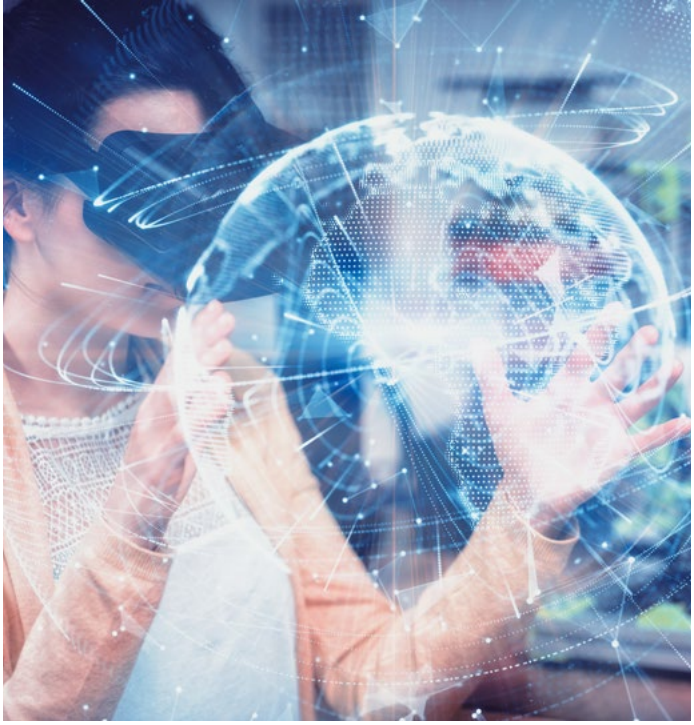
thinktech
STM Teknolojik Düşünce Merkezi



Artırılmış Gerçeklik ve Gizlilik Riskleri

Yapay zekâ, makine öğrenmesi, yüksek hızlı internet, süper bilgisayarlar ve bulut bilişim gibi teknolojiler günlük hayatta yerlerini sağlamlaştırırken; sanal gerçeklik, artırılmış gerçeklik ve karma gerçeklik kavramları da dikkatleri üzerlerine çekmeye devam ediyor.

Sanal gerçeklik, kullanıcısına verdiği sentetik deneyimlerle farklı bir dünya vadediyor. Ancak sanal gerçeklikten farklı olarak, sentetik deneyimleri gerçek dünya ile birleştirerek kullanıcısının gerçek çevresi ile de etkileşime girmesine imkân veren artırılmış gerçeklik, sanal dünyanın aksine, gerçek yer, zaman ve görsel etkileşimine ihtiyaç duyuyor. Bu özelliği nedeniyle artırılmış gerçeklik, kullanıcıların hareketlerinin izlendiği, görsellerinin kaydedildiği ve özel hayatlarının ihlal edilebildiği bir dizi riski beraberinde getiriyor[1].

2021 yılında küresel pazarda 108 milyar dolarlık bir büyüklüğe sahip olan ve 2024 yılına kadar pazar değerinin 162 milyar dolara çıkması beklenen sanal ve artırılmış gerçeklik teknolojilerinin, insanları ve kuruluşları gelecekte nasıl etkileyeceğinin ve potansiyel risklerinin detaylı bir şekilde incelenmesi gerekiyor[2].

Artırılmış Gerçekliğin Olumlu ve Olumsuz Etkileri

Artırılmış gerçeklik tüketicilere benzersiz bir deneyim imkânı sunuyor. Ticari anlamda firmaların müşterilerine çok çeşitli hizmetleri sunmasına yardımcı olurken, tüketiciler almayı düşündükleri eşyaların evlerinde nasıl görüneceğini veya bir kıyafetin kendilerine yakışıp yakışmayacağını bu hizmetleri satın almadan tecrübe edebiliyor. Turistik bölgelerde gezginlere doğayla ilgili güzellikleri ve detayları kamera görseli üzerinden gösterebilen akıllı telefon uygulamaları tur rehberlerinin yerini alma potansiyeli taşıyor.

Hiç bilmediğiniz bir araç veya ekipmanın tamirinde bütün kullanma kılavuzunu okumaya çalışmak yerine artırılmış gerçeklik, gerekli işleme doğrudan ulaşılmasını sağlıyor ve nasıl hareket edilmesi gerektiğini gösterebiliyor.

Artırılmış gerçekliğin bir diğer ticari avantajı da reklam alanında öne çıkıyor. Uygulandığı her yerde firma reklamlarının kullanılabilmesi tüketiciye daha kolay ulaşılmasını sağlıyor.

Reklam potansiyeli markaların çok çeşitli promosyonlarla tüketici karşısına çıkmasına da olanak sunuyor. Tekdüzeliği ortadan kaldırarak rekabeti güçlendirme açısından öne çıkabilen bu teknoloji her geçen gün yeni avantajlarla insanların hayatında yer ediniyor[3].

1 https://spectrum.ieee.org/augmented-reality-and-the-surveillance-society
2 https://theappsolutions.com/blog/development/augmented-reality-challenges/
3 https://www.intelivita.com/blog/benefits-of-augmented-reality/

Artırılmış gerçeklik gelişen teknolojilerin ışığında güçlenmeye devam ediyor. Ancak bazı uzmanlar, iş modelleri açısından henüz sürdürülebilir bir artırılmış gerçeklik uygulamasının oluşturulamadığına dikkat çekiyor. Bunun sebebi olarak, teknolojinin henüz çok erken evrelerinde olması gösteriliyor. Pokemon GO gibi hızla parlayan ve insanların hevesi geçtiğinde yeni içeriklere devam edemeyen artırılmış gerçeklik uygulamaları bu teknolojinin kullanım açısından vazgeçilmez bir duruma gelmeden yeterli başarı elde edemeyeceğini gösteriyor. Bununla birlikte, ortaya çıkan gizlilik ihlali olasılığı, artırılmış gerçeklik ve benzeri teknolojilerin en büyük dezavantajını oluşturuyor. Bu sorunun aşılmasında iki ayrı yaklaşım öne çıkıyor. Öncelikle artırılmış gerçeklik teknolojisini kullanacak kişilerin güvenlik zafiyetleri ve olası riskler konusunda yeterince bilgilendirilmesi ve bilinçlendirilmesi gerekiyor[2].

Yüz tanıma uygulamaları gibi yıllardır kullanılan teknolojilerin artırılmış gerçeklik ile bir araya gelmesiyle kişilerin mahremiyeti konusu soru işaretlerine yol açıyor. Artırılmış gerçeklik gözlüklerine yüklenebilen bir uygulama, yüz tanıma ile bireylerin algılanmasına ve bu kişilerin isim, soy isim ile birlikte diğer kişisel bilgilerinin de görünmesine yardım edebiliyor. Her ne kadar masum gibi görünse de bu uygulama kişisel verilerin ihlalinde önemli bir risk yaratıyor. Benzer şekilde evinize yerleştireceğiniz bir mobilya için artırılmış gerçeklik ile odaların ölçülerinin alınması, kitaplığınızda bulunan kitapların adlarının taranarak listelenmesi veya mutfağınızda hangi yiyeceklerin bulunduğunun kaydedilmesi özel hayatın ihlali sayılabiliyor. Bu örnekler tüketici davranışlarının ölçülmesi ve analizi için masum gibi görünse de kişilerin sınıflandırılması veya istenmeyen etiketlemelere maruz kalınmasına neden olma potansiyeli açısından tehlike arz ediyor[4].

Savunma Sanayiinde Artırılmış Gerçeklik Neler Vadediyor?
Artırılmış gerçeklik, savunma sanayiinde de ilgiyle karşılanıyor. Taktik artırılmış gerçeklik adıyla orduların kullanımına sunulan teknoloji, askerlerin coğrafi konumlarının takip edilmesine imkân verirken, kullanılan bir başlık ekranı ile askerlere de savaş alanı hakkında detaylı bilgi sunabiliyor. Hedeflerin belirlenmesi, uydu izleme ile görünmeyen hedeflerin dahi işaretlenmesi ve riskli güzergâhların önceden yapılacak uyarıyla tercih edilmemesinin sağlanması taktik artırılmış gerçeklik ile mümkün kılınıyor.

Artırılmış gerçeklik, insanların savaşa yaklaşım şeklini değiştirme olanağı tanıyor. Doğru teknoloji ile kullanıcılar daha fazla operasyonel ve durumsal farkındalık kazanabilirken, durumları hakkında daha iyi yargılarda bulunma imkânı sağlanıyor.

Artırılmış gerçeklik, daha az maliyetli ve sürükleyici olan başarılı muharebe eğitimi deneyimlerine imkân vererek, birliklerin gerçek hayat senaryolarına daha hazırlıklı olmasını sağlayabiliyor, hatta daha etkili askeri araç ve ekipmanlar oluşturmaya bile yardımcı olabiliyor[5].

Ancak artırılmış gerçeklik teknolojisinin faaliyet gösterebilmesi için ihtiyaç duyduğu konum ve görsel bilgi de bir diğer açıdan risk oluşturuyor. Askerlerin bağlı olduğu artırılmış gerçeklik sisteminin düşman güçler tarafından hack'lenmesi, askerlerin konumlarının kolaylıkla tespiti ile hayati risk yaratırken, başlık ekranlarına gönderilecek yanlış bilgilerle hedeflerin karıştırılması veya askerlerin tuzağa çekilmesi gibi riskleri de içinde barındırıyor.

Artırılmış Gerçekliğin Gözetim Amaçlı Kullanım Olasılığı
İster sivil ister askeri amaçlı kullanım olsun, artırılmış gerçekliğin ihtiyaç duyduğu veriler, özel hayatın ihlalinden ticari kuruluşlara istem dışı veri sağlanmasına kadar birçok hukuksal ve etik riskleri beraberinde getiriyor.

4 https://www.theverge.com/c/22746078/ar-privacy-crisis-rethink-computing
5 https://www.xrtoday.com/augmented-reality/what-impact-is-ar-having-on-the-military-sector/

Facebook'un yürüttüğü Aria Projesi, gelecekte akıllı gözlüklerin günümüz akıllı telefonlarının yerine geçmesini hedefliyor. Bu projede kullanılacak akıllı gözlükler kullanıcılarına sürekli reklam ve görsel bilgi sunarken, aynı anda görünen bütün verileri kaydederek başka insanlarla ilgili özel bilgiler dahil her şeyin hizmet veren kurumca elde edilme olasılığını gündeme taşıyor. Bu olasılık günümüz toplumunda endişeyle karşılanırken, benzer tip birçok uygulamanın bu teknolojiyi kullanabilmesi için benzer riskleri alması gerektiğini gösteriyor[1].

Herhangi bir kullanıcının artırılmış gerçeklik cihazının hack'lenmesi özel hayatın ve kişisel bilgilerin gizliliğinin ihlal edilmesi riskini yaratırken, bu hizmeti sunan kurumların ne gibi güvenlik önlemleri alacağı hâlen tartışılıyor. Artırılmış gerçeklik cihazlarından elde edilen verilerin yerel veya bulut sistemlerde mi yoksa alternatif veri merkezlerinde mi depolanacağı, bu depolama alanının güvenliğinin nasıl sağlanacağı ve bu verilerin hizmet veren kuruluşlar tarafından başka kişilerle paylaşım sınırlamaları tartışmaların başında geliyor.

Artırılmış Gerçekliğin Gizlilik Sorunlarına Çözümler

Artırılmış gerçeklik teknolojisi ister Wi-Fi, ister kablolu, ister 5G olsun mutlaka bir internet bağlantısına ihtiyaç duyuyor. Bu teknoloji ile ilgili uygulama verileri ağırlıklı olarak bulut sistemlerde depolandığından her bağlantı türünde bir risk ortaya çıkabiliyor. Bağlantıların hack'lenmesi veya bozulmasına karşı ise güçlü şifreleme teknolojileri ve bir dizi doğrulama uygulamaları mevcut gizlilik endişelerine çözüm yaratma potansiyeline sahip bulunuyor[6].

5G teknolojisi iletişimi güçlendirdiği gibi sanal ve artırılmış gerçeklik uygulamalarını da güçlendiriyor. Artırılmış gerçeklik teknolojisi bağlantı hızı arttıkça daha efektif bir performans sergiliyor. Bununla birlikte çevre ve aktiviteler hakkında toplanan verilerin yoğunluğu ile de başa çıkılabiliyor. 5G teknolojisinin temelinde güvenlik unsurları titizlikle tasarlandığından, artırılmış gerçeklik gizlilik konusundaki endişeleri de bir nebze azaltılabiliyor. Her 5G ağ bileşeni, aynı ağda olsa bile, herhangi bir işlemden önce kimliği doğrulayarak yetkilendirmeye ihtiyaç duyuyor. Bu uygulama, kimlik sahtekârlığı güvenlik açıklarını önlemek için Wi-Fi 6 gibi çeşitli erişim protokolleri aracılığıyla gerçekleştirilebiliyor.

5G teknolojisi ayrıca bir kullanıcının kimliğinin yetkisiz olarak alınmasını önlemek ve sahte baz istasyonu veya vatoz saldırıları yoluyla gözetime karşı koruma sağlamak için bir abonelik tanımlayıcısı kullanıyor. Bu sayede bütün bağlantıların kimler tarafından gerçekleştirildiği kontrol altında tutulabiliyor[7].

Artırılmış gerçeklik cihazlarının güvenliğinin iki aşamalı olarak düşünülmesi gerekiyor. İlk aşama internet bağlantısı için kullanılan yöntemin güvenliğini oluştururken, ikinci aşama ise kullanılan cihazın donanımsal olarak güvenli kılınması yöntemini kapsıyor.

Build38 isimli bir şirket bu alanda kullanılabilecek bir bağlantı güvenlik anahtarı benzeri donanım hizmeti sunuyor. Şirketlere sundukları Güvenilir Uygulama Kiti (Trusted Application Kit -T.A.K) özellikle mobil bankacılık gibi uygulamaların güvenliğinde tercih ediliyor. Sağlık, endüstriyel IoT ve finans sektörü hedefiyle hareket eden şirket, donanımsal güvenlik ile yazılımların hack'lenmesi veya dışarıdan yetkisiz modifiye edilmesi gibi risklere karşı güvenlik çözümleri yaratıyor[8].

Kablosuz bağlantı teknolojilerinde kullanılan WPA3 gibi en son şifreleme sistemleri bile bazı güvenlik açıkları içeriyor. Bu açıkların giderilmesi amacıyla yapılacak güncellemeler ise hat genişliği ve bağlantı hızı sorunlarına neden olabiliyor. Kurumsal WPA2 şifrelemeleri daha stabil bir güvenlik altyapısı oluştururken, birçok artırılmış gerçeklik destekli giyilebilir akıllı cihaz bu güvenlik standartlarını henüz desteklemiyor. Şifreleme teknolojilerinin daha yaygın şekilde desteklenmesi güvenlik ve gizlilik sorunlarına bir çözüm olasılığı sunuyor.

6 https://www.xrtoday.com/augmented-reality/what-cyber-security-risks-are-there-in-ar/
7 https://www.verizon.com/business/resources/articles/s/how-5g-can-help-augmented-reality-security-risks-and-privacy/
8 https://aithority.com/technology/virtual-reality-technology/why-organizations-should-be-wary-of-the-security-risks-posed-by-augmented-reality/

Artırılmış gerçeklik cihazlarının verilerinin bulut veya cihaz üzerinde saklanmasındansa daha yerel bir sunucuda veya kişisel bilgisayarlarda saklanması veri güvenliği açısından bir önlem olarak düşünülüyor[9].

ABD'nin Kuzey Karolina Üniversitesi araştırmacılarının yaptığı bir çalışma ise özellikle akıllı gözlük benzeri artırılmış gerçeklik uygulaması kullanan cihazlarda kullanılacak bir görsel şifreleme yönteminin görüntü özelinde gizliliği artırabileceğini gösteriyor. Görsel Kod adı verilen sistem, çoklu görsellerin birleşiminden oluşan bir şifreleme yöntemi ile sadece akıllı cihazda anlam verilecek şekilde bir araya gelecek resimlerin veri transferi sırasında ele geçirilmesi durumunda anlaşılır olmayacak şekilde değiştirilmesini sağlıyor.

Araştırmacılar bu güvenlik önleminin bir noktaya kadar yeterli olabileceğini, ancak bütün güvenlik risklerinin ortadan kalkması için hâlen kamera sisteminin devre dışı bırakılması veya kapatılmasının gerekli olacağını belirtiyor. Aksi durumda artırılmış gerçeklik uygulaması ile çalışan bütün kameralı akıllı cihazlardan görüntü alınma riski devam ediyor[10].

Teknoloji her geçen gün hızla gelişmeye devam ediyor. 90'lı yıllarda *Uzay Yolu* veya *Yıldız Savaşları* gibi bilim kurgu dizileri ve filmlerinde bahsi geçen hologram, sanal gerçeklik ve akıllı gözlükler gibi teknolojiler gerçek hayatta yer edinmeye başlıyor. Artırılmış gerçeklik teknolojisi de bir bilim kurgu ürünü gibi görünse de yaygınlaşan kullanım alanlarıyla geleceğin vazgeçilmez teknolojilerinden biri olma yolunda ilerliyor. Ancak her yeni teknolojide yaşanan güvenlik ve gizlilik zafiyetleri, kullanıcıların kişisel bilgilerinin çalınma veya kötü amaçlı kullanılma olasılığı ve bu teknolojilerin amacı dışında yasal olmayan süreçlerde tercih edilme riski çeşitli endişeleri gündeme getiriyor. Bu teknolojiye uygun güvenlik altyapılarının oluşturulması ve ülkelerin gerek yerel gerekse uluslararası regülasyonlarla ciddi kontrol mekanizmaları oluşturması gizlilik ile ilgili kaygıları bir nebze olsun azaltabilir. Sivil anlamda yaşanan kaygılara bulunacak çözümler çeşitlilik göstermekle beraber savunma sanayiinde daha ciddi bir güvenlik açığı olasılığı görülüyor. Askeri birliklerce kullanılacak artırılmış gerçeklik teknolojilerinin güvenliğinin titizlikle oluşturulması, yanlış yönlendirmelerin oluşmaması ve operasyonel başarı için kritik önem taşıyor.

Yakın gelecekte akıllı telefonların yerini alabilecek akıllı gözlükler, dijital lensler ile bulut bilişim bağlantılı artırılmış gerçeklik uygulamalarının bir araya gelmesi hayatı kolaylaştırabileceği kadar kişisel sınırların ve gizliliğin sınırlarını zorlayacak gibi görünüyor.

Bu nedenle, artırılmış gerçeklik teknolojileri ile ilgili hizmetler sunan ve cihazlar üreten kuruluşların ister sivil ister askeri alanda olsun güvenlik açıklarını detaylı bir şekilde incelemesi ve bilgi güvenliğini sağlaması gerekiyor. Bu şekilde mahremiyete saygı gösterecek yazılım altyapılarının oluşturulması geleceğin bu önemli teknolojisinin benimsenmesini hızlandırabilir.

9 https://www.forbes.com/sites/forbestechcouncil/2019/09/06/cybersecurity-and-the-explosion-of-augmented-reality/?sh=715a93763c07
10 https://chowdera.com/2021/07/20210720044124984b.html