# YAPAY ZEKA MODELLERİNİN AÇIKLIĞI: KAMU POLİTİKASI BELİRLEYİCİLERİ İÇİN KILAVUZ

OECD'nin "Yapay Zeka Modellerinin Açıklığı" başlıklı raporu (Ağustos 2025, No. 44), açık ağırlıklı foundation modellerin hukuki sonuçlarını ele alan uluslararası bir politika belgesidir.

Bu infografik, raporun temel bulgularını hukukçular için özetlemekte ve özellikle lisanslama belirsizlikleri, sorumluluk sorunları ve fikri mülkiyet/kişisel veri koruma risklerine odaklanmaktadır.

## GELENEKSEL AÇIK KAYNAK VE YZ AÇIK KAYNAK FARKI

| Geleneksel Açık Kaynak | | YZ "Açık Kaynak" |
|---|---|---|
| Kaynak kodu **tamamen açık.** Görülebilir, değiştirilebilir, dağıtılabilir. Lisans şartları net ve öngörülebilir. | TEMEL TANIM | Terim çoğunlukla **yanıltıcı.** Model ağırlıkları kaynak kod değil. Bileşenler parça parça şeffaf olabilir. |
| **Tek bileşen:** Kaynak Kodu | BİLEŞENLER | **Farklı bileşenler:** Eğitim Kodu Çıkarım Kodu Model Ağırlıkları Eğitim Verisi |
| Lisans şartları açık. Telif hakkı koruması net. Sorumluluk çerçevesi belirli. | HUKUKİ ÇERÇEVE | Yazılım lisansları uygun değil. Fikri mülkiyet belirsiz. Sorumluluk sınırları muğlak. |

## AÇIK AĞIRLIKLI TEMEL MODEL TANIMI (OPEN-WEIGHT MODELS)

OECD, "YZ açık kaynak" yerine "açık ağırlıklı model" terimini kullanmayı tercih etmiştir.

- **Daha net ve yanıltıcı olmayan bir terim.**
- **Sadece ağırlıkların açık olduğunu belirtiyor.**
- **Lisans, veri veya kod konusunda yanlış varsayım yaratmıyor.**

# AÇIK AĞIRLIKLI TEMEL MODEL TANIMI NELERI KAPSAMAKTADIR?

## TÜM YZ MODELLERİ

**Temel Modeller (Foundation Models)**
(Genel amaçlı, büyük)
Örneğin: GPT-4, Claude, LLaMA, Stable Diffusion

← OECD Raporu buraya odaklanıyor.

**Diğer YZ Modelleri:**
Örneğin: Spam filtresi, Yüz tanıma, Ses tanıma

← Model Açıklığı Çerçevesi (Model Openness Framework - MOF)

## YARARLAR

### İnovasyon ve Araştırma Özgürlüğü

Yeni uygulamalar geliştirme ve verimlilik. Bilimsel araştırma ve teknik ilerleme için erişim. Geliştirme verimliliği ve maliyet Tasarrufu.

### Dış Denetim ve Hesap Verebilirlik

Bağımsız uzmanların model performansını değerlendirmesi, hata ve önyargıların tespiti.

### Rekabet Hukuku Perspektifi

Piyasaya giriş engellerinin azalması. Tekelleşmenin önlenmesi. Yetenek gelişimi ve dijital eşitlik

### Kontrol ve erişilebilirlik

Hassas veri yönetimi, kamu ve özel sektörün hassas verileri üçüncü taraflara göndermeden yerel işlemesi. Uyumluluk ve açıklanabilirlik araştırması

## RISKLER

### Fikri Mülkiyet İhlali

Eğitim verisindeki telif haklı içeriğin yetkisiz kullanımı. Model ağırlıklarından orijinal eserlerin çıkarılması.

### Kişisel Verilerin Korunması İhlali

Model ağırlıklarında kişisel veri. Silme hakkı uygulanamaz. Üyelik çıkarım saldırıları.

### Çocuk Cinsel İstismar Materyali ve Rızasız Mahrem Görüntü

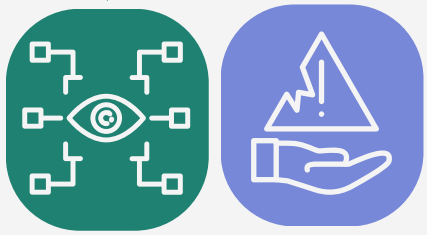
Açık ağırlıklı görüntü üretme modellerinin çocuk istismarı ve rızasız mahrem içerik üretiminde kullanılması

### Siber Suçlar

Gelişmiş phishing, kötü amaçlı yazılım, bilişim sistemlerine yetkisiz erişim için kullanım. Orijinal güvenlik katmanları ve filtrelerin kaldırılması

**Dijital Güvenlik Testleri**

Kırmızı Ekiplerin (red team) potansiyel saldırı senaryolarını yasal olarak test etmesi, dijital güvenlik ve korumaları İyileştirme, istenmeyen ve zararlı davranışları önleme.



**Geliştirici Sorumluluğu ve Kontrol Kaybı**

Açık model ile yapılan zararlı kullanımda orijinal geliştiricinin sorumluluğu muğlak. Kontrolsüz hızlanma.

## TÜM BUNLAR HUKUKÇULAR IÇIN NEDEN ÖNEMLI?

### Lisanslama Hukukundaki Belirsizlikler

Model Ağırlıklarının Lisanslanması: Geleneksel açık kaynak yazılım lisanslarının YZ model ağırlıklarına doğrudan uygulanamaması, yeni lisans türlerinin geliştirilmesini ve mevcut lisansların (örneğin, Apache 2.0, MIT, Creative Commons) YZ bağlamında yorumlanmasını zorunlu kılmaktadır.

### Sorumluluk ve Hesap Verebilirlik

Güvenlik Önlemlerinin Aşılması: Açık ağırlıklı modellerin kötü niyetli aktörler tarafından kolayca yeniden ayarlanabilmesi ve geliştiricinin orijinal güvenlik önlemlerinin bypass edilebilmesi, hukuki sorumluluğun tespitini son derece zorlaştırmaktadır. Modelin piyasadan geri çekilmesinin zorluğu da hukuki risk yönetimi açısından önemli bir değerlendirme noktasıdır.

### Fikri Mülkiyet (IP) ve Veri Gizliliği Hukuku

Eğitim Verisi Riski: Kapalı modeller yerine açık ağırlıklı modellerin benimsenmesi, hassas verilere sahip kamu kurumları ve işletmeler için verilerin üçüncü taraf satıcılarla paylaşılmaması yönünde bir avantaj sunarak, veri egemenliği ve gizliliği düzenlemelerine uyumu kolaylaştırabilir.Ancak bu avantaj, modelin eğitim verilerinden telif hakkıyla korunan materyali ezberleyip sızdırma potansiyeli (data extraction attacks) gibi riskleri ortadan kaldırmaz.

### Risk Değerlendirme ve Yönetmelik Uyumu

Bütünsel Risk Çerçevesi: Rapor, YZ açıklığına ilişkin kararların bütünsel bir risk değerlendirme çerçevesi içinde ele alınması gerektiğini belirtmektedir. Açıklığın inovasyon ve rekabet üzerindeki fırsat maliyetlerini (opportunity costs) de yasal stratejilere dahil etmeleri gerekecektir.

Kaynak: https://www.oecd.org/content/dam/oecd/en/publications/reports/2025/08/ai-openness_958d292b/02f73362-en.pdf


Hazırlayan:
Av. Özden Serinay Öz
Av. Rümeysa Kırpat

Tasarım: Av. Ayşenur Kölgesiz

İstanbul Barosu Bilişim Hukuku Komisyonu
Yapay Zekâ Çalışma Grubu