HAKEMLİ Denetişim
Ortak Aklın Harmanı
Kamu İç Denetçileri Derneği Meşrutiyet Caddesi Konur Sokak No: 36/6 Kızılay - ANKARA
www.kidder.org.tr/denetisim/ • denetisim@kidder.org.tr
ISSN 1308-8335
Yıl: 15, Sayı: 29, 112-126, 2024

Teorik Makale

GÜVENİLİR YAPAY ZEKÂ VE İÇ DENETİM

(TRUSTWORTHY ARTIFICIAL INTELLIGENCE AND INTERNAL AUDIT)

Şafak AĞDENİZ [1]

ÖZ

Yapay zekâ teknolojileri bugün hemen her alanda kullanılmaktadır. Kullanılan yapay zekâ uygulamalarının yasal, etik, güvenlik vb. açılardan ortaya çıkan riskleri yapay zekâ uygulamalarının güvenirliği açısından sorgulanmasına neden olmuş ve güvenilir yapay zekâ alanında düzenlemeler yapılmaya başlanmıştır. Güvenilir yapay zekâ için ise bu sistemlerin denetimi gündeme gelmiştir. Bu açıdan değerlendirildiğinde iç denetçilerin güvenilir yapay zekâ ile ilgili işletmelere sunacağı önemli katkılar olacaktır. İç denetim üst yönetime yapay zekâ uygulamalarının işletmelere kuruluşu aşamasında bu sistemlerin olası riskleri hakkında danışmanlık hizmeti vererek ve yapay zekâ uygulamalarının veri ve algoritma denetimlerini gerçekleştirerek güvence sağlayabilir. Bu kapsamda çalışmanın amacı güvenilir yapay zekâ denetimi ve işletmelere bu konuda iç denetim faaliyetinin sağlayacağı katkılar olarak belirlenmiş ve bu amaca yönelik olarak da betimsel analiz yöntemi kullanılmıştır. İç denetçiler yapay zekâ uygulamalarına ilişkin işletme tarafından oluşturulan iç kontrol faaliyetlerinin denetimini gerçekleştirerek ve yapay zeka sistemlerinin risk değerlendirmelerinde danışmanlık yaparak işletmelere değer katabilecektir.

Anahtar Kelimeler: İç Denetim, Yapay Zekâ, Algoritma Denetimi, Veri Denetimi
Jel Kodları: M40, M42, O33

ABSTRACT

Artificial intelligence technologies are used in almost every field today. The artificial intelligence applications used are legal, ethical, security, etc. The risks arising from these aspects have caused the reliability of artificial intelligence applications to be questioned and regulations have begun to be made in the field of reliable artificial intelligence. For reliable artificial intelligence, the control of these systems has come to the fore. When evaluated from this perspective, internal auditors will have significant contributions to businesses related to reliable artificial intelligence. Internal audit can provide assurance by providing consultancy services to senior management about the possible risks of these systems during the installation of artificial intelligence applications to businesses and by performing data and algorithm audits of artificial intelligence applications. In this context, aim of the study was determined as trustworthy artificial intelligence auditing and the contributions of internal audit activity to businesses in this regard, and the descriptive analysis method was used for this aim. Internal auditors will be able to add value to businesses by auditing the internal control activities created by the business regarding artificial intelligence applications and providing consultancy in the risk assessments of artificial intelligence systems.

Keywords: *Internal Audit, Artificial Intelligence, Algorithm Audit, Data Audit*
Jel Codes: *M40, M42, O33*

1. GİRİŞ

Temeli 1950'li yıllarda atılan yapay zekâ özellikle son 10 yılda büyük bir ivme kazanmıştır. İnsan hayatını kolaylaştıran yapay zekâ işletmelerin de birçok sürecini kolaylaştırmıştır. Dünya Ekonomik Forumu (World Economic Forum-WEF) tarafından yayınlanan Geleceğin İşleri Raporu 2023'te işletmelerin %75'inden fazlasının gelecek 5 yıl içinde yapay zekâ teknolojilerini uygulamak istediği belirtilmektedir. Yapay zekâ teknolojilerinin kullanıldığı iş alanlarından biri de denetimdir. Yapay zekâ teknolojilerinin denetim aracı olarak denetçiler tarafından kullanılmasıyla icra edilen denetim

[1] Doç. Dr., Eskişehir Osmangazi Üniversitesi, OrcID: 0000-0003-0373-4694, agdenizsafak@gmail.com

faaliyetinin daha etkin, etkili ve verimli olacağı birçok çalışmada ele alınmış ve yapay zekânın denetimde kullanılması gerekliliği belirtilmiştir. Literatürde denetim 4.0, sürekli denetim, çevik denetim, uzaktan denetim gibi kavramlarla ifade edilen denetimin icrasında yapay zekânın pratik uygulamaları mevcuttur. İç denetçiler ve üst düzey yöneticiler her zaman değişikliklerle çalışma zorluğuyla karşı karşıyadır, ancak söz konusu bu değişikliklere uyum sorunu son birkaç yılda işletmelerin mevcut sistemlerine yapay zekâyı entegre etme yönündeki yatırımlarının ivme kazanmasıyla daha da artmıştır (Kinkela & Harris, 2022, s. 40).

Yapay zekâ teknolojisinin yükselişiyle birlikte bu teknolojilerin kullanımından kaynaklanan yasal, etik ve güvenlik ile ilgili sonuçları iş dünyasında ve toplumda giderek daha önemli hale gelmektedir (Koshiyama vd., 2022, s.41). Meta, eski adıyla Facebook yapay zekâ kullanımı ile ilgili tartışmaların odağında yer alan işletmelerden biri olarak yapay zekâ algoritmalarının kötüye kullanımına ilişkin incelemelerden geçmiştir (IIA, 2017a, s.12). Bu kapsamda literatürde yerini alan güvenilir yapay zekâ kavramı üzerinde konuşulmaya ve bu alanda düzenlemeler yapılmaya başlanmıştır. İşletmelerin yapay zekâ risklerinin farkında olması ve bu riskleri yönetebilmeleri için gerekli adımları atmaları gerekmektedir. İşletmeler iç kontrol sistemleri aracılığıyla yapay zekâ kaynaklı riskleri için menfaat sahiplerine karşı güvence verebilirler. Bu süreçte iç kontrol sisteminin bir gerekliliği olan iç denetim faaliyeti yapay zekâ risklerinin belirlenmesinde ve bu risklere ilişkin oluşturulan kontrolleri denetleyerek işletmelere önemli katkılar sunabilecektir. Bu kapsamda birçok alanda kullanılan yapay zekânın kendisi de ayrı bir denetim konusu olarak gündeme gelmektedir.

Yapay zekâ uygulamalarının insan beynine bağlı olması ve dolayısıyla insan kaynaklı hatalara açık olması muhtemeldir. Bu nedenle kullanılan yapay zekâ teknolojisinin denetim alanına uygunluğunun değerlendirilmesi, getireceği riskler denetçinin risk analizinde ele alması gereken konulardandır (Yıldız & Ağdeniz, 2019, s.99). Yapay zekâ, gelişmiş robotik, 3D baskı, blok zinciri ve nesnelerin interneti gibi yıkıcı teknolojilerin artan kullanım hızı karşısında iç denetçilerin bu teknolojilere ve bu teknolojilerin getirdiği risklere karşı kuruma değer katma çabası artmaktadır (Wright, 2017). Yapay zekâ kullanımının yaygın ve hızlı büyümesi göz önüne alındığında, iç denetçilerin yapay zekânın nasıl çalıştığına, iş dünyasındaki ve kamudaki pratik uygulamalarına ve kuruluşlara sunduğu riskler ve fırsatlara ilişkin derin bir anlayış geliştirmeleri önemlidir. Yapay zekâ teknolojilerinin iş dünyasına hızla dahil edilmesinin denetim açısından ortaya çıkaracağı zorlukları aşağıda sıralanmıştır (Naqvi, 2020, s.8):

- Denetçilerin hazırlıklı olmadığı yeni türde riskler ortaya çıkacaktır.
- Denetçileri hizmet sunum sistemlerini yeniden düşünmeye zorlayacaktır.
- Denetçilerin var olan riskleri ortaya çıkarması yerine, ortaya çıkacak riskin bir adım önünde kalmasını gerektirecektir.

Yapay zekâ sistemlerinin veya daha dar kapsamda makine öğrenmesi denetimi, literatürde sıklıkla "yapay zekâ denetimi" veya “algoritma denetimi” olarak adlandırılan, yeni ortaya çıkan ve önemli bir denetim alanıdır. Yapay zekâ denetimi, finans, sağlık hizmetleri, gibi çeşitli uygulamalardaki yapay zekâ sistemlerinin adaletini, şeffaflığını, hesap verebilirliğini, yanlılığını ve etik sonuçlarını değerlendirmeyi içermektedir. Söz konusu yapay zekâ denetimi 2023 yılında gerçekleştirilen G7 Zirvesinde de ele alınmıştır. Zirvede yapay zekâ alanında yaşanan gelişmelerin büyük bir hızla ilerlemesi sonucu yapay zekâ endüstrisinin bağlayıcı veya etik kurallardan yoksun bir şekilde ilerlemesinin ciddi toplumsal zararlara neden olabileceği belirtilmiş ve bu bağlamda güvenilir yapay zekâ için uluslararası teknik standartların geliştirilmesi ve benimsenmesi konusu ele alınmıştır (European Commision, 2023).

Yapılan bu açıklamalar ışığında çalışmanın amacı güvenilir yapay zekâ için yapay zekâ denetimi hakkında bilgi vermek olarak belirlenmiştir. Bu kapsamda çalışmada veri denetimi ve algoritma denetimi konuları ele alınmaktadır. Çalışma ile iç denetim açısından yapay zekâ denetimi literatürüne katkı sağlanacağı ve iç denetçilerin bu alanda ortaya çıkan fırsatlara ilişkin farkındalıklarının artırılacağı değerlendirilmektedir. Çalışmanın birinci bölümü giriş olup çalışma hakkında genel bilgiler sunulmuştur. Çalışmanın ikinci bölümünde yapay zekâ denetimi hakkında literatür taramasına yer verilmiştir. Üçüncü bölümde genel olarak güvenilir yapay zekâ kavramı ele alınacaktır. Dördüncü bölümde ise güvenilir yapay zekâ için iç denetçilerin gerçekleştirebileceği güvence faaliyetleri kavramsal olarak anlatılacaktır.

2. YAPAY ZEKÂ DENETİMİ ALANINDA YAPILMIŞ ÇALIŞMALAR

Yapay zekânın denetim amacı olarak kullanılmasına ilişkin çalışmaların nispeten yeni olduğu söylenebilir. Yapay zekâ denetiminin literatürde algoritma denetimi ve makine öğrenmesi denetimi gibi adlarla da anıldığı görülmektedir. Bu alanda yapılan ilk çalışmalardan biri Sandvig vd. tarafından 2014 yılında yapılmıştır. Yazarlar Amerikan Havayolları’nın rezervasyon sorununa çözüm bulmak amacıyla IBM ile kurulan online rezervasyon sistemi üzerinden kullanılan algoritmaların yanlılığına ve etik sorunlarına dikkat çekmiş ve algoritmaların da denetlenmesi gerektiğini belirtmişlerdir. Clavell vd. (2020) çalışmalarında Telefónica Innovación Alpha tarafından geliştirilen kişiselleştirilmiş bir sağlık önerisi uygulaması olan REM!X'in Algoritmik Denetimini örnek olay araştırması üzerinden yapmışlardır. Koshiyama & Kazim (2022) çalışmalarında algoritma denetimi adı altında yapay zekânın, makine öğrenmesinin risklerine yer vermiş ve

algoritma denetiminin temel bileşenlerini ele almışlardır. Landers & Behrend (2023) çalışmalarında yapay zekâ modellerinin adillik önyargısına dikkat çekerek denetçilere bu alandaki denetimleri için bir çerçeve sunulmuştur. Munoko vd. (2020) çalışmalarında denetim mesleğinin yapay zekâ teknolojilerini benimserken dikkate alması gereken potansiyel etik sorunları ele almaktadır. Bandy (2021) çalışmasında algoritma denetimi alanında yapılan çalışmaların sistematik bir araştırmasını yapmıştır. Yazar ele alınan 62 adet çalışmada algoritmik sistemlerde ayrımcılık, çarpıtma, istismar ve yanlış yargılama olmak üzere dört sorun tespit etmiştir. Yapay zekânın etik yönünü ele alan bir diğer çalışma ise Brown vd. (2021) tarafından yapılmıştır. Yazarlar çalışmalarında yapay zekâ algoritmalarının etik açıdan değerlendirmeleri gerektiğini ele alarak algoritmaların etik denetimi için bir çerçeve önermişlerdir. Minkkinen vd. (2022) ise çalışmalarında yapay zekâ teknolojilerinin ilerlemesiyle ortaya çıkan sürekli denetim kavramının yapay zekânın denetiminde kullanılabilirliğini kavramsal olarak ele almış ve bu denetimde kullanılabilecek araçlar ve çerçeveleri irdelemişlerdir. Yapay zekâ denetimi alanında yapılan son çalışmalardan biri Mökander vd. (2023) tarafından geniş dil modellerinin (Long Language Models-LLM) denetimini ele almaktadır. Yazarlar geniş dil modellerinin getirmiş olduğu riskleri belirtmiş ve bu modellerin denetimi için bir model önerisinde bulunmuştur.

Literatürde yapay zekâ denetiminin genellikle dış denetim bağlamında ele alındığı görülmektedir. Ancak iç denetçilerin sistemlere doğrudan erişimi, daha önce tanımlanamayan riskleri ortaya çıkarmak amacıyla genellikle dış değerlendirmeler için mevcut olmayan ek bilgileri birleştirmesi yapay zekâ denetiminde daha etkili olabilecektir (Raji vd., 2020, s.35). Raji vd. (2020) tarafından yapılan bir çalışmada yapay zekâ denetimi iç denetim bağlamında ele alınmış ve yapay zekânın risklerinin denetimi konusunda iç denetçiler için bir çerçeve önerilmiştir. Söz konusu çerçeve kapsam belirleme, haritalama, kanıt toplama, test etme ve yansıma olmak üzere beş bölümden oluşmaktadır. Bu çalışmada ise yapay zekâ denetiminde veri denetimi ve algoritma denetimine odaklanılmış ve bu alanda iç denetçilerin denetimlerde uygulayabilecekleri kontrol prosedürleri hakkında bilgi verilmiştir.

3. GÜVENİLİR YAPAY ZEKÂ

Yapay zekâ matematik, mantık, istatistik, dilbilim, psikoloji gibi birçok disiplinin katılımıyla gelişmiştir. İnsan tarzı zekâyı mekanikleştirme olasılığını içeren ilk makale 1950 yılında Alan Turing tarafından yazılan "Computing Machinery and Intelligence" adlı çalışmadır (Nilsson, 2018, s.65). "Yapay zekâ" kavramının ilk olarak geçtiği metin ise McCarthy ve arkadaşlarının araştırma yapmak için Rockefeller Vakfı'na sundukları 2 Eylül 1955 tarihli resmi başvuru yazısı olarak bilinmektedir (Say, 2018, s.85). Yapay zekânın tohumları üç temel bilimsel etkinlikte ortaya atılmıştır. Bu etkinlikler (Nilsson, 2018, s.75) Tablo 1'de verilmiştir.

Tablo 1. Yapay Zekâ'nın Gelişiminde Kilometre Taşları

Yıl	Etkinlik
1955	Öğrenen Makineler Oturumu-Los Angeles
1956	Yapay Zekâ Yaz Araştırması Projesi- Dartmouth Koleji
1958	Düşünce Süreçlerinin Mekanikleşmesi- Birleşik Krallık

(Nillson 2018'den yararlanarak yazar tarafından oluşturulmuştur).

Türkiye'de ise hemen hemen aynı zamanlarda Prof. Dr. Cahit Arf, 1958 yılında ilk yapay zekâ seminerini gerçekleştirmiştir. Bu seminerde "Makine Düşünebilir Mi ve Nasıl Düşünebilir" başlıklı makaleyi sunmuştur. Yapay zekâ alanındaki çalışmalarda, ilk olarak zekâ gerektiren bazı işleri belirleme ve bu işleri makinelere nasıl yaptırılacağı belirlenmiştir. Bu nedenle 1950'li ve 1960'lı yıllarda yapay zekâ çalışmalarının bulmaca çözme, satranç ve dama gibi oyunları oynama, basit sorulara cevap verme gibi alanlarda yapıldığı görülmektedir (Nilsson, 2018, s.75). Yapay zekânın temel hedefi insan zekâsının birebir taklit edilebilmesidir. Günümüzde insan beyninin bir ürünü olan yapay zekânın henüz insan zekâsının yerini alabilmesi mümkün görülmemektedir. Yapay zekânın doğal zekâya rağmen kullanılmasının nedenleri yapay zekânın aşağıdaki özelliklerinden kaynaklanmaktadır (Yıldız, 2009, s.25):

- ***Belgelendirilebilirlik:*** Doğal zekâ süreçleri tam olarak ortaya çıkarılamadığı için bir insanın karar verme sürecinin belgelendirilebilmesi mümkün değildir.
- ***Verimlilik:*** İnsan doğası gereği her zaman aynı performans ile çalışamamaktadır. Yorgunluk, stres, uykusuzluk gibi insana özgü birtakım özellikler insan zekâsının kullanımını doğrudan etkilemektedir. Ancak yapay zekâ teknolojisi insana özgü bu durumlardan bağımsızdır ve her zaman aynı verimlilikte çalışabilmektedir.
- ***Kalıcılık:*** Doğal zekâ insan ömrü ile sınırlıdır. Ölüm ile birlikte doğal zekâda ölmektedir. Ancak yapay zekâ dijital ortamlarda saklanabilmekte, aktarılabilmekte ve kopyalanabilmektedir.

- ***Objektiflik:*** İnsan doğası gereği duygusallıkla karar verebilmektedir. Söz konusu bu durum bazen yanlış ve yanlı kararların verilebilmesine neden olmaktadır. Oysa yapay zekâ teknolojisi belirli bir olayda her zaman aynı karara varmaktadır.

İşletmeler yukarıda sayılan özelliklerin sunduğu fırsatları değerlendirmek adına yapay zekâ uygulamalarını giderek artan oranda faaliyetlerinde kullanmaktadırlar. Ancak yapay zekâ uygulamalarının beraberinde getirdiği ve her geçen gün değişen riskleri de mevcuttur. Yapay zekânın özellikle literatürde üzerinde durulan etik, yanlılık, veri güvenliği vb. riskleri iyi analiz edilmelidir. Kaspersky ve Ghent üniversitesinin yapay zekânın insan davranışları üzerindeki sosyal etkisi ve bu etkinin yol açtığı tehdit ve risklere ilişkin gerçekleştirdikleri çalışmalarında çarpıcı sonuçlar bulunmuştur. Katılımcıların %40'ının, sadece kişisel yaka kartı ile girilebilen yerlere, robotların girebilmesi için kilidi açtıkları görülmüştür. Ayrıca çalışmaya katılanlardan biri hariç diğerlerinden kişisel bilgilerin yapay zeka robotu tarafından kısa sürede elde edildiği tespit edilmiştir (Belpaeme vd., 2019). Bir diğer araştırmada ise veriden beslenen yapay zekânın veri riskine dikkat çekilmektedir. Gartner firması tarafından yapılan bir ankete göre işletmeler, yılda ortalama 15 milyon dolarlık kayıptan zayıf veri kalitesinin sorumlu olduğuna inanmaktadır. Ayrıca, ankete katılan işletmelerin yaklaşık %60'ının, ilk etapta verileri ölçmedikleri için kötü verilerin işletmelerine ne kadara mal olacağını bilmedikleri belirtilmiştir (Bansal, 2021). Sayılan bu risklerin olası sonuçları arasında itibar kaybı, hisse değerinin kaybı, idari para cezaları ve davalar da yer alabilir (Calagna vd., 2021, s.6). Yapay zekâ uygulamalarına güvenerek onlardan yararlanabilmek için yapay zekânın olası etik, yasal ve diğer risklerinin gözetilmesi gerekmektedir. Bu bağlamda son yıllarda uluslararası düzey toplantılarda üzerinde durulan konulardan biri güvenilir yapay zekâdır. Güvenilir yapay zekâ alanında devam eden veya tartışılan bazı önemli uluslararası düzenlemeler ve çalışmalar Tablo 2'de özetlenmiştir.

Tablo 2. Güvenilir Yapay Zekâ Alanında Yapılan Düzenlemeler

AB (Avrupa Birliği)	Avrupa Komisyonu Yapay Zekâ Yasası: AB üye ülkeleri arasında yapay zekâ için uyumlu bir düzenleyici çerçeve oluşturmayı amaçlayan "Avrupa Birliği Yapay Zekâ Yasası" (EU Artificial Intelligence Act) 14 Haziran 2023 yılında Avrupa Parlamentosu tarafından kabul edilmiştir (European Parliament, 2023).
ABD (Amerika Birleşik Devletleri)	Yapay Zekâ Yönetişim İlkeleri: ABD'nde tek bir kapsamlı yapay zekâ düzenlemesi bulunmamakla birlikte, çeşitli federal kurum ve kuruluşlar yapay zekâ yönetişimi için yönergeler ve ilkeler yayınlamıştır. Bu kuruluşlardan ikisi NIST (Ulusal Standartlar ve Teknoloji Enstitüsü) ve FTC (Federal Ticaret Komisyonu)'dir (Fazlıoğlu, 2023).
Kanada	Kanada'nın Yapay Zekâ Etik Yönergeleri: Kanada, adalet, şeffaflık, hesap verebilirlik ve güvenlik de dahil olmak üzere sorumlu yapay zekâ gelişimini teşvik etmek için yapay zekâ etik kuralları geliştirmiştir. 2018 yılında "Yapay Zekânın Sorumlu Geliştirilmesine İlişkin Montreal Deklarasyonu" ve 2023 yılında "Gelişmiş Üretken Yapay Zeka Sistemlerinin Sorumlu Geliştirilmesi ve Yönetimine İlişkin Kurallar" adlı rehber yayınlanmıştır (Ulusal Yapay Zekâ Stratejisi, 2021, s.29).
Birleşik Krallık	Birleşik Krallık, etik yapay zekâ gelişimi için şeffaflık, hesap verebilirlik ve adalet gibi ilkeleri vurgulayan yönergeler yayınlamıştır. Bu yönergelerin amacı yapay zekâ teknolojilerinin geliştirilmesine bilgi vermektir. 29 Mart 2023'te yapay zekâ risklerini belirlemek ve ele almak için "Yapay Zekâ Düzenleme Beyaz Kitabını" (Artificial Intelligence Regulation White Paper) yayınlamıştır (Robert vd., 2023).
Artificial Intelligence HLEG (Yapay Zeka Üst Düzey Uzman Grubu)	Güvenilir Yapay Zekâ için Etik Kılavuz İlkeleri ve Değerlendirme Listesi yayınlanmıştır (Ulusal Yapay Zekâ Stratejisi, 2021, s.28).
ISO (Uluslararası Standardizasyon Örgütü)	ISO/IEC Standartları: ISO ve IEC (Uluslararası Elektroteknik Komisyonu), yapay zekâ sistemlerinde gizlilik için ISO/IEC 27701 ve yapay zekâ güvenilirliği için ISO/IEC 23894 dahil olmak üzere yapay zekâ için uluslararası standartlar geliştirmek üzerinde çalışmalar yürütmektedir (www.iso.org).
OECD (Ekonomik İşbirliği ve Kalkınma Örgütü)	OECD Yapay Zekâ Kılavuzları: Etik ve demokratik değerleri göz önünde bulundurarak yapay zekâ politikaları ekosistemini güçlendirmek amacıyla 2019 yılında yayımlanan OECD Yapay Zekâ

	Konsey Tavsiye Kararı, 2019 yılında G20 Yapay Zekâ İlkeleri adı ile kabul edilmiştir (Ulusal Yapay Zekâ Stratejisi, 2021, s.53).
GPAI (Yapay Zekâ Konusunda Küresel Ortaklık)	GPAI yapay zekânın sorumlu bir şekilde geliştirilmesini ve yaygınlaştırılmasını ilerletmek için hükümetleri ve uzmanları bir araya getiren uluslararası bir girişimdir. Yapay zekâ etiğine, politikasına ve en iyi uygulamalara odaklanmaktadır (Ulusal Yapay Zekâ Stratejisi, 2021, s.31).
UNESCO (Birleşmiş Milletler Eğitim, Bilim ve Kültür Örgütü)	UNESCO yapay zekânın etik boyutlarını araştırmaktadır. Yapay Zekâ Etiğine İlişkin Tavsiye Kararı, Kasım 2021'de UNESCO'nun Genel Konferansında 193 Üye Devlet tarafından kabul edilmiştir (Unesco, 2023).
WEF (Dünya Ekonomik Forumu)	WEF, şeffaf ve kapsayıcı yapay zeka sistemlerinin sorumlu küresel tasarımını ve piyasaya sürülmesini desteklemek için sektör liderlerini, hükümetleri, akademik kurumları ve sivil toplum kuruluşlarını birleştiren Yapay Zeka Yönetişim İttifakı oluşturmuştur. Ayrıca, "Yapay Zekâ Çözümlerinin Özel Sektör Tarafından Tedarikine İlişkin Rehber" 2023 yılı Haziran ayında yayınlanmıştır (www.weforum.org).

Yapay zekâ risklerinin yönetimi için yapılan son düzenlemelerden biri de Standartlar ve Teknoloji Ulusal Enstitüsü (National Institute of Standards and Technology-NIST) tarafından 2023 yılı Ocak ayında yayınlanan Yapay Zekâ Risk Yönetimi Çerçevesi AI-RMF 1.0'dır. Söz konusu çerçeve iki bölümden oluşmaktadır. Çerçevenin ilk bölümü riskin tanımı, yapay zekâ riskleri ve güvenilir bir yapay zekânın özelliklerini tanımlamaktadır. İkinci bölüm ise yapay zekâ risk yönetim çerçevesinin temelleri ve profillerini açıklamaktadır. NIST Yapay Zekâ Risk Yönetimi Çerçevesi AI-RMF 1.0'da güvenilir yapay zekânın yedi özelliği aşağıdaki gibi belirtilmiştir (NIST, 2023, s.12):

- Güvenlilik,
- Dayanıklılık,
- Açıklanabilirlik/yorumlanabilirlik,
- Geliştirilmiş gizlilik,
- Zararlı önyargı yönetimi ile adillik,
- Hesap verebilirlik/şeffaflık
- Geçerlilik/güvenirlilik.

Güvenilir yapay zekâ hakkında Türkiye'de yapılan bir çalışma ise Türkiye Cumhuriyeti Cumhurbaşkanlığı Dijital Dönüşüm Ofisi ile T.C. Sanayi ve Teknoloji Bakanlığı tarafından 2021 yılı Ağustos ayında yayınlanan Türkiye Ulusal Yapay Zekâ Stratejisi'dir. Söz konusu çalışmada Türkiye'nin güvenilir yapay zekâ alanından yapılan çalışmalara katılımının sağlanacağı ve bu alanda faaliyetler gerçekleştirileceği belirtilmiştir. Çalışmada 8 adet güvenilir yapay zekâ ilkesi belirtilmiştir. Bu ilkeler aşağıda sıralanmıştır (Ulusal Yapay Zekâ Stratejisi, 2021, ss.60-61):

- Ölçülülük,
- Emniyet ve güvenlik
- Tarafsızlık,
- Mahremiyet,
- Şeffaflık ve açıklanabilirlik,
- Sorumluluk ve hesap verebilirlik,
- Veri egemenliği,
- Çok paydaşlı yönetim,

Ulusal Yapay Zekâ Stratejisinde güvenilir yapay zekâ ile ilgili belirlenen ilkelerin uluslararası düzenlemelerle uyumlu olduğu görülmektedir.

4. GÜVENİLİR YAPAY ZEKÂNIN DENETİMİNDE İÇ DENETİM

Son on yıldır çok hızlı bir şekilde ilerleyen yapay zeka uygulamaları ve bu uygulamaların kullanımı da bir o kadar yaygınlaşmıştır. Bugün tıp, eğitim, sağlık, finans gibi hemen hemen tüm alanlarda yapay zekâ kullanımı giderek yaygınlaşmaktadır. Yapay zekânın denetim alanında da etkilerini görmek mümkündür. Yapay zekâ ile birlikte denetimde niş alanlar oluşmuş ve oluşan bu niş alanlarda denetim yapabilecek nitelikte denetçilere talebin giderek arttığı görülmektedir (Naqvi, 2020, s.12). İç denetim, yapay zekâ uygulamalarının getirdiği risk ve fırsatlara ilişkin gerek danışmanlık gerekse güvence faaliyetleriyle üst yönetimi desteklemek suretiyle kuruma değer katma işlevini yerine getirebilecektir. Yapay zekâ uygulamalarının beraberinde getirdiği ve iç denetim birimleri tarafından dikkate alınması gereken fırsatlar ve tehditlere örnekler Tablo 3'te verilmiştir:

Tablo 3. Yapay Zekâ Fırsat ve Tehditleri

Fırsatlar	Tehditler
Veri işleme döngüsünün kısaltılması.	Yapay zekâ teknolojisinin yapısında, insanlardan kaynaklanan tanımlanmamış, ve tespit edilmemiş, yanlılığın var olması riski.
Kusursuz ve hatasızsa tekrarlanabilen makine hareketleriyle insan hareketlerini ikame ederek hataların azaltabilmesi.	Yapay zekâ teknolojisinin yapısında insanlardan kaynaklanan mantık hatalarının bulunması riski
Çok zaman alan faaliyetleri, zamandan tasarruf sağlayan (süreç otomasyonu) faaliyetlerle ikame ederek işçilik süresinin ve maliyetinin azaltabilmesi.	Yapay zekânın yeterli test ve gözetimden geçirilmemesinin etik açıdan sorgulanır nitelikte sonuçlar doğurma riski.
Potansiyel olarak tehlike arz eden durumlarda insanların, robot veya insansız hava araçlarıyla ikame edilmesinin sağlanması.	Yapay zekâ ürünlerinin ve hizmetlerinin zarara yol açıp mali duruma ve/veya itibara zarar verecek sonuçlar doğurma riski.
Belirli pazarlarda, bazı ürünleri piyasaya sürmek ve satmaktan tutun da, salgın hastalıkları ve doğal felaketleri önceden tespit etmeye kadar her konuda daha iyi tahminlerde bulunabilmesi.	Müşterilerin veya diğer paydaşların kurumun yapay zekâ projelerini kabul etmeme veya benimsememe riski.
Yapay zekâ projeleri aracılığıyla kurumun gelirlerini arttırabilme ve yönetebilme ve kurumun pazar payını arttırabilme	İşletmenin, yapay zekâya yatırım yapmadığı takdirde, rakiplerinin gerisinde kalma riski.
	Yapay zekâya (altyapı, araştırma ve geliştirme ve yetenek kazanma) yatırım yapmanın kabul edilebilir bir yatırım getirisi sağlamama riski.

(IIA, 2017a, s.8'den yararlanarak yazar tarafından oluşturulmuştur).

Yapay zekâ uygulamalarından kaynaklanan risklerin yönetimi ve bu kapsamda güvenilir yapay zekâ işletmeler için giderek daha önemli olmaktadır. Bu kapsamda uluslararası kuruluşlar tarafından gerek işletmelere gerek denetçilere rehberlik edebilmek adına çalışmalar yayınlanmaktadır. Bu çalışmalardan biri de Treadway Komisyonu Sponsor Kuruluşlar Komisyonu (The Committee of Sponsoring Organizations of the Treadway Commision-COSO) tarafından 2021 yılında yapay zekâ risklerinin yönetimi konusunda yayınlanan rehberdir. COSO Kurumsal Risk Yönetimi- Riskin Strateji ve Performansla Uyumlaştırılması Çerçevesi'nde (COSO Enterprise Risk Management Integrating with Strategy and Performance), yapay zekânın potansiyelini gerçekleştirmeye yardımcı olmak için risk yönetimini yapay zekâ stratejisi ve performansıyla uyumlu hale getirebileceği belirtilmektedir. Söz konusu çerçevenin 5 ilkesi yapay zekâ uygulamalarının yönetiminde işletmelere aşağıda belirtilen şekilde yol göstermektedir (Calagna vd., 2021, s.22):

- **Yönetişim ve Kültür:** Yapay zekâ programı için yönetişim yapısının oluşturulması için işletmenin yapay zekâyı ne zaman ve nasıl kullanacağının belirlenmesi ve önerilen yapay zekâ girişimlerinin amaç, hedef ve etik hususların tanımlanması gerekir. Yapay zekâ programına liderlik edecek, risk ve performans gözetimi sağlayacak üst düzey bir yöneticinin belirlenmesi gerekir.
- **Strateji ve Hedef Belirleme**: Tüm paydaşlarla birlikte yapay zekânın stratejik, teknik, düzenleyici ve operasyonel risklerini yönetmek için strateji taslağı hazırlanmalıdır. Belirlenen stratejinin yürütülmesi için işletmenin yapay zekâ teknik altyapısının uygun olup olmadığı değerlendirilmelidir.
- **Performans:** Belirlenen strateji ve hedeflere ulaşılmasını engelleyebilecek risklerin belirlenmesi gerekir. Bu kapsamda işletmenin kullandığı her yapay zekâ modeli için ideal olmayan stratejik sonuçların,

operasyonel başarısızlıkların veya önyargıların potansiyel etkilerinin ölçülmesi gerekir. Ayrıca algoritmanın verileri nasıl yönettiğini ve kullandığını ve istenmeyen herhangi bir önyargıya neden olup olmadığı değerlendirilir.

- **Gözden Geçirme ve Düzeltme:** Belirlenen yapay zekâ risklerinde bir değişiklik olup olmadığı, revizyon gerekliliği gibi konular gözden geçirilir. Farkındalık ve karar verme desteği için yapay zekâ risklerine ilişkin üst düzey yöneticilere ve yönetim kuruluna rapor verilmelidir.
- **Bilgi, İletişim ve Raporlama:** Yapay zekâ risklerini yönetmek ve şeffaflık için paydaşlara rapor vermek için bir yaklaşım belirlenmelidir. Yöneticiler ve yönetim kurulları için raporlama için gösterge tablolar geliştirilmelidir. Yapay zekâ performansını ve risk yönetimi eylemleri farkındalık amacıyla dış paydaşlara açıklanmalıdır.

İç kontrolün önemli bir unsuru olan iç denetim, işletmelerin kurumsal yönetim, risk yönetimi ve iç kontrol süreçlerinin etkinliğini değerlendirmek ve geliştirmek amacıyla gerçekleştirilen bağımsız ve objektif danışmanlık ve güvence faaliyetidir (Selimoğlu & Özbek, 2018, s.11). İç denetim işletmelerin yapay zekâ uygulamalarına ilişkin yol haritası oluştururken başvuracakları işletme içi önemli bir birimdir. Yapay zekâ bağlamında iç denetimin rolü; bir işletmenin kısa, orta ve uzun vadede değer yaratma becerisi üzerinde yapay zekânın ne ölçüde olumlu ya da olumsuz etkili olacağını değerlendirmek, anlamak ve bildirmek için o işletmeye yardımcı olmaktır (IIA, 2017a). İç denetim birimi tarafından yapay zekâ uygulamalarına ilişkin riskler ve fırsatlar değerlendirilerek gerek denetim gerekse güvence alanında önemli katkılar sağlanacaktır. İç denetim birimi yapay zekâ alanında aşağıda verilen faaliyetleri gerçekleştirmek suretiyle kuruma değer katabilir (IIA, 2017a):

- Yapay zekânın risk değerlendirmesine dâhil edilmesi ve yapay zekânın risk temelli denetim planına dâhil edilmesinin değerlendirilmesi,
- Yapay zekâyı araştıran işletmelerde, iç denetimin bağımsızlığını korumak suretiyle yapay zekâ projelerine dâhil olarak tavsiye sunulması,
- Yapay zekâyı işletme faaliyetlerinde kullanan işletmelerde kullanılan algoritmalar ve bu algoritmaların dayandığı verilerin güvenilirliğine ilişkin risklerin yönetimi konusunda güvence verilmesi,
- İşletmenin yapay zekâ kullanımına ilişkin ahlaki ve etik sorunların ele alındığı konusunda güvence verilmesi.

Yapay zekâ denetimi tıpkı finansal işlemlerin doğruluk, tamlık ve yasallık açısından denetlenebilmesi gibi, yapay zekâ sistemlerinin tasarımı ve kullanımında teknik sağlamlık, yasal uyumluluk veya önceden tanımlanmış etik ilkelere bağlılık açısından denetlenebilmesidir (Mökander vd., 2023, s.6). Yapay zekâ denetiminin temel hedefi işletmelerin yapay zekâ uygulamalarının şeffaflığını, açıklanabilirliğini, yanlılığını ve etik sonuçlarını değerlendirmektir. Ancak, iç denetim açısından yapay zekâ denetiminin birtakım zorlukları mevcuttur. Bu zorluklar Tablo 4'te verilmiştir.

Tablo 4. Yapay Zekâ Denetiminin Zorlukları

Yapay zekâ denetimine yönelik henüz yeterince olgunlaşmış denetim çerçeveleri ve düzenlemelerinin olmaması
Yapay zekâ denetimine ilişkin ilk örneklerin sayısının yeterli olmaması
Yapay zekâ ile ilgili tanımlama ve sınıflandırmalarda belirsizlik olması
Yapay zekâ teknolojisinin doğası olarak yeni geliştiriliyor olması
Yapay zekâ denetimine ilişkin açık bir rehberin olmaması
Stratejik başlama noktasının olmaması
Yapay zekâ denetçisi için yeni ve hızlı bir şekilde gelişen yapay zeka denetimlerinin kısa bir sürede öğrenilmesi gerekliliği
Yapay zekâ tarafından üçüncü taraflara dış kaynak kullanımının yarattığı tedarikçi riski

(ISACA, 2018, s.8)

Tablo 4'te sayılan yapay zekâ denetiminin zorlukları arasında diğer hususları da etkileyen en önemli kısıt bu alandaki yasal düzenlemelerin henüz tam anlamıyla oluşturulmamış olmasıdır. Yaşanan gelişmelerin uygulamalara etkisi ile bu uygulamalara ilişkin yasal uyum ve düzenlemeler arasında doğal olarak bir zaman farkı söz konusudur. Yapay zekâ denetimi ile ilgili birçok düzenleme yapıldığı görülmekle beraber henüz bu düzenlemelerin belirli standartlara dönüştürülemediği görülmektedir. Yapay zekâ denetimi alanındaki bir yaklaşım COBIT (Control Objectives for Information and Related Technology- Bilgi ve İlgili Teknolojiye İlişkin Kontrol Hedefleri) 2019 çerçevesidir. Bu çerçeve yapay zekâ stratejisi ile ilgili birçok risk örneğine yer vermektedir (ISACA, 2018, s.6). Ayrıca, Deloitte'un Güvenilir Yapay Zekâ (Trustworthy AI™ [2] Framework) Çerçevesi, yapay zekâya özgü riskleri ve etik hususları anlamak ve değerlendirmek için bir araç olarak hizmet edebilir (Calagna v.dd., 2021, s.10). Yapay zekâ denetimi ile ilgili yayınlanan

[2] AI™ ifadesindeki TM, Tescili korunan marka anlamına gelen "Trade Mark (Ticari Marka)" kelimesinin baş harfleridir.

son çerçevelerden biri ise Bilgi Komiserliği Ofisi (Information Commissioner's Office-ICO) tarafından 2022 Mayıs ayında hazırlanan ve kamuoyunun görüşüne sunulan Yapay Zekâ Denetim Çerçevesine İlişkin Rehber'dir.

Bir işletmenin yapay zekâ denetiminin başlangıç noktası, yapay zekâ ile ilgili denetimin kapsamını ve hedeflerini tanımlamak ve kuruluşa yönelik riskleri dikkate almaktır (ISACA, 2018, s.6). Aynı zamanda yapay zekâya ilişkin işletmenin kurumsal yönetimi ve iç kontrol süreçleri de ele alınmalıdır. Güvenilir yapay zekânın temel özelliklerini de dikkate alacak şekilde yapay zekâ denetiminde bu uygulamalara ilişkin adillik, ön yargı tespiti, şeffaflık, açıklanabilirlik, sorumluluk, düzenlemelere uyum, veri gizliliği ve güvenliği, etik sorunlar, performans ve sağlamlık gibi hususlara ilişkin alınan kontroller değerlendirilmektedir. Bu kapsamda, yapay zekâya ilişkin denetleme konusu hususlar ana başlıkları itibariyle aşağıda verilmiştir (IIA, 2018, s.2):

- Yapay zekâ tasarımına müdahale eden istem dışı insan önyargıları riskinin tespit edilip edilmediği ve doğru yönetilip yönetilmediği,
- Yapay zekâ sonuçlarının asıl amacı yansıttığından emin olmak için yapay zekânın etkin bir şekilde test edilip edilmediği,
- Bir karmaşıklık olması durumunda yapay zekâ teknolojilerinin şeffaflık sağlayıp sağlayamayacağı,
- Yapay zekâ çıktısının yasal, etik, sorumlu ve duyarlı bir şekilde kullanılıp kullanılmadığı.

Güvenilir yapay zekâ için belirtilen özellikler işletmelerin kurumsal yönetimine, yapay zekâ sistemleri tarafından kullanılan verilere, yapay zekâ modellerinin ve algoritmalarının seçimine ve bunları oluşturanların aldığı kararlar ile bunları sağlayan insanlarla etkileşimlere bağlıdır (NIST, 2023, s.11). Yapay zekâ destekli sistemler, verinin barındırdığı özelliklerden ve örüntülerden öğrenen, bu doğrultuda güncellenebilen arama ve tahminleme yapabilen gelişmiş algoritmalar kullanmaktadır (Ulusal Yapay Zekâ Stratejisi, 2021, s.12). Bu kapsamda yapay zekâ denetiminin başlangıç noktasını veri denetimi ve algoritma denetimi olmak üzere ele alabiliriz.

4.1. Veri Denetimi

Veri yeni yüzyılın petrolü olarak değerlendirilen, emek, sermaye, girişimcilik gibi üretim faktörlerinden biri olarak nitelendirilmektedir. Yapay zekâ araştırmalarının yürütülmesi ve uygulamalarının geliştirilmesi için hem ilgili alanda geniş ölçekli veri kümelerine hem de bu veriler üzerinde işlem yapabilecek yüksek kapasiteli bilişim altyapılarına ihtiyaç duyulmaktadır (Ulusal Yapay Zekâ Stratejisi, 2021, s. 27). G7 zirvesinde, Japonya Dijital İşler Bakanı Taro Kono, "Üretken yapay zekâ eğer dayandığı veriler sahte ise sahte haberler ve toplum için yıkıcı çözümler üretir" diyerek yapay zekânın veri ve güvenlik riskine dikkat çekmiştir (www.voaturkce.com). Veri riski, yapay zekâ sistemlerinin eğitim ve karar alma için güvendiği verilerle ilişkili potansiyel tehditleri ve güvenlik açıklarını ifade etmektedir. Yapay zekâ denetimi kapsamında veri risklerinin denetimi önemli bir başlangıç adımıdır. Yapay zekânın eğitiminde kullanılan "veri" nitelik ve nicelik yönünden ana denetim konularından biri olacaktır. Verinin kalitesi, miktarı, güvenilirliği, güvenliği, yanlılığı gibi her bir özelliği ayrı birer denetim konusudur (Ağdeniz, 2020, s.28). Büyük veri denetimi konusunda iç denetçilere yardımcı olmak adına IIA tarafından "GTAG:Büyük Verileri Anlamak ve Denetlemek" adlı tamamlayıcı rehber yayınlanmıştır. Söz konusu bu rehberde büyük verilere ilişkin denetim kapsamı dört başlık altında toplanmıştır (IIA, 2017c, s.19).

- Program yönetişimi,
- Teknoloji kullanılabilirliği ve performansı,
- Güvenlik ve gizlilik,
- Veri kalitesi, yönetimi ve raporlama.

Veri kalitesi her zaman önemlidir ancak yapay zekâ modellemede daha çok önemlidir. Basitleştirilmiş, önyargılı veriler, kasıtsız olarak hatalı sonuçlara yol açabilmektedir (Beckstrom, 2021, s.40). Eğer aynı veriler hem modeli oluşturmak (eğitim aşamasında) hem de performansı doğrulamak (test veya doğrulama sırasında) için kullanılıyorsa, performans ölçümleri büyük olasılıkla şişirilecektir. Bu aşırı uyum (overfitting) yeni, bilinmeyen üretim verileri üzerinde kullanıldığında performans kaybına yol açacaktır. Yapay zekâdaki veri riskinin denetimi, yapay zekâ teknolojilerinin etkili kullanımını sağlamak için veri ile ilgili risklerin değerlendirilmesini ve azaltılmasını içermektedir. Tablo 5'te veri kalitesinin sağlanmasında yapılacak iç denetim faaliyetine ilişkin kontrol hedefleri ve prosedürleri yer almaktadır.

Tablo 5. Veri Kalitesi Kontrol Hedefleri ve Kontrol Faaliyetleri

Kontrol Hedefleri	Kontrol Faaliyetleri
Yapay zekâda kullanılan algoritmaların dayandığı verilerin güvenirliği hakkında güvence sağlamak.	• Yapay zekâ'ya girişi yapılan ham verilerin bir örneğinin alınması. • İşletmenin, yapay zekâ sonuçlarını gerçek yaşamdaki sonuçlarla doğrulamak için gereken yöntemleri uyguladığını ve bu ikisi arasındaki tutarsızlıkları sürekli olarak ölçmek, izlemek, belirlemek ve düzeltmek için gereken politikalar ve prosedürlerin mevcut olduğunun doğrulanması.
Veri girdisinin uyumlulaştırıldığına ve doğruluğu maksimize edilecek şekilde normalize edildiğine dair güvence sağlamak.	• İşletmenin veri doğruluğu ve sağlamlığı sorunlarını sürekli olarak ölçmek, izlemek, belirlemek ve düzeltmek için gereken politikalara ve prosedürlere sahip olduğunun doğrulanması. • İşletmenin, değişiklik yapılması halinde yöntemlerin ve sonuçların değiştirilme gerekçelerini de içeren bir veri uyumlulaştırma çerçevesini tutarlı olarak izlediğinin ve gözettiğinin teyit edilmesi.
Birleştirilmiş verilerin tam olduğu hakkında güvence sağlamak.	• İşletmenin veri giriş yanlılığını sınırlandırmak için gereken politikalara ve prosedürlere sahip olduğunun doğrulanması.
Veri tamlığının ölçülerek izlendiği ve karar alma süreçlerini etkileyen önemli istisnaların tanımlandığı ve açıklandığı hakkında güvence sağlamak.	• Ölçüm raporlarının gözden geçirilmesi. • Karar alma sorumluluğunda olanların veri kalitesiyle ilgili önemli istisnalar hakkında açıklama alıp almadıklarını ve bunlar üzerinde düşünüp düşünmediklerinin değerlendirilmesi.

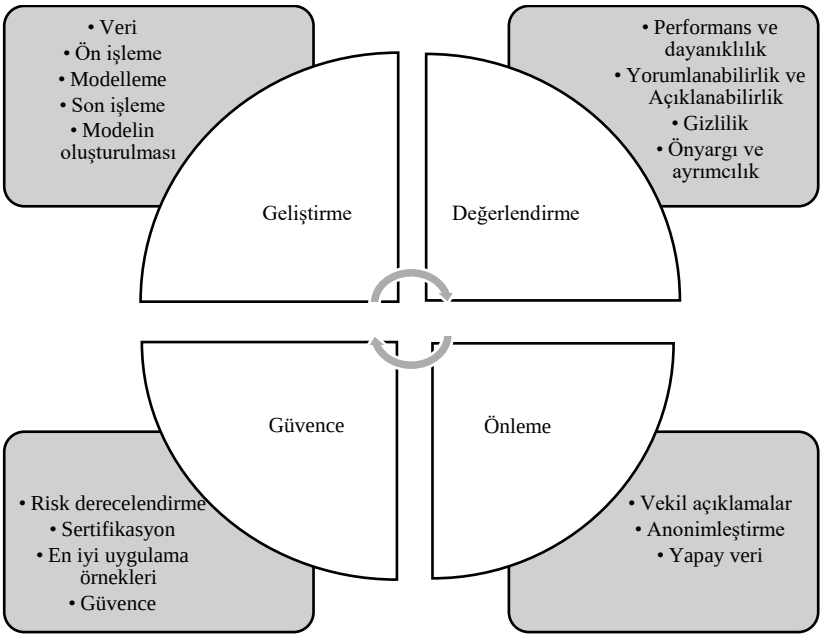
(IIA, 2017b, s.13)

Kişisel verilerin korunması ve işlenmesi konusu da veri denetimi açısından ele alınması gereken konulardan biridir. Kişisel verilerin hukuka aykırı olarak kullanılması ve paylaşılması işletmeler açısından başlıca veri güvenliği ve gizliliği risklerindendir. Kişisel veri işleme esaslı yapay zekâ çalışmalarında ilk aşamadan itibaren kişisel verilerin korunması ile ilgili yürürlükteki mevzuata uyum sağlanması ve tüm yapay zekâ uygulamalarının tasarımdan itibaren veri koruma ilkesine göre geliştirildiğine ve yönetildiğine (KVKK, 2021, s.11) ilişkin güvence kontrol hedeflerinden biri olacaktır. Veri riskinin denetimi işletmelerde yapay zekâ yönetişiminin önemli bileşenlerinden biridir. Yapay zekânın veri kaynaklı risklerinin denetiminde ICO tarafından yayınlanan taslak rehber de kullanılabilir. Rehberde bir kuruluşun yapay zekâ sistemlerinin geliştirilmesinde veya bu sistemlerin kurulumunda veri koruma önlemlerinin tasarlanıp tasarlanmadığı değerlendirilmekte ve bu kapsamda verilerin adil, yasal ve şeffaf bir şekilde kullanımı gibi temel risklerinin yönetimi konuları ele alınmaktadır.

4.2. Algoritma Denetimi

Yapay zekânın ve makine öğreniminin hızlı gelişimi, hayatları benzeri görülmemiş bir ölçekte iyileştirme potansiyeline sahip güçlü algoritmaların ortaya çıkmasına yol açmıştır (Brown vd., 2021). Algoritmalar insan beyni tarafından üretilmektedir. İnsandan kaynaklı hata ve yanlılık algoritma performansını doğrudan etkileyecektir (IIA, 2017). Kullanılan algoritmaların risklerinin yönetimi algoritma denetimi konusunu gündeme getirmektedir. Algoritma denetimi, bir algoritmanın yasallığını, etiğini ve güvenliğini değerlendirme, hafifletme ve güvence altına alma araştırması ve uygulaması olarak tanımlanabilir (Koshiyama vd., 2022, s.41). Güvenilir yapay zekâ özelliklerinden performans ve dayanıklılık, önyargı ve ayrımcılık, yorumlanabilirlik ve açıklanabilirlik, algoritma gizliliği gibi hususların algoritma denetiminde denetim konusu olarak ele alınacak konu başlıklardır. Koshiyama vd. (2022) çalışmalarında algoritma denetiminde uygulanacak aşamaları geliştirme, değerlendirme, önleme ve güvence olmak üzere dört başlık altında ele almıştır.

Şekil 1. Algoritma Denetimi Aşamaları [3]



(Koshiyama vd., 2022, s.42)

Algoritma denetiminde geliştirme aşamasında algoritmada kullanılacak veriler ve verilerin işlenmesine ilişkin kontrol faaliyetleri denetlenir. İşletmeler yapay zeka uygulamalarını üçüncü taraflardan da edinebilirler. Nitekim Şekil 1'de verilen yapay zeka denetiminin zorluklarından biri de bu hususdur. Üçüncü taraf ürünlerin edinim ve kurulumundan önce bu ürünlerden kaynaklı herhangi bir güvenlik riskine sebep olabilecek zafiyet veya açıklığının olup olmadığı kontrol edilmelidir (Şahinaslan vd., 2023, s.54). NIST, COBIT, ISO 27001 gibi birçok uluslararası standart üçüncü taraf risk yönetim süreçlerine dair kontrollere yer vermektedir (EY, 2020, s.22). Tedarik edilen teknolojinin veri ve algoritma risklerinin belirlenerek bu risklere ilişkin kontrol faaliyetleri geliştirilmesi ve bu kontrol faaliyetlerinin denetimi ile olası risklerin en aza indirilmesi sağlanabilecektir. İç denetim tarafından, üçüncü taraflardan edinilen uygulamalar kapsamında ele alınması gereken ilk husus yapılan sözleşmeler olmalıdır. Sözleşmelerde, algoritmaların temel girdisi veriler ve algoritma denetiminde dikkat edilecek başlıca unsurların varlığı kontrol edilmelidir. Veri güvenliği ile ilgili birçok yasal düzenleme ve standart, birlikte çalışılan üçüncü tarafların denetimi maddesini içermektedir (EY, 2020, s.4). Dolayısıyla üçüncü taraf denetimleri gerçekleştirilebilir. Kullanılan verilerin, sözleşme süresi bittiğinde yeni kullanılacak sisteme aktarımı konusunun sözleşmede varlığının değerlendirilmesi bir diğer hususdur. Sözleşmede algoritmanın kullanımı, güvenliği, gizliliği ve hukuki yükümlülükleri konularında net ifadeler bulunup bulunmadığı ve tedarik edilen algoritmanın önyargılı olup olmadığı, açıklanabilirliği, yasal düzenlemelere uyumu konuları Tablo 5'te verilen kontrol faaliyetleri ile denetlenebilir. Değerlendirme aşamasında geliştirilen algoritmanın güvenilirliğine ilişkin belirlenen parametrelere ilişkin kontrol faaliyetleri denetlenir. Azaltma aşmasında, denetim değerlendirmesinde belirlenen sorunlar ele alınarak yeniden gözden geçirilir. Bir dereceye kadar model geliştirmenin belirli aşamalarına "eklenti" görevi görürler ve dolayısıyla modelin yeniden eğitilmesini ve yeniden değerlendirilmesini gerektirirler. Güvence aşamasında algoritmanın önceden belirlenmiş standartlara, uygulamalara veya düzenlemelere uygun olduğuna ilişkin kontrol faaliyetleri denetlenir. Algoritma denetimlerinde uygulanacak kontrol hedefleri ve kontrol faaliyetleri Tablo 6'da verilmiştir.

[3] Vekil açıklamalar, kullanılan algoritmaların karar verme süreçlerine ilişkin yapılacak açıklamaları/yorumları ifade etmektedir.

Tablo 6. Algoritma Denetimi Kontrol Hedefleri ve Kontrol Prosedürleri

Kontrol Hedefleri	Kontrol Faaliyetleri
Algoritmanın geliştirilme aşamasında yeterli yönetişim desteğini aldığının, kaynak kullanımının yeterliliğine dair güvence sağlamak.	• İlgili paydaşların (sahip, doğrulayıcı, kullanıcı) açıkça tanımlanması. • Paydaşların rollerinin tanımlanması ve takip edilmesi (örneğin, sahibi algoritmanın kullanımını onaylar, doğrulayıcı geliştirici işlevi için 'ikinci çift göz' rolünü yerine getirir, kullanıcı algoritmanın kullanımına ilişkin geri bildirim sağlar). • Ayrılması gereken roller (örneğin geliştirici ve doğrulayıcı) arasında net bir ayrım mevcut olduğunun tespit edilmesi. • Yapay zekâ geliştirme ekiplerindeki ırk, cinsiyet, cinsel yönelim, yaş, ekonomik koşullar vb. potansiyel önyargıya bağlı hususların değerlendirilmesi. • Algoritmanın risk kategorisinin (yüksek veya düşük) belirlenmesi. • Düzenleyici gerekliliklerin listelenmesi (örneğin, AB Yapay Zekâ Yasası uyarınca uygunluk değerlendirmesi ve algoritmanın geliştirilmesinde sürüm kontrolü)
Algoritma sağlamlığının ve algoritma sonuçlarına ilişkin güvence sağlanması.	• Dahili yönergelerin uygulandığının ve belgelendiğinin tespit edilmesi. • Modelin nasıl çalıştığının yeterince belgelendiğinin tespit edilmesi. • Algoritmaların neden olabileceği tüm potansiyel zararları içeren bir risk kaydı mevcudiyetinin belirlenmesi. • Tüm yeni algoritmalar için, etik riskler dahil tüm olası risklerin belgelenmesini içeren bir etki değerlendirmesinin yapılması. • Algoritmanın ve ayarlarının (örneğin, hiper parametreler)[4] sağlamlığının ve teorik temellere dayandığının belirlenmesi. • Algoritmanın iyileştirilmesine yönelik yaklaşımların kullanıldığının belirlenmesi. • Riskler için azaltıcı önlemlerin mevcudiyeti ve kullanımının belirlenmesi. • Algoritma performansının doğrulanması için testlerin gerçekleştirilmesi. • Algoritmanın sonuçları, konunun uzman görüşleri veya diğer kıyaslamalarla (örneğin, diğer platformlardan veya diğer algoritmalardan elde edilen sonuçlar) karşılaştırılması. • Gerektiğinde algoritmaya veya verilere ilişkin uzman görüşünden yararlanılması. • Algoritmanın varsayımları ve sınırlamaları açıklandığının belirlenmesi. • Yüksek riskli uygulamalar için algoritmalar tarafından alınan kararların açıklanabilirliği ve insanlar tarafından yorumlanabilirliğinin belirlenmesi.
Uygulamanın geliştirilen algoritma ile eşleştiğine dair güvence verilmesi	• Uygulama sürecinin belgelendiğinin tespit edilmesi. • Algoritmada veya verilerde yapılan değişikliklerin açıklanıp, belgelendiğinin tespit edilmesi. • Algoritma prototipinin (kod, veri, model, çıktı) uygulamaya uygunluğunun tespit edilmesi. • Güvenlik açıklarını keşfetmek için testlerin gerçekleştirilmesi.
Algoritmanın amaca uygun olmayan yanlış sonuçlar vermediğine dair güvence verilmesi	• Algoritmanın kullanımına ilişkin belgeler mevcut olduğunun tespit edilmesi. • Algoritmanın kullanımının amacına ve dokümantasyona uygun olduğunun tespit edilmesi. • Personelin algoritmanın nasıl kullanılacağı konusunda bilgi sahibi olduğunun tespit edilmesi. • Uygulanan bir kullanıcı geri bildirim döngüsü varlığının tespit edilmesi.
Algoritma izlemelerinin yapıldığına dair güvence verilmesi	• Performans ölçütleri (örneğin, performans doğruluğu) ve kabul edilebilir eşiklerin tanımlandığının tespit edilmesi. • İzleme sıklığının yeterliliğinin ve takibinin tespit edilmesi (örneğin, kendi kendine öğrenen algoritmalar için izleme sürekli olabilir). • Algoritmanın varsayımları ve sınırlamalarının, algoritmanın belirtilen amacı ve kullanımı için geçerliliğinin tespit edilmesi.
Uygulamaya konulan algoritmanın izlendiğine ilişkin güvence verilmesi	• Takip edilen bir inceleme sıklığı setinin mevcudiyetinin tespit edilmesi. • Algoritmanın kullanımının hâlâ amacına uygun olduğunun, algoritma hakkında hâlâ yeterli bilgi ve anlayışın mevcut olduğunun tespit edilmesi.

[4] Kullanılan algoritmalarda bazı parametrelerin ne olduğuna da ayrıca karar verilmesi gerekir. Modeli tasarlayan kişinin karar verdiği ve değişkenlik gösteren parametreler, hiper parametre olarak adlandırılır. Örneğin Knn algoritmasında kullanılacak k değerinin ne olacağı modeli tasarlayan kişi tarafından belirlenen bir hiper parametredir.

	• İnceleme sonucunda yeniden parametrelendirme gerçekleştirildiğinin tespit edilmesi (örneğin, kendi kendine öğrenen algoritmalar için hiperparametrelerin otomatik olarak yeniden kalibre edildiği algoritmaların dinamik kalibrasyonu yapılabilir) • İncelemenin sonuçlanması halinde iyileştirmeler yapıldığının tespit edilmesi. • İncelemenin sonuçlanması halinde yeniden geliştirmenin yapıldığının tespit edilmesi.
Algoritma kalitesine ilişkin güvence sağlanması.	• Takip edilen dahili yönergelerin belgelendiğinin tespit edilmesi. • Risk analizi ve sınıflandırma (örneğin yüksek riskli algoritmaların doğru şekilde tanımlanması) değerlendirmesi yapıldığının tespit edilmesi. • Geliştirme sürecinin, algoritmanın kullanıldığı temel soruna uygun olup olmadığına ilişkin bir değerlendirmenin varlığının tespit edilmesi (örneğin, geliştirme ekibinin yeterince çeşitli olması, algoritmaların seçiminde kavramsal sağlamlığın bulunması). • Algoritmanın performansına ilişkin bir değerlendirme yapıldığının test edilmesi (örneğin istatistiksel testler, k-katlı çapraz doğrulama, yetersiz/fazla uyum analizi, duyarlılık analizi vb.). • Bulgular, öneriler ve bulunan önem dereceleri konusunda geliştiricilere ve kullanıcılara danışıldığının tespit edilmesi. • Doğrulama aşamasından elde edilen sonuçlar takip edildiğinin tespit edilmesi.

(Sandu vd. 2022'den uyarlanmıştır)

Uygulanacak kontrol faaliyetleri ile algoritmalarla ilişkili risklerin değerlendirilmesi ve azaltılması için yapılandırılmış bir yaklaşım sağlanarak algoritmaların etkili, etik, düzenlemelere ve standartlara uygun olduğuna ilişkin güvence sağlanabilecektir.

5. SONUÇ

Birçok alanda fayda sağlayan, insanların ve işletmelerin işlerini kolaylaştıran yapay zekânın sağladığı fırsatların yanında getirmiş olduğu riskler mevcuttur. Yapay zekâ uygulamalarının temeli olan veri ve algoritmaların yanlılık, önyargı, açıklanabilirlik, etik vb. riskleri üzerinde çalışmalar son yıllarda hız kazanmıştır. Yapay zekâ uygulamalarının riskleri güvenilir yapay zekâ tartışmalarının doğmasına neden olmuştur. Bugün bu alanda birçok kuruluş tarafından farklı düzenlemeler yapıldığı ve bu sorunun uluslararası toplantılarda ele alındığı görülmektedir. Güvenilir yapay zekâ, işletmeler içindeki yapay zekâ uygulamalarının bütünlüğünü ve güvenilirliğini artırarak bu teknolojilerin sorumlu ve etik kullanımını teşvik etmektedir.

Güvenilir yapay zekânın sağlanmasında yapay zekâ denetimi ise denetçiler açısından güncel bir denetim alanıdır. Yapay zekânın denetlenmesi, yapay zekâ teknolojilerinin sorumlu, etik, yasal ve düzenleyici gerekliliklere uygun olarak geliştirilmesini, dağıtılmasını ve kullanılmasını sağlamak için önemli bir adımdır. Yapay zekâ denetimi, uygulamalara olan güveni ve hesap verebilirliği teşvik ederken potansiyel önyargıların, şeffaflık sorunlarının ve etik kaygıların giderilmesine yardımcı olacaktır. Güvenilir yapay zekâ denetimi bağımsız denetim ve iç denetim olmak üzere iki şekilde gerçekleştirilebilir. Çalışmada yapay zekâ denetimi iç denetim bağlamında ele alınmıştır. Risk yönetimi konusunda iyi bir deneyim sahibi olan iç denetim mesleği risk kavramının içinde barındırdığı fırsatlara odaklanmayı bilerek yapay zekâ denetimi ile işletmelere değer katma konusunda önemli bir yere sahip olacaktır. İç denetçiler, etik ilkelere bağlılığı, mevzuata uygunluğu, risk yönetimini ve şeffaflığı değerlendirerek güvenilir yapay zekânın geliştirilmesine ve sürdürülmesine katkıda bulunur.

İç denetçiler için yapay zekâ denetiminde veri ve algoritma denetimleri başlangıç noktası olarak alınabilir. Bu çalışmada da yapay zekâ denetimi veri ve algoritma denetimi konularını ele almıştır. Yapay zekâ uygulamalarının temeli olan verinin kalitesi, büyüklüğü, yanlılığı, gizliliği gibi birtakım noktalar denetimlerde uygun kontrol faaliyetleri ile değerlendirilmelidir. Yapay zekâ uygulamalarında kullanılan algoritmalar için ise algoritmanın geliştirme ve uygulama sonrasındaki aşamaları da dahil olmak üzere bu aşamalarda yanlılık, önyargı, açıklanabilirlik, şeffaflık, performans gibi kriterleri algoritma denetimi kapsamında denetleme konularıdır. İç denetim ayrıca yapay zekâ uygulamalarının işletmelere entegre edilmesi aşamasında danışmanlık faaliyeti de sağlayabilir.

Yapay zekâ denetiminin en önemli kısıtlarından biri bu alanda denetçilere rehberlik edecek düzenlemelerin henüz tam olarak geliştirilememesidir. Yaşanan gelişmelerin uygulamalara etkisi ile bu uygulamalara ilişkin yasal uyum ve düzenlemeler arasında bir zaman farkı söz konusudur. Yapay zekâ ve makine öğrenimi sistemlerinin geliştirilmesi ve devreye alınmasıyla birlikte yeni zorluklar ve etik hususlar ortaya çıktıkça, yapay zekâ denetimi alanı sürekli olarak gelişmektedir. Bu alanda birçok ülke ve uluslararası standart belirleme kuruluşu tarafından çalışmalar yürütülmekte ve

kamuoyu ile paylaşılmaktadır. Uluslararası İç Denetçiler Enstitüsü (The Institute of Internal Auditors-IIA) tarafından Uluslararası İç Denetim Standartları için yaşanan gelişmelere uyum sağlanabilmesi adına revize etme çalışmaları yürütülmektedir. Revize edilecek Uluslararası İç Denetim Standartları için yayınlanan Taslak Metinde, Kaynakların Yönetimi İlkesi altında 10.3 Teknolojik Kaynaklar başlığı altında yeni bir standarda yer verildiği görülmektedir. Söz konusu bu standardın iç denetim faaliyetinin ifasında kullanılacak teknolojik kaynaklar hakkında olduğu görülmektedir.

Yapay zekâ toplumun çeşitli yönleriyle giderek daha fazla bütünleştikçe, yapay zekâ denetimi de onun sorumlu kullanımını sağlama da önemli bir rol oynamaya devam edecektir. Yapay zekâ uygulamalarının tasarımında ve denetiminde dikkate alınması gereken çok çeşitli teknik, etik, yasal ve pratik konular göz önüne alındığında, çok disiplinli olmak gerektiği açıkça görülmektedir (Landers ve Behrend, 2022, s.47). Bu kapsamda iç denetçiler için kritik konulardan biri de yetkinlik olacaktır. İç denetçilerin yapay zekâ ve uygulamaları hakkında kendilerini geliştirmeleri yapılacak denetimlerin etkinliğini ve etkililiğini aynı zamanda bu alandaki nitelikli iç denetçi istihdamına olan talebi artıracaktır.

Kaynakça

Ağdeniz, Ş. (2020). *İç denetçiler neden makine öğrenmesi kullanmak zorunda?.* İç Denetim Kuruma Değer Katmak, Edt. Halis Kıral, Ankara:Seçkin Yayıncılık.

Bandy, J. (2021). Problematic machine behavior: A systematic literature review of algorithm audits. *Proceedings of the acm on human-computer interaction, 5*(CSCW1), 1-34.

Bansal. (2021, Ekim). https://www.forbes.com/sites/forbestechcouncil/2021/10/14/flying-blind-how-bad-data-undermines-business/?sh=11efc97229e8 adresinden alındı. (Erişim Tarihi, 27 Eylül 2023).

Beckstrom, J.R. 2021.Auditing machine learning algorithms. *International Journal of Government Auditing*, Winter, 40-42.

Belpaeme, T., Deschuyteneer, J., Oetringer, D. &Wolferrt, P. (2019). *The potential of social robots for persuasion and manipulation:a proof of concept study*. https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2019/10/14081257/Robots_social_impact_eng.pdf adresinden alınmıştır. (Erişim Tarihi, 10 Eylül 2023)

Brown, S., Davidovic, J., & Hasan, A. (2021). The algorithm audit: scoring the algorithms that score us. *Big Data & Society*, *8*(1). https://doi.org/10.1177/2053951720983865

Calagna, K., Cassidy, B. & Park, A. (2021). *Applying The Coso Framework And Principles To Help Implement And Scale Artificial Intellıgence*. https://www.wlrk.com/docs/Realize-the-Full-Potential-of-Artificial-Intelligence.pdf adresinden alındı. (Erişim Tarihi, 10 Eylül 2023)

Clavell, G.G., Zamorano, M.M., Castillo, C., Smith, O. & Matic, A. (2020, February). Auditing Algorithms: On Lessons Learned and the Risks of Data Minimization. In *proceedings of the AAAI/ACM conference on AI, ethics, and society*, (ss. 265-271).February 7-8, Newyork.

European Commision (2023). https://ec.europa.eu/commission/presscorner/detail/en/ip_23_5379. (Erişim Tarihi, 6 Kasım 2023).

European Parliament (2023). https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence. (Erişim Tarihi, 6 Kasım 2023).

EY (2020). EY *Türkiye üçüncü taraf kaynaklı teknoloji ve siber risk yönetimi değerlendirme raporu kasım 2020*. https://assets.ey.com/content/dam/ey-sites/ey-com/tr_tr/pdf/2020/11/ucuncu-taraf-kaynakli-teknoloji-ve-siber-risklerinizi-nasil-yonetiyorsunuz.pdf adresinden alındı. (Erişim Tarihi, 4 Aralık 2023)

Fazlıoğlu, M. (2023). *US federal ai governance:laws, policies and strategies*. https://iapp.org/resources/article/us-federal-ai-governance/ adresniden alındı. (Erişim Tarihi, 6 Kasım 2023)

IIA. (2017a). *Küresel bakış açıları ve anlayışlar yapay zekâ- iç denetim mesleğine ilişkin dikkate alınması gerekenler*

IIA. (2017b). *Küresel bakış açıları ve anlayışlar- IIA'nın yapay zekâ denetim çerçevesi, pratik uygulamalar, bölüm a.*

IIA. (2017c). *GTAG:understanding and auditing big data.*

IIA. (2018). *Küresel bakış açıları ve anlayışlar- IIA'nın yapay zekâ denetim çerçevesi, pratik uygulamalar, bölüm b.*

IIA. (2023). *Global internal audit standards 2023 draft for public comment.*

Information Commissioner's Office. (2020, Şubat). *Guidance on the AI Auditing Framework: Draft Guidance for Consultation.* Retrieved February 11, 2021, https://ico.org.uk/media/about-the-ico/consultations/ 2617219/guidance-on-the-ai-auditing-framework-draft-for-consultation.pdf adresinden alındı.

ISACA. (2018) *Auditing Artificial Intelligence*. https://ec.europa.eu/futurium/en/system/files/ged/auditing-artificial-intelligence.pdf. adresinden alındı. (Erişim Tarihi, 19 Haziran 2023)

Kinkela, K. & Harris, P. (2022). COSO new guidelines to aid internal auditors for implementing artifical ıntelligence. *Internal Auditing, 37*(1), 40-43.

Koshiyama, A.,Kazim, E., Treleaven, P., Rai, P., Szpruch, L., Pavey, G., Ahamat, G., Leutner, F., Goebel, R., Knight, A., Adams, J., Hitrova, C., Barnett, J., Nachev, P., Barber, D., Chamorro-Premuzic, T., Klemmer, K., Gregorovic, M., Khan, S. & Lomas, E. (2021). (ss. 33-44), Towards Algorithm Auditing: A Survey on Managing Legal, Ethical and Technological Risks of AI, ML and Associated Algorithms *Proceedings of the 2020 conference on fairness accountability and transparency*. Available at SSRN: https://ssrn.com/abstract=3778998 or http://dx.doi.org/10.2139/ssrn.3778998

Koshiyama, A., Kazim, E. & Treleaven, P. (2022). Algorithm auditing: managing the legal, ethical and technological risks of artifical intelligence, machine learning ans associated algortihms. *Computer, 55*(4), 40-50.

KVKK, (2021). *Yapay zeka alanında kişisel verilerin korunmasına dair tavsiyeler.* https://www.kvkk.gov.tr/Icerik/7048/Yapay-Zeka-Alaninda-Kisisel-Verilerin-Korunmasina-Dair-Tavsiyeler adresinden alındı. (Erişim Tarihi, 7 Kasım 2023)

Landers, R. N., & Behrend, T. S. (2023). Auditing the AI auditors: A framework for evaluating fairness and bias in high stakes AI predictive models. *American Psychologist*, *78*(1), 36.

Minkkinen, M., Laine, J. & Mäntymäki, M. Continuous auditing of artificial intelligence: a conceptualization and assessment of tools and frameworks. *DISO* **1**, 21 (2022). https://doi.org/10.1007/s44206-022-00022-2

Mökander, J., Schuett, J., Kirk, H. R., & Floridi, L. (2023). Auditing large language models: a three-layered approach. *AI and Ethics*, 1-31.

Munoko, I., Brown-Liburd, H. L., & Vasarhelyi, M. (2020). The ethical implications of using artificial intelligence in auditing. *Journal of Business Ethics, 167*, 209-234.

Naqvi, Al. (2020). Artificial intelligence for audit, forensic accounting and valuation. John Wiley and Sons.

Nilsson, N.J. (2018). Yapay zekâ geçmişi ve geleceği. İstanbul:Boğaziçi Üniversitesi Yayınevi.

NIST. (2023). *Artificial intelligence risk management framework* (AI RMF 1.0). https://doi.org/10.6028/NIST.AI.100-1 adresinden alındı. (Erişim Tarihi, 10 Eylül 2023)

Raji, I.D., Smart, A. White, R. N., Mitchell, M., Gebru, T., Hutchinson, B., Smith-Loud, J., Theron, D., & Barnes, P. (2020). Closing the AI Accountability Gap: Defining an End-to-End Framework for Internal Algorithmic Auditing. In Conference on Fairness, Accountability, and Transparency (FAT* '20), January 27–30, 2020, Barcelona, Spain. ACM, New York, NY, USA, 12 pages. https://doi.org/10.1145/3351095. 3372873

Roberts, H., Babuta, A., Morley, J., Thomas, C., Taddeo, M.&Floridi, L. (2023). Artificial intelligence regulation in the united kingdom:a path to good governance and global leadership?. *Internet Policy Review, 12*(2), 1-31.

Sandu, I., Wiersma, M. & Manichand, D. (2022). Time to audit your algortihms. *Maandblad voor Accountancy en Bedrijfseconomie 96*(7/8), 253–265 DOI 10.5117/mab.96.90108

Sandvig, C., Hamilton, K., Karahalios, K., & Langbort, C. (2014). Auditing algorithms: research methods for detecting discrimination on internet platforms. *Data and discrimination: converting critical concerns into productive inquiry*, *22*(2014), 4349-4357.

Say, C. (2018). Yapay zekâ. İstanbul:Bilim ve Gelecek Kitaplığı.

Selimoğlu, S.K. & Özbek, C.Y. (2018). İç denetim. Ankara:Nobel Yayınevi.

Şahinaslan, Ö., Şahinaslan, E., & Küçükali, E. (2023). Üçüncü taraf yazılım bileşenlerinden kaynaklanan zayıflıkların tespiti ve yönetimine ilişkin bir uygulama. *Denetişim*, (28), 53-74.

Ulusal Yapay Zekâ Stratejisi. (2021). https://cbddo.gov.tr/SharedFolderServer/Genel/File/TR-UlusalYZStratejisi2021-2025.pdf adresinden alınmıştır. (Erişim Tarihi, 10 Eylül 2023).

Yıldız, B. (2009). Finansal analizde yapay zeka. İstanbul: Beta.

Yıldız, B. & Ağdeniz, Ş. 2019. Denetim 4.0'ın teknolojik altyapısı. *Muhasebe ve Denetime Bakış, 58,* 83-102.

WEF. (2023). *The future of jobs report 2023.* https://www.weforum.org/publications/the-future-of-jobs-report-2023/ adresinden alınmıştır. (Erişim Tarihi, 15 Mayıs 2023).

Wright, C. (2017). Tomorrow's ERM today. *Internal Auditor,* 18-19.

İnternet Kaynakları

ISO. (2023*). ISO/IEC information technology artificial intelligence guidance on risk management*. http://www.iso.org. (Erişim Tarihi, 6 Kasım, 2023)

Unesco (2023). *Ethics of artificial intelligence*. https://www.unesco.org/en/artificial-intelligence/recommendation-ethics. (Erişim Tarihi, 6 Kasım 2023)

VOA Türkçe. (2023). *G7 risk temelli yapay zeka düzenlemesi benimsenmeli*. https://www.voaturkce.com/a/g7-risk-temelli-yapay-zekâ-duzenlemesi-benimsenmeli/7073561.html. (Erişim Tarihi, 19 Haziran 2023)

WEF. (2023). *AI governance alliance*. http://www.weforum.org. (Erişim Tarihi, 6 Kasım, 2023)