DEEPFAKE: GERÇEKLİK ALGISINI TEMELDEN SARSAN TEKNOLOJİ

Dr. Batuhan Mumcu – Kültür ve Turizm Bakan Yardımcısı

2022 yılında, Ukrayna'da devlet televizyonu ‘hack’lendi ve Devlet Başkanı Volodimir Zelenski'nin ordusuna silah bırakma çağrısında bulunduğu bir video yayınlandı. Görüntüler sosyal medyada da hızla dolaşıma girdi. Olayın ardından derhal resmi makamlarca videonun sahte olduğu açıklansa da görüntüler ülkede kısa süreli bir panik havası yaşanmasına neden oldu.

2023 yılının son aylarında, Papa Francis’in “beyaz puf mont” giymiş görüntüsü sosyal medyada milyonlarca kişi tarafından paylaşıldı. Görüntü oldukça ikna ediciydi. Ne var ki gerçek değildi. Bir yapay zekâ algoritması tarafından oluşturulmuştu.

Bu örnekler, iletişim çağında karşı karşıya olduğumuz en yeni ve belki de en tehlikeli tehdidi oldukça net bir şekilde gözler önüne seriyor: Gerçekliğin kendisini taklit eden, hatta yerinden eden bir teknoloji: Deepfake.

DEEPFAKE NEDİR VE NEDEN TEHLİKELİDİR?

Türkçeye farklı şekillerde çevrilmeye çalışılsa da, henüz üzerinde uzlaşılmış yerli bir karşılığı bulunmadığından özgün haliyle “deepfake”, İngilizce “deep learning” (derin öğrenme) ve “fake” (sahte) sözcüklerinin birleşiminden oluşur. Yapay zekâ ile eğitilmiş derin öğrenme algoritmaları kullanarak bir kişinin görüntüsünü, sesini ve mimiklerini taklit edebilen dijital içeriklere verilen isimdir. Terim, ilk kez 2017 yılında Amerika merkezli bir sosyal medya platformu olan Reddit platformundaki kullanıcılar tarafından yayılan sahte videolarla popülerleşmiştir (Chesney & Citron, 2019).

Bu teknolojiyle üretilmiş içerikler, bireysel mahremiyeti ihlal etmekle kalmaz; siyasal, ekonomik ve toplumsal güvenliğe de doğrudan zarar verebilir. Bir liderin hiç söylemediği sözleri söylediği izlenimini vermek, bir gazetecinin sahte bir itirafta bulunduğu videoyu dolaşıma sokmak veya bir şirket CEO’sunun yatırımcıları yanıltacak açıklamalar yapmış gibi gösterilmesi; bu teknolojiyle artık mümkündür.

Deepfake teknolojisiyle oluşturulmuş bir içerikle, bir devlet yetkilisi başka bir ülkeye savaş ilan ediyormuş gibi gösterilebilir. Bir askerî yetkili, kamuoyuna moral bozucu açıklamalarda bulunuyormuş gibi sunulabilir. Yani artık bir video gördüğümüzde, “bu gerçekten oldu mu?” sorusu kaçınılmaz hale gelmiştir.

Paylaşılma amaçları bakımından deepfake kullananları Westerlund dört başlık altında toplamıştır. Bunlar; deepfake teknolojisini eğlenme, mizah veya hobi vs. amaçlı kullanan kimseler, siyasi aktörler, manipülasyon tekniğini kullanan art niyetli kişiler, medya sektöründe faaliyet gösteren meşru aktörler (Westerlund, 2019).

İlk örnekleri 2017'de görülse de bugün geldiği nokta, bireylerin yanı sıra devletlerin güvenliğini tehdit edebilecek düzeydedir (Chesney & Citron, 2019).

Nitekim, 2022 yılında Hindistan'da yayılan bir deepfake video, dinî gerilimleri körüklemiş ve haftalar süren protestolara neden olmuştu (BBC, 2022).

İletişim, temelde güvene dayanır. Haberin, görselin, videonun ya da beyanın "gerçek" olduğu varsayımı, tüm medyanın ve kamuoyunun işleyişini mümkün kılar. Ancak deepfake teknolojisi bu varsayımı temelden sarsıyor. Jean Baudrillard'ın "simülasyon" kuramı, bu gelişmeleri öngörmüşçesine anlam kazanıyor: Gerçeğin yerini alan görüntüler, sonunda "hiper-gerçek" bir evren yaratıyor (Baudrillard, 1994). Yani artık bir görüntü gerçeğin değil, gerçeğin bir kopyasının kopyası olabilir.

Deepfake teknolojisinin siyasal iletişimde kötüye kullanılabileceğine dair endişeler de büyüyor. 2024 ABD seçimleri öncesinde, dönemin ABD Başkanı Joe Biden'ın yapay zekâyla oluşturulmuş sahte ses kaydı birçok seçmeni manipüle etmeyi başardı (New York Times, 2024). Benzer bir risk, Türkiye gibi kırılgan bir coğrafyada konumlanan bölgesel aktörlerde daha da yüksek.

TÜRKİYE'DEKİ ÖRNEKLER VE ULUSAL GÜVENLİK BOYUTU

Türkiye, jeopolitik konumu ve bölgesel etkisi nedeniyle dijital manipülasyonların hedefi hâline gelen ülkelerden biridir. Deepfake ülkemizde henüz doğrudan bir kriz yaratmamış olsa da kullanılan teknoloji giderek daha gerçekçi hâle gelmekte ve bu durum, toplumsal algının manipülasyona açık hale gelmesine zemin hazırlamaktadır.

Türkiye'de deepfake teknolojisinin yaygınlaşma biçimi, bugüne dek daha çok eğlence ve parodi amaçlı içeriklerle sınırlı görünmektedir. Bu içerikler ilk bakışta zararsız ve mizahi görünse de TikTok, Instagram ve YouTube Shorts gibi kısa video platformlarında; Cumhurbaşkanı Recep Tayyip Erdoğan başta olmak üzere birçok siyasetçi, sanatçı ve televizyon yüzü, yapay zekâ tarafından oluşturulmuş ses veya yüz kopyalarıyla çeşitli içeriklere konu edilmektedir.

Sadece liderlerin değil, bazı kamu görevlilerinin ya da devlet kurumlarının sözcülerinin de seslendirme veya video montaj teknikleriyle "sözde beyanlarda" bulunuyormuş gibi gösterildiği örnekler zaman zaman sosyal medya dolaşımına girmektedir.

Bu tarz içeriklerin en büyük riski, parodi ile manipülasyon arasındaki sınırın silikleşmesidir. Bugün gülünüp geçilen bir video, yarın ciddi bir bilgi kirliliği aracına dönüşebilir. Özellikle seçim dönemleri, kriz anları ya da diplomatik hassasiyet içeren gündemlerde, bu içeriklerin etkisi tahmin edilenden çok daha yıkıcı olabilir.

Bu nedenle, Türkiye'de henüz büyük bir "deepfake vakası" yaşanmamış olması, tehdidin olmadığı anlamına gelmemelidir. Aksine, bu görece sessizlik; konunun gerektiği ciddiyetle ve zamanında ele alınmasını, yasal ve kurumsal hazırlıkların şimdiden yapılmasını zorunlu kılmaktadır.

Cumhurbaşkanlığı İletişim Başkanlığı'nın kurduğu Dezenformasyonla Mücadele Merkezi, bu tip içerikleri anlık olarak analiz etmekte ve kamuoyunu doğru bilgilendirmektedir.

Ancak doğrulama mekanizmaları teknolojinin gelişme hızı karşısında çoğu zaman yetersiz kalıyor. Washington Post'un 2023'te yaptığı bir araştırmada sahte videoların gerçeklerinden %30 daha hızlı yayıldığı belirtilirken, bu da klasik medya okuryazarlığının artık yetersiz kaldığını gösteriyor.

HUKUKİ VE ETİK SINIRLAR

ABD, Çin ve AB ülkeleri, deepfake içeriğin etik sınırlarını belirlemeye çalışmış, bu konuda 2020 sonrası hızla yasal altyapılarını güçlendirmiştir. Deepfake teknolojisinin kullanımını düzenleyen hukuk sistemlerinin bazıları, bu teknolojinin hukuka aykırı kullanımından doğan sonuçları özel hukukla, bazıları ceza hukukuyla, bazıları ise hem özel hukukla hem de ceza hukukuyla çözmeye çalışmıştır.

Deepfake teknolojisinin kullanımına ilişkin ilk yasal düzenlemeler haliyle söz konusu teknolojinin doğduğu yer olan Amerika'da 2019 yılında yapılmıştır. Amerika'daki düzenlemelerin yapıldığı hemen hemen aynı tarihlerde Çin'de de yasal düzenleme çalışmaları başlamıştır. Avrupa Birliği'nde 2024'te yürürlüğe giren AI Act (Yapay Zekâ Yasası), deepfake içeriklerin açık şekilde etiketlenmesini zorunlu kılmıştır.

Ancak mesele sadece hukuki değil, aynı zamanda etik. Teknolojinin sunduğu bu gücün sınırları nerede başlar, nerede biter? Bu soruyu sadece teknik değil, ahlaki bir sorumlulukla da cevaplamalıyız.

TÜRKİYE'DE HUKUKİ DÜZENLEME VAR MI?

Şu an itibarıyla Türkiye'de doğrudan deepfake içeriklerle mücadele etmeye yönelik henüz kapsamlı bir yasal düzenleme bulunmuyor. Mevcut bazı yasalar, bu içeriklerin oluşturulması veya paylaşılması halinde dolaylı olarak devreye girebilir.

Türk Ceza Kanunu kapsamında; kişisel verilerin izinsiz paylaşılması (Madde 136), özel hayatın gizliliğini ihlal (Madde 134), hakaret (Madde 125) ve iftira (Madde 267) gibi suçlar nedeniyle yargılama yapılabilir. Ayrıca, ilgili fiillerin sorun yarattığı alanlara ilişkin farklı hukuki düzenlemeler kapsamında da çeşitli yargılamalar söz konusu olabilir.

Kişisel Verilerin Korunması Kanunu (KVKK) bireylerin görüntü ve seslerinin rızaları dışında kullanılmasını kişisel veri ihlali saymakta, ancak yapay üretim verilerin kapsamı halen tartışmalıdır.

Ayrıca 2022 yılında Türk Ceza Kanunu'na eklenen 217/A maddesi, yani kamuoyunda bilinen adıyla Dezenformasyon Yasası, "kamu barışını bozmaya elverişli şekilde, halk arasında endişe, korku veya panik yaratmak saikiyle gerçeğe aykırı bir bilgiyi, alenen yaymayı" suç saymaktadır. Bu kapsamda üretilen ve gerçek dışı içeriklerle kamuoyunu yanıltmayı amaçlayan deepfake videolar, eğer kamu düzenini tehdit eder nitelikteyse, bu hüküm çerçevesinde cezai yaptırımla karşılaşabilir. Ancak yasanın uygulanmasında içerik niyeti, yayılma biçimi ve etkisi gibi unsurların dikkatle değerlendirilmesi gerekmektedir.

Türk Medeni Kanunu (TMK), kişilik haklarının korunması kapsamında deepfake içeriklere karşı mağdurlara bazı hukuki imkanlar tanımaktadır. Özellikle TMK m. 24 ve 25 hükümleri uyarınca, bir kişinin sesi veya görüntüsü rızası dışında ve menfaatine aykırı şekilde bir deepfake içerikte kullanıldığında bu durum kişilik hakkı ihlali sayılır.

5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi Hakkında Kanun, içerik sağlayıcıların sorumluluğunu düzenler. Ancak mevcut haliyle, deepfake videoların tespiti ve kaldırılması sürecinde bu yasa teknik açıdan yetersiz kalmaktadır.

Sonuç olarak, Türkiye'de deepfake teknolojisinin doğurabileceği risklere karşı mevcut mevzuatın kısmen koruma sağladığı, ancak teknolojik gelişmelere paralel olarak özel bir yasal çerçeveye duyulan ihtiyacın giderek daha belirgin hale geldiği açıktır.

Türkiye’de de benzer bir düzenleme için Avrupa Birliği’nin 2024'te devreye aldığı AI Act gibi, açıkça deepfake içeriklere işaret eden ve bu içeriklerin “etiketlenmesini” zorunlu kılan bir çerçeve Türkiye için de yol gösterici olabilir.

Ayrıca, devlet yetkililerinin ve kurumlarının görüntü ve seslerinin, yapay içeriklerle izinsiz kullanılmasına karşı “resmî kimlik güvenliği” tanımı yapılarak ciddi ölçüde koruma sağlanması gündeme alınabilir.

TOPLUMSAL FARKINDALIK VE MEDYA OKURYAZARLIĞI

Hukuki düzenlemelerin yanında en az onlar kadar önemli bir mesele de medya okuryazarlığıdır. Toplumun dijital içerikler karşısında sorgulayıcı bir refleks geliştirmesi artık hayati önemdedir.

Toplumun, “gördüğüne değil; doğrulanmış olana inanma” refleksi geliştirmesi bireylerin doğru bilgiye erişmesini sağlayacaktır.

Teknolojik tehditler karşısında yalnızca devletin değil, toplumun da sorumluluğu vardır. Medya okuryazarlığı eğitimleri, bu alanda umut verici adımlardandır. İlköğretim düzeyinden başlayarak müfredatlara, yapay içerik farkındalığını içeren bölümlerin eklenmesiyle, genç nesillerin dijital dünyada daha bilinçli bireyler olmaları hedeflenmektedir.

TRT, Anadolu Ajansı, RTÜK gibi kurumlarımız da “gerçek ile sahte içerik nasıl ayırt edilir” temalı eğitim ve içeriklerle bu sürece katkı sağlamaktadır.

SONUÇ: SAHTE GERÇEKLİK ÇAĞINDA HAKİKATİ ARAMAK

İletişim çağının en büyük zaferi, bireyin sesini küresel ölçekte duyurabilmesiydi. Ancak bugün, aynı teknolojik olanaklar, bireyin sesini bir başkasının ona ait olmayan sesiyle bastırabiliyor.

Deepfake teknolojisi, gerçeğin ve güvenin sınandığı bir dönemi beraberinde getirdi. Bu teknolojinin bazı avantajlar sunduğu ve doğru kullanıldığında faydalı olabileceği kabul edilmelidir. Örneğin; Mona Lisa’yı, Salvador Dali’yi hayattaymış gibi konuşturabilen söz konusu videolar doğru şekilde uygulandığında sanat alanı için olumlu gibi görünürken (Yadav & Salmani,2019; Giasano, 2019) bu durum, siyasal iletişim açısından son derece yıkıcı sonuçlara sebebiyet verme potansiyeline sahiptir. Deepfake içeriklerin kötü niyetli veya yanlış kullanımı durumunda ciddi sorunların ortaya çıkması kaçınılmazdır.

Bu teknolojinin iletişim ortamını tahrip etmesine karşı önlem almak, hem yasalarla hem de medya etiğiyle mümkündür. Ancak en önemlisi, toplumun medya okuryazarlığı düzeyini yükseltmek, “gördüğüne hemen inanmama” refleksini geliştirmek zorundayız. Dijital teknolojilerin insan hayatını önemli

ölçüde değiştirdiği günümüzde klasik medya okuryazarlığının yanında dijital okuryazar olmak önemlidir. Çünkü gerçek, savunulması gereken bir değer olarak artık her zamankinden daha kırılgan.

Ülkemizde de söz konusu tehdide yönelik bir farkındalık gelişmiş; hem dijital altyapının güçlendirilmesi hem de iletişim politikalarının güncellenmesi yoluyla bu tür saldırılara karşı dirençli bir yapı inşa etme yönünde kararlı adımlar atılmaktadır.

Kaynakça

- Baudrillard, J. (1994). Simulacra and Simulation. University of Michigan Press.
- BBC News. (2022). "India deepfake video sparks real-world violence."
- Chesney, R. & Citron, D. (2019). Deepfakes and the New Disinformation War: The Coming Age of Post-Truth Geopolitics. Foreign Affairs, 98(1), 147–155.
- New York Times. (2024). Fake Biden robocall tests boundaries of AI and election law.
- Washington Post. (2023). "Deepfakes spread faster than real videos, study finds."
- Westerlund, M. (2019). The Emergence of Deepfake Technology: A Review. Technology Innovation Management Review, 9(11): 40-53.
- Yadav, D., & Salmani, S. (2019). Deepfake: A Survey on Facial Forgery Technique Using Generative Adversarial Network. 2019 International Conference on Intelligent Computing and Control Systems (ICCS). Jun 27, 2019 – Jun 28, 2019, Secunderabad, India.