TEKNOLOJİ KOMİTESİ

Çalışma Rehberi

1. Yapay Zeka ve Siber Güvenlik:
Tehditler ve Savunma Mekanizmaları
2. Yapay Zekanın Etik Sınırları:
Otonom Karar Alma ve Hesap Verebilirlik
3. İş Gücünde Yapay Zeka:
Risk Altındaki Meslekler
4.İnsan-AI İşbirliği:
Yerinden Edilme mi, Dönüşüm mü?

BELXTFL

İçindekiler

Moderatörlerden Mektup

Sayın Katılımcılar,

Sabırsızlıkla beklediğimiz bu muhteşem konferansta ve heyecan verici komitede sizlerin moderatörleriniz olmaktan büyük onur duyuyoruz. Umuyoruz ki önümüzdeki bu iki gün hepimiz için verimli geçecek ve ufkumuzu genişletecek. Sayın Prof. Dr. İbrahim Arpacı'ya teşrifleri için teşekkür eder, kendilerinin vizyoner bakış açısıyla çalıştayımıza değerli katkılar sağlayacağına olan inancımızı ifade ederiz.

Bu komite, günümüzün en kritik dönüşüm alanlarından biri olan yapay zekâ ve dijital teknolojilerin güvenlik, etik, iş gücü ve insan-makine etkileşimi üzerindeki etkilerini çok boyutlu biçimde ele almayı amaçlamaktadır.

İçinde bulunduğumuz dönem, teknolojinin yalnızca bir araç olmaktan çıkıp karar alma süreçlerine doğrudan etki eden bir yapıya dönüştüğü bir süreci temsil etmektedir. Yapay zekâ destekli siber saldırılardan deepfake teknolojilerine, algoritmik önyargıdan otonom sistemlerin sorumluluk tartışmalarına kadar birçok konu artık teorik birer ihtimal değil, doğrudan karşı karşıya olduğumuz gerçekliklerdir.

Çalıştay süresince dört ana eksen üzerinde ilerleyeceğiz: yapay zekâ destekli siber tehditler ve savunma mekanizmaları, yapay zekânın etik sınırları ve hesap verebilirlik, otomasyonun iş gücü üzerindeki dönüştürücü etkileri ve son olarak insan ile yapay zekâ arasındaki iş birliği modellerinin geleceği. Bu başlıkların her biri, yalnızca teknolojik değil aynı zamanda hukuki, ekonomik ve toplumsal sonuçlar da doğurmaktadır.

Gündem maddelerinin altında gerçek hayattaki durumlarda bağlantı kurabilmeniz için eklediğimiz, konularla ilişkin haberlere ulaşabilirsiniz. Söz konusu kaynaklar yabancı dilde olup, sayfa üzerinden Türkçeye çevrilerek incelenebilir. Herhangi bir aksaklıkla karşılaşmanız durumunda tarafınıza Türkçe çevirileri ayrıca iletilecektir. Herhangi bir sorunuz olması halinde bizimle iletişime geçebilirsiniz.

Verimli, yoğun ve düşündürücü iki gün geçirmeyi umuyor; tüm katılımcılarla birlikte güçlü bir akademik tartışma ortamı oluşturmayı hedefliyoruz.

Saygılarımızla,
Teknoloji Komitesi Moderatörleri
Ebrar Begüm Aslan & Levent Kırım

1. Giriş

Yapay zekâ ve dijital teknolojiler, 21. yüzyılın en hızlı gelişen alanlarından biri olarak devletlerin, şirketlerin ve toplumların yapısını köklü biçimde dönüştürmektedir. Sağlık, eğitim, ekonomi, iletişim ve savunma gibi birçok sektörde yaygın olarak kullanılan yapay zekâ sistemleri; verimliliği artırmakta, karar alma süreçlerini hızlandırmakta ve teknolojik gelişimi ileri taşımaktadır. Ancak bu hızlı dönüşüm, beraberinde önemli etik, ekonomik ve güvenlik sorunlarını da getirmektedir. Özellikle siber güvenlik alanında yapay zekâ destekli saldırıların artması, deepfake teknolojilerinin bilgi manipülasyonunda kullanılabilmesi ve otonom kötü amaçlı yazılımların gelişmesi, küresel ölçekte yeni tehditlerin ortaya çıkmasına neden olmaktadır.

Bunun yanı sıra yapay zekânın otonom karar alma kapasitesi; hesap verebilirlik, mahremiyet, insan hakları ve etik sınırlar konusunda uluslararası düzeyde tartışmalara yol açmaktadır. Algoritmaların tarafsızlığı, veri güvenliği ve yapay zekâ sistemlerinin bireyler üzerindeki etkileri günümüzde en önemli meselelerden biri haline gelmiştir. Aynı zamanda otomasyon teknolojilerinin gelişmesi, iş gücü piyasasında büyük değişimlere neden olmakta; bazı mesleklerin dönüşmesine veya ortadan kalkmasına yol açarken yeni çalışma alanlarının oluşmasını da beraberinde getirmektedir. İnsan ve yapay zekâ arasındaki ilişkinin geleceği, teknolojik ilerlemenin toplumsal etkileri açısından kritik önem taşımaktadır.

Bu komite, yapay zekânın siber güvenlikten etik meselelere, iş gücü dönüşümünden insan-AI iş birliğine kadar uzanan çok boyutlu etkilerini ele alarak teknolojik gelişmelerin küresel sistem üzerindeki sonuçlarını incelemeyi amaçlamaktadır.

Aşağıda komite ile ilgili anahtar kelimelere ulaşabiliriniz.

1.1. Anahtar Kelimeler

- **Yapay Zekâ (AI):** İnsan benzeri öğrenme, analiz etme ve karar verme yeteneğine sahip bilgisayar sistemlerini ifade eder. Siber güvenlik alanında hem saldırı hem savunma amacıyla kullanılmaktadır.

- **Siber Güvenlik:** Bilgisayar sistemlerini, ağları ve verileri dijital saldırılardan koruma sürecidir. Devletler, şirketler ve bireyler için kritik öneme sahiptir.
- **Yapay Zekâ Destekli Siber Saldırılar:** Yapay zekâ teknolojileri kullanılarak gerçekleştirilen gelişmiş dijital saldırılardır. Bu saldırılar daha hızlı, uyarlanabilir ve tespit edilmesi daha zor olabilir.
- **Veri Gizliliği (Data Privacy):** Bireylerin kişisel bilgilerinin korunması ve izinsiz kullanılmasının engellenmesi ilkesidir. Yapay zekâ çağında önemli bir tartışma konusudur.
- **Yapay Zekâ Etiği:** Yapay zekânın insan haklarına, adalet ilkesine ve etik değerlere uygun şekilde geliştirilmesini ve kullanılmasını amaçlayan kurallar bütünüdür.

2. Gündem Maddesi 1: Yapay Zekâ Kaynaklı Siber Tehditler ve Savunma Mekanizmaları

2.1. Gündem Maddesinin Tanımı

İnternetin küresel ölçekte yaygınlaşması ve dijital teknolojilerin günlük yaşamın merkezine yerleşmesiyle birlikte siber güvenlik, modern dünyanın en kritik meselelerinden biri haline gelmiştir. Günümüzde bankacılık işlemlerinden sağlık kayıtlarına, devlet belgelerinden askeri iletişim ağlarına kadar milyarlarca veri dijital sistemlerde saklanmaktadır. Bu durum, bilgi güvenliğini yalnızca bireysel bir sorun olmaktan çıkarıp ulusal güvenlik meselesi haline getirmiştir. Özellikle yapay zekâ teknolojilerinin son yıllarda hızla gelişmesi, siber güvenlik alanında hem savunma hem de saldırı mekanizmalarını büyük ölçüde değiştirmiştir. Yapay zekâ artık yalnızca verilen komutları yerine getiren bir sistem değil; veri analiz edebilen, örüntüleri tespit edebilen, öğrenebilen ve belirli ölçülerde bağımsız karar verebilen bir teknolojiye dönüşmüştür. Bu durum, siber saldırıların daha karmaşık hale gelmesine neden olurken aynı zamanda savunma sistemlerini de daha güçlü hale getirmiştir.

Geçmişte gerçekleştirilen siber saldırılar çoğunlukla insanlar tarafından manuel olarak yürütülürken, günümüzde yapay zekâ destekli sistemler sayesinde saldırılar otomatik biçimde gerçekleştirilebilmektedir. Özellikle makine öğrenimi algoritmaları,

milyonlarca veri örneğini inceleyerek güvenlik açıklarını çok kısa sürede tespit edebilmekte ve saldırı stratejilerini buna göre değiştirebilmektedir. Örneğin geleneksel kötü amaçlı yazılımlar belirli bir kod yapısına sahip olduğu için antivirüs programları tarafından kolayca algılanabiliyordu. Ancak yapay zekâ destekli kötü amaçlı yazılımlar, kendi kodlarını değiştirerek tespit edilmekten kaçabilmektedir. “Polymorphic malware” adı verilen bu yazılımlar, her saldırıda farklı bir dijital imza oluşturarak güvenlik sistemlerinin onları tanımasını zorlaştırmaktadır. Bazı gelişmiş zararlı yazılımlar ise girdikleri sistemdeki güvenlik önlemlerini analiz ederek davranışlarını değiştirebilmekte ve böylece aylar boyunca fark edilmeden çalışabilmektedir.

Yapay zekânın siber saldırılarda kullanıldığı en dikkat çekici alanlardan biri **phishing saldırılarıdır**. Geçmişte phishing mesajları genellikle yazım hataları içeren, kolay fark edilen sahte e-postalardan oluşurken, günümüzde yapay zekâ sayesinde son derece gerçekçi mesajlar üretilebilmektedir. Yapay zekâ sistemleri, sosyal medya hesapları, çevrim içi alışkanlıklar ve kamuya açık veriler üzerinden kişiler hakkında detaylı analiz yapabilmektedir. Bu sayede saldırganlar, hedef kişiye özel hazırlanmış mesajlar oluşturarak kullanıcıların güvenini kazanabilmektedir. Örneğin bir çalışanın yöneticisinden geldiğini düşündüğü sahte bir e-posta aracılığıyla şirket verileri ele geçirilebilmekte veya finansal dolandırıcılık gerçekleştirilebilmektedir. Özellikle büyük şirketlere yönelik gerçekleştirilen “**spear phishing**” saldırılarında yapay zekâ kullanımı son yıllarda ciddi ölçüde artmıştır.

Siber güvenlik alanında yapay zekânın en tehlikeli kullanım biçimlerinden biri de deepfake teknolojileridir. Deepfake, yapay zekâ kullanılarak sahte görüntü, ses veya video oluşturulması anlamına gelmektedir. Bu teknoloji sayesinde bir kişinin hiç söylemediği sözler söylemiş gibi gösterilmesi veya hiç yapmadığı eylemleri gerçekleştirmiş gibi yansıtılması mümkündür. İlk başlarda eğlence amacıyla kullanılan deepfake teknolojileri, zamanla siyasi manipülasyon ve dolandırıcılık gibi alanlarda ciddi tehdit oluşturmaya başlamıştır. Özellikle seçim dönemlerinde yayılan sahte videolar, kamuoyunu manipüle ederek toplumsal istikrarsızlığa yol açabilmektedir. Bunun yanı sıra bazı şirketlerde yöneticilerin sesleri taklit edilerek çalışanlardan milyonlarca dolarlık para transferleri istenmiş ve bu yöntemle büyük finansal dolandırıcılıklar gerçekleştirilmiştir. Uzmanlara göre deepfake teknolojilerinin

gelişmesi, gelecekte “görüntü kanıtı” kavramının güvenilirliğini ciddi biçimde sarsabilir.

Gösterge	Değer
Kurumların AI destekli saldırı deneyimleme oranı	%75+
Ortalama veri ihlali maliyeti	4-5 milyon $
Tespit süresindeki AI avantajı	%30-50

Yapay zekâ yalnızca saldırı mekanizmalarında değil, savunma sistemlerinde de büyük rol oynamaktadır. Geleneksel güvenlik sistemleri yalnızca önceden tanımlanmış tehditleri algılayabilirken, yapay zekâ destekli sistemler bilinmeyen saldırıları da tespit edebilmektedir. Özellikle bankalar, devlet kurumları ve büyük teknoloji şirketleri; ağ trafiğini sürekli analiz eden yapay zekâ sistemleri kullanmaktadır. Bu sistemler, normal kullanıcı davranışlarını öğrenerek olağan dışı hareketleri anında fark edebilmektedir. Örneğin bir çalışanın hesabına farklı bir ülkeden aniden erişim sağlanması veya kısa süre içerisinde olağan dışı veri transferi gerçekleştirilmesi durumunda sistem otomatik olarak alarm verebilmekte hatta erişimi engelleyebilmektedir. Bazı gelişmiş yapay zekâ sistemleri, saldırıya uğrayan bir ağı insan müdahalesi olmadan izole ederek saldırının yayılmasını önleyebilmektedir.

Yapay zekâ ve siber güvenlik ilişkisi devletler açısından da büyük önem taşımaktadır. Günümüzde birçok ülke, siber saldırıları geleneksel askeri tehditlerle eşdeğer görmektedir. Çünkü enerji santralleri, havaalanları, sağlık sistemleri, su altyapıları ve askeri ağlar gibi kritik sistemlerin dijitalleşmesi, olası bir siber saldırının fiziksel sonuçlar doğurabilmesine neden olmaktadır. Örneğin bir enerji altyapısına yönelik büyük çaplı siber saldırı, milyonlarca insanın elektriksiz kalmasına yol açabilir. Benzer şekilde hastanelerin dijital sistemlerine yapılan saldırılar sağlık hizmetlerini tamamen durdurabilmektedir. Bu nedenle devletler, yapay zekâ destekli savunma

sistemlerine milyarlarca dolarlık yatırımlar yapmaktadır. Aynı zamanda ülkeler arasında görünmeyen bir “siber silahlanma yarışı” oluşmuş durumdadır.

Ancak teknolojinin bu kadar hızlı gelişmesine rağmen uluslararası hukuk sistemleri aynı hızda ilerleyememektedir. Günümüzde yapay zekâ destekli siber saldırılara yönelik küresel ölçekte bağlayıcı ve kapsamlı düzenlemeler bulunmamaktadır. Siber saldırıların kaynağının tespit edilmesi çoğu zaman zor olduğu için devletler arasında suçlama krizleri yaşanabilmektedir. Ayrıca yapay zekânın kötü amaçlı kullanımını sınırlandıracak etik kuralların eksikliği, gelecekte çok daha büyük güvenlik sorunlarına yol açabileceği endişesini artırmaktadır. Bu nedenle yapay zekâ ve siber güvenlik konusu yalnızca teknik değil; aynı zamanda hukuki, siyasi ve etik boyutlarıyla ele alınması gereken küresel bir mesele haline gelmiştir.

2.2. Anahtar Terimler

- **Deepfake Teknolojisi:** Yapay zekâ kullanılarak sahte görüntü, video veya ses oluşturulmasını sağlayan teknolojidir. Dezenformasyon ve dolandırıcılık amacıyla kullanılabilmektedir.
- **Phishing / Hedefli Oltalama:** Kullanıcıları kandırarak şifre, banka bilgisi veya kişisel veri elde etmeyi amaçlayan siber saldırı yöntemidir. Yapay zekâ sayesinde daha gerçekçi hale gelmiştir.
- **Zararlı Yazılım (Malware):** Bilgisayar sistemlerine zarar vermek, veri çalmak veya sistemi kontrol etmek amacıyla geliştirilen yazılımlardır. Virüsler ve fidye yazılımları bu kategoriye girer.
- **Veri İhlali:** Gizli veya kişisel bilgilerin yetkisiz kişiler tarafından ele geçirilmesi durumudur. Büyük şirketler ve devlet kurumları için ciddi risk oluşturur.
- **Kritik Altyapı:** Enerji, sağlık, ulaşım ve iletişim gibi toplumun işleyişi için hayati öneme sahip sistemlerdir. Siber saldırıların temel hedefleri arasında yer alır.
- **Ulusal Siber Güvenlik:** Bir devletin dijital altyapısını ve vatandaşlarının verilerini siber tehditlere karşı koruma politikalarını ifade eder.

- **Dezenformasyon:** Yanlış veya manipüle edilmiş bilgilerin toplum üzerinde etki yaratmak amacıyla yayılmasıdır. Deepfake teknolojileriyle birlikte etkisi artmıştır.
- **Bilgi Savaşı (Information Warfare):** Bilginin propaganda, manipülasyon veya dijital araçlar yoluyla stratejik amaçlarla kullanılmasıdır. Özellikle siyasi süreçlerde etkili olmaktadır.
- **Siber Savunma Mekanizmaları:** Siber saldırıları önlemek, tespit etmek ve etkilerini azaltmak amacıyla kullanılan güvenlik sistemleri ve stratejileridir.
- **Uluslararası Siber Hukuk:** Siber saldırılar, veri güvenliği ve dijital haklarla ilgili uluslararası kuralları ve hukuki düzenlemeleri kapsar.
- **Otonom Zararlı Yazılım:** İnsan müdahalesi olmadan hareket edebilen ve kendi kararlarını verebilen gelişmiş kötü amaçlı yazılımlardır. Yapay zekâ destekli siber tehditlerin en tehlikeli örneklerinden biridir.
- **Siber Terörizm:** Siyasi, ideolojik veya toplumsal amaçlarla dijital sistemlere yönelik gerçekleştirilen siber saldırıları ifade eder. Kritik altyapıları hedef alarak büyük çaplı kaos ve korku yaratmayı amaçlayabilir.
- **Çok Faktörlü Kimlik Doğrulama (MFA):** Kullanıcıların bir sisteme giriş yaparken birden fazla doğrulama yöntemi kullanmasını sağlayan güvenlik sistemidir. Şifreye ek olarak telefon kodu veya biyometrik doğrulama gibi yöntemler içerir.
- **Siber Casusluk:** Devletler, şirketler veya gruplar tarafından gizli bilgi elde etmek amacıyla gerçekleştirilen dijital casusluk faaliyetleridir. Genellikle stratejik, askeri veya ekonomik bilgi toplamak için kullanılır.

2.3. Vaka İncelemeleri

2.3. Vaka İncelemesi: Hong Kong Deepfake CEO Dolandırıcılığı

2024 yılında Hong Kong'da gerçekleşen bir olay, yapay zekâ destekli siber tehditlerin ulaştığı boyutu gözler önüne sermiştir. Bir şirket çalışanı, üst düzey yöneticilerin katıldığı düşünülen çevrim içi bir toplantıya dahil olmuş ve toplantıda gördüğü kişilerin şirketin gerçek yöneticileri olduğuna inanmıştır. Ancak daha sonra bu kişilerin yapay zekâ kullanılarak oluşturulmuş deepfake görüntü ve ses kayıtları olduğu ortaya çıkmıştır. Toplantı sırasında çalışan, yöneticilerden geldiğini düşündüğü talimatlar doğrultusunda yaklaşık 25 milyon dolar tutarında para transferi

gerçekleştirmiştir. Olay, geleneksel güvenlik önlemlerinin yalnızca teknik saldırılara karşı yeterli olmadığını, yapay zekâ destekli kimlik sahteciliği ve sosyal mühendislik yöntemlerinin de ciddi bir güvenlik tehdidi oluşturduğunu göstermiştir. Bu vaka, deepfake teknolojilerinin finansal dolandırıcılık, kurumsal güvenlik ve dijital kimlik doğrulama sistemleri üzerindeki etkilerine ilişkin küresel tartışmaları yeniden gündeme taşımıştır.

İlgili Olayın Haberi: [Finance worker pays out $25 million after video call with deepfake 'chief financial officer' | CNN]

3. Gündem Maddesi 2: Yapay Zekanın Etik Sınırları, Otonom Karar Alma ve Hesap Verebilirlik

3.1. Gündem Maddesinin Tanımı

Yapay zekâ teknolojilerinin hızla gelişmesi, insan hayatının birçok alanında büyük dönüşümlere yol açmıştır. Günümüzde yapay zekâ sistemleri yalnızca veri işleyen araçlar olmaktan çıkmış; analiz yapabilen, öğrenebilen ve belirli ölçülerde bağımsız karar verebilen sistemlere dönüşmüştür. Sağlık sektöründe hastalık teşhislerinden finans alanında kredi değerlendirmelerine, eğitimden güvenlik uygulamalarına kadar birçok alanda yapay zekâ tabanlı sistemler aktif olarak kullanılmaktadır. Bu gelişmeler verimliliği artırırken aynı zamanda önemli etik ve hukuki tartışmaları da beraberinde getirmektedir. Özellikle yapay zekânın otonom karar alma kapasitesinin artması, insan kontrolünün sınırları ve hesap verebilirlik konularını küresel ölçekte önemli bir mesele haline getirmiştir.

Yapay zekâ sistemleri, karar alma süreçlerinde büyük miktarda veriyi analiz ederek insanlardan çok daha hızlı sonuçlar üretebilmektedir. Ancak bu sistemlerin tamamen tarafsız olduğu düşüncesi her zaman gerçeği yansıtmamaktadır. Yapay zekâ algoritmaları, beslendikleri verilerde bulunan önyargıları öğrenebilmekte ve bu önyargıları karar mekanizmalarına yansıtarak ayrımcılığa neden olabilmektedir. Örneğin işe alım süreçlerinde kullanılan bazı yapay zekâ sistemlerinin belirli cinsiyetleri veya etnik grupları dezavantajlı duruma düşürdüğü görülmüştür. Benzer şekilde yüz tanıma teknolojilerinde yaşanan hata oranları, bireysel haklar ve

mahremiyet konusunda ciddi endişeler yaratmaktadır. Bu durum, yapay zekâ sistemlerinin etik sınırlarının belirlenmesi gerektiğini ortaya koymaktadır.

Bir diğer önemli tartışma konusu ise hesap verebilirliktir. Yapay zekâ sistemleri yanlış bir karar verdiğinde sorumluluğun kimde olacağı günümüzde hâlâ net bir şekilde belirlenememiştir. Otonom araçların neden olduğu kazalar, yapay zekâ destekli sağlık sistemlerinde gerçekleşen yanlış teşhisler veya algoritmaların sebep olduğu veri ihlalleri, bu tartışmanın en önemli örnekleri arasında yer almaktadır. Böyle durumlarda sorumluluğun yazılımı geliştiren şirkete mi, sistemi kullanan kuruma mı yoksa teknolojiyi denetlemeyen devletlere mi ait olduğu konusunda farklı görüşler bulunmaktadır. Uluslararası hukuk sistemlerinde bu konuya ilişkin kapsamlı düzenlemelerin eksik olması da önemli bir sorun oluşturmaktadır.

Yapay zekânın etik sınırları yalnızca teknik değil; aynı zamanda insan hakları, mahremiyet, adalet ve toplumsal güven açısından da değerlendirilmesi gereken bir konudur. Özellikle devletlerin ve büyük teknoloji şirketlerinin topladığı büyük veri miktarı, bireylerin dijital özgürlükleri konusunda endişeleri artırmaktadır. Yapay zekâ sistemlerinin şeffaflığı, insan denetiminin korunması ve algoritmaların adil biçimde çalışmasının sağlanması, günümüzde uluslararası toplumun en önemli tartışma başlıklarından biri haline gelmiştir. Bu nedenle yapay zekâ teknolojilerinin gelişimi kadar, bu teknolojilerin etik ve hukuki çerçeveler içerisinde düzenlenmesi de büyük önem taşımaktadır.

3.2. Anahtar Terimler

- **Black Box AI (Kara Kutu Yapay Zekâ)**: Karar alma süreci insanlar tarafından tam olarak anlaşılamayan yapay zekâ sistemleridir. Bu durum, sistemlerin neden belirli kararlar verdiğinin açıklanmasını zorlaştırır.
- **Algorithmic Bias (Algoritmik Önyargı):** Yapay zekâ sistemlerinin eğitildiği verilerde bulunan önyargıları öğrenerek ayrımcı veya adaletsiz sonuçlar üretmesi durumudur.
- **Otonom Karar Alma:** Yapay zekânın insan müdahalesi olmadan bağımsız şekilde analiz yapıp karar verebilme kapasitesidir.

- **İnsan Denetimi (Human Oversight) :** Yapay zekâ sistemlerinin tamamen bağımsız hareket etmesini önlemek amacıyla insan kontrolü altında tutulması ilkesidir.
- **Yüz Tanıma Teknolojisi:** Bireyleri yüz özellikleri üzerinden tanımlayan yapay zekâ tabanlı biyometrik güvenlik sistemidir.
- **Tahmine Dayalı Polislik:** Yapay zekâ kullanılarak suç ihtimali yüksek bölgelerin veya kişilerin analiz edilmesine dayanan güvenlik uygulamasıdır.
- **Surveillance AI (Gözetim Amaçlı Yapay Zekâ):** Toplumun izlenmesi, veri toplanması ve davranışların analiz edilmesi amacıyla kullanılan yapay zekâ sistemleridir.
- **Veri Gizliliği:** Bireylerin kişisel verilerinin izinsiz erişim ve kullanıma karşı korunmasını ifade eder.
- **İşe Alım Algoritmalarında Önyargı:** Yapay zekâ destekli işe alım sistemlerinin belirli gruplara karşı ayrımcı sonuçlar üretmesi durumudur.
- **Otonom Silah Sistemleri:** İnsan müdahalesi olmadan hedef seçebilen ve saldırı gerçekleştirebilen yapay zekâ destekli silah sistemleridir.
- **Etik Hesap Verebilirlik:** Yapay zekâ sistemlerinin neden olduğu zarar veya hatalarda sorumluluğun kimde olduğuna ilişkin etik anlayıştır.
- **AI Regulation (Yapay Zekâ Regülasyonu):** Yapay zekâ teknolojilerinin güvenli ve etik kullanımını sağlamak amacıyla oluşturulan yasal düzenlemeler ve denetim mekanizmalarıdır.
- **Deep Learning (Derin Öğrenme):** Yapay zekânın büyük miktardaki veriyi analiz ederek öğrenmesini sağlayan gelişmiş makine öğrenimi yöntemidir.

3.3. Vaka İncelemeleri

3.3.1 Vaka İncelemesi: Amazon İşe Alım Algoritması

2018 yılında Amazon tarafından geliştirilen yapay zekâ destekli işe alım sistemi, özgeçmişleri analiz ederek uygun adayları belirlemek amacıyla kullanılmaktaydı. Ancak sistemin geçmiş işe alım verileriyle eğitilmesi, algoritmanın erkek adayları daha avantajlı değerlendirmesine yol açtı. Yapılan incelemeler sonucunda sistemin kadın adayları sistematik olarak daha düşük puanladığı ortaya çıktı ve proje sonlandırıldı. Bu olay, yapay zekâ sistemlerinin eğitildiği verilerde bulunan toplumsal

önyargıları öğrenebileceğini ve bu önyargıları karar alma süreçlerine yansıtabileceğini göstermiştir. Vaka, algoritmik önyargı, adalet, şeffaflık ve hesap verebilirlik tartışmalarının en bilinen örneklerinden biri olarak kabul edilmektedir.

İlgili Olayın Haberi: Amazon ditched AI recruiting tool that favored men for technical jobs

3.3.2. Vaka İncelemesi: Libya İç Savaşı ve Yapay Zekâ Destekli Otonom Silah Sistemleri

2021 yılında Birleşmiş Milletler Güvenlik Konseyi için hazırlanan uzman raporu, Libya iç savaşında kullanılan bazı yapay zekâ destekli insansız hava araçlarının, insan müdahalesi olmaksızın belirli hedefleri takip etme ve saldırı gerçekleştirme kapasitesine sahip olabileceğini ortaya koymuştur. Raporda özellikle otonom özellikler taşıyan dolaşan mühimmat sistemlerinin (loitering munition) çatışma ortamında kullanıldığı belirtilmiştir. Her ne kadar sistemlerin tamamen bağımsız şekilde ölümcül kararlar verip vermediği kesin olarak doğrulanmamış olsa da, rapor yapay zekâ destekli silahların savaş alanlarında giderek daha fazla rol oynadığını göstermesi açısından büyük önem taşımaktadır. Olay, bir hedefin belirlenmesi ve etkisiz hâle getirilmesi sürecinde insan kontrolünün ne ölçüde korunması gerektiği sorusunu gündeme getirmiş; otonom silah sistemlerinin uluslararası insancıl hukuk, etik sorumluluk ve hesap verebilirlik ilkeleriyle nasıl bağdaştırılacağı konusunda küresel tartışmaları hızlandırmıştır. Özellikle yanlış hedef tespiti veya sivil kayıplar yaşanması durumunda sorumluluğun kime ait olacağı konusu, yapay zekâ destekli silah sistemleri hakkındaki en önemli hukuki ve etik meselelerden biri olarak değerlendirilmektedir.

İlgili Olayın Haberi: Autonomous Drone Strike In Libya Subject Of Recent United Nations Report : NPR

4. Gündem Maddesi 3: İş Gücünde Yapay Zekâ ve Risk Altındaki Meslekler

4.1 Gündem Maddesinin Tanımı

Yapay zekâ teknolojilerinin son yıllarda hızla gelişmesi, küresel iş gücü piyasasında önemli değişimlerin yaşanmasına neden olmuştur. Sanayi Devrimi'nden bu yana teknolojik yenilikler çalışma hayatını sürekli dönüştürmüş olsa da yapay zekânın ortaya çıkardığı değişim, önceki dönüşümlerden daha kapsamlı ve hızlı gerçekleşmektedir. Günümüzde yapay zekâ sistemleri yalnızca fiziksel görevleri otomatikleştirmekle kalmamakta; veri analizi, içerik üretimi, müşteri hizmetleri, muhasebe ve karar destek süreçleri gibi zihinsel emek gerektiren alanlarda da kullanılmaktadır. Bu durum, işletmelerin verimliliğini artırırken aynı zamanda birçok mesleğin geleceği konusunda tartışmaları da beraberinde getirmektedir. Özellikle rutin ve tekrarlayan görevlerin yapay zekâ sistemleri tarafından yerine getirilebilmesi, bazı iş kollarının dönüşeceği veya ortadan kalkabileceği yönündeki endişeleri artırmıştır.

Yapay zekânın iş gücü üzerindeki etkileri sektörlere göre farklılık göstermektedir. Üretim sektöründe robotik sistemler ve otomasyon teknolojileri uzun süredir kullanılmakta olsa da günümüzde yapay zekâ destekli yazılımlar hizmet sektöründe de yaygınlaşmaya başlamıştır. Bankacılık alanında kredi değerlendirme süreçleri, müşteri hizmetlerinde sohbet botları, hukuk alanında belge inceleme sistemleri ve medya sektöründe içerik üretim araçları birçok görevi insan müdahalesine ihtiyaç duymadan gerçekleştirebilmektedir. Özellikle veri girişi, çağrı merkezi hizmetleri, temel muhasebe işlemleri ve rutin büro işleri gibi standartlaşmış görevlerin otomasyondan en fazla etkilenebilecek alanlar arasında olduğu düşünülmektedir. Buna karşılık yaratıcılık, eleştirel düşünme, liderlik ve karmaşık insan ilişkileri gerektiren mesleklerin yapay zekâ tarafından tamamen ikame edilmesinin daha zor olduğu değerlendirilmektedir.

Ancak yapay zekânın iş gücü üzerindeki etkileri yalnızca iş kayıplarıyla sınırlı değildir. Tarih boyunca teknolojik gelişmeler bazı meslekleri ortadan kaldırırken aynı zamanda yeni iş alanlarının ortaya çıkmasını da sağlamıştır. Yapay zekâ

mühendisliği, veri bilimi, algoritma denetimi, siber güvenlik ve dijital etik uzmanlığı gibi yeni meslekler son yıllarda hızla büyüyen alanlar arasında yer almaktadır. Bu nedenle birçok uzman, gelecekte yaşanacak sürecin yalnızca bir “yerinden edilme” değil, aynı zamanda bir “iş gücü dönüşümü” olarak değerlendirilmesi gerektiğini savunmaktadır. Bununla birlikte çalışanların yeni beceriler kazanabilmesi ve değişen ekonomik koşullara uyum sağlayabilmesi için eğitim sistemlerinin ve mesleki gelişim programlarının güncellenmesi gerektiği ifade edilmektedir.

Yapay zekâ ve istihdam ilişkisi aynı zamanda ekonomik eşitsizlik, sosyal adalet ve çalışma hakları gibi konuları da gündeme getirmektedir. Teknolojik dönüşümden elde edilen ekonomik kazançların nasıl paylaşılacağı, işini kaybeden çalışanların nasıl destekleneceği ve yapay zekâ kaynaklı iş gücü değişimlerinin toplum üzerindeki etkilerinin nasıl yönetileceği günümüzde birçok devletin karşı karşıya olduğu önemli sorunlar arasında yer almaktadır. Bu nedenle yapay zekânın iş gücü üzerindeki etkileri yalnızca ekonomik değil; aynı zamanda sosyal, siyasi ve etik boyutlarıyla ele alınması gereken küresel bir mesele olarak değerlendirilmektedir.

4.2. Anahtar Terimler

- **Otomasyon:** İnsanlar tarafından gerçekleştirilen görevlerin makine veya yazılımlar vasıtasıyla otomatik olarak gerçekleştirilmesidir.
- **Evrensel Temel Gelir (UBI):** Her vatandaşa koşulsuz ve düzenli gelir sağlanmasını öngören sosyal politika modelidir. Yapay zekâ kaynaklı işsizlik tartışmalarında sıkça gündeme gelmektedir.
- **Teknolojik İşsizlik:** Teknolojik gelişmeler sonucunda bazı işlerin ortadan kalkması nedeniyle ortaya çıkan işsizlik türüdür.
- **Augmentation (İnsan Yeteneklerini Güçlendirme):** Yapay zekânın insanların yerini almak yerine onların verimliliğini ve karar alma kapasitesini artırmak amacıyla kullanılmasıdır.
- **Yapay Zekâ Temettüsü (AI Dividend):** Yapay zekânın sağladığı ekonomik kazanç ve verimlilik artışını ifade eder. Bu kazancın nasıl paylaşılacağı önemli bir tartışma konusudur.
- **Dijital Taylorizm:** Çalışanların performansının algoritmalar aracılığıyla izlenmesi ve iş süreçlerinin verimlilik amacıyla optimize edilmesidir.

- **Moravec Paradoksu:** İnsanlar için zor olan analitik görevlerin yapay zekâ tarafından kolay yapılabilmesine karşın, insanlar için basit görünen algısal ve sosyal görevlerin makineler için zor olmasıdır.
- **Mesleki Kutuplaşma:** Orta beceri gerektiren işlerin azalırken yüksek ve düşük beceri gerektiren işlerin artması durumudur.
- **Yetenek Açığı:** İş piyasasının talep ettiği beceriler ile çalışanların sahip olduğu beceriler arasındaki uyumsuzluktur.
- **İnsan-Makine Tamamlayıcılığı:** İnsanların ve yapay zekâ sistemlerinin birbirlerinin güçlü yönlerini tamamlayarak birlikte çalışmasıdır.
- **Dördüncü Sanayi Devrimi:** Yapay zekâ, büyük veri ve otomasyon teknolojilerinin üretim ve hizmet sektörlerine entegre edildiği yeni sanayi dönemidir.
- **İnsan Sermayesi:** Bireylerin sahip olduğu bilgi, eğitim, deneyim ve becerilerin ekonomik değeridir.
- **Gig Ekonomisi:** Kısa süreli, proje bazlı ve serbest çalışma modellerine dayanan ekonomik sistemdir.
- **Yeniden Beceri Kazandırma (Reskilling):** Çalışanların değişen iş piyasasına uyum sağlayabilmeleri için yeni beceriler edinmesi sürecidir.

5. Gündem Maddesi 4: İnsan–AI İş Birliği, İş Gücü Dönüşümü ve Yerinden Edilme Tartışması

5.1. Gündem Maddesinin Tanımı

Yapay zekâ teknolojilerinin gelişmesiyle birlikte çalışma hayatının geleceğine ilişkin tartışmalar yeni bir boyut kazanmıştır. İlk dönemlerde yapay zekânın temel etkisinin insan emeğinin yerini almak olacağı düşünülmüş ve birçok mesleğin tamamen ortadan kalkacağı yönünde öngörüler yapılmıştır. Ancak günümüzde birçok uzman, yapay zekânın yalnızca bir otomasyon aracı olmadığını, aynı zamanda insan yeteneklerini destekleyen ve geliştiren bir teknoloji olarak değerlendirilebileceğini savunmaktadır. Bu nedenle yapay zekânın iş dünyasındaki etkileri yalnızca “yerinden edilme” kavramı üzerinden değil, insan ve yapay zekâ arasındaki iş birliği modelleri üzerinden de incelenmektedir.

Günümüzde sağlık, eğitim, mühendislik, finans ve medya gibi birçok sektörde yapay zekâ sistemleri çalışanlara yardımcı araçlar olarak kullanılmaktadır. Doktorlar teşhis süreçlerinde yapay zekâ destekli analizlerden yararlanırken, mühendisler karmaşık verileri değerlendirmek için yapay zekâ sistemlerinden destek almaktadır. Benzer şekilde gazeteciler, araştırmacılar ve hukuk uzmanları da büyük miktardaki bilgiyi daha hızlı analiz edebilmek amacıyla yapay zekâ araçlarını kullanmaktadır. Bu durum, yapay zekânın bazı görevleri üstlenirken insanların yaratıcılık, eleştirel düşünme, etik değerlendirme ve sosyal iletişim gibi alanlarda önemli roller üstlenmeye devam edeceğini göstermektedir.

Bununla birlikte insan-yapay zekâ iş birliğinin yaygınlaşması yeni sorunları da beraberinde getirmektedir. Yapay zekâ sistemlerine aşırı bağımlılık, çalışanların bazı becerilerini zamanla kaybetmesine neden olabilirken; algoritmaların hatalı sonuçlar üretmesi durumunda karar alma süreçlerinin güvenilirliği de tartışma konusu haline gelmektedir. Ayrıca iş yerlerinde görev dağılımının nasıl yapılacağı, çalışanların hangi alanlarda yeniden eğitileceği ve yapay zekâ destekli çalışma modellerinin iş gücü üzerindeki etkileri konusunda farklı görüşler bulunmaktadır. Özellikle düşük ve orta beceri gerektiren bazı mesleklerde dönüşüm sürecinin daha hızlı gerçekleşmesi, ekonomik ve sosyal eşitsizliklerin artabileceği yönündeki endişeleri güçlendirmektedir.

İnsan ve yapay zekâ arasındaki ilişkinin geleceği, yalnızca teknolojik gelişmeler açısından değil; aynı zamanda ekonomik verimlilik, çalışma hakları, eğitim politikaları ve toplumsal refah açısından da büyük önem taşımaktadır. Gelecekte başarılı iş modellerinin, insan yaratıcılığı ile yapay zekânın hesaplama ve analiz kapasitesini bir araya getiren hibrit çalışma sistemleri üzerine kurulacağı öngörülmektedir. Bu nedenle insan-AI iş birliği konusu, teknolojinin insan emeğinin yerini alıp almayacağı sorusunun ötesinde, insanların ve yapay zekâ sistemlerinin birlikte nasıl daha verimli ve sürdürülebilir bir çalışma düzeni oluşturabileceğini inceleyen küresel bir mesele olarak değerlendirilmektedir.

5.2. Anahtar Terimler

- **İnsan-Yapay Zekâ İş Birliği:** İnsanların ve yapay zekâ sistemlerinin ortak hedeflere ulaşmak için birlikte çalışmasını ifade eder. Yapay zekâ analitik destek sağlarken insanlar yaratıcılık ve muhakeme becerilerini kullanır.
- **Human-in-the-Loop (İnsan Döngüde):** Yapay zekâ tarafından oluşturulan karar veya önerilerin son aşamada bir insan tarafından denetlenmesini ve onaylanmasını öngören çalışma modelidir.
- **Human-on-the-Loop (İnsan Gözetimde):** Yapay zekâ sistemlerinin büyük ölçüde bağımsız çalıştığı, ancak insanların gerektiğinde müdahale edebildiği denetim modelidir.
- **İnsan-Yapay Zekâ Güveni:** Kullanıcıların yapay zekâ sistemlerinin güvenilirliğine, doğruluğuna ve tutarlılığına duyduğu güven düzeyidir.
- **Algoritma Kaçınması:** İnsanların, algoritmaların insanlardan daha başarılı olduğu durumlarda bile yapay zekâ kararlarına güvenmek istememesi eğilimidir.
- **Otomasyon Yanlılığı:** İnsanların yapay zekâ veya otomatik sistemlerin önerilerini sorgulamadan doğru kabul etme eğilimidir.
- **Hibrit İş Gücü:** İnsan çalışanların ve yapay zekâ sistemlerinin aynı çalışma ortamında birlikte görev aldığı iş gücü yapısıdır.

5.3. Vaka İncelemeleri

5.3.1. Vaka İncelemesi: Amazon'da Yapay Zekâ Destekli Çalışan Gözetimi ve Algoritmik Yönetim

The Guardian’da yer alan habere göre Amazon, depo çalışanlarının performansı yapay zekâ destekli sistemlerle sürekli olarak izlenmekte ve analiz edilmektedir. Bu sistemler; çalışanların görev tamamlama hızını, mola sürelerini ve günlük üretkenlik seviyelerini gerçek zamanlı veriler üzerinden değerlendirerek iş akışını doğrudan yönlendirmektedir.

Çalışanlar ve sendikalar, bu uygulamanın iş yerinde sürekli bir “algoritmik gözetim” ortamı oluşturduğunu ve çalışanların sürekli performans baskısı altında çalışmasına neden olduğunu belirtmiştir. Bu durum, iş gücünün yalnızca verimlilik metrikleri

üzerinden değerlendirilmesi nedeniyle “dijital taylorizm” kavramı ile ilişkilendirilmektedir.

Eleştiriler, yapay zekâ destekli bu tür sistemlerin verimliliği artırsa da çalışan mahremiyetini zayıflattığını, karar alma süreçlerinde şeffaflık sorunları yarattığını ve insan özerkliğini sınırladığını vurgulamaktadır.

Bu vaka, yapay zekânın iş gücünde yalnızca bir otomasyon aracı değil, aynı zamanda çalışma hakları, etik sınırlar ve insan-AI iş birliğinin geleceği açısından kritik bir tartışma alanı oluşturduğunu göstermektedir.

İlgili Olayın Haberi: [‘Constantly monitored’: the pushback against AI surveillance at work | AI (artificial intelligence) | The Guardian]

SORULAR

1. Bir devletin kritik altyapısına yönelik yapay zekâ destekli bir siber saldırı sonucunda elektrik şebekeleri çökerek sivil ölümler meydana gelirse, bu saldırı uluslararası hukuk kapsamında silahlı saldırı (armed attack) olarak değerlendirilmeli midir? Eğer değerlendirilecekse mağdur devletin meşru müdafaa hakkının sınırları ne olmalıdır?
2. Yapay zekâ sistemlerinin sürekli veri toplama ve öğrenme ihtiyacı, bireysel mahremiyet ile siber güvenlik arasındaki dengeyi uzun vadede sürdürülebilir kılabilir mi?
3. Yapay zekâ tabanlı saldırı ve savunma teknolojilerinin aynı anda özel şirketler tarafından geliştirilmesi, siber güvenlikte “rekabet mi yoksa küresel risk artışı mı” doğurmaktadır?
4. Deepfake, phishing ve otonom zararlı yazılımlar gibi yapay zekâ destekli tehditler, siber güvenlik stratejilerinin yeniden tasarlanmasını nasıl zorunlu kılmaktadır?
5. Black box (kara kutu) yapay zekâ sistemlerinde karar süreçlerinin tam olarak açıklanamaması, bu sistemlerin kritik alanlarda (sağlık, güvenlik, adalet) kullanımını sınırlandırmayı gerekli kılar mı?

6. Algoritmik önyargı nedeniyle ayrımcı kararlar veren yapay zekâ sistemlerinde “etik sorumluluk” yalnızca teknik bir hata olarak mı görülmeli, yoksa hukuki yaptırımlarla mı düzenlenmelidir?
7. Yapay zekâya aşırı bağımlılığın çalışanların yaratıcılık, eleştirel düşünme ve problem çözme becerilerini uzun vadede zayıflatma riski, insan-AI iş birliği modelinin sürdürülebilirliğini tehdit eder mi?
8. Yüz tanıma ve gözetim amaçlı yapay zekâ sistemlerinin (surveillance AI) devletler tarafından güvenlik gerekçesiyle yaygın kullanımı, veri gizliliğini fiilen ortadan kaldıran bir “normalleşme” süreci yaratıyor olabilir mi?
9. Otonom silah sistemlerinde insan denetimi (human oversight) zorunlu olsa bile, karar süresinin saniyelere indiği çatışma ortamlarında bu denetim gerçekten işlevsel kabul edilebilir mi?
10. Yapay zekâ tarafından geliştirilen ve insan müdahalesi olmadan hedef seçebilen otonom zararlı yazılımların kullanımı, kimyasal ve biyolojik silahlara benzer şekilde uluslararası anlaşmalarla tamamen yasaklanmalı mıdır; yoksa belirli koşullar altında devletlerin kullanımına izin verilmeli midir?
11. Otomasyon ve yapay zekâ nedeniyle “teknolojik işsizlik” artarken, devletler iş kaybını azaltmak için yeniden beceri kazandırma (reskilling) politikalarını nasıl uygulamalıdır ve ne ölçüde zorunlu hale getirmelidir?
12. Dijital taylorizm kapsamında çalışan performansının algoritmalarla sürekli izlenmesi, iş verimliliğini artırırken çalışan hakları ve mahremiyet üzerinde kabul edilebilir bir sınırı aşıyor mu?