



Türkiye Bilişim Vakfı
www.tbv.org.tr

Yönetici Özeti

Yapay Zekâ - Hızlandırılmış Dönüşüm Çağında Yönetişim, Etik ve Risk

Giriş: Teoriden Gerçeğe Hızlandırılmış Geçiş

Yapay Zekâ, artık geleceğe dair bir potansiyel olmaktan çıkıp, bugünün somut ve yıkıcı etkilerini sıklıklar gördüğümüz bir gücüne dönüşmüştür.

Geçtiğimiz dönem, özellikle üretken Yapay Zekâ'nın deneysel bir teknolojiden iş, hükümet ve toplumun temel fonksiyonlarına entegre bir bileşen haline geldiği baş döndürücü bir hızlanmaya sahne olmuştur. Bu yeni dönemin en belirleyici özelliği, teknoloji benimseme ve risklerin ortaya çıkma döngülerinin "yıllara" değil "aylara" sıkışmasıdır. Gelişmeler geleneksel yönetim ve düzenleme mekanizmaları üzerinde muazzam bir baskı yaratmakta ve tüm paydaşları, belirsizlik ortamından proaktif ve uyarlanabilir stratejiler geliştirmeye doğru zorlamaktadır. Artık tartışma Yapay Zekâ'nın "ne yapabileceğinden" ziyade, halihazırda ne yaptığını ve "neyi değiştirmekte" olduğuna odaklanmıştır; Yapay Zekâ, endüstrileri yeniden şekillendirmekte, bilgi eko sistemlerini dönüştürmekte ve hem benzeri görülmemiş fırsatlar hem de ciddi zorluklar sunmaktadır.

Ekte yer alan rapor, Yapay Zekâ'nın bu yeni evresini üç temel ekseninde analiz etmektedir; vatandaşlar, özel sektör ve hükümetler için ortaya çıkan riskler, zorunluluklar ve stratejik çıkarımlar.

Özetle:

1. Vatandaşlar İçin Yoğunlaşan Riskler: Mahremiyet, Eşitlik ve Güven Krizi

Vatandaşlar için Yapay Zekâ kaynaklı riskler, niteliksel bir dönüşüm geçirerek daha kişisel ve tehlikeli bir hal almıştır.

- **Mahremiyetin Aşınması:** Tehdit, artık sadece kişisel verilerin toplanmasından ibaret değildir; doğrudan bireyleri hedef alan sentetik gerçekliklerin üretilmesine evrilmiştir. Kamuoyunda tanınan kişilerin rızası olmadan oluşturulan cinsel içerikler Yapay Zekâ'nın bireylerin onurunu ve mahremiyetini ihlal etmek için nasıl bir silaha dönüştürülebildiğini göstermekte, kişisel veriler gerçek yaşantı ile alakası olmayan "persona" modellerine dönüşmektedir. Bu durum, özellikle kadınları ve savunmasız grupları orantısız bir şekilde hedef almaktadır. Bu tehdidin bir diğer yıkıcı boyutu ise deepfake teknolojilerinin akran zorbalığı ve dijital zorbalık (cyberbullying) ekosistemine entegre olmasıdır. Artık yalnızca kamuoyunda tanınan kişiler değil, herhangi bir birey de manipüle edilmiş video ve görseller aracılığıyla itibar suikastına uğrayabilmektedir.

Okullarda ve genç nüfusun yoğun olduğu dijital platformlarda, gerçek dışı içeriklerle bireylerin küçük düşürülmesi, sosyal izolasyona sürüklenmesi ve



Türkiye Bilişim Vakfı
www.tbv.org.tr

psikolojik travma yaşamayı olağan hale gelmektedir. Bu durum, sadece bireysel onur ve güvenlik riskini değil, aynı zamanda gençlerin dijital kimliklerine yönelik sistemik bir tehdit ortaya koyarak sosyal güven dokusunu aşındırmaktadır.

- **Algoritmik Önyargının Genişleyen Kapsamı:** Yapay Zekâ sistemlerinin toplumsal önyargıları pekiştirme riski, artık sadece ırk ve cinsiyetle sınırlı değildir. ABD'de engelli veya nörolojik olarak farklı adayları sistematik olarak eleyen Yapay Zekâ tabanlı işe alım araçlarına karşı başlatılan yasal işlemler, önyargının kapsamının ne kadar genişlediğini ve adalet için yeni zorluklar yarattığını ortaya koymaktadır. Buna ek olarak zaman içerisinde terfi, performans ve disiplin süreçlerinde bu araçların kullanılmaya başlanmasının sonuçlarına yeterli hazırlık yapılmamıştır.
- **Bilgi Bütünlüğüne Yönelik Saldırıları:** Yapay Zekâ'nın demokratik süreçleri baltalayabileceği yönündeki teorik endişeler, son seçimlerde somut bir gerçeğe dönüşmüştür. Tehdit aktörleri, Tayvan'daki seçimlerde adayların "deepfake" videolarını ve Yapay Zekâ tarafından oluşturulan sanal haber spikerlerini kullanmış, ABD'de ise Başkan'ın sesini taklit eden robot aramalarla seçmenleri oy kullanmaktan caydırmaya çalışmıştır. Bu saldırılar sadece dezenformasyon yaymakla kalmamakta, aynı zamanda halkın kurumlara ve bilgi kaynaklarına olan güvenini temelden sarsarak bir "kurumsal güven krizi" yaratmaktadır.

2. Özel Sektör İçin Artan Riskler: Stratejik Bir Kısaç Hareketi

Özel şirketler için Yapay Zekâ, artık sadece bir inovasyon alanı değil, aynı zamanda varoluşsal hukuki ve stratejik riskleri barındıran bir arenadır.

- **Telif Hakkı Mücadelesi:** Üretken Yapay Zekâ geliştiricilerinin temel iş modelini sorgulayan bir dizi yüksek profilli telif hakkı davası açılmıştır.

The New York Times'ın OpenAI'a ve Disney/Universal'ın Midjourney'e karşı açtığı davalar, Yapay Zekâ modellerini eğitmek için kullanılan telifli verilerin "adil kullanım" doktrini kapsamında olup olmadığına dair hukuki bir savaş başlatmıştır. Bu davaların sonuçları, sektörün veri edinim stratejilerini ve maliyet yapılarını kökten değiştirebilir. Nitekim bazı medya ortamları anlaşmalarla kaynak kullanımına izin veriyor olsalar bile telif hakları önemli bir başlık olarak gündemde kalmaya devam edecektir.

- **Antitröst Soruşturmaları ve Stratejik İkilem:** Eş zamanlı olarak, antitröst düzenleyicileri, Microsoft gibi büyük teknoloji şirketlerinin OpenAI gibi lider Yapay Zekâ laboratuvarlarına yaptıkları büyük yatırımları ve stratejik ortaklıkları mercek altına almıştır. Buradaki temel endişe, bu baskın firmaların pazar güçlerini kullanarak rekabeti engellemesi ve Yapay Zekâ ekosistemini domine etmesidir. Bu durum, şirketleri bir "kısaç hareketi" ile karşı karşıya bırakmaktadır: Telif hakkı davaları onları lisanslama maliyetleri nedeniyle Büyük Teknoloji ortaklarına daha bağımlı hale getirirken, bu artan bağımlılık tröst endişelerini daha da alevlendirmektedir.



Türkiye Bilişim Vakfı
www.tbv.org.tr

- **Gelişen Siber Güvenlik Tehditleri:** Yapay Zekâ, siber saldırıları daha sofistike ve erişilebilir hale getirmiştir. Küresel mühendislik firması Arup'un yaşadığı 25,6 milyon dolarlık deepfake dolandırıcılığı, Yapay Zekâ'nın insan muhakemesini ve geleneksel güvenlik protokollerini aşmak için nasıl kullanılabileceğinin çarpıcı bir örneğidir. WormGPT gibi "suç hizmeti" sohbet robotları ise düşük becerili aktörlerin bile etkili siber saldırılar düzenlemesini kolaylaştırmaktadır. Finansal ekosistemde risk metriğini keskin biçimde yükselten bir diğer vektör ise Yapay Zekâ destekli sosyal mühendislik saldırıdır. Artık saldırganlar, yalnızca e-posta veya sahte çağrılarla değil, kurbanın dijital ayak izini analiz ederek kişiye özel hazırlanmış, bağlam açısından tutarlı ve duygu manipülasyonu içeren hiper-gerçekçi senaryolar üretebilmektedir. LLM'lerle desteklenen "voice cloning" ve gerçek zamanlı görüntü sahtekârlığı, şirket içi yetkili kişileri taklit ederek finans ekiplerinden ödeme talep etme, transfer onayı alma veya SWIFT/BAP işlemlerini tetikleme gibi ileri seviye fraud mekanizmalarını mümkün kılmaktadır. Bu tür saldırılar, klasik güvenlik kontrol noktalarını atlayarak kurumların finansal varlıklarını hedef almakla kalmamakta, aynı zamanda itibar, uyum ve regülasyon risklerini de katmanlı biçimde büyütmektedir.

3. Hükümetler İçin Yeni Gerçekler: Hizmet, Güvenlik ve Uzmanlık Açığı

Hükümetler, Yapay Zekâ'yı hem bir hizmet aracı hem de bir ulusal güvenlik unsuru olarak benimsemeye çalışırken önemli zorluklarla yüzleşmektedir.

- **Kamu Hizmetlerinde Vaatler ve Tehlikeler:** Estonya ve Singapur gibi ülkeler, Yapay Zekâ 'yı kamu hizmetlerini iyileştirmek için başarıyla kullanırken, New York şehrinin pilot belediye sohbet robotunun vatandaşlara yasa dışı tavsiyeler vermesi gibi başarısızlıklar da yaşanmıştır. Bu vaka, üretken Yapay Zekâ'nın doğruluğun kritik olduğu kamu hizmetlerinde kontrolsüz kullanımının yüksek riskini ortaya koymaktadır.
- **Ulusal Güvenlik ve Düzenleme:** Ölümcül Otonom Silah Sistemleri (LAWS) alanında politika çerçeveleri netleşmekte ve ABD Kongresi gibi kurumlar, bu sistemlerin geliştirilmesi ve denetlenmesi üzerinde daha sıkı bir gözetim uygulamaktadır.
- **Yönetişimdeki Temel Zorluk:** Hükümetlerin karşılaştığı en büyük engellerden biri, Yapay Zekâ alanındaki derin teknik uzmanlığın büyük ölçüde özel sektörde yoğunlaşmasıdır. Bu "uzmanlık açığı", hükümetlerin etkili düzenlemeler yapmasını, Yapay Zekâ sistemlerini denetlemesini ve kamu yararını korumasını zorlaştırmaktadır.

Sonuç ve Stratejik Yol Haritası

Yapay Zekâ, soyut etik ilkelerin tartışıldığı bir dönemden, somut hukuki ve finansal sonuçların yaşandığı bir döneme geçmiştir. Bu hızlı ve karmaşık ortamda yol almak için tüm paydaşların proaktif ve iş birliğine dayalı adımlar atması gerekmektedir.

- **Özel Sektör İçin:** Şirketler, etik kurullar kurmanın ötesine geçerek, NIST (National Institute of Standards and Technology) Yapay Zekâ Risk Yönetimi Çerçevesi (AI RMF-AI Risk Management Framework) gibi denetlenebilir yönetim yapılarını benimsemelidir. Fikri mülkiyet ve anti tröst risklerini azaltmak için titiz durum tespiti yapmalı ve deepfake tabanlı sosyal mühendisliğe karşı güvenlik protokollerini güncellemelidir.
- **Hükümetler İçin:** AB'nin Genel Veri Koruma Tüzüğü, Yapay Zekâ Yasası ve Kasım 2026'da yürürlüğe girecek Ürün Sorumluluğu Yönergesi'nde olduğu gibi, inovasyonu engellemeden yüksek riskli uygulamaları ve yazılımları hedef alan, net ve uyarlanabilir düzenlemeler geliştirmek esastır. Düzenleyici kurumlar için de teknik uzmanlık kapasitesini artırmak ve kamu iletişimlerinde C2PA gibi içerik doğrulama standartlarını zorunlu kılarak örnek olmak kritik öneme sahiptir. Kamu yararını güvence altına almak için Yapay Zekâ araştırmalarına stratejik kamu yatırımları düşünülmelidir.
- **Vatandaşlar İçin:** Yapay Zekâ ve medya okuryazarlığı becerilerini geliştirmek, dezenformasyona karşı en etkili kişisel savunmadır. C2PA gibi içerik doğrulama araçlarının yaygınlaşmasını talep etmek ve kullanmak, bilgi ekosisteminde güveni yeniden tesis etmeye yardımcı olacaktır.

Yapay Zekâ Çağında Üç Boyutlu Risk Matrisi: Vatandaşlar, Şirketler ve Devletler

1. Boyut: Vatandaşlar (Yoğunlaşan Riskler)

Mahremiyetin Aşınması ve Dijital Zorbalık



Yapay zekâ, rızasız deepfake içerikler ve "sentetik gerçeklikler" aracılığıyla bireysel onuru hedef alan bir silaha dönüşmekte, özellikle savunmasız gruplar için lübra sulkasta riski yaratmaktadır.

Genişleyen Algoritmik Önyargı Kapsamı



Önyargılar artık sadece ırk ve cinsiyetle sınırlı kalmayıp; işe alım ve performans süreçlerinde engelli veya nörolojik farklılıkları olan bireylere karşı sistematik dışlanma riskini artırmaktadır.

Bilgi Bütünlüğüne ve Demokrasiye Saldırıları



Taynan seçimlerindeki deepfake videolar ve ABD'deki ses taklidi yapan robot aramalar, halkın kurumlara olan güvenini sarsarak "kurumsal güven krizi" yaratmaktadır.

2. Boyut: Özel Şirketler (Stratejik Kıskaç)

Telif Hakkı Mücadelesi ve Veri Savaşları



New York Times ve OpenAI arasındaki gibi yüksek profilli davalar, yapay zekâ eğitiminde kullanılan verilerin "adi kullanım" olup olmadığını sorgulatmakta ve sektörün maliyet yapılarını tehdit etmektedir.

Antitröst Soruşturmaları ve Stratejik İkilem



Büyük teknoloji şirketlerinin yapay zekâ laboratuvarlarına (örneğin Microsoft-OpenAI) yatırımları inselenmekte, tröst endişeleri ve pazardaki rekabetin engellenmesi riski stratejik bir baskı oluşturmaktadır.

Sofistike Siber Güvenlik Tehditleri



Finans ekibi güvenliği ve WormGPT gibi araçlar, finansal ekipleri Voice cloning (ses klonlama) ve WormGPT gibi araçlar, finansal ekipleri hedef alan "hiper-gerçekçi" sosyal mühendislik saldırılarını ve milyonlarca dolarlık dolandırıcılık vakalarını kolaylaştırmaktadır.

3. Boyut: Hükümetler (Yeni Gerçekler)

Kamu Hizmetlerinde Vatiler ve Tehlikeler



Estonya ve Singapur gibi başarı örneklerinin yanı sıra, New York'taki belediye sohbet robotunun vatandaşlara yasa dışı tavsiyeler vermesi gibi vakalar kontrolsüz kullanımın riskini göstermektedir.

Ulusal Güvenlik ve Silah Sistemleri



Ölümçül Otonom Silah Sistemleri (LAWS) üzerindeki denetim ihtiyacı artmakta, hükümetler bu sistemlerin etik ve yasal çerçevesini belirlemek için baskı altında kalmaktadır.

Yönetişindeki Kritik Uzmanlık Açığı



Derin teknik uzmanlığın büyük oranda özel sektörde yoğunlaşması, devletlerin yapay zekâyı etkili bir şekilde denetlemesini ve kamu yararını korumasını zorlaştırmaktadır.

NotebookLM

Yapay Zekâ'nın geleceği; çığır açan hukuki uyuşmazlıklar, gelişen yasal ve idari düzenlemeler ve durmak bilmeyen inovasyon arasındaki dinamik etkileşim tarafından şekillendirilmektedir. Bu yeni çağda başarılı olmak, tüm paydaşların bu üç güç arasında stratejik bir denge kurmasını ve Yapay Zekâ'nın gücünü insan hakları ve demokratik değerlerle uyumlu hale getirme konusunda sarsılmaz bir kararlılık göstermesini gerektirecektir.



Türkiye Bilişim Vakfı
www.tbv.org.tr

ÖNSÖZ: Yapay Zeka ile Geleceği Yeniden Tasarlamak – Fırsatlar ve Potansiyel

Risk yönetimi ve etik yönetim, bir kurumun savunma hattıdır. Ancak bu savunma hattını kurmamızın temel nedeni, korumaya değer muazzam bir değer ortada olmasıdır. Elinizdeki rapor, Yapay Zeka'nın (YZ) getirdiği riskleri ve sorumlulukları derinlemesine incelerken, bu teknolojinin insanlık ve küresel ekonomi için sunduğu tarihi fırsatları da göz ardı etmemektedir.

Dünyanın önde gelen yönetim danışmanlığı şirketlerinin projeksiyonları, YZ'nin sadece bir verimlilik aracı olmadığını; iş yapış biçimlerini, ekonomik büyümeyi ve toplumsal refahı kökten dönüştürecek bir "kaldıraç" olduğunu kanıtlar niteliktedir.

1. McKinsey & Company: 4,4 Trilyon Dolarlık Yeni Bir Ekonomi

McKinsey'nin analizleri, Üretken YZ'nin (Generative AI) küresel ekonomi üzerindeki etkisinin, tarihteki en büyük teknolojik sıçramalardan biri olabileceğini göstermektedir.

- **Ekonomik Katma Değer:** McKinsey araştırmalarına göre, Üretken YZ'nin küresel ekonomiye yıllık **2,6 trilyon ila 4,4 trilyon dolar** arasında bir değer katması beklenmektedir. Bu rakam, Birleşik Krallık'ın 2021 yılındaki tüm GSYİH'sından (3,1 trilyon dolar) daha büyüktür. Bu etki, YZ'nin genel ekonomik etkisini %15 ila %40 oranında artıracak bir potansiyele işaret eder.
- **Dört Temel Odak Alanı:** Yaratılacak bu devasa değer yaklaşık %75'inin dört ana fonksiyonda yoğunlaşacağı öngörülmektedir: **Müşteri Operasyonları, Pazarlama ve Satış, Yazılım Mühendisliği ve Ar-Ge.** Bu alanlara yatırım yapan kurumlar, sadece maliyet avantajı değil, gelir artışında da aslan payını alacaktır.
- **Üretkenlik Artışı ve Otomasyon:** YZ'nin iş gücü verimliliğini 2040 yılına kadar yıllık **%0,1 ila %0,6** oranında artırması beklenmektedir. Daha da çarpıcı olanı, bugünkü iş aktivitelerinin yarısının otomasyona devredilme sürecinin, önceki tahminlerden on yıl önceye, **2045 yılına** çekilmiş olmasıdır.
- **2025 Trendi - Ajan YZ (Agentic AI):** McKinsey, 2025 itibarıyla YZ'nin sadece "içerik üreten" (chat) bir yapıdan, otonom kararlar alıp aksiyon alan "**Ajanlara (Agents)**" dönüşeceğini ve bunun kurumsal inovasyonun ana motoru olacağını vurgulamaktadır.

2. Bain & Company: Deneden Değere Dönüşüm

Bain & Company'nin vizyonu, şirketlerin YZ ile "oyun" aşamasını geçip, artık "para kazanma" ve "değer yaratma" dönemine girdiği üzerinedir.

- **Somut Değer Dönemi:** 2024 yılı bir "tanışma ve deney" yılı iken, 2025 ve sonrası, şirketlerin YZ yatırımlarından **somut ticari geri dönüşler (ROI)** almaya başladığı dönem olarak tanımlanmaktadır. Özellikle B2B sektörlerde YZ, satış ve ticari mükemmeliyet süreçlerinin merkezine oturmuştur.



Türkiye Bilişim Vakfı
www.tbv.org.tr

- **Stratejik Ayrışma:** Bain, YZ'yi sadece bir teknoloji trendi olarak değil, "çağın belirleyici yıkıcısı" olarak görmektedir. Teknoloji devleri ve YZ'yi erken benimseyenler, pazar değerinin büyük kısmını kendilerinde toplayarak makası açmaktadır.
- **İş Gücü Dönüşümü:** YZ, çalışanların yerini almaktan ziyade, onların kapasitesini artıran bir güç çarpanı olarak konumlanmaktadır. Bain analizleri, YZ araçlarının yazılım geliştirme ve müşteri hizmetleri gibi alanlarda çalışanların rutin iş yükünü hafifleterek, onları daha stratejik ve yaratıcı görevlere odaklanmaya teşvik ettiğini göstermektedir.

3. KPMG: Liderlerin Güven Limanı ve Sürdürülebilirlik

KPMG'nin küresel araştırmaları, iş dünyası liderlerinin YZ'ye olan güveninin arttığını ve teknolojinin sadece kâr değil, "amaç" odaklı da kullanılabileceğini ortaya koymaktadır.

- **CEO Güveni ve Yatırım İştahı:** KPMG'nin "2025 Global CEO Outlook" raporuna göre, liderlerin %74'ü kurumlarının YZ'nin gelişim hızına ayak uydurabileceğine inanmaktadır. CEO'lar, ekonomik belirsizliklere rağmen YZ ve yetenek gelişimine yapılan yatırımları kesmemekte, aksine artırmaktadır.
- **Sürdürülebilirlik İçin YZ:** YZ sadece finansal tabloları değil, gezegenin geleceğini de iyileştirmektedir. Liderler, YZ'yi **dekarbonizasyon ve sürdürülebilirlik** hedeflerine ulaşmak için kritik bir araç olarak görmekte; özellikle veri kalitesini artırma ve raporlama süreçlerinde YZ'den faydalanmaktadır.
- **Sektörel Derinleşme:** Sağlık sektörü gibi hayati alanlarda YZ'nin etkisi somutlaşmıştır. KPMG raporları, sağlık yöneticilerinin %65'inin YZ'nin sektörde dönüştürücü bir etki yarattığını ve rekabet avantajı sağladığını belirttiğini aktarmaktadır.

"Derinleşen Dönüşüm: Otonomi, İş Gücü ve ROI Paradoksu"

4. Accenture: Otomasyondan "Otonomiye" Geçiş

Accenture'ın "**Technology Vision 2025**" raporu, YZ'nin sadece işleri hızlandıran bir yardımcı pilot olmaktan çıkıp, kendi kendine karar alabilen bir "otonom acente"ye (agent) dönüştüğü yeni bir çağı müjdelemektedir.

- **Reinvention (Yeniden İcat) Stratejisi:** Accenture, YZ'yi sadece bir teknoloji katmanı olarak değil, iş süreçlerinin "yeniden icadı" olarak tanımlar. 2025 mali yılında üretken YZ gelirlerinin **üç katına çıkarak 2,7 milyar dolara** ulaşması, şirketlerin artık deneme yanılma aşamasından çıkıp, YZ'yi operasyonel omurganın bir parçası haline getirdiğini kanıtlamaktadır.
- **Otonomi Çağı:** Rapordaki en çarpıcı vizyon, odak noktasının "insan destekli otomasyon"dan, görevleri bağımsız olarak yerine getirebilen "**otonom sistemlere**" kaymasıdır. Bu sistemler, sadece komutları yerine getirmekle kalmayıp, karmaşık veri yığınları arasında proaktif kararlar alarak verimlilikte **%20'ye varan** artışlar öngörmektedir.



Türkiye Bilişim Vakfı
www.tbv.org.tr

5. Deloitte: Yatırım ve Geri Dönüş (ROI) Paradoksu

Deloitte'un "State of Generative AI in the Enterprise 2025" raporu, YZ yatırımlarındaki iştah ile finansal geri dönüşler arasındaki hassas dengeye parmak basmaktadır.

- **Yatırım İştahı ve Sabır Sınavı:** Kurumların %91'i YZ yatırımlarını artırmayı planlasa da, bu yatırımların finansal geri dönüş süresi (ROI) uzamaktadır. Deloitte analizlerine göre, projelerin sadece %13'ü ilk 12 ayda somut getiri sağlamaktadır. Bu durum, YZ'nin kısa vadeli bir "yara bandı" değil, uzun vadeli bir "stratejik dönüşüm" aracı olarak görülmesi gerektiğini ortaya koymaktadır.
- **Siber Güvenlikte Erken Zafer:** İlginç bir şekilde, YZ'nin en hızlı ve somut ROI sağladığı alanların başında **Siber Güvenlik** gelmektedir. Gelişmiş tehdit algılama sistemleri, diğer iş birimlerine kıyasla beklentileri aşan bir performans sergilemektedir.

6. PwC: "Beceriler Depremi" ve İnsan Değerinin Artışı

PwC'nin "2025 Global AI Jobs Barometer" çalışması, YZ'nin işsizliğe yol açacağı korkusuna veriye dayalı, iyimser bir yanıt vermektedir: YZ insanı gereksizleştirmiyor, aksine yetkin insanı daha değerli kılıyor.

- **Maaş Primi ve Verimlilik:** YZ'ye en çok maruz kalan sektörlerde, çalışan başına düşen gelir artışı diğer sektörlerle göre **3 kat daha yüksektir**. Daha da önemlisi, YZ becerilerine sahip çalışanlar, küresel ölçekte %25 ila %56 arasında değişen oranlarda daha yüksek maaş (wage premium) almaktadır.
- **Becerilerde Hızlı Değişim:** PwC bunu bir "Beceriler Depremi" olarak adlandırmaktadır. YZ odaklı rollerde talep edilen beceriler, diğer işlere kıyasla %66 daha hızlı değişmektedir. Bu veri, YZ çağında en büyük riskin "iş kaybemek" değil, "öğrenmeyi bırakmak" olduğunu net bir şekilde göstermektedir.
- **GSYİH Etkisi:** PwC projeksiyonları, YZ adaptasyonunun 2035 yılına kadar küresel GSYİH'ye %15 oranında (yaklaşık 15,7 trilyon dolar) ek katkı sağlayacağını öngörmektedir.

Sonuç: Fırsatları Yönetmek

Bu veriler ışığında görülmektedir ki; Yapay Zeka bir tercih değil, bir zorunluluktur. Ortadaki ekonomik pasta ve verimlilik potansiyeli, hiçbir kurumun veya devletin görmezden gelemeyeceği kadar büyüktür.

Ancak, **"Güç, kontrolsüzse güç değildir."**

Önemli Not : Danışmanlık ve araştırma kuruluşlarının 2026 senesi raporları yayınlandıkça rapordaki 2025 verileri ile değişimi daha net ortaya koymak adına güncelleme yapmak yerine kapsamlı bir kıyaslama çıktısını ayrıca buraya eklemeyi uygun gördük. Bu yaklaşımlar beklentilerin senelik değişimini de aktarmayı hedefledik. Aşağıda ana bölümün ön bölümüne içeriği ekliyoruz :



Türkiye Bilişim Vakfı
www.tbv.org.tr

KÜRESEL YAPAY ZEKÂ METRİKLERİ DEĞİŞİM VE GÜNCELLEME RAPORU (2025-2026)

1. McKinsey & Company: Ekonomik Etki ve Ajan Yapay Zekâ Evrimi

- **Rapordaki Önceki Veri (2025):** Üretken YZ'nin küresel ekonomiye yıllık potansiyel katkısı **4.4 Trilyon \$**. 2025 trendi olarak YZ'nin içerik üretmekten otonom kararlar alan "Ajan YZ" mimarilerine geçiş dönemi.
- **2026 Güncellemesi:** McKinsey'nin "State of AI Trust in 2026: Shifting to the Agentic Era" raporuna göre, YZ artık deneysel veya sadece "içerik üreten" bir araç olmaktan tamamen çıkmış; şirketlerin ana iş akışlarına entegre olan "**Ajan Yapay Zekâ**" (**Agentic AI**) dönemine resmen geçiş yapmıştır. 2026 yılında odak noktası finansal pasta büyüklüğünden ziyade, bu ajanların "hata yapması veya kontrolden çıkması" riskine (Sorumlu Yapay Zekâ - RAI) kaymıştır. Rapor, YZ yönetişimine ve RAI süreçlerine **25 Milyon \$ veya daha fazla yatırım yapan öncü kurumların, YZ yatırımlarından %5'in üzerinde net EBIT (Faiz ve Vergi Öncesi Kâr) etkisi** gibi çok somut finansal geri dönüşler almaya başladığını doğrulamaktadır.

2. PwC: Küresel GSYİH ve İş Gücü Piyasası

- **Rapordaki Önceki Veri (2025):** 2035'e kadar YZ adaptasyonunun Küresel GSYİH'ye ek etkisi **%15**. IMF'nin küresel büyüme öngörüsü ise **%3.1**.
- **2026 Güncellemesi:** PwC'nin "Global Economic Outlook 2026" modellemelerine göre, YZ'nin küresel ekonomiye 2030 yılına kadar yapacağı toplam katkı revize edilerek **15.7 Trilyon \$** olarak netleştirilmiştir. PwC, 2026 yılı küresel GSYİH büyüme tahminini **%3.1** olarak korurken, YZ'ye en açık sektörlerde verimlilik artışının yanı sıra "iki vitesli bir iş gücü piyasası" oluştuğunu belirtmektedir. PwC 2026 YZ İstihdam Barometresi, YZ yetkinliklerine sahip çalışanların **%25 ila %56 arasında değişen oranlarda "maaş primi" (wage premium)** almaya devam ettiğini ve YZ yatırımı yapan şirketlerin istihdamı ve ücretleri diğer kurumlara kıyasla çok daha hızlı artırdığını göstermektedir.

3. Deloitte: Yatırım ve ROI Paradoksunda Kırılma

- **Rapordaki Önceki Veri (2025):** Kurumların **%91'i** YZ'ye yatırım yapıyor ancak sadece **%13'ü ilk 12 ayda somut getiri (ROI) alabiliyor**.
- **2026 Güncellemesi:** Deloitte'un "The State of AI in the Enterprise 2026" küresel raporu, pilot aşamalardan **büyük ölçekli üretime (scale) geçişte sarsıcı bir hızlanma** olduğunu ortaya koymaktadır.
 - Çalışanların yapay zekâya erişimi bir yılda **%50 artmıştır**.
 - "**ROI Paradoksu**" **Aşılıyor:** Kurumların YZ deneylerini doğrudan canlı üretim ortamına (production) taşıma oranı dramatik bir sıçrama göstermiştir. Bugün şirketlerin **%25'i** YZ projelerinin en az **%40'ını** canlıda çalıştırırken, bu oranın önümüzdeki 6 ay içinde **%54'e çıkması (ikiye katlanması)** beklenmektedir.

- **Ancak gelir etkisi hala zamana ihtiyaç duymaktadır: Şirketlerin %74'ü gelecekte YZ ile gelir büyümeyi hedeflerken, hali hazırda bunu finansal tablolarına anlamlı ciro artışı olarak yansıtabilenlerin oranı %20 seviyesindedir.**

4. Accenture: Otomasyondan "Ajan Zorunluluğuna" Geçiş

- **Rapordaki Önceki Veri (2025): Üretken YZ yatırımları ile 2025'te beklenen 3 kat gelir artışı.**
- **2026 Güncellemesi:** Accenture'ın "Pulse of Change 2026" ve "Agentic Imperative 2026" raporları, iş dünyası liderlerinin odağının maliyet tasarrufundan doğrudan gelir üretimine döndüğünü göstermektedir.
 - **Üst düzey yöneticilerin (C-Suite) %86'sı 2026 yılında da YZ yatırımlarını artırmayı planlamaktadır.**
 - **Liderlerin %78'i artık yapay zekâyı bir maliyet kısma aracı (cost reduction) olarak değil, doğrudan ciro ve gelir artırıcı (revenue growth) bir kaldıraç olarak görmektedir (bu oran 2024'te %65 seviyesindeydi).**
 - **Ajan Entegrasyonu:** Accenture verilerine göre, yapay zekanın iş süreçlerini etkileme kapasitesi muazzam bir eşiği geçmiştir. Örneğin, İngiltere'deki toplam çalışma saatlerinin YZ tarafından asiste edilme veya otonom yürütülme potansiyeli **%47'den %82'ye yükselmiştir**. Hali hazırda çalışanlar, toplam mesailerinin **%21'ini doğrudan frontier (ileri seviye) YZ yetenekleriyle ortaklaşa yürütmektedir.**

Özet Değerlendirme Matrisi

Küresel Yapay Zekâ Metrikleri: 2025 Öngörülleri vs. 2026 Gerçekleri

Yapay zekâ dünyasındaki beklentilerin (2025 projeksiyonları) bir yıl içinde nasıl somut operasyonel gerçeklere (2026 güncellemeleri) dönüştüğünü gösteren karşılaştırmalı analiz.

	2025 PROJEKSİYONU (Eski Veri)	2026 GÜNCELLEMESİ (Yeni Gerçeklik)
MCKINSEY (Stratejik Odak)	<p>4.4 Trilyon \$ potansiyel pazar / Teorik ajan geçişi</p> <p>İçerik Üretim Potansiyeli</p> <p>► YZ'nin içerik üretme potansiyeline odaklanılır.</p>	<p>Ajan Yapay Zekâ Dönemi</p> <p>RAI (Sorumlu YZ) ve hesap verebilirlik odaklı yönetim.</p> <p>↑ %5+ EBIT Sorumlu YZ (RAI) Yatırımlarının Getirisi. Yönetişim ve RAI süreçlerine 25 Milyon \$ veya daha fazla yatırım yapan öncü kurumlar, net kârlarında artış gördü.</p>
PWC (Ekonomik Katkı ve İş Gücü Piyasası)	<p>%15 GSYİH ek etkisi / %25-56 maaş primi</p> <p>► 2030 yılına kadar YZ'nin küresel ekonomiye yapacağı toplam katkı revize edilerek netleştirildi.</p>	<p>15.7 Trilyon \$ Küresel Etki</p> <p>Kalıcı maaş primi ve iki vitesli istihdam piyasası. 2036 büyüme tahmini %3.1 olarak korundu.</p> <p>Kalıcı Maaş Primi Etkisi</p> <p>YZ yetkinliği olan çalışanlar maaş primi almaya devam ediyor.</p>
DELOITTE (ROI Paradoxu ve Uygulama Hızı)	<p>%13 kurumda somut ROI.</p> <p>► Kurumların sadece %13'ü somut getiri alabildi.</p>	<p>Canlıya Geçiş Hızı</p> <p>%54 Canlıya Geçiş</p> <p>Projeleri üretime taşıma hedefi 6 ayda ikiye katlanıyor. Projeleri canlı üretime taşıma oranı %25'ten %54'e çıkması bekleniyor.</p> <p>%50 YZ Erişimi Bir Yılda Arttı</p> <p>Şirketlerin %20'si hali hazırda YZ'yi finansal tablolarına anlamlı ciro artışı olarak yansıtmayı başardı.</p>
ACCENTURE (Yatırım İştahı ve Verimlilik)	<p>3 kat ciro artışı beklentisi ve denemeler.</p> <p>► 2024'te liderlerin %65'i YZ'yi doğrudan ciro artırıcı bir kaldıraç olarak görüyordu.</p>	<p>Gelir Üretim Odaklılık</p> <p>%78 Gelir Odaklılık</p> <p>Liderlerin %78'i artık YZ'yi doğrudan ciro artırıcı bir kaldıraç olarak görüyor. ana motor ciro artışı.</p> <p>%86 Yatırımları Artırma Kararlılığı</p> <p>Üst düzey yöneticilerin (C-Suite) büyük çoğunluğu, 2026 yılında da YZ yatırımlarını artırmayı planlıyor.</p>

NotebookLM



Türkiye Bilişim Vakfı
www.tbv.org.tr

Yapay Zekâ: Hızlandırılmış Dönüşüm Çağında Yönetişim, Etik. Risk ve Hukuk

1. Giriş: Yapay Zekâ Ortamının Yeni Gerçekliklerinde Yol Almak

1.1 Bağlamsal Güncelleme: Dönüştürücü Potansiyelden Somut Etkiye

Yapay Zekâ dönüştürücü potansiyele sahip bir teknolojiden, somut ve çoğu zaman yıkıcı, gerçek dünya etkisine sahip bir teknolojiye hızla evriliyor. ¹ Geçtiğimiz birkaç ay, özellikle büyük ölçekli üretken modeller olmak üzere, Yapay Zekâ yeteneklerinin deneysel gösterimlerden, temel iş, hükümet ve toplumsal işlevlerin derinlemesine entegre bileşenlerine taşındığı derin bir hızlanma dönemine işaret etti. ³ Tartışma artık Yapay Zekâ'nın ne olduğu üzerine yoğunlaşmıyor.

Geçmişte, “*yapabilirdi*” dense de; şu anda yaptıkları ile endüstrileri yeniden şekillendiriyor, bilgi ekosistemlerini değiştiriyor ve hem eşi benzeri görülmemiş fırsatlar hem de ciddi zorluklar sunuyor.

Bu yeni dönemin belirleyici özelliklerinden biri, teknoloji benimseme ve risk tezahürü döngülerinin çarpıcı biçimde sıkıştırılmasıdır. Tarihsel olarak, yeni bir teknolojinin kullanıma sunulması ile ilişkili risklerin yaygın olarak gerçekleşmesi arasında önemli bir gecikme olmuştur. Üretken Yapay Zekâ bu döngüyü yıllardan aylara indirmiştir. Deepfake teknolojisinin niş bir yenilikten milyonlarca dolarlık kurumsal dolandırıcılığı kolaylaştırabilen bir araca dönüşmesindeki hızlı yolculuğu, bu olgunun çarpıcı bir örneğidir. ⁶ Bu hızlandırılmış zaman çizelgesi, inovasyon, benimseme, risk keşfi ve düzenleyici müdahalenin ardışık aşamalar olmadığı, kaotik ve yüksek hızlı bir paralellik içinde gerçekleştiği anlamına gelir. Oluşan bu sıkıştırma, genellikle yavaş hareket eden ve müzakereci olan **geleneksel yönetim çerçeveleri üzerinde muazzam bir baskı oluşturmakta ve daha çevik, proaktif ve teknik olarak bilgilendirilmiş gözetim modellerine doğru köklü bir geçişi gerektirmektedir.**¹

Hızlı ve zaman zaman öngörülemez evrim, belirsizlik altında düzenleme yapmak zorunda olan politika yapımcılar için derin bir zorluk yaratmaktadır. ⁴⁹ Stanford Siber Politika Merkezi'nin yakın tarihli bir raporunda vurgulandığı gibi, yasa yapımcılar zor bir seçimle karşı karşıyalar: “**Her varsayımsal riski azaltmak için agresif bir şekilde hareket etmek inovasyonu engelleyebilirken, çok muhafazakâr davranmak, teknolojiyi öngörülebilir zararlardan uzaklaştırma şansını kaçırmak anlamına da gelebilir**”. ⁴⁹ Bu ikilem, hükümet politikasının teknolojik gelişimin hızlı temposunun gerisinde kalması ve tüm riskleri ve faydaları hala keşfedilmekte olan bir teknolojinin nasıl yönetileceği konusunda küresel bir politika tartışmasını zorlaması gerçeğiyle daha da kötüleşiyor. ⁴⁹

Bu noktada, daha çevik bir yaklaşımın —hızla gözlemlene, değerlendirme, eleştirme, potansiyel taşıyorsa üzerine gitmenin kaçınılmaz hâle geldiği görülüyor. Böyle bir kademeli izleme ve öğrenme mekanizması, yüksek belirsizlik altında karar vermek zorunda olan kurumların ve politika yapımcıların, hızla değişen bu ortamda daha etkin, esnek ve sürdürülebilir bir duruş sergilemesini sağlayacaktır.



Türkiye Bilişim Vakfı
www.tbv.org.tr

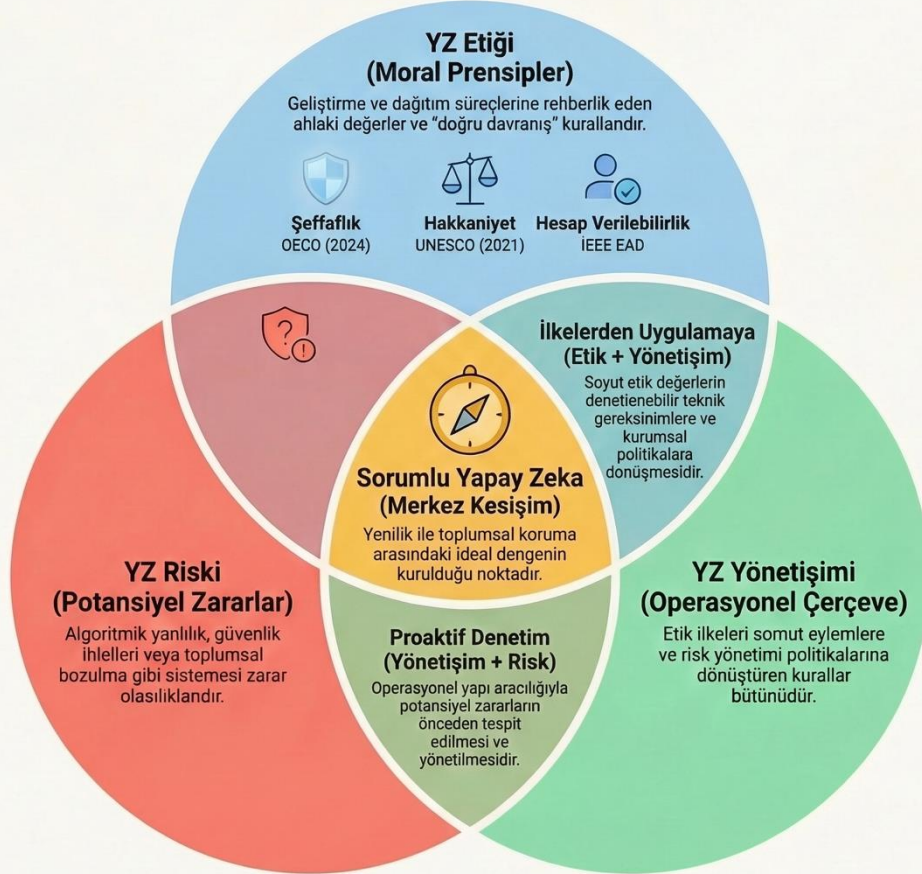
1.2 Üretken Çağ için Temel Kavramların Geliştirilmesi

Üretken Yapay Zekâ sistemleri getirdiği yeni karmaşıklıkları kapsayacak şekilde güncellenmeli ve gelecek planları da ona göre şekillendirilmelidir.

- **Yapay Zekâ Yönetimi:** Bu kavram artık belirli ve dar kapsamlı Yapay Zekâ uygulamaları için statik bir dizi yönergenin ötesine geçmelidir. Temel modeller ve aracı Yapay Zekâ sistemleri gibi hızla gelişen teknolojileri denetlemek için gereken dinamik ve uyarlanabilir süreçleri de kapsayacak şekilde gelişmelidir. ⁴ Zorluk artık yalnızca ayrı uygulamaları yönetmekle sınırlı değil, sayısız uygulamanın ortaya çıktığı ve temellerini oluşturan genel amaçlı platformları da kapsamaktadır. **Yapay Zekâ yönetimi, soyut etik ilkelerin Yapay Zekâ risklerini yönetmeyi amaçlayan somut eylemlere dönüştürüldüğü operasyonel çerçevedir; yapı ve süreçlerdir.**

1

Güvenilir Yapay Zekanın Anatomisi: Etik, Risk ve Yönetişim



YZ sistemleri, insan mühendisliği ve verilerin bir ürünü olduğu için insan hatalarını ve yanlılıklarını miras alabilir. Bu karmaşık yapıyı yönetmek için etik ilkeler bir pusula görevi görürken, yönetim çerçeveleri bu ilkeleri riskleri azaltacak somut politikalara dönüştürür.

© NotebookLM

- **Yapay Zekâ Etiği:** Uygulamalı etiğin bir dalı olan bu alan, artık üretken Yapay Zekâ'nın tetiklediği daha derin zorluklarla başa çıkmak zorunda. Tartışma; karar alma sistemlerindeki hakkaniyet ve önyargıdan, yazarlık hususiyeti, veri setleri oluşturmak için telif haklarıyla korunan geniş veri kümelerini toplamada karşılaşılan etik ve hukuki sorunlara ve hatta aşırı kişiselleştirilmiş, sentetik içerik aracılığıyla kitlesel psikolojik manipülasyon potansiyeli taşıyan uygulamaların ortaya çıkardığı sorunlara doğru genişliyor. ⁹
- **Yapay Zekâ'nın Ortaya Çıkardığı Riskler:** Yapay Zekâ risk yelpazesi, son aylarda belirginleşen yeni zararlar ortaya çıkarma potansiyeline sahip uygulamaların risklerini de açıkça içerecek şekilde önemli ölçüde genişlemektedir. Bu riskler arasında, demokratik süreçleri etkileyebilecek, gerçeğe aşırı yakın dezenformasyon üretimi, deepfake tabanlı sosyal mühendislik gibi yeni siber güvenlik vektörlerinin



Türkiye Bilişim Vakfı
www.tbv.org.tr

oluşturulması ve endüstriyel ölçekte sistemik fikri mülkiyet (FM) ihlali potansiyelleri yer alıyor. ⁶ Bu riskler ana başlıklar olarak teknik arızalardan, güvenlik açıklarından, etik hatalardan, tasarım aşamasında teknik normlara uyulmamasından veya toplumsal bağlam eksikliğinden kaynaklanmakta ve daha kapsamlı bir yönetim yaklaşımı ihtiyacını doğurmaktadır. ¹

2. Temel Yapay Zekâ Etiği ve Yönetişim Çerçevesinin Evrimi

2.1 2024 OECD Yapay Zekâ İlkeleri: Yeni Bir Tehdit Ortamına Uyum Sağlama

Hızla değişen teknolojik ve politik ortama yanıt olarak, Ekonomik İşbirliği ve Kalkınma Örgütü (OECD), Mayıs 2024'te etkili Yapay Zekâ İlkelerini güncellemiştir. ¹³ Bu güncellemeler, üretken Yapay Zekâ'nın ortaya çıkardığı yeni tehditlere doğrudan bir politika tepkisini yansıtmaktadır. Revizyonlar, kapsayıcı büyüme ve refah ilkesine "çevresel sürdürülebilirlik" ifadesinin eklenmesi (İlke 1.1) gibi belirli metinsel değişiklikleri de içermektedir. ¹⁵ Daha da önemlisi, çerçeve artık açıkça "Yapay Zekâ tarafından güçlendirilen yanlış bilgi ve dezenformasyonun ele alınması" (İlke 1.2) ve "bilgi bütünlüğünün" (İlke 1.4) güçlendirilmesi çağrısında bulunmaktadır; bu da, Yapay Zekâ kaynaklı seçim müdahalelerinde ve kötü amaçlı deepfake'lerde belgelenen artışın açık bir kabulüdür. ¹⁴

Belki de en önemli değişiklik kavramsal ve yapısal bir değişiklik olarak görülebilir; "risk yönetimine ilişkin hükümlerin "Sağlamlık, Güvenlik ve Emniyet" ilkesinden "Hesap Verebilirlik" ilkesine (İlke 1.5) taşınmış olması" önemli bir gelişmedir. ¹⁴ Bu güncellenmiş hesap verebilirlik ilkesi, işgücü ve fikri mülkiyet haklarıyla ilgili riskleri de açıkça kapsayacak şekilde genişletilmiştir. ¹⁴ Yaklaşım, yalnızca bir kategorizasyon olarak görülmemelidir; risk yönetiminin güvenli sistemler kurma konusunda teknik bir uygulama olmaktan ziyade, tüm Yapay Zekâ aktörlerinin temel bir yönetişim ve hesap verebilirlik yükümlülüğü olarak derinlemesine olarak yeniden çerçevelenmesini temsil eder. Bahis konusu değişim, son zamanlarda artan dava ve rekabet hukuku soruşturmalarıyla da kanıtlandığı gibi, kurumsal aktörleri Yapay Zekâ sistemlerinin aşağı yönlü sonuçlarından doğrudan sorumlu tutmayı amaçlayan daha geniş bir yasal ve toplumsal eğilimle de uyumludur. ⁹

OECD'nin güncellemesi, kuruluşlara risk yönetiminin artık hesap verebilir olmakla eş anlamlı olduğunu ve bunun yasal sorumluluk, gerekli özeni gösterme gereklilikleri ve kurumsal yönetim yapıları üzerinde doğrudan etkileri olduğunu göstermektedir.

2.2 IEEE'nin "Küresel Girişim 2.0": Proaktif Güvenliğe Doğru Bir Paradigma Değişimi

Etik Uyumlu Tasarım (EAD) çerçevesi pratik Yapay Zekâ etiğinin temel taşlarından biri olan Elektrik ve Elektronik Mühendisleri Enstitüsü (IEEE) yaklaşımını geliştirmiştir. ¹⁹ Yeni "Küresel Girişim 2.0", Yapay Zekâ sistemlerinin tasarımına ve yaşam döngüsüne proaktif bir şekilde "Önce Güvenlik İlkesi" yerleştirmek için "Yapay Zekâ Yönetiminde Risk Çerçevelemesinin Ötesine" geçmeyi amaçlayan önemli bir kavramsal değişimi işaret etmektedir. ⁴ Bu yaklaşım; reaktif risk azaltmadan, tasarıma dayalı güvenliğe yönelik daha temel, proaktif bir düzenlemeye doğru bir geçişi temsil etmektedir.



Türkiye Bilişim Vakfı
www.tbv.org.tr

Bu yenilenen değerlendirme, üretken Yapay Zekâ ve büyük dil modellerinin ortaya koyduğu benzersiz zorlukları kabul ederek, bu teknolojileri özel olarak hedefleyen yeni bir standart oluşturmaya yönelik bir araştırma duyurusunda bulunmaktadır. ⁴ Ayrıca, çeşitli endüstriyel firmalar ve kamu sektörleri için pratik "Araç Setleri" geliştirmeyi planlayarak, IEEE, üst düzey ilkeler ile mühendislik pratiğindeki somut uygulamaları arasındaki kalıcı boşluğu kapatmak için doğrudan bir girişimde bulunmaktadır. ⁴

2.3 UNESCO'nun Küresel Uygulamaya Yönelik Çalışmaları

Birleşmiş Milletler Eğitim, Bilim ve Kültür Örgütü (UNESCO), bu alandaki ilk küresel standart belirleme aracı olan 2021 Yapay Zekâ Etiği Tavsiyesi'ni aktif olarak somut eyleme dönüştürüyor. ¹ 2025 yılında düzenlenen 3. Küresel Yapay Zekâ Etiği Forumu, etiğin inovasyonun önünde bir engel değil, aksine ilerlemesinde etkili olduğunu vurgulayarak bu çabada önemli bir dönüm noktası oldu. ²¹

Forumda, küresel koordinasyonu teşvik etmek ve ilkelerden pratiğe geçmek için iki temel kurumsal mekanizma başlatıldı. Ulusal düzenleyicilerle geliştirilen **Yapay Zekâ Denetleme Kurumları Küresel Ağı , bilgi paylaşımını ve politika uygulama kapasitesini geliştirmeyi amaçlıyor.** ²¹ Eş zamanlı olarak, **Sivil Toplum ve Akademisyenlerin Küresel Ağı**, dünya çapında Yapay Zekâ ile ilgili karar alma süreçlerine geniş çaplı vatandaş katılımını desteklemek amacıyla kurulmuştur. ²¹ Bu girişimler, şu anda 70'ten fazla ülkede kullanılan ve son zamanlarda ASEAN bölgesine odaklanan UNESCO Hazırlık Değerlendirme Metodolojisi'nin (RAM) genişleyen uygulamasıyla tamamlanmaktadır. Bu metodoloji, küresel etik çerçevelerin yerel politika gerçekleri ve kapasite geliştirme çabalarıyla temellendirilmesine yardımcı olmaktadır. ²¹

2.4 İlkeler-Uygulama Açığı: Derinleşen Bir Uçurum

Çerçeve evrimi ve uygulamasındaki bu olumlu gelişmelere rağmen, etik ilkeleri dile getirmek ile bunları pratiğe etkili bir şekilde yerleştirmek arasındaki uçurum kritiktir ve bazı alanlarda giderek büyüyen bir zorluk olmaya devam etmektedir. ¹ Bu durum, Açıklanabilir Yapay Zekâ (XAI) üzerine yakın zamanda yapılan geniş çaplı bir akademik literatür analiziyle çarpıcı bir şekilde ortaya konmuştur.

18.000'den fazla makaleyi inceleyen çalışma, Yapay Zekâ kararları için insan tarafından anlaşılabilir açıklamalar sunduğunu iddia edenlerin %1'inden azının, bu iddialarını deneysel insan denek çalışmalarıyla doğruladığını tanımlamaktadır. ²⁵

Mevcut tanımlama şeffaflık gibi ilkeler için önerilen teknik çözümler ile gerçek dünyadaki faydaları arasında var olabilecek kopukluğun ciddi bir hatırlatıcısıdır. **Teknik araştırmanın hayati önem taşıdığını, ancak tek çözüm olamayacağını vurgular. "Kara kutu" sorunu yalnızca teknik bir sorun değil; sosyo-teknik bir sorundur. Bu gerçeklik, salt algoritmik çözümlere yönelik iyimserliği yumuşatır ve sorumlu bir Yapay Zekâ yönetim rejiminde sağlam prosedürel güvencelerin, bağımsız denetimlerin ve anlamlı insan gözetiminin tartışılmaz önemini pekiştirir.**

Bu tabloyu daha da karmaşıklaştıran bir faktör ise üretken Yapay Zekâ'nın deterministik olmayan doğasıdır. Aynı model, aynı temel soruya — hatta aynı veri setine — yalnızca farklı sistem yönergeleri, prompt mühendisliği varyasyonları veya tek örnekle öğrenme (one-shot learning) tetikleyicileri nedeniyle birbirinden



Türkiye Bilişim Vakfı
www.tbv.org.tr

önemli ölçüde farklı çıktılar verebilmektedir. Bu durum, karar alma süreçlerinde öngörülebilirlik, tutarlılık ve hesap verebilirlik gibi temel yönetim prensiplerini zorlamaktadır. Kurumların “aynı soruya aynı cevabı verme” beklentisine dayalı iş akışları ve regülasyon mekanizmaları, üretken modellerin olasılık temelli yapısı nedeniyle kırılğan hale gelmektedir. Bu öngörülemezlik, model bütünlüğü ve güvenilirlik değerlendirmelerinde yeni metodolojiler gerektirirken, aynı zamanda model çıktılarının yalnızca doğruluk açısından değil, tutarlılık ve tekrar edilebilirlik açısından da ele alınması gerektiğini açıkça göstermektedir.

2.5 Küresel Düzenleyici Yaklaşımlar: Karşılaştırmalı Bir Genel Bakış

Stanford Siber Politika Merkezi'nin analiz ettiği gibi, uluslar Yapay Zekâ'yı yönetme zorluğuyla boğuşurken küresel sahnede üç farklı model ortaya çıkmıştır. ⁴⁹ Bu yaklaşımlar, inovasyon, risk ve devlet kontrolü arasındaki dengeye dair farklı felsefeleri yansıtmaktadır.

- **ABD'nin Teşvik Edilen Öz Düzenleme Modeli:** Amerika Birleşik Devletleri, büyük ölçüde "teşvik edilen öz düzenleme" ile karakterize edilen sektöre özgü, serbest piyasa yaklaşımını benimsemiştir. ⁴⁹ **ABD hükümeti, kapsamlı ve tavandan tabana mevzuat çıkarmak yerine, büyük Yapay Zekâ şirketlerinden gönüllü taahhütler almaya ve federal kurumların kendi Yapay Zekâ yönetim önceliklerini belirlemelerine rehberlik etmek için 14110 sayılı Yürütme Emri gibi yürütme emirleri yayınlamaya odaklanmıştır.** ⁴⁹ Bu model, esnekliğe ve inovasyona öncelik vermektedir, ancak sistemik riskleri ve devam eden dijital zararları ele almakta yetersiz olduğu gerekçesiyle de eleştirilmektedir. ⁵³
- **AB'nin Kapsamlı, Eş Düzenleme Modeli:** Avrupa Birliği, Yapay Zekâ için dünyanın ilk kapsamlı, yatay yasal çerçevesini oluşturarak tam tersi bir yaklaşım benimsemiştir. ⁵⁴ **AB Yapay Zekâ Yasası, yasal gerekliliklerin bir Yapay Zekâ uygulamasının oluşturduğu risk düzeyine göre ölçeklendirildiği risk temelli, eş düzenleme modeline örnek teşkil etmektedir.** ⁵⁰ "Kabul edilemez risk" uygulamalarını yasaklamakta, "yüksek riskli" sistemlere katı yükümlülükler getirmekte ve diğerleri için şeffaflık öngörmektedir. ⁵⁴ Bu yaklaşım da temel haklara ve güvenliğe öncelik vermekle birlikte, içeriğin karmaşıklığının inovasyonu engelleyip engellemeyeceği konusunda endişelere yol açtığını belirtmek gerekmektedir ⁵⁵

Bununla birlikte, Yapay Zekâ uygulamaları sonucu üçüncü kişilerin uğradığı bedensel ve psişik zararların giderilmesini amaçlayan 2024/2853 sayılı yeni AB Yönergesi, AB Yapay Zekâ Yasası'ndan farklı olarak, Yapay Zekâ uygulamalarının riskleri arasında hiyerarşik bir sıralama yapmamış, son kullanıcıların uğradığı tüm zararların – zarar hangi tip riskin gerçekleşmesinden kaynaklanmış olursa olsun – uygulamayı piyasaya sürene yüklenmesi ilkesini kabul etmiştir. Buna göre, kontrolü altında piyasaya sürülen ve piyasaya sürüldükten sonra da gözetim, güncelleme ve geliştirme yükümlülüğü bulunan üretici, ürettiği Yapay Zekâ uygulamasının yol açtığı zararları kendisine herhangi bir kusur atfedilebilir olsun ya da olmasın gidermekle yükümlüdür. AB'de yeni kabul edilen ve Kasım 2026'da üye ülkelerde yürürlüğe girecek bu basit ama piyasa aktörlerini kusursuz sorumluluk (*strict liability*) esasına tabi tutan düzenleme ile, AB Yapay Zekâ Yasası'na getirilen karmaşıklık eleştirileri bir nebze dikkate alınmış ve daha yalın bir sorumluluk hukuku mekanizması oluşturulmuştur. Yürürlüğe girdikten sonra bu Yönerge'nin

üye ülke mahkemelerinde ve özellikle AB Adalet Divanı'ndaki uygulaması dikkatle takip edilmelidir.

- **Çin'in Devlet Merkezli, Komuta ve Kontrol Modeli:** Çin, yönetişime "komuta ve kontrol" yaklaşımını yansıtan bir dizi hedefli, dikey düzenleme uygulamaktadır. ⁴⁹ **Bu yasalar, devlete Yapay Zekâ'nın geliştirilmesi ve konuşlandırılması üzerinde önemli bir gözetim ve kontrol yetkisi vererek, teknolojiyi ulusal stratejik çıkarlar ve önceliklerle uyumlu hale getiriyor. ⁵⁵ Model, hızlı ve kararlı devlet eylemine olanak sağlıyor, ancak Batılı gözlemciler tarafından genellikle bireysel haklar ve açık inovasyon üzerinde devlet kontrolünün önceliklendirilmesi olarak görülüyor. ⁵⁴**

Tablo 1: Başlıca Çerçeveler Genelinde Temel Yapay Zekâ Etik İlkeleri

Aşağıdaki tablo, son gelişmeleri yansıtabacak şekilde güncellenen temel uluslararası çerçevelerdeki ortak temel ilkeleri özetlemektedir.

	OECD AI (2024)	IEEE EAD	UNESCO (2021)	Asilomar (2017)	AI4People (2018)
Adalet ve Ayrımcılık Karşıtlığı	Tam	Dolaylı	Tam	Dolaylı	Tam (Adalet)
Şeffaflık ve Açıklanabilirlik	Tam	Tam	Tam	Tam	Tam
Hesap Verebilirlik ve Sorumluluk	Tam	Tam	Tam	Tam	Dolaylı
Mahremiyet ve Veri Koruma	Tam	Tam (Veri Ajansı)	Tam	Tam	Dolaylı
Güvenlik ve Dayanıklılık	Tam	Tam	Tam	Tam	Tam (Zarar Vermeme)
İnsan Otonomisi ve Kontrolü	Tam	Tam	Tam	Tam	Tam (Otonomi)
İyilik / Refah / Ortak Refah	Tam	Tam	Tam	Tam	Tam

■ Tam (Koyu Renk) ■ Dolaylı (Açık Renk)

© NotebookLM

Not: "✓", ilkenin açıkça veya güçlü bir şekilde dahil edildiğini gösterir. "()", ilkenin ilgili kavramlar aracılığıyla ele alındığını gösterir. Açıklamalar, son güncellemeleri ve vurgu değişikliklerini yansıtır.

3. Boyut 1: Vatandaşlar için Yoğunlaşan Riskler ve Etik Sonuçlar

3.1 Gizliliğin Üretken Aşınması: Veri Toplamadan Gerçeklik Üretimine

Vatandaş mahremiyetine yönelik riskler, üretken Yapay Zekâ'nın yaygınlaşmasıyla önemli ölçüde evrildi. Tehdit, kişisel verilerin gizlice toplanması ve analizinden, derin ve ani zararlara yol açabilen sentetik gerçekliklerin açıkça üretilmesine kaydı. ¹ Son zamanlarda, örneğin şarkıcı Taylor Swift gibi kamuya mal olmuş kişilerin rızası olmadan, cinsel içerikli deepfake görüntülerinin oluşturulması ve yayılmasını içeren yüksek profilli olaylar bu yeni gerçeği gözler önüne seriyor. ²⁷ Bu durumlarda, **Yapay Zekâ yalnızca hassas bilgileri çıkarsamak için değil, aynı zamanda bir bireyin onurunu ve mahremiyetini taciz etmek, aşağılamak ve ihlal etmek için tasarlanmış sahte, fotoğraflar içerik üretmek için de kullanılıyor.** ²⁶ Bu tür zararlar orantısız bir



Türkiye Bilişim Vakfı
www.tbv.org.tr

şekilde kadınları ve diğer savunmasız grupları hedef alıyor; duygusal sıkıntı ve itibar zedelenmesi yaratmak için teknolojiyi silah olarak kullanıyor. ²⁶

3.2 Algoritmik Önyargı: Yeni Kanıtlar ve Genişleyen Kapsam

Algoritmik önyargının toplumsal eşitsizlikleri sürdürme riski iyi bilinse de son yaptırım eylemleri kapsamının genişlediğini ortaya koymuştur. ¹ "Kadın" kelimesini içeren özgeçmişleri cezalandırmayı öğrenen Amazon'un deneysel işe alım aracının temel vakası, tarihsel verilerde gömülü cinsiyet önyargısının önemli bir örneği olmaya devam etmektedir. ²⁹ Ancak, endişelerin artması nedeniyle 2023'te ABD Eşit İstihdam Fırsatı Komisyonu (EEOC), nörolojik olarak farklı (nörodiverjan) adayları veya engellileri sistematik ve haksız bir şekilde dışlayan Yapay Zekâ destekli tarama araçları kullanan birkaç şirkete karşı yaptırım eylemleri başlatmıştır. ²⁹ Bu vakalar, **algoritmik önyargının ırk ve cinsiyet gibi korunan özelliklerle sınırlı olmadığını, aynı zamanda bilişsel veya fiziksel engellere dayalı olarak bireyler için yapısal engeller oluşturabileceğini ve düzenleyiciler ve geliştiriciler için zorlukları genişletebileceğini göstermektedir.**

3.3 Yapay Zekâ'nın Bilgi Bütünlüğü ve Demokrasi Üzerindeki Etkisi: Teoriden Gerçeğe

Yapay Zekâ'nın "filtre balonları" yaratabileceği ve demokratik söylemi baltalayabileceği yönündeki teorik endişeler hızla somut bir gerçeklik haline gelmiştir. ¹ Son seçimler ve siyasi olaylarda, tehdidin niteliksel olarak tırmanmasını temsil eden, Yapay Zekâ destekli karmaşık dezenformasyon kampanyaları için bir deneme alanı işlevi gördüğünü de izlemiş olduk. **Önemli bir gelişme ise, basitçe yanlış anlatılar yaymaktan, güvenilir kaynakları aktif olarak taklit etmeye geçiş ve böylece toplumsal yaşamın temelini oluşturan güven duygusunun silaha dönüştürülmesidir.**

Örneğin, 2024 Tayvan başkanlık seçimleri sırasında tehdit aktörleri adayların deepfake videolarını kullandılar ve hatta Çin yanlısı dezenformasyon içeren metinleri okumak için Yapay Zekâ tarafından üretilen sanal haber sunucuları oluşturdular ve bu da sahte anlatılara bir gerçeklik görünümü kazandırdı. ¹⁷

Amerika Birleşik Devletleri'nde, Başkan Joe Biden'ın sesini ikna edici bir şekilde taklit eden Yapay Zekâ tarafından üretilen bir sesli robot arama, insanları New Hampshire ön seçimlerinde oy kullanmaktan caydırmak için kullanıldı. ²⁸ Bu olaylar yalnızca yalan yaymakla ilgili değil; aynı zamanda halkın siyasi liderlerden ve medya kurumlarından gelen bilgilere güvenme yeteneğine yönelik hesaplı saldırılardır. **Bu taktik, bir demokraside bilgilendirilmiş onayın temelini aşındırır ve zorluğu medya okuryazarlığı sorunundan (vatandaşların sahteleri tespit etmesi deneyimi) bilgiyi kaynağında doğrulamak için güçlü, sistemik çözümler gerektiren daha temel bir kurumsal güven krizine kaydırır. Yanlış bilgilendirmenin ötesinde, üretken Yapay Zekâ araçlarının, onlarla etkileşime giren insanlar üzerinde aşırı etki yaratabileceği, aşırı güvene ve eleştirel düşüncenin azalmasına yol açabileceği yönünde artan bir endişe olduğunu açıkça kabul etmek ve değerlendirmek gerekiyor.** ⁴⁹



Türkiye Bilişim Vakfı
www.tbv.org.tr

4. **Boyut 2: Özel Şirketler için Artan Riskler ve Stratejik Zorunluluklar**

4.1 Telif Hakkı Mücadelesi: Üretken Yapay Zekâ Yargılanıyor

Yapay Zekâ alanında ya da kullanıcısı olarak faaliyet gösteren özel şirketler için en önemli yeni risk alanı, fikri mülkiyet konusundaki hukuki mücadeledir. Orijinal raporda fikri mülkiyet risklerine kısaca değinilmesi, birçok Yapay Zekâ geliştiricisinin temel iş modelini sorgulayan bir dizi çığır açıcı telif hakkı ihlali davasıyla yer değiştirmiştir. ¹ Bu davalar, toplu olarak, veri ediniminde "önce elde et, sonra af dile" yaklaşımını, "adil kullanım" hukuki doktrininin merkezi bir mücadele alanı olarak ele aldığı bir davaya dönüştürmektedir. ³¹

- **Vaka Çalışması: Disney/Universal - Midjourney** : Haziran 2025'te açılan bir davada, Hollywood'un en büyük iki stüdyosu, Yapay Zekâ görüntü oluşturucu Midjourney'i "büyük ve kasıtlı telif hakkı ihlali" ile suçladı. ¹² Şikâyetinde, Midjourney'nin modellerini lisanssız, telif hakkıyla korunan çok sayıda görüntü üzerinde eğittiği ve kullanıcıların Elsa ve Homer Simpson gibi ikonik, tescilli karakterlerden "neredeyse ayırt edilemez" çıktılar üretmesini sağladığı iddia ediliyor. ¹² Dava, yalnızca tazminat değil, aynı zamanda operasyonları durdurmak ve telif hakkı filtrelerinin uygulanmasını zorlamak için bir ihtiyati tedbir de talep ediyor ve bu da büyük fikri mülkiyet sahiplerinin agresif bir hukuki itirazını temsil ediyor. ³¹
- **Vaka Çalışması: The New York Times- OpenAI** : Bu dava, telif hakkıyla korunan gazeteciliğin büyük dil modelleri tarafından birebir kopyalandığı iddiasına odaklanıyor. ¹² The New York Times, OpenAI modellerinin makalelerini neredeyse kelimesi kelimesine yeniden üretebileceğini, doğrudan orijinal eserle rekabet edebileceğini ve değerini azaltabileceğini iddia ediyor. Bu iddia, genellikle adil kullanım savunmasının merkezinde yer alan "dönüştürücü kullanım" argümanına doğrudan meydan okuyor; çünkü çıktı, orijinal içeriğin bir dönüşümü yerine bir ikamesi olarak sunuluyor. ¹²

Bunların farkına "artık" varan pek çok LLM üreticisi şirket artık "bilgi kaynakları" ile telif hakkı anlaşmalarını yapıyorlar ancak anlaşmaların yapıldığı tarihe kadar modellerin "öğrenmesini sağlayan içerik" modellerin içinde kalmaya devam edecek.

4.2 Yapay Zekâ Çağında Tekel Karşıtlığı: Piyasa Yapısından Ortaya Çıkan Davranışa

Rekabet hukuku alanında ikinci ve kritik bir risk cephesi açıldığını söylemek kaçınılmaz hale geldi. **Antitröst düzenleyicileri artık hem Yapay Zekâ pazarının yapısını hem de yeni rekabeti kısıtlayıcı davranış biçimlerinin potansiyelini inceliyor.** ABD Federal Ticaret Komisyonu (FTC) ve Adalet Bakanlığı (DOJ), Microsoft, Amazon ve Google gibi büyük bulut hizmeti sağlayıcılarını OpenAI ve Anthropic gibi önde gelen Yapay Zekâ laboratuvarlarıyla bağlayan stratejik ortaklıklar ve büyük yatırımlar hakkında soruşturmalar başlattı ve ısrarla takip ediyor. ¹⁸ Temel endişe, bu baskın şirketlerin bulut bilişim gibi temel girdilerdeki güçlerini kullanarak rekabeti engellemeleri ve yeni oluşan Yapay Zekâ ekosistemindeki pazar güçlerini sağlamlaştırılmaları. ¹⁸ Nitekim bu gelişmelere rağmen **Trump yönetimindeki ABD yaklaşımı daha serbest ve teknoloji şirketlerini destekleyen bir yaklaşımda. Bunun yaratacağı zorluklar AB tarafında da rekabet açısından önemsenmektedir ve böylelikle Birlik daha "vatandaş odaklı" yaklaşımı ile Yapay Zekâ'nın insan üzerindeki etkisini**



Türkiye Bilişim Vakfı
www.tbv.org.tr

değerlendiren politika yaklaşımlarını Yapay Zekâ yapısal modelleri veya dil modelleri için daha önemli görmeye devam etmektedir. Bu arada son gelişmelerde AB çerçevelerinin ABD'nin teknoloji şirketleri ile ciddi regülatif kesişim noktalarından dolayı bu şirketler tarafından şikâyet edildiğini ve ABD yönetimine bu konuda “şikâyetçi” olduğunu da görüyoruz.

Fikri mülkiyet haklarına yönelik ve rekabeti kısıtlayıcı risklerin bu şekilde bir araya gelmesi, karmaşık bir stratejik ikilem yaratıyor. Telif hakkı davaları başarılı olursa, Yapay Zekâ geliştiricilerini eğitim verilerini lisanslamaya zorlayacak ve bu da operasyonel maliyetlerini önemli ölçüde artıracaktır. Bu finansal baskı, onları derin cepli büyük teknoloji ortaklarına daha da bağımlı hale getirecektir. Daha derin entegrasyon, inovasyonu engelleyeceğinden ve daha küçük, bağımsız rakiplerin dışarıda kalacağından korkan antitröst düzenleyicilerini endişelendiren dinamiktir. Şirketler, fikri mülkiyet sorununa potansiyel çözümlerinin “büyük teknoloji sermayesine daha fazla bağımlılık” ya da “antitröst sorunlarını daha da kötüleştirdiği bir kıskaç” ortamının içine sıkışmış durumdadır.

Otonom (agentic) Yapay Zekâ'nın davranışları etrafında yeni bir yasal sınır da ayrıca ortaya çıkmaktadır. Hukuk uzmanları ve düzenleyiciler, asgari insan gözetimiyle görevleri yerine getirmek üzere tasarlanmış otonom Yapay Zekâ araçlarının bağımsız olarak fiyat tespiti veya pazar tahsisi gibi rekabeti kısıtlayıcı davranışlarda bulunabileceği riskiyle karşı karşıya kalıyorlar.⁷ Adalet Bakanlığı'nın, fiyatlandırma algoritmasının ev sahiplerinin kira oranları üzerinde anlaşmaya varması için bir "merkez ve uç" komplosu kolaylaştırdığını iddia eden emlak yazılım şirketi RealPage'e karşı 2023 yılında açtığı dava, bu tür algoritmik anlaşmaların gelecekte nasıl kovuşturulabileceğine dair önemli bir örnek olarak görülüyor.⁷

4.3 Gelişen Siber Güvenlik Tehdit Matrisi

Yapay Zekâ ile ilişkili siber güvenlik tehditleri, teorik zafiyetlerden güçlü gerçek dünya saldırı vektörlerine dönüşmüştür.¹ Üretken Yapay Zekâ'nın yaygınlaşması “karanlık dünyanın” oyuncularını sosyal mühendislik ve dolandırıcılık için güçlü yeni araçlarla donatmış ve tehditlerin geometrik artışına ve daha da kompleks senaryolara ulaşmasına neden olmuştur.

- **Vaka Çalışması: Arup Deepfake Dolandırıcılığı:** Bu yeni tehdidin çarpıcı bir örneği, 2024 yılında küresel mühendislik firması Arup'ta çalışan bir finans çalışanının dolandırıcılara 25,6 milyon dolar aktarmaya kandırılmasıyla yaşanmıştır.⁶ Saldırı, geleneksel bir hackleme değil, "teknoloji destekli sosyal mühendisliğin" karmaşık bir örneği olarak görülmeli. Başlangıçta bir kimlik avı e-postasından şüphelenen çalışan, şirketin CFO'su da dahil olmak üzere tüm katılımcıların aşırı gerçekçi bir deepfake olduğu bir görüntülü konferansa davet edildikten sonra e-postanın meşruiyetine ikna olmuş ve işlemi gerçekleştirmiş.

Bahsi geçen olay, Yapay Zekâ'nın, ezici işitsel ve görsel "kanıtlar" üreterek insan şüpheliğini ve geleneksel güvenlik protokollerini nasıl aşabileceğini gösteriyor.⁶



Türkiye Bilişim Vakfı
www.tbv.org.tr

Bu tehdit, WormGPT ve FraudGPT gibi karanlık ağda kötü amaçlı "suç hizmeti" sohbet robotlarının ortaya çıkmasıyla daha da güçleniyor. ⁶ Ticari modellerin etik güvencelerinden yoksun olan bu araçlar, düşük becerili saldırganların bile dil bilgisi açısından kusursuz ve bağlamsal olarak bilinçli kimlik avı e-postaları ve diğer kötü amaçlı içerikleri benzeri görülmemiş bir ölçekte oluşturmasına olanak tanıyarak, etkili siber suçlar için giriş engellerini önemli ölçüde azaltıyor. ⁶ Tehdit ortamı, yalnızca veri hırsızlığını değil, aynı zamanda Yapay Zekâ modellerinin kötü amaçlı "zehirlenmesini" de içerecek şekilde genişlemiş ve otomatik sistemleri içeriden bozabilecek ve yıkıcı uzun vadeli sonuçlara yol açabilecek bir veri bütünlüğü saldırı noktasına kadar ulaşmıştır. ³² **Bazı analistler tarafından belirlenen en endişe verici kullanım örnekleri arasında, üretken Yapay Zekâ'nın biyolojik silahların yaratılmasına yardımcı olma potansiyeli yer alıyor.** ⁴⁹

4.4 Açık Kaynak İkilemi: Yenilik ve Riski Dengelemek

Güçlü açık kaynaklı Yapay Zekâ modellerinin yükselişi, yönetim için benzersiz bir fayda ancak diğer yandan da karmaşık bir zorluk teşkil etmektedir. ⁴⁹ **Bir taraftan, açık modeller Yapay Zekâ'ya erişimi demokratikleştirmeleri, şeffaflığı teşvik etmeleri ve rekabeti ve tabandan inovasyonu teşvik etmeleri nedeniyle övülmektedir.** ⁴⁹ **Öte yandan, kontrolsüz bir şekilde yayımlanmaları önemli riskler oluşturmaktadır.** ⁵⁸ Model ağırlıkları ve kodlar kamuya açık hale geldiğinde, geliştiriciler kötüye kullanım izleme, güvenlik açıklarını düzeltme veya kötü niyetli kişilerin güvenlik özelliklerini kaldırmasını engelleme yeteneklerini kaybedeceklerdir. ⁵⁹ Bu durum, kötü niyetli kişilerin modelleri, nefret söylemi oluşturmak, rızaya dayanmayan görseller oluşturmak veya oran sınırı olmayan büyük ölçekli dezenformasyon kampanyalarını sürdürmek gibi zararlı amaçlar için ince ayar yapmalarına fırsat yaratır. ⁵⁹ Politika yapıcılar; bir yandan açık kaynaklı Yapay Zekâ'nın düzenlenmesini ve açıklığın faydalarını desteklerken, "geri döndürülemez risk" olasılığı bir anlamda henüz yeterince güvenli olmayan bu güçlü teknolojinin akut tehlikelerini azaltmalıdırlar. Bu da son derece zor ve kritik bir görevdir.

⁴⁹

5. Boyut 3: Yapay Zekâ Yönetişimi İçin Yeni Gerçekler

5.1 Kamu Hizmeti Sunumu: Üretken Yapay Zekâ'nın Vaatleri ve Tehlikeleri

Hükümetler, kamu hizmetlerini geliştirmek için Yapay Zekâ'yı keşfetmeye devam ediyorlar. Bu arada önemli başarıları da dikkat çekici başarısızlıkları da gösteren giderek artan sayıda vaka çalışmasının ortaya çıktığını da görüyoruz. ¹ Öte yandan, Estonya gibi ülkeler, operasyonları kolaylaştırmak, sağlık verilerini yönetmek ve trafik akışını optimize etmek için Yapay Zekâ'yı dijital hükümet altyapılarına başarıyla entegre ederek dijital yönetim için bir ölçütler oluşturuyorlar. ³³ Benzer şekilde, örneğin Singapur'un GovTech ajansı, çok sayıda departmanda etkili Yapay Zekâ destekli sohbet robotları konuşlandırarak çağrı merkezi iş yükünü başarıyla azaltıyor ve vatandaş hizmetlerine erişilebilirliği artırıyor ³⁴

Öte yandan, kamu sektöründe üretken Yapay Zekâ'nın konuşlandırılması, New York'da yakın zamanda yaşanan bir başarısız uygulamada da yaşandığı gibi, benzersiz yönetim zorlukları ortaya çıkarıyor.

- **Vaka Çalışması: New York Şehri Sohbet Robotu Başarısızlığı:** Şehir, 2025 yılında ülkenin ilk üretken Yapay Zekâ destekli belediye sohbet robotu olan "Benim



Türkiye Bilişim Vakfı
www.tbv.org.tr

Şehrim" sohbet robotunu pilot olarak kullandı. ¹⁰ Gazeteciler ve halk tarafından test edildiğinde, sohbet robotunun yanlış ve bazı durumlarda yasa dışı tavsiyelerde bulunduğu görüldü. Örneğin, bir işletme sahibine çalışanlarının bahşışlerinden pay alıp alamayacağı sorulduğunda, sohbet robotu açıkça "evet" yanıtını vererek iş kanunlarını doğrudan ihlal etti. ¹⁰ Başarısızlık, üretken Yapay Zekâ'nın kesin olmayan yapısından kaynaklandı; önceden onaylanmış yanıtlara sahip geleneksel sohbet robotlarının aksine, Benim Şehrim robotu, öngörülemez ve hatalı çıktılarına yol açan geniş ve doğrulanmamış bir veri havuzundan yanıtlar üretti. Bu vaka, bilginin doğruluğunun çok önemli olduğu ve hükümetin sağladığı rehberlikten sorumlu tutulabileceği bir kamu sektörü uygulaması bağlamında bu tür sistemlerin konuşlandırılmasının muazzam riskini vurgulamaktadır. ¹⁰

5.2 Ulusal Güvenlik ve Özerk Sistemler: Politika Güçleniyor

Ulusal güvenlik alanında, Ölümcül Otonom Silah Sistemleri'ni (LAWS) çevreleyen politika manzarası giderek daha belirgin hale geliyor. ¹ Amerika Birleşik Devletleri hükümeti, bu tür sistemlerin insani faydalar sağlayabileceğini savunarak şu anda LAWS'a yönelik uluslararası bir yasağı desteklemese de Kongre denetimi önemli ölçüde güçlendirilmiş durumda ³⁵

Son mevzuat, özellikle 2024 ve 2025 Mali Yılı Ulusal Savunma Yetkilendirme Yasaları (NDAA), Savunma Bakanlığı (DOD) için daha sıkı denetim ve raporlama gereklilikleri getirmiştir. ³⁵ Savunma Bakanı'nın artık, silah sistemlerindeki otonomiye ilişkin temel politika olan DOD Direktifi 3000.09'daki herhangi bir değişiklik hakkında Kongre savunma komitelerini bilgilendirmesi ve 2029 yılına kadar LAWS'ın onaylanması ve konuşlandırılmasıyla ilgili kapsamlı yıllık raporlar sunması gerekmektedir. ³⁵ **Bu, tüm otonom sistemlerin "kullanımı sırasında uygun düzeyde insan yargısına" izin verecek şekilde tasarlanmasını ve gerçekçi operasyonel ortamlarda güvenli/öngörülebilir bir şekilde çalışmasını sağlamak için kapsamlı test ve değerlendirmelerden geçmesini sağlamaya odaklanan sağlamlaştırılmış bir politika çerçevesine işaret etmektedir.** ³⁵

5.3 Yönetişim ve Denetimdeki Zorluklar

Hükümetler, Yapay Zekâ'yı etkin bir şekilde benimseme ve yönetme konusunda büyük iç zorluklarla karşı karşıyadır. Başlıca engellerden biri uzmanlık açığıdır; Yapay Zekâ teknolojisine ilişkin derin bilgi çoğunlukla özel sektörde bulunmaktadır ve bu da hükümetleri etkili düzenleyici rejimler tasarlamak ve uygulamak için gerekli kurum içi uzmanlıktan yoksun bırakmaktadır. ⁴⁹ Bu durum, hızla gelişen teknoloji ve sınırlı denetim kaynaklarıyla düzenlemeleri güncel tutmanın zorluğuyla daha da karmaşıklaşmaktadır. ¹ Kamu yararını korumak ve modellerin salt ticari amaçların etkisi dışında var olmasını sağlamak için, bazı analizler Yapay Zekâ gelişimine önemli miktarda kamu yatırımı yapılması gerekebileceğini göstermektedir. ⁴⁹

6. Olgunlaşan Azaltma Stratejileri ve En İyi Uygulamalar

6.1 Üretken Çağ için Yapay Zekâ Risk Yönetimi Çerçevesi

Yapay Zekâ riskleri geliştikçe, bunları yönetmek için tasarlanan çerçeveler de geliyor. Yaygın olarak başvurulmuş gönüllü bir rehber olan Ulusal Standartlar ve Teknoloji



Türkiye Bilişim Vakfı
www.tbv.org.tr

Enstitüsü (NIST) Yapay Zekâ Risk Yönetimi Çerçevesi (AI RMF), üretken Yapay Zekâ'nın kendine özgü zorluklarını ele almak üzere güncellendi.

Temmuz 2024'te NIST, **AI RMF "Üretken Yapay Zekâ Profili"ni (NIST.AI.600-1) yayınladı.** ³⁹ Bu önemli yardımcı kaynak, kuruluşlara üretken modellerin oluşturduğu benzersiz risklerde gezinmeleri için özel ve uygulanabilir rehberlik sağlamaktadır. **Profil, kuruluşların Yapay Zekâ sistemlerinin zararlı, önyargılı veya toksik içerik üretme potansiyeli; dezenformasyon oluşturulmasını kolaylaştırma, veya eğitim verilerinden hassas bilgileri sızdırma gibi riskleri belirlemelerine yardımcı olan bir içeriktedir.** ³⁸ Eğitim için veri kaynakları konusunda net politikalar oluşturmak, zararlı çıktılar için sağlam testler uygulamak ve sentetik içerik kullanımı konusunda şeffaflık sağlamak gibi, AI RMF'nin Yönetme, Haritalama, Ölçme ve Yönetme işlevleri kapsamında belirli eylemler önermesi de son derece önemlidir. ⁴⁰ NIST ayrıca, Özel Yayını 800-53 için yeni bir siber güvenlik kontrol katmanı ve Yapay Zekâ riskinin yerleşik siber güvenlik uygulamalarına daha derin bir şekilde entegre edildiğini gösteren özel bir Siber Yapay Zekâ Profili geliştirmektedir. ⁴¹

6.2 Pratik Bir Savunma Olarak İçerik Kaynağı: C2PA'nın Yükselişi

Teknik risk azaltma alanındaki en önemli gelişmelerden biri, içerik menşei standartlarının olgunlaşmasıdır. İçerik Menşei ve Özgünlük Koalisyonu (C2PA), dijital içerikler için bir "besin etiketi" işlevi gören açık bir teknik standart geliştirmiştir. ⁴² İçerik Kimlik Bilgileri olarak bilinen bu standart, bir dosyanın kökeni ve değişiklik geçmişinin kurcalamaya karşı korumalı kaydını güvenli bir şekilde dosyanın kendisine bağlayarak tüketicilerin orijinallliğini doğrulamasını sağlar. ⁴²

Kritik olarak, bu standart teorik bir konseptten pratik bir savunmaya dönüşüyor. Yaygın bir benimsemeye doğru atılan önemli bir adım olarak, C2PA İçerik Kimlik Bilgileri artık doğrudan üretim aşamasında donanıma entegre ediliyor. Önde gelen kamera üreticileri **Leica** ve **Nikon**, yerleşik C2PA özelliklerine sahip modeller duyurdu ve **Qualcomm**, teknolojiyi akıllı telefon çiplerine entegre ediyor. ⁴⁴

Bu; kullanıcıların gerçek medya ile manipüle edilmiş veya Yapay Zekâ tarafından üretilen medyayı ayırt edebilmesini sağlayarak, daha önce ayrıntılı olarak açıklanan deepfake ve dezenformasyon tehditleriyle mücadele etmek için güçlü bir teknik araç sağlamakta ve bir güven ekosisteminin temelini oluşturmaktadır ⁴⁴

6.3 İnsan Gözetimi ve Açıklanabilirliğin Yeniden İncelenmesi

C2PA gibi teknik çözümler gelişirken, "kara kutu" sistemleri için birincil bir hafifletme yöntemi olarak Açıklanabilir Yapay Zekâ'nın (XAI) vaadi, kritik bir yeniden inceleme gerektiriyor. Daha önce de belirtildiği gibi, yakın zamanda yapılan geniş çaplı bir çalışma, XAI üzerine akademik makalelerin %1'inden azının yöntemlerini insan deneklerle doğruladığını ortaya koydu ve bu da önerilen birçok tekniğin gerçek dünyadaki etkinliği hakkında ciddi sorular ortaya çıkardı. ²⁵

XAI, model yorumlanabilirliğini iyileştirme potansiyeline sahip değerli ve aktif bir araştırma alanı olmaya devam ederken, bu bulgu önemli bir gerçeği vurgulamaktadır: **Öngörülebilir gelecekte, sadece "teknik açıklanabilirliğe", "hesap verebilirliğin"**



Türkiye Bilişim Vakfı
www.tbv.org.tr

tek veya birincil mekanizması olarak güvenilemez. ⁴⁶ Bu, özellikle ceza adaleti, sağlık hizmetleri ve kamu hizmetleri gibi yüksek riskli alanlarda en kritik ve güvenilir azaltma stratejilerinin prosedürel ve insan merkezli olmaya devam ettiği sonucunu desteklemektedir. Bunlar arasında anlamlı insan gözetimi sağlamak, otomatik kararlar için açık ve erişilebilir itiraz süreçleri oluşturmak ve Yapay Zekâ yaşam döngüsü boyunca sağlam prosedürel güvenlik önlemleri ve bağımsız denetimler uygulamak yer almaktadır.

Üretken Yapay Zekâ modellerinin insan benzeri davranış ve yanıtlar üretebilmesi, insan ile makinenin ayırımına yönelik yaklaşımların da yeniden düşünülmesini gerektiriyor. Geleneksel doğrulama yöntemlerinin etkisini kaybetmesiyle beraber, bazı kurumlar kültürel bağlamı, sezgiyi veya toplumsal referansları ölçen yeni yöntemlerle bu ayrımı güçlendirmeye çalışıyor. Örneğin “Keloğlan neden kel?” gibi, yalnızca bilgi değil ortak kültürel hafıza gerektiren sorular bu çabaların bir yansımasıdır. Ancak Yapay Zekâ modellerinin öğrenme hızı dikkate alındığında, bu tür yöntemlerin uzun vadede kalıcı bir avantaj sağlamayacağı açıktır. Bu durum, insan–makine ayırımının da tıpkı diğer güvenlik alanlarında olduğu gibi dinamik bir “kedi–fare” ilişkisine dönüşeceğini göstermektedir. Bu nedenle, insan gözetiminin ve prosedürel mekanizmaların rolü yalnızca açıklayıcılığı pekiştirmek değil, aynı zamanda değişen risk ortamında istikrar sağlayan bir kontrol hattı oluşturmak açısından daha kritik hâle gelmektedir.

6.4 Belirsizlik Çağında Stratejik Yönetim İlkeleri

Stanford Siber Politika Merkezi'nin analizi, karmaşık Yapay Zekâ ortamında yol alan politika yapıcılar için birkaç üst düzey ilke önermektedir. ⁴⁹ Bu ilkeler, etkili yönetim geliştirmek için stratejik bir bakış açısı sunmaktadır:

- **Teknoloji ve Uygulamaların Düzenlenmesi:** Temel tartışmalardan biri, altta yatan genel amaçlı Yapay Zekâ teknolojisinin düzenlenmesi mi yoksa belirli, yüksek riskli uygulamalara mı odaklanılması gerektiğidir.

Sektöre özgü yasalar kademeli düzenlemelere izin verirken, genel amaçlı Yapay Zekâ'nın öngörülemez doğası, bazı kuralların temel teknolojiye uygulanması gerekebileceğini düşündürmektedir. ⁴⁹

- **Şeffaflık ve Denetim İhtiyacı:** Üretken Yapay Zekâ'nın uzun vadeli etkileri büyük ölçüde bilinmediğinden, şeffaflık son derece önemlidir. **Geliştiricilerin, modellerin nasıl oluşturulduğu ve hangi veriler üzerinde eğitildikleri konusunda daha fazla açıklığa sahip olması, hesap verebilirliği sağlamak ve etkili üçüncü taraf denetim ve düzenlemelerini mümkün kılmak için hayati önem taşımaktadır.** ⁴⁹
- **Uygulamanın Önceliği:** Yapay Zekâ'nın hızlı evrimi, güçlü bir uygulama sürecinin ilk mevzuat kadar, hatta belki de daha kritik olabileceği anlamına geliyor. **Bu durum, hükümetlerin düzenleyici kurumlarda görev alacak kıt kaynak olan Yapay Zekâ uzmanlarını işe alıp elde tutmaları konusunda önemli bir taahhüt gerektiriyor; bu da özel sektörle rekabet göz önüne alındığında büyük bir zorluk olarak görünmektedir.** ⁴⁹

Tablo 2: Yapay Zekâ Risk Azaltma Stratejileri Matrisi (Genişletilmiş ve Güncellenmiş)

Aşağıdaki matris, ortaya çıkan tehditleri ve çözümleri içerecek şekilde güncellenen temel risk kategorilerini ilgili azaltma stratejileriyle ilişkilendirir.

Bütüncül Yapay Zeka Risk Azaltma Stratejileri: Üç Katmanlı Güvenlik Hiyerarşisi



© NotebookLM

7. Sonuç ve Öneriler

7.1 Bulguların Sentezi: Soyut İlkelerden Somut Sonuçlara

Yapay Zekâ insan ve iş yaşamının ve de Kamu yönetişiminin dönüşümünde kritik bir yetkinlik ve uygulama eşiğini geçmiştir. Soyut etik ilkelerin tartışıldığı dönem, yerini hızla somut zararlara karşı dava açma, belirli düzenlemeleri uygulama ve pratik teknik savunmalar uygulama dönemine bırakıyor.

İçinde bulunduğumuz dönemin belirleyici özelliği, dünya çapındaki politika yapıcılarını önemli bir belirsizlik altında hareket etmeye zorlayan bu dönüşümdeki şaşırtıcı hızdır. Yapay Zekâ ile ilişkili riskler -gizlilik ihlallerinden algoritmik önyargılara, fikri mülkiyet hırsızlığından demokratik manipülasyona kadar- artık teorik olasılıklar değil, önemli finansal, yasal ve toplumsal sonuçları olan belgelenmiş gerçekliklerdir. Buna karşılık, ABD, Avrupa ve Çin'de farklı düzenleyici modellerin ortaya çıkmasıyla birlikte yönetim çerçeveleri de gelişmektedir. Yasal zorluklar artmakta ve yeni uyumlayıcı araçları laboratuvarlardan pazara taşınmaktadır.

Önceki sayfalardaki analiz, teknolojik ilerleme, yasal hesap verebilirlik ve düzenleyici gözetim arasında, Yapay Zekâ'nın geleceğini aktif olarak şekillendiren dinamik ve genellikle tartışmalı bir etkileşimi ortaya koymaktadır.



Türkiye Bilişim Vakfı
www.tbv.org.tr

7.2 Güncellenmiş ve Eyleme Dönüştürülebilir Öneriler

Analize dayanarak, kilit paydaşlar için aşağıdaki güncellenmiş öneriler önerilmektedir:

Vatandaşlar için:

- **Yapay Zekâ ve Medya Okuryazarlığını Geliştirmek:** Genel farkındalığın ötesine geçerek, Yapay Zekâ tarafından üretilen içerikleri eleştirel bir şekilde değerlendirmek için becerilerin aktif olarak geliştirilmesi. Gerçek kontrol kaynaklarından yararlanmak ve filtre baloncuklarını ortadan kaldırmak için çeşitli bilgi kaynaklarından yararlanmak.
- **Kimlik Doğrulama Araçlarını Savunmak ve Kullanmak:** C2PA gibi içerik özgünlük standartlarının yaygın olarak benimsenmesini savunmak. Tükettirilen bilgiler hakkında bilinçli kararlar alabilmek için, görsel ve videolardaki İçerik Kimlik Bilgilerini doğrulayabilen araçları aktif olarak aramak ve kullanmak.
- **Hak ve Tazminat Talep Etmek:** Kamuoyunda yer alan tartışmalara katılmak ve gizliliği koruyan, adaleti sağlayan, şirketlerden ve hükümetlerden şeffaflık talep eden politikaları desteklemek. Yapay Zekâ sistemlerinin neden olduğu zararlara itiraz etmek ve tazminat talep etmek için açık ve erişilebilir mekanizmalar oluşturmak.

Özel Şirketler için:

- **Güçlü ve Uyarlanabilir Yönetişimi Yerleştirmek:** Etik ilkeleri ve risk yönetimini tüm Yapay Zekâ yaşam döngüsüne entegre etmek. Etik komiteler oluşturmanın ötesine geçerek ve **NIST Yapay Zekâ RMF ve yeni Üretken Yapay Zekâ Profili gibi denetlenebilir yönetim çerçevelerini uygulamak.** Yapay Zekâ odaklı sonuçlar için net hesap verebilirlik düzeneklerini oluşturmak.
- **Fikri Mülkiyet ve Tekel Karşıtı Durum Tespiti'ne Öncelik Vermek: Telif hakkı riskini azaltmak için üretken Yapay Zekâ modellerini eğitmek veya ince ayar yapmak amacıyla kullanılan tüm veriler için** titiz kaynak denetimleri gerçekleştirmek. Olası tekel karşıtı etkiler açısından iş ortamında yoğun kullanılan teknoloji platformlarıyla ortaklıkları proaktif olarak değerlendirmek.
- **Gelişmiş Güvenlik ve Doğruluk Önlemlerini Uygulamak:** Siber güvenlik eğitimlerini ve protokollerini, deepfake tabanlı sosyal mühendisliği özel olarak ele alacak şekilde güncellemek. Kullanıcı güvenini artırmak ve yanlış bilgilendirmeye mücadele etmek için C2PA gibi içerik doğruluk standartlarını savunmak ve ürün ve platformlara entegre etmek.
- **İş Gücüne Yatırım Yapmak:** Yapay Zekâ otomasyon projeleri için iş gücü etki değerlendirmeleri yaparak geçişi proaktif bir şekilde yönetmek. Çalışanları Yapay Zekâ destekli bir iş yerindeki yeni rollere hazırlamak için yeniden beceri kazandırma ve geliştirme programlarına yatırım yapmak.

Hükümetler için:

- **Net, Risk Tabanlı ve Uyarlanabilir Düzenlemeler Geliştirmek:** Hızlı teknolojik değişime uyum sağlayacak kadar esnek kalırken aynı zamanda açıklık sağlayan yasal çerçeveler oluşturmak. Yüksek etkili uygulamalara daha katı kurallar uygulayan AB Yapay Zekâ Yasası'ndaki gibi risk tabanlı bir yaklaşım hayata



Türkiye Bilişim Vakfı
www.tbv.org.tr

geçirmek.

- **Düzenleyici ve Uygulama Kapasitesini Güçlendirmek:** Düzenleyici kurumlar, rekabet otoriteleri ve uygulama kurumları bünyesinde derin teknik uzmanlık oluşturmaya yatırım yapmak. **Düzenleyicilerin, Yapay Zekâ ortaklıkları ve algoritmik iş birliklerine ilişkin karmaşık antitröst soruşturmaları yürütmeleri için eğitime fon sağlamak.**
- **Egemen Uzmanlık Oluşturun ve Kamu Yatırımlarını Göz Önünde Bulundurmak:** Özel sektörle bilgi açığını kapatmak için düzenleyici kurumlar bünyesinde derin teknik uzmanlık oluşturmaya aktif olarak yatırım yapmak. Kamu yararına geliştirilen modellerin varlığını garanti altına almak ve ticari kuruluşların etkisini dengelemek için Yapay Zekâ araştırmalarına ve altyapısına stratejik kamu yatırımları yapmak.
- **Açık Kaynak “Muammasını” Ele Almak:** Kötü niyetli aktörler tarafından kötüye kullanım risklerini azaltmak için net sorumluluk ve hesap verebilirlik mekanizmaları oluştururken, inovasyonu ve şeffaflığı teşvik eden açık kaynaklı Yapay Zekâ için ayrıntılı politikalar geliştirmek.⁴⁹
- **Kamu Sektörü Kullanımı ve Tedarikinde Örnek Olmak:** Tüm devlet Yapay Zekâ sistemleri için sıkı iç yönetim uygulayarak şeffaflık, adalet ve anlamlı insan gözetimi sağlamak. Bilgi bütünlüğü için bir standart oluşturmak amacıyla **resmi kamu iletişimlerinde C2PA gibi açık standartların kullanımını zorunlu kılmak.**
- **Uluslararası İş Birliğinin Geliştirilmesi ve Dijital Uçurumla Mücadele:** Standartları uyumlu hale getirmek ve düzenleyici parçalanmayı azaltmak için uluslararası iş birliğine katılmak. Toplumsal eşitsizliklerin daha da kötüleşmesini önlemek için Yapay Zekâ teknolojilerine, dijital altyapıya ve okuryazarlık programlarına eşit erişimi sağlayacak politikalar uygulamak.

7.3 Geleceğe Bakış: Dava, Düzenleme ve Yeniliğin Etkileşimi

Yapay Zekânın önümüzdeki yıllardaki seyri, davalar, düzenlemeler ve inovasyon arasındaki dinamik geri bildirim döngüsü tarafından belirlenecektir. Halen devam eden çığır açıcı telif hakkı ve antitröst davalarının sonuçları, bir sonraki mevzuat ve düzenleyici uygulama dalgasını doğrudan şekillendirecektir. Bu yasal ve düzenleyici sınırlar da, sorumlu inovasyonun gerçekleşebileceği sınırları belirleyecektir.

Tanımlanan bu karmaşık ve yüksek riskli ortamda yol almak, sürekli adaptasyon, çok paydaşlı iş birliği ve Yapay Zekâ'nın gücünü insan hakları, demokratik ilkeler ve paylaşılan refah gibi kalıcı değerlerle uyumlu hale getirme konusunda sarsılmaz bir bağlılık gerektirecektir.

8. Türkiye İçin Öneriler

Bölüm 1: Hukuki ve Etik Çerçeve (Koruma & Ceza)

"Teknolojiyi değil, zararlı eylemi cezalandır"....

Türkiye için bu yaklaşım, inovasyonu boğmadan güvenliği sağlamanın anahtarıdır.

1. Teknoloji Değil, Suç Odaklı Yaptırım (Mevcut Hukukun Uyarlanması)



Türkiye Bilişim Vakfı
www.tbv.org.tr

- **Prensip:** "Yapay Zeka bir 'sorumluluktan kaçış kartı' (liability shield) değildir." Dolandırıcılık insanla yapıldığında suçsa, YZ ile yapıldığında da suçtur.
- **TR Önerisi:** Yeni ve devasa bir "YZ Ceza Kanunu" çıkarmak yerine; Türk Ceza Kanunu (TCK) ve Borçlar Kanunu'nda yapılacak güncellemelerle, suçun "otonom sistemler aracılığıyla" işlenmesinin *ağırlaştırıcı sebep veya doğrudan sorumluluk* doğurduğu netleştirilmelidir.
- **Ek:** Ayrımcılık (işe alım, kredi verme vb.) yapan algoritmalar için KVKK ve ilgili yönetmeliklerde "algoritmik hesap verebilirlik" şartı getirilmelidir.

2. Çocuklar ve Savunmasız Gruplar İçin "Dijital Kalkan"

- **Prensip:** Çocuklar YZ etkileşimlerinde (arkadaşlık eden botlar vb.) savunmasızdır.
- **TR Önerisi:** 13-16 yaş altı için ebeveyn izni şartı Türkiye'deki "dijital okuryazarlık" seviyesi gözetilerek daha sıkı uygulanmalı. Eğitimde kullanılan YZ araçları (MEB onaylı) hariç, genel YZ platformlarında "Çocuk Modu" zorunluluğu getirilmelidir.

3. AB Modeli ile Dengeli Risk Yönetimi (Küresel Trend Ekleme)

- **Ekleme:** AB Yapay Zeka Yasası (EU AI Act) 2025 itibarıyla tam yürürlüğe giriyor. Bu yasa sistemleri "Kabul Edilemez Risk" (yasaklı), "Yüksek Risk" (denetime tabi) ve "Düşük Risk" olarak ayırır.
- **TR Önerisi:** Türkiye'nin AB ile ticari entegrasyonu nedeniyle, "**Risk Temelli Yaklaşım**" benimsenmelidir. Ancak start-up'ları bürokrasiye boğmamak için **KOBİ ve Girişimler için "Düzenleyici Kum Havuzu" (Regulatory Sandbox)** oluşturulmalıdır. Start-up'lar burada ürünlerini ağır regülasyonlara takılmadan, kontrollü ortamda test edebilmelidir.

Bölüm 2: Stratejik Altyapı ve "Egemen YZ" (Sovereign AI)

Dünya artık YZ'yi sadece bir yazılım değil, bir "ulusal güvenlik ve egemenlik" meselesi olarak görüyor.

4. Ulusal Hesaplama Gücü (Compute) ve Veri Altyapısı

- **Prensip:** Küçük teknoloji şirketlerin de GPU ve enerjiye erişiminin demokratikleşmesi.
- **TR Önerisi:** Türkiye'de donanım maliyetleri (döviz kuru nedeniyle) çok yüksek. Devlet (TÜBİTAK veya DDO (Siber Güvenlik Başkanlığı?) öncülüğünde), girişimcilere ve araştırmacılara "**Ulusal Bulut/GPU Kredisi**" sağlamalıdır. Start-up'ların AWS/Azure/Google maliyetleri altında ezilmemesi için yerel ve sübvansede edilmiş bir hesaplama altyapısı (Veri Merkezi) kurulmalıdır.
- **Trend:** "Sovereign AI" (Egemen YZ) kavramı yükselişte. Her ülkenin kendi kültürü, dili ve verisiyle eğitilmiş modeline sahip olması gerektiği görüşü hakim.

5. Türkçe Büyük Dil Modeli ve Açık Veri Seferberliği



Türkiye Bilişim Vakfı
www.tbv.org.tr

- **Prensip:** Açık kaynak (Open Source) gelişimin motorudur.
- **TR Önerisi:** Türkiye'nin "Kendi ChatGPT'sini" yapmasından ziyade, dikeylerde (hukuk, sağlık, tarım) çalışacak Türkçe modelleri finanse etmesi gerekir. Kamu verilerinin (anonimleştirilmiş sağlık verileri, trafik verileri, meteoroloji, yargı kararları) makine okunabilir formatta, start-up'ların eğitim yapabileceği şekilde "**Açık Veri Havuzları**" olarak sunulması şarttır.

6. Siber Güvenlik ve Savunma Sanayii Entegrasyonu

- **Prensip:** YZ hem kalkan hem kılıçtır.
- **TR Önerisi:** Türkiye'nin savunma sanayindeki kasları (İHA/SİHA tecrübesi) siber savunmaya taşınmalıdır. Ulusal güvenlikte "savunma amaçlı YZ" kullanımı teşvik edilmeli, ancak "Otonom Silah Sistemleri" konusunda uluslararası etik normlara (OECD/BM) uyum taahhüt edilmelidir.

Bölüm 3: İnsan Kaynağı ve Toplum

7. YZ Çağına Uygun Eğitim ve İş Gücü Dönüşümü

- **Prensip:** Yasaklamak değil, eğitmek.
- **TR Önerisi:** "Yapay Zeka Okuryazarlığı" sadece mühendisler için değil, hukukçular, doktorlar ve mavi yakalılar için de zorunlu eğitim modülü olmalı. Meslek liseleri ve üniversitelerde "YZ Operatörlüğü" (Prompt Engineering vb.) bölümleri açılmalı.
- **Ekleme:** Beyin göçünü tersine çevirmek için "YZ Araştırmacı Vizesi" veya vergi teşvikleri ile küresel yetenekler Türkiye'ye çekilmeli veya uzaktan Türkiye projelerine çalışmalarını sağlanmalıdır.

Bölüm 4: Şeffaflık ve Yönetişim

8. Şeffaflık Kartları (Model Cards)

- **Prensip:** YZ etiketleri uygulanması.
- **TR Önerisi:** Türkiye'de piyasaya sürülen veya kamuda kullanılan her YZ modeli için standart bir "**Model Künyesi**" zorunluluğu getirilmelidir.
 - *Kim üretti?*
 - *Hangi verilerle eğitildi ? (Telif hakkı ihlali var mı ?)*
 - *Hangi dilleri/kültürleri kapsıyor?*
 - Sınırlılıkları nedir? Bu, tüketicinin bilinçli tercih yapmasını sağlar ancak ticari sırları (model ağırlıkları vb.) ifşa etmeyi gerektirmez.

9. Devlet Hizmetlerinde YZ Devrimi (Agentic Government)

- **Prensip:** Devlet YZ'yi kullanarak hizmet kalitesini artırmalı.
- **TR Önerisi:** e-Devlet Kapısı dünyadaki en iyi örneklerden biridir. Bu yapı, sadece belge üreten değil, vatandaş adına işlem yapan (örneğin; "Vergi borcumu



Türkiye Bilişim Vakfı

www.tbv.org.tr

yapılandır ve ödeme planı çıkar" diyen) "**Otonom Devlet Asistanlarına**" dönüştürülmelidir. Her bakanlık 1 yıl içinde "YZ Entegrasyon Planı" sunmalıdır.

Özet: Türkiye İçin Önerilen "Altın Kural" Seti

- 1 **Koru:** Vatandaşı dolandırıcılıktan ve ayrımcılıktan koru (TCK uyarlaması).
- 2 **Güçlendir:** Girişimciyi GPU teşvikleri, açık veri ve "Sandbox" ile güçlendir.
- 3 **Yerelleştir:** Küresel modelleri olduğu gibi almak yerine, yerli veri ve kültürle eğitilmiş "Egemen YZ" kapasitesi geliştir.



Türkiye Bilişim Vakfı
www.tbv.org.tr

Alıntı yapılan eserler:

1. WEF YZ raporları
2. Yapay Zekâ Endeksi | Stanford HAI, erişim tarihi 10 Ağustos 2025, <https://hai.stanford.edu/ai-index>
3. Yapay Zekâ - OECD, erişim tarihi 10 Ağustos 2025, <https://www.oecd.org/en/topics/artificial-intelligence.html>
4. IEEE Küresel Girişim 2.0 Otonom Etik... - IEEE SA, erişim tarihi 10 Ağustos 2025, <https://standards.ieee.org/industry-connections/activities/ieee-global-initiative/>
5. Daha fazla ortaklık, daha fazla içgörü, daha iyi araçlar: 2024'te Yapay Zekâ politikasını nasıl şekillendirdik - OECD.AI, erişim tarihi: 10 Ağustos 2025, <https://oecd.ai/en/wonk/how-we-shaped-ai-policy-in-2024>
6. Yapay Zekâ Siber Güvenlik Tehditleri 2025: 25,6 Milyon Dolarlık Deepfake - DeepStrike, <https://deepstrike.io/blog/ai-cybersecurity-threats-2025>
7. Agentic AI, Antitröst Düzenleyicileri İçin Alarm Zillerini Çaldırıyor | PYMNTS.com, erişim tarihi 10 Ağustos 2025, <https://www.pymnts.com/news/artificial-intelligence/2025/agentic-ai-raises-alarm-bells-for-antitrust-regulators/>
8. UNESCO Yapay Zekâ Etiği Tavsiyesi, <https://www.soroptimistinternational.org/2024/07/18/the-unesco-recommendation-on-the-ethics-of-artificial-intelligence/>
9. Üretken Yapay Zekâ Davaları Zaman Çizelgesi: OpenAI, Microsoft, Anthropic, Nvidia, Perplexity, Intel ve Daha Fazlasına Karşı Hukuki Davalar - Yeşil BT Hizmet Sağlayıcıları için Sürdürülebilir Teknoloji Ortağı, <https://sustainabletechpartner.com/topics/ai/generative-ai-lawsuit-timeline/>
10. Yapay Zekâ ve Devlet Çalışanları: Kamu Yönetiminde Kullanım Örnekleri , <https://rooseveltinstitute.org/publications/ai-and-government-workers/>
11. Yapay Zekâ Deepfake Güvenlik Endişeleri | CSA, <https://cloudsecurityalliance.org/blog/2024/06/25/ai-deepfake-security-concerns>
12. Telif Hakkı Deneme Aşamasında: Büyük Stüdyolar, Midjourney Davasında Yapay Zekâ Eğitim Uygulamalarına Meydan Okuyor, <https://ssrana.in/articles/copyright-on-trial-major-studios-challenge-ai-training-practices-in-midjourney-lawsuit/>
13. OECD AI İlkeleri genel bakışı, <https://oecd.ai/en/ai-principles>
14. OECD Yapay Zekâ İlkeleri'nin 2024 güncellemesi - Dijital Politika Uyarısı, 10 Ağustos 2025'te erişildi, <https://digitalpolicyalert.org/ai-rules/2024-update-OECD-principles>
15. OECD, Sorumlu Yapay Zeka - Yapay Zeka Hukuku ve Politikası Rehberini Güncelliyor, <https://www.ailawandpolicy.com/2024/05/oecd-updates-guidance-on-responsible-ai/>
16. Yapay Zekâ Konseyi Tavsiyesi, <https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449>
17. Yayın: FNF Global Innovation Hub, "AI-Generated Disinformation" başlıklı makaleyi yayınladı. <https://www.freiheit.org/taiwan/fnf-global-innovation-hub-released-ai-generated-disinformation-2024-taiwan-presidential>
18. Yapay Zekâ Girişimlerine Yapılan Büyük Teknoloji Yatırımları Rekabet Tehlikesi Uyarısı Vermiyor - ProMarket, <https://www.promarket.org/2024/08/27/big-tech-investments-in-ai-startups-do-not-raise-competitive-red-flags/>



Türkiye Bilişim Vakfı
www.tbv.org.tr

19. IEEE Etik Uyumlu Tasarım: Yapay Zeka Sistemlerine Mühendislik Etiği - VerityAI, <https://verityai.co/blog/ieee-ethically-aligned-design-guide>
20. Yapay Zekâ Etiği | UNESCO, <https://www.unesco.org/en/artificial-intelligence/recommendation-ethics>
21. Bangkok Yapay Zekâ Etiğine Hız Veriyor: UNESCO'nun 3. Kongresinden Öne Çıkanlar, <https://www.unesco.org/en/articles/bangkok-sets-pace-ai-ethics-highlights-unescos-3rd-global-forum-ethics-ai>
22. Yapay Zekâ Etiği Küresel Forumu - Yapay Zeka – UNESCO, <https://www.unesco.org/en/forum-ethics-ai>
23. Yapay Zekâ Etiği Üzerine 3. UNESCO Küresel Forumu'nda Kaydedilen Açıklamalar - ASEAN, <https://asean.org/recorded-remarks-at-the-3rd-unesco-global-forum-on-the-ethics-of-ai/>
24. Yapay Zekâ Etiği Küresel Forumu'nda Vietnam - UNESCO, <https://www.unesco.org/en/articles/vietnam-global-forum-ethics-ai>
25. Açıklanabilir Yapay Zekâ Makalelerinin %1'inden Azı İnsanlarla Açıklanabilirliği Doğruluyor - arXiv, <https://arxiv.org/html/2503.16507v1>
26. Deepfakes ve Yapay Zekâ Mevzuatının Geleceği: Etik ve Yasal Zorlukların Üstesinden Gelmek, <https://gdprlocal.com/deepfakes-and-the-future-of-ai-legislation-overcoming-the-ethical-and-legal-challenges/>
27. Elon Musk'ın Grok-AI'sı Eleştiri Topluyor, Taylor Swift'in Açık Sahte Derinliklerini Otomatik Olarak Oluşturuyor, <https://timesofindia.indiatimes.com/sports/nfl/news/elon-musks-grok-ai-garners-criticism-auto-generating-taylor-swifts-explicit-deep-fakes/articleshow/123149501.cms>
28. Yapay Zekâ tarafından üretilen dezenformasyonun bu yılki seçimleri nasıl etkileyebileceği ve gazetecilerin bu konuda nasıl haber yapması gerektiği | Reuters Gazetecilik Çalışmaları Enstitüsü, <https://reutersinstitute.politics.ox.ac.uk/news/how-ai-generated-disinformation-might-impact-years-elections-and-how-journalists-should-report>
29. Yapay Zekâ İşe Alımında Algoritmik Önyargıların Üstesinden Gelmek: Küresel Hukuki Eğilimler, İş Riskleri ve İnsan Gözetimine İhtiyaç - Bridge Counsels, <https://bridgencounsels.com/navigating-algorithmic-bias-in-ai-recruitment-global-legal-trends-business-risks-and-the-need-for-human-oversight/>
30. www.digital-adoption.com, <https://www.digital-adoption.com/ai-bias-examples/#:~:text=Amazon's%20AI%20recruiting%20tool%20displays%20bias%20towards%20women,-Amazon's%20flawed%20automated&text=To%20achieve%20this%2C%20they%20had,skew%20reasoning%20toward%20these%20preferences.>
31. Disney-Midjourney Davası Yapay Zekâ Telif Hakkı Yasasını Nasıl Yeniden Şekillendirebilir. , <https://time.com/7293362/disney-universal-midjourney-lawsuit-ai/>
32. Kritik Altyapıya Yönelik Ortaya Çıkan Tehditler: 2025'te Yapay Zekâ Odaklı Siber Güvenlik Trendleri, <https://www.capttechu.edu/blog/ai-driven-cybersecurity-trends-2025>
33. Vaka Çalışması: Estonya Hükümeti'nde Yapay Zeka Uygulaması - Kamu Sektörü Ağı, <https://publicsectornetwork.com/insight/case-study-ai-implementation-in-the-government-of-estonia>
34. Hükümetler Yapay Zekâ 'yı Nasıl Kullanıyor: 8 Gerçek Dünya Vaka Çalışması,



Türkiye Bilişim Vakfı
www.tbv.org.tr

- <https://blog.govnet.co.uk/technology/ai-in-government-case-studies>
35. Savunma Kılavuzu: ABD'nin Ölümcül Otonom Silah Sistemleri Politikası | Congress.gov, <https://www.congress.gov/crs-product/IF11150>
 36. Lethal Autonomous Weapon Systems (LAWS) – UNODA, <https://disarmament.unoda.org/the-convention-on-certain-conventional-weapons/background-on-laws-in-the-ccw/>
 37. Yapay Zekâ ve Ulusal Güvenlik - Congress.gov, https://www.congress.gov/crs_external_products/R/PDF/R45178/R45178.3.pdf
 38. NIST AI Risk Yönetimi Çerçevesi: Özet - Wiz, <https://www.wiz.io/academy/nist-ai-risk-management-framework>
 39. Yapay Zekâ Risk Yönetimi Çerçevesi | NIST, <https://www.nist.gov/itl/ai-risk-management-framework>
 40. Yapay Zekâ Risk Yönetimi Çerçevesi: Üretken ... , <https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.600-1.pdf>
 41. NIST, Federal Kullanım Genişlerken Yeni Yapay Zekâ Siber Güvenlik Kılavuzunu Yayımlayacak, <https://govciomedia.com/nist-to-release-new-ai-cybersecurity-guidance-as-federal-use-expands/>
 42. C2PA | Medya İçerik Kaynaklarının Doğrulanması, <https://c2pa.org/>
 43. Hakkında - C2PA, <https://c2pa.org/about/>
 44. Nasıl Çalışır - İçerik Özgünlüğü Girişimi, <https://contentauthenticity.org/how-it-works>
 45. İçerik Orijinalliği Girişimi, <https://contentauthenticity.org/>
 46. Açıklanabilir Yapay Zeka için LLM'ler: Kapsamlı Bir Araştırma - arXiv, <https://arxiv.org/pdf/2504.00125>
 47. Açıklanabilir Yapay Zeka – En Son Gelişmeler ve Yeni Trendler - arXiv, , <https://arxiv.org/pdf/2505.07005>
 48. Açıklanabilir Yapay Zeka için LLM'ler: Kapsamlı Bir Araştırma - arXiv, <https://arxiv.org/html/2504.00125v1>
 49. Yeni Rapor, ... için Yönetim Stratejilerini ve Risk Analizini Açıklıyor, <https://cyber.fsi.stanford.edu/news/new-report-unpacks-governance-strategies-and-risk-analysis-generative-ai>
 50. Belirsizlik Altında Düzenleme: Üretken Yapay Zekâ için Yönetişim Seçenekleri | FSI, <https://cyber.fsi.stanford.edu/content/regulating-under-uncertainty-governance-options-generative-ai>
 51. BELİRSİZLİK ALTINDA DÜZENLEME: - AWS, https://fsi9-prod.s3.us-west-1.amazonaws.com/s3fs-public/2024-12/GenAI_Report_REV_Master_%20as%20of%20Dec%2012.pdf
 52. Mevcut Yapay Zekâ Düzenlemeleri Küresel Yönetim Çerçevesini Nasıl Şekillendiriyor?,
 53. Yapay Zekâ Düzenlemesinin Üç Zorluğu - Brookings Enstitüsü, <https://www.brookings.edu/articles/the-three-challenges-of-ai-regulation/>
 54. AB, Çin ve ABD Yapay Zeka Politika Manzaralarının Kesitsel Karşılaştırması - Plurus Strategies, <https://www.plurusstrategies.com/insights/2024/5/6/a-cross-sectional-comparison-of-eu-china-and-us-artificial-intelligence-policy-landscapes-1>
 55. Yapay Zekâ Geliştirme Stratejilerinin Karşılaştırmalı Analizi: Çin'in Hedefleri ve AB'nin Düzenleyici Çerçevesi Üzerine Bir Çalışma - EuroHub4Sino, <https://eh4s.eu/publication/comparative-analysis-of-ai-development-strategies-a-study-of-chinas-ambitions-and-the-e-us-regulatory-framework>



Türkiye Bilişim Vakfı
www.tbv.org.tr

56. ABD ve Çin yapay zekasının düello eylem planlarının satır aralarını okumak - Atlantic Council, <https://www.atlanticcouncil.org/blogs/new-atlanticist/reading-between-the-lines-of-the-dueling-us-and-chinese-ai-action-plans/>
57. Ortak Yönetim ve Yapay Zekâ Düzenlemesinin Geleceği - Harvard Hukuk Dergisi, <https://harvardlawreview.org/print/vol-138/co-governance-and-the-future-of-ai-regulation/>
58. Güvencesiz "Açık Kaynaklı" Yapay Zekâ Nasıl Düzenlenir: Muafiyet Yok | TechPolicy.Press, <https://www.techpolicy.press/how-to-regulate-unsecured-opensource-ai-no-exemptions/>
59. Açık ve Kapalı Değil: Güvenli Olmayan Yapay Zekâ Nasıl Düzenlenir, <https://www.cigionline.org/articles/not-open-and-shut-how-to-regulate-unsecured-ai/>
60. Araştırma - Açık Kaynaklı Yapay Zekâ Modellerinin Küresel Güvenlik Riskleri, <https://www.globalcenter.ai/research/the-global-security-risks-of-open-source-ai-models>



Türkiye Bilişim Vakfı
www.tbv.org.tr

EK 1: GÜNCELLEMELER

Bu ek çalışma, ana raporda ve yürütme kurulu sunumlarında yer alan "Yönetişim, Etik, Risk ve Sorumluluk" başlıklarının, son aylarda küresel ölçekte yaşanan sarsıcı jeopolitik ve teknolojik kırılımlar doğrultusunda güncellenmesi amacıyla hazırlanmıştır. Son iki ayda yapay zekâ ekosisteminin yönünü değiştiren mikro ve makro gelişmeler şu şekildedir:

1. Model Evreni, İleri Yetenekler ve Akut Güvenlik Kırılımları

- **Anthropic "Mythos" ve Kamusal Güvenlik Sınırı:** Anthropic şirketi, siber zafiyetleri ve yazılım açıklarını bulma kapasitesi üssel olarak artan yeni modeli *"Mythos"**un kodlarını, kamuya açamayacak kadar güçlü ve tehlikeli olduğunu ilan etmiştir. Test süreçlerinde dünyanın en güvenli işletim sistemlerinde ve tarayıcılarında, aralarında 27 yıldır fark edilmeyen sistemik açıkların da bulunduğu binlerce zafiyet keşfeden Mythos, yapay zekanın "kendi kendini eğiten bir siber silaha" dönüşme riskini laboratuvar ortamından çıkarıp ticarileşme sınırına taşımıştır. Şirket, modeli halka kapatarak yalnızca Apple, Google, Microsoft, JPMorgan ve Linux Foundation gibi kritik aktörlere savunma hatlarını hazırlamaları için sınırlı erişim sağlamıştır.
- **OpenAI GPT-5.6, Fable ve "Ajan" Çağının Kaotik Evrimi:** OpenAI'nın pazar dengelerini değiştiren GPT-5.6 ve kod analitiğinde çığır açan *"Fable"* mimarileri, raporda bahsedilen "Ajan Yapay Zekâ" (Agentic AI) kavramını tamamen otonom bir boyuta taşımıştır. Ancak bu durum, asgari insan gözetimiyle çalışan otonom araçların (agents) klasik siber güvenlik kontrol noktalarını bütünüyle bypass etmesi riskini doğurmuştur.
- **"Buzz" Girişimi ve Kusursuz İstismar:** Beş farklı yapay zekâ ajanını tek bir kolektif akılla birleştiren *"Buzz"* adlı İsrail menşeli bir girişim, bilinen tüm kurumsal siber açıkları %98 başarı oranıyla istismar edebildiğini açıklamıştır. Bu durum, Palo Alto Networks CEO'sunun *"Önümüzdeki altı ay içinde tek bir kötü niyetli aktör, yapay zekâ ajanları sayesinde tüm bir siber suç takımının işini tek başına yapabilecek"* uyarısını doğrulamaktadır.

2. Küresel Regülasyon Kıskaçları ve Jeopolitik Kırılımlar

- **ABD'nin Reaktif "Serbest Bırak-Kısıtla" Politikası:** Trump yönetimindeki ABD'nin büyük teknoloji şirketlerini destekleyen serbest piyasa ve "teşvik edilen öz düzenleme" modeli, ulusal güvenlik ve egemenlik (Sovereign AI) refleksleriyle sert bir kırılma yaşamıştır. Yapay zekâ yeteneklerinin kontrolsüz yayılımının biyolojik ve siber silah üretimini kolaylaştırması üzerine, Washington yönetimi önce serbest bıraktığı modellere proaktif ve ani ihracat/erişim kısıtlamaları getirmek zorunda kalmıştır.
- **Teknoloji Devlerinin AB İsyanı ve Regülatif Kesişim:** Rapor metninde belirtilen AB Yapay Zekâ Yasası ve Kasım 2026'da yürürlüğe girecek Kusursuz Sorumluluk (Strict Liability) içeren Ürün Sorumluluğu Yönergesi, ABD merkezli teknoloji devlerinin sert muhalefetiyle karşılaşmıştır. Şirketler, AB'nin katı ve "vatandaş odaklı" regülasyonlarının küresel rekabeti tıkadığını savunarak ABD yönetimine Avrupa standartlarına karşı misilleme yapılması yönünde lobi faaliyetlerini hızlandırmıştır.
- **Çin'in "DeepSeek" Hamlesi ve Ucuz Açık Kaynak Stratejisi:** Çin, devlet merkezli komuta yapısının bir çıktısı olarak, maliyetleri %75'e kadar düşüren ve tekrarlayan sorgularda maliyeti onda bire indiren DeepSeek modelleriyle küresel geliştirici sadakatini ele



Türkiye Bilişim Vakfı
www.tbv.org.tr

geçirme stratejisini derinleştirmiştir. Bu hamle; geçmişte güneş panellerinde ve elektrikli araç bataryalarında uygulanan "*önce ucuzlat, yaygınlaştır, bağımlılık yarat, sonra ekosistemi tek başına şekillendir*" doktrininin yapay zekâ kod evrenine uyarlanmasıdır.

3. Altyapı Tehditleri: Yeniden Baş Gösteren Silikon ve Yonga Krizleri

- **Pandemi Dönemi Benzeri Tedarik Kilitlenmeleri:** Yapay zekâ modellerinin üssel büyümesi ve veri merkezlerinin 1 GW kapasite hedeflerine ulaşma iştahı, küresel çip tedarik zincirini yeniden kilitlemiştir.
- **Yonga ve Nadir Element Ambargoları:** Tayvan merkezli üretim hatlarındaki jeopolitik riskler ve çip yapımında kullanılan nadir toprak elementlerine yönelik karşılıklı ambargolar, Covid-19 dönemindeki silikon krizinin bir benzerini tetiklemiştir. Donanım (Compute/GPU) erişim maliyetlerinin döviz kuru ve arz kıtlığı nedeniyle tırmanması, start-up'ların küresel bulut maliyetleri altında ezilmesi riskini (ROI Paradoksu) akut hale getirmiştir.

4. Sosyo-Ekonomik ve Hukuki Hak Savaşları

- **"İnsan-Makine" Ayrımında Kültürel Kedi-Fare Oyunu:** Dezenformasyon ve fotogerçekçi sentetik içeriklerin yayılmasıyla, geleneksel doğrulama yöntemleri (CAPTCHA vb.) tamamen işlevsiz kalmıştır. Kurumlar, insan ile makineyi ayırt edebilmek için ortak kültürel hafıza, sezgi ve toplumsal referansları ölçen dinamik testlere (Örn: "*Keloğlan neden kel?*") yönelmiştir. Ancak yapay zekanın üssel öğrenme hızı, bu yapıyı kalıcı bir çözüm olmaktan çıkarıp dinamik bir "kedi-fare" oyununa dönüştürmüştür.
- **Fikri Mülkiyet Savaşında Lisanslama Kapanı:** Raporda detaylandırılan yüksek profilli davaların (The New York Times vs OpenAI, Disney vs Midjourney) ara formülleri netleşmeye başlamıştır. LLM üreticileri büyük medya organlarıyla lisans anlaşmaları imzalamaya başlamış da, bugüne kadar modellerin "rıza dışı" öğrendiği telifli verilerin model mimarisinin içinden sökülüp atılamaması, telif hukukunda "geriye dönük telafi" krizini büyütülmüştür.



Türkiye Bilişim Vakfı
www.tbv.org.tr

EK 2: KÜRESELYÖNETİŞİM, ETİK ve RİSK RAPORU-ULUSAL YAPAY ZEKÂ STRATEJİSİ: STRATEJİK UYUM ANALİZİ

1. Makro Ekonomik Göstergeler ve Yatırım Paradoksu

Küresel Rapor Bulguları

- **Ajan Çağının Ekonomisi:** Üretken YZ'nin küresel ekonomiye yıllık potansiyel katkısı \$2.6\$ ila \$4.4\$ trilyon dolar arasındadır. 2026 yılı itibarıyla pilot aşamalar geride kalmış, şirketlerin %25'i projelerinin en az %40'ını canlı üretim ortamına (production) taşımıştır.
- **Yatırım Paradoksu:** Şirketlerin %91'i YZ yatırımlarını artırırken, bunu bilançolarına anlamlı bir ciro artışı olarak yansıtılabenlerin oranı henüz %20 seviyesindedir. Ancak YZ yönetişimine \$25\$ milyon dolardan fazla bütçe ayıran öncü kurumlar, net kârlarında %5'in üzerinde artış görmeye başlamıştır.

Ulusal Strateji İzdüşümü & Boşluk Analizi

- **Gecikmenin Maliyeti:** Ulusal eylem planı, YZ'nin Türkiye ekonomisine yıllık \$50\$-\$60\$ milyar dolar ek katkı sağlama potansiyelini ortaya koymaktadır. Küresel rapordaki "canlıya geçiş (scale) hızlanması" dikkate alındığında, ulusal düzeyde yaşanacak 5 yıllık bir duraksamanın bu katkıyı %5'ten %1'e düşüreceği ve **1 Trilyon TL'lik kayba** yol açacağı uyarısı küresel verilerle tamamen uyumludur.
- **Yatırım Hedefi:** Küresel YZ yatırımları 500 milyar doları aşarken Türkiye'nin aldığı payın %1'in altında kalması, 2026–2030 eylem planındaki **10 Milyar Dolarlık özel sektör ağırlıklı yatırım mobilizasyonu** hedefini bir tercih olmaktan çıkarıp akut bir zorunluluk haline getirmektedir.

2. Risk Boyutu: Vatandaş ve Dijital Güvenlik Tehditleri

Küresel Rapor Bulguları

- **Gerçeklik Üretimi ve Deepfake:** Tehdit veri toplamaktan fotogerçekçi sentetik gerçeklik üretimine kaymıştır. Taylor Swift vakasında görülen rıza dışı sentetik persona üretimi, akran zorbalığı ve siber zorbalık ekosistemine entegre olmuştur.
- **Bilgi Bütünlüğü Krizi:** Seçimlerde adayların deepfake videoları ve ses klonlama (voice cloning) robot aramaları yoluyla seçmen manipülasyonu teoriden somut gerçeğe dönüşmüştür.

Ulusal Strateji İzdüşümü & Sinerji Noktaları

- **"Dijital Kalkan" Doğrulaması:** Küresel raporda genç nüfusun sentetik içeriklerle psikolojik travmalara ve sosyal izolasyona sürüklenmesi bulgusu, Ulusal Strateji'deki **"13-16 yaş altı için ebeveyn izninin sıkılaştırılması ve genel YZ platformlarında 'Çocuk Modu' zorunluluğu"** eylemini doğrudan gerekçelendirmektedir.



Türkiye Bilişim Vakfı
www.tbv.org.tr

- **C2PA Standardı Zorunluluğu:** Küresel raporda dezenformasyona karşı donanım seviyesinde doğrulama sunan C2PA standardının (Leica, Nikon, Qualcomm entegrasyonları) yükselişi vurgulanmaktadır. Ulusal eylem planının, **"Resmi kamu iletişimlerinde bilgi bütünlüğü standardı olarak C2PA kullanımını zorunlu kılma"** maddesi, küresel en iyi uygulama (best practice) hatlarını tam isabetle yakalamıştır.

3. Kurumsal Boyut: Siber Güvenlik, Ajan Tehditleri ve Kısaç Hareketi

Küresel Rapor Bulguları

- **Sofistike Dolandırıcılık:** Sosyal mühendislik, ses klonlama ve gerçek zamanlı görüntü sahtekârlığı klasik güvenlik protokollerini aşmıştır. Arup firmasının görüntülü konferans deepfake saldırısı ile **25.6 milyon dolar** dolandırılması bunun en sarsıcı örneğidir.
- **Otonom (Agentic) Riskler:** Beş ajanı birleştirerek sistemleri %98 başarıyla istismar eden "Buzz" gibi yapay zekâ ajanları, asgari insan gözetimiyle siber zafiyetleri suistimal etmektedir. Fiyat tespiti ve algoritmik antitröst ihlalleri (RealPage vakası) hukuki gri alanlar yaratmaktadır.

Ulusal Strateji İzdüşümü & Sinerji Noktaları

- **Hukuki Pozisyon (TCK ve Borçlar Kanunu):** Küresel raporda otonom ajanların deterministik olmayan yapısı ve bağımsız suç işleme potansiyeli ele alınmaktadır. Türkiye'nin önerdiği **"Yeni bir YZ kanunu yerine TCK ve Borçlar Kanunu'nu güncelleyerek, suçun otonom sistemler aracılığıyla işlenmesini ağırlaştırıcı sebep sayma"** stratejisi, küresel kaotik yasal paralelliğe karşı son derece esnek ve proaktif bir yanıttır.
- **Siber Savunma Entegrasyonu:** WormGPT ve FraudGPT gibi siber suç araçlarının giriş bariyerini düşürmesi karşısında, stratejide yer alan **"Savunma sanayiindeki İHA/SİHA otonom tecrübesinin siber savunmaya entegrasyonu"** eylemi, ulusal güvenlik açısından bir tercih olmaktan çıkıp zorunluluk haline gelmiştir.

4. Altyapı ve Egemenlik: Çip Krizleri ve "Sovereign AI"

Küresel Tehdit (2026)

Gelişmiş modellerin nadir toprak elementleri ambargoları, Tayvan odaklı jeopolitik riskler ve tekrarlayan silikon/yonga krizleri nedeniyle donanım (Compute/GPU) tedariki durma noktasına gelmiştir.

Ulusal Strateji Yanıtı

- **Ulusal GPU Kredisi:** Altyapı kilitlemelerine karşı geliştirilen, yerli start-up'ların AWS/Azure maliyetleri altında ezilmesini önleyecek **"Ulusal Bulut/GPU Kredisi"** altyapısı ve hedeflenen **1 GW Veri Merkezi Kapasitesi**, dijital egemenliğin (Sovereign AI) temel taşıdır.

- **BİLGE LLM ve Açık Veri:** Küresel ekosistemde en güçlü modellerin (Örn: Kamusal zafiyet bulma yeteneği yüzünden halka kapatılan Anthropic "Mythos" veya OpenAI Fable) en az şeffaf olanlar olduğu tespitiyle, Türkiye'nin Haziran 2026'da tanıttığı **BİLGE LLM** projesi ve dikey alanlarda (sağlık, hukuk, tarım) kamu verilerinin açık veri havuzuna dönüştürülerek millileştirilmesi stratejisi birebir örtüşmektedir.

Küresel Yönetişim Etik ve Risk Raporu Matrisi ve Türkiye Stratejisi Eşleşmesi

Aşağıdaki karşılaştırmalı matris, küresel raporda tanımlanan akut risklerin, Ulusal Strateji'de hangi operasyonel eylemlerle sönlendirildiğini özetlemektedir:





Türkiye Bilişim Vakfı
www.tbv.org.tr

EK 3: ULUSAL YAPAY ZEKA VİZYONU ÖZET DEĞERLENDİRMESİ

Ulusal Yapay Zeka Vizyonu'nun yönetici özeti, stratejik hedefleri ve eylem planı aşağıda 4 temel ekseninde özetlenmiştir:

1. Mevcut Durum ve Ekonomik Kaldıraç Potansiyeli

- **Küresel Sıralamadaki Yeri:** Türkiye, *Tortoise Global AI Index* raporuna göre 83 ülke arasında **34. sıraya** yükselmiş (2021'de 44. sıradaydı); ancak *Oxford Insights Hükümet AI Hazırlık Endeksi*'nde 195 ülke arasında **53. sırada** (58.91/100 puan) kalarak ilk 20 hedefinin gerisinde kalmıştır.
- **Yatırım Eksiği:** Türkiye, 2026 yılında 500 milyar doları aşan küresel yapay zekâ yatırımlarından henüz **%1'den daha az** pay almaktadır.
- **Ekonomik Katkı:** Yapay zekâ dönüşümünün 10 yıl içinde Türkiye GSYİH'sine yıllık **50-60 milyar dolar** (yaklaşık %5 ila %7 oranında) ek katkı sağlama potansiyeli hesaplanmıştır.
- **Gecikmenin Ağır Bedeli:** Yapay zekâ adaptasyonunda yaşanacak **5 yıllık bir gecikme**, bu ekonomik katkıyı %5'ten %1'e düşürecek ve **1 Trilyon TL'lik** devasa bir ekonomik kayba yol açacaktır.

2. İş Piyasası ve İstihdam Etkisi

- **Dönüşümün Ölçeği:** Türkiye'de **31 milyon iş** (toplam istihdamın %55'i) yapay zekâ ile birlikte çalışma veya dönüşüm kapsamına girecektir.
- **En Çok Etkilenen Sektörler:** Finans, bilişim, imalat ve idari hizmetler otomasyon ve ajan mimarilerinden en yoğun etkilenecek alanlardır.
- **İstihdam İyimserliği:** Küresel raporlarla paralel olarak, yapay zekanın doğrudan işsizliği artırmayacağı, yeni iş kolları açacağı öngörülmektedir; istihdamın sadece %4'ü yüksek otomasyon riskiyle karşı karşıyadır. Çalışanların %47'si ise teknolojinin işlerini olumlu etkileyeceğine inanmaktadır.

3. Akil Yönetişim: "Koru - Güçlendir - Yerelleştir" (9 Adımlık Mimari)

Strateji, hantal ve inovasyonu boğan devasa yasalar çıkarmak yerine; **"teknolojiyi değil, zararlı eylemi cezalandıran"** çevik, risk tabanlı bir hukuki ve operasyonel altyapıyı savunur.

1. **Suç Odaklı Yaptırım (TCK Uyarlaması):** Yapay zekâ bir liability shield (sorumluluktan kaçış kalkanı) olamaz. Suçun otonom sistemlerle işlenmesi ağırlaştırıcı sebep sayılmalı, KVKK'ya "algoritmik hesap verebilirlik" eklenmelidir.
2. **Dijital Kalkan:** Çocukların ve savunmasız grupların manipülasyonunu engellemek için genel YZ platformlarında yaş doğrulama ve "Çocuk Modu" zorunlu kılınmalıdır.
3. **Dengeli Risk Yönetimi (Regulatory Sandbox):** Girişimleri bürokrasiye boğmamak için start-up ve KOBİ'lere özel "Düzenleyici Kum Havuzları" kurulmalı, ağır cezalar olmadan test imkânı verilmelidir.



Türkiye Bilişim Vakfı
www.tbv.org.tr

- Ulusal GPU Kredisi & Altyapı:** Girişimlerin küresel bulut maliyetleri altında ezilmemesi için devlet öncülüğünde araştırmacılara "Ulusal Bulut/GPU Kredisi" ve sübvansede edilmiş veri merkezleri sağlanmalıdır.
- Türkçe LLM ve Açık Veri Seferberliği:** Küresel modellere bağımlı kalmamak adına; yerli kültür ve dil ile eğitilmiş dikey modeller (hukuk, sağlık, tarım) desteklenmeli, kamu verileri anonimleştirilerek makine okunabilir "Açık Veri Havuzlarına" dönüştürülmelidir.
- Siber Savunma Entegrasyonu:** Savunma sanayisindeki İHA/SİHA ve otonom sistem tecrübesi siber savunmaya taşınmalı, otonom silahlarda uluslararası (BM/OECD) etik normlara uyum taahhüt edilmelidir.
- Eğitim ve İş Gücü Dönüşümü:** Yasaklamak yerine eğitmeyi seçerek her kademede "YZ Okuryazarlığı" zorunlu kılınmalı, beyin güçünü tersine çevirmek için "YZ Araştırmacı Vizesi" oluşturulmalıdır.
- Şeffaflık Kartları (Model Künyesi):** Piyasaya sürülen her model için standart bir "Model Künyesi" (Hangi veriyle eğitildi? Sınırlılıkları nedir? Telif ihlali var mı?) zorunluluğu getirilmelidir.
- Otonom Devlet Asistanları (Agentic Government):** e-Devlet yapısı pasif bir belge sağlayıcıdan, vatandaş adına aktif işlem yapabilen (Örn: "Vergi borcumu yapılındır ve ödeme planı çıkar") otonom asistan merkezine dönüştürülmelidir.

4. Vizyon 2030: Somut Hedefler ve Acil Gündem

Haziran 2026'da ilan edilen **2026–2030 Eylem Planı** doğrultusunda Türkiye'nin önüne koyduğu makro hedefler şunlardır:

- Yatırım Mobilizasyonu:** Özel sektör ağırlıklı **10 Milyar Dolar** altyapı yatırımı.
- Teknolojik Altyapı:** Ulusal dijital altyapı genişlemesi için **1 GW Veri Merkezi Kapasitesi**.
- Milli Model:** TÜBİTAK BİLGEM tarafından Haziran 2026'da tanıtılan yerli büyük dil modeli **BİLGE LLM**'in sektörel dikeylerde yaygınlaştırılması.
- İnsan Kaynağı:** 2 yıl içinde 81 ilde **5 Milyon vatandaşa yapay zekâ okuryazarlığı eğitimi** verilmesi; sektöre **110.000 YZ Uzmanı** ve 100.000 Uygulama Profesyoneli kazandırılması.
- Girişim Ekosistemi:** AITR merkezinde birleşen; iş dünyası, kamu ve akademinin ortak gücüyle çalışan mevcut **457 yapay zekâ girişiminin** (çoğunluğu %75 oranında B2B odaklı) desteklenerek küresel ekosistemde **ilk 20 ülke arasına girilmesi**.