

DEEPPFAKE BİLGİ NOTU





DEEPPFAKE BİLGİ NOTU

74

DEEPFAKE BİLGİ NOTU

KVKK Yayınları No: 75

Nisan 2025, Ankara

KİŞİSEL VERİLERİ KORUMA KURUMU

Adres: Nasuh Akar Mahallesi 1407. Sokak No: 4 Çankaya/ANKARA

Telefon: 0 312 216 50 00

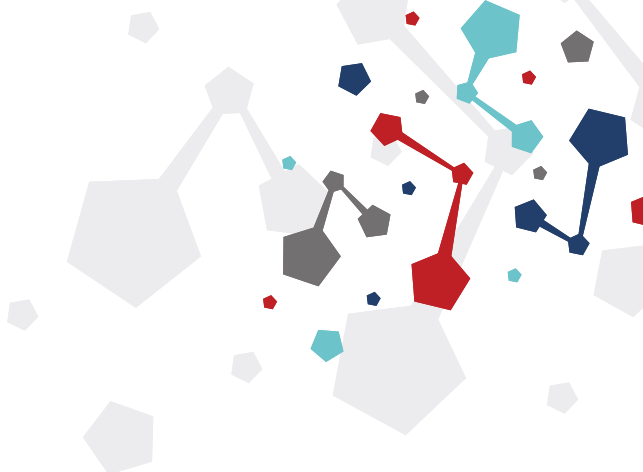
Web: www.kvkk.gov.tr



“Bu kitapta yer alan içeriklerin, bireysel kullanım dışında izin alınmadan kısmen ya da tamamen kopyalanması, çoğaltılması, kullanılması, yayınlanması ve dağıtılması kesinlikle yasaktır. Bu yasağa uymayanlar hakkında 5846 sayılı Fikir ve Sanat Eserleri Kanunu uyarınca yasal işlem yapılacaktır. Ürünün tüm hakları saklıdır.”

©Kişisel Verileri Koruma Kurumu





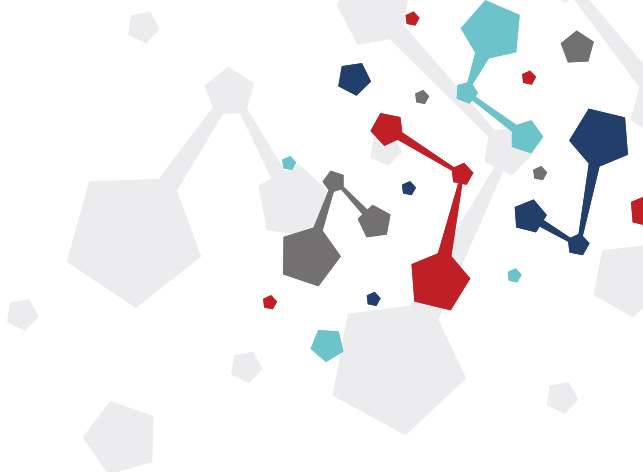
İÇİNDEKİLER

DEEPFAKE BİLGİ NOTU	7
1) Deepfake Nedir?	7
2) Deepfake Ne İşe Yarıyor?	7
3) Deepfake Nasıl Bir Tehdit Oluşturuyor?	8
4) Deepfake Nasıl Tespit Edilir?	8
5) Deepfake Teknolojisinin Tehditlerine Karşı Ne Yapılmalıdır?	9

A decorative vertical bar on the left side of the page, featuring a series of stacked geometric shapes in two shades of blue. The shapes include downward-pointing chevrons, rounded rectangles, and a central zigzag pattern.

DEEPFAKE

BİLGİ
NOTU



DEEPFAKE BİLGİ NOTU

1) Deepfake Nedir?

İngilizce *deep learning* (derin öğrenme) ve *fake* (sahte) kelimelerinin birleşimiyle oluşan *deepfake* (derin kurgu ya da derin sahte) için farklı Türkçe çeviriler kullanılmaktaysa da genel kabul görmüş bir karşılığı bulunmadığından burada da "deepfake" olarak kullanılacaktır. **Deepfake, insanların yüz, hareket ve sesini gerçeğe uygun olacak şekilde taklit etmek veya değiştirmek için yapay zekâ teknikleri aracılığıyla fotoğrafların, videoların veya seslerin kullanılmasıdır.** Bu yöntem ile oldukça gerçekçi içeriklerin oluşturabilmesi için görece az sayıda video, fotoğraf veya ses kaydı kullanılması yeterli olabilmektedir.

2) Deepfake Ne İşe Yarıyor?

Deepfake içerikler sinema sektörü gibi alanların yanı sıra, kişisel amaçlar, reklam, itibarsızlaştırma, finansal veya siyasi yarar elde etme gibi konularda kullanılabilir. Deepfake teknolojisiyle ünlü tablolarda yer alan portrelerin mimikleri hareket ettirilebilmekte veya hayatta olmayan ünlü bir kişi yeniden seyirciyle buluşturulabilmektedir.

3) Deepfake Nasıl Bir Tehdit Oluşturuyor?

Deepfake teknolojisinin insanlar için bir tehdit niteliği taşımasının sebebi kişisel verilerin bir sürece tabi tutularak manipüle edilmesidir. Deepfake'in sahte video ve sahte sesler oluşturarak manipülasyon yapma, finansal zarar oluşturma, siber zorbalık, dolandırıcılık gibi potansiyel tehlike tarafı günümüzde gitgide daha yaygın hale gelmektedir. Özellikle teknolojik olarak dezavantajlı konumda bulunan çocuklar ve yaşlılar, şantaj ve tehdit ile çıkar sağlama amacı güden saldırganlar için önemli bir hedef konumundadır.

Ses ve görüntü gibi kişisel veriler alınıp başka kişisel verilerle karıştırılarak gerçeklikten uzak bir kişisel veri ortaya çıkarılmaktadır. Gerçek olmayan ama içinde gerçek kişisel veri bulunduran karma bir içerik elde edilmiş olur. Elde edilen sahte içerikle, gerçek bir kişisel veri gibi insanları aldatmak mümkün hale gelmektedir. Bu anlamda deepfake içeriklerde kişisel verilere yönelik suç ve kabahatler de ortaya çıkabilmektedir.

4) Deepfake Nasıl Tespit Edilir?

Bir içeriğin deepfake olduğunu anlamanın bazı yolları vardır. Çeşitli kaynaklardan elde edilen bilgilere göre deepfake içeriğe dair aşağıdaki sorular bir ipucu olabilir:¹

- Videodaki kişinin doğal olmayan göz hareketler var mı veya göz kırpmıyor mu?

¹ <https://www.media.mit.edu/projects/detect-fakes/overview/>



- İçerikteki yüz pürüzsüz veya çok kırışık görünüyor mu?
- İçerikteki kişide gözlük varsa gözlükte parlama var mı ya da kişi hareket ettiğinde parlamanın açısı değişiyor mu?
- Görüntüdeki kişinin yüz ifadesi söyledikleriyle aynı duyguyu yansıtıyor mu?
- Baş ve vücut birbiriyle uyumlu hareket halinde mi?
- Saçlardaki tutamlar birbiriyle uyumsuz ya da donuk mu?
- Dişlerde tüm dişlerin ana hatları var mı?
- Yavaşlatıldığında doğal olmayan görüntüler ortaya çıkıyor mu?
- Bir soru sorulduğunda mantıklı bir cevap verebiliyor mu?
- Ses tonunda robotik bir ifade var mı?

5) Deepfake Teknolojisinin Tehditlerine Karşı Ne Yapılmalıdır?

Deepfake içerikler ile birlikte yanlış bilginin yayılmasının önüne geçmek veya kişilerin zarara uğramasını önlemek için en önemli görev gerçek kişilere düşmektedir. Öncelikle, kişiler kişisel verilerinin paylaşımına dikkat etmelidir. Unutulmamalıdır ki deepfake içerikler için en çok kullanılan kaynaklar sosyal medya vb. platformlardır. Örnek olarak deepfake videoların genellikle yüz ve ses verisi kullanılarak oluşturulması düşünüldüğünde, kişilerin sosyal medyada yüzünün ve sesinin görüldüğü içerikleri paylaşmasıyla ilgili bir hassasiyet taşıması önem arz edecektir. Bunlarla birlikte deepfake içeriklerin varlığı ve teh-

ditleri hakkında bilgi sahibi olmak ve farkındalık oluşturmak da önemlidir. Deepfake videoları tespit etmek için sunulan bazı araçlardan faydalanmak da videoların tespit edilebilmesine imkân tanıyabilir.

Birçok deepfake uygulaması ücretli ya da ücretsiz bir şekilde kullanılabilir. Bu yazılım ve uygulamaların kullanım alanlarının sınırlandırılması ve kullanıcıların kullanım amaçlarının kontrol edilmesi gerekmektedir. Herkes tarafından kolayca kullanılmamalıdır.

Deepfake teknolojisinden korunmak için kurumlar; ağ ve siber güvenlik operasyonlarını etkili bir şekilde yönetmeli, merkezi bir raporlama ve izleme birimi oluşturmalı, şirket içi iletişim kanallarını geliştirmeli ve halkla ilişkiler departmanı ile bağlantıyı koparmamalıdır.

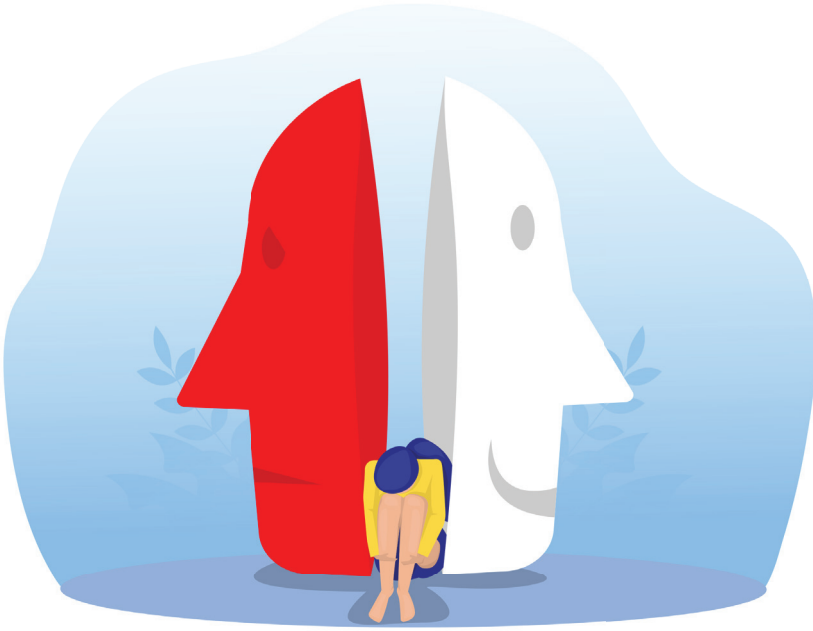
Teknolojinin beraberinde getirdiği risk ve tehditleri bertaraf etmek adına yine teknolojinin kendisine ihtiyaç duyulmaktadır. Bu noktada özellikle sosyal medya ve içerik sağlayıcı platformlarda karakter ya da kimlik hırsızlığı amacıyla deepfake teknolojisinin kullanılmasının engellenmesini sağlayacak anti-deepfake yazılımlarının geliştirilmesi gerekmektedir. Söz konusu yazılımlar ve çözümler dijital kimliğe sahip olan herkes tarafından aktif olarak kullanılmalıdır. Bunların yanında siber güvenlik şirketleri;²

- Deepfake ile oluşturulan içerikleri tespit edecek araçların geliştirilmesi,

² <https://secromix.com/blog/deepfake-nedir-korunma-yollari-neler/>

- Deepfake videolarının incelenmesi,
- Deepfake içerikleri orijinal video veya fotoğraf vb. içeriklerden ayırmak için deepfake
- İçeriğinde kullanılan orijinal içeriklerin referans olması için veri tabanlarının oluşturulması,
- Deepfake teknolojisine ilişkin kullanıcıların farkındalığının artırılması,
- Deepfake ile gerçekleştirilebilecek siber saldırılara karşı savunma yöntemlerinin geliştirilmesi

gibi çeşitli önlemler alabilirler.







Adres: Nasuh Akar Mahallesi
1407. Sokak No: 4
Çankaya / ANKARA
Telefon: 0 312 216 50 00
Web: www.kvkk.gov.tr



kvkkurumu