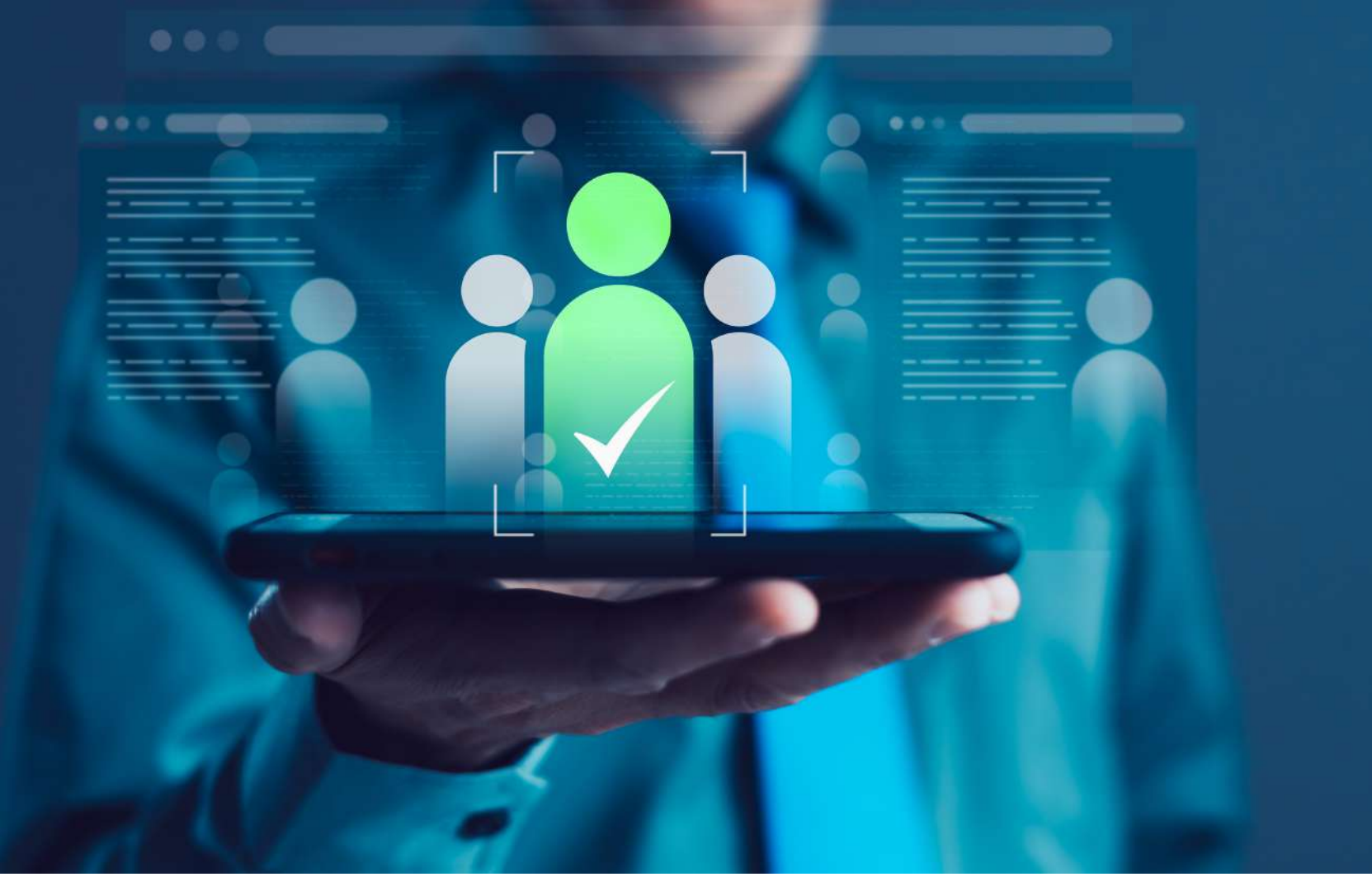




Dijital Sömürgecilik Çağı ve Gözetim Kapitalizmi

Verinin yeni petrole, insan deneyiminin ise ham maddeye dönüştüğü günümüzde, özgür irademizin algoritmalar tarafından nasıl kuşatıldığını anlamak artık bir tercih değil, zorunluluk. Profesör Shoshana Zuboff'un "Gözetim Kapitalizmi" (Surveillance Capitalism) olarak adlandırdığı yeni bir ekonomik düzen içerisinde dijital çağın şafağında her adımımızın izlendiği, analiz edildiği ve satıldığı bir gerçeklik ile karşı karşıyayız. Bu yazıda, insan deneyiminin nasıl bir ticari meta haline geldiğini, dijital profillemenin görünmez mekanizmalarını ve Cambridge Analytica skandalını inceleyeceğiz.

Gözetim Kapitalizminin Doğuşu

Gözetim kapitalizmi, insan deneyimini davranışsal verilere dönüştürmek için çerçevelenen yeni bir veri temelli tahakküm sistemidir. Bu sistemin kökleri 2001 yılındaki "dot-com balonuna" kadar dayanıyor. Bu dönemde bazı teknoloji şirket-

lerinin, yatırımcı güvenini pekiştirmek ve reklam gelirlerini artırmak amacıyla, kullanıcıların dijital ayak izlerini, yalnızca hizmetlerini iyileştirmek için değil; aynı zamanda kullanıcı davranışlarını öngörmek ve yönlendirmek için kullanmaya başlamasıyla, bu modelin temelleri atılmış oldu.

Bu sistemde verilerin bir kısmı hizmeti iyileştirmek için kullanılırken, geri kalanı "davranışsal artık" (behavioral surplus) olarak ayrılıyor. Bu artık veri, yapay zekâ ve makine öğrenimi süreçlerinden geçirilerek "tahmin ürünlerine" dönüştürülüyor. Bu ürünler, kullanıcıların şimdi ve daha sonra ne yapacağını tahmin etmeyi amaçlıyor. Bu tahminler şirketlerin, gelecekteki kullanıcı davranışlarını öngörme ve yönlendirme gücü olarak alınıp satılıyor. Gözetim kapitalistleri, her ne kadar çerez politikaları ve aydınlatma metinleri sunsalar da kullanıcıların rızası olmadan onların deneyimlerini ham madde olarak kullanabiliyorlar.

Gözetim kapitalistleri, genellikle özel hayatımızın mahremiyetini, yasal veya toplumsal bir izin almaksızın, “ücretsiz ham madde” olarak kullanıyor. Buradaki ham madde, insan zihninin ve davranışlarının iç dünyası. Verilerimiz kullanılarak üretilen bilgiye erişimimiz olmadığı gibi, bu bilginin bizi nasıl yönettiği üzerinde de genellikle kontrolümüz bulunmuyor.

Dijital Profillemeye ve Türetilmiş Verinin Gücü

Şirketlerin kullanıcıları hakkında ne bildiği sorusu, genellikle verdiğimiz isim, e-posta veya doğum tarihi ile sınırlı sanılıyor. Oysa asıl tehlike, “dijital profillemeye” ve özellikle “türetilmiş veri” (inferred data) kavramlarında yatıyor. Profillemeye kavramı, bir gerçek kişinin işteki performansı, ekonomik durumu, sağlığı, kişisel tercihleri, ilgi alanları, güvenilirliği, davranışları ve konumu gibi hususların analiz edilmesi veya tahmin edilmesi olarak karşımıza çıkıyor.

Görünmeyen Veri: Türetilmiş Bilgi

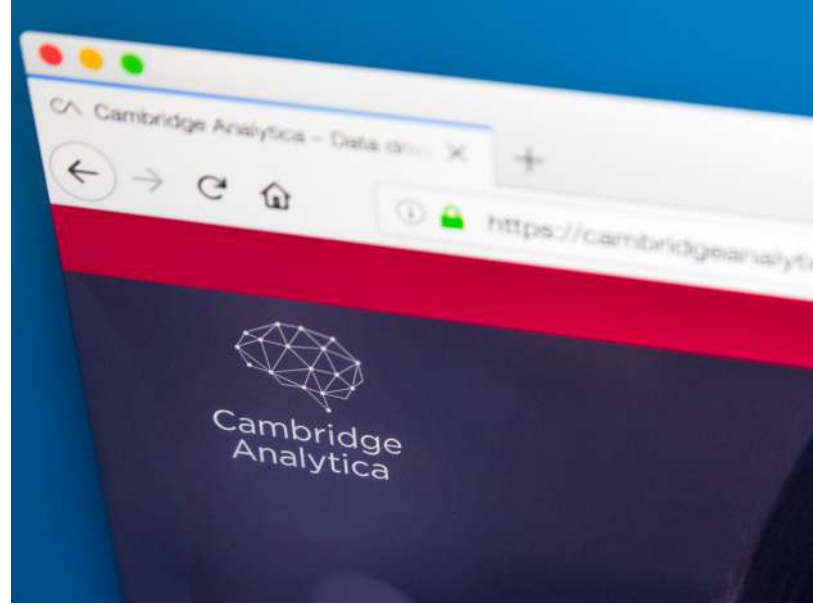
Sistemin en güçlü silahı, kullanıcının doğrudan sağlamadığı, ancak algoritmaların analizler sonucu çıkarsadığı türetilmiş veriler. Örneğin, bir kullanıcının sosyal medyadaki beğenileri, sadece basit tercihler gibi görünse de alan araştırmaları, sadece bu beğenilere bakarak kişinin cinsel yönelimini, siyasi görüşünü, etnik kökenini ve hatta zekâ seviyesini yüksek doğrulukla tahmin etmenin mümkün olduğunu gösteriyor.

Bu veriler, psikolojide yaygın olarak kullanılan “Beş Büyük Faktör” (Big Five) kişilik modeli (açıklık, sorumluluk, dışa dönüklük, uyumluluk, nevroitiklik faktörleri) kullanılarak analiz ediliyor. Kullanıcı sisteme “ben endişeli biriyim” demese bile, algoritmalar gezinme hızı, yazılan kelimeler veya etkileşim saatlerinden kullanıcının nevroitiklik seviyesini türetebiliyor. Bu, kullanıcının bilgisi dışında kullanıcının kişilik detaylarını ortaya çıkarabiliyor.

Sadece Reklam Değil

Bu teknolojinin kullanım alanı kullanıcılara sadece bir ayakkabı satmakla sınırlı değil. Sigortacılık, finans, sağlık ve siyaset gibi kritik alanlarda, hayatı doğrudan etkileyen kararlar bu algoritmalarla alınıyor. Bu konuda en çarpıcı örneklerden birisi ise NATO Stratejik İletişim Mükemmeliyet Merkezi (NATO's Strategic Communications Centre of Excellence) bünyesinde 2019 yılında yürütülen bir çalışmadır. Söz konusu çalışmada araştırmacılar, bir askerî tatbikat sırasında askerleri hedef olarak sosyal medya üzerinden açık kaynak verilerini topladı ve “honeypot” (bal küpü) adı verilen sahte sayfalar ve gruplar oluşturdu. Sadece Instagram ve Facebook verileri kullanılarak, askerlerin konumları, birlik hareketleri ve tatbikat tarihleri tespit edilebildi. Daha da ürkü-

tücü olanı, araştırmacılar elde ettikleri profillemeye verilerini kullanarak askerleri görev yerlerini terk etmeye veya emirlerle uymamaya teşvik edecek manipülatif mesajlar kurgulayabildiler. Facebook, kullanıcıların iş yeri bilgilerini gizleseler bile “önerilen arkadaşlar” özelliği sayesinde birliklerin haritasının çıkarılmasına istemeden de olsa olanak sağladı. Bu durum, kişisel verilerin sadece bir gizlilik sorunu değil, aynı zamanda bir hibrit savaş zafiyeti olduğunu kanıtlıyor.



Cambridge Analytica Skandalı

Bu teorik çerçevenin, demokratik süreçleri manipüle etmek amacıyla nasıl etkili bir araca dönüştüğü, 2018 yılında patlak veren Cambridge Analytica skandalı üzerinden somut biçimde örneklenebilir. Cambridge Analytica, Facebook üzerinden milyonlarca kullanıcının verisini, “This Is Your Digital Life” adlı masum görünen bir kişilik testi uygulaması aracılığıyla topladı. Uygulamayı indiren yaklaşık 270.000 kişi, sadece kendi verilerini değil, arkadaşlarının verilerini de rızaları olmadan şirkete açmış oldu. Bu sayede, kullanıcı profillerinden elde edilen ve seçmen kütükleriyle eşleştirilen milyonlarca Facebook verisi kullanılarak kapsamlı bir veri tabanı oluşturuldu; bu veri tabanı üzerinden algoritmik hedefleme yapıldı ve kullanıcıların korkuları ile önyargılarını hedef alan modellerin inşa edilmesi mümkün hale geldi. Böylece seçmenler, psikolojik profillerine göre mikro-hedefleme yoluyla sınıflandırılarak kişiselleştirilmiş siyasi mesajlara maruz bırakıldı. Şirketin elindeki verileri psikografik profillemeye amacıyla kullandığı; seçmenleri yalnızca demografik özelliklerine göre değil, kişilik özelliklerine göre de hedeflediği ortaya çıktı. Örneğin “nevroitik” ve “endişeli” olarak profilelenen seçmenlere güvenlik kaygılarını tetikleyen, sınır



güvenliği veya suç oranlarına ilişkin korku temalı görseller sunulurken; “geleneksel” ve “kapalı” olarak sınıflandırılan seçmenlere ise vatanseverlik ve geleneksel değer vurgusu içeren mesajlar iletildiği belirlendi. Bu süreçte seçmenlerin, rasyonel karar vericiler olarak kamusal bir tartışmanın öznesi olmaktan çıkarılıp; duygusal ve bilişsel zayıflıkları hedef alınarak oy verme davranışları yönlendirilebilir nesneler haline getirilmesi hedeflendi.

Şirketin bu yolla hem İngiltere’deki Brexit seçimlerine hem de ABD’deki seçimlere etki ettiği iddiaları gündemi sarstı. Olayın sonucunda Cambridge Analytica şirketi kapatılırken Facebook’a 5 milyar dolar ceza kesildi. Bu da bir teknoloji şirketine verilen en yüksek “gizlilik ihlali” cezası oldu. Skandal, kişisel verilerin sadece ticari bir meta değil, aynı zamanda bir enforsasyon savaşı ve siyasi mühendislik aracı olduğunu gösterdi.

Neler Yapılabilir?

Sosyal medya platformları genellikle “biz sadece platformuz” diyerek sorumluluktan kaçmaya çalışsa da Cambridge Analytica örneği, bu platformların kötü niyetli olunduğu zaman demokrasinin altını oyan birer silah haline gelebileceğini gösteriyor. Peki, benzer skandalların yaşanmaması için neler yapılabilir? Bu noktada yasal düzenlemeler ve etik standartlar hayati önem taşıyor:

- 1. Şeffaflık:** Algoritmaların nasıl karar verdiği genellikle bir “kara kutu” (black box) olarak kalıyor. Avrupa Birliği’nin Genel Veri Koruma Tüzüğü (General Data Protection Regulation- GDPR) gibi düzenlemeler, otomatik karar alma süreçlerinde (örneğin kredi reddi veya işe alım) kullanılan mantığın bireylere açıklanmasını zorunlu kılıyor. Bireylerin, kendileri hakkında bir profil oluşturulduğunda bunun mantığını, önemini ve doğuracağı sonuçları bilme hakkına sahip olması gerekiyor. Ayrıca, Kişisel Verileri Koruma Kanunu’na (KVKK) göre ilgili kişi için söz konusu kişisel veri işleme faaliyetinin şeffaf olması ve veri sorumlusunun aydınlatma yükümlülüğüne uygun hareket etmesi gerekiyor.
- 2. Türetilmiş Veri Koruması:** Kullanıcının rızası olmadan, algoritmik tahminlerle üretilen hassas verilerin kullanımının sıkı kurallara bağlanması gerekiyor. Toplanmayan ancak hesaplanan bu verilerin de kişisel veri sayılması ve koruma altına alınması gerekiyor.
- 3. Otomatik Kararlara İtiraz Hakkı:** Bireylerin, sadece otomatik sistemler tarafından verilen, kendilerini olumsuz etkileyen ve hukuki veya benzeri önemli etkiler doğuran kararlara itiraz etme ve insan müdahalesi talep etme hakkının güçlendirilmesi gerekiyor. Bir algoritma kullanıcıyı



“riskli” bulunduğunda, ilgili durumun izah edebileceği bir insan muhatap bulunması önem arz ediyor. Ayrıca KVKK’nın 11’inci maddesinin 1’inci fıkrasının (g) bendinde kişisel verileri işlenen kişilerin, işlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle aleyhe bir sonucun ortaya çıkmasına itiraz hakkı düzenlenmiş bulunuyor.

- 4. Dijital Okuryazarlık:** Yukarıda ele alınan yasal düzenlemeler kullanıcıları korumakla birlikte yeterli çözüm sunmuyor. Kullanıcıların, ücretsiz hizmetlerin bedelinin kendi verileri olduğunu anlaması ve dijital ayak izlerini yönetme konusunda bilinçlenmesi gerekiyor.

Sonuç olarak, gözetim kapitalizmi ve dijital profillemeye pratiklerinin, yalnızca bireysel mahremiyeti değil, demokratik karar alma süreçlerini ve hukukun temel ilkelerini de doğrudan tehdit eden sistemik bir sorun olduğu anlaşıyor. Kişisel verilerin ekonomik değer uğruna sınırsız biçimde toplanması ve algoritmik tahminlere dayalı olarak bireylerin davranışlarının yönlendirilmesi, bireyi özne olmaktan çıkarıp tahmin edilebilir bir nesneye indirgiyor. Bu durum, demokratik toplumların temelini oluşturan özgür irade, eşitlik ve hesap verebilirlik ilkelerine tehdit oluşturuyor. Dolayısıyla mesele, yalnızca bireysel gizlilik tercihleriyle çözülebilecek teknik bir sorun olmaktan öte siyasal, hukuki ve etik boyutları olan yapısal bir güç ilişkisi meselesi olarak karşımıza çıkıyor. Etkin yasal düzenlemeler, güçlü denetim mekanizmaları ve eleştirel dijital okuryazarlık olmaksızın, dijital teknolojilerin sunduğu imkânlar özgürleştirici olmaktan ziyade yeni bir dijital tahakküm biçimine dönüşme riski taşıyor.

