmayacaktır.

3. Mevcut kişilere, nesnelere, yerlere veya diğer varlıklara veya olaylara önemli ölçüde benzeyen ve bir kişiye yanlış bir şekilde gerçek veya güvenilir gibi görünen görüntü, ses veya video içeriği ("deep fake") üreten veya değiştiren bir yapay zekâ sisteminin kullanıcıları, bu içeriğin yapay olarak üretildiğini veya değiştirildiğini belirtmelidir.

4ncak, suçların tespiti, önlenmesi, soruşturulması ve kovuşturulması amacıyla kullanımına kanunla izin verildiği veya AB Temel Haklar Şartı'nda güvence altına alınan ifade özgürlüğü ve sanat ve bilim özgürlüğü hakkının kullanıldığı ve üçüncü kişilerin hak ve özgürlükleri için

risklerini hesaba katmaları ile ilgili olarak düzenleme yapıldığı ifade edilmektedir[121]. Buna göre; şeffaflık yükümlülükleri, (i) insanlarla etkileşime giren, (ii) duyguları tespit etmek veya biyometrik verilere dayanarak (sosyal) kategorilerle ilişkileri belirlemek için kullanılan veya (iii) içerik üreten veya içeriği değiştiren ("*deep fakes*") sistemler için geçerlidir. Kişiler, bir yapay zekâ sistemi ile etkileşime girdiğinde, duygu veya karakteristik özellikleri otomatik araçlarla tanındığında bu durum hakkında bilgilendirilmelidir. Gerçek içeriğe önemli ölçüde benzeyen görüntü, ses veya video içeriği oluşturuluyor veya bunları işlemek için bir yapay zekâ sistemi kullanılıyorsa, bunların otomatik araçlarla oluşturulduğunu belirtme yükümlülüğü olmalıdır. Bunun belirtilmesi, kişilerin bilinçli seçimler yapmalarına ve belirli bir durumdan geri adım atmalarına izin vermesini sağlayacaktır.

Bu düzenlemelerin yanı sıra "*Dezenformasyona İlişkin Uygulama Kurallarının Güçlendirilmesine İlişkin Avrupa Komisyonu Rehberi*"nde[122] COVID-19 hastalığının ortaya çıkardığı güçlüklerden birinin dezenformasyon olduğu ve bu bağlamda dezenformasyonla mücadeleye yönelik benimsenen kuralların[123] güçlendirilmesi yoluna gidilmesi gerektiği ifade edilmektedir. Söz konusu güçlendirilmiş kurallarda, izin verilmeyen manipülatif davranışlar alanındaki manipülatif tekniklerin tamamını kapsayan ve bunlara karşı efektif tepkiler gerektiren yeni taahhütlerin ortaya koyulması gerektiği belirtilmektedir. Keza bu taahhütlerde, imza sahiplerinin deepfake gibi gelişen manipülatif teknikleri de ele alması gerekmektedir[124].

---

uygun güvencelere tabi olan durumlarda birinci fıkra hükmü uygulanmaz.

4. Fıkra 1, 2 ve 3, bu Regülasyonun Başlık III'ünde belirtilen gereklilikleri ve yükümlülükleri etkilemeyecektir."

[121] Teklif'in Açıklayıcı Notu, par. 5.2.4, "*Transparency Obligations for Certain AI Systems (Title IV)*".

[122] "*European Commission Guidance on Strengthening the Code of Practice on Disinformation*". Rehber metni için bkz. <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021DC0262&qid=1622473657967&from=EN> Erişim Tarihi 31.05.2021.

[123] Avrupa müktesebatında dezenformasyonla ilgili atılan güncel adımlar için bkz. 15.12.2020 tarihli "*Dijital Hizmetler Kanunu (Digital Services Act)*" teklifi, <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020PC0825&from=en> Erişim Tarihi 31.05.2021; "*Dezenformasyon İle İlgili Uygulama Kuralları (Code of Practice on Disinformation)*", <https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation> Erişim Tarihi 31.05.2021.

[124] Rehber, m. 6.

VI. TÜRKİYE'DE DEEPFAKE'İN TEHLİKELERİNE KARŞI CEZA HUKUKU VE TEKNOLOJİK İMKÂNLARLA MÜCADELENİN DURUMUNA İLİŞKİN DEĞERLENDİRME VE DE LEGE FERENDA ÖNERİLER

Deepfake'in yurt dışında ortaya çıkmış olması sebebiyle çalışmada deepfake örnekleri de yabancı ülkelerden verilmiştir. Ancak belirtmek gerekir ki, ülkemizde deepfake içerik üretiminde gözle görünür bir artış söz konusudur. Örneğin, merhum oyuncu Kemal Sunal'ın The Mask adında yabancı filmdeki başrol oyuncusunun yerine oynuyor gibi[125] ve bir bankanın reklam filminde kendisini o reklam filminde oynuyor gibi[126] gösterildiği videolar üretilmiştir. Yine örneğin, İbrahim Tatlıses'in Narcos adındaki yabancı dizide oynuyormuş gibi gösterildiği[127] videolar üretilmiştir. Teknolojinin yaygınlaşması ve kişiler hakkındaki bilhassa görüntü ve ses verilerinin internette artmasıyla birlikte, bu türden deepfake içeriklerinin ünlü olmayan kişiler için üretilmesi de mümkündür[128].

Yukarıda ifade edildiği üzere, deepfake teknolojisinin gelişmesiyle birlikte, deepfake içeriklerinin tespit edilmesi teknolojisi de gelişmektedir. Örneğin yakın zamanda ülkemizde bir şirket, deepfake içeriklerini tespit ettiğini belirttiği bir program geliştirmiştir[129]. Bu doğrultuda deepfake'e karşı teknolojik mücadele edilmesi ve teknolojik gelişmelere önem verilmesi gerektiği açıktır.

Deepfake'in tehlikeleriyle hukuken mücadele edilmesi hususu ülkemizde henüz güncel bir sorun haline gelmemiştir. Dolayısıyla bu hususta hukuki bir düzenleme yapılmamıştır. Ancak özellikle ileride bu hususta çalışmaların yapılması gerekeceğini öngörmek zor değildir. Nitekim bazı ülkelerin bu hususta hukuki düzenleme yapılmasına yönelik adımlar atmaya başladığı yukarıda belirtilmişti. Bu bağlamda, ülkemizde ceza hukuku açısından ne şekilde düzenlemeler yapılabileceğini irdelemek gerekir.

---

[125] Bkz. <https://www.youtube.com/watch?v=HrYe9cEZ8V0> Erişim Tarihi 21.02.2021; Nabiyev, s. 619.

[126] Bkz. <https://www.youtube.com/watch?v=fPiwmoxa0QE> Erişim Tarihi 21.02.2021.

[127] Bkz. <https://www.youtube.com/watch?v=22VmhEdv5wA> Erişim Tarihi 21.02.2021.

[128] Lossau, s. 3. Özellikle sosyal medya platformlarında paylaşılan (fotoğraf, video, ses gibi) veriler deepfake oluşturmakta kolayca kullanılabilmektedir. Bkz. Aksoy Retornaz, s. 100, 101.

[129] "*Deepware Scanner*" adındaki açık kaynaklı ("*open-sourced*") bu program için bkz. <https://deepware.ai/about/> Erişim Tarihi 21.02.2021.

Yukarıda deepfake içeriklerinin araç olarak kullanılabileceği suçlardan bahsedildi. Söz konusu suçların oluşması bakımından, mevcut düzenlemeler karşısında, bir deepfake içeriğinin oluşturulması bir suçun işlenmesinde kullanılıyorsa oluşan suç bağlamında failin sorumluluğu yoluna gidilecektir. Diğer yandan, deepfake içeriklerinin kullanılmasının bazı suçlarda daha fazla cezayı gerektiren bir nitelikli hal olarak düzenlenmesi yoluna gidilebilir. Bilhassa iftira, suç uydurma, şantaj, hakaret, dolandırıcılık ile fikir ve sanat eserleriyle ilgili hak ihlali suretiyle işlenen suçlarda daha fazla cezayı gerektiren bir nitelikli hal olarak, bu suçların deepfake içerikleri üretmek[130], kullanmak, ifşa etmek ve yaymak suretiyle gerçekleştirilmeleri düzenlenebilir. Nitekim bu suçların temel halinin işlenmesindeki fiilin gerçekleştirilişi ile deepfake teknolojisinin kullanılması suretiyle gerçekleştirilişi arasında hem harcanan çaba bakımından hem de hileli bir davranış olması sebebiyle haksızlık bakımından fark bulunduğunu söyleyebiliriz. Ayrıca her ne kadar deepfake içeriklerinin tespitine yönelik teknoloji gelişse de bunların tam bir güvenilirlikle tespit edilebildiğini söylemek de mümkün değildir. Dolayısıyla bu içeriklerin aldatıcılıkları oldukça yüksek olmaktadır[131]. Bazı suçlar bakımından deepfake hususunda boşlukların bulunması sebebiyle daha ayrıntılı değerlendirme yapmak gerekmektedir:

I. Kişisel verilere ilişkin olarak TCK'da (m. 135, 136, 138) ve KVKK'da (m. 17) yer alan suçlardaki hareketler, hukuka aykırı olarak kişisel veriyi *kaydetmek*, *vermek*, *yaymak*, *ele geçirmek*, yok edilmesi gereken kişisel veriyi *yok etmemek*, silinmesi gereken kişisel veriyi *silmemek* ve anonimleştirilmesi gereken kişisel veriyi *anonimleştirmemek* şeklindedir. Deepfake teknolojisinin kullanılmasındaki hareketin motifi ise, kişisel verileri *bir sürece tabi tutarak manipüle etmek*tir. Elbette, deepfake içeriğinin üretilmesi için gerçekleştirilmesi halinde kişisel veriyi kaydetmek, vermek, yaymak ve ele geçirmek hareketleri suç teşkil edecektir. Ancak burada ayrıca veriyi bir *süreçten geçirmek* söz konusudur. Daha açık ifadeyle, orijinal bir kişisel veri, başka verilerle kaynaştırılmak suretiyle manipüle edilmiş bir veri ortaya çıkarılmaktadır. Bu itibarla deepfake içeriğindeki kişisel veri, manipüle edilmiş bir kişisel veridir. Dolayısıyla esasen gerçekle bağdaşmayan ve gerçekmiş gibi görünen, ama bir yönüyle ise gerçek kişisel verileri barındıran

[130] Almanya'da deepfake ile ilgili bir suçun ihdas edilmesi halinde, bu içeriklerin sadece yayılmasının değil, içerdiği zarar potansiyelinin büyüklüğü sebebiyle üretilmesinin de cezalandırılmasının gerekeceği ifade edilmektedir. Bkz. Lantwin, Rechtliche Herausforderungen, s. 578.

[131] Chesney/Citron, Looming Challenge, s. 1753.

bir karma ürün elde edilmiş olmaktadır. Keza, elde edilen bu sahte içerik, gerçek bir kişisel veri görünümünde insanları aldatıcı kabiliyeti de haiz bulunmaktadır. Dolayısıyla, gerçek bir kişisel verinin salt kaydedilmesi, verilmesi, yayılması veya ele geçirilmesi değil, aynı zamanda o kişisel veri üzerinde manipülasyon yapılması da söz konusudur. Bu sebeple, bilişim sistemlerinin kullanılması suretiyle hukuka aykırı bir şekilde; başkasına ait görüntü veya sesi değiştirme ya da başkasına ait olan görüntü veya sesi bir başka kişinin görüntü veya sesinde kullanma ya da üretilen bu içeriği yayma veya ifşa etme fiilleri bakımından bir suç tanımına yer verilmesi gerektiği kanaatindeyiz.

II. Müstehcenlik suçunun kapsamı dışında kalan hususa burada tekrar değinmek gerekir. Yetişkinlerin rızasıyla yer aldığı bir müstehcen ürünün üretilmesi, TCK m. 226'da sayılan fiillerin gerçekleştirilmesinde kullanılmadıkça müstehcenlik suçuna vücut vermemesi bakımından anlaşılabilir mahiyettedir. Buna karşılık, deepfake içerik olarak bir müstehcen ürünün üretilmesinde, eğer görüntüsü mevcut olan kişilerin rızası söz konusu değilse, böyle bir ürünün salt üretilmesinin de bir haksızlık teşkil ettiğinde şüphe yoktur[132]. Ancak müstehcenlik suçu, bu ürünlerin salt üretilmesi bakımından önleyici mahiyette değildir. Belirtmek gerekir ki, cinsel nitelikte deepfake medya içeriğinin üretilmesinde o içerikte aslında yer almayan ama yer almış gibi gösterilen kişinin yüzü ve bedenine ilişkin diğer görüntüleri kişisel veri niteliğindedir. Yukarıda ifade ettiğimiz üzere bilişim sistemlerinin kullanılması suretiyle hukuka aykırı bir şekilde; başkasına ait görüntü veya sesi değiştirme ya da başkasına ait olan görüntü veya sesi bir başka kişinin görüntü veya sesinde kullanma ya da üretilen bu içeriği yayma veya ifşa etme fiilleri bakımından bir suç tanımına yer verilmesi gerekmektedir. Böyle bir suç tanımının ihdas edilmesiyle birlikte, hukuka aykırı olarak kişilerin kişisel verilerinin bir sürece tabi tutularak manipüle edilmesi, dolayısıyla bir deepfake medya içeriğinde kişilerin rızası hilafına yer almaları kapsama alınmış

[132] Benzer şekilde bkz. Lantwin, Strafrechtliche Bekämpfung, s. 81. Doktrinde, "*cinsel içerikli görüntüleri rızaya aykırı olarak ifşa etme, yayma, erişilebilir kılma veya üretme*" fiilleri bakımından, TCK'da "*özel hayata ve hayatın gizli alanına karşı suçlar*" arasında ayrı bir suçun ihdas edilmesi gerektiği ifade edilmektedir. Bu suç kapsamında, deepfake medya içeriklerinin de yer alması gerektiği ve bu medya içeriklerinde sadece yüzü kullanılan kişinin de bu ihdas edilecek suç bağlamında mağdur olacağı belirtilmektedir. Bkz. Aksoy Retornaz, s. 85, 115, 142. Keza bu suçun ihdasını öneren yazar, önerdiği suç tanımında deepfake medya içeriklerinin üretilmesine, "*bir kişinin siber alanda cinsel içerikli görüntülerini rızaya aykırı olarak ... siber alanın sağladığı kolaylıktan faydalanarak üreten*" ifadesiyle yer vermektedir. Bkz. Aksoy Retornaz, s. 142

olmaktadır. Bu suçun ihdasında, üretilen medya içeriğinin cinsel nitelikte olması durumuna yönelik olarak daha fazla ceza verilmesini gerektiren bir nitelikli hale yer vermek isabetli olacaktır. Keza üretilen deepfake medya içeriklerinin kişilerin onur, şeref ve saygınlığını rencide edici nitelikte olması halinde, hakaret suçu da oluşacaktır.

III. Bir başka değerlendirme, seçimlerde yasak propaganda yapmak suçu bakımından yapılmalıdır. Yukarıda açıklandığı üzere, suçun tanımında yer alan, "*ne suretle olursa olsun seçimin düzenini bozabilecek veya oy vermenin tam bir serbestlikle yapılmasına tesir edebilecek mahiyette söz, yazı veya sair suretlerle propaganda yapmak* veya *asılsız şayialar çıkarmak*" fiilinde, eğer davranışın "*oy verme gününden önceki günün saat 18.00'inden sonra ve oy verme gününde*" gerçekleştirilmesi şartı bu fiil bakımından geçerli değilse, bu düzenlemenin deepfake içeriklerinin üretilmesi-kullanılması suretiyle seçimi manipüle etmek bakımından genel mahiyette bir düzenleme olduğu söylenebilir. Nitekim, sadece "*oy verme gününden önceki günün saat 18.00'inden sonra ve oy verme gününde*" geçerli bir zaman için değil, her zaman için bir koruma sağlamaktadır. Ancak aksi halde, deepfake içeriklerinin üretilmesi-kullanılması suretiyle seçimi manipüle etmek bakımından bu hüküm etkili bir koruma sağlamayacaktır. Nitekim bu durumda sadece "*oy verme gününden önceki günün saat 18.00'inden sonra ve oy verme gününde*" geçerli bir zaman için bir yasaklama yoluna gidilmektedir. Bu düzenlemenin anlaşılır hale getirilmesi gerektiği açıktır. Ayrıca deepfake teknolojisinin kullanılması suretiyle gerçekleştirilen bir propagandanın, sıradan bir asılsız propaganda olmadığı, nitelikli ve ikna edici olabilecek içeriklere sahip olabileceği ve gerçekleştirilen davranışın daha fazla haksızlık içeriğine sahip olacağına dikkat edilmelidir.

Keza hem *Teksas Seçim Kanunu*'nun 255.004 numaralı maddesi vasıtasıyla hem ABD'de getirilmek istenen *DAA Kanun Tasarısı*'nda hem Kaliforniya'daki kanun tasarılarında hem de *Yapay Zekâ ve Robotik konusundaki Avrupa Komisyonu Kararı*'nda vurgulanan bir hususa tekrar değinmek gerekir. Söz konusu düzenlemelerde, ulusal güvenlik ve seçim manipülasyonu ile deepfake arasında ciddi bir bağlantı kurulmaktadır. Deepfake'in sebep olabileceği en büyük tehlikelerden birinin seçimleri etkileyebilecek olması gösterilmektedir[133]. Nitekim bu doğrultuda *Teksas Seçim Kanunu*'nun

[133] Bu hususdaki tehlikeler, temel olarak "*seçim manipülasyonu*", "*sosyal ayrışmanın artması*" ve "*devlet kurumları ve yetkililere olan güvenin azalması*" şeklinde ele alınmaktadır. Ayrıntılı değerlendirmeler için bkz. Waldemarsson, s. 9 vd.

255.004 numaralı maddesinde deepfake içeriklerle seçim manipülasyonu suç olarak düzenlenmiştir. Aynı doğrultuda ABD'de DAA Kanun Tasarısı'nda deepfake aracılığıyla seçime müdahale etmenin suç olarak düzenlenmesi yoluna gidilmektedir. Ayrıca "*Deep Fake Görev Gücü*"nün kurulması ve bu görev gücünün yılda en az bir kere gizli oturumda ABD'nin iç işlerine ve seçimlerine etki etmeye yönelik deepfake'lerin ele alınması düzenlenmektedir. Keza Kaliforniya'da seçime katılan adayların itibarını zedelemek veya bir seçmeni aday lehine veya aleyhine oy vermesi için kandırmak amacıyla deepfake içeriklerinin kullanılması yasaklanacaktır. Dolayısıyla aktüel olmaması sebebiyle deepfake'lerin seçim üzerinde oluşturabileceği etkilerin ülkeler nezdinde tam olarak deneyimlenmemiş olmasına rağmen, seçimler üzerindeki etkilerinin önemli olacağı öngörülmektedir[134]. Bu hususun, aktüel bir tehlike haline dönüşmeden bir an önce ülkemiz seçim ve ceza hukuku mevzuatı bakımından da değerlendirilmesinde yarar bulunmaktadır. Keza hem benzer bir kamu gücü biriminin oluşturulması hem de mevcut düzenlemedekinden daha fazla miktarda bir soyut cezayı içerecek biçimde seçimlerin manipülasyonuna özel olarak bir suçun ihdas edilmesi; bilhassa, bilişim sistemlerinin kullanılması suretiyle başkasına ait görüntü veya sesin değiştirilmesi ya da başkasına ait olan görüntü veya sesin bir başka kişinin görüntü veya sesinde kullanılması suretiyle üretilen medya içeriklerinin ulusal güvenliği ya da seçimin akıbeti veya güvenliğini tehlikeye düşürecek biçimde kullanma, ifşa etme veya yayma fiillerinin cezalandırılması yoluna gidilmesinin isabetli olacağı kanaatindeyiz. Böylece ifade hürriyetinin kullanılmasının tehlikeye düşürülmemesi amacıyla suçun somut tehlike suçu olarak düzenlenmesinin isabetli olacağı düşüncesiyle[135] ihdas edilecek bu suçun bir somut tehlike suçu olması gerekmektedir. Keza bu deepfake medya içeriklerinin cinsel nitelikte olması durumuna yönelik olarak daha fazla ceza verilmesini gerektiren bir nitelikli hale yer vermek isabetli olacaktır.

---

[134] Bilhassa, seçimleri ve siyasi hayatı etkilemek için üretilecek deepfake içeriklerinde politikacıların görüntülerinin pornografik medya içeriğinde kullanılması ihtimaline dikkat çekilmektedir. Bkz. Lantwin, Strafrechtliche Bekämpfung, s. 79. Deepfake içerik oluşturmaktaki amacın seçimleri doğrudan etkilemesi bakımından değil, fakat politikacıların itibarının zedelenmesi bakımından bu hususta bir örnek 2019 yılında Malezya'da yaşanmıştır. İki siyasetçi arasında geçen müstehcen içerikli sahte olarak oluşturulmuş olduğu iddia edilen bir video yayınlanmıştır. Söz konusu videonun bir deepfake olup olmadığının tespit edilemediği belirtilmekle birlikte, bir deepfake içerik olduğu ileri sürülmüştür. Bkz. Yavuz, s. 37.

[135] Deepfake içeriklerinin siyasi bağlamda üretilmeleri ve kullanılmalarının ceza hukuku yaptırımlarına tabi tutulması hususunda ifade ve sanat hürriyetinin lehine istisnaların sağlanması gerektiğine dikkat çekilmektedir. Bkz. Lantwin, Strafrechtliche Bekämpfung, s. 82.

IV. Son olarak, deepfake teknolojisinin kullanım sınırlarının belirlenmesi bakımından da bir pozitif hukuk düzenlemesinin gerekliliğini vurgulayabiliriz. Nasıl ki kişisel veriler bakımından özel bir koruma alanı sağlanmaya ve bu alanın düzenlenmesine çalışılmışsa, deepfake teknolojisinin kullanımının da düzenlenmesi gerekir. Nitekim bu teknolojinin kullanım sınırlarıyla birlikte, hukuka uygunluğun maddi şartları ortaya koyulabilecektir. Örneğin, sanatsal bir çalışma kapsamında veya salt parodi amaçlı eğlence içerikli videoların deepfake ile hazırlanmasının şartları böylece pozitif hukuk dayanağına kavuşacaktır. Ancak böyle bir düzenleme yapılırken, yapay zekâ teknolojilerinin gelişmesini engelleyici bir yöntemin benimsenmemesine dikkat edilmelidir.

SONUÇ

Deepfake olarak tabir edilen sahte medya içeriklerinin üretimi gittikçe kolaylaşmakta ve bu sebeple yaygınlaşmaktadır. Başta kişisel verilere ilişkin suçlar ve müstehcenlik suçları olmak üzere pek çok suçun işlenmesinde deepfake teknolojisi ve içerikleri kullanılabilir niteliktedir. Konunun ayrıca ulusal güvenlik ve siyasi yönü de bulunmaktadır.

İç hukukunda deepfake ile ilgili ilk adımı atan ve deepfake içeriklere ilişkin suç tanımlarına yer veren ülkeler Virginia ve Teksas olmuştur. Keza ABD'de deepfake hususunda geniş kapsamlı olarak DAA Kanun Tasarısı sunulmuştur. Avrupa Komisyonu da *algı manipülasyonu uygulamalarını cezalandıran* bir hukuki düzenleme yapılması gerektiğine ve deepfake ile yapay zekânın kötüye kullanımına dikkat çekmektedir. Bu gelişmelere ülkemizin kayıtsız kalmaması gerekir. Büyük olasılıkla, ülkeler milletlerarası sözleşmeler imzalamak suretiyle deepfake'in tehlikeleriyle mücadeleyi genişletecektir. Nitekim sınır aşan suçlar söz konusu olduğunda, bu tür suçlarla mücadele için çeşitli sözleşmelerin imzalanması yoluna gidilmektedir[136]. Yapılması muhtemel sözleşmelerden önce diğer ülke uygulamaları Türkiye için bir yol gösterici nitelik arz edebilir. Keza teknolojik gelişmelerin gerisinde kalmayan ve ihtiyaçları karşılayan iç hukuk düzenlemeleri öngörülmelidir.

Önemle belirtmek gerekir ki, deepfake'in tehlikeleriyle mücadelede kanun koyucunun suçların ihdas edilmesi yönünde irade sergilemesi halinde ceza hukukunun *ultima ratio* niteliği gözden uzak tutulmamalıdır. Her ne kadar ceza hukuku yaptırımları son çare olsa da yukarıda ifade edildiği gibi

[136] Mahmut Koca/İlhan Üzülmez, Türk Ceza Hukuku Genel Hükümler, 13. Baskı, Seçkin Yayıncılık, 2020, s. 36.

deepfake; maddi ve manevi varlığı koruma ve geliştirme hakkı, özel hayata ve aile hayatına saygı gösterilmesini isteme ve özel hayatın ve aile hayatının gizliliği hakkı, kişisel verilerin korunmasını isteme hakkı, düşünce ve kanaat hürriyeti ile düşünce ve kanaatleri açıklama ve yayma hakkı, bilim ve sanat hürriyeti gibi hukuki değerlere ilişkin hak ihlaline yol açabilmektedir. Bu hukuki değerler, halihazırda farklı suçlarla korunmaya çalışılmaktadır. Dolayısıyla hukuki değerlerin önemine binaen bu değerlerin korunmasına yönelik olarak suçlar ihdas edilmektedir. Deepfake de bu sebeple diğer ülke hukuklarında ceza hukukunun alanına girmektedir. Elbette deepfake'in tehlikelerine karşı hukuki mücadele, öncelikle özel hukuk ve idare hukuku alanında yapılacak düzenlemelerle sağlanmalıdır[137]. Özel hukuk ve idare hukukunun müdahale alanının yetersiz kaldığının suç politikasıyla tespiti halinde ceza hukuku yaptırımları uygulanmalıdır. Belirtmek gerekir ki, halihazırdaki suç tanımları ve korunan hukuki değerlere bakıldığında, cezaya muhtaçlık ve layıklık bağlamında deepfake haksızlıklarının ceza hukukunun müdahale alanına dahil olması makul görünmektedir.

Ayrıca bu teknolojinin gelişmesine ve faydalı alanlarda kullanılmasına yönelik destekleyici nitelikte hukuki adımların atılması gerekir.

Çalışmanın sonucu olarak deepfake'in tehlikelerine karşı ülkemizde atılması gereken adımları şu şekilde sıralayabiliriz:

- Salt hukuki düzenlemeler, deepfake'in yol açabileceği tehlikelerin önüne geçebilmek bakımından yeterli olmayacaktır. Ülkemizde, deepfake içeriklerinin tespit edilebilmesine yönelik bilişim programları üretilmeye başlanmış olmakla birlikte, bir ulusal politika olarak da bu tür teknolojik gelişmelerin teşvik edilmesi ve bu konuda yol kat edilmesi gerekmektedir.

- Deepfake ile hukuken mücadele edilmesi hususu ülkemizde güncel hale gelmemiştir. Deepfake'e ilişkin genel mahiyette bir pozitif hukuk metninin yürürlüğe koyulması ve bu teknolojinin hukuk zemininde ele alınmasına gereklilik bulunmaktadır. Daha açık bir ifadeyle, esasen yapay zekâ uygulamalarına ilişkin ayrı bir kanun düzenlemesi yapılması isabetli olacaktır. Bu kanunda deepfake'e ilişkin düzenlemelere de yer verilmesiyle bu alan hukuki bir temele kavuşabilecektir.

[137] Belirtmek gerekir ki, çalışmada ceza hukuku bağlamında değerlendirmelerde bulunulmuştur. Bu sebeple, özel hukuk ve idare hukuku bağlamındaki yaptırımlar çalışmanın kapsamı dışında olduğundan bu husus ayrıntılı olarak irdelenmemiştir.

- İftira, suç uydurma, şantaj, hakaret, dolandırıcılık ile fikir ve sanat eserleriyle ilgili hak ihlali suretiyle işlenen suçların deepfake içerikleri üretmek ve deepfake teknolojisini kullanmak suretiyle işlenmeleri halleri, haksızlık içerikleri dolayısıyla daha fazla cezayı gerektiren bir nitelikli hal olarak düzenlenebilir.

- Deepfake içeriklerin üretilmesi için gerçekleştirilmesi halinde, kişisel veriyi kaydetmek, vermek, yaymak ve ele geçirmek hareketleri suç teşkil edecektir. Ancak deepfake teknolojisinin kullanılmasındaki hareketin motifi esasen kişisel verilerin *bir sürece tabi tutularak manipüle edilmesi*dir. Bu sebeple, kişisel verilere ilişkin olarak deepfake teknolojisinin kullanılmasına ayrıca yer verilmesi gerekir. Böylece, deepfake medya içeriklerinin üretilmesi, kullanılması, yayılması ve ifşa edilmesine yönelik olarak genel mahiyette bir suç ihdas edilmiş olacaktır.

- Deepfake içeriklerin seçimlerin manipülasyonunda kullanılması bağlamında, deepfake hususunun aktüel bir tehlike haline dönüşmeden bir an önce ülkemiz seçim ve ceza hukuku mevzuatı bakımından değerlendirilmesinde yarar bulunmaktadır. Seçimlerin Temel Hükümleri ve Seçmen Kütükleri Hakkında Kanun'daki mevcut suç tanımından daha fazla miktarda bir soyut cezayı içerecek biçimde ulusal güvenlik ile seçimlerin manipülasyonuna özel olarak bir suç ihdası yoluna gitmek isabetli olacaktır.

KAYNAKÇA

Açıkgöz E. İ, Bilişim Sistemi Aracılığıyla Haksız Yarar Sağlama Suçu, Adalet Yayınevi, 2020.

Agarwal S/Farid H/Gu Y/He M/Nagano K/Li H, "Protecting World Leaders Against Deep Fakes", 2019, The IEEE Conference on Computer Vision and Pattern Recognition (CVPR) Workshops, s. 38-45, <https://openaccess.thecvf.com/content_CVPRW_2019/papers/Media%20Forensics/Agarwal_Protecting_World_Leaders_Against_Deep_Fakes_CVPRW_2019_paper.pdf> Erişim Tarihi 24.10.2019.

Akarslan H, Bilişim Suçları, 2. Baskı, Seçkin Yayıncılık, 2015.

Akbulut B, Bilişim Alanında Suçlar, 2. Baskı, Seçkin Yayıncılık, 2017.

Akbulut B, Ceza Hukuku Genel Hükümler, 4. Baskı, Adalet Yayınevi, 2017.

Aksoy Retornaz E, Bir Siber Taciz Biçimi: Cinsel İçerikli Görüntüleri Rızaya Aykırı Olarak İfşa Etme, Yayma, Erişilebilir Kılma veya Üretme Suçu (Revenge Porn ve Deep Fake), On İki Levha Yayıncılık, 2021.

Artuk M. E/Gökcen A/Alşahin M. E/Çakır K, Ceza Hukuku Genel Hükümler, 11. Baskı, Adalet Yayınevi, 2017.

Babayiğit B, Kumar Oynanması İçin Yer ve İmkân Sağlama Suçu, Adalet Yayınevi, 2021.

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

Blitz M. J, "Lies, Line Drawing, and (Deep) Fake News", 2018, 71(1), Oklahoma Law Review, Symposium: Falsehoods, Fake News, and the First Amendment, s. 58-116.

Breen D. C, "Silent No More: How Deepfakes Will Force Courts to Reconsider Video Admission Standards", 2021, 21(1), Journal of High Technology Law, s. 122-164.

Charniak E, Introduction to Deep Learning, The MIT Press, 2018.

Chawla R, "Deepfakes: How a Pervert Shook the World", 2019, 4(6), International Journal of Advance Research and Development, s. 4-8.

Chesney R/Citron D. K, "21st Century-Style Truth Decay: Deep Fakes and the Challenge for Privacy, Free Expression, and National Security", 2019, 78(4), Maryland Law Review, s. 881-891.

Chesney R/Citron D. K, "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security" 2019, 107(6), California Law Review, s. 1753-1820.

Ciftci U. A/Demir İ/Yin L, "FakeCatcher: Detection of Synthetic Portrait Videos using Biological Signals", 2019, arXiv:1901.02212, s. 1-14, <https://arxiv.org/pdf/1901.02212v2.pdf> Erişim Tarihi 24.10.2019.

Citron D. K, "Prepared Written Testimony and Statement for The Record", 2019, House Permanent Select Committee on Intelligence, s. 1-11, <https://docs.house.gov/meetings/IG/IG00/20190613/109620/HHRG-116-IG00-Wstate-CitronD-20190613.pdf> Erişim Tarihi 26.10.2019.

Citron D. K, "Sexual Privacy", 2019, 128(7), Yale Law Journal, s. 1870-1960.

Delfino R. A, "Pornographic Deepfakes: The Case for Federal Criminalization of Revenge Porn's Next Tragic Act", 2019, 88(3), Fordham Law Review,

s. 887-938.

Demirbaş T, Ceza Hukuku Genel Hükümler, 11. Baskı, Seçkin Yayıncılık, 2016.

Demircan T, Bilişim Alanında Suçlar, Legal Yayınevi, 2016.

Deshpande A/Kumar M, Artificial Intelligence for Big Data, Packt, 2018.

Dülger M. V, Bilişim Suçları ve İnternet İletişim Hukuku, 8. Baskı, Seçkin Yayıncılık, 2020.

Elmas Ç, Yapay Zeka Uygulamaları, 5. Baskı, Seçkin Yayıncılık, 2021.

Ferraro M. F, Deepfake Legislation: A Nationwide Survey - State and Federal Lawmakers Consider Legislation to Regulate Manipulated Media, WilmerHale 2019, <https://www.wilmerhale.com/-/media/files/shared_content/editorial/publications/wh_publications/client_alert_pdfs/20190925-deepfake-legislation-a-nationwide-survey.pdf> Erişim Tarihi 18.02.2021.

Ferraro M. F/Tompros, L. W, "New York's Right to Publicity and Deepfakes Law Breaks New Ground", 2021, 38(4), The Computer & Internet Lawyer, s. 1-4.

Fido D/Harper C/Davis M/Petronzi D/Worrall S, "Intrasexual Competition As a Predictor of Women's Judgements of Revenge Pornography Offending", 2019, PsyArXiv Preprints, s. 1-39, <https://psyarxiv.com/pwmqu/> Erişim Tarihi 17.02.2021.

Floridi L, "Artificial Intelligence, Deepfakes and a Future of Ectypes", 2018, 31(3), Philosophy & Technology, s. 317-321.

Franks M. A/Waldman A. E, "Sex, Lies, and Videotape: Deep Fakes and Free Speech Delusions", 2019, 78(4), Maryland Law Review, s. 892-898.

Goodfellow I. J/Pouget-Abadie J/Mirza M/Xu B/ Warde-Farley D/ Ozair S/ Courville A/ Bengio Y, "Generative Adversarial Nets", 2014, arXiv:1406.2661v1, s. 1-9, <https://arxiv.org/pdf/1406.2661.pdf> Erişim Tarihi 14.03.2021.

Güera D/Delp E. J, "Deepfake Video Detection Using Recurrent Neural Networks", 2018, 5th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS), s. 1-6, <https://ieeexplore.ieee.org/document/8639163> Erişim Tarihi 24.10.2019.

Hall H. K, "Deepfake Videos: When Seeing Isn't Believing", 2018, 27(1),

Catholic University Journal of Law and Technology, s. 50-76.

Hamilton R. J, "New Technologies in International Criminal Investigations", 2018, 112, Proceedings of the 112th Annual Meeting, International Law in Practice, Cambridge Univesity Press, s. 131-133.

Harris D, "Deepfake: False Pornography is Here and the Law Cannot Protect You", 2019, 17, Duke Law & Technology Review, s. 99-128.

Hasan H. R/Salah K, "Combating Deepfake Videos Using Blockchain and Smart Contracts", 2019, 7, IEEE Access, s. 41596-41606, <https://ieeexplore.ieee.org/document/8668407> Erişim Tarihi 24.10.2019.

İçel K, Ceza Hukuku Genel Hükümler, Yenilenmiş Bası, Beta Yayıncılık 2016.

Kaya M. B, Teknik ve Hukuki Boyutlarıyla İnternete Erişimin Engellenmesi, On İki Levha Yayıncılık, 2010.

King T. C/Aggarwal N/Taddeo M/Floridi L, "Yapay Zekâ Suçu: Öngörülebilir Tehditleri ve Çözüm Yolları Üzerine Disiplinler Arası Bir Analiz" in Hasan Dursun (Çev.), Yener Ünver (Ed.), Karşılaştırmalı Güncel Ceza Hukuku Serisi 21, Ceza Hukukunda Robot, Yapay Zeka ve Yeni Teknolojiler, Seçkin Yayıncılık, 2021, s. 247-288.

Koca M/Üzülmez İ, Türk Ceza Hukuku Genel Hükümler, 13. Baskı, Seçkin Yayıncılık, 2020.

Koca M/Üzülmez İ, Türk Ceza Hukuku Özel Hükümler, 7. Baskı, Adalet Yayınevi, 2020.

Koenig A, "'Half the Truth is Often a Great Lie': Deep Fakes, Open Source Information, and International Criminal Law", 2019, 113, American Journal of International Law, s. 250-255.

Koopman M/Rodriguez A. M/Geradts Z, "Detection of Deepfake Video Manipulation", 2018, The 20th Irish Machine Vision and Image Processing Conference, IMVIP 2018, s. 133-136, <https://www.researchgate.net/publication/329814168_Detection_of_Deepfake_Video_Manipulation/link/5c1bdf7da6fdccfc705da03e/download> Erişim Tarihi 25.10.2019.

Korshunov P/Marcel S, "Vulnerability Assessment and Detection of Deepfake Videos", 2019, Idiap Publications, The Idiap Research Institute, s. 1-6, <http://publications.idiap.ch/downloads/papers/2019/Korshunov_ICB_2019.pdf> Erişim Tarihi 24.10.2019.

Kshetri N, "China's Social Credit System: Data, Algorithms and Implications",

2020, March/April, IT Professional, s. 14-18.

Külçür İ. E, Ceza Hukukunda Yer Bakımından Uygulama, On İki Levha Yayıncılık, 2017.

Lantwin T, "Deep Fakes - Düstere Zeiten für den Persönlichkeitsschutz? Rechtliche Herausforderungen und Lösungsansätze", 2019, 9, MMR-Zeitschrift für IT-Recht und Recht der Digitalisierung, s. 574-578.

Lantwin T, "Strafrechtliche Bekämpfung missbräuchlicher Deep Fakes – Geltendes Recht und möglicher Regelungsbedarf", 2020, 2, MMR-Zeitschrift für IT-Recht und Recht der Digitalisierung, s. 78-82.

Li Y/Lyu S, "Exposing DeepFake Videos By Detecting Face Warping Artifacts", 2019, arXiv:1811.00656v3, s. 46-52, <https://arxiv.org/abs/1811.00656> Erişim Tarihi 24.10.2019.

Lossau N, "Deep Fake: Gefahren, Herausforderungen und Lösungswege", 2020, 382, Analysen und Argumente, Konrad-Adenauer-Stiftung, s. 1-9.

Maden M, Ceza Hukukunda Kişisel Verilerin Korunması, Adalet Yayınevi, 2021.

Mohsin K, "Yapay Zekânın Düzenlenmesi ve Yapay Zekâ Suçları" in Jülide Yaşar (Çev.), Yener Ünver (Ed.), Karşılaştırmalı Güncel Ceza Hukuku Serisi 21, Ceza Hukukunda Robot, Yapay Zeka ve Yeni Teknolojiler, Seçkin Yayıncılık, 2021, s. 229-245.

Nabiyev V, Yapay Zeka, 6. Baskı, Seçkin Yayıncılık, 2021.

Nguyen T. T/Nguyen C. M/Nguyen D. T/Nguyen D. T/Nahavandi S, "Deep Learning for Deepfakes Creation and Detection", 2019, arXiv:1909.11573, s. 1-16, <https://arxiv.org/abs/1909.11573> Erişim Tarihi 24.10.2019.

Orta M, Bilişim Suçları ve Elektronik Delillerin Toplanması Muhafazası Değerlendirilmesi Sunulması (Adli Bilişim), Yetkin Yayınevi, 2015.

Öhman C, "Introducing the Pervert's Dilemma: A Contribution to the Critique of Deepfake Pornography", 2019, February, Ethics and Information Technology, s. 1-17.

Özbek V. Ö, "İnternet Kullanımında Ortaya Çıkabilecek Bazı Ceza Hukuku Sorunları", 2002, 4(1), Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, s. 101-158.

Özbek V. Ö/Doğan, K/Bacaksız, P/Tepe, İ, Türk Ceza Hukuku Genel

Hükümler, 7. Baskı, Seçkin Yayıncılık, 2016.

Özgenç İ, Türk Ceza Hukuku Genel Hükümler, 16. Bası, Seçkin Yayıncılık, 2020.

Pfefferkorn R, "'Deepfakes' in the Courtroom", 2020, 29(2), Boston University Public Interest Law Journal, s. 245-276.

Pirim H, "Yapay Zeka", 2006, 1(1), Journal of Yaşar University, s. 81-93.

Ramar S, Artificial Intelligence How It Changes the Future, Kendi Basımı (Independently Published), 2019, <https://www.scribd.com/document/466365329/Artificial-Intelligence-How-It-Changes-the-Future> Erişim Tarihi 25.10.2019.

Reinsel D/Gantz J/Rydning J, The Digitization of the World - From Edge to Core, IDC White Paper, 2018.

Russell S. J/Norvig P, Artificial Intelligence A Modern Approach, Third Edition, Pearson Publishing, 2011.

Sabir E/Cheng J/Jaiswal A/AbdAlmageed W/Masi I/Natarajan P, "Recurrent Convolutional Strategies for Face Manipulation Detection in Videos", 2019, arXiv:1905.00582v3, s. 80-87, <https://arxiv.org/abs/1905.00582v3> Erişim Tarihi 24.10.2019.

Sarı M/Özbayoğlu A. M, "Classification of Turkish Documents Using Paragraph Vector", 2018, 2018 International Conference on Artificial Intelligence and Data Processing (IDAP), s. 1-5, <https://ieeexplore.ieee.org/document/8620813> Erişim Tarihi 24.10.2019.

Sınar H, "İnternetin Ortaya Çıkardığı Hukuki Sorunlara Bir Ceza Hukuku Yaklaşımı", 2001, 17(1-2), Milletlerarası Hukuk ve Milletlerarası Özel Hukuk Bülteni, s. 355-372.

Siekierski B. J, Deep Fakes: What Can Be Done About Synthetic Audio and Video?, Brief Series Publication No. 2019-11-e, Library of Parliament, 2019.

Solo A. M. G, "Combating Online Defamation and Doxing in the United States", 2019, The 20th International Conference on Internet Computing and Internet of Things, s. 75-77, <https://www.researchgate.net/publication/334604707_Combating_Online_Defamation_and_Doxing_in_the_United_States/link/5d35856ba6fdcc370a5495c3/download> Erişim Tarihi 24.10.2019.

Sönmez G/Çelik E, "Anonimlik ile İllegalite Arasında: Deep Web, Dark Web ve Devlet Dışı Silahlı Aktörlerin Uluslararası Siber Faaliyetleri", 2020, 22(1), Güvenlik Çalışmaları Dergisi, s. 66-88.

Sukhodolov A. P/Bychkov A. V/Bychokova A. M, "Yapay Zekâ Teknolojileri Kullanılarak İşlenen Suçlar İçin Ceza Politikası: Devlet, Sorunlar, Beklentiler" in Jocelyne Alayan (Çev.), Yener Ünver (Ed.), Karşılaştırmalı Güncel Ceza Hukuku Serisi 21, Ceza Hukukunda Robot, Yapay Zeka ve Yeni Teknolojiler, Seçkin Yayıncılık, 2021, s. 207-214.

Tezcan D/Erdem M. R/Önok M, Teorik ve Pratik Ceza Özel Hukuku, 18. Baskı, Seçkin Yayıncılık, 2020.

Tezcan D/Erdem M. R/Önok M, Uluslararası Ceza Hukuku, 4. Baskı, Seçkin Yayıncılık, 2017.

Thornton P/Fromlowitz P/Sylla A/Fleeson R/Pennisi M. K, "Deepfakes: An EU and U.S. Perspective", 2020, Spring/Summer, Hogan Lovells-Global Media Technology and Communications Quarterly (GMCQ), s. 30-35.

Thornton P/Sylla A/Fromlowitz P, "The War against Deepfakes", 2020, 285, Managing Intellectual Property, s. 29-30.

Turan M, Bilişim Hukuku, Seçkin Yayıncılık, 2016.

Uşaklıoğlu A. Y, Dijital Hukuk, 2. Baskı, Seçkin Yayıncılık, 2021.

Wagner T. L/Blewer A, "'The Word Real Is No Longer Real': Deepfakes, Gender, and the Challenges of AI-Altered Video", 2019, 3(1), Open Information Science, s. 32-46.

Waldemarsson C, Disinformation, Deepfakes & Democracy, The Alliance of Democracies Foundation, 2020.

Walorska A. M, "Deepfakes & Desinformation", 2020, Mai, Friedrich-Naumann-Stiftung für die Freiheit, s. 1-31.

Wittmer S/Steinebach M, "Computergenerierte Kinderpornografie zu Ermittlungszwecken im Darknet", 2019, 10, MMR-Zeitschrift für IT-Recht und Recht der Digitalisierung, s. 650-653.

Yamaoka-Enkerlin A, "Disrupting Disinformation: Deepfakes and the Law", 2020, 22(3), New York University Journal of Legislation and Public Policy, s. 725-750.

Yavuz C, Cinsel İçerikli Görüntülerin Rıza Dışı Paylaşımı İntikam Pornosu, Seçkin Yayıncılık, 2021.

http://www.kylesconverter.com/
https://assets.publishing.service.gov.uk/
https://capitol.texas.gov/
https://deeptracelabs.com/
https://deepware.ai/
https://dictionary.cambridge.org/
https://digital-strategy.ec.europa.eu/
https://docs.house.gov/
https://eur-lex.europa.eu/
https://intelligence.house.gov/
https://jsis.washington.edu/
https://law.lis.virginia.gov/
https://leginfo.legislature.ca.gov/
https://lis.virginia.gov/
https://malegislature.gov/
https://statutes.capitol.texas.gov/
https://towardsdatascience.com/
https://uscode.house.gov/
https://www.abc.net.au/
https://www.berliner-zeitung.de/
https://www.bu.edu/
https://www.congress.gov/
https://www.merriam-webster.com/
https://www.reuters.com/
https://www.vice.com/
https://www.wsj.com/
https://www.yourdictionary.com/
https://www.youtube.com/