T.C. CUMHURBAŞKANLIĞI
İLETİŞİM BAŞKANLIĞI

KAMU KURUMLARI İÇİN

YAPAY ZEKÂ SÖZLÜĞÜ

İÇİNDEKİLER

ÖN SÖZ.....5
BÖLÜM A - TEMEL KAVRAMLAR.....9
BÖLÜM B - VERİ VE ALTYAPI.....21
BÖLÜM C - ÜRETKEN YAPAY ZEKÂ VE MODEL AİLELERİ.....33
BÖLÜM D - ETİK, GÜVEN VE YÖNETİŞİM.....45
BÖLÜM E - HUKUK, UYGULAMA VE KURUMSAL KULLANIM.....53
BÖLÜM F - AJANLAR, PROTOKOLLER VE ENTEGRASYON.....61
BÖLÜM G - YAPAY ZEKÂ GÜVENLİĞİ.....69
KAYNAKÇA.....77

ÖN SÖZ

Yapay zekâ; kamu kurumlarının hizmet üretim biçimlerini, karar destek süreçlerini, veri işleme alışkanlıklarını, vatandaşla kurduğu iletişim kanallarını ve yöntemini dönüştüren dijital teknolojilerin en ileri aşamasıdır. Söz konusu araçlar, hayatın her alanında kapsamlı dönüşümlere yol açması bakımından oldukça önemlidir. Bu çerçevede yapay zekâyı ve yol açtığı değişimi anlamak büyük önem arz etmektedir. Yapay zekâya ilişkin kavramların doğru anlaşılması, ortak bir terminolojinin kurulması ve teknolojik gelişmelerin yönetimi, hukuki ve etik boyutlarıyla birlikte ele alınması; sağlıklı, güvenilir ve sürdürülebilir bir kurumsal yapı için hayatidir.

İletişim Başkanlığı olarak, yapay zekânın imkanlarından istifade ederken, olumsuz etkilerine karşı da tedbir almak amacıyla çalışmalarımızı sürdürüyoruz. Türkiye'nin dijital egemenliğini tahkim etmek ve dezenformasyonla mücadelede öncü bir rol üstlenmek temel vizyonumuzdur. Bu vizyon doğrultusunda geliştirdiğimiz "Yapay Zekâ Kalkanı" yaklaşımı, devletimizin dijital varlıklarının ve ürettiği resmî bilginin vatandaşlarımızın yanı sıra yapay zekâ sistemleri için de güvenilir ve öncelikli bir başvuru kaynağı olmasını hedeflemektedir. Amacımız, küresel bilgi ekosisteminde Türkiye'nin epistemik egemenliğini ve sağlıklı bir iletişim düzenini tesis etmektir. Günümüzde stratejik iletişim, çatışma alanları ve krizler birbirinden

ayrı düşünülemez. Tehditler artık sadece konvansiyonel silahlardan değil, sistematik dezenformasyonlardan ve manipülasyon gibi art niyetli girişimlerden de kaynaklanmaktadır. Böylesi bir dönemde, yapay zekâ sistemlerinin doğrulanmamış iddiaları tekrarlamasını önlemek ve sadece doğru bilgilere dayanmasını sağlamak ulusal güvenliğimizin ayrılmaz bir parçasıdır.

Elinizdeki **Yapay Zekâ Sözlüğü** kitabı, bu anlayışın bir sonucudur ve kamu yöneticileri, hukuk birimleri, denetçiler, uzmanlar, iletişim ekipleri ve uygulayıcı personel için ortak bir başvuru kaynağı oluşturmak amacıyla hazırlanmıştır. Çalışmanın temel yaklaşımı, her terimi kısa bir tanımla sınırlı bırakmamak; kamuda kullanım örneği, kurumsal dikkat notu ve ilişkili terimler eşliğinde kavramları bağlamına oturtmaktır. Böylece okuyucunun, teknik bir ifadeyi yalnızca ezberlemesi değil, bu ifadenin kurum içi süreçlerde ne anlama gelebileceğini somut biçimde görmesi hedeflenmiştir.

Sözlükte yer alan bölüm yapısı, yapay zekâ alanını kamu kurumlarının ihtiyaç duyduğu bakış açısıyla katmanlı biçimde ele almaktadır. Temel kavramlar ve öğrenme yöntemleri, veri ve altyapı başlıkları, üretken yapay zekâ uygulamaları, etik ve yönetişim ilkeleri, hukuk ve kamu uygulaması çerçevesi ile ajan sistemleri ve yapay zekâ güvenliği gibi yeni nesil alanlar, bir bütünlük içinde sunulmuştur. Bu yapı, konu üzerine çalışmaya yeni başlayan ya da bu alanda belirli bir uygulama hazırlığı yürüten okuyucunun kavramlar arasındaki ilişkiyi adım adım kurmasına imkân tanımaktadır.

Kamu kurumlarında yapay zekâ kullanımının başarı ölçütü yalnızca hız, verimlilik veya teknik doğruluk değildir. Aynı zamanda şeffaflık, hesap verebilirlik, insan denetimi, mahremiyet, güvenlik ve kamu yararı ilkelerinin korunması da gereklidir. Elinizdeki sözlük, tam da bu nedenle, yapay zekâyı ne sihirli bir çözüm aracı olarak ne de bütünüyle uzak durulması gereken bir tehdit olarak görmektedir. Amaç; kavramları yerli yerine oturtan, riskleri görünür kılan, dijital alanda hakikati esas alan ve kurumsal kapasiteyi güçlendiren dengeli bir referans çerçevesi sunmaktır.

Yapay Zekâ Sözlüğü'nün, Cumhurbaşkanımız Sayın Recep Tayyip Erdoğan'ın ortaya koyduğu Türkiye Yüzyılı vizyonu doğrultusunda, devletimizin dijital hafızasının güçlendirilmesi ve yapay zekâ çağında kamu bilgisinin korunması hedeflerimize önemli bir katkı sunacağına inanıyorum. Bu değerli eserin hazırlanmasında emeği geçen çalışma arkadaşlarıma teşekkür ediyor, sözlüğün kurumlarımız ve ülkemiz için hayırlı olmasını diliyorum.

Prof. Dr. Burhanettin Duran
T.C. Cumhurbaşkanlığı İletişim Başkanı

Bölüm Planı

Kod	Bölüm	Terim Sayısı
A	Temel Kavramlar	21
B	Veri ve Altyapı	19
C	Üretken Yapay Zekâ ve Model Aileleri	19
D	Etik, Güven ve Yönetişim	13
E	Hukuk, Uygulama ve Kurumsal Kullanım	10
F	Ajanlar, Protokoller ve Entegrasyon	13
G	Yapay Zekâ Güvenliği	12

BÖLÜM A

TEMEL KAVRAMLAR

Yapay zekâya ilişkin tartışmalar çoğu zaman tekil bir teknoloji başlığı etrafında yürütülse de kamu kurumları açısından esas ihtiyaç, kavramları birbirinden ayıran berrak bir ortak dildir. Yapay zekâ, algoritma, model, veri kümesi, sınıflandırma ya da doğal dil işleme gibi temel kavramlar, yalnızca teknik ekiplerin gündeminde yer alan uzmanlık terimleri değildir; politika üretiminden denetime, tedarikten iletişime kadar çok geniş bir kurumsal alana dokunur. Bu nedenle temel kavramların açık, tutarlı ve aynı zamanda uygulamaya dönük biçimde tanımlanması, kurumlar arasında ortak anlayış kurulmasının ilk şartıdır.

Kamu bağlamında kavramların doğru anlaşılması, yalnızca terminolojik bir hassasiyet değil, aynı zamanda yönetsel bir gerekliliktir. Çünkü hangi sistemin basit bir otomasyon olduğu, hangisinin makine öğrenmesi içerdiği, hangisinin üretken nitelik taşıdığı ya da hangisinin öngörüye dayalı karar desteği sunduğu doğru ayırt edilemediğinde; beklentiler, risk analizleri ve sorumluluk mekanizmaları da bulanıklaşır. Bu bölümde yer alan terimler, yapay zekâ alanının temel kavramlarını kamu kurumlarındaki belge işleme, hizmet planlama, çağrı merkezi yönetimi, arşiv düzenleme ve analiz süreçleri çerçevesinde ele almaktadır.

Bölümün son kısmında yer alan öğrenme yöntemleri ise bugün sıkça duyulan teknik ifadelerin arka planını anlaşılır kılmakta-

dır. Denetimli, denetimsiz, yarı denetimli ve öz denetimli öğrenme yaklaşımlarının yanı sıra takviyeli öğrenme, federatif öğrenme, sıfır atış ve az atış öğrenme gibi güncel yöntemler; sistemlerin hangi verilerle, hangi koşullarda ve hangi sınırlılıklar içinde geliştirildiğini açıklamak bakımından önem taşır. Böylece okuyucu, sonraki bölümlerde karşılaşacağı daha ileri kavramları yalnızca isim düzeyinde değil, yöntem ve amaç düzeyinde de daha sağlam bir zeminde değerlendirebilir.

Bu bölümdeki terim sayısı	21

TERİMLER

A1 - Yapay Zekâ / *Artificial Intelligence (AI)*

Tanım	Yapay zekâ, bilgisayar sistemlerinin normalde insan zekâsıyla ilişkilendirilen öğrenme, örüntü tanıma, çıkarım yapma, karar desteği sunma ve içerik üretme gibi işlevleri yerine getirebilmesini sağlayan yöntemlerin genel adıdır.
Kamuda kullanım örneği	Bir kamu kurumu, vatandaştan gelen binlerce başvuruyu konu başlığına göre ön sınıflandırma yapmak ve ilgili birime yönlendirmek için yapay zekâ destekli bir sistem kullanabilir. Böylece işlem süreleri kısalır ve insan kaynağı daha nitelikli işlere yönlendirilebilir.
Kurumsal dikkat notu	Yapay zekâ sistemleri nihai kamu otoritesinin yerine geçmez; insan sorumluluğunu destekleyen araçlar olarak konumlandırılmalıdır.
İlişkili terimler	Algoritma, model, makine öğrenmesi, karar destek sistemi

A2 - Algoritma / *Algorithm*

Tanım	Algoritma, belirli bir problemi çözmek veya bir görevi yerine getirmek amacıyla tanımlanmış adımlar bütünüdür. Yapay zekâ sistemleri de dâhil olmak üzere dijital süreçlerin temel işleyiş mantığı algoritmalar aracılığıyla kurulur.
Kamuda kullanım örneği	Bir belediyenin çağrı merkezi taleplerini aciliyet seviyesine göre sıralayan sistem, arka planda belirli kuralları ve ölçütleri esas alan bir algoritma ile çalışır.
Kurumsal dikkat notu	Algoritmanın hangi ölçütleri kullandığı şeffaf biçimde denetlenmezse kamu güveni zedelenebilir.
İlişkili terimler	Şeffaflık, açıklanabilirlik, sınıflandırma, risk sınıflandırması

A3 - Model / *Model*

Tanım	Model, verideki örüntüleri öğrenerek yeni veriler üzerinde tahmin, sınıflandırma, öneri veya üretim yapabilen matematiksel ve hesaplamalı yapıdır. Yapay zekâ uygulamalarında model, sistemin asıl karar veya çıktı üreten çekirdeğini oluşturur.
Kamuda kullanım örneği	Bir sosyal hizmet birimi, yoğun başvuru dönemlerinde hangi ilçelerde hizmet talebinin artacağını öngörmek için geçmiş verilerle eğitilmiş bir model kullanabilir.
Kurumsal dikkat notu	Modelin başarısı yalnızca yazılıma değil; veri kalitesine, kullanım amacına ve güncel koşullara uygunluğa bağlıdır.
İlişkili terimler	Veri kümesi, eğitim verisi, test verisi, performans göstergesi

A4 - Makine Öğrenmesi / *Machine Learning*

Tanım	Makine öğrenmesi, bir sistemin tüm kuralların önceden tek tek tanımlanmasına ihtiyaç duymadan, verideki örüntülerden öğrenerek görev yerine getirmesini sağlayan yapay zekâ yaklaşımıdır. Günümüzde kamu uygulamalarında kullanılan çok sayıda sınıflandırma, tahminleme ve öneri sistemi bu yaklaşım temelinde geliştirilmektedir.
Kamuda kullanım örneği	Bir kamu sağlık kurumunda randevu iptal olasılıklarını tahmin ederek kapasite planlaması yapmak için makine öğrenmesi kullanılabilir.
Kurumsal dikkat notu	Makine öğrenmesi sonuçları geçmiş verinin izlerini taşır; bu nedenle öğrenilmiş önyargıları modele taşınma riski vardır.
İlişkili terimler	Denetimli öğrenme, denetimsiz öğrenme, veri önyargısı, adillik

A5 - Derin Öğrenme / *Deep Learning*

Tanım	Derin öğrenme, çok katmanlı yapay sinir ağları kullanarak karmaşık örüntüleri öğrenen makine öğrenmesi alt alanıdır. Görüntü, ses ve doğal dil işleme gibi yüksek boyutlu veri türlerinde özellikle güçlü sonuçlar üretmektedir.
Kamuda kullanım örneği	Bir arşiv dijitalleştirme projesinde taranmış evraklardaki damga, imza veya metin örüntülerini ayırt etmek için derin öğrenme tabanlı çözümler kullanılabilir.
Kurumsal dikkat notu	Derin öğrenme sistemleri yüksek doğruluk sunsa da açıklanabilirlik seviyesi değişkenlik gösterebilir; bu nedenle yüksek etkili süreçlerde insan denetimi gerekir.
İlişkili terimler	Yapay sinir ağı, bilgisayarlı görü, doğal dil işleme, yorumlanabilirlik

A6 - Yapay Sinir Ağı / *Artificial Neural Network*

Tanım	Yapay sinir ağı, insan beynindeki sinir bağlantılarından esinlenen ve katmanlar hâlinde çalışan hesaplamalı model yapısıdır. Verideki karmaşık ilişkileri yakalamak için çok sayıda bağlantılı düğümden yararlanır.
Kamuda kullanım örneği	Afet yönetiminde farklı sensörlerden ve saha raporlarından gelen verileri birlikte işleyerek riskli bölgeleri öne çıkaran sistemlerde yapay sinir ağları kullanılabilir.
Kurumsal dikkat notu	Yapay sinir ağlarının sonuçları güçlü olabilir; ancak kararın nasıl oluştuğunu sade biçimde açıklamak her zaman kolay olmayabilir.
İlişkili terimler	Derin öğrenme, model, açıklanabilirlik, güvence

A7 - Sınıflandırma / *Classification*

Tanım	Sınıflandırma, verilerin önceden belirlenmiş kategorilerden birine atanması sürecidir. Kamu kurumlarında belge türü ayırma, başvuru konusu belirleme ve risk seviyelerini ayırt etme gibi birçok işlem bu yaklaşımla yapılabilir.
Kamuda kullanım örneği	Bir bakanlığın elektronik başvuru sisteminde gelen taleplerin "bilgi talebi", "şikâyet", "teknik destek" ve "başvuru güncelleme" olarak otomatik ayrılması sınıflandırma örneğidir.
Kurumsal dikkat notu	Yanlış sınıflandırma, vatandaşın yanlış birime yönlendirilmesine veya işlem gecikmesine yol açabilir.
İlişkili terimler	Algoritma, makine öğrenmesi, etiket, test verisi

A8 - Tahminleme / *Prediction / Forecasting*

Tanım	Tahminleme, geçmiş ve mevcut verilerden hareketle geleceğe ilişkin olası durumların hesaplanmasıdır. Kamu yönetiminde talep yoğunluğu, hizmet başvurusu, bakım ihtiyacı veya kaynak kullanımı gibi alanlarda yararlanılabilir.
Kamuda kullanım örneği	Kış aylarında kar yağışı ve trafik yoğunluğu verilerini kullanan bir büyükşehir belediyesi, yol bakım ekiplerinin hangi bölgelerde konuşlandırılacağını tahminleme modelleriyle planlayabilir.
Kurumsal dikkat notu	Tahmin, kesin bilgi değildir; karar vericiyi destekleyen olasılıksal bir araç olarak görülmelidir.
İlişkili terimler	Model, performans göstergesi, karar destek sistemi, risk sınıflandırması

A9 - Doğal Dil İşleme / *Natural Language Processing (NLP)*

Tanım	Doğal dil işleme, insan dilindeki metin ve konuşmaları bilgisayarların analiz etmesini, anlamasını ve gerektiğinde yanıt üretmesini sağlayan yapay zekâ alanıdır. Kamu kurumlarında yazışma, başvuru metni, çağrı kaydı ve basın izleme verileri üzerinde yaygın kullanım potansiyeline sahiptir.
Kamuda kullanım örneği	Bir iletişim birimi, günlük basın taramasındaki haberleri konu başlıklarına ayırmak ve kritik gelişmeleri özetlemek için doğal dil işleme araçlarından yararlanabilir.
Kurumsal dikkat notu	Doğal dil işleme araçları yüksek fayda sunsa da bağlam hataları, yorum farkları ve hassas verilerin korunması bakımından dikkatle değerlendirilmelidir.
İlişkili terimler	Büyük dil modeli, istem, özetleme, halüsinasyon

A10 - Bilgisayarlı Görü / *Computer Vision*

Tanım	Bilgisayarlı görü, görüntü ve video verilerinin yapay zekâ yardımıyla analiz edilmesini sağlayan alandır. Nesne tanıma, sahne yorumlama, belge görüntüsü işleme ve görsel inceleme gibi işlevleri kapsar.
Kamuda kullanım örneği	Bir tapu arşivinde eski belgelerin taranmış kopyalarındaki mühür, mülk adı ve form düzenini tespit etmek için bilgisayarlı görü çözümleri kullanılabilir.
Kurumsal dikkat notu	Görüntü verileri kişisel veri ve mahremiyet boyutu taşıyabileceğinden erişim, veri güvenliği, saklama ve işleme süreçleri dikkatle yönetilmelidir.
İlişkili terimler	Derin öğrenme, çok kipli model, mahremiyet, veri egemenliği

A11 - Denetimli Öğrenme / *Supervised Learning*

Tanım	Denetimli öğrenme, doğru çıktıları bilinen örneklerle eğitilen makine öğrenmesi yaklaşımıdır. Sistem, etiketlenmiş veriler üzerinden hangi girdinin hangi sonuca karşılık geldiğini öğrenir.
Kamuda kullanım örneği	Geçmişte uzmanlarca doğru konuya atanmış vatandaş talepleri kullanılarak yeni başvuruları otomatik yönlendiren bir sistem eğitilebilir.
Kurumsal dikkat notu	Etiketli veri kalitesiz veya tutarsızsa sistem yanlış davranışları da öğrenebilir; veri kalitesi de denetlenmelidir.
İlişkili terimler	Etiket, eğitim verisi, test verisi, sınıflandırma

A12 - Denetimsiz Öğrenme / *Unsupervised Learning*

Tanım	Denetimsiz öğrenme, önceden etiketlenmemiş veriler içindeki örüntüleri, kümeleri veya ilişkileri keşfetmeye çalışan makine öğrenmesi yaklaşımıdır. Daha çok veri keşfi ve eğilim analizi için kullanılır.
Kamuda kullanım örneği	Bir kamu kurumunun çağrı merkezi kayıtları üzerinde çalışılarak daha önce resmi kategoriye alınmamış yeni sorun kümeleri tespit edilebilir.
Kurumsal dikkat notu	Denetimsiz öğrenme bulguları doğrudan karar temeli olarak değil; analitik keşif aracı olarak yorumlanmalıdır.
İlişkili terimler	Makine öğrenmesi, veri kümesi, öznitelik, tahminleme

A13 - Takviyeli Öğrenme / *Reinforcement Learning*

Tanım	Takviyeli öğrenme, bir yapay zekâ ajanının çevresiyle etkileşime girerek, doğru eylemler için ödül ve yanlış eylemler için ceza alarak deneme yanılma yoluyla en iyi stratejiyi öğrenmesi yöntemidir. Sistem, uzun vadeli ödülü en üst düzeye çıkarmayı hedefler.
Kamuda kullanım örneği	Bir akıllı şehir uygulamasında trafik ışıklarının süreleri, kavşaklardaki anlık araç yoğunluğuna göre takviyeli öğrenme algoritmalarıyla dinamik olarak ayarlanarak trafik akışı optimize edilebilir.
Kurumsal dikkat notu	Takviyeli öğrenme modelleri gerçek dünyada beklenmedik durumlara karşı hassas olabilir; bu nedenle simülasyon ortamlarında kapsamlı testler yapılmadan doğrudan kritik altyapılara entegre edilmemelidir.
İlişkili terimler	Makine öğrenmesi, yapay zekâ ajanı, insan geri bildirimli takviyeli öğrenme

A14 - Yarı Denetimli Öğrenme / *Semi-Supervised Learning*

Tanım	Yarı denetimli öğrenme, az miktarda etiketli veri ile çok miktarda etiketsiz verinin birlikte kullanıldığı makine öğrenmesi yaklaşımıdır. Etiketleme maliyetinin yüksek olduğu durumlarda modelin performansını artırmak için kullanılır.
Kamuda kullanım örneği	Bir sağlık kurumunda tıbbi görüntülerin sınıflandırılmasında, uzmanlar tarafından etiketlenmiş az sayıda röntgen görüntüsü ile binlerce etiketsiz görüntü birlikte kullanılarak modelin hastalık tespit başarısı artırılabilir.
Kurumsal dikkat notu	Etiketsiz verilerin kalitesi ve dağılımı, modelin doğruluğunu doğrudan etkiler; verilerin temsil edici olduğundan emin olunmalıdır.
İlişkili terimler	Denetimli öğrenme, denetimsiz öğrenme, etiket, eğitim verisi

A15 - Öz Denetimli Öğrenme / *Self-Supervised Learning*

Tanım	Öz denetimli öğrenme, sistemin dışarıdan insan tarafından sağlanan etiketlere ihtiyaç duymadan, verinin kendi içindeki yapıyı kullanarak kendi etiketlerini oluşturduğu ve öğrendiği yöntemdir. Özellikle büyük dil modellerinin eğitiminde temel bir yaklaşımdır.
Kamuda kullanım örneği	Bir kamu kurumunun devasa metin arşivindeki belgeler, öz denetimli öğrenme ile analiz edilerek kurumun kendine özgü dil yapısını ve terminolojisini anlayan bir temel model geliştirilebilir.
Kurumsal dikkat notu	Bu yöntem çok büyük veri kümeleri ve yüksek hesaplama gücü gerektirir; veri güvenliği ve altyapı maliyetleri dikkate alınmalıdır.
İlişkili terimler	Temel model, büyük dil modeli, denetimsiz öğrenme

A16 - Transfer Öğrenme / *Transfer Learning*

Tanım	Transfer öğrenme, bir görevi çözerken elde edilen bilginin, farklı ancak ilişkili başka bir görevin çözümünde başlangıç noktası olarak kullanılmasıdır. Modelin sıfırdan eğitilmesine kıyasla zaman ve veri tasarrufu sağlar.
Kamuda kullanım örneği	Genel Türkçe metinler üzerinde eğitilmiş bir dil modeli, transfer öğrenme yöntemiyle sadece hukuk metinleri üzerinde kısa bir ek eğitimden geçirilerek mevzuat analizinde yüksek başarı gösterecek hâle getirilebilir.
Kurumsal dikkat notu	Kaynak modelin içerdiği olası önyargılar veya hatalar, hedef modele de aktarılabilir; bu nedenle kaynak modelin güvenilirliği önemlidir.
İlişkili terimler	İnce ayar, temel model, makine öğrenmesi

A17 - Federatif Öğrenme / *Federated Learning*

Tanım	Federatif öğrenme, verilerin merkezi bir sunucuda toplanması yerine, modelin verilerin bulunduğu farklı cihazlarda veya kurumlarda yerel olarak eğitilmesi ve sadece öğrenilen güncellemelerin merkezde birleştirilmesi yöntemidir.
Kamuda kullanım örneği	Farklı hastaneler, hasta verilerini birbirleriyle paylaşmadan, kendi verileri üzerinde yerel olarak eğittikleri modellerin sonuçlarını birleştirerek ortak ve daha güçlü bir teşhis modeli geliştirebilirler.
Kurumsal dikkat notu	Veri mahremiyetini korumak için güçlü bir yöntem olsa da, uç cihazların güvenliği ve ağ bağlantılarının şifrelenmesi kritik önem taşır.
İlişkili terimler	Mahremiyet, veri egemenliği, uç yapay zekâ, siber güvenlik

A18 - Sıfır Atış Öğrenme / *Zero-Shot Learning*

Tanım	Sıfır atış öğrenme, bir modelin eğitim aşamasında hiç karşılaşmadığı yeni bir sınıfı veya görevi, yalnızca o sınıfın tanımına veya özelliklerine dayanarak doğru bir şekilde tanıyabilmesi veya yerine getirebilmesi yeteneğidir.
Kamuda kullanım örneği	Bir belge sınıflandırma sistemi, eğitim verisinde hiç bulunmayan yeni bir kategoriyi, sadece bu kategorinin anlamsal tanımını kullanarak doğru bir şekilde sınıflandırabilir.
Kurumsal dikkat notu	Sıfır atış performansı genellikle modele özel eğitim verilmiş durumlara göre daha düşüktür; kritik kararlarda tek başına güvenilmemelidir.
İlişkili terimler	Büyük dil modeli, istem tasarımı, az atış öğrenme

A19 - Az Atış Öğrenme / *Few-Shot Learning*

Tanım	Az atış öğrenme, modelin yeni bir görevi veya kavramı öğrenmek için geniş bir örnek kümesi yerine, sınırlı sayıda örnekle başarılı sonuçlar üretebilmesi yaklaşımıdır.
Kamuda kullanım örneği	Bir çağrı merkezi asistanına, yeni başlatılan bir kamu hizmetiyle ilgili sadece üç adet örnek soru-cevap çifti verilerek, vatandaşlardan gelecek benzer soruları doğru yanıtlaması sağlanabilir.
Kurumsal dikkat notu	Verilen az sayıdaki örneğin kalitesi ve temsil gücü çok yüksektir; yanıltıcı örnekler modelin tamamen yanlış yönlenmesine neden olabilir.
İlişkili terimler	İstem tasarımı, sıfır atış öğrenme, ince ayar

A20 - Sürekli Öğrenme / *Continual / Lifelong Learning*

Tanım	Sürekli öğrenme, bir yapay zekâ sisteminin zaman içinde yeni veriler ve görevler geldikçe, daha önce öğrendiği bilgileri unutmadan bilgi birikimini sürekli olarak güncellemesi ve genişletmesi yeteneğidir.
Kamuda kullanım örneği	Bir siber güvenlik tehdit algılama sistemi, geçmiş yıllardaki saldırı türlerini tanıma yeteneğini kaybetmeden, her gün ortaya çıkan yeni zararlı yazılım örüntülerini sürekli olarak öğrenip kendini güncelleyebilir.
Kurumsal dikkat notu	Modelin yeni bilgileri öğrenirken eski doğruları unutmadığından emin olmak için düzenli doğrulama testleri yapılmalıdır.
İlişkili terimler	Model, eğitim verisi, performans göstergesi

A21 - İnsan Geri Bildirimli Takviyeli Öğrenme / *Reinforcement Learning from Human Feedback (RLHF)*

Tanım	İnsan geri bildirimli takviyeli öğrenme, modelin ürettiği çıktıların insanlar tarafından değerlendirilip puanlanması ve bu puanların modeli daha güvenli, faydalı ve insan tercihlerine uygun hâle getirmek için ödül sinyali olarak kullanılmasıdır.
Kamuda kullanım örneği	Bir kamu kurumu için geliştirilen metin üretme asistanının verdiği yanıtlar, kurum uzmanları tarafından resmî dile uygunluk ve doğruluk açısından puanlanarak modelin kurumsal üslubu öğrenmesi sağlanabilir.
Kurumsal dikkat notu	Geri bildirim veren kişilerin kendi önyargıları modele yansıyabilir; bu nedenle değerlendirici havuzunun çeşitli ve kurumsal ilkelere hâkim olması gerekir.
İlişkili terimler	Takviyeli öğrenme, ince ayar, insan denetimi, önyargı

BÖLÜM B

VERİ VE ALTYAPI

Yapay zekâ projelerinin başarısı çoğu zaman model seçiminden önce veri düzenine, kurumsal kayıt kalitesine ve altyapı mimarisine bağlıdır. Kamu kurumlarında veri; arşivlerden başvuru sistemlerine, sensör kayıtlarından yazışma havuzlarına kadar çok farklı kaynaklarda dağınık biçimde bulunabilir. Bu nedenle yapay zekâ uygulamalarını anlamak, yalnızca model kavramını değil; verinin nasıl toplandığını, temizlendiğini, saklandığını, etiketlendiğini ve güvenli biçimde erişilebilir kılındığını da kavramayı gerektirir.

Bu bölüm, veriyi yapay zekâ projelerinin ham girdisi olmanın ötesinde, kurumsal güven ve sürdürülebilirlik zemini olarak ele almaktadır. Zayıf veri kalitesi, eksik etiketleme, önyargılı kayıtlar veya belirsiz veri yönetişimi yapıları; en gelişmiş modelin dahi kamu yararı üretmesini engelleyebilir. Aynı şekilde bulut bilişim, yerel kurulum, uç yapay zekâ ve uygulama programlama arayüzleri gibi altyapı bileşenleri de sadece teknik tercihler değildir; mahremiyet, erişim yetkisi, maliyet, süreklilik ve denetim kapasitesi üzerinde doğrudan etki doğurur.

Kamu kurumları bakımından veri ve altyapı konusu, aynı zamanda kurumsal hafızanın ve idari sorumluluğun korunmasıyla ilgilidir. Bir sistemin hangi veriye dayandığı, bu verinin hangi süreyle saklandığı, hangi birimce güncellendiği ve hangi güvenlik tedbirleriyle işlendiği açık değilse, yapay zekâ uygulamalarının şeffaf ve hesap

verebilir biçimde yürütülmesi güçleşir. Bu bölümdeki kavramlar, kamu yöneticilerinin teknik ayrıntı içinde kaybolmadan yapay zekâ altyapısının hangi sorular üzerinden değerlendirilmesi gerektiğini görebilmesi için bir çerçeve sunmaktadır.

Bu bölümdeki terim sayısı	19

TERİMLER

B1 - Veri Kümesi / *Dataset*

Tanım	Veri kümesi, belirli bir amaç doğrultusunda bir araya getirilmiş yapılandırılmış veya yapılandırılmamış veri bütünüdür. Yapay zekâ modelleri veri kümeleri üzerinden eğitilir, sınanır ve iyileştirilir.
Kamuda kullanım örneği	Bir ulaştırma kurumunun geçmiş trafik yoğunluğu, kaza zamanı ve yol durumu verilerini içeren birleşik kayıt havuzu, hizmet planlama modelleri için veri kümesi oluşturabilir.
Kurumsal dikkat notu	Veri kümesinin kaynağı, kapsamı ve güncelliği belgelenmeden güvenilir sonuç beklenmemelidir.
İlişkili terimler	Eğitim verisi, test verisi, veri kalitesi, veri yönetişimi

B2 - Eğitim Verisi / *Training Data*

Tanım	Eğitim verisi, modelin örüntü öğrenmesi için kullanılan ana veri setidir. Modelin hangi ilişkileri kuracağı büyük ölçüde bu verinin niteliği tarafından şekillendirilir.
Kamuda kullanım örneği	Bir kurum içi belge asistanı, geçmiş genelgeler, sık sorulan sorular ve standart yazışma örnekleriyle eğitildiğinde kurumsal terminolojiye daha uygun sonuçlar verebilir.
Kurumsal dikkat notu	Eğitim verisine yanlış, eski veya tek taraflı kayıtlar yüklenirse modelin davranışı da aynı yönde sorunlu olabilir.
İlişkili terimler	Test verisi, ince ayar, veri önyargısı, veri kalitesi

B3 - Test Verisi / *Test Data*

Tanım	Test verisi, modelin eğitim aşamasından ayrı tutulan ve performansının nesnel biçimde ölçülmesinde kullanılan veri setidir. Modelin gerçek koşullara ne kadar hazır olduğunu göstermeye yardımcı olur.
Kamuda kullanım örneği	Bir başvuru sınıflandırma sisteminin yeni kayıtlar üzerindeki doğruluğu, daha önce sisteme gösterilmemiş test verisi üzerinden kontrol edilebilir.
Kurumsal dikkat notu	Eğitim verisi ile test verisinin karışması performansı olduğundan yüksek gösterir ve yanıltıcı güven duygusu oluşturur.
İlişkili terimler	Eğitim verisi, performans göstergesi, güvence, pilot uygulama

B4 - Etiket / *Label*

Tanım	Etiket, bir veri örneğine atanan doğru sınıf, kategori veya sonuç bilgisidir. Denetimli öğrenme süreçlerinde modelin neyi öğrenmesi gerektiğini gösterir.
Kamuda kullanım örneği	Vatandaş dilekçelerinin uzmanlarca "imar", "ulaşım", "çevre", "sosyal yardım" gibi başlıklara ayrılması etiketleme sürecinin bir örneğidir.
Kurumsal dikkat notu	Farklı personelin farklı ölçütlerle etiketleme yapması veri tutarlılığını bozabilir; ortak kılavuz gerekir.
İlişkili terimler	Denetimli öğrenme, sınıflandırma, veri kalitesi, açıklanabilirlik

B5 - Öznitelik / *Feature*

Tanım	Öznitelik, bir veri örneğini tanımlayan ölçülebilir değişken veya niteliktir. Model, kararlarını bu öznitelikler arasındaki ilişkiler üzerinden kurar.
Kamuda kullanım örneği	Bir su tüketim analizi sisteminde mahalle, mevsim, nüfus yoğunluğu ve geçmiş tüketim miktarı ayrı ayrı öznitelik olarak kullanılabilir.
Kurumsal dikkat notu	Uygun olmayan öznitelik seçimi model performansını düşürebilir; hassas değişkenlerin kullanımı ise adillik riski doğurabilir.
İlişkili terimler	Veri kümesi, model, adillik, önyargı

B6 - Veri Yönetişimi / *Data Governance*

Tanım	Veri yönetişimi, verinin toplanması, saklanması, paylaşılması, işlenmesi ve silinmesiyle ilgili kurumsal kuralların, rollerin ve sorumlulukların bütünüdür. Kamu yapay zekâ uygulamalarında güvenilirliğin temelidir.
Kamuda kullanım örneği	Bir kurum, hangi verinin hangi birimce erişilebileceğini, hangi süreyle tutulacağını ve hangi amaç dışında kullanılamayacağını veri yönetişimi politikasıyla belirleyebilir.
Kurumsal dikkat notu	Veri yönetişimi zayıf olan kurumlarda teknik başarı elde edilse bile hukuki ve idari riskler büyür.
İlişkili terimler	Veri egemenliği, mahremiyet, uyum, denetim izi

B7 - Veri Kalitesi / *Data Quality*

Tanım	Veri kalitesi; verinin doğru, güncel, tam, tutarlı ve kullanım amacına uygun olması durumudur. Yapay zekâ sistemlerinin isabet oranı veri kalitesiyle doğrudan ilişkilidir.
Kamuda kullanım örneği	Adres kayıtları eksik veya mükerrer olan bir veri tabanı kullanıldığında, saha hizmet planlaması yapan bir kamu sistemi yanlış bölgelere kaynak ayırabilir.
Kurumsal dikkat notu	Düşük veri kalitesi, çoğu zaman model sorunu gibi görünür; oysa asıl problem veri hazırlık aşamasında olabilir.
İlişkili terimler	Eğitim verisi, etiket, veri temizleme, veri önyargısı

B8 - Veri Önyargısı / *Data Bias*

Tanım	Veri önyargısı, veri kümesinin belirli grupları, davranışları veya durumları sistematik biçimde eksik, fazla ya da çarpık temsil etmesi sonucu yapay zekâ sistemlerinde yanlılık üretmesidir.
Kamuda kullanım örneği	Geçmiş kayıtlarda belirli mahallelerden daha fazla şikâyet gelmiş olması, modelin bu mahalleleri otomatik olarak daha riskli görmesine yol açabilir.
Kurumsal dikkat notu	Veri önyargısı çoğu zaman teknik bir hata değil; geçmiş uygulamalardaki dengesizliklerin sayısal ortama taşınmış hâlidir.
İlişkili terimler	Adillik, önyargı, algoritmik etki değerlendirmesi, insan denetimi

B9 - Uygulama Programlama Arayüzü / *Application Programming Interface (API)*

Tanım	API, farklı yazılım sistemlerinin birbirleriyle standart biçimde veri alışverişi yapmasını sağlayan teknik arayüzdür. Yapay zekâ sistemleri çoğu zaman başka kurumsal uygulamalarla API üzerinden bütünleşir.
Kamuda kullanım örneği	Bir e-Devlet hizmeti, vatandaş başvurusuna ilişkin durum bilgisini farklı kurum kayıtlarından API yoluyla çekerek tek ekranda sunabilir.
Kurumsal dikkat notu	API tasarımı yapılırken erişim yetkisi, hız sınırı, kayıt tutma ve siber güvenlik önlemleri mutlaka tanımlanmalıdır.
İlişkili terimler	Model bağlam protokolü, denetim izi, siber güvenlik, orkestrasyon

B10 - Bulut Bilişim / *Cloud Computing*

Tanım	Bulut bilişim, işlem gücü, depolama ve yazılım hizmetlerinin uzak sunucu altyapıları üzerinden esnek biçimde sağlanmasıdır. Yapay zekâ uygulamaları için ölçeklenebilir kaynak erişimi sunar.
Kamuda kullanım örneği	Yoğun dönemlerde işlem kapasitesi ihtiyacı artan bir kamu kurumu, belirli analitik yükleri güvenli bulut altyapısında yürütebilir.
Kurumsal dikkat notu	Bulut tercihi yapılırken veri egemenliği, mevzuat uyumu, şifreleme ve hizmet sürekliliği birlikte değerlendirilmelidir.
İlişkili terimler	Yerel kurulum, veri egemenliği, siber güvenlik, çıkarım

B11 - Yerel Kurulum / *On-Premises Deployment*

Tanım	Yerel kurulum, yazılım ve yapay zekâ sistemlerinin kurumun kendi veri merkezi veya kontrol ettiği altyapı üzerinde çalıştırılmasıdır. Özellikle hassas verilerle çalışan kamu kurumlarında önem taşır.
Kamuda kullanım örneği	Savunma, güvenlik veya kritik ulusal altyapıyla ilişkili bir kurum, kurumsal dil modelini dış ortam yerine kendi kapalı veri merkezinde çalıştırmayı tercih edebilir.
Kurumsal dikkat notu	Yerel kurulum veri kontrolünü artırsa da bakım, güncelleme ve kapasite maliyetleri daha yüksek olabilir.
İlişkili terimler	Veri egemenliği, küçük dil modeli, bulut bilişim, siber güvenlik

B12 - Siber Güvenlik / *Cybersecurity*

Tanım	Siber güvenlik, bilgisayar tabanlı sistemlerin, ağların, verilerin ve hizmetlerin yetkisiz erişim, saldırı, manipülasyon ve kesintilere karşı korunmasını ifade eder. Yapay zekâ altyapıları bu koruma çerçevesinin kritik bir parçasıdır.
Kamuda kullanım örneği	Kurum içi yapay zekâ asistanına yalnızca yetkili personelin erişebilmesi, kayıtların şifreli tutulması ve sorgu hareketlerinin izlenmesi siber güvenliğin parçasıdır.
Kurumsal dikkat notu	Güvenlik yalnızca ağ savunması değildir; istem manipülasyonu, veri sızıntısı ve yetkisiz araç erişimi de bu kapsamda değerlendirilmelidir.
İlişkili terimler	Mahremiyet, veri egemenliği, denetim izi, model bağlam protokolü

B13 - Çıkarım / *Inference*

Tanım	Çıkarım, eğitilmiş bir modelin gerçek kullanım anında yeni bir girdiye yanıt, tahmin veya karar üretmesi sürecidir. Eğitim aşaması tamamlandıktan sonra sistemin günlük çalışma biçimini ifade eder.
Kamuda kullanım örneği	Vatandaşın sisteme yazdığı bir soruya kurum asistanının o anda yanıt üretmesi, modelin çıkarım sürecidir.
Kurumsal dikkat notu	Çıkarım aşamasında hız, maliyet ve güvenlik kadar hangi verilerin modele gösterildiği de önemlidir.
İlişkili terimler	Model, bağlam penceresi, küçük dil modeli, bulut bilişim

B14 - Uç Yapay Zekâ / *Edge AI*

Tanım	Uç yapay zekâ, verinin merkezi sunucuya gönderilmeden, verinin üretildiği cihaza veya ona yakın bir noktada işlenmesi yaklaşımıdır. Düşük gecikme, bağlantı bağımsızlığı ve mahremiyet avantajı sağlayabilir.
Kamuda kullanım örneği	Saha ekiplerinin kullandığı mobil cihazlarda görüntüden hızlı hasar tespiti yapılması, verinin tamamı merkeze aktarılmadan uç yapay zekâ ile gerçekleştirilebilir.
Kurumsal dikkat notu	Uç yapay zekâ mahremiyet avantajı sunsa da cihaz güvenliği ve model güncellemeleri düzenli yönetilmelidir.
İlişkili terimler	Yerel kurulum, bilgisayarlı görü, siber güvenlik, çıkarım

B15 - Yeşil Yapay Zekâ / *Green AI*

Tanım	Yeşil yapay zekâ, yapay zekâ sistemlerinin geliştirilmesi, eğitilmesi ve çalıştırılması sırasında enerji tüketimini, donanım yükünü ve çevresel etkiyi azaltmayı hedefleyen yaklaşımı ifade eder. Bu yaklaşım, yalnızca model başarısına değil; sürdürülebilirlik performansına da odaklanır.
Kamuda kullanım örneği	Bir kamu kurumu, aynı işi gören iki model arasında seçim yaparken sadece doğruluk oranını değil; işlem başına enerji tüketimini ve altyapı ihtiyacını da dikkate alarak daha sürdürülebilir çözümü tercih edebilir.
Kurumsal dikkat notu	Yeşil yapay zekâ, performanstan tamamen vazgeçmek anlamına gelmez; kurumsal ihtiyaç ile kaynak kullanımı arasında dengeli karar verilmesini gerektirir.
İlişkili terimler	Enerji verimliliği, karbon ayak izi, model verimliliği, bulut bilişim

B16 - Enerji Verimliliği / *Energy Efficiency*

Tanım	Enerji verimliliği, bir yapay zekâ sisteminin belirli bir görevi yerine getirirken mümkün olan en düşük enerji tüketimiyle çalışabilme kapasitesidir. Eğitim ve çıkarım aşamalarında kullanılan işlem gücü, donanım seçimi ve yazılım optimizasyonları bu verimliliği etkiler.
Kamuda kullanım örneği	Kurum içi belge özetleme hizmetinde aynı kaliteyi sunan daha hafif bir modelin tercih edilmesi, sunucu tüketimini azaltarak enerji verimliliği sağlayabilir.
Kurumsal dikkat notu	Enerji verimliliği yalnızca veri merkezinin toplam tüketimiyle değil; işlem başına harcanan kaynak ve kullanım yoğunluğu ile birlikte değerlendirilmelidir.
İlişkili terimler	Yeşil yapay zekâ, model verimliliği, çıkarım, uç yapay zekâ

B17 - Karbon Ayak İzi / *Carbon Footprint*

Tanım	Karbon ayak izi, bir yapay zekâ sisteminin eğitimi, çalıştırılması ve altyapı kullanımından kaynaklanan toplam sera gazı etkisini ifade eder. Hesaplama yoğunluğu, enerji kaynağı ve kullanım süresi bu etkiyi doğrudan belirler.
Kamuda kullanım örneği	Büyük ölçekli bir model eğitimi planlayan kamu kurumu, kullanılacak veri merkezi altyapısının enerji kaynağını ve işlem süresini değerlendirerek projenin karbon ayak izini önceden hesaplayabilir.
Kurumsal dikkat notu	Karbon ayak izi değerlendirmesi yapılmadığında, teknik olarak başarılı görünen projeler kurumsal sürdürülebilirlik hedefleriyle çelişebilir.
İlişkili terimler	Yeşil yapay zekâ, enerji verimliliği, bulut bilişim, model verimliliği

B18 - Model Verimliliği / *Model Efficiency*

Tanım	Model verimliliği, bir modelin doğruluk, hız, bellek kullanımı ve işlem maliyeti arasında dengeli performans sunabilme düzeyidir. Amaç, gereksiz kaynak tüketmeden kullanım amacına uygun sonuç üretmektir.
Kamuda kullanım örneği	Bir çağrı merkezi asistanında çok büyük bir model yerine daha küçük ama yeterli doğruluk sağlayan bir modelin seçilmesi, model verimliliği açısından daha uygun olabilir.
Kurumsal dikkat notu	En büyük model her zaman en uygun model değildir; kullanım senaryosu, gecikme süresi ve bütçe birlikte değerlendirilmelidir.
İlişkili terimler	Enerji verimliliği, model sıkıştırma, küçük dil modeli, çıkarım

B19 - Model Sıkıştırma / *Model Compression*

Tanım	Model sıkıştırma, bir yapay zekâ modelinin boyutunu ve hesaplama ihtiyacını azaltırken kabul edilebilir performans düzeyini korumaya yönelik tekniklerin genel adıdır. Budama, nicemleme ve bilgi damıtma gibi yöntemleri kapsayabilir.
Kamuda kullanım örneği	Saha personelinin taşınabilir cihazlarında çalışan görüntü analiz modelinin daha hızlı ve düşük donanım gereksinimiyle çalışması için model sıkıştırma uygulanabilir.
Kurumsal dikkat notu	Sıkıştırma işlemi sonrasında doğruluk, adillik ve güvenlik performansı yeniden test edilmelidir; kaynak tasarrufu kalite kaybını gizlememelidir.
İlişkili terimler	Model verimliliği, uç yapay zekâ, küçük dil modeli, enerji verimliliği

BÖLÜM C

ÜRETKEN YAPAY ZEKÂ VE MODEL AİLELERİ

Üretken yapay zekâ, son yıllarda kamu kurumları açısından en görünür teknoloji başlıklarından biri hâline gelmiştir. Metin yazabilen, özet çıkarabilen, görsel oluşturabilen, belge düzenleyebilen ya da farklı türdeki içerikleri birlikte yorumlayabilen sistemler; hem verimlilik beklentilerini artırmış hem de yeni risk alanlarını görünür kılmıştır. Bu nedenle üretken yapay zekâ kavramlarının yalnızca popüler kullanımıyla değil, teknik ve kurumsal karşılıklarıyla anlaşılması önem taşır.

Bu bölümde büyük dil modeli, küçük dil modeli, istem tasarımı, ince ayar, halüsinasyon, çok modlu model, muhakeme modeli ve geri getirmeli artırılmış üretim gibi kavramlar bir bütün içinde ele alınmaktadır. Amaç, kamu görevlilerinin yalnızca hangi aracın ne yaptığını değil; bu araçların hangi veri ve bağlamla çalıştığını, hangi durumlarda güvenilir sonuç ürettiğini ve hangi sınırlılıklarla kullanılmaları gerektiğini anlayabilmesidir. Özellikle metin odaklı kamu süreçlerinde, üretken sistemlerin cevap üretme kabiliyeti kadar hata yapma biçimi de önemlidir.

Üretken yapay zekâ araçları kamuda taslak hazırlama, belge sınıflandırma, özetleme, soru yanıtlama ve hizmet kanallarını güçlendirme gibi alanlarda ciddi imkanlar sunabilir. Bununla birlikte bu araçlar, kurumsal doğrulama ve insan denetimi olmaksızın doğrudan karar verici olarak konumlandırıldığında mevzuat, güvenlik ve kamu

güveni bakımından sorunlar doğurabilir. Bölüm boyunca verilen terimler, üretken yapay zekâyı heyecan uyandıran bir yenilik alanı olarak değil; kontrollü, belgelendirilebilir ve amaca uygun kullanılacak bir kamu aracı olarak değerlendirmeyi hedeflemektedir.

Bu bölümdeki terim sayısı	19

TERİMLER

C1 - Üretken Yapay Zekâ / *Generative AI*

Tanım	Üretken yapay zekâ, mevcut örüntülerden öğrenerek yeni metin, görsel, ses, video veya kod üretebilen sistem sınıfıdır. Bu sistemler büyük veri kümelerinden öğrenerek daha önce doğrudan yazılmamış ya da oluşturulmamış içerikler üretebilir.
Kamuda kullanım örneği	Bir kamu kurumu, uzun toplantı tutanaklarını kısa yönetici özetlerine dönüştürmek veya sık sorulan sorular için taslak yanıt üretmek amacıyla üretken yapay zekâdan yararlanabilir.
Kurumsal dikkat notu	Üretilen içerik doğrudan yayımlanmamalı; doğruluk, hukuk uygunluğu ve kurumsal üslup bakımından gözden geçirilmelidir.
İlişkili terimler	Büyük dil modeli, istem, halüsinasyon, insan denetimi

C2 - Büyük Dil Modeli / *Large Language Model (LLM)*

Tanım	Büyük dil modeli, çok büyük hacimli metinler üzerinde eğitilmiş ve doğal dili anlama, üretme, özetleme, dönüştürme ve soru yanıtlama gibi görevlerde yüksek esneklik sağlayan model sınıfıdır. Günümüzde birçok kurumsal yapay zekâ uygulamasının merkezinde bu modeller bulunmaktadır.
Kamuda kullanım örneği	Kurum içi mevzuat arama asistanı, geniş kapsamlı belge havuzu üzerinde çalışan büyük dil modeli sayesinde personelin hızlı bilgiye erişmesini sağlayabilir.
Kurumsal dikkat notu	Büyük modeller yüksek yetenek sunsa da maliyet, gizlilik ve yanlış üretim riski nedeniyle denetimli kullanım gerektirir.
İlişkili terimler	Küçük dil modeli, temel model, bağlam penceresi, geri getirmeli artırılmış üretim

C3 - İstem / *Prompt*

Tanım	İstem, üretken yapay zekâ sistemine verilen komut, soru, talimat veya bağlamsal girdidir. Modelin üreteceği çıktının niteliği, çoğu zaman istemin açıklığına ve yapılandırılmasına bağlıdır.
Kamuda kullanım örneği	Bir uzman, "aşağıdaki metni resmi rapor diliyle üç paragrafta özetle" şeklinde açık bir istem vererek daha kullanılabilir sonuç alabilir.
Kurumsal dikkat notu	Belirsiz istemler hatalı, eksik veya aşırı genel sonuçlara yol açabilir; kurumsal kullanım için standart istem şablonları geliştirilmelidir.
İlişkili terimler	İstem tasarımı, bağlam penceresi, büyük dil modeli, halüsinasyon

C4 - İstem Mühendisliği / *Prompt Design / Prompt Engineering*

Tanım	İstem mühendisliği, istenen çıktı niteliğine ulaşmak için istemlerin sistematik biçimde hazırlanması ve iyileştirilmesidir. Görev amacı, bağlam, rol tanımı ve çıktı biçimi gibi unsurlar bu sürecin parçasıdır.
Kamuda kullanım örneği	Bir kurum, basın bülteni taslağı, toplantı özeti ve politika notu üretimi için ayrı istem şablonları geliştirerek sonuç tutarlılığını artırabilir.
Kurumsal dikkat notu	İyi istem mühendisliği verimlilik sağlar; ancak yanlış istem, modelin hassas bilgi istemesine veya uygun olmayan içerik üretmesine neden olabilir.
İlişkili terimler	İstem, halüsinasyon, insan denetimi, kurumsal üslup

C5 - Bağlam Penceresi / *Context Window*

Tanım	Bağlam penceresi, bir modelin tek işlemde dikkate alabildiği toplam bilgi miktarını ifade eder. Bu kapsam, kullanıcının sorusunu, ek belgeleri, önceki mesajları ve sistem talimatlarını içerebilir.
Kamuda kullanım örneği	Çok sayıda mevzuat metni aynı anda modele yüklendiğinde, bağlam sınırı aşılıyorsa bazı bölümler gözden kaçabilir; bu nedenle belge parçalama ve önceliklendirme yapılmalıdır.
Kurumsal dikkat notu	Uzun dosyalarda bağlam sınırı görünmez bir risk oluşturur; çıktı tam görünse de kritik bir madde göz ardı edilmiş olabilir.
İlişkili terimler	Büyük dil modeli, geri getirmeli artırılmış üretim, çıkarım, istem

C6 - İnce Ayar / *Fine-Tuning*

Tanım	İnce ayar, önceden eğitilmiş bir modelin belirli kurum ihtiyaçları, terminoloji seti veya görev yapısı doğrultusunda ek veriyle uyarlanmasıdır. Bu yöntem, genel amaçlı modelin kuruma daha uygun davranmasını sağlayabilir.
Kamuda kullanım örneği	Bir kurum, kendi resmi yazışma diline uyumlu özet üretimi için modeli geçmiş kurumsal metinlerle ince ayardan geçirebilir.
Kurumsal dikkat notu	İnce ayar yapılırken kullanılan verilerin doğruluğu ve izin durumu dikkatle değerlendirilmelidir.
İlişkili terimler	Eğitim verisi, küçük dil modeli, temel model, veri yönetişimi

C7 - Geri Getirmeli Artırılmış Üretim / *Retrieval-Augmented Generation (RAG)*

Tanım	Geri getirmeli artırılmış üretim, model çıktısının dış bilgi kaynaklarından çekilen güncel veya kurum içi verilerle desteklenmesi yaklaşımıdır. Bu yöntem, modelin yalnızca eğitim dönemindeki bilgiyle sınırlı kalmasını önlemeye yardımcı olur.
Kamuda kullanım örneği	Bir bakanlık asistanı, yanıt üretmeden önce güncel genelgeleri ve resmî sıkça sorulan sorular havuzunu tarayarak daha doğru açıklama sunabilir.
Kurumsal dikkat notu	RAG yapısı doğruluğu artırabilir; ancak getirilen kaynağın da güvenilir ve güncel olması gerekir.
İlişkili terimler	Bağlam penceresi, büyük dil modeli, veri yönetişimi, denetim izi

C8 - Halüsinasyon / *Hallucination*

Tanım	Halüsinasyon, modelin gerçekte dayanağı olmayan, yanlış veya uydurma içerik üretmesi durumudur. Özellikle üretken yapay zekâ kullanımında en çok dikkat edilmesi gereken risklerden biridir.
Kamuda kullanım örneği	Bir kurum asistanı, yürürlükte olmayan bir genelge numarası veya mevcut olmayan bir mevzuat maddesi üretirse bu durum halüsinasyon örneğidir.
Kurumsal dikkat notu	Resmî yazışma, mevzuat yorumu ve kamuoyu açıklamalarında halüsinasyon riski mutlaka insan kontrolüyle yönetilmelidir.
İlişkili terimler	İstem, geri getirmeli artırılmış üretim, insan denetimi, güvence

C9 - Çok Modlu Sistem / *Multimodal System*

Tanım	Çok modlu sistem, metin, görsel, ses, tablo ve video gibi farklı veri türlerini birlikte işleyebilen yapay zekâ yapısını ifade eder. Kamu uygulamalarında belge, görüntü ve çağrı kaydı gibi farklı kaynakların birlikte değerlendirilmesine imkân tanır.
Kamuda kullanım örneği	Bir afet koordinasyon merkezinde metin raporları, saha fotoğrafları ve sesli ihbar kayıtları birlikte analiz edilerek durum değerlendirmesi yapılabilir.
Kurumsal dikkat notu	Farklı veri türlerini bir araya getiren sistemlerde mahremiyet ve veri sınıflandırması daha dikkatli yönetilmelidir.
İlişkili terimler	Çok modlu model, bilgisayarlı görü, doğal dil işleme, uç yapay zekâ

C10 - Sentetik Veri / *Synthetic Data*

Tanım	Sentetik veri, gerçek veriyi doğrudan kullanmadan, istatistiksel özellikleri benzer olacak biçimde yapay olarak üretilen veri kümesidir. Gizlilik riski yüksek alanlarda test ve geliştirme amacıyla yararlı olabilir.
Kamuda kullanım örneği	Gerçek hasta verisi yerine anonimleştirilmiş örüntülere dayalı sentetik veri kullanılarak bir sağlık yönlendirme uygulaması test edilebilir.
Kurumsal dikkat notu	Sentetik veri kullanımı mahremiyet avantajı sunsa da gerçek dünyayı yeterince temsil edip etmediği ayrıca sınanmalıdır.
İlişkili terimler	Veri kümesi, mahremiyet, test verisi, güvence

C11 - Küçük Dil Modeli / *Small Language Model (SLM)*

Tanım	Küçük dil modeli, büyük dil modellerine kıyasla daha sınırlı parametre yapısına sahip; ancak daha hızlı, daha düşük maliyetli ve çoğu zaman alan odaklı çalışmaya uygun model sınıfıdır. Özellikle kuruma özgü senaryolarda verimli çözümler sunabilir.
Kamuda kullanım örneği	Sadece kurumsal mevzuat ve iç prosedürlere yanıt veren bir iç kullanım asistanı, küçük dil modeli ile kurum veri merkezinde daha kontrollü biçimde çalıştırılabilir.
Kurumsal dikkat notu	Küçük modeller her görev için yeterli olmayabilir; ancak veri egemenliği ve maliyet dengesi bakımından kamu için güçlü bir seçenektir.
İlişkili terimler	Büyük dil modeli, yerel kurulum, ince ayar, veri egemenliği

C12 - Temel Model / *Foundation Model*

Tanım	Temel model, çok geniş veri kaynakları üzerinde önceden eğitilmiş ve farklı görevler için uyarlanabilen genel amaçlı model sınıfıdır. Büyük dil modelleri ve çok modlu modeller çoğu zaman temel model yaklaşımının örnekleridir.
Kamuda kullanım örneği	Bir kamu kurumu, genel amaçlı bir temel modeli alıp kendi belge havuzu ve süreçleriyle uyarlayarak özel kullanım senaryoları oluşturabilir.
Kurumsal dikkat notu	Temel model seçimi, kurumsal ihtiyaç, lisans koşulları, güvenlik ve maliyet çerçevesinde değerlendirilmelidir.
İlişkili terimler	Büyük dil modeli, ince ayar, sınır model, küçük dil modeli

C13 - Muhakeme Modeli / *Reasoning Model*

Tanım	Muhakeme modeli, çok adımlı düşünme, ara değerlendirme yapma ve karmaşık problem çözme görevlerinde güçlendirilmiş model yaklaşımını ifade eder. Özellikle zincirleme değerlendirme gereken görevlerde öne çıkar.
Kamuda kullanım örneği	Bir mevzuat analizi sisteminde farklı düzenlemeler arasındaki uyum ilişkisini değerlendirmek ve olası çelişkileri işaretlemek için muhakeme modeli kullanılabilir.
Kurumsal dikkat notu	Muhakeme yeteneği yüksek modeller ikna edici ama hatalı sonuçlar da üretebilir; bu nedenle uzman doğrulaması zorunludur.
İlişkili terimler	Sınır model, büyük dil modeli, açıklanabilirlik, insan denetimi

C14 - Sınır Model / *Frontier Model*

Tanım	Sınır model, belirli bir dönemde genel amaçlı yapay zekâ yeteneklerinin en ileri seviyesini temsil eden uç nokta model sınıfıdır. Bu modeller çoklu görev başarısı, yüksek muhakeme kapasitesi ve geniş kullanım alanlarıyla öne çıkar.
Kamuda kullanım örneği	Çok farklı veri türlerini birleştiren, gelişmiş analiz yapan ve çok adımlı işlem gerektiren ulusal ölçekte dijital hizmet uygulamalarında sınır modeller değerlendirme konusu olabilir.
Kurumsal dikkat notu	Sınır modeller yüksek kapasite sunar; ancak yönetişim, maliyet, güvenlik ve veri kontrolü bakımından daha sıkı değerlendirme gerektirir.
İlişkili terimler	Temel model, muhakeme modeli, çok modlu model, risk sınıflandırması

C15 - Çok Modlu Model / *Multimodal Model*

Tanım	Çok modlu model, metin, görsel, ses veya video gibi farklı girdi türlerini doğrudan birlikte işleyebilen model sınıfıdır. Çok modlu sistemler çoğu zaman bu tür modeller üzerinde inşa edilir.
Kamuda kullanım örneği	Bir kurum, dilekçe metnini, ekindeki belge fotoğrafını ve sesli açıklamayı birlikte değerlendirerek daha bütüncül ön inceleme yapabilir.
Kurumsal dikkat notu	Çok modlu kullanım, veri sınıflandırması ve erişim yetkilerinin ayrı ayrı değil; birleşik bir bütün olarak ele alınmasını gerektirir.
İlişkili terimler	Çok modlu sistem, bilgisayarlı görü, doğal dil işleme, mahremiyet

C16 - Token / *Token*

Tanım	Token, bir üretken modelin metni işlerken kullandığı temel parçalardan her biridir. Bir kelimenin tamamı, bir kelime parçası, noktalama işareti veya kısa bir sembol dizisi token olarak temsil edilebilir; model girdileri ve çıktıları bu birimler üzerinden hesaplanır.
Kamuda kullanım örneği	Bir kamu uzmanı uzun bir mevzuat metnini modele yüklediğinde, sistem metni karakter karakter değil token birimleri üzerinden işler; bu nedenle belge uzunluğu bağlam sınırı açısından token sayısıyla değerlendirilir.
Kurumsal dikkat notu	Token sayısı arttıkça işlem maliyeti, gecikme süresi ve bağlam kullanımı da artabilir; uzun belgelerde parçalara ayırma stratejisi gerekebilir.
İlişkili terimler	Bağlam penceresi, büyük dil modeli, çıkarım, maksimum çıktı uzunluğu

C17 - Sıcaklık Parametresi / *Temperature*

Tanım	Sıcaklık parametresi, üretken modelin bir sonraki sözcük ya da token seçerken ne kadar çeşitli ve yaratıcı davranacağını etkileyen ayardır. Düşük sıcaklık daha öngörülebilir ve tutarlı çıktılar üretmeye eğilimliyken, yüksek sıcaklık daha çeşitli ancak daha değişken sonuçlar doğurabilir.
Kamuda kullanım örneği	Resmî yazışma taslağı hazırlayan bir kamu asistanında sıcaklık değerinin düşük tutulması, daha tutarlı ve kurumsal üsluba yakın çıktı alınmasına yardımcı olabilir.
Kurumsal dikkat notu	Sıcaklık parametresi tek başına kalite garantisi sağlamaz; görev türüne göre diğer üretim ayarları ve insan kontrolüyle birlikte değerlendirilmelidir.
İlişkili terimler	Olasılık eşiği, istem, büyük dil modeli, halüsinasyon

C18 - Olasılık Eşiği / *Top-p*

Tanım	Olasılık eşiği veya Top-p, modelin bir sonraki token seçimi sırasında yalnızca toplam olasılığı belirli bir eşik değere ulaşan en güçlü adaylar arasından seçim yapmasını sağlayan ayardır. Böylece model, çok düşük olasılıklı seçenekleri dışarıda bırakarak kontrollü çeşitlilik üretebilir.
Kamuda kullanım örneği	Vatandaş sorularına verilen yanıtların çok dağılmaması istenen bir kurum asistanında Top-p değeri dikkatle ayarlanarak hem akıcılık hem de yanıt tutarlılığı dengelenebilir.
Kurumsal dikkat notu	Top-p ve sıcaklık ayarları birlikte ele alınmalıdır; uygunsuz değer kombinasyonları aşırı tekdüze ya da aşırı oynak sonuçlara yol açabilir.
İlişkili terimler	Sıcaklık parametresi, token, istem mühendisliği, halüsinasyon

C19 - Maksimum Çıktı Uzunluğu / *Maximum Output Length*

Tanım	Maksimum çıktı uzunluğu, modelin tek bir işlemde üretebileceği en yüksek çıktı miktarını belirleyen sınırdır. Bu sınır çoğu zaman token cinsinden tanımlanır ve yanıtın ne kadar ayrıntılı olabileceğini doğrudan etkiler.
Kamuda kullanım örneği	Bir kamu kurumu, kısa yönetici özeti almak istediğinde düşük; ayrıntılı değerlendirme notu istediğinde daha yüksek maksimum çıktı uzunluğu ayarı kullanarak üretim davranışını yönlendirebilir.
Kurumsal dikkat notu	Çok düşük sınırlar eksik yanıt üretimine, çok yüksek sınırlar ise maliyet artışına ve gereksiz ayrıntıya yol açabilir; görev amacına uygun ayar yapılmalıdır.
İlişkili terimler	Token, bağlam penceresi, sıcaklık parametresi, çıkarım

BÖLÜM D

ETİK, GÜVEN VE YÖNETİŞİM

Kamu kurumlarında yapay zekâ kullanımı yalnızca teknik doğruluk meselesi değildir; aynı zamanda hak temelli yaklaşım, kurumsal meşruiyet ve kamu güveni meselesidir. Bir sistemin hızlı, düşük maliyetli ya da yüksek doğrulukta çalışması tek başına yeterli kabul edilemez. Vatandaşları etkileyen süreçlerde açıklanabilirlik, adillik, hesap verebilirlik, insan denetimi ve risk yönetimi birlikte düşünülmedikçe teknolojik kapasite kamu değeri üretmek yerine yeni sorun alanları yaratabilir.

Bu bölümde güvenilir yapay zekâ çerçevesini oluşturan temel yönetişim kavramları bir araya getirilmektedir. Şeffaflık, açıklanabilirlik, insan denetimi, algoritmik etki değerlendirmesi, uyum, mahremiyet ve veri egemenliği gibi terimler; yapay zekâ sistemlerinin yalnızca nasıl geliştirileceğini değil, hangi yönetsel ilkeler ışığında işletileceğini de tanımlar. Özellikle kamu kurumlarında kullanılan sistemlerin karar süreçlerine etkisi arttıkça, teknik ekiplerle hukukçuların, denetçilerin ve politika geliştiricilerin aynı kavramlar etrafında konuşabilmesi hayati hâle gelmektedir.

Etik ve yönetişim başlıkları çoğu zaman soyut ilkeler gibi görünse de aslında günlük uygulamaya doğrudan yansır. Vatandaşın itiraz hakkı, modelin hangi veriyle eğitildiğinin kaydı, riskli işlem alanlarında insan onayının zorunlu tutulması ya da sistem performansının düzenli olarak yeniden değerlendirilmesi bu ilkelerin pra-

tik karşılıklarıdır. Bu bölüm, kamu kurumlarında sorumlu yapay zekâ yaklaşımının yalnızca iyi niyet beyanı değil; ölçülebilir, izlenebilir ve kurumsallaştırılabilir bir yönetim pratiği olduğunu vurgulamaktadır.

Bu bölümdeki terim sayısı	13

TERİMLER

D1 - Güvenilir Yapay Zekâ / *Trustworthy AI*

Tanım	Güvenilir yapay zekâ; güvenli, adil, açıklanabilir, mahremiyeti gözeten, denetlenebilir ve kamu yararına uygun biçimde tasarlanmış yapay zekâ anlayışıdır. Kamu kurumları açısından yalnızca çalışan değil, aynı zamanda güven veren sistemler esastır.
Kamuda kullanım örneği	Vatandaş başvurularını önceliklendiren bir sistem devreye alınmadan önce doğruluk, adillik, açıklanabilirlik ve insan müdahalesi ölçütleri üzerinden ayrı ayrı değerlendirilmesi güvenilir yapay zekâ yaklaşımıdır.
Kurumsal dikkat notu	Güvenilirlik sonradan eklenen bir unsur değil; tasarımın en başında kurulması gereken bir ilkedir.
İlişkili terimler	Adillik, açıklanabilirlik, insan denetimi, güvence

D2 - Hesap Verebilirlik / *Accountability*

Tanım	Hesap verebilirlik, yapay zekâ sisteminin tasarımı, işletimi ve sonuçlarından kimin sorumlu olduğunun açık biçimde belirlenmesidir. Kamu yönetiminde sorumluluk hiçbir zaman tamamen sisteme devredilemez.
Kamuda kullanım örneği	Bir kurumda kullanılan öneri sistemi yanlış yönlendirme yaptığında, teknik ekip, iş sahibi birim ve karar verici arasındaki sorumluluk zincirinin önceden tanımlanmış olması gerekir.
Kurumsal dikkat notu	Bir yapay zekâ sisteminin ürettiği sonucun tek başına gerekçe olarak gösterilmesi, kamu yönetimi açısından yeterli kabul edilemez; kararın sorumluluğu ve denetim çerçevesi açık biçimde tanımlanmalıdır.
İlişkili terimler	Denetim izi, insan denetimi, şeffaflık, uyum

D3 - Şeffaflık / *Transparency*

Tanım	Şeffaflık, bir yapay zekâ sisteminin ne amaçla kullanıldığının, hangi verilerden yararlandığının ve hangi sınırlar içinde çalıştığının anlaşılır biçimde ortaya konmasıdır. Kamu kurumlarında bu ilke kurumsal güveni artırır.
Kamuda kullanım örneği	Bir dijital kamu hizmetinde vatandaşın karşısına çıkan yönlendirme sisteminin otomatik analiz içerdiğinin, bilgilendirme metniyle açıkça belirtilmesi şeffaflık örneğidir.
Kurumsal dikkat notu	Şeffaflık, tüm teknik ayrıntıları ifşa etmek anlamına gelmez; anlaşılır düzeyde bilgilendirme sunmak anlamına gelir.
İlişkili terimler	Açıklanabilirlik, hesap verebilirlik, denetim izi, algoritmik etki değerlendirmesi

D4 - Açıklanabilirlik / *Explainability*

Tanım	Açıklanabilirlik, bir yapay zekâ sisteminin neden belirli bir sonuç ürettiğinin insan tarafından anlaşılabilir şekilde ortaya konabilmesidir. Özellikle vatandaşları etkileyen değerlendirme süreçlerinde önem taşır.
Kamuda kullanım örneği	Bir başvuru önceliklendirme sisteminin hangi temel ölçütler nedeniyle dosyayı yüksek önceliğe aldığını açıklayabilmesi, kamu denetimi açısından önemlidir.
Kurumsal dikkat notu	Açıklanamayan sonuçlar, teknik olarak isabetli görünse bile kamu nezdinde meşruiyet sorunu doğurabilir.
İlişkili terimler	Yorumlanabilirlik, şeffaflık, insan denetimi, güvenilir yapay zekâ

D5 - Yorumlanabilirlik / *Interpretability*

Tanım	Yorumlanabilirlik, modelin iç yapısının veya karar mekanizmasının teknik olarak çözümlenebilir ve anlaşılabilir olmasıdır. Açıklanabilirlik daha geniş kullanıcı anlayışına odaklanırken yorumlanabilirlik daha teknik bir düzeyi ifade eder.
Kamuda kullanım örneği	Bir risk puanlama modelinde hangi değişkenin kararı hangi oranda etkilediğini analiz edebilen teknik ekipler yorumlanabilirlikten yararlanır.
Kurumsal dikkat notu	Yorumlanabilirlik düzeyi düşük olan sistemlerde ek güvence, test ve uzman incelemesi gerekir.
İlişkili terimler	Açıklanabilirlik, model, güvence, performans göstergesi

D6 - Adillik / *Fairness*

Tanım	Adillik, yapay zekâ sistemlerinin bireyler veya gruplar arasında haksız, ayrımcı ya da sistematik olarak olumsuz sonuçlar üretmemesini ifade eder. Özellikle kamu hizmetlerinde dijital ortamda eşit hizmet ilkesinin korunması açısından kritik önemdedir.
Kamuda kullanım örneği	Bir sosyal destek yönlendirme aracının farklı bölgelerden gelen başvurulara benzer koşullarda benzer değerlendirme yapıp yapmadığının test edilmesi adillik incelemesidir.
Kurumsal dikkat notu	Adillik yalnızca teknik eşitlik değildir; toplumsal bağlam, erişim farkları ve hizmet etkisi de dikkate alınmalıdır.
İlişkili terimler	Önyargı, veri önyargısı, algoritmik etki değerlendirmesi, insan denetimi

D7 - Önyargı / *Bias*

Tanım	Önyargı, veri, model veya süreç kaynaklı olarak belirli sonuçların sistematik biçimde bir yöne sapmasıdır. Yapay zekâ bağlamında bu sapma, özellikle kamu hizmetlerinde adaletsizlik yaratma riski taşır.
Kamuda kullanım örneği	Geçmiş kayıtları esas alan bir sistem belirli bölge başvurularını otomatik olarak daha düşük öncelikli görmeye başlarsa bu durum önyargı göstergesi olabilir.
Kurumsal dikkat notu	Önyargı çoğu zaman açık bir hata mesajı üretmez; performans iyi görünürken dahi eşitsizlik oluşabilir.
İlişkili terimler	Adillik, veri önyargısı, insan denetimi, güvenilir yapay zekâ

D8 - İnsan Denetimi / *Human Oversight*

Tanım	İnsan denetimi, yapay zekâ destekli süreçlerde nihai gözetim, müdahale, düzeltme ve durdurma yetkisinin insanda kalmasını ifade eder. Kamu alanında bu ilke temel güvencelerden biridir.
Kamuda kullanım örneği	Bir belge özetleme sistemi taslak öneri sunsa da nihai metnin yayımlanması öncesinde ilgili uzman veya yönetici onayı alınması insan denetimi uygulamasıdır.
Kurumsal dikkat notu	İnsan denetimi yalnızca sembolik imza olmamalı; gerçekten müdahale edilebilir bir süreç tasarlanmalıdır.
İlişkili terimler	Hesap verebilirlik, halüsinasyon, ajan yönetişimi, karar destek sistemi

D9 - Güvence / *Assurance*

Tanım	Güvence, bir yapay zekâ sisteminin belirlenen amaçlara, kurumsal standartlara ve güvenlik beklentilerine uygun biçimde çalıştığını göstermek için yürütülen test, doğrulama ve kanıtlama süreçlerini ifade eder.
Kamuda kullanım örneği	Yeni devreye alınacak bir kurum asistanının hata oranı, hassas bilgi sızdırmama kapasitesi ve mevzuat doğruluğu ayrı senaryolarla sınanabilir.
Kurumsal dikkat notu	Güvence süreci tek seferlik bir uygulama olarak ele alınmamalı; sistemde yapılan güncellemeler doğrultusunda düzenli olarak yenilenmelidir.
İlişkili terimler	Test verisi, performans göstergesi, siber güvenlik, pilot uygulama

D10 - Algoritmik Etki Değerlendirmesi / *Algorithmic Impact Assessment (AIA)*

Tanım	Algoritmik etki değerlendirmesi, bir yapay zekâ sisteminin toplumsal, hukuki, yönetsel ve ekonomik etkilerini devreye almadan önce sistematik biçimde inceleme sürecidir. Özellikle yüksek etkili kamu uygulamalarında önem kazanır.
Kamuda kullanım örneği	Bir kamu kurumunun başvuru önceliklendirme sistemi, yaygın kullanıma açılmadan önce vatandaş hakları, eşit erişim, itiraz mekanizması ve insan denetimi açısından etki değerlendirmesine tabi tutulabilir.
Kurumsal dikkat notu	Etki değerlendirmesi yalnızca teknik ekip değil; hukuk, iş sahibi birim ve yönetişim paydaşlarıyla birlikte yürütülmelidir.
İlişkili terimler	Risk sınıflandırması, adillik, şeffaflık, hesap verebilirlik

D11 - Mahremiyet / *Privacy*

Tanım	Mahremiyet, bireylere ait bilgilerin toplanması, işlenmesi ve paylaşılması üzerinde korunmuş hak ve denetim çerçevesini ifade eder. Kamu yapay zekâ uygulamalarında kişisel veri işleme süreçleri mahremiyet bakımından hassas değerlendirme gerektirir.
Kamuda kullanım örneği	Vatandaş başvurularını özetleyen bir sistemde yalnızca gerekli verilerin işlenmesi ve yetkisiz erişimin engellenmesi mahremiyet yaklaşımının parçasıdır.
Kurumsal dikkat notu	Faydalı görünen her veri işleme faaliyeti meşru değildir; veri minimizasyonu ilkesi gözetilmelidir.
İlişkili terimler	Veri egemenliği, siber güvenlik, veri yönetişimi, yerel kurulum

D12 - Veri Egemenliği / *Data Sovereignty*

Tanım	Veri egemenliği, verinin hangi hukuk düzenine, hangi kurumsal yetkiye ve hangi teknik kontrol ortamına tabi olduğunun açık biçimde tanımlanmasıdır. Kamu kurumları için stratejik ve hukuki önem taşır.
Kamuda kullanım örneği	Bir kamu kurumu, hassas belge verilerini yalnızca ülke içindeki kontrollü altyapılarda işleyerek veri egemenliği ilkesini güçlendirebilir.
Kurumsal dikkat notu	Veri egemenliği yalnızca fiziksel konum meselesi değildir; erişim, yönetim ve yetkilendirme boyutları da içerir.
İlişkili terimler	Yerel kurulum, bulut bilişim, mahremiyet, veri yönetişimi

D13 - Ajan Yönetişimi / *Agent Governance*

Tanım	Ajan yönetişimi, özerk veya yarı özerk yapay zekâ ajanlarının hangi yetki sınırları içinde çalışacağını, hangi işlemleri kendi başına yapabileceğini ve hangi aşamalarda insan onayı gerekeceğini belirleyen yönetişim çerçevesidir. Özellikle ajan tabanlı sistemlerin yaygınlaştığı yeni dönemde kritik hâle gelmiştir.
Kamuda kullanım örneği	Kurum içi bir yapay zekâ ajanının belge taslağı hazırlamasına izin verilirken, dış kurumlara gönderim yapmasının yalnızca insan onayıyla mümkün olması ajan yönetişimi yaklaşımıdır.
Kurumsal dikkat notu	Ajan yetkileri açık biçimde tanımlanmazsa düşük riskli yardımcı araçlar zamanla kontrolsüz işlem başlatan yapılara dönüşebilir.
İlişkili terimler	İnsan denetimi, yapay zekâ ajanı, araç kullanımı, denetim izi

BÖLÜM E

HUKUK, UYGULAMA VE KURUMSAL KULLANIM

Yapay zekâ teknolojilerinin kamu kurumlarında kalıcı değer üretmesi, teknik kapasitenin hukuk, idari süreçler ve hizmet tasarımıyla uyumlu biçimde bir araya getirilmesine bağlıdır. Kurumsal kullanımın güvenilir bir zemine oturabilmesi, karar yetkisi, itiraz mekanizması, kayıt düzeni ve mevzuatla ilişkinin açık biçimde belirlenmesini gerektirir. Bu nedenle kamu uygulaması perspektifi, yapay zekâyı yalnızca teknoloji yatırımı olarak değil; kurumsal süreçlerin yeniden tasarlanmasını gerektiren bir yönetişim alanı olarak ele alır.

Bu bölümde karar destek sistemlerinden pilot uygulamaya, dijital kamu hizmetlerinden idari sorumluluğa kadar geniş bir kavramsal çerçeve sunulmaktadır. Amaç, yapay zekâ projelerinin nasıl başlatılacağı, hangi ölçekte test edileceği, hangi aşamada yaygınlaştırılacağı ve hangi hukuki-idari sınırlar içinde işletileceği konusunda ortak bir referans oluşturmaktır. Kamu hizmetlerinde kullanılan sistemlerin etkisi çoğu zaman doğrudan vatandaşa yansıdığı için, teknik tasarım ile hizmet tasarımı arasındaki bağ bu bölümün merkezinde yer almaktadır.

Kamu uygulaması bakımından asıl mesele, yapay zekânın insan emeğini bütünüyle ikame etmesi değil; daha tutarlı, daha hızlı ve daha izlenebilir süreçler kurmaya katkı sağlamasıdır. Bu katkı ancak görev tanımları, onay noktaları, performans ölçütleri ve sorumluluk zinciri netleştirildiğinde sürdürülebilir hâle gelir. Bölüm boyunca

yer verilen kavramlar, kamu kurumlarının yapay zekâ projelerini deneysellikten kurumsallaşmaya taşırken hangi yönetsel sorulara dikkat etmesi gerektiğini görünür kılmaktadır.

Bu bölümdeki terim sayısı	10

TERİMLER

E1 - Karar Destek Sistemi / *Decision Support System*

Tanım	Karar destek sistemi, karar vericilere veri, analiz, öngörü veya öneri sunarak değerlendirme sürecini destekleyen sistemdir. Kamu kurumlarında bu tür sistemler, nihai kararı insan otoritesine bırakırken karmaşık bilgiyi daha yönetilebilir hâle getirebilir.
Kamuda kullanım örneği	Bir afet koordinasyon merkezinde, gelen ihbarları yoğunluk ve kritik ihtiyaç ölçütlerine göre sıralayan ancak nihai saha sevk kararını insan yöneticinin verdiği yapı karar destek sistemi örneğidir.
Kurumsal dikkat notu	Karar desteği ile otomatik karar verme karıştırılmamalıdır; sistem öneri sunar, sorumluluk insanda kalır.
İlişkili terimler	İnsan denetimi, risk sınıflandırması, performans göstergesi, yapay zekâ ajanı

E2 - Otomasyon / *Automation*

Tanım	Otomasyon, belirli iş süreçlerinin insan müdahalesi olmadan ya da çok sınırlı müdahaleyle yürütülmesidir. Yapay zekâ ile birleştiğinde daha karmaşık işlem akışlarının otomatik yürütülmesi mümkün hâle gelebilir.
Kamuda kullanım örneği	Rutin belge kayıt numarası verme, standart bildirim oluşturma veya eksik evrak kontrolü gibi işlemler otomasyonla hızlandırılabilir.
Kurumsal dikkat notu	Otomasyon uygun alanlarda verimlilik sağlar; ancak istisna yönetimi ve itiraz kanalları korunmalıdır.
İlişkili terimler	Bot, yapay zekâ ajanı, insan-makine iş birliği, denetim izi

E3 - Risk Sınıflandırması / *Risk Classification*

Tanım	Risk sınıflandırması, yapay zekâ uygulamalarının bireyler, kurumlar ve kamu hizmetleri üzerindeki olası etkilerine göre farklı risk düzeylerinde değerlendirilmesi yaklaşımıdır. Yüksek etkili sistemler daha sıkı denetime ihtiyaç duyar.
Kamuda kullanım örneği	Basit belge özetleme aracı düşük riskli kabul edilirken, vatandaşın haklarını etkileyen puanlama veya önceliklendirme sistemi daha yüksek risk sınıfına alınabilir.
Kurumsal dikkat notu	Her yapay zekâ uygulamasına aynı yönetişim düzeyini uygulamak doğru değildir; risk temelli yaklaşım gerekir.
İlişkili terimler	Algoritmik etki değerlendirmesi, insan denetimi, güvenilir yapay zekâ, uyum

E4 - Uyum / *Compliance*

Tanım	Uyum, bir yapay zekâ sisteminin ilgili mevzuata, kurumsal ilkelere, standartlara ve iç süreçlere uygun biçimde geliştirilmesi ve işletilmesidir. Kamu kurumlarında teknik başarı, hukuki ve idari uyumdan bağımsız düşünülemez.
Kamuda kullanım örneği	Bir kurumsal asistanın devreye alınmasından önce veri işleme, arşivleme, erişim yetkisi ve kayıt tutma boyutlarının ilgili düzenlemelerle uyumlu hâle getirilmesi gerekir.
Kurumsal dikkat notu	Uyum son aşamada yapılan bir kontrol değil; tasarım boyunca izlenen bir ilke olmalıdır.
İlişkili terimler	Veri yönetişimi, denetim izi, kamu alımı, mahremiyet

E5 - Denetim İzi / *Audit Trail*

Tanım	Denetim izi, sistemin hangi verileri ne zaman kullandığını, hangi işlemlerin kim tarafından tetiklendiğini ve hangi çıktının nasıl oluştuğunu geriye dönük incelemeye imkân veren kayıt zinciridir. Kamu hesap verebilirliği için kritik önemdedir.
Kamuda kullanım örneği	Bir yapay zekâ asistanının hangi belgeyi hangi tarihte kaynak göstererek yanıt ürettiğinin kayıt altına alınması denetim izinin parçasıdır.
Kurumsal dikkat notu	Kayıt tutmayan sistemler kısa vadede pratik görünse de itiraz, denetim ve güvence süreçlerinde ciddi sorun yaratır.
İlişkili terimler	Hesap verebilirlik, şeffaflık, siber güvenlik, ajan yönetişimi

E6 - Kamu Alımı / *Public Procurement*

Tanım	Kamu alımı, kamu kurumlarının mal, hizmet veya teknoloji çözümlerini belirli usuller çerçevesinde tedarik etme sürecidir. Yapay zekâ çözümlerinin seçimi de bu çerçevede teknik ve yönetsel dikkat gerektirir.
Kamuda kullanım örneği	Bir kurum, yapay zekâ destekli belge yönetim sistemi satın alırken teknik şartnameye açıklanabilirlik, veri güvenliği, log kaydı ve bakım sorumluluğu maddeleri koyabilir.
Kurumsal dikkat notu	Yalnızca performans vaadine odaklanan alım süreçleri, sonradan yönetişim ve veri kontrolü sorunları doğurabilir.
İlişkili terimler	Uyum, veri egemenliği, performans göstergesi, pilot uygulama

E7 - Pilot Uygulama / *Pilot Implementation*

Tanım	Pilot uygulama, bir yapay zekâ çözümünün sınırlı kapsamda ve kontrollü koşullarda denenerek performansının, risklerinin ve kurumsal uyumunun değerlendirilmesi sürecidir. Kamu kurumlarında geniş ölçekli yaygınlaştırmadan önce geliştirme sağlar.
Kamuda kullanım örneği	Kurum içi yazışma özetleme aracı önce tek genel müdürlükte altı haftalık pilotla denenip sonuçları değerlendirilebilir.
Kurumsal dikkat notu	Pilot uygulama başarı gösterse bile tüm kurum için otomatik geçerlilik sağlamaz; kapsam genişledikçe yeni riskler doğabilir.
İlişkili terimler	Güvence, performans göstergesi, risk sınıflandırması, karar destek sistemi

E8 - Performans Göstergesi / *Performance Metric*

Tanım	Performans göstergesi, bir yapay zekâ sisteminin doğruluk, hız, kapsayıcılık, hata oranı, kullanıcı memnuniyeti veya hizmet etkisi gibi ölçütlerle değerlendirilmesini sağlayan nicel ya da nitel göstergedir.
Kamuda kullanım örneği	Bir dijital asistan için yanıt doğruluğu, ortalama yanıt süresi, insan operatöre yönlendirme oranı ve vatandaş memnuniyet puanı birlikte izlenebilir.
Kurumsal dikkat notu	Yalnızca teknik doğruluk ölçümü yeterli değildir; kamu yararı ve hizmet kalitesi de değerlendirilmelidir.
İlişkili terimler	Test verisi, güvence, pilot uygulama, dijital kamu hizmeti

E9 - İnsan-Makine İş Birliği / *Human-AI Collaboration*

Tanım	İnsan-makine iş birliği, insan uzmanlığı ile yapay zekâ kapasitesinin aynı süreçte birbirini tamamlayacak biçimde kullanılmasıdır. Kamu kurumlarında hedef çoğu zaman insanın yerini almak değil; karar kalitesini ve işlem hızını artırmaktır.
Kamuda kullanım örneği	Hukuk birimi, mevzuat taramasını yapay zekâ aracına yaptırıp nihai yorum ve görüş metnini uzman ekip tarafından tamamlayabilir.
Kurumsal dikkat notu	İş birliği modeli kurulmadığında ya sisteme aşırı güven oluşur ya da araçtan hiç verim alınamaz.
İlişkili terimler	İnsan denetimi, karar destek sistemi, yapay zekâ asistanı, otomasyon

E10 - Dijital Kamu Hizmeti / *Digital Public Service*

Tanım	Dijital kamu hizmeti, kamu hizmetlerinin dijital kanallar üzerinden daha erişilebilir, hızlı ve etkili biçimde sunulmasını ifade eder. Yapay zekâ, bu hizmetleri kişiselleştirme ve hızlandırma potansiyeli taşır.
Kamuda kullanım örneği	Bir vatandaş, dijital hizmet portalında günlük dile yakın ifadelerle soru sorarak hangi belgeyi hangi sırayla hazırlaması gerektiğini öğrenebilir.
Kurumsal dikkat notu	Dijital kolaylık sağlanırken erişilebilirlik, eşit hizmet ve alternatif başvuru kanalları korunmalıdır.
İlişkili terimler	Yapay zekâ asistanı, karar destek sistemi, adillik, şeffaflık, mahremiyet

BÖLÜM F

AJANLAR, PROTOKOLLER VE ENTEGRASYON

Yapay zekâ alanındaki son dönüşüm, yalnızca yanıt üreten modellerden, araç kullanabilen ve çok adımlı iş akışları yürütebilen ajan sistemlerine geçişle belirginleşmektedir. Bu yeni dönem, kamu kurumları açısından hem önemli verimlilik fırsatları hem de yeni yönetişim soruları doğurmaktadır. Çünkü bir sistemin yalnızca içerik üretmesi ile belge araması, veri çekmesi, alt görevler planlaması ve sonuçları insan onayına sunması arasında niteliksel bir fark bulunmaktadır.

Bu bölüm, yapay zekâ ajanı, ajansal yapay zekâ, çok ajanlı sistem, araç kullanımı, orkestrasyon, model bağlam protokolü ve A2A gibi giderek daha sık duyulan kavramları sade ve uygulamaya dönük biçimde açıklamaktadır. Amaç, kamu kurumlarının yakın gelecekte karşılaşacağı bu yeni mimari dili anlaşılır kılmak ve farklı otomasyon düzeyleri arasındaki farkları görünür hâle getirmektir. Özellikle arka plan ajanları ile kullanıcıyla doğrudan etkileşen arayüz ajanları arasındaki ayrım, görev ve yetki sınırlarının kurulması bakımından önemlidir.

Ajan sistemleri kamuda rapor hazırlama, belge toplama, mevzuat tarama, süreç izleme ve kurumsal asistan senaryolarında güçlü destek sunabilir. Bununla birlikte özerklik düzeyi arttıkça kayıt tutma, yetki sınırı, sorumluluk zinciri ve güvenlik doğrulaması da daha kritik hâle gelir. Bu nedenle bu bölümdeki terimler yalnızca teknolojik

yenilikleri tanıtmak için değil; yeni kuşak yapay zekâ sistemlerinin kamuda nasıl kontrollü ve hesap verebilir biçimde konumlandırılabileceğini tartışmak için bir giriş zemini olarak tasarlanmıştır.

Bu bölümdeki terim sayısı	13

TERİMLER

F1 - Yapay Zekâ Ajanı / *AI Agent*

Tanım	Yapay zekâ ajanı, belirli bir hedef doğrultusunda görev planlayabilen, gerektiğinde araçlardan yararlanabilen ve belirli ölçüde özerk biçimde adım atabilen yapıdır. Klasik sohbet sistemlerinden farkı, yalnızca yanıt vermekle kalmayıp süreç yönetebilmesidir.
Kamuda kullanım örneği	Kurum içi bir ajan, uzman talebi üzerine ilgili genelgeleri bulabilir, özet çıkarabilir, eksik belge listesini hazırlayabilir ve sonucu onay için personele sunabilir.
Kurumsal dikkat notu	Ajan kavramı yüksek özerklik ihtimali taşıdığı için yetki sınırları, kayıt mekanizmaları ve insan onay noktaları açıkça tanımlanmalıdır.
İlişkili terimler	Ajansal yapay zekâ, araç kullanımı, ajan yönetişimi, orkestrasyon

F2 - Ajansal Yapay Zekâ / *Agentic AI*

Tanım	Ajansal yapay zekâ, planlama, alt görevlere ayırma, araç kullanma ve gerektiğinde geri bildirimle yol değiştirme yeteneği olan sistem yaklaşımını ifade eder. Bu yaklaşım, salt cevap üreten modellerden daha eylem odaklıdır.
Kamuda kullanım örneği	Bir kamu kurumunda ajansal sistem, gelen rapor talebini analiz edip ilgili veri kaynaklarını sırayla tarayabilir, ara özetler çıkarabilir ve sonuç taslağını hazırlayabilir.
Kurumsal dikkat notu	Ajansal sistemler üretkenlik sağlasa da yanlış hedef veya yanlış araç seçimi durumunda hata etkisi büyüyebilir.
İlişkili terimler	Yapay zekâ ajanı, görev ayrıştırma, ajansal akıl yürütme, insan denetimi

F3 - Yapay Zekâ Asistanı / *AI Assistant*

Tanım	Yapay zekâ asistanı, kullanıcı sorularına yanıt veren, bilgiye erişimi kolaylaştıran ve çoğu zaman kullanıcı yönlendirmesiyle çalışan destekleyici sistemdir. Ajanlara kıyasla genellikle daha düşük özerklik düzeyine sahiptir.
Kamuda kullanım örneği	Personelin mevzuat sorularına kurum içi belge havuzundan yanıt veren ekran tabanlı bilgi yardımcısı, yapay zekâ asistanı örneğidir.
Kurumsal dikkat notu	Asistan ile ajan arasındaki fark açık biçimde tanımlanmadığında kullanıcı, sistemin bilgi vermenin ötesine geçerek kendi adına işlem başlatabileceğini düşünebilir.
İlişkili terimler	Yapay zekâ ajanı, bot, geri getirmeli artırılmış üretim, insan-makine iş birliği

F4 - Bot / *Bot*

Tanım	Bot, genellikle önceden tanımlı kurallar veya sınırlı görev yapısı ile çalışan otomatik yazılım bileşenidir. Her bot yapay zekâ ajanı değildir; bazı botlar oldukça basit otomasyon mantığıyla çalışır.
Kamuda kullanım örneği	Bir kurum sitesinde çalışma saatleri, evrak listesi ve iletişim bilgisi gibi standart sorulara yanıt veren basit konuşma aracı bot olarak tanımlanabilir.
Kurumsal dikkat notu	Botların sahip oldukları kapasitenin üzerinde değerlendirilmesi, kullanıcı beklentisini bozabilir; bu nedenle kapasite ve sınırlar açıkça belirtilmelidir.
İlişkili terimler	Otomasyon, yapay zekâ asistanı, yapay zekâ ajanı, şeffaflık

F5 - Görev Ayrıştırma / *Task Decomposition*

Tanım	Görev ayrıştırma, karmaşık bir işi daha küçük ve yönetilebilir alt görevlere bölme yaklaşımıdır. Ajan tabanlı sistemler, çok adımlı işleri yürütürken bu yöntemden yararlanır.
Kamuda kullanım örneği	"Aylık hizmet raporu hazırla" talebi; veri toplama, özet çıkarma, tablo oluşturma ve yönetici notu hazırlama gibi alt görevlere ayrıştırılabilir.
Kurumsal dikkat notu	Alt görevlerin yanlış kurgulanması toplam çıktının kalitesini düşürür; görev zinciri kurumsal mantığa uygun tasarlanmalıdır.
İlişkili terimler	Ajansal yapay zekâ, orkestrasyon, araç kullanımı, ajansal akıl yürütme

F6 - Ajansal Akıl Yürütme / *Agentic Reasoning*

Tanım	Ajansal akıl yürütme, bir sistemin görevin ilerleyişine göre ara değerlendirme yapması, bir sonraki adımı seçmesi ve gerektiğinde stratejisini güncellemesidir. Araçlardan gelen sonuçlarla planın yeniden şekillenmesi bu kavramın parçasıdır.
Kamuda kullanım örneği	Bir ajan, aradığı veriyi ilk kaynakta bulamazsa ikinci kaynağa yönelip elde ettiği bilgiler ışığında rapor yapısını yeniden kurabilir.
Kurumsal dikkat notu	Bu tür sistemler ikna edici görünse de akıl yürütme kalitesi her zaman doğruluk anlamına gelmez; uzman kontrolü gereklidir.
İlişkili terimler	Muhakeme modeli, görev ayrıştırma, yapay zekâ ajanı, insan denetimi

F7 - Çok Ajanlı Sistem / *Multi-Agent System*

Tanım	Çok ajanlı sistem, birden fazla ajanın farklı rolleri üstlenerek aynı iş akışı içinde birlikte çalıştığı yapıdır. Bu mimari, karmaşık görevlerin uzmanlaşmış alt bileşenler arasında paylaşılmasını sağlar.
Kamuda kullanım örneği	Bir rapor hazırlama sisteminde bir ajan veri toplar, bir diğeri özet çıkarır, bir diğeri mevzuat uyumunu kontrol eder ve son karar için insan uzmana sunar.
Kurumsal dikkat notu	Birden fazla ajanın birlikte çalıştığı ortamlarda sorumluluk zinciri ve log kaydı daha da önem kazanır.
İlişkili terimler	Orkestrasyon, Agent2Agent Protokolü, ajan yönetişimi, denetim izi

F8 - Arka Plan Ajanı / *Background Agent*

Tanım	Arka plan ajanı, kullanıcı ile doğrudan etkileşime girmeden perde arkasında veri toplama, eşleştirme, izleme veya hazırlık işlemleri yürüten ajan türüdür. Görünmeyen ama iş akışını destekleyen katmandır.
Kamuda kullanım örneği	Gelen başvuruların ek belgelerini sistemlerden otomatik derleyip uzmanın ekranına hazır hâlde getiren yapı arka plan ajanı olarak tasarlanabilir.
Kurumsal dikkat notu	Arka planda çalışan sistemler görünmez olduğu için yetki kontrolü ve kayıt tutma daha da kritik hâle gelir.
İlişkili terimler	Yapay zekâ ajanı, orkestrasyon, denetim izi, ajan yönetişimi

F9 - Etkileşimli Ortak / *Interactive Partner / Surface Agent*

Tanım	Etkileşimli ortak, kullanıcıyla doğrudan temas kuran, soru alan, seçenek sunan ve süreci kullanıcıyla birlikte yürüten ajan ya da ajan benzeri arayüz katmanıdır. Ajan sistemlerinin görünen yüzü olarak işlev görür.
Kamuda kullanım örneği	Personelin ekran üzerinden taleplerini ilettiği ve sürecin hangi aşamada olduğunu izlediği yapay zekâ destekli çalışma paneli etkileşimli ortak işlevi görebilir.
Kurumsal dikkat notu	Kullanıcı arayüzü, sistem kapasitesine ilişkin yanıltıcı bir izlenim oluşturmamalı; hangi adımlarda insan onayı gerektiğini açıkça göstermelidir.
İlişkili terimler	Yapay zekâ asistanı, yapay zekâ ajanı, şeffaflık, insan-makine iş birliği

F10 - Araç Kullanımı / *Tool Use / Tool Calling*

Tanım	Araç kullanımı, modelin veya ajanın yalnızca metin üretmekle kalmayıp dış araçlara, veritabanlarına, hesaplayıcılara veya iş akışı bileşenlerine başvurabilmesi yeteneğidir. Modern ajan mimarilerinin temel unsurlarından biridir.
Kamuda kullanım örneği	Bir kurumsal ajanın, yanıt üretmeden önce resmî belge yönetim sisteminden kayıt çekmesi veya takvim sisteminden uygun zaman araması araç kullanımı örneğidir.
Kurumsal dikkat notu	Araçlara yetkisiz erişim ciddi güvenlik ve yetki devri sorunları doğurabilir; izin modeli açık kurulmalıdır.
İlişkili terimler	Model bağlam protokolü, yapay zekâ ajanı, orkestrasyon, siber güvenlik

F11 - Orkestrasyon / *Orchestration*

Tanım	Orkestrasyon, birden fazla modelin, ajanın, veri kaynağının ve aracın belirli bir düzen içinde koordine edilmesi sürecidir. Karmaşık iş akışlarının yönetilebilir ve tutarlı kalmasını sağlar.
Kamuda kullanım örneği	Bir kurumda başvuru işleme sistemi; belge okuma modeli, mevzuat arama modülü, özetleme aracı ve onay ekranı arasında orkestrasyon kurarak bütünleşik hizmet sunabilir.
Kurumsal dikkat notu	Orkestrasyon tasarımı zayıfsa sistem parçaları birbirini tekrar edebilir, yanlış sırada çalışabilir veya kayıt dışı işlem başlatabilir.
İlişkili terimler	Çok ajanlı sistem, araç kullanımı, görev ayrıştırma, Agent2Agent Protokolü

F12 - Model Bağlam Protokolü / *Model Context Protocol (MCP)*

Tanım	Model Bağlam Protokolü, dil modellerinin dış veri kaynakları, uygulamalar ve servislerle standart ve güvenli biçimde iletişim kurmasını amaçlayan açık bir protokol yaklaşımıdır. Böylece modelin dış dünya ile kontrollü bağlantısı daha düzenli hâle gelir.
Kamuda kullanım örneği	Kurum içi asistanın belge arşivi, mevzuat veritabanı ve takvim sistemi gibi kaynaklara standart arayüzle bağlanması MCP yaklaşımıyla yönetilebilir.
Kurumsal dikkat notu	Protokol standardı güvenliği kolaylaştırabilir; ancak her bağlantının yetki kapsamı ayrıca tanımlanmalıdır.
İlişkili terimler	Araç kullanımı, API, siber güvenlik, orkestrasyon

F13 - Agent2Agent Protokolü / *Agent2Agent Protocol (A2A)*

Tanım	Agent2Agent Protokolü, farklı ajanların veya farklı sağlayıcılara ait ajan sistemlerinin standart biçimde iletişim kurmasını hedefleyen birlikte çalışabilirlik yaklaşımıdır. Çok ajanlı yapılarda koordinasyonu kolaylaştırır.
Kamuda kullanım örneği	Farklı kurumlarda çalışan yapay zekâ bileşenlerinin belirli yetki sınırları içinde bilgi alışverişi yaparak ortak süreç yürütmesi gelecekte A2A benzeri protokollerle mümkün olabilir.
Kurumsal dikkat notu	Ajanlar arası iletişim arttıkça veri paylaşımı, sorumluluk zinciri ve güvenlik sınırlarının açık biçimde yönetilmesi daha kritik hâle gelir.
İlişkili terimler	Çok ajanlı sistem, orkestrasyon, ajan yönetişimi, denetim izi

BÖLÜM G

YAPAY ZEKÂ GÜVENLİĞİ

Yapay zekâ sistemleri kamu hizmetlerinde yaygınlaştıkça, güvenlik konusu klasik bilgi güvenliği çerçevesinin ötesine geçen yeni boyutlar kazanmaktadır. Bir modelin yanıltılması, istem enjeksiyonu ile yönlendirilmesi, eğitim verisinin zehirlenmesi ya da çıktılar üzerinden mahremiyet sızıntısı yaşanması; artık yalnızca teknik ekiplerin değil, kurum yönetiminin de dikkatle izlemesi gereken risk alanlarıdır. Bu nedenle yapay zekâ güvenliği, hem siber güvenlik disiplininin bir uzantısı hem de üretken ve öğrenen sistemlere özgü yeni bir uzmanlık alanı olarak değerlendirilmelidir.

Bu bölümde düşmanca saldırı, model zehirleme, model çalma, üyelik çıkarım saldırısı, arka kapı saldırısı ve kırmızı takım testi gibi kavramlar; kamu kurumlarının maruz kalabileceği somut güvenlik senaryoları üzerinden açıklanmaktadır. Ayrıca yapay zekâ güvenlik duvarı, model sağlamlığı, gizlilik korumalı hesaplama ve diferansiyel gizlilik gibi savunma ve koruma odaklı kavramlar da bu çerçevenin tamamlayıcı parçaları olarak ele alınmaktadır. Böylece okuyucu yalnızca saldırı türlerini değil, kurumsal dayanıklılığı artırabilecek karşılıkları da birlikte görebilmektedir.

Kamu açısından yapay zekâ güvenliğinin önemi, bu sistemlerin çoğu zaman kritik altyapılarla, vatandaş verileriyle ve yüksek güven gerektiren hizmet süreçleriyle ilişkili olmasından kaynaklanır. Bir güvenlik zafiyeti yalnızca teknik arıza anlamına gelmez; kamu güveni-

nin zedelenmesi, kişisel verilerin açığa çıkması, yanlış yönlendirme ve hizmet sürekliliğinin bozulması gibi geniş sonuçlar doğurabilir. Bu bölüm, yapay zekâ güvenliğini teknoloji sonrasında düşünülen bir ek tedbir olarak değil; tasarım, test, devreye alma ve izleme süreçlerinin ayrılmaz parçası olarak konumlandırmaktadır.

Bu bölümdeki terim sayısı	12

TERİMLER

G1 - Düşmanca Saldırı / *Adversarial Attack*

Tanım	Düşmanca saldırı, bir yapay zekâ modelini yanıltmak ve yanlış karar vermesini sağlamak amacıyla, girdilere insan gözüyle fark edilemeyen ancak modelin çıktısını tamamen değiştiren küçük, kasıtlı değişiklikler eklenmesidir.
Kamuda kullanım örneği	Bir trafik izleme sisteminde, dur tabelasının üzerine yapıştırılan küçük ve anlamsız görünen bir çıkartma, sistemin tabelayı yanlış algılamasına ve tehlikeli bir karar vermesine neden olabilir.
Kurumsal dikkat notu	Görüntü, ses veya metin işleyen kritik sistemler, düşmanca saldırılara karşı dayanıklılık testlerinden geçirilmeden devreye alınmamalıdır.
İlişkili terimler	Siber güvenlik, model sağlamlığı, bilgisayarlı görü

G2 - İstem Enjeksiyonu / *Prompt Injection*

Tanım	İstem enjeksiyonu, kötü niyetli bir kullanıcının, üretken yapay zekâ sistemine verilen girdinin içine gizlenmiş talimatlar yerleştirerek, modelin orijinal görevini atlamasını ve istenmeyen eylemleri gerçekleştirmesini sağlamasıdır.
Kamuda kullanım örneği	Bir kamu kurumunun web sitesindeki sohbet botuna, sistemin güvenlik talimatlarını aşmaya yönelik gizli komutlar girilerek hassas bilgilere erişim denenebilir.
Kurumsal dikkat notu	Kullanıcı girdileri doğrudan modele iletilmemeli; araya filtreleme, doğrulama ve güvenlik katmanları eklenmelidir.
İlişkili terimler	İstem tasarımı, büyük dil modeli, yapay zekâ güvenlik duvarı

G3 - Model Zehirleme / *Model Poisoning / Data Poisoning*

Tanım	Model zehirleme, saldırganların bir yapay zekâ modelinin eğitim veya ince ayar sürecinde kullanılan veri kümesine kasıtlı olarak hatalı, yanıltıcı veya zararlı veriler ekleyerek modelin gelecekteki davranışlarını bozmasıdır.
Kamuda kullanım örneği	Bir siber tehdit algılama sisteminin eğitim verisine, belirli bir zararlı yazılım türünü güvenli olarak etiketleyen veriler sızdırılarak, sistemin o saldırıyı tespit etmesi engellenebilir.
Kurumsal dikkat notu	Eğitim verilerinin kaynağı, bütünlüğü ve değiştirilmediği kriptografik yöntemlerle doğrulanmalı; dış kaynaklı veriler sıkı denetimden geçirilmelidir.
İlişkili terimler	Eğitim verisi, veri kalitesi, arka kapı saldırısı

G4 - Model Çalma / *Model Extraction / Model Stealing*

Tanım	Model çalma, bir saldırganın hedef modele çok sayıda sorgu göndererek ve aldığı yanıtları analiz ederek, o modelin işleyiş mantığını veya parametrelerini kopyalayıp kendi sisteminde yeniden oluşturmasıdır.
Kamuda kullanım örneği	Bir kamu kurumunun yüksek maliyetle geliştirdiği ve uygulama programlama arayüzü üzerinden hizmete sunduğu özel bir risk analiz modeli, sürekli sorgularla taklit edilerek yetkisiz kişilerce kullanılabilir.
Kurumsal dikkat notu	Uygulama programlama arayüzü erişimlerinde hız sınırları, anomali tespiti ve sorgu davranış analizi uygulanarak olağandışı kullanım kalıpları engellenmelidir.
İlişkili terimler	Uygulama programlama arayüzü, siber güvenlik, çıkarım

G5 - Üyelik Çıkarım Saldırısı / *Membership Inference Attack*

Tanım	Üyelik çıkarım saldırısı, bir saldırganın eğitilmiş bir yapay zekâ modelinin çıktılarını analiz ederek, belirli bir kişinin veya veri kaydının o modelin eğitim veri kümesinde yer alıp almadığını tespit etmeye çalışmasıdır.
Kamuda kullanım örneği	Bir hastanenin nadir bir hastalık için eğittiği teşhis modeline sorgular gönderen bir saldırgan, belirli bir vatandaşın sağlık verilerinin bu modelin eğitiminde kullanıldığını ortaya çıkarabilir.
Kurumsal dikkat notu	Kişisel verilerle eğitilen modellerde mahremiyet sızıntısı riski yüksektir; diferansiyel gizlilik gibi koruyucu teknikler kullanılmalıdır.
İlişkili terimler	Mahremiyet, eğitim verisi, diferansiyel gizlilik

G6 - Arka Kapı Saldırısı / *Backdoor Attack*

Tanım	Arka kapı saldırısı, modelin eğitim aşamasında içine gizli bir tetikleyici yerleştirilmesidir. Model normal durumlarda doğru çalışırken, tetikleyiciyi gördüğünde saldırganın belirlediği yanlış veya zararlı çıktıyı üretir.
Kamuda kullanım örneği	Bir yüz tanıma tabanlı güvenlik geçiş sistemine, sadece belirli bir aksesuarı takan kişileri yetkili olarak tanıyacak şekilde gizli bir arka kapı yerleştirilebilir.
Kurumsal dikkat notu	Dışarıdan hazır alınan modellerin iç yapısı tam olarak bilinmediğinden, bu tür modeller kritik süreçlerde kullanılmadan önce güvenlik testlerinden geçirilmelidir.
İlişkili terimler	Model zehirleme, siber güvenlik, temel model

G7 - Kırmızı Takım Testi / *Red Teaming*

Tanım	Kırmızı takım testi, bağımsız güvenlik uzmanlarının veya otomatik araçların, bir yapay zekâ sisteminin zafiyetlerini, önyargılarını ve güvenlik açıklarını bulmak amacıyla sisteme kasıtlı olarak saldırması ve onu zorlaması sürecidir.
Kamuda kullanım örneği	Bir kamu kurumunun yeni devreye alacağı değerlendirme yapay zekâsı, kırmızı takım uzmanları tarafından ayrımcı kararlar vermeye veya veri sızdırmaya zorlanarak test edilebilir.
Kurumsal dikkat notu	Kırmızı takım testleri sadece devreye alım öncesinde değil, sistem güncellendikçe ve yeni tehditler ortaya çıktıkça düzenli olarak tekrarlanmalıdır.
İlişkili terimler	Güvence, siber güvenlik, algoritmik etki değerlendirmesi

G8 - Yapay Zekâ Güvenlik Duvarı / *AI Firewall / Guardrails*

Tanım	Yapay zekâ güvenlik duvarı, model ile kullanıcı arasına yerleştirilen, modele giden istemleri ve modelden dönen çıktıları gerçek zamanlı olarak denetleyen, filtreleyen ve zararlı veya uygunsuz içerikleri engelleyen güvenlik katmanıdır.
Kamuda kullanım örneği	Bir bakanlığın vatandaş iletişim asistanı, kullanıcının uygunsuz taleplerini modele ulaşmadan engelleyen ve modelin yanlışlıkla üretebileceği hassas bilgileri dışarı çıkmadan durduran bir güvenlik duvarı ile korunabilir.
Kurumsal dikkat notu	Güvenlik duvarı kuralları, kurumun etik ilkeleri ve mevzuat gereksinimleriyle tam uyumlu olacak şekilde düzenli olarak güncellenmelidir.
İlişkili terimler	İstem enjeksiyonu, siber güvenlik, uyum

G9 - Derin Sahte / *Deepfake*

Tanım	Derin sahte, yapay zekâ teknikleri kullanılarak, bir kişinin yüzünün, sesinin veya hareketlerinin gerçeğinden ayırt edilemeyecek kadar inandırıcı bir şekilde başka bir videoya veya ses kaydına kopyalanması veya sıfırdan üretilmesidir.
Kamuda kullanım örneği	Üst düzey bir kamu yöneticisinin sesini taklit eden derin sahte bir telefon aramasıyla, alt kademedeki personele yetkisiz talimatlar verilerek dolandırıcılık yapılabilir.
Kurumsal dikkat notu	Kurum içi iletişimde ses ve görüntülerin doğruluğunu teyit edecek kriptografik imzalar veya çok faktörlü kimlik doğrulama yöntemleri kullanılmalıdır.
İlişkili terimler	Üretken yapay zekâ, siber güvenlik, çok kipli model

G10 - Model Sağlamlığı / *Model Robustness*

Tanım	Model sağlamlığı, bir yapay zekâ sisteminin beklenmedik girdiler, gürültülü veriler, eksik bilgiler veya kasıtlı düşmanca saldırılar karşısında performansını koruyabilme ve doğru kararlar vermeye devam edebilme kapasitesidir.
Kamuda kullanım örneği	Bir afet yönetim sisteminin, sahadan gelen sensör verilerinin bir kısmı kopsa veya hatalı sinyaller içerse bile, genel durumu doğru analiz etmeye devam edebilmesi model sağlamlığının bir göstergesidir.
Kurumsal dikkat notu	Sağlamlık, modelin sadece laboratuvar ortamındaki test verilerinde değil, gerçek dünyanın karmaşık ve öngörülemez koşullarında da test edilmesini gerektirir.
İlişkili terimler	Düşmanca saldırı, performans göstergesi, güvence

G11 - Gizlilik Korumalı Hesaplama / *Privacy-Preserving Computation*

Tanım	Gizlilik korumalı hesaplama, verilerin şifrelenmiş veya gizlenmiş hâldeyken bile üzerinde matematiksel işlemler ve yapay zekâ analizleri yapılabilmesini sağlayan kriptografik teknikler bütünüdür.
Kamuda kullanım örneği	İki farklı bakanlık, vatandaşların kişisel verilerini birbirleriyle açık metin olarak paylaşmadan, gizlilik korumalı hesaplama yöntemleriyle ortak bir veri analizi yaparak dolandırıcılık ağlarını tespit edebilir.
Kurumsal dikkat notu	Bu teknikler yüksek güvenlik sağlasa da, mevcut durumda hesaplama sürelerini ve maliyetlerini önemli ölçüde artırabilir.
İlişkili terimler	Mahremiyet, veri egemenliği, siber güvenlik

G12 - Diferansiyel Gizlilik / *Differential Privacy*

Tanım	Diferansiyel gizlilik, bir veri kümesinden elde edilen sonuçları ya da modeli, kişilerin kimliğini veya özel verisini ele vermeyecek şekilde belirsizleştirerek koruyan bir yöntemdir.
Kamuda kullanım örneği	Bir istatistik kurumu, nüfus sayımı verilerini araştırmacılara açarken diferansiyel gizlilik uygulayarak, genel demografik eğilimlerin doğru analiz edilmesini sağlarken hiçbir bireyin kişisel bilgilerinin açığa çıkmamasını garanti edebilir.
Kurumsal dikkat notu	Belirsizleştirme düzeyi arttıkça gizlilik artar; ancak veriden elde edilen sonuçların doğruluğu azalabilir. Bu nedenle gizlilik ile fayda arasında uygun bir denge kurulmalıdır.
İlişkili terimler	Mahremiyet, üyelik çıkarım saldırısı, sentetik veri

KAYNAKÇA

No	Kaynak	Bağlantı
1	OECD.AI - Glossary of Terms on AI	https://oecd.ai/en/dashboards/policy-initiatives/glossary-of-terms-on-ai
2	UNESCO - Recommendation on the Ethics of Artificial Intelligence	https://www.unesco.org/ethics-ai/en/node/302
3	NIST - The Language of Trustworthy AI: An In-Depth Glossary of Terms	https://www.nist.gov/publications/language-trustworthy-ai-depth-glossary-terms
4	European Commission - EU-US Terminology and Taxonomy for Artificial Intelligence	https://digital-strategy.ec.europa.eu/en/library/eu-us-terminology-and-taxonomy-artificial-intelligence-second-edition
5	NTIA - AI Accountability Policy Report Glossary of Terms	https://www.ntia.gov/issues/artificial-intelligence/ai-accountability-policy-report/glossary-of-terms
6	World Bank - GovTech Glossary	https://www.worldbank.org/en/programs/govtech/gtmi/gtmi-glossary
7	New York City - Artificial Intelligence Principles and Definitions	https://www.nyc.gov/assets/oti/downloads/pdf/about/artificial-intelligence-principles-definitions.pdf

8	IBM - What Are AI Agents?	https://www.ibm.com/think/topics/ai-agents
9	Red Hat - SLMs vs LLMs: What are small language models?	https://www.redhat.com/en/topics/ai/llm-vs-slm
10	Google Cloud - What is Model Context Protocol (MCP)?	https://cloud.google.com/discover/what-is-model-context-protocol
11	Google Developers Blog - A2A: A New Era of Agent Interoperability	https://developers.googleblog.com/en/a2a-a-new-era-of-agent-interoperability/
12	NVIDIA - What Are Frontier AI Models and How They Work	https://www.nvidia.com/en-us/glossary/frontier-models/