

Yapay Zekâ Etiği, Güvenlik, Doğrulama ve Gelecek

Prof.Dr.Hüseyin ÇAKIR
Gazi Üniversitesi

Yapay Zekâ Etiği

Yapay Zekâ Etiği, yapay zekâ sistemlerinin geliştirilmesi, kullanılması ve sonuçlarının değerlendirilmesi sırasında **adalet, şeffaflık, güvenlik, gizlilik, insan hakları** ve **sorumluluk** gibi etik ilkelerin dikkate alınmasını ifade eder.



Yapay Zeka ve Uygulamaları - Copyright © 2026

Temel Etik İlkeler

Adalet
Her bireye eşit ve ayrımcılık yapmayan bir yaklaşım.

Şeffaflık
Sistemlerin nasıl çalıştığının açık ve anlaşılır olması.

Güvenlik
Kötüye kullanım ve risklere karşı koruma.

Gizlilik
Kişisel verilerin korunması ve gizliliğe saygı.

İnsan Hakları
İnsan onuruna, özgürlüklere ve temel haklara saygı.

Sorumluluk
Hesap verebilirlik ve olası sonuçların üstlenilmesi.



Yapay zekânın güçlü olması, her kullanımının doğru veya etik olduğu anlamına gelmez.

Önemli olan yalnızca

"Yapay zekâ ne yapabilir?"

sorusu değil, aynı zamanda

"Yapay zekâ bunu yapmalı mı?" sorusudur.



Yapay Zekâ Etiği Neden Önemlidir?

Yapay zekâ;

1. İnsanlar hakkında karar verebilir,
2. Kişisel verileri işleyebilir,
3. İçerik üretebilir,
4. Öğrencileri değerlendirebilir,
5. İşe alım süreçlerinde kullanılabilir,
6. Sağlık ve finans gibi kritik alanlarda kararları destekleyebilir.



Yapay Zeka ve Uygulamaları - Copyright © 2026

Bu nedenle yapay zekânın

nasıl, hangi amaçla ve hangi sınırlar içerisinde

kullanıldığı önem taşır.

1 Yapay Zekâ Teknolojisi



Yapay zekâ, verileri analiz eden, öğrenen ve karar verebilen teknolojilerdir.

2 Kullanım Amacı



- Eğitim
- Sağlık
- İş süreçleri
- Çevre
- Toplum

Yapay zekâ, insanların yaşamını kolaylaştırmak, verimliliği artırmak ve toplumsal fayda sağlamak için kullanılır.

3 Etik İlkeler



- Adalet
- İnsan onuru
- Gizlilik
- Şeffaflık
- Eşitlik

Yapay zekâ uygulamalarında insan hakları, adalet, şeffaflık, gizlilik ve eşitlik gibi etik ilkeler esas alınır.

4 Risklerin Değerlendirilmesi



- Güvenlik riskleri
- Taraflılık
- Veri ihlalleri
- Toplumsal etkiler

Olası riskler önceden tespit edilir, etkileri analiz edilir ve gerekli önlemler alınır.

5 İnsan Denetimi



Yapay zekâ sistemleri, insan gözetimi ve denetimi altında çalışır.

6 Sorumlu Kullanım



- Güvenli
- Adil
- Şeffaf
- Sürdürülebilir

Yapay zekâ, insan ve toplum yararını ön planda tutarak, sorumlu ve sürdürülebilir bir şekilde kullanılır.

Yapay Zeka ve Uygulamaları - Copyright © 2026

Yapay Zekâ Etiğinin Temel İlkeleri

İlke	Açıklama
Adalet	Sistemlerin ayrımcılık oluşturmaması
Şeffaflık	Yapay zekânın nasıl ve neden kullanıldığının mümkün olduğunca açıklanması
Hesap verebilirlik	Ortaya çıkan sonuçlardan sorumlu kişi/kurumların belirli olması
Gizlilik	Kişisel ve hassas verilerin korunması
Güvenlik	Sistemin kötüye kullanım ve güvenlik risklerine karşı korunması
İnsan denetimi	Kritik kararların yalnızca yapay zekâya bırakılmaması
Doğruluk ve güvenilirlik	Üretilen bilgilerin kontrol edilmesi
İnsan onuru	İnsan haklarının ve temel özgürlüklerin korunması
Sorumluluk	Yapay zekâ kullanımının sonuçlarının üstlenilmesi

Yapay Zekâda Etik İlkeler

Daha adil, güvenli, şeffaf ve insan odaklı bir gelecek için...

İlke	Açıklama
Adalet	Sistemlerin ayrımcılık oluşturmaması
Şeffaflık	Yapay zekânın nasıl ve neden kullanıldığının mümkün olduğunca açıklanması
Hesap verebilirlik	Ortaya çıkan sonuçlardan sorumlu kişi/kurumların belirli olması
Gizlilik	Kişisel ve hassas verilerin korunması
Güvenlik	Sistemin kötüye kullanım ve güvenlik risklerine karşı korunması
İnsan denetimi	Kritik kararların yalnızca yapay zekâya bırakılmaması
Doğruluk ve güvenilirlik	Üretilen bilgilerin kontrol edilmesi
İnsan onuru	İnsan haklarının ve temel özgürlüklerin korunması
Sorumluluk	Yapay zekâ kullanımının sonuçlarının üstlenilmesi

Yapay Zeka ve Uygulamaları - Copyright © 2026

Adalet ve Algoritmik Önyargı

Nasıl Olur?

1. **Eğitim Verileri**
   Geçmiş verilerde var olan önyargılar sisteme girdi olarak kullanılır.
2. **Öğrenme Süreci**
   Yapay zekâ, bu veriler dahilinde kalıpları öğrenir.
3. **Karar Verme**
   Sistem, öğrendiği kalıplara göre gelecekteki adayları değerlendirir.
4. **Önyargı Tekrarı**
   Sonuçta, geçmişteki adaletsizlikler yeni kararlara da yansır.

Örnek: İşe Alım Sistemi

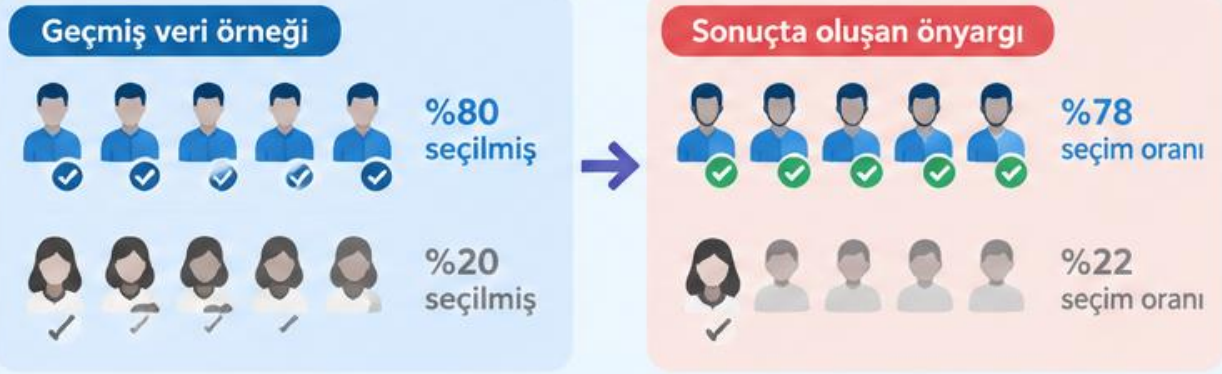


Geçmiş Veriler
Daha önce belirli bir gruptan gelen adaylar daha fazla seçilmiş.

Yapay Zekâ Eğitimi
Sistem bu durumu öğrenerek modelini oluşturur.

Yeni Aday Değerlendirmesi
Sistem, benzer özelliklere sahip adayları daha yüksek puanlar.

Haksız Tercih
Sonuçta, aynı grup adaylar haksız biçimde tercih edilir.



Bu Neden Önemli?

Eşit Fırsatlar
Herkes için adil ve tarafsız bir sistem gereklidir.

Toplumsal Etki
Algoritmik önyargılar, toplumsal eşitsizlikleri derinleştirebilir.

Güven
Daha adil ve şeffaf sistemler, güveni artırır.

Doğru Çözümler
Veri çeşitliliği, adil algoritma tasarımları ve düzenli denetim bu riski azaltır.

Yapay Zeka ve Uygulamaları - Copyright © 2026

Şeffaflık

1 **Yapay zekâ kullanılıyor mu?**

Sistemde yapay zekâ kullanılıp kullanılmadığı açıkça belirtilmelidir.

2 **Hangi amaçla kullanılıyor?**

Yapay zekânın hangi sorunu çözmek veya hangi hedefe ulaşmak için kullanıldığı açıklanmalıdır.

3 **Hangi veriler kullanılıyor?**

Hangi veri kaynaklarının, veri türlerinin ve nasıl kullanıldığı belirtilmelidir.

4 **Sonuç nasıl oluşturuluyor?**

Veri işleme, modelleme, ve karar süreci adım adım açıklanmalıdır.

5 **Kararın sorumlusu kim?**

Sistemi geliştiren, yöneten ve kararından sorumlu kurum veya kişiler açıkça belirtilmelidir.

6 **Hatalı sonuç durumunda ne yapılabilir?**

Yanlış veya eksik sonuçlarda başvuru, düzeltme ve itiraz süreçleri tanımlanmalıdır.

Kritik Alanlarda Şeffaflık Daha Önemlidir

Eğitim
Öğrenme süreçleri ve öğrenci verileri

Sağlık
Tanı, tedavi ve hasta verileri

Hukuk
Karar süreçleri ve adalet

Finans
Kredi, risk ve işlem verileri

İşe alım
Aday değerlendirme ve karar süreçleri

Gizlilik ve Kişisel Verilerin Korunması



Özellikle aşağıdaki bilgiler gelişigüzel yapay zekâ araçlarına yüklenmemelidir.

- T.C. kimlik numarası
- Telefon numarası
- Adres
- Öğrenci bilgileri
- Sağlık bilgileri
- Personel bilgileri
- Finansal bilgiler
- Özel nitelikli kişisel veriler
- Gizli kurum belgeleri

Prof.Dr.Hüseyin ÇAKIR
Gazi Üniversitesi

Yapay Zekâ ve Akademik Etik



1. Makaleyi tamamen yapay zekâya yazdırmak doğru mudur?
2. Yapay zekânın ürettiği kaynaklar kullanılabilir mi?
3. Yapay zekâ tarafından oluşturulan metin nasıl kontrol edilmelidir?
4. Yapay zekâ kullanımı beyan edilmeli midir?
5. Öğrencinin ödevini tamamen yapay zekâya yaptırması akademik açıdan uygun mudur?

Yapay Zekâ ve Akademik Etik

Temel yaklaşım



Yapay Zekâ = Yardımcı Araç

+



Araştırmacı / Öğrenci = Bilimsel ve Akademik Sorumlu

→



Daha iyi araştırmalar, daha güçlü akademik gelecek!

Düşünme
Eleştirel düşünme becerinizi kullanın.

Doğrulama
Bilgileri mutlaka kontrol edin.

Özgün Katkı
Kendi fikirlerinizi ortaya koyun.

Akademik Sorumluluk
Doğru atıf yapın, kurallara uyun.



Yapay Zeka ve Uygulamaları - Copyright © 2026

Yapay Zekâ ve Akademik Dürüstlük

Öğrencinin ödevini tamamen yapay zekâya yaptırması



Kendi çabasını ve öğrenme sürecini ortadan kaldırmak, gerçek öğrenmeyi engeller.

Yapay zekâ tarafından üretilen bilgileri kontrol etmeden kullanması



Yanlış, eksik veya güncel olmayan bilgiler akademik hatalara yol açabilir.

Sahte kaynakları gerçekmiş gibi göstermesi



Uydurma veya güvenilir olmayan kaynaklar, bilimsel çalışmanın değerini düşürür.

Yapay zekâ tarafından oluşturulan metni kendi özgün çalışması gibi sunması



Bu durum, intihal olarak değerlendirilir ve akademik dürüstlüğe aykırıdır.

Yapay Zeka ve Uygulamaları - Copyright © 2026

Daha sorumlu bir kullanım için:

1 Yapay zekâdan fikir alma



Konu hakkında farklı bakış açıları ve öneriler alabilirsin.

2 Konuyu açıklatmak



Karmaşık konuları daha iyi anlamak için açıklama isteyebilirsin.

3 Taslak oluşturmak



Yazı, proje veya sunumlar için ilk taslakları hazırlayabilirsin.

4 Dil ve ifade geliştirmek



Metnini daha akıcı, anlaşılır ve doğru bir dille vazabilirsin.

5 Kodlama desteği almak



Kod yazarken örnekler, açıklamalar ve hata çözümleri isteyebilirsin.

6 Hataları tespit ettirmek



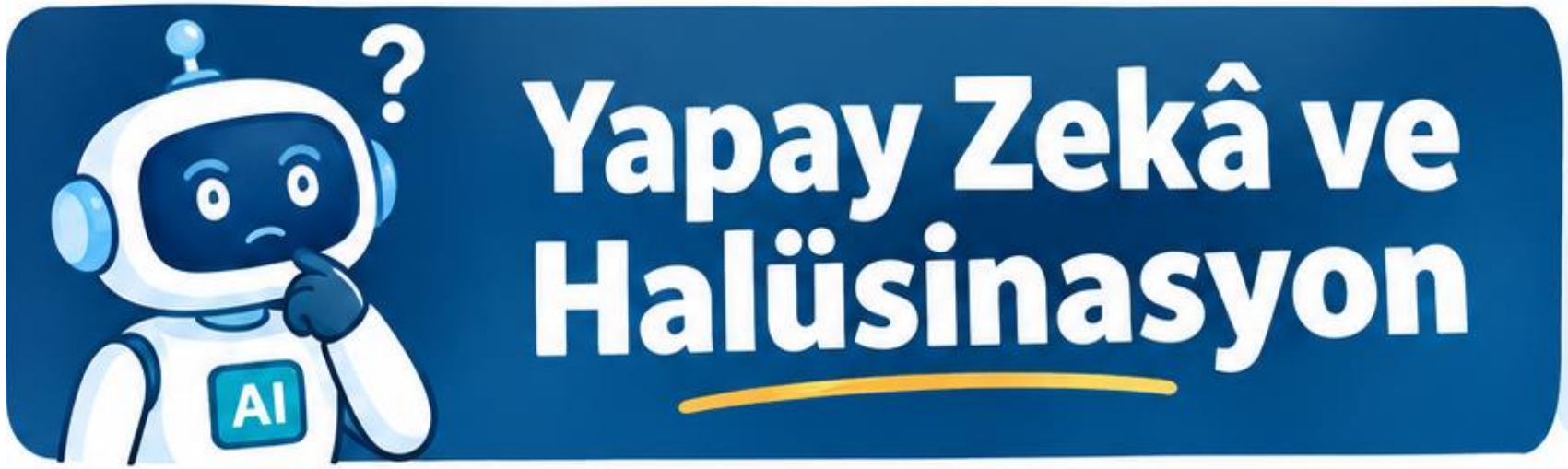
Metnini, verini veya kodunu kontrol ettirerek hataları görebilirsin.

7 Sonucu insan tarafından doğrulamak



Elde ettiğin bilgileri mutlaka sen kontrol et, kendi değerlendirmeni yap.

Yapay Zeka ve Uygulamaları - Copyright © 2026



Yapay Zekâ ve Halüsinasyon

Yapay zekâ bazen gerçek olmayan bilgileri doğruymuş gibi üretebilir.

Örneğin: Yapay zekâ aşağıdaki gibi hatalı veya uydurma bilgiler üretebilir:



Var olmayan bir makale adı

"Örneğin: Yapay Zekâ ve Eğitimde Toplumsal Dönüşüm"



Gerçek olmayan bir DOI

"Örneğin: 10.1234/xyz.5678 (yoktur)



Yanlış bir istatistik

"Örneğin: "Dünyada yapay zekâ kullanımı %87 arttı." (güvenilir veri değildir)



Uydurma bir kaynak

"Örneğin: "Smith, J. (2023). AI in Education. Global Press." (gerçek değildir)



Hatalı bir tarih

"Örneğin: "2025 yılında yapılan bir araştırma..." (gerçek olmayabilir)



Bu nedenle:

AI çıktısı ≠ Kesin doğru

Unutma!

Yapay zekâ bir araçtır.
Ürettiği bilgileri mutlaka kontrol etmeli, güvenilir kaynaklarla doğrulamalı ve eleştirel düşünmeliyiz.

Yapay Zeka ve Uygulamaları - Copyright © 2026

İnsan Denetimi

Yapay zekânın karar verdiği her süreç aynı derecede riskli değildir.

Düşük risk

"Bu metni daha anlaşılır hale getir."

İnsan kontrolü yine yararlı olmakla birlikte risk daha düşüktür.



Yüksek risk

"Bu öğrencinin üniversiteye kabul edilip edilmemesine karar ver."

Burada yalnızca yapay zekâya güvenmek ciddi etik sorunlar oluşturabilir.



İlke

Risk arttıkça insan denetimi de artırılmalıdır.



Yapay Zeka ve Uygulamaları - Copyright © 2026

Yapay Zekâ Etiğinde Sorumluluk

Yapay zekâ bir hata yaptığında:

"Yapay zekâ yaptı."

ifadesi tek başına sorumluluğu ortadan kaldırmaz.



Örnek Senaryo

Bir kurum yapay zekâ kullanarak öğrenci değerlendirmesi yapıyorsa;

Kurum	Sistemi Geliştirenler	Sistemi Kullanan Karar Vericiler
Sistemi kullanan, politikalarını belirleyen ve denetleyen taraf.	Yazılımı taşarlayan, modeli eğiten ve sistemi geliştiren ekip.	Sonuçları değerlendiren, karar veren ve uygulayan kişiler.

Bu üç tarafın sorumlulukları birlikte ele alınmalıdır.

Unutmayalım!

Yapay zekâ etiğinde asıl önemli olan, hatalarda sorumluluğu paylaşmak ve hesap verebilirliği sağlamaktır.



Daha güvenli ve adil bir gelecek için...

Prof.Dr.Hüseyin ÇAKIR
Gazi Üniversitesi

Yapay Zekâ Etiği ve Eğitim

Eğitimde etik kullanım için:

Öğretmen
- AI kullanımını öğrencilere açıklamalı.
- Öğrencileri doğrulama konusunda eğitmeli.
- Kişisel öğrenci verilerini korumalı.
- AI kullanımına ilişkin kurallar belirlemeli.

Öğrenci
- Yapay zekâ kullanımını gerektiğinde belirtmeli.
- Üretilen bilgileri doğrulamalı.
- Kendi düşünsel katkısını korumalı.
- Akademik dürüstlük ilkelerine uymalı.

Kurum
- AI kullanım politikaları oluşturmalı.
- Veri güvenliğini sağlamalı.
- Etik kullanım konusunda eğitim vermeli.
- İnsan denetimini korumalı.





Yapay Zekâ Etiğinde 7 Temel Soru

Bir yapay zekâ aracını kullanmadan önce şu sorular sorulabilir:

Yapay Zeka ve Uygulamaları - Copyright © 2026

1 Neden kullanıyorum?



Amacımı netleştirerek daha doğru bir kullanım sağlarım.

2 Hangi verileri paylaşacağım?



Kişisel ve hassas verilerimi korumak için paylaşacağım verileri dikkatle seçerim.

3 Bu kullanım adil mi?



Herkes için eşit, kapsayıcı ve ayrımcılıktan uzak bir kullanım olmasına dikkat ederim.

4 Sonuç yanlış olabilir mi?



Yapay zekânın hatalı veya eksik sonuçlar üretebileceğini unutmam.

5 Sonucu nasıl doğrulayacağım?



Bilgileri farklı kaynaklardan kontrol ederek doğruluğunu teyit ederim.

6 Kararın sorumlusu kim?



Son kararın insan tarafından verildiğini ve sorumluluğun bana ait olduğunu bilirim.

7 İnsan denetimi gerekli mi?



Özellikle önemli ve kritik kararlarda mutlaka insan denetimini sağlarım.



Yapay Zeka ve Uygulamaları - Copyright © 2026

Örnek Etik Senaryo

Bir öğretmen, öğrencilerin sınav sonuçlarını bir yapay zekâ aracına yükleyerek öğrencilerin başarı düzeylerini tahmin etmek istiyor.



Öğretmenin öncelikle şunları düşünmesi gerekir:

1. Öğrenci verilerinin paylaşılması uygun mu?
2. Kişisel bilgiler anonimleştirildi mi?
3. Kullanılan sistem verileri nasıl işliyor?
4. Tahminler ne kadar güvenilir?
5. Model bazı öğrenci gruplarına karşı önyargılı olabilir mi?
6. Sonuçlar öğrenciler hakkında kesin karar vermek için kullanılacak mı?
7. Öğretmenin nihai değerlendirme yetkisi korunuyor mu?

Yapay Zeka ve Uygulamaları - Copyright © 2026

Kişisel Veriler ve Gizlilik

Kişisel veriler ve gizlilik, yapay zekâ sistemleri kullanılırken kişilere ait bilgilerin korunması, güvenli şekilde işlenmesi ve yalnızca gerekli amaçlarla kullanılması konusunu ifade eder.

Yapay zekâ araçları çok miktarda veriyi işleyebildiği için, kullanıcıların **hangi bilgileri** yapay zekâya verdiği ve bu bilgilerin **nasıl kullanıldığı** büyük önem taşır.

Yapay zekâya verilen kişisel bilgiler

- Ad, soyad
- E-posta adresi
- Telefon numarası
- Konum bilgisi
- Eğitim / meslek bilgisi
- Diğer kişisel veriler



Gizliliğin korunması için

- Veriler güvenli şekilde saklanmalıdır.
- Sadece gerekli amaçlarla kullanılmalıdır.
- Kullanıcıların onayı alınmalıdır.
- Veri paylaşımı ve erişim kontrol altında olmalıdır.

Yapay Zeka ve Uygulamaları - Copyright © 2026


Kişisel Veri Nedir?
Kişisel veri, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgidir.

Örnekler


Ad ve soyadı



T.C. kimlik numarası


Telefon numarası


E-posta adresi


Ev veya iş adresi


Öğrenci numarası


IP adresi


Fotoğraf


Ses kaydı


Konum bilgisi


Eğitim bilgileri



Sınav sonuçları


Personel bilgileri

Özel Nitelikli Kişisel Veriler

Bazı kişisel veriler daha yüksek koruma gerektirir.



Örneğin:



Sağlık bilgileri



Biyometrik veriler



Genetik veriler



Ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili veriler



Sendika üyeliği



Din veya mezhep bilgisi



Siyasi düşünce



Felsefi veya dini inançlar

Yapay Zeka ve Uygulamaları - Copyright © 2026

Yapay Zekâya Hangi Veriler Yüklenmemelidir?

Özellikle açıkça gerekli olmadığı sürece:









T.C. kimlik numarası



Şifreler



Kredi kartı bilgileri



Sağlık kayıtları



Öğrenciye ait ayrıntılı kişisel bilgiler



Personel özlük bilgileri



Gizli kurum belgeleri



Ticari sırlar



Özel yazışmalar



Kimlik veya pasaport görüntüleri

Anonimleştirme ve Takma Adlandırma

Anonimleştirme

Kişinin kimliğinin belirlenmesini mümkün olmayacak şekilde verilerin değiştirilmesi veya kaldırılmasıdır.

Örnek



Adı: Ahmet Yılmaz
TC Kimlik No: 12345678901
E-posta: ahmet@ornek.com
Telefon: 0555 123 45 67

→

Anonimleştirilmiş Veri

Kişinin kimliği, veriden tamamen çıkarılmıştır. Artık geri dönüş mümkün değildir.

Takma Adlandırma (Pseudonymization)

Kişinin gerçek kimliği yerine farklı bir kod kullanılmasıdır.

Örnek



Ahmet Yılmaz
TC Kimlik No: 12345678901
E-posta: ahmet@ornek.com
Telefon: 0555 123 45 67

→

Takma Ad

Ö001
(Pseudonym)

Örneğin: Ahmet Yılmaz → Ö001

Ancak burada önemli bir nokta vardır:
Eğer Ö001 kodunun arkasındaki kişinin kim olduğu başka bir veri aracılığıyla belirlenebiliyorsa,
veri tamamen anonim hâle gelmiş olmayabilir.

"Anonimleştirme" kimliği tamamen ortadan kaldırır.
"Takma adlandırma" ise kimliği gizler, ancak **geri dönüş riski taşıyabilir.**

KVKK Açısından Yapay Zekâ Kullanımı

Kişisel verileriniz koruma altında!



Türkiye'de kişisel verilerin korunması açısından **6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK)** önemli bir hukuki çerçevedir.

Yapay zekâ kullanımı, kişisel verilerin korunmasına ilişkin mevcut yükümlülükleri ortadan kaldırmaz.

Yapay zekâ kullanırken özellikle şu konular dikkate alınmalıdır:

1. Verinin hangi amaçla işlendiği
2. Veri işleme için hukuki dayanak
3. Gereğinden fazla veri işlenmemesi
4. Veri güvenliği
5. İlgili kişinin hakları
6. Veri aktarımı
7. Veri sorumlusu ve veri işleyen ilişkileri
8. Özel nitelikli kişisel verilerin korunması

Gizlilik ve Yapay Zekâ Araçları

Bir yapay zekâ aracını kullanmadan önce mümkün olduğunca şu sorular sorulmalıdır:

Soru	Neden önemli?
Veriler saklanıyor mu?	Veri güvenliği
Ne kadar süre saklanıyor?	Veri kontrolü
Veriler model eğitiminde kullanılıyor mu?	Gizlilik
Veriler üçüncü taraflarla paylaşılıyor mu?	Veri aktarımı
Veri hangi ülkede işleniyor?	Hukuki gereklilikler
Kurumsal veri kullanımı destekleniyor mu?	Kurumsal güvenlik
Verileri silme seçeneği var mı?	Kullanıcı kontrolü

Öğrenciler İçin Basit Gizlilik Kuralı



Yapay zekâya bir belge veya bilgi göndermeden önce:

“Bu bilgiyi yabancı bir kişiye versem sorun olur muydu?”

sorusunu düşünmek faydalıdır.

Hayır

Eğer cevap **“Hayır”** ise, veri genellikle gönderilebilir.

Güvenle paylaşabilirsiniz.

Evet

Eğer cevap **“Evet”** ise, veri yapay zekâya gönderilmeden önce **mutlaka yeniden değerlendirilmelidir.**

Önce gözden geçirin, sonra paylaşın.

Yapay Zeka ve Uygulamaları - Copyright © 2026

Yapay Zekâ ve Telif



Yapay zekâ ve telif, yapay zekâ kullanılarak oluşturulan veya yapay zekâ sistemlerine verilen metin, görsel, ses, video, kod ve diğer içeriklerin **telif hakkı, kullanım izni, lisans ve fikrî mülkiyet** açısından değerlendirilmesini ifade eder.

Yapay Zekâ ve Telif



Değerlendirme Alanları

Telif Hakkı
İçeriğin kime ait olduğu ve korunup korunmadığı.

Kullanım İzni
İçeriğin hangi koşullarda kullanılabileceği.

Lisans
Kullanım şartlarını belirleyen resmî izinler.

Fikrî Mülkiyet
Eser, buluş ve yaratımların hukuki koruması.

Yapay zekâ ile bir içerik oluşturulabilmesi, **o içeriğin otomatik olarak serbestçe kullanılabileceği** anlamına gelmez.


Telif Hakkı Nedir?
Telif hakkı, bir eseri meydana getiren kişinin eser üzerindeki hukuken korunan haklarını ifade eder.

Örneğin:


Kitap


Makale


Fotoğraf


Resim


Müzik


Video


Film


Yazılım


Grafik


Eğitim materyali

Yapay Zekâ Tarafından Oluşturulan İçeriğin Sahibi Kim?



Bu konuda tek ve bütün durumlara uygulanabilecek basit bir cevap vermek doğru değildir.

Örneğin:

> "Yapay zekâ tarafından oluşturulan her içerik kesin olarak kullanıcının telifli eseridir." demek doğru değildir.



Telif korumasında **insanın yaratıcı katkısının niteliği, kullanılan içerikler,**, **ilgili ülkenin hukuku** ve **platformun kullanım koşulları** gibi unsurlar önem taşıyabilir.

Bu nedenle özellikle

- **Ticari kullanımlarda**
- **Akademik kullanımlarda**
- **Hukuki açıdan önemli kullanımlarda**

İlgili **mevzuat** ve **profesyonel hukuki görüş** dikkate alınmalıdır.

Yapay Zeka ve Uygulamaları - Copyright © 2026

Telif Açısından Riskli ve Daha Güvenli Yaklaşımlar

Riskli yaklaşım	Daha güvenli yaklaşım
İnternetten bulunan görseli doğrudan kullanmak	Lisansını kontrol etmek
Telifli kitabın tamamını AI'a yüklemek	Gereksiz içeriği paylaşmamak
Başkasının metnini kaynak göstermeden kullanmak	Kaynağı belirtmek
AI kaynaklarını doğrulamadan kullanmak	Orijinal kaynağı kontrol etmek
Ünlü bir kişinin görüntüsünü izinsiz kullanmak	İzin ve kullanım koşullarını değerlendirmek
Telifli müziği videoya eklemek	Uygun lisanslı müzik kullanmak
AI çıktısının otomatik olarak telifsiz olduğunu düşünmek	Platform ve hukuk koşullarını kontrol etmek

Creative Commons ve Açık Lisanslar



creative commons

Creative Commons, farklı kombinasyonlarla birden fazla lisans türünü içeren **bir lisans ailesidir.**

Bu nedenle:

"Creative Commons = Her şekilde ücretsiz kullanabilirim." anlayışı **yanlıştır.**

YANLIŞ!

Örneğin bazı lisanslar:

Atıf (BY)
Eser sahibine atıf yapılmasını şart koşar.
Atıf zorunludur.

Ticari Olmayan (NC)
Ticari kullanımın sınırlandırılmasını belirler.
Ticari kullanım yapılamaz.

Türetilmemiş (ND)
Türetilmiş eserlerin paylaşım koşullarını belirler.
Değişiklik yapılamaz.

Aynı Lisansla Paylaş (SA)
Türetilmiş eserlerin aynı lisansla paylaşılmasını şart koşar.
Aynı lisansla paylaşılmalıdır.

Lisansın türü mutlaka kontrol edilmelidir.

BY NC SA

Lisans bilgisi eserde mutlaka belirtilir.



Yapay Zeka ve Uygulamaları - Copyright © 2026

Telif İçin 5K Kontrolü

Yapay zekâ ile içerik üretmeden veya üretilen içeğği kullanmadan önce:

1 Kaynak	2 Kimlik	3 Kullanım hakkı	4 Koşullar	5 Kaynak gösterme
				
İçerik nereden geliyor?	Eserin sahibi kim?	Bu içeriği kullanma iznim var mı?	Lisans veya platform kullanım şartları ne diyor?	Atıf veya kaynak belirtmek gerekiyor mu?

Yapay Zeka ve Uygulamaları - Copyright © 2026

Deepfake ve Dezenformasyon

Deepfake

Yapay zekâ kullanılarak bir kişinin görüntüsünün, yüzünün, sesinin veya davranışlarının gerçeğe çok yakın biçimde değiştirilmesi ya da yapay olarak oluşturulmasıdır.



Dezenformasyon

Yanlış veya yanıltıcı bilgilerin kaşıtlı olarak üretilmesi ve yayılmasıdır.



Birlikte Etkisi

Bu iki kavram birleştiğinde yapay zekâ, **gerçekmiş gibi görünen** ancak gerçekte **sahte olan içeriklerin** çok hızlı ve geniş **kitlelere yayı**lmasını mümkün hâle getirebilir.



Deepfake (gerçekçi içerik) + **Dezenformasyon** (yanıltıcı bilgi)



Hızlı Yayılım → Geniş Kitlelere Ulaşım

Ne Yapmalıyız?

Dijital dünyada gördüğümüz her içeriğe hemen inanmamalı, doğrulama adımlarını mutlaka uygulamalıyız.

- Kaynağı sorgula
- Tarihi ve hesapları kontrol et
- Görselleri doğrula
- Farklı kaynaklarla karşılaştır
- Eleştirel düşün ve sorgula

Daha bilinçli bir dijital toplum için... Gerçek, araştıranların elinde!

Yapay Zeka ve Uygulamaları - Copyright © 2026

Deepfake Nedir?

Deepfake, **Deep Learning** (Derin Öğrenme) ve **Fake** (Sahte) kelimelerinden oluşur.

Yapay zekâ modelleri kullanılarak:







Yapay zekâ, kişinin yüzünü başka bir yüze dönüştürebilir.

1 Yüz Dönüştürme



Bir kişinin yüzü başka bir yüze dönüştürülebilir.

2 Ses Taklidi



Bir kişinin sesi taklit edilebilir.

3 Söz Değiştirme



Bir kişinin söylemediği sözleri söylüyormuş gibi gösteren video oluşturulabilir.

4 Fotoğraf ve Video Manipülasyonu



Fotoğraf ve videolar gerçekçi biçimde değiştirilebilir.

5 Hayal Ürünü Olaylar



Gerçekte hiç gerçekleşmemiş olaylar oluşturulabilir.

Yapay Zeka ve Uygulamaları - Copyright © 2026

Deepfake Türleri

Tür	Açıklama
Face Swap	Bir kişinin yüzünün başka bir kişinin yüzüyle değiştirilmesi
Face Reenactment	Yüz ifadelerinin değiştirilmesi
Lip Sync	Dudak hareketlerinin farklı bir konuşmaya uyarlanması
Voice Cloning	Bir kişinin sesinin yapay zekâ ile taklit edilmesi
Synthetic Video	Gerçek olmayan kişinin veya olayın video olarak oluşturulması
Image Manipulation	Görselin yapay zekâ ile değiştirilmesi

Deepfake Nerelerde Kullanılabilir?

Deepfake teknolojisinin yalnızca kötü amaçlarla kullanılması söz konusu değildir.



Yapay Zeka ve Uygulamaları

Olumlu Kullanım Alanları



Film ve sinema

Karakterleri canlandırmak, özel efektler oluşturmak veya tarihi kişileri yeniden hayata döndürmek.



Sanatsal çalışmalar

Yeni sanat eserleri üretmek, mevcut eserleri dönüştürmek ve yaratıcılığı desteklemek.



Eğitim materyalleri

Sanal öğretmenler, interaktif ders içerikleri ve kişiselleştirilmiş öğrenme deneyimleri sunmak.



Tarihsel canlandırmalar

Geçmişteki olayları ve kişileri gerçeğe yakın şekilde canlandırmak.



Dil ve seslendirme

Farklı dillerde doğal ses oluşturmak ve çeviri süreçlerini kolaylaştırmak.



Erişilebilirlik uygulamaları

İşitme ve konuşma engelliler için ses ve görüntü tabanlı çözümler sunmak.



Oyun ve eğlence

Oyun karakterlerini gerçekçi hale getirmek, kişiselleştirilmiş içerikler oluşturmak.



Araştırma

Yapay zekâ, tıp, psikoloji gibi alanlarda yeni yöntemler geliştirmek ve veri analizlerini desteklemek.

Kötüye Kullanımın Riskleri



Sahte haber ve propaganda

Seçimlere, toplumsal olaylara veya kişilere yönelik manipülatif içerikler üretilebilir.



Kimlik hırsızlığı ve dolandırıcılık

Kişilerin yüz ve sesleri izinsiz kullanılarak maddi ve manevi zararlar verilebilir.



Itibar zedeleme

Gerçek olmayan görüntü ve videolarla bireylerin veya kurumların itibarı zayıflatılabilir.



Manipülasyon ve güven kaybı

Toplumda bilgiye güven azalabilir, gerçek ve sahte ayırt etmek zorlaşabilir.



Yasal ve etik sorunlar

Kişisel verilerin izinsiz kullanımı, özel hayatın ihlali ve yasal yaptırımlar gündeme gelebilir.

Deepfake'in Riskleri

Gerçek gibi görünen her şey, gerçek olmayabilir!



Deepfake teknolojisi:

- Sahte haber üretiminde
- Dolandırıcılıkta
- Kimlik taklidinde
- İtibar saldırılarında
- Manipülasyonda
- Siber saldırılarda
- Seçmen davranışını etkilemede
- Kişilerin izinsiz görüntü veya seslerinin kullanımında

kötüye kullanılabilir.





Anne, acil paraya ihtiyacim var. Hemen gönderir misin?

Özellikle ses klonlama, kişinin yakını veya yetkili bir kişiymiş gibi davranılan dolandırıcılık girişimlerinde kullanılabilir.

Yapay Zeka ve Uygulamaları - Copyright © 2026

Dezenformasyon Nedir?

Dezenformasyon, yanlış veya yanıltıcı bilgilerin **bilerek ve kasıtlı olarak** yayılmasıdır.



Yapay Zeka ve Uygulamaları - Copyright © 2026

Örneğin:



Gerçekte gerçekleşmemiş bir olayı olmuş gibi göstermek...



ve bunu insanların inanmasını sağlamak amacıyla yaymak.



Dezenformasyon Örnekleri

Dezenformasyon, yanlış veya yanıltıcı bilgilerin kasıtlı olarak yayılmaşıdır.

Bu tür içerikler, bireyleri yanıltabilir, toplumsal algıyı etkileyebilir ve yanlış kararlar alınmasına neden olabilir.

Sahte haber

SON DAKİKA

Türkiye'de bugün tüm okullar tatil edildi!

Milli Eğitim Bakanlığı'ndan açıklama geldi.



Haber Portalı · 12.04.2025

Gerçekmiş gibi sunulan, ancak doğru olmayan haberlerdir.

Manipüle edilmiş fotoğraf





Görseller üzerinde yapılan oynamalarla gerçeği çarpıtan fotoğraflardir.

Bağlamından koparılmış video



Eski bir videonun güncel olaylarla ilişkilendirilerek yanlış şekilde paylaşılmasıdır.

Uydurma istatistik

Yapılan bir ankete göre halkın %92'si uzaylıların varlığına inanıyor.



Kaynağı olmayan veya gerçek verilerle desteklenmeyen istatistiklerdir.

Yapay Zeka ve Uygulamaları - Copyright © 2026

Sahte sosyal medya hesabı



Gerçek bir kişiye aitmiş gibi görünen, ancak sahte amaçlarla oluşturulmuş hesaplardır.

Yanlış başlık



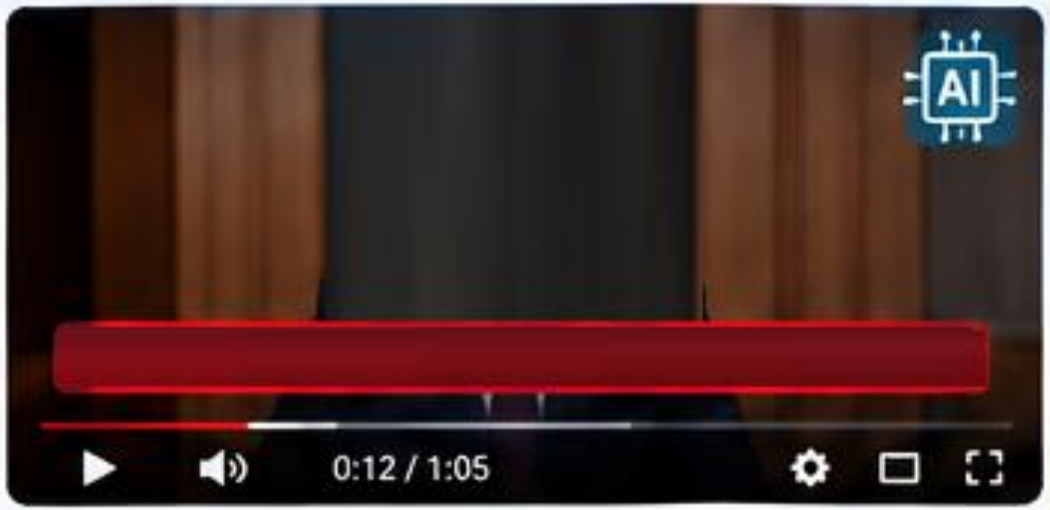
Belediye, başıboşköpekleri toplatmaya başladı!

Vatandaşlar,uygulamaya büyük tepki gösterdi.

İçeriği yansıtmayan, dikkat çekmek için yanıltıcı şekilde hazırlanan başlıklardır.

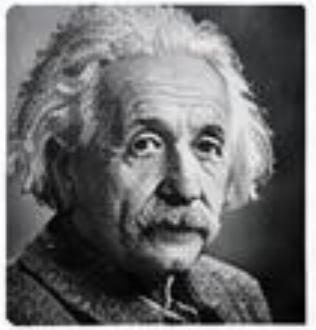
Yapay Zeka ve Uygulamaları - Copyright © 2026

Yapay zekâ ile oluşturulmuş sahte video



Yapay zekâ araçlarıyla üretilen, gerçekmiş gibi gösterilen sahte videolardır.

Gerçek olmayan alıntılar



"Başarının sırrı, hiç vazgeçmemektir."

Albert Einstein

Ünlü kişilere aitmiş gibi gösterilen, ancak gerçekte söylemedikleri sözlerdir.

Yapay Zeka ve Uygulamaları - Copyright © 2026

Deepfake + Dezenformasyon

Yapay zekâ, dezenformasyon üretimini daha kolay ve inandırıcı hâle getirebilir.


1
Gerçek kişi
Ünlü bir siyasetçi, uzman veya tanınmış bir kişi.
2
Yüz / Ses verisi
Yüz görüntüleri, ses kayıtları ve diğer biyometrik veriler toplanır.
3
Deepfake modeli
AI
Bu veriler, yapay zekâ modeliyle işlenir ve yeni bir içerik üretilir.
4
Sahte konuşma
Gerçek kişiye benzer görüntü ve sesle sahte bir konuşma oluşturulur.
5
Sosyal medya paylaşımı
12 B
4,2 B
8,7 B
Sahte içerik sosyal medyada hızla paylaşılır.
6
Yanlış bilgi
SON DAKİKA
Ünlü isimden şok açıklama!
Sahte içerik, gerçek haber gibi sunularak yanlış bilgiye dönüşür.
7
Kitlelerin etkilenmesi
Yanlış bilgi, geniş kitlelere ulaşır ve toplumsal etkiler oluşturur.

Deepfake Nasıl Anlaşılabilir?

Deepfake tespitinde tek bir işarete güvenmek doğru değildir.

Görsel

- Yüz ve boyun çevresinde olağandışı geçişler
- Doğal olmayan yüz ifadeleri
- Göz hareketlerinde tutarsızlık
- Işık ve gölge uyumsuzluğu
- El, parmak veya aksesuar hataları
- Görüntüde yapaylık


Yüz-boyun geçişinde anormallik


Doğal olmayan yüz ifadesi


Göz hareketlerinde tutarsızlık


Işık ve gölge uyumsuzluğu


El/parmak hatası


Görüntüde yapaylık

Ses

- Doğal olmayan tonlama
- Garip duraklamalar
- Kelimeler arasında olağandışı geçişler
- Duygu ve ses tonunun uyuşmaması
- Arka plan sesi ile konuşmanın uyumsuzluğu


Doğal olmayan tonlama


Garip duraklamalar


Olağandışı kelime geçişleri


Duygu ve ses tonu uyumsuzluğu


Arka plan sesi ile uyumsuzluk

Video

- Dudak hareketleri ile sesin uyuşmaması
- Kareler arasında yüz değişiklikleri
- Işık koşullarındaki tutarsızlık
- Arka plan ve kişi hareketlerinin uyumsuzluğu


Dudak hareketleri ile sesin uyuşmaması


Kareler arasında yüz değişiklikleri


Işık koşullarındaki tutarsızlık


Arka plan ve hareket uyumsuzluğu

Yapay Zeka ve Uygulamaları - Copyright © 2026

Dezenformasyon Nasıl Kontrol Edilir?

Bir içerik gördüğümüzde hemen paylaşmak yerine:

DUR

Hemen paylaşma, biraz düşün.

KONTROL ET

Bilgiyi sorgula, detayları incele.

DOĞRULA

Güvenilir kaynaklarla karşılaştır, doğruluğunu teyit et.

PAYLAŞ

Emin olduktan sonra paylaş.

Yapay Zeka ve Uygulamaları - Copyright © 2026

6 Adımda Kontrol Et

1 Kaynağa bak



İçeriği kim paylaşmış? Hesabın güvenilirliği, daha önceki paylaşımları ve kimliği incelenmeli.

2 Tarihi kontrol et



Yeni **bir olay mı**, eski bir olay yeniden mi dolaşıma sokulmuş?

3 Orijinal kaynağı bul



Video veya fotoğraf ilk nerede yayınlanmış? İlk kaynağı bularak değişiklik olup olmadığını kontrol et.

4 Farklı kaynaklarla karşılaştır



Aynı olay güvenilir başka kaynaklarda yer alıyor mu?

5 Bağlamı kontrol et



Görüntü gerçekten iddia edilen olayla mı ilgili? Tarih, yer, olay bağlamı doğru mu?

6 Kanıt ara



İddia için bağımsız kanıt bulunuyor mu? Resmi açıklamalar, uzman görüşleri veya doğrulanabilir veriler incelenmeli.

Yapay Zeka ve Uygulamaları - Copyright © 2026

Görsel ve Video Doğrulama

Bir görselin veya videonun gerçekliğini araştırırken şu adımları izleyin:







Yapay Zeka ve Uygulamaları - Copyright © 2026

Dezenformasyon yalnızca görsel veya video şeklinde değildir.

Yapay zekâ:



- Var olmayan makaleler
- Uydurma istatistikler
- Sahte alıntılar
- Gerçek olmayan kişiler
- Yanlış tarih bilgileri

Yapay Zeka ve Uygulamaları - Copyright © 2026

Eğitimde Deepfake ve Dezenformasyon

Dijital dünyada doğruyu bulmak senin elinde!

Yapay Zeka ve Uygulamaları - Copyright © 2026



Öğrencilere Kazandırılacak Beceriler

- Kaynak sorgulama
- Görsel doğrulama
- Haber doğrulama
- Kaynak karşılaştırma
- Yapay zekâ çıktısını sorgulama
- Dijital medya okuryazarlığı
- Eleştirel düşünme
- Manipülasyonu fark etme

Yapay Zeka ve Uygulamaları - Copyright © 2026

Deepfake ve Dezenformasyon Örneği

Yapay Zeka ve Uygulamaları - Copyright © 2026



Öğrencinin Yapması Gerekenler

1. Videoyu hemen **paylaşmamak.**
2. Hesabın **güvenilirliğini kontrol etmek.**
3. Videonun **tarihini** araştırmak.
4. Bilim insanının **gerçek hesaplarını kontrol etmek.**
5. Güvenilir **haber kaynaklarına** bakmak.
6. İddianın **orijinal kaynağını** araştırmak.
7. Görüntünün **eski bir videodan** değiştirilip değiştirilmediğini kontrol etmek.

Yapay Zeka ve Uygulamaları - Copyright © 2026





Deepfake Karşısında 7D Modeli

Gördüğün her şey gerçek olmayabilir. Doğruyu bulmak senin elinde!

1 D Dur



İçeriği hemen paylaşma.

2 D Düşün



İddia mantıklı mı?

3 D Doğrula



Güvenilir kaynaklara bak.

4 D Detaylandir



Tarih, yer ve bağlamı kontrol et.

5 D Diğer kaynaklara bak



Bağımsız kaynaklarla karşılaştır.

6 D Djital izi araştır



Görsel veya videonun ilk kaynağını bul.

7 D Dağıtma



Doğrulanmamış içeriği paylaşma.

Yapay Zeka ve Uygulamaları - Copyright © 2026

Yapay Zekâ Çıktılarını Doğrulama

Yapay zekâ sistemlerinden alınan cevapların **doğru, güvenilir, güncel, kaynaklara dayalı** ve **amaca uygun** olup olmadığının kontrol edilmesi yapay zekâ **çıktılarının doğrulanması** olarak ifade edilir.



Yapay zekâ oldukça akıcı ve ikna edici cevaplar üretebilir. Ancak **akıcı ve özgüvenli bir cevap, doğru cevap olduğu anlamına gelmez.**

Yapay Zeka ve Uygulamaları - Copyright © 2026



Nasıl Doğrulanır?

- **Doğruluk** — Bilgi doğru mu?
- **Güvenilirlik** — Kaynaklar güvenilir mi?
- **Güncellik** — Bilgi güncel mi?
- **Kaynaklara Dayalı Olma** — Kaynak belirtilmiş mi?
- **Amaca Uygunluk** — İhtiyacınıza uygun mu?

Temel ilke:

Yapay zekâdan gelen bilgi doğrulanmadan kesin bilgi olarak kabul edilmemelidir.

Neden Yapay Zekâ Çıktılarını Doğrulamalıyız?

Yapay zekâ, çok güçlü bir araçtır. Ancak her zaman **doğru, güncel ve güvenilir** bilgi vermez. Bu nedenle çıktılarını mutlaka kontrol etmeliyiz.

Yanlış bilgi üretebilir.
Gerçek olmayan, uydurma bilgiler verebilir.

Var olmayan kaynaklar oluşturabilir.
Gerçek olmayan makale, kitap veya web sitesi adları verebilir.

Yanlış tarih verebilir.
Eski veya gelecekteki tarihler hakkında hatalı bilgi sunabilir.

İstatistikleri yanlış yorumlayabilir.
Sayısal verileri hatalı analiz edebilir veya yanlış oranlar verebilir.



Bu tür hatalar genellikle **halüsinasyon (hallucination)** olarak adlandırılır.

Matematiksel hata yapabilir.
Hesaplamalarda yanlış sonuçlar üretebilir.

Güncel olmayan bilgi kullanabilir.
Eski verilerle yanıt verebilir, güncellemeleri kaçırabilir.

Sorudaki bağlamı yanlış anlayabilir.
Soruya tam olarak odaklanaamayabilir, farklı bir anlam yükleyebilir.

Önyargılı sonuçlar üretebilir.
Kalıplaşmış yargılara dayalı yanıtlar verebilir.

Gerçek kişilere veya olaylara ilişkin yanlış bilgiler verebilir.
Var olmayan alıntılar, yanlış isimler veya olaylar uydurabilir.

Kaynak Doğrulama

Yapay zekâ tarafından sunulan bilgiler her zaman doğru olmayabilir.
Bu nedenle kaynakları mutlaka kontrol edin.



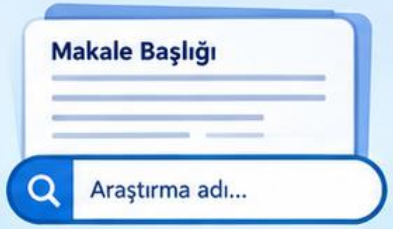
"2024 yılında yapılan bir araştırmaya göre öğrencilerin %87'si yapay zekâ kullanmaktadır."





- ✓ Yazar
- ✓ Yayın yılı
- ✓ DOI
- ✓ Yayıncı
- ✓ İçerik

1 Araştırmanın adını isteyin.



2 Makalenin yazarlarını bulun.



3 Yayın yılını kontrol edin.



4 DOI veya yayıncı sayfasını kontrol edin.



5 Makalenin gerçekten bu sonucu içerip içermediğini inceleyin.



Özellikle akademik çalışmalarda

Kaynak adı + DOI + yazar + yıl + gerçek içerik birlikte doğrulanmalıdır.

Güncellik Kontrolü

Bazı bilgiler zaman içinde değişir.

Bu nedenle, elde ettiğimiz bilgilerin ne zaman doğru olduğunu kontrol etmek önemlidir.

- Yasalar
- Yönetmelikler
- Yazılım özellikleri
- Ürün fiyatları



- İstatistikler
- Üniversite yönetmelikleri
- Akademik indeksler
- Yapay zekâ modellerinin özellikleri

Bu nedenle:

"Bu bilgi ne zaman doğruydu?"

sorusu da sorulmalıdır.



Yapay Zeka ve Uygulamaları - Copyright © 2026

Sayısal Verileri Doğrulama

Yapay zekâ matematiksel veya istatistiksel sonuçlar verirken hata yapabilir.

Örneğin:

“ Deney grubunun ortalaması 78, kontrol grubunun ortalaması 72 ve $p<0.05$ olduğundan deney yöntemi kesin olarak daha etkilidir.”

Burada yalnızca p-değerine bakmak yeterli değildir.



Kontrol Edilmesi Gerekenler:

- Ortalama doğru mu?
- Standart sapmalar doğru mu?
- Örneklem büyüklüğü doğru mu?
- Kullanılan test uygun mu?
- Varsayımlar sağlanıyor mu?
- p-değeri doğru hesaplanmış mı?
- Etki büyüklüğü nedir?
- Sonuç gerçekten nedensellik gösteriyor mu?

Yapay Zeka ve Uygulamaları - Copyright © 2026

Sayısal Verileri Doğrulama

Yapay zekâ matematiksel veya istatistiksel sonuçlar verirken hata yapabilir.

Örnek

"Deney grubunun ortalaması 78, kontrol grubunun ortalaması 72 ve $p<0.05$ olduğundan deney yöntemi kesin olarak daha etkilidir."

Burada yalnızca p-değerine bakmak yeterli değildir.



Grup	Ortalama	Standart Sapma	n
Deney	78	10.2	30
Kontrol	72	11.5	30

Bu sadece bir örnektir. Gerçek sonuçlar, başka kontrollerle doğrulanmalıdır.

Kontrol Edilmesi Gerekenler

1. Ortalama doğru mu?
2. Standart sapmalar doğru mu?
3. Örneklem büyüklüğü doğru mu?
4. Kullanılan test uygun mu?
5. Varsayımlar sağlanıyor mu?
6. p-değeri doğru hesaplanmış mı?
7. Etki büyüklüğü nedir?
8. Sonuç gerçekten nedensellik gösteriyor mu?

Yapay Zeka ve Uygulamaları - Copyright © 2026

Görsel Çıktıların Doğrulanması

Yapay zekâ tarafından oluşturulan görsellerde aşağıdaki unsurlar hatalı olabilir. Bu tür bilgileri kullanmadan önce mutlaka kontrol edin.

Yapay Zeka ve Uygulamaları

Yazılar

Türkiye'nin başkenti İstanbul'dur.

Türkiye'nin başkenti Ankara'dır.

Yazım hataları, yanlış kelimeler ve dil bilgisi hataları olabilir.

Sayılar

12.856

12.658

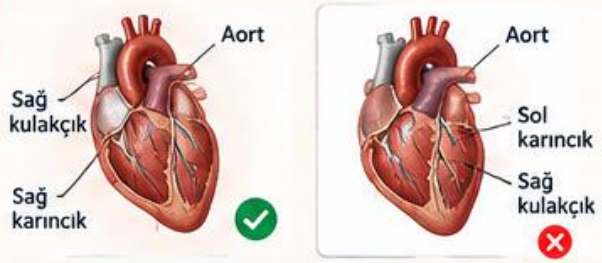
Rakamlar yanlış yazılabilir, sayılar karıştırılabilir veya hesaplamalar hatalı olabilir.

Grafikler



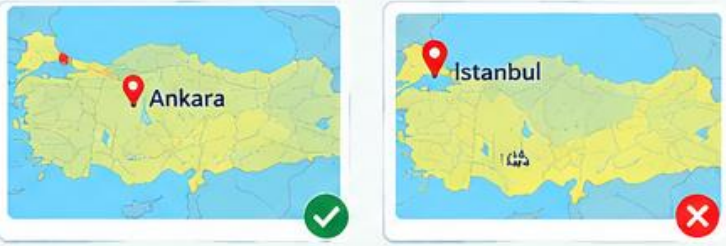
Grafiklerde eksenler, ölçekler, veriler ve etiketler hatalı olabilir.

Anatomik yapılar



Organlar, kemikler, kaslar ve diğer anatomik yapılar yanlış gösterilebilir.

Haritalar



Ülke sınırları, şehirler, konumlar ve coğrafi bilgiler hatalı olabilir.

Teknik parçalar



Parçaların şekli, boyutları, bağlantıları ve teknik özellikleri yanlış olabilir.

Tarihsel ayrıntılar



Tarih, kişi, olay ve dönemlere ait bilgiler hatalı verilebilir.

Güvenilirlik Seviyeleri

AI çıktıları üç kategoriye ayrılabilir.

Yüksek Güven

Güvenilir bağımsız kaynaklarla doğrulanmış bilgi.



- Resmi kurumlar
- Akademik yayınlar
- Güvenilir haber siteleri

Örnek:
"Dünya Sağlık Örgütü'ne (WHO) göre günlük 10.000 adım sağlığa iyi gelir."

Orta Güven

Mantıklı görünen ancak bağımsız olarak doğrulanması gereken bilgi.



- Kaynak kontrolü gerekir
- Farklı kaynaklarla karşılaştırılmalı
- Ek doğrulama yapılmalı

Örnek:
"Bu diyet yöntemiyle haftada 2 kilo verebilirsiniz."

Düşük Güven

Kaynağı bulunamayan, çelişkili veya doğrulanamayan bilgi.



- Kaynak yok
- Çelişkili bilgiler
- Doğrulanamaz iddialar

Örnek:
"Bu ilaç tüm hastalıkları kesin olarak iyileştirir."

Kullanım İlkesi

Doğrula → Kullan → **Kontrol Et → Sonra Kullan** → **Doğrulanamıyorsa → Kullanma**

Yapay Zeka ve Uygulamaları - Copyright © 2026

"AI Çıktısını Doğrulama" Kontrol Listesi

Bir yapay zekâ cevabını kullanmadan önce:

- ☐ 1 Bilgi gerçekten doğru mu?
- ☐ 2 Kaynak var mı?
- ☐ 3 Kaynak gerçekten mevcut mu?
- ☐ 4 Kaynak iddiayı destekliyor mu?
- ☐ 5 Bilgi güncel mi?
- ☐ 6 Sayılar doğru mu?
- ☐ 7 Hesaplamalar doğru mu?
- ☐ 8 Bağlam doğru mu?
- ☐ 9 Farklı güvenilir kaynaklar aynı bilgiyi veriyor mu?
- ☐ 10 Yapay zekâdan gelen yorum ile gerçek veri birbirinden ayrılmış mı?
- ☐ 11 Kişisel/etik/hukuki risk var mı?

Yapay Zeka ve Uygulamaları - Copyright © 2026