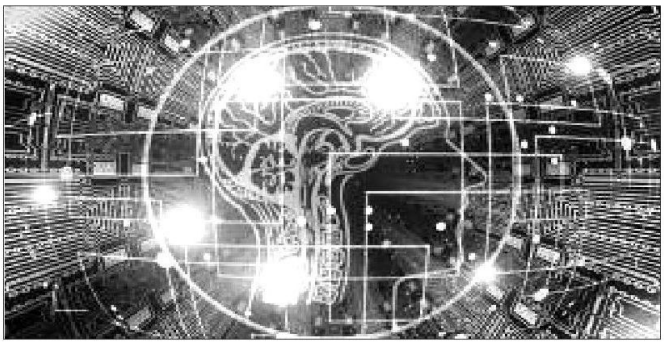

Uzmanından vatandaşlara yapay zeka temelli "deep fake" manipülasyonu uyarısı

ANKARA (AA) - Yapay zeka ve derin öğrenme tekniklerinin kullanımıyla ortaya çıkan derin sahtecilik (deep fake) teknolojisinin yaygınlaşması sahte video ve ses kaydı temelli veri manipülasyonlarını artırarak, birçok kişinin mağdur olmasına neden oluyor. AA'nın, "Yapay Zeka Çağına Doğru" başlıklı dosyasının yedinci haberinde yapay zeka ve derin öğrenme teknikleri kullanarak oluşturulan "deep fake" teknolojisinin sebep olduğu mağduriyetler ele alındı.

Söz konusu teknoloji, kullanıcıların yüzlerinin başka videolara yerleştirilmesi ve ses sentezi tekniklerinin kullanılmasıyla gerçekçi görüntü ve ses üretimine imkan tanıyor. Üretilen bu görüntü ve sesler, başta sosyal medya platformları olmak üzere, dijital platformlarda kullanıldığında birçok olumsuz sonuç ve dezenformasyona neden olabiliyor. OSTİM Teknik Üniversitesi Yapay Zeka Mühendisliği Bölüm Başkanı Dr. Murat Şimşek, deep fake ve yapay zeka tarafından geliştirilen veri manipülasyonları nedeniyle tüketicilerin mağduriyet yaşayabildiklerini söyledi.

Şimşek, yapay zeka uygulamalarının kullanıcıların verdiği verileri kaydettiğine ve bu verileri izinsiz olarak kullanabildiğine dikkati çekerek, "Mesela herhangi bir videoyu yapay zekayla işlediğiniz takdirde artık o video yapay zekanın ürünü oluyor, istemediğiniz görüntü ve ses bilgileriyle istemediğiniz şekilde manipülasyon yapılmasına izin vermiş oluyorsunuz." dedi. Yapay zekay ile sahte fotoğraflar, videolar, görüntüler ve ses kayıtları oluşturulabildiğini dile getiren Şimşek, ABD'de bir şirketin üst düzey yöneticisinin (CEO) yapay zekayla türetilmiş bir video ile yaklaşık 21 milyon dolar zarara uğradığını belirtti.

"Yapay zeka okur yazarlığına sahip olunmalı"

Şimşek, kullanıcıların yapay zeka okur yazarlığına sahip olmalarının önemine işaret ederek, "Yani kabile dönemlerinde eskiden uçak görüldüğünde mızrak atıldığı gibi yapay zekadan kaçmamak lazım. Ancak koşulsuz şekilde de yapay zekanın verdiği her bilgiyi kabul etmemekte fayda var." diye konuştu.

ChatGPT, Microsoft Copilot gibi yapay zeka uygulamalarının her iş için kullanabilir hale geldiklerini anlatan Şimşek, burada elde edilen bilgilerin doğrulamaya muhtaç olduğunu kaydetti.

Şimşek, yapay zeka ürünlerinin oluşturduğu bilgilerin "kesin doğru" gibi kullanıldığında mağduriyetlere yol açabileceğini anlatarak, şu değerlendirmede bulundu:

"Yanlış bilgileri doğru olarak kullanabiliyoruz. Bu tarz durumlar yaşamamak için yapay zekayı hayatımıza entegre etmeliyiz. Ancak yapay zekanın elde ettiğimiz bilgilerini de sorgulamalıyız. Örnek vermek gerekirse bir videoyu gördüğümüzde buna hemen inanıp işlem yapmamamız lazım. Çünkü yapay zekayla manipülasyon yapmak artık çok daha kolay. Eskiden daha amatör şekilde montaj ve manipülasyon gerçekleştirilebiliyordu. Ancak şu anda yapay zekayla hem yüksek kalitede hem de kısa sürede veri manipülasyonu ve video montajı yapılabiliyor. Onun için her gördüğümüze inanmayalım. Yapay zeka okur yazarlığına sahip olalım ve yapay zeka araçlarını bilinçli olarak kullanalım."

"Derin sahtecilikle mücadele teknikleri geliştirilmeli"

İftira, şantaj, manipülasyon ve propagandanın sık karşılaşılan mağduriyetler olduğunu dile getiren Şimşek, özellikle video ve ses montajıyla oluşturulan sahte görüntülerin kişilerin itibarını zedeleyerek maddi ve manevi zararlara yol açabileceğini söyledi. Şimşek, "deep fake" tabir edilen içeriklerin kişilerin mahremiyetlerine de zarar verebileceğini belirterek, "Sahte videolar veya ses kayıtları aracılığıyla yapılan manipülasyonlar, kamuoyunu yanıltarak dezenformasyona neden olabilir. Mağduriyetlerin ve bu teknolojinin kötüye kullanımının engellenmesi için hem teknoloji şirketlerinin hem de yasal düzenlemelerin güçlendirilmesi gerekiyor. Toplumun bilinçlendirilmesi ve derin sahtecilikle mücadele eden tekniklerin geliştirilmesi de büyük önem taşıyor."