Yüzümle Mutluyum Derneği

DİJİTAL HAKLAR VE YAPAY ZEKÂ: BİYOMETRİK TEKNOLOJİLERDE GÖRÜNÜR FARKLILIK EŞİTLİĞİ



Kodlanan Ön Yargılar
Algoritmik Çağda "Normal Yüz" İllüzyonu

GİRİŞ

Yapay zekâ, makine öğrenmesi ve bilgisayarlı görü (computer vision) sistemleri, artık hayatın görünmez altyapısını oluşturmaktadır. Finansal işlemlerden adli süreçlere, kamusal hizmetlerden akıllı cihazların kilit mekanizmalarına kadar her yerde kararları algoritmalar vermektedir. Ancak genel kanının aksine, bu teknolojiler matematiksel olarak tamamen nötr, nesnel veya tarafsız değildir. Bir algoritma, özünde onu tasarlayan mühendislerin, veri etiketleme süreçlerindeki insan faktörünün ve modelleri eğitmek için kullanılan veri setlerinin (dataset) **kültürel, sosyal ve estetik ön yargılarını** taşır. Yapay zekâ, toplumsal dışlama mekanizmalarını veri üzerinden öğrenerek bu ayrımcılıkları çok **daha sistematik ve görünmez bir şekilde yeniden üretme potansiyeline** sahiptir.

Dijital ekosistemin hızla yaygınlaşan biyometrik katmanları, tarihsel olarak **"ortalamaya indirgenmiş, simetrik ve normatif" kabul edilen tek tip bir insan yüzü modelini referans alarak** inşa edilmektedir. Hak temelli yaklaşım, teknolojideki bu yapısal kurguyu ciddi bir hak ihlali olarak tanımlar:

Algoritmaların insanı tek tipleştiren estetik kalıplara ve keskin simetri çizgilerine göre eğitilmesi, dijital dünyada yeni bir ayrımcılık türü olan **Algoritmik Lookism (Görsel Ayrımcılık)** olgusunu doğurmuştur. Fiziksel çevre, mimari engellerle insanı dışlayabiliyorsa; dijital çevre de kod satırları, veri setleri ve biyometrik bariyerlerle görünür farklılığı olan bireyleri sistemin dışına itebilir.

Bu kitapçığın temel amacı; doğumsal veya sonradan edinilmiş görünür farklılığı olan bireylerin **dijital dünyada karşılaştığı algoritmik engelleri ve "biyometrik dışlanma" (biometric exclusion) süreçlerini** deşifre etmektir. Teknoloji liderleri, yazılım geliştiriciler ve veri bilimciler için hak temelli, etik ve insan çeşitliliğine saygılı bir yapay zekâ standardının nasıl inşa edileceğini operasyonel ve kavramsal parametreleriyle ortaya koymaktadır.



Bölüm 1: Veri Setlerindeki Tek Tiplik ve Kaynak Veri Yanlılığı (Data Bias)

Bir yapay zekâ modelinin başarısı, doğruluğu ve kapsayıcılığı, **eğitildiği verinin niteliği ve çeşitliliğine** doğrudan bağlıdır. Günümüzde derin öğrenme (deep learning) tabanlı bilgisayarlı görü modellerini eğitmek için kullanılan küresel ölçekteki milyonlarca görsel barındıran veri setleri incelendiğinde, derin bir **temsili adaletsizlik** göze çarpar.

Veri Setlerinin Estetik Sınırları ve Temsil Krizi

Yapay zekâ modellerinin bir nesneyi veya insan yüzünü tanıması için binlerce farklı örnek görmesi gerekir. Ancak yüz tanıma modellerinin eğitildiği havuzlar, ezici bir çoğunlukla **simetrik, pürüzsüz ve normatif yüz hatlarına sahip bireylerden** oluşur. Doğumsal sendromlar, yarık dudak/damak, yüz felci, yanık, yara veya ameliyat izleri gibi görünür farklılıklar bu veri setlerinde neredeyse hiçbir temsiliyete sahip değildir. Model, insan yüzünün ne olduğunu öğrenirken bu çeşitliliği görmediği için, dijital dünyada insan çehresinin sınırlarını yapay olarak daraltmaktadır.

Nadir Durumların "Gürültü" (Noise) Olarak Kodlanmasının Matematiksel Analizi

Makine öğrenmesi algoritmaları, optimizasyon süreçlerinde istatistiksel genellemelere dayanır. Bir algoritma, eğitildiği veri havuzunda çok az sayıda temsil edilen veya hiç bulunmayan veri tipleriyle karşılaştığında, matematiksel maliyet fonksiyonunu (loss function) minimize etmek adına bu verileri birer **"gürültü" (noise)** veya sistemin dengesini bozan bir **"aykırı değer" (outlier)** olarak sınıflandırma eğilimindedir.

Yapay zekâ felsefesi ve veri etiği açısından bu durum, insan çeşitliliğinin bilgisayar tarafından "matematiksel bir hata" veya "sistem dışı sapma" olarak kabul edilmesi anlamına gelir. Temsilde adaletin sağlanması; yapay zekanın toplumsal gerçeği doğru algılayabilmesi için **eğitim verilerine görünür farklılıkları içeren görsel girdilerin etik, anonim, hak ihlali yaratmayan ve doğru yöntemlerle entegre edilmesini** zorunlu kılar. Kaynak **veri yanlılığı (data bias)** çözülmeden, adil bir yapay zekâ inşa etmek matematiksel olarak imkansızdır.



Bölüm 2: Kimlik Doğrulama Sistemleri ve Dijital Erişilebilirlik Engelleri

Dijital dönüşüm; finansal işlemler, kamu hizmetlerine erişim (e-Devlet sistemleri), uzaktan çalışma onayları ve sınır güvenliği gibi en kritik alanlarda **biyometrik kimlik doğrulama sistemlerini** standart birer güvenlik kapısı haline getirmiştir. Ancak bu sistemlerin **esneklikten uzak teknolojik altyapısı, görünür farklılığı olan bireyler için aşılması imkansız dijital bariyerler** üretmektedir.

Kimlik Doğrulama ve Canlılık Testi (Liveness Detection) Algoritmalarının Çöküşü

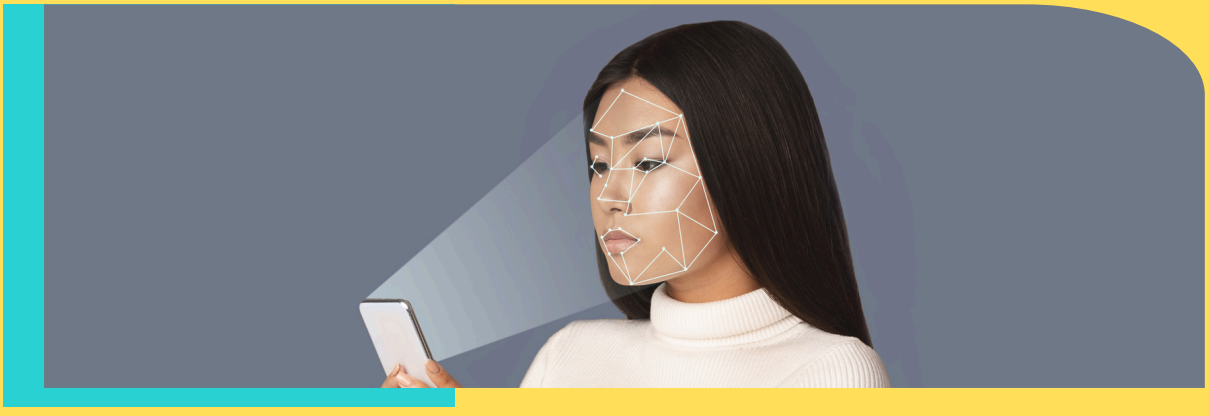
Modern mobil bankacılık uygulamaları veya dijital cüzdanlar, kimlik hırsızlığını ve dolandırıcılığı önlemek adına kullanıcıdan sadece durağan bir yüz fotoğrafı istemez; aynı zamanda **"canlılık testi" (liveness detection)** talep eder. Bu aşamada yapay zekâ, kullanıcının gözünü kırpmasını, gülümsemesini, başını sağa veya sola çevirmesini ister ve bu esnada yüzdeki **mikro kas hareketlerini, simetri eksenlerini ve derinlik haritasını** tarar.

Yüz asimetrisi olan, yüz felci geçmişi bulunan veya doğumsal farklılıklardan dolayı kas yapısı standart şablonlara uymayan bireyler bu testleri gerçekleştirmeye çalıştıklarında, algoritmaların katı sınırları devreye girer. Algoritma, yüzün bir tarafındaki hareketsizliği veya asimetriyi **"canlı olmama", "maske kullanımı", "fotoğraf üzerinden sistemi aldatma girişimi" veya "sistem hatası"** olarak yorumlar. Sonuç olarak, kullanıcının işlemi doğrudan reddedilir ve hesabı güvenlik gerekçesiyle bloke edilir.

Dijital Vatandaşlık Haklarının Mahrumiyeti ve Çözüm Arayışı

Bireyin kendi yasal resmi işlemlerini yürütememesi, banka hesaplarına erişememesi, uzaktan mülakat veya sınav sistemlerine dahil olamaması, sadece teknik bir yazılım hatası (bug) olarak geçiştirilemez. Bu durum, **anayasal düzeyde bir temel dijital vatandaşlık hakkı ihlalidir.** Fiziksel dünyada bir binaya rampa koymamak nasıl bir erişilebilirlik suçuysa, dijital dünyada da bir yüzü asimetrisi nedeniyle sistemin dışına itmek aynı derecede bir dışlamadır.

Akıllı cihaz üreticilerinden kamu kurumlarının biyometrik altyapılarına kadar tüm donanım ve yazılımlar; insan yüzünün değişken, asimetrik ve benzersiz doğasını bir hata/güvenlik açığı değil, doğal bir girdi varyasyonu olarak kabul edecek **teknik esneklik ve tolerans standartlarına (threshold tuning)** kavuşturulmalıdır.



Bölüm 3: Duygu Analizi ve Karakter Tahmin Algoritmalarındaki Tehlikeler

Yapay zekâ ekosisteminde yükselen ve etik açıdan en çok tartışılan alanlardan biri, bilgisayarlı görü (computer vision) modelleri aracılığıyla insan yüzünden **duygu analizi (emotion recognition) veya psikolojik profil/karakter tahmini yapmaya çalışan sistemler**dir. Bu sistemler, insan çehresini piksellere bölerek mikroskobik yüz hareketlerinden derin anlamlar çıkarma iddiasındadır. Ancak bu iddia, arkasında çok ciddi bir algoritmik ayrımcılık riski barındırır.

Duygu Analizinde Doğrusallık Yanılgısı
Geleneksel duygu analizi algoritmaları, **Paul Ekman'ın "Evrensel Duygu Teorisi"ni** temel alarak kurgulanır. Bu teoriye göre **yedi temel duygu (mutluluk, üzüntü, öfke, şaşkınlık, korku, tiksinme, küçümseme),** yüz kaslarının belirli ve çizgisel hareketleriyle dışa vurulur. Algoritma; kaşların çatılma açısını, göz kapaklarının aralığını veya dudak kenarlarının simetrik kıvrımını ölçerek bir skor üretir.
Görünür farklılığı, yüz asimetrisi, kısmi yüz felci veya nadir sendromlara bağlı kas yapısı varyasyonları olan bir birey, tamamen nötr veya sakin bir ruh halindeyken bile bu algoritmaların dar kalıpları tarafından yanlış sınıflandırılmaktadır. Örneğin, bir yüz asimetrisi algoritma tarafından "kronik güvensizlik", "şüphe" veya "agresif bir ruh hali" olarak yorumlanabilmektedir. Bu durum, **bireyin gerçek hislerinin dijital bir sistem tarafından tamamen çarpıtılması** anlamına gelir.

Yapay Bilimin Dijitalleşmesi ve "Dijital Fizyognomi"
Özellikle İnsan Kaynakları (İK) süreçlerinde, adayların **video mülakatlar sırasındaki ses tonunu, kelime seçimlerini ve en çok da yüz ifadelerini yapay zekâ ile tarayan akıllı işe alım araçları** yaygınlaşmaktadır. Bu araçlar, **adayın "özgüvenini, dürüstlüğünü, stres yönetimini veya kurumsal kültüre uyumunu"** puanlar.
Görünür farklılığı olan bir profesyonel, liyakati, eğitimi ve tecrübesi ne kadar yüksek olursa olsun, yüz hatlarını standart simetri şablonuna göre puanlayan bir yapay zekâ filtresi tarafından **ilk aşamada elenme riskiyle** karşı karşıyadır. Bu pratik, 19. yüzyılda kalmış ve bilimsel geçerliliği tamamen reddedilmiş olan **fizyognomi (yüz hatlarından karakter ve suç eğilimi okuma) teorilerinin, modern dünyada "yapay zekâ nesnelliği" maskesi altında yeniden canlandırılmasıdır.** Algoritmik lookism üreten ve insan onurunu zedeleyen bu **sahte-bilimsel (pseudo-science) yazılım katmanları,** liyakat esaslı istihdam piyasasının önündeki en tehlikeli dijital barikattır.



Bölüm 4: Dijital Haklar, Regülasyonlar ve Yapay Zekâ Mevzuatı

Teknolojinin insan hakları aleyhine sınırları zorlaması, küresel ölçekte çok sıkı yasal regülasyonların doğmasını zorunlu kılmıştır. Dijital hak savunuculuğu, bu yasal süreçleri yakından takip etmek ve görünür farklılıkları hukuki metinlerin koruma kalkanı altına almakla yükümlüdür.

Küresel Yapay Zekâ Yasaları ve "Yüksek Riskli" Sınıflandırma

Avrupa Birliği Yapay Zekâ Yasası (EU AI Act), yapay zekâ sistemlerini yarattıkları risk seviyelerine göre kategorize eder. İşe alım süreçlerinde kullanılan algoritmalar, biyometrik kimlik doğrulama sistemleri ve duygu analizi yazılımları bu yasada **"Yüksek Riskli" (High-Risk) kategorisinde** sınıflandırılmıştır.

Bu sınıflandırma, söz konusu yazılımları geliştiren teknoloji şirketlerine çok ağır yasal ve teknik sorumluluklar yükler. Ancak mevcut mevzuatlarda; ırk, cinsiyet, yaş veya engellilik gibi korunan statüler net bir şekilde tanımlanmışken, **"görünür farklılıklar, yüz anomalileri veya edinsel fiziksel özellikler" gibi Lookism alanına giren kavramlar** henüz gri alandadır. Uluslararası içtihatların ve ulusal yapay zekâ politikalarının, ayrımcılık yasağı maddelerine **"fiziksel çeşitlilik ve yüz özellikleri" terimini açık bir yasal statü olarak** eklemesi şarttır.

Algoritmik Ayrımcılık Etki Değerlendirmesi (Bias Impact Assessment)

Yasal düzenlemeler, teknoloji geliştiren kurumlara ürünlerini piyasaya sürmeden önce **sıkı denetim yükümlülükleri** getirmelidir. Bir yazılım firması, geliştirdiği bilgisayarlı görü modelinin toplumun hiçbir kesimini fiziksel özellikleri nedeniyle dışlamadığını, reddetmediğini veya yanlış sınıflandırmadığını kanıtlamak zorundadır.

Bunun yolu, bağımsız etik kurullar tarafından onaylanan **Algoritmik Ayrımcılık Etki Değerlendirmesi (Bias Impact Assessment)** süreçleridir. Bu denetimlerden geçemeyen, yani görünür farklılığı olan bireylerde yüksek hata oranı veren sistemlerin ticari olarak tescillenmesi ve kamusal alanda kullanımı engellenmelidir. Veri mahremiyeti (KVKK ve GDPR) kapsamında da, bireylerin rızası dışında biyometrik yüz verilerinin taranması ve bu veriler üzerinden estetik/psikolojik kategorizasyon yapılması **en ağır hukuki yaptırımlara** bağlanmalıdır.

Bölüm 5: Yazılımcılar ve Veri Bilimciler İçin "Kapsayıcı Kodlama" Standartları

Yapay zekâda adaleti ve yüz eşitliğini sağlamak, sadece yasal zorunluluklarla değil, kodun yazıldığı ve modelin eğitildiği ilk andaki teknik parametrelerin hak temelli felsefeyle yeniden kurgulanmasıyla mümkündür. Veri bilimciler ve yazılım mühendisleri için geliştirilen temel kapsayıcı kodlama standartları şunlardır:

1. Algoritmik Tolerans Payı ve Eşik Değerlerinin Kalibrasyonu (Threshold Tuning)

Yüz tanıma ve kimlik doğrulama modelleri, iki görüntünün aynı kişiye ait olup olmadığını anlamak için **matematiksel bir "benzerlik skoru" (similarity score)** hesaplar. Sistem, bu skorun önceden belirlenmiş bir **"eşik değerinin" (threshold)** üstünde olmasını bekler. Güvenlik kaygılarıyla bu eşik değerinin çok katı ve keskin simetri çizgilerine göre ayarlanması, **görünür farklılığı veya asimetrisi olan bireylerde sistemin sürekli hata vermesine (False Rejection)** yol açar.

Yazılım mimarları, sistemin güvenlik protokollerini zafiyete uğratmadan, **insan yüzünün asimetrik ve değişken doğasını tolere edebilecek dinamik, esnek ve kapsayıcı eşik değeri kalibrasyonları (threshold tuning)** geliştirmelidir.

2. Sentetik Veri (Synthetic Data) ile Etik Çeşitlilik Çoğaltımı

Eğitim veri setlerindeki çeşitlilik krizini çözmenin en büyük engeli, gerçek kişilerin biyometrik verilerini toplamanın yarattığı gizlilik ve mahremiyet ihlalleridir. Bu noktada devreye **Sentetik Veri (Synthetic Data) teknolojisi** girmektedir.

Veri bilimciler; doğumsal sendromları, skarları, yarık dudak/damak yapılarını veya yüz asimetrilerini **anatomik olarak tamamen doğru, onurlu ve gerçekçi bir şekilde modelleyen sentetik (yapay olarak üretilmiş) yüz görselleri** tasarlamalıdır. Yapay zekâ modelleri, bu sentetik ama kapsayıcı veri havuzlarıyla eğitilerek ve test edilerek, **gerçek hayattaki insan çeşitliliğini tanıma konusunda** optimize edilmelidir.

3. Yazılım Kalite Güvence (QA) Süreçlerinde Çeşitlilik Protokolleri

Bir yazılımın "çalışıyor" kabul edilmesi için test süreçlerinden başarıyla geçmesi gerekir. Geleneksel QA (Quality Assurance) süreçleri, sistemleri sadece standart ve simetrik yüz modelleriyle test eder. Kapsayıcı kodlama standardı, yazılım test senaryolarına "fiziksel çeşitlilik ve görünür farklılık" protokollerinin eklenmesini zorunlu kılar. **Bir biyometrik sistem, insanlığın tüm görünür farklılık varyasyonlarında sorunsuz çalışmadığı sürece "kalite onay kodu" almamalıdır.**

Bölüm 6: Teknoloji Liderleri ve Yazılım Şirketleri İçin Kapsayıcılık Kontrol Listesi

Bir teknoloji şirketinin, AR-GE merkezinin ya da yapay zekâ modelinin "görünür farklılıklar ve dijital haklar açısından kapsayıcı" olup olmadığını denetlemek amacıyla hazırlanan kurumsal kontrol listesi şudur:

- **Veri Seti Kapsayıcılığı:** Geliştirdiğimiz bilgisayarlı görü (computer vision) ve derin öğrenme modellerinin eğitim veri setlerinde, görünür farklılığı olan bireyler hak ihlali yaratmadan, adil, doğru ve anonim bir şekilde temsil ediliyor mu?

- **Algoritmik Esneklik Analizi:** Canlılık testi (liveness test) ve biyometrik kimlik doğrulama yazılımlarımız; yüz asimetrilerini, felç izlerini veya kalıtsal özellikleri bir "güvenlik açığı, sistem hatası ya da sahte profil" olarak algılamayacak teknik tolerans paylarına (thresholds) sahip mi?

- **Etik İK ve Değerlendirme Filtreleri:** Kurumumuz bünyesinde geliştirilen veya üçüncü partilerden tedarik edilen İK ve aday değerlendirme yazılımları; lookism (görsel ayrımcılık) üreten, yüz hatlarından anlam çıkaran "duygu analizi ve karakter tahmini" katmanlarından tamamen arındırılmış mı?

- **Teknik Denetim ve Raporlama:** Piyasaya sürdüğümüz biyometrik ürünler için bağımsız etik kurallara uyumlu "Algoritmik Ayrımcılık Etki Değerlendirmesi" (Bias Impact Assessment) süreçleri işletiliyor ve şeffaf olarak raporlanıyor mu?

- **Sivil Toplum ve Bilgi Köprüsü:** Yapay zekâ geliştirme, veri etiketleme ve yazılım test (QA) ekiplerimiz; algoritmik lookism ve veri etiği konusunda Türkiye'de bu bilincin öncüsü olan Yüzümle Mutluyum Derneği'nin ve Face Equality International'ın küresel ilkelerine dair kurumsal eğitime ve bilgi düzeyine sahip mi?

Bu rehber kitapçık, dijital dönüşüm süreçlerinde ve yapay zekâ teknolojilerinde "Yüz Eşitliği" farkındalığını artırmak amacıyla Yüzümle Mutluyum Derneği tarafından teknoloji liderleri, yazılım geliştiriciler, veri bilimciler ve veri etiği kurulları için hazırlanmıştır.

Face Equality International'ın (FEI) Türkiye'deki tek temsilcisi olan derneğimiz; fütüristik teknolojilerin, biyometrik sistemlerin ve akıllı algoritmaların dış görünüşe dayalı ayrımcılığa (lookism) alet olmamasını sağlamak, yapay zekâ çağında görünür farklılığı olan tüm bireylerin eşit, onurlu ve adil dijital haklara erişmesini güvence altına almak için faaliyet göstermektedir.