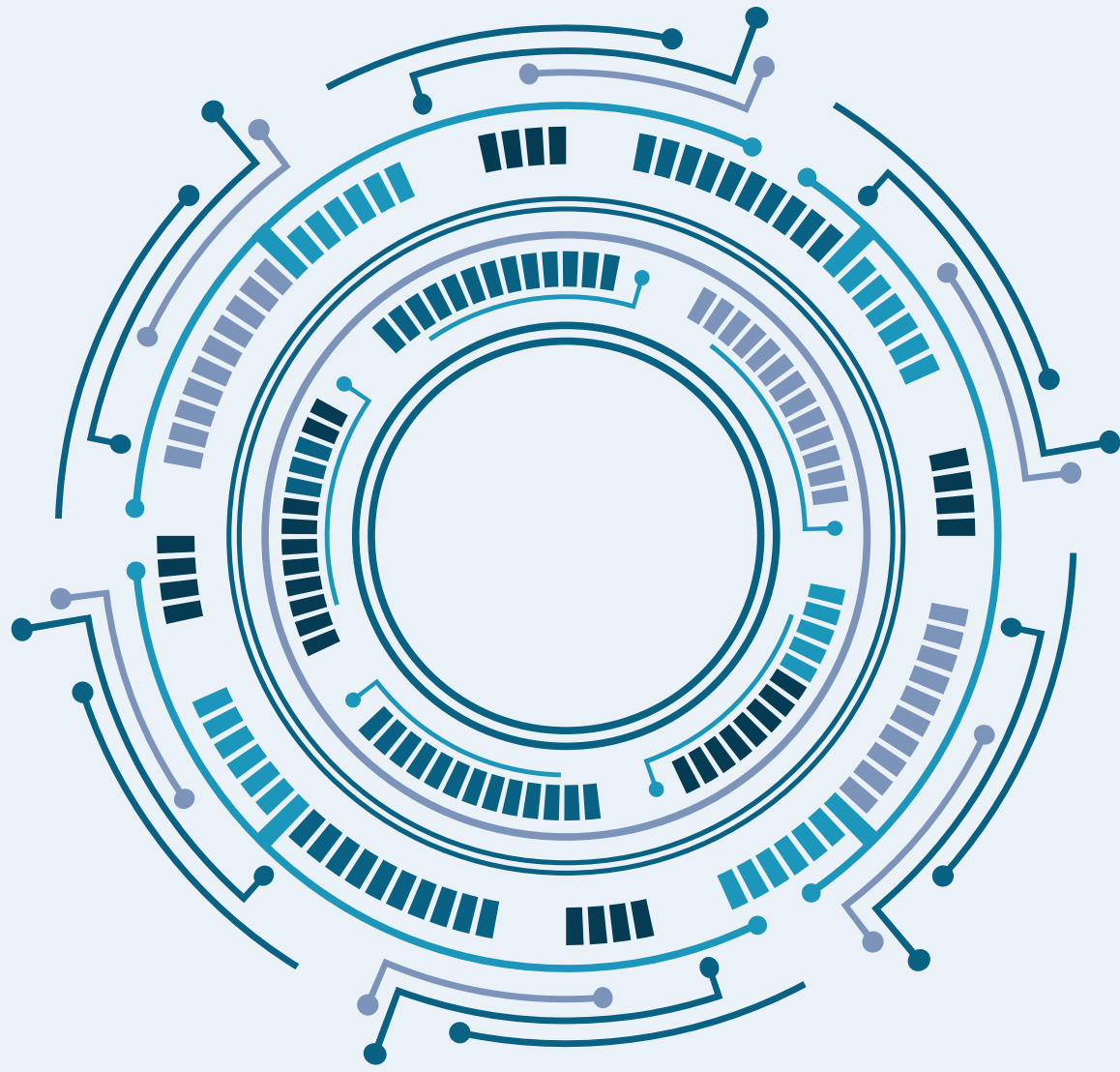




DEEFAKE

VE

KİŞİSEL VERİLERİN KORUNMASI

Deepfake nedir?

Deepfake içerikler genel olarak ne işe yarar?

Deepfake tehdit oluşturur mu?

Deepfake teknolojisinin kötü amaçlarla kullanılması sonucu ortaya çıkan tehditlere karşı ne yapılabilir?



DEEPFAKE NEDİR?

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 bulunmamaktadır.

Genel anlamda deepfake, insanların yüzlerini, hareketlerini ve seslerini gerçeğe uygun olacak şekilde taklit etmek veya değiştirmek için yapay zekâ teknikleri aracılığı ile fotoğrafların, videoların veya seslerin kullanılmasıdır.





DEEPPFAKE İÇERİKLER GENEL OLARAK NE İŞE YARAR?

Deepfake içerikler sinema ve reklam sektörü gibi alanların yanı sıra, kişisel amaçlar için kullanılabilmektedir.

Örneğin deepfake teknolojisi sayesinde ünlü tabloları yer alan portrelerin mimikleri hareket ettirilebilmekte veya hayatta olmayan ünlü bir kişi yeniden seyirciyle buluşturulabilmektedir.





DEEPPFAKE TEHDİT OLUŞTURUR MU?

Deepfake teknolojisi kötü amaçlarla kullanıldığı takdirde, insanlar için tehdit niteliği taşıyabilmektedir. Bu çerçevede kişisel verilerin bir sürece tâbi tutulması sonucunda sahte görüntü ve sahte sesler oluşturulması, siber zorbalık, şantaj, finansal zarar ve dolandırıcılık gibi tehlikeler ortaya çıkmaktadır.

Örneğin ses ve görüntü gibi kişisel verilerin başka kişisel verilerle karıştırılarak gerçeklikten uzak bir kişisel veri meydana getirilebilmektedir. Böylelikle 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.



DEEPFAKE TEKNOLOJİSİNİN KÖTÜ AMAÇLARLA KULLANILMASI SONUCU ORTAYA ÇIKAN TEHDİTLERE KARŞI NE YAPILABİLİR?

Deepfake içerikler ile birlikte yanlış bilginin yayılmasının önüne geçmek veya kişilerin zarara uğramasını önlemek için en önemli görev bireylere düşmektedir. Öncelikle bireyler kişisel verilerinin paylaşımına dikkat etmelidir. Unutulmamalıdır ki; deepfake içerikler için en çok kullanılan kaynaklar sosyal medya vb. platformlardır. Bu nedenle deepfake içeriklerin varlığı ve olası tehditler hakkında bilgi sahibi olmak önemlidir. Diğer yandan deepfake teknolojisinin zararlı etkilerinden korunmak için şirket, kurum ve kuruluşlar; ağ ve siber güvenlik operasyonlarını etkili bir şekilde yönetmeli, merkezi bir raporlama ve izleme birimi oluşturmalı, organizasyonları içinde iletişim kanallarını geliştirmeli ve halkla ilişkiler departmanı ile bağlantı halinde olmalıdır.

Özellikle sosyal medya ve içerik sağlayıcı platformlarda karakter ya da kimlik hırsızlığı amacıyla deepfake teknolojisinin kullanılmasının engellenmesini sağlayacak anti-deepfake yazılımlarının geliştirilmesi son derece önem taşımaktadır.

Öte yandan çeşitli kaynaklara göre:

- Deepfake ile oluşturulan içerikleri tespit edecek araçların geliştirilmesi,
- Deepfake videolarının incelenmesi,
- Deepfake içerikleri orijinal video veya fotoğraf vb. içeriklerden ayırmak için deepfake içeriğinde 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 birtakım önlemlerin alınabileceği öngörülmektedir.

