

**EDİTÖR**

*Doç. Dr. Güzide ŞENEL*

**FİNANS**

*Alanında Araştırmalar ve Değerlendirmeler*

**MART**  
**2025**

**İmtiyaz Sahibi • Yaşar Hız**  
**Genel Yayın Yönetmeni • Eda Altunel**  
**Yayına Hazırlayan • Gece Kitaplığı**  
**Editör • Doç. Dr. Güzide ŞENEL**

**Birinci Basım • Mart 2025 / ANKARA**

**ISBN • 978-625-388-244-0**

© copyright

Bu kitabın yayın hakkı Gece Kitaplığı'na aittir.  
Kaynak gösterilmeden alıntı yapılamaz, izin almadan  
hiçbir yolla çoğaltılamaz.

**Gece Kitaplığı**

**Adres:** Kızılay Mah. Fevzi Çakmak 1. Sokak Ümit Apt  
**No:** 22/A Çankaya/ANKARA Tel: 0312 384 80 40

[www.gecekitapligi.com](http://www.gecekitapligi.com)  
[gecekitapligi@gmail.com](mailto:gecekitapligi@gmail.com)

**Baskı & Cilt**  
Bizim Buro  
**Sertifika No:** 42488

# **Finans Alanında Arařtırmalar ve Deęerlendirmeler**

**Mart 2025**

Editör:  
Doç. Dr. Güzide ŐENEL



# İÇİNDEKİLER

## BÖLÜM 1

### FİNTEK UYGULAMALARININ KAMU ÇALIŞANLARI ÜZERİNDEKİ FİNANSAL ETKİLERİNİN İNCELENMESİ

*Mesut ASLAN, Esra KIRTEKE* .....1

## BÖLÜM 2

### BANKACILIKTA SİBER GÜVENLİK VE RİSK YÖNETİM

*İdris ADIGÜZEL*.....21

## BÖLÜM 3

### ENDÜSTRİ 4.0 İLE DİJİTALLEŞME DÖNEMİNDEN ENDÜSTRİ 5.0 KİŞİSELLEŞTİRME SÜRECİNE

*Emel ABA ŞENBAYRAM*.....39

## BÖLÜM 4

### BORSA İSTANBUL'DA TOPSIS YÖNTEMİYLE İŞLEM GÖREN ENERJİ ŞİRKETLERİNİN FİNANSAL PERFORMANSININ ANALİZİ

*Samet BÜYÜKYILMAZ, Ayşegül AK*.....57



# BÖLÜM 1

## FİNTEK UYGULAMALARININ KAMU ÇALIŞANLARI ÜZERİNDEKİ FİNANSAL ETKİLERİNİN İNCELENMESİ

*Mesut ASLAN<sup>1</sup>*

*Esra KIRTEKE<sup>2</sup>*

---

1 Dr. Öğretim Üyesi, Bingöl Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, İşletme Bölümü, [mesutaslan@bingol.edu.tr](mailto:mesutaslan@bingol.edu.tr), 0000-0003-2338-7474

2 Yüksek Lisans Öğrenci, Bingöl Üniversitesi İktisadi ve İdari Bilimler Fakültesi İşletme Bölümü, [esrakirteke44@gmail.com](mailto:esrakirteke44@gmail.com), 0009-0002-0337-5863

## GİRİŞ

Finans, banka işlemleri, fon ve kredi işlemleri gibi tüm finans türlerini kapsayan geniş bir kavramdır (Dahlquist ve Knight, 2022). Finansal teknoloji (Fintek) ise finans ile teknolojinin birleşmesi sonucu ortaya çıkan bir yenilikçilik kavramıdır. Fintek, sadece finansal işlemleri değil, aynı zamanda teknolojik araçları kullanarak bu işlemleri daha hızlı ve verimli bir şekilde gerçekleştiren uygulamalarla da ilişkilidir. Fintek, çok sayıda uzman tarafından farklı şekillerde yorumlanmıştır. Örneğin, William J. Magnuson, Fintek terimini hukuki açıdan değerlendirerek, “Öncelikle Telefon ve Online Platformlarda Finansal Hizmetler Sağlayan Şirketler” olarak tanımlamaktadır (Magnuson, 2017).

Fintek kavramı, 19. yüzyılda finans sektöründe teknolojik cihazların kullanılmaya başlandığı dönemde şekillenmeye başlamıştır. Ancak, 20. yüzyılın ortalarından itibaren bu kavram çok daha fazla boyut kazanmıştır. 1960’lı yıllarda teknolojik araçların kullanımının artması ve iş bağlantılarının kurulmaya başlanması, Fintek’in sektörde önemli bir yere ulaşmasına zemin hazırlamıştır. 1980’li yıllara gelindiğinde ise teknolojinin sürekli gelişmesi, finans sektörünü de derinden etkilemiş ve Fintek 2.0 olarak bilinen dönem başlamıştır. Fintek 2.0, yapay zekanın kullanılmadığı, teknolojik araçların deneyimli ekipler tarafından kullanıldığı bir dönemi ifade eder. Ancak, 3.0 olarak adlandırılan yeni dönemle birlikte yapay zeka ve diğer ileri teknolojiler, Fintek hizmetlerini daha da dönüştürmüş ve bu alanda bir devrim oluşturmuştur.

Finansal Teknoloji (Fintek) terimi, 1990’ların başlarından itibaren “Finansal Hizmetler Teknoloji Konsorsiyumu” gibi organizasyonlar tarafından kullanılmaya başlanmıştır (Arner, Barberis ve Buckley, 2016, s.47; Güven ve Yaşar, 2017, s.127-130). Günümüzde, Fintek uygulamaları finansal sektördeki yenilikçi çözümleri hızla artırmaktadır. Özellikle dijital bankacılık, yapay zeka, blockchain (Blok Zinciri) ve mobil ödeme sistemleri gibi teknolojiler, finansal işlemlerin hızını artırarak verimliliği büyük ölçüde geliştirmiştir. Bu teknolojiler, kamu çalışanları ve yatırımcılar açısından önemli kolaylıklar sağlamaktadır. Ayrıca, kamu finans yönetiminde de Fintek’in önemli bir rolü vardır.

Fintek, geleneksel bankacılıkta nakit alışverişlerinin ve yüz yüze yapılan işlemlerin dijitalleşmesiyle, tek tuşla gerçekleştirilmesine olanak sağlamıştır. Bu dönüşüm, bankacılık işlemlerini son derece kolaylaştırmış ve insanların finansal işlemlerini çok daha hızlı yapabilmelerine olanak tanımıştır. Mobil bankacılık, dijital cüzdanlar ve genel bankacılık sistemleri gibi örnekler, Fintek’in hayatımıza nasıl entegre olduğunu gösteren önemli uygulamalardır (Ozili, 2020, s.23-124). Öte yandan, mobil ödeme sistemleri (Apple Pay, Google Pay), dijital cüzdanlar ve blockchain tabanlı



ödeme sistemleri de para transferlerini hızlandırmıř ve maliyetleri düşürmüřtür (Arner, Barberis ve Buckley, 2016, s.24).

Bu çalışmanın amacı, kamu çalışanlarının finans sektöründe Fintek uygulamalarının etkisini ve katkısını tespit etmektir. Günümüzde teknolojinin hızlı bir şekilde gelişmesi, finans sektöründe köklü deęişimlere yol açmakta ve Fintek uygulamaları bu dönüşümün öncüsü olmaktadır. Kamu çalışanlarının bu yeni teknolojilere ne kadar adapte oldukları ve bu uygulamaların iş süreçlerine ne gibi faydalar sağladığı, sektördeki verimlilięi artırma potansiyeli açısından büyük önem taşımaktadır. Ayrıca, Fintek'in sunduęu yenilikçi hizmetlerin kamu hizmetleriyle nasıl entegre edilebileceęi, kamu sektöründe maliyet etkinlięini ve hizmet kalitesini yükseltme konusunda fırsatlar oluşturabilir. Bu bağlamda, çalışma, hem teorik hem de pratik açıdan önemli çıkarımlar sunmayı hedeflemektedir.

## 2.Literatür Taraması

Fintek uygulamaları, teknoloji çağında bireylere büyük kolaylıklar sunmakta ve bunun doğrudan ve dolaylı pek çok etkisi bulunmaktadır. Özellikle kamu çalışanları, finansal işlemlerini daha kolay ve verimli bir şekilde yönetebilmek için Fintek uygulamalarını tercih etmektedir. Tasarruf tedbirleri ve benzeri kararların alındığı günümüzde, finans sektöründeki çalışanların işlerini daha hızlı ve etkili bir şekilde gerçekleřtirmeleri Fintek'in sağladığı avantajlar arasında yer almaktadır. Kamu çalışanlarının finans sektöründeki Fintek uygulamalarından nasıl etkilendięini belirlemek amacıyla yapılan birçok araştırma bulunmaktadır. Bu çalışmaların bazılarına Tablo 1'de yer verilmiştir.

Tablo1: Literatür Taraması

| YURT İÇİNDE YAPILMIř OLAN ÇALIřMALAR |  |                         |  |
|--------------------------------------|--|-------------------------|--|
| YAZAR/YIL                            | KONU   | YÖNTEM                  | SONUÇ  |
| <b>CANBAZ ve ERBAř (2021)</b>        | Katılım Bankacılıęında Fintek Eğilimleri ve Sektöre Katkıları        | Nitel Arařtırma Yöntemi | Analizlerden elde edilen sonuçlara göre uygun yöntem modelleri oluşturulması, analiz açısından arařtırmacılara finansal teknoloji alt yapılarına yoğunlařıldığı alanlar incelenip bu alanların finans sektörüne katkı sağlayacağı tespit edilmiştir. |
| <b>KARAÇAYIR ve AFřAR (2021)</b>     | Fintek Yatırımlarının Belirleyicileri: AB Ülkeleri Ve Türkiye Örneęi | Panel veri              | Analizlerden elde edilen sonuçlara göre işsizlik oranı ve enflasyon oranının Fintek yatırımları üzerinde anlamlı herhangi bir etkiye sahip olmadığı tespit edilmiştir.   |

|                                     |   |                                 |  |
|-------------------------------------|---|---------------------------------|--|
| <b>BULAZAR ve KÜÇÜKÇOLAK (2021)</b> | Finans Sektöründe Fintek Etkisi   | SPSS                            | Analizlerden elde edilen sonuçlara göre tüm dünya da finans sektöründe Fintek gelişmelerinin pozitif etkisi tespit edilmiştir.   |
| <b>ERDEN ve TOPAL (2021)</b>        | Türkiye’de ve Dünyada İslami Fintek Sektörünün Gelişimi   | Betimleyici Araştırma Yöntemi   | Analizlerden elde edilen sonuçlara göre Fintek’lerin ve İslami Fintek’lerin geleneksel finans piyasasına pozitif etkilerinin olduğu tespit edilmiştir.                               |
| <b>CANDEMİR (2020)</b>              | Bankacılık Sektöründe Yeni Trendler ve Teknolojik Gelişmeler: Fintek Sektörü Üzerine Bir Uygulama | Swot yöntemi                    | Analizlerden elde edilen sonuçlara göre Türk bankalarının Fintek teknolojileri sayesinde teknolojik gelişmeleri iyi uygulayabildikleri tespit edilmiştir.                            |
| <b>KÖMÜRCÜOĞLU ve AKYAZI (2020)</b> | Finansal Teknolojilerdeki (Fintek) Gelişmeler: Fırsatlar ve Riskler                               | İstatiksel Desen Tanıma Yöntemi | Analizlerden elde edilen sonuçlara göre Fintek çalışmalarının sektör için fırsatlar ve riskler barındırdığı tespit edilmiştir.   |
| <b>SEZAL (2020)</b>                 | Fintek Hizmetlerinin Finans Sektörüne Etkileri ve Sağlanan Devlet Teşvikleri                      | SPSS                            | Analizlerden elde edilen sonuçlara göre dünyada ve Türkiye’de fintek uygulama alanları, Fintek girişimlerine sağlanan devlet destekleri hakkında bilgi verileceği tespit edilmiştir. |
| <b>GENÇ ve KÜÇÜKÇOLAK (2020)</b>    | Türkiye’de Fintek Sektörü   | SPSS                            | Analizlerden elde edilen sonuçlara göre Fintek sektöründeki gelişme ve bu gelişmenin sektörün geleceği için olumlu olacağı tespit edilmiştir.  |
| <b>DEMİRDÖĞEN (2020)</b>            | Avrupa’daki İslami Fintek Ekosisteminin Analizi   | SPSS                            | Analizlerden elde edilen sonuçlara göre Avrupa’daki İslami Fintek şirketleri ve ürünlerinin karşılaştırılarak sektörde daha fazla kullanılacağı tespit edilmiştir.                   |
| <b>ÇAĞIL ve CANDEMİR (2020)</b>     | Türk Bankacılık Sektörünün Fintekler Karşısında Awot Analizi                                      | SWOT analizi                    | Analizlerden elde edilen sonuçlara göre Türk bankalarının Fintek’leri bir fırsat olarak gördüğü tespit edilmiştir.   |

| <b>DEMİRDÖĐEN<br/>(2020)</b>                      | İslami Fintek Eko-<br>sistemi Üzerine Bir<br>Deęerlendirme                                | Nitel Bir<br>Arařtırma                | Analizlerden elde edilen<br>sonuçlara göre İslami<br>Finteklerin gelişmesinin İslami<br>bankalarla entegrasyonu<br>daha çabuk sağlanacağı tespit<br>edilmiştir.  |
|---|---|---------------------------------------|--|
| <b>YURTDIŐINDA YAPILMIŐ OLAN ÇALIŐMALAR</b>       |   |                                       |  |
| <b>YAZAR/YIL</b>                                  | <b>KONU</b>   | <b>YÖNTEM</b>                         | <b>SONUÇ</b>   |
| <b>RABBANİ KHAN<br/>ve THALASSİNOS<br/>(2020)</b> | Yapay Zeka ve Maki-<br>ne Öğrenimi Fintek<br>Endüstrisine Nasıl<br>Sızıyor?               | İstatiksel<br>Desen Tanıma<br>Yöntemi | Analizlerden elde edilen<br>sonuçlara göre Finansal<br>analiz ve müşteri katılımı gibi<br>olağanüstü faydaları nedeniyle<br>yapay zeka (YZ) ve makine<br>öğreniminin (YÖ) kullanımının<br>finans piyasasında geliştięi<br>tespit edilmiştir.                               |
| <b>RAJ<br/>(2020)</b>                             | Al ve Makine Öğre-<br>nimi Fintek Endüstri-<br>sine Nasıl Sızıyor?<br>Müşteri Düşüncesi   | İstatiksel<br>Desen Tanıma<br>Yöntemi | Analizlerden elde edilen<br>sonuçlara göre Para Piyasası<br>daha kolay ve hızlı işlemler<br>talep etmeye devam ettikçe,<br>yapay zeka ve makine<br>öğrenimi gibi yeni ortaya çıkan<br>teknolojilerin Fintek sektörüne<br>daha fazla ihtiyaç duyacağı<br>tespit edilmiştir. |
| <b>ALİ, HASHMİ VE<br/>HASSAN<br/>(2019)</b>       | İslami Fintekin<br>Küresel Manzarası:<br>Fırsatlar, Zorluklar<br>ve Önümüzdeki<br>Gelecek | Nitel Bir<br>Arařtırma                | Analizlerden elde edilen<br>sonuçlara göre İslami Fintek<br>endüstrisi incelendiğinde<br>finansal teknolojinin karşılaştığı<br>zorlukların aşılacağı tespit<br>edilmiştir.   |
| <b>AZİZA<br/>(2024)</b>                           | Finansal Teknoloji-<br>nin Zekât Kurum-<br>larının Şeffaflığı<br>Üzerindeki Etkileri      | NVIVO ile<br>Analiz                   | Analizlerden elde edilen<br>sonuçlara göre bu çalışmada<br>sunulan içgörüler, teknolojinin<br>zekât kurumlarında şeffaflığı<br>ve etkinliği artırmadaki rolüne<br>dair bakış açısı sunacağı tespit<br>edilmiştir.  |
| <b>BUÇAK vd.,<br/>(2018)</b>                      | Fintek düzenleyici<br>arbitraj ve gölge<br>bankaların yükseliői                           | İstatistiki Veri<br>Yöntemi           | Analizlerden elde edilen<br>sonuçlara göre düzenleyici<br>farklılıklar ve teknolojik<br>avantajların büyümeye katkıda<br>bulunabileceęi tespit edilmiştir.   |

|  |   |                             |  |
|--|---|-----------------------------|--|
| <b>TEMELKOV<br/>(2018)</b>                   | Fintech Firmaları Bankalar İçin Fırsat mı Tehdit mi?                          | Pearson Correlation ve SPSS | Analizlerden elde edilen sonuçlara göre Fintek'in ilgili ve rekabetçi finansal bankalara yardımcı olabilecek stratejiler geliştireceği tespit edilmiştir.  |
| <b>KIM, CHOI VE LEE<br/>(2017)</b>           | Ekonomik Sistem ve Finansal Okuryazarlık: Kuzey Koreli Mültecilerden Kanıtlar | SPSS                        | Analizlerden elde edilen sonuçlara göre Finansal okuryazarlığın erken yaşam evrelerinde geliştirildiği ve sonraki evrelerde kolayca değiştirilemeyeceği tespit edilmiştir.   |
| <b>ARNER, BARBERİS VE BUCKLEY<br/>(2016)</b> | Fintekin 150 Yılı: Evrimsel Bir Analiz.                                       | SPSS                        | Analizlerden elde edilen sonuçlara göre, Fintek'in ekonomi ve toplumda finansın rolüne dair uzun süredir süregeldiği tartışmaların bir parçası olduğu ve bu konuda coğrafi perspektiflerin de göz önünde bulundurulması gerektiği tespit edilmiştir. |

Literatürde yapılan araştırmalara bakıldığında, Fintek uygulamalarının dünya genelinde finans sektörü üzerinde önemli etkiler oluşturduğu ve bu etkinin her geçen yıl daha da arttığı görülmektedir. Çeşitli çalışmalar, bu etkileşimi farklı açılardan inceleyerek finans sektöründeki değişimlere dair analizler sunmaktadır. Bu çalışmaların çoğunda, özellikle kamu çalışanlarının Fintek uygulamalarından nasıl etkilendiği ve bu etkilerin sektörde nasıl şekillendiği detaylı bir şekilde ele alınmıştır. Kamu çalışanlarının mobil bankacılık, dijital bankacılık, Apple Pay gibi Fintek uygulamalarını tercih etme oranlarındaki artışa dikkat çekilirken, güvenlik ve koruma mevzuatlarının daha dar kapsamlı ve özgül incelemelere tabi tutulması gerektiği vurgulanmaktadır. Ancak bu çalışmalardan farklı olarak, bu araştırma bireylerin, özellikle kamu çalışanlarının, finans sektöründe Fintek uygulamalarını hem zaman hem de performans açısından tercih etmelerinin sebeplerine odaklanmaktadır. Bu özgün yaklaşım, Fintek uygulamalarının kullanıcılar üzerindeki etkilerini sadece bir tercih meselesi olarak değil, aynı zamanda bireysel verimlilik ve zaman yönetimi perspektifinden de incelemeyi amaçlamaktadır. Çalışma, bu yeni bakış açısıyla literatüre katkı sağlamak ve daha derinlemesine bir anlayış geliştirmeyi hedeflemektedir.

### 3. Veri Seti ve Yöntem

Veri setinin özellikleri betimsel istatistik yönteminde kullanılan istatistiksel yöntemlerdir ve analizlerde genellikle başvurulan bir tekniktir (Gujarati, 2009 s. 25) Bu yöntemler, verinin merkezi eğilim ölçüleri (ortalama, medyan, mod), dağılım ölçüleri (standart sapma, varyans) ve şekil

ölçüleri (çarpıklık, basıklık) gibi istatistiksel özetlerle ifade edilmesini sağlar (Wooldridge, 2016 s. 3). Özellikle veri setlerinde, deęişkenlerin temel yapısını anlamak ve modelleme öncesinde doęru çıkarımlar yapmak için betimsel istatistiklerden yararlanır.

Ölçeğin yapı geçerliğini ölçmek amacıyla yapılan Faktör analizi öncesinde, verilerin normal dağılım eğilimine uygun olup olmadığını belirlemek için normallik testi, veri yapısının Faktör analizine göre hazırlandığını belirlemek için Kaiser-Meyer-Olkin (KMO) ve ölçme aracının faktör yapılarına ayırt etmek için Barlett's testi yapılmıştır (Usta, 2013, s.237).

Faktör analizi (FA), birden fazla verinin farklı deęişkenlerle bir araya gelerek az sayıda kavramsal olarak anlamlı yeni deęişkenler (faktörler, boyutlar) ortaya çıkarmayı amaçlayan çok deęişkenli bir istatistik olarak açıklanabilir. Daniel'e (1988) göre faktör analizi, bir grup deęişkenin kovaryans türünü incelemek ve bu deęişkenler arasındaki ilişkileri, faktör olarak adlandırılan çok sık gözlenemeyen gizli deęişkenleri göstermek üzere düzenlenmiş bir tekniktir (Büyüköztürk, 2002 s. 472).

Bu çalışmada veri toplamada online anket kullanılmıştır. Bu çalışma için gözlemler den veri toplamak olanaklı olmasına rağmen, "geleneksel veriler elde etme ve dolayısıyla analiz imkanı" ayrıcalığı nedeniyle anket yöntemi yapılmıştır (Çetin, 2008 s. 102). Ankette toplamda 24 soru sorulmuştur. Bu sorulardan 6 tanesi kişisel ve demografik bilgiler 18 tanesi ise kamu çalışanlarının finans sektöründe finans etkisi ile ilgilidir. Hipotezlerin çözümlene sonuçlarının deęerlendirilmesinde, (5) Kesinlikle Katılıyorum, (4) Katılıyorum, (3) Kısmen Katılıyorum, (2) Katılmıyorum, (1) Kesinlikle Katılmıyorum, biçiminde istatistik ortalama yöntemi kullanılmıştır. Elde edilen verilerin yorumlanmasında SPSS Statistics programı kullanılmıştır. Verilerin detaylı yorumlanmasında Betimsel İstatistik, SPSS Faktör Analizi, KMO ve Barlett testi, Güvenirlilik testi ve Tek Örneklem T-Testi kullanılmıştır.

Toplam 441 katılımcının cevapladığı ankette verilerle ölçeğin açıklayıcı ve doęrulatoryıcı faktör analizi yapılarak güvenilirlik katsayısı sonuçlarına ulaşılmıştır. Katılımcılar Kamuda çalışan güvenlik, eğitim, sağlık ve idari hizmetler alanlarında çalışmaktadır. Ankete katılan katılımcılar, tesadüfi örnekleme yöntemiyle belirlenmiştir. Kamuda çalışanların finans sektöründe fintek etkisinin tespitinde aşağıdaki hipotezler kurulmuştur.

Tablo 2. Araştırmaya İlişkin Hipotezler

| HİPOTEZLER  |
|---|
| <b>H1:</b> Kamu çalışanlarının finansal sektörle ilişkisi ile Fintek uygulamalarının etkisi arasında anlamlı bir ilişki vardır.   |
| <b>H2:</b> Kamu çalışanlarının teknolojik uygulamalar üzerindeki etki düzeyi ile Fintek uygulamalarının düzeyi arasında anlamlı bir ilişki vardır.                      |
| <b>H3:</b> Kamu çalışanlarının teknolojik uygulamaları tercih etme düzeyi ile finansal sektörün gelişim düzeyi arasında anlamlı bir ilişki vardır.                      |
| <b>H4:</b> Kamu çalışanlarının teknolojik uygulamaları etkin kullanımı konusunda aldıkları eğitim ile Fintek uygulamalarının düzeyi arasında anlamlı bir ilişki vardır. |
| <b>H5:</b> Fintek uygulamalarının düzeyi ile finansal sektörün gelişim seviyesi arasında anlamlı bir ilişki vardır.   |
| <b>H6:</b> Kamu çalışanlarının finansal sektördeki etki düzeyi ile finansal teknoloji uygulamalarının düzeyi arasında anlamlı bir ilişki vardır.                        |
| <b>H7:</b> Finansal teknoloji düzeyi, kamu çalışanlarının cinsiyetine göre farklılık göstermektedir.  |
| <b>H8:</b> Finansal teknoloji düzeyi, kamu çalışanlarının ikamet ettikleri yere göre farklılık göstermektedir.  |
| <b>H9:</b> Finansal teknoloji düzeyi, kamu çalışanlarının gelir düzeylerine göre farklılık göstermektedir.  |
| <b>H10:</b> Finansal teknoloji düzeyi, kamu çalışanlarının genel çevresine göre farklılık göstermektedir.   |

#### 4. Analiz ve Bulgular

Çalışmada katılımcıların demografik özelliklerini ve Fintek kullanım düzeylerini belirlemek amacıyla bir anket uygulanmıştır. Katılımcılara uygulanan ankette, demografik özelliklerini belirlemek için 6 soru sorulmuş, Fintek kullanım düzeylerini öğrenmek amacıyla ise 18 soru yöneltilmiştir. Veri analizi SPSS yöntemiyle yapılmış olup, elde edilen verilerin yorumlanmasında normal aritmetik ortalama ve yüzde dağılımlar ölçeği kullanılmıştır. Anket, 05.02.2025 ile 17.02.2025 tarihleri arasında çeşitli istihdam alanlarında çalışan 169 (%39,4) kadın ve 260 (%60,6) erkek olmak üzere toplam 429 kamu çalışanına yönelik gerçekleştirilmiştir. Ankete ait ekonomik ve demografik bilgiler, Tablo 1’de sunulmuştur.

Tablo 3. Ekonomik ve Demografik Bilgiler

| Ölçek             | Veri        | Frekans | Yüzde       | Ölçek  | Veri                    | Frekans | Yüzde       |
|-------------------|-------------|---------|-------------|--|-------------------------|---------|-------------|
| 1. Cinsiyet       | Kadın       | 169     | 39,4        | 5. Kaç yıldır kamu sektöründe çalışıyorsunuz?  | 0-5                     | 59      | 13,8        |
|                   | Erkek       | 260     | <b>60,6</b> |  | 6.-10                   | 140     | 32,6        |
| 2. Yaş            | 0-24        | 26      | 6,1         |  | 11-15                   | 200     | <b>46,6</b> |
|                   | 25-34       | 131     | 30,5        |  | 16 ve üzeri             | 30      | 7           |
|                   | 35-45       | 189     | <b>44,1</b> | 6. Hanenizde çalışan kişi sayısı?              | 0-1                     | 79      | 18,4        |
|                   | 46 ve üzeri | 83      | 19,3        |  | 2-3                     | 310     | <b>72,2</b> |
| 3. Öğrenim Durumu | İlköğretim  | 5       | 1,2         |  | 4 ve üzeri              | 40      | 9,3         |
|                   | Ortaöğretim | 2       | 0,5         | 7. Fintek kavramının anlamını biliyor musunuz? | Kesinlikle Katılmıyorum | 0       | 0           |
|                   | Lise        | 30      | 7,3         |  | Katılmıyorum            | 0       | 0           |
|                   | Üniversite  | 374     | <b>91</b>   |  | Kararsızım              | 364     | <b>89,7</b> |
| 4. İstihdam Şekli | Güvenlik    | 99      | 23,1        |  | Katılıyorum             | 40      | 9,9         |
|                   | Eğitim      | 138     | <b>32,2</b> | Kesinlikle Katılıyorum                         | 7                       | 0,4     |             |
|                   | Sağlık      | 127     | 28,4        |  |                         |         |             |
|                   | Diğer       | 60      | 16,3        |  |                         |         |             |

Tablo 3'te Kamu çalışanlarının finans sektöründe fintek etkisinin tespitini belirlemek amacıyla yapılan anketin katılımcılarının demografik sonuçları sunulmuştur. Katılımcıların cinsiyet dağılımına baktığımızda, %39,4'ü kadın, %60,6'nın ise erkek olduğu görülmektedir. Bu, anketin daha fazla erkek katılımcı tarafından yanıtlandığını gösteriyor. Ancak, kadın ve erkek oranları arasında belirgin bir fark bulunmaktadır. Yaş dağılımında ise katılımcıların büyük bir kısmı 35-45 yaş aralığındadır (%44,1). Bu, anketin daha çok orta yaş grubu katılımcılarından oluştuğunu göstermektedir. 25-34 yaş aralığı ise %30,5 ile ikinci sıradadır. 46 yaş ve üzeri katılımcı oranı %19,3, 0-24 yaş aralığı ise %6,1 gibi küçük bir orana sahiptir. Bu durum, genellikle kamu sektöründe çalışmaya başlayan bireylerin daha ileri yaşlarda bu alanda deneyim kazandıklarını göstermektedir. Öğrenim durumu açısından, katılımcıların büyük çoğunluğu (%91) üniversite mezunu. Bu durum kamu sektöründe çalışanların büyük bir kısmının eğitim düzeyinin yüksek olduğunu göstermektedir. Lise mezunu katılımcılar ise %7,3, ortaöğretim ve ilköğretim mezunu olan katılımcılar ise toplamda %1,7 gibi küçük bir orana sahiptir. Bu, eğitilmiş ve nitelikli bir iş gücünün olduğu ve Fintek uygulamaları ile ilgilenen katılımcıların eğitim

düzeylerinin yüksek olduğunu göstermektedir. İstihdam şekli açısından, katılımcıların çoğunluğu eğitim (%32,2) ve sağlık (%28,4) sektörlerinde çalışmaktadır. Bu durum kamu çalışanlarının önemli bir kısmının bu iki sektörde yoğunlaştığını göstermektedir. Güvenlik sektöründe çalışan katılımcılar %23,1 oranında, diğer sektörlerde çalışanlar ise %16,3 oranında yer almaktadır.

Kaç yıldır kamu sektöründe çalışıldığına bakıldığında, katılımcıların %46,6'sı 11-15 yıldır kamu sektöründe çalışmaktadır. Bu durum deneyimli bir iş gücünün sektörde yer aldığını göstermektedir. 6-10 yıl arasında çalışanların oranı %32,6, 16 yıl ve üzeri çalışanların oranı ise %7 gibi küçük bir orana sahiptir. İlk 5 yılda çalışanlar ise %13,8 gibi küçük bir oranı oluşturmaktadır. Hanedeki çalışan kişi sayısı açısından, katılımcıların büyük çoğunluğunun (%72,2) 2-3 kişi arasında çalışan üyeye sahip olduğu görülmektedir. Bu durum, katılımcıların çoğunun hanelerinde birden fazla çalışan bulunduğunu ve finansal teknolojilere daha yatkın bir aile yapısına sahip olabileceğini göstermektedir. 4 ve üzeri çalışan olan haneler %9,3, 0-1 çalışan olan haneler ise %18,4 oranında bulunmaktadır. Fintek kavramının anlamını bilme durumuna baktığımızda, katılımcıların %89,7'si "kararsızım" seçeneğini işaretlemiş, yani çoğunluk Fintek kavramını ya tam olarak anlamamış ya da kesin bir görüş belirtmemiş. %9,9'u "katılıyorum" seçeneğini seçerken, %0,4'ü "kesinlikle katılıyorum" demiştir. Bu durum, katılımcıların çoğunluğunun Fintek hakkında bilgi sahibi olmadığını, ancak küçük bir kısmının bu kavramı anlamış veya benimsemiş olduğunu göstermektedir.

Tablo 4. Normallik testi

| Testler  | Kolmogorov-Smirnova |     |      | Shapiro-Wilk |     |      |
|--|---------------------|-----|------|--------------|-----|------|
|  | İstatistik          | df  | Sig. | İstatistik   | df  | Sig. |
| <b>Kamu Çalışanlarının Finans Sektöründe Fintek Etkisi Tespiti</b> | ,116                | 429 | ,000 | ,949         | 429 | ,000 |

Tablo 4'te Normallik testinin sonuçları sunulmuştur. Normal Dağılım gösteren anket sonuçlarında p-değeri > 0.00 olması ve histogram grafiğinin de çan eğrisi şeklinde olması gerekir. Normallik testi sonuçlarına göre verilerimizin normal dağılım ölçeğine göre %5 anlamlılık düzeyinde veri normal dağılmıyor. Likert tipi uygulanan ölçekli anketlerde bu durumla karşılaşılabilir. Böyle sonuçlar çıktığında çarpıklık ve basıklık değerlerine bakılacaktır.



Tablo 5. arpıklık ve Basıklık

| Ölçekler   | arpıklık-Basıklık Deęeri | İstatistik | Std. Hata |
|--|---------------------------|------------|-----------|
| Kamu alıřanlarının Finans Sektöründe Fintek Etkisi Tespiti Ölçeęi | arpıklık                 | 0,126      | 0,118     |
|  | Basıklık                  | -1,150     | 0,235     |

Tablo 5'te arpıklık ve basıklık deęerlerine ait sonuçlar sunulmuřtur. Faktör analizine bakılmadan önce verilerin normal daęılıp daęılmadığını bulmak için normallik testine bakılmıřtır. Kolmogrov-Smirnov testi deęeri ( $p > .000$ ) anlamlı ıktığından, ölçekten alınan puanların normal daęılım gösterip göstermediğini belirlememiz amacıyla arpıklık ve basıklık deęerlerine bakılmıřtır. Bu konuda bilgili olan kiři Tabachnick'tir. Tabachnick ve Fidell'e (2012) göre arpıklık ve basıklık katsayılarının -1.5 ile +1.5 arasında olması durumunda verilerin normal daęılım gösterdiği varsayılmaktadır. Mesleki etik veri sonuçlarına bakıldığında arpıklık ve basıklık katsayısı -1.68 ve 2,05'dir. Normallik testi sonuçlarına göre verilerimizin normal daęılım göstermedięi görülmektedir. Ancak, basıklık ve arpıklık deęeri +2 ile -2 aralıęındaki verilerin sonuçlarının normal daęılım gösterdiği kabul edilmektedir (Akyol, 2021 s. 95). Tablo 4'teki verilere bakıldığında bu veriler, kamu alıřanlarının finans sektöründe Fintek etkisini tespit etmeye yönelik ölçekte, arpıklık deęerinin 0,126 ile simetrik bir daęılımı, basıklık deęerinin ise -1,150 ile daha düz ve yayvan bir daęılımı iřaret ettiğini göstermektedir. Bu, verilerin uç deęerlerden uzak ve merkezi eęilimde yoğunlařtığını, dolayısıyla analiz için uygun olduğunu belirtmektedir.

Tablo 6. KMO ve Bartlett Testi

|  |             |      |
|--|-------------|------|
| <b>Kaiser-Meyer-Olkin Örnekleme Yeterlilięi Ölçüsü</b> |             | ,935 |
| <b>Bartlett'in Küresellik Testi</b>                    | <b>Df</b>   | ,153 |
|  | <b>Sig.</b> | ,000 |

Tablo 6'da KMO ve Bartlett Testi sonuçlarına ulařılmıřtır. 18 maddeden oluřan kamu alıřanlarının finans sektöründe fintek etkisinin tespiti verilerinin faktör analizine uygun olup olmadığđ Kaiser-Meyer-Olkin (KMO) ve Bartlett Testleri yapılarak incelenmiřtir. Tablo 5'e bakıldığında Kaiser-Meyer-Olkin sonucumuz 0,935'dir. Bu sonuç 0,70 ve üstü olması beklenir. Literatürde bu deęerin 0,90 ve üstü olması sonuçların örnekleme yeterlilięi çok yüksek, faktör analizi için mükemmel uygunluk olduğunu

gösterir. Sig değerinin ,000 olması sonuçların anlamlı olduğunu gösterir. Böyle sonuçlarda verilerin verilerin faktör analizine uygun olduğunu ve faktörlerin güvenilir bir şekilde çıkarılabileceğini işaret etmektedir.

*Tablo 7.Faktörlerin Varyansı Açıklama Oranları*

| Bileşenler        | Başlangıç Özdeğerleri |             |            | Faktörler     |               |               |
|-------------------|-----------------------|-------------|------------|---------------|---------------|---------------|
|                   | Toplam                | Varyansın % | Yığılmış % | Toplam        | Varyansın %   | Yığılmış %    |
| <b>1.Faktör</b>   | 13,654                | 75,857      | 75,857     | <b>75,857</b> | <b>84,446</b> | <b>91,138</b> |
| <b>2. Faktör</b>  | 1,546                 | 8,589       | 84,446     |               |               |               |
| <b>3. Faktör</b>  | 1,205                 | 6,692       | 91,138     |               |               |               |
| <b>4. Faktör</b>  | ,547                  | 3,038       | 94,176     |               |               |               |
| <b>5. Faktör</b>  | ,281                  | 1,562       | 95,738     |               |               |               |
| <b>6. Faktör</b>  | ,173                  | ,962        | 96,700     |               |               |               |
| <b>7. Faktör</b>  | ,124                  | ,690        | 97,390     |               |               |               |
| <b>8. Faktör</b>  | ,092                  | ,510        | 97,900     |               |               |               |
| <b>9. Faktör</b>  | ,071                  | ,395        | 98,295     |               |               |               |
| <b>10. Faktör</b> | ,067                  | ,373        | 98,668     |               |               |               |
| <b>11. Faktör</b> | ,058                  | ,321        | 98,989     |               |               |               |
| <b>12. Faktör</b> | ,045                  | ,247        | 99,237     |               |               |               |
| <b>13. Faktör</b> | ,032                  | ,177        | 99,413     |               |               |               |
| <b>14. Faktör</b> | ,027                  | ,149        | 99,563     |               |               |               |
| <b>15. Faktör</b> | ,025                  | ,136        | 99,699     |               |               |               |
| <b>16. Faktör</b> | ,022                  | ,122        | 99,821     |               |               |               |
| <b>17. Faktör</b> | ,019                  | ,103        | 99,924     |               |               |               |
| <b>18. Faktör</b> | ,014                  | ,076        | 100,000    |               |               |               |

Tablo 7’de Faktör analizi sonuçları bulunmaktadır. Faktör, ölçekteki maddelerinin birbiriyle arasındaki korelasyon sonuçlarına göre oluşmaktadır. Tablo 6’ya baktığımızda, İlk faktör, %75,857’lik bir varyansı açıklayarak en büyük paya sahiptir ve toplamda %84,446’ya ulaşmaktadır. Diğer faktörlerin açıklanan varyans oranları daha düşüktür ve toplam varyans, 18. faktörde %100’e ulaşmaktadır. Bu durum modelin büyük bir kısmının ilk birkaç faktör tarafından açıklandığını göstermektedir.

Tablo 8. Tanımlayıcı İstatistikler

| <b>Kamu Çalışanlarının Finans Sektöründe Fintek Etkisi Tespiti Ölçeği Alt boyutları</b>  | <b>Ortalama</b> | <b>Standart Sapma</b> | <b>N</b> |
|--|-----------------|-----------------------|----------|
| <b>1.Kamu çalışanları finans sektöründe fintek kavramının anlamını bilmektedir.</b>  | 3,65            | 0,839                 | 429      |
| <b>2.Kamu çalışanları finansal işlemleri gerçekleştirmek için geleneksel bankacılık yerine fintek çözümlerini tercih etmektedir.</b> | 3,87            | 0,561                 | 429      |
| <b>3.Kamu çalışanlarının finansal sektörde dijital bankacılık uygulamalarının kullanımı artmaktadır.</b>                             | 4,14            | 0,345                 | 429      |
| <b>4.Kamu çalışanlarının finansal sektörde mobil ödeme yöntemleri kullanmaları günlük işlemlerini kolaylaştırdığı bilinmektedir.</b> | 4,20            | 0,651                 | 429      |
| <b>5.Kamu çalışanlarının kredi veya yatırım işlemlerinde fintek tabanlı danışmanlık hizmetlerinin kullanımı artmaktadır.</b>         | 2,99            | 1,213                 | 429      |
| <b>6.Kamu çalışanlarının fintek çözümleri finansal işlemleri güvenli hale getirmektedir.</b>   | 2,34            | 1,396                 | 429      |
| <b>7.Fintek çözümleri maaş,ek ödemeler ve diğer finansal işlemleri yönetmekte kolaylık sağlar.</b>                                   | 4,37            | 0,482                 | 429      |
| <b>8.Kamu çalışanları için fintek tabanlı çözümler sıklıkla kullanılmaktadır.</b>  | 2,86            | 1,209                 | 429      |
| <b>9.Kamuda çalışanların finans yönetimi fintek uygulamaları ile değişmektedir.</b>  | 4,55            | 0,499                 | 429      |
| <b>10.Kamu çalışanları için geliştirilen fintek uygulamalarında daha fazla alternatif oluşturulması beklenmektedir.</b>              | 3,87            | 1,382                 | 429      |
| <b>11.Fintek çözümlere erişimde kamu çalışanları için rehberlik ve eğitim sağlar.</b>  | 1,73            | 1,283                 | 429      |

|  |      |       |     |
|--|------|-------|-----|
| <b>12.Fintek uygulamalarının güvenilir olduğu bilinmektedir.</b>   | 3,08 | 1,237 | 429 |
| <b>13.Geleneksel bankalara göre fintek müşteri hizmetleri daha etkin kullanılmaktadır.</b>                 | 4,08 | 1,017 | 429 |
| <b>14.Fintek çözümleri,kamu çalışanlarının uzun vadeli finansal planlamalarını olumlu etkiler.</b>         | 2,93 | 1,166 | 429 |
| <b>15.Gelecekte fintek çözümlerinin kamu çalışanları için daha yaygın ve etkili olacağı bilinmektedir.</b> | 4,06 | 0,513 | 429 |
| <b>16.Kamu çalışanlarına yönelik fintek eğitimlerinin artırılması gerekmektedir.</b>                       | 3,63 | 0,883 | 429 |
| <b>17.Türkiye’de fintek uygulamalarında yasal düzenlemeler gerekmektedir.</b>                              | 4,39 | 0,488 | 429 |
| <b>18.Fintek sektöründeki gelişmeler finans sektörünü olumlu etkilemektedir.</b>                           | 4,44 | 0,497 | 429 |

Tablo 8’de Kamu çalışanlarının finans sektöründe fintek etkisinin tespiti ölçeği maddeleri ve tanımlayıcı istatistik bilgileri sunulmuştur. Ölçme araçlarının uygulamaya hizmet etmesi, onun ölçmek istediği özelliği doğru şekilde ölçmesiyle ilişkilidir(Çınar, Demir, 2010, s.24-33). Doğru ve güvenilir bir ölçüm sonucuna ulaşılamayan doğru ölçüm yapıp, kullanılma amacına hizmet etmeyen bir ölçme aracının kullanılmaması gerekmektedir(Karasar, 2006, s.145-160). Böyle bir sonuçta ise ölçme araçlarının güvenilirliğinin ve geçerliğinin birlikte ele alınmalıdır. Geçerlilik ve güvenilirlik analizleri öncesi, ölçekte yer alan soruların ve elde edilen sonuçlara bakılarak tanımlayıcı istatistikler Tablo 7’de sunulmuştur. Ölçekteki sorular incelendiğinde maddelerin ortalamalarının belirlenen ortalamanın üzerinde olduğu, buda kamu çalışanlarının finans sektöründe Fintek etkisinin olumlu olduğu ve ölçekte yer alan soruların hedeflenen hipotezlerin ise pozitif bir eğilim içinde olduğunu göstermektedir. Bu bulgu, kamu çalışanlarının finans sektöründe Fintek uygulamalarının artacağını ve bu uygulamaların dijital bankacılık ile mobil ödemeler aracılığıyla gerçekleştirileceğini desteklemektedir.

Tablo 9. Güvenilirlik Analizi Sonuçları

| ÖLÇEK   | MADDE SAYISI | CRONBACH’S ALPHA KATSAYISI |
|---|--------------|----------------------------|
| <b>Kamu Çalışanlarının finans Sektöründe Fintek Etkisi Ölçeği</b> | 18           | ,971                       |

Tablo 9’da Gvenilirlik test verileri sunulmuřtur. Gvenirlilik analizi deęerlerine gre, yaptığımız likert tipi lek anketimizin gvenirlilik katsayısı 0,971’dir. Genellikle deęer 0,70 ve zeri olması halinde gvenilir olduęu kabul edilirken, Cronbach’s Alpha deęeri 0,90’ın zerinde bulunmuř veri sonularının ok yksek gvenirlik olduęunu gstermektedir. Bu durum anket sorularının birbiriyle tutarlı ve ok gvenilir seviyesine sahip olduęunu gstermektedir.

Tablo 10. Tek rneklem İstatistikleri

| HİPOTEZLER  | $\bar{x}$ | S     | T    | Sig. (2-tailed) |
|---|-----------|-------|------|-----------------|
| 1.Kamu alıřanlarının finansal sektr fintek etkisi arasında anlamlı bir iliřki vardır.   | 3,60      | 1,150 | 4,23 | < 0,05          |
| 2.Kamu alıřanlarının teknolojik uygulamalar zerindeki etki dzeyi ile fintek uygulamaları dzeyi arasında anlamlı bir iliřki vardır.  | 3,87      | 1,369 | 2,00 | < 0,090         |
| 3.Kamu alıřanlarının teknolojik uygulamaları tercih etmesi dzeyi ile finansal sektr dzeyi arasında anlamlı bir iliřki vardır.   | 4,14      | 1,638 | 2,05 | < 0,05          |
| 4. Kamu alıřanlarının teknolojik uygulamaları etkin bir şekilde kullanabilme dzeyi ile aldıkları eęitim ve Fintek uygulama dzeyleri arasında anlamlı bir iliřki bulunmaktadır. | 4,20      | 1,419 | 1,85 | < 0,060         |
| 5.Finansal sektrde medyanın, kamu alıřanları zerindeki Fintek uygulama dzeyiyle anlamlı bir iliřkisi bulunmamaktadır  | 2,99      | 1,160 | 4,47 | < 0,050         |
| 6. Fintek uygulamaları dzeyi ile finansal sektr seviyesi arasında anlamlı bir iliřki yoktur.  | 2,34      | 1,366 | 2,62 | < 0,078         |
| 7. Finansal sektr konusunda kamu alıřanlarının etki dzeyi ile finansal teknoloji dzeyi arasında anlamlı bir iliřki vardır.  | 4,37      | 1,276 | 3,23 | < 0,005         |
| 8. Finansal sektr konusunda kamu alıřanlarının aldıkları eęitimin etki dzeyi ile finansal teknoloji dzeyi arasında anlamlı bir iliřki bulunulamamıřtır.                       | 2,86      | 1,239 | 2,45 | < 0,005         |
| 9. Finansal teknoloji dzeyi kamu alıřanlarının cinsiyetine gre farklılık gstermektedir.   | 4,55      | 1,442 | 2,00 | < 0,60          |
| 10. Finansal teknoloji dzeyi kamu alıřanlarının kredi kartı kullanımlarına gre farklılık gstermektedir.   | 3,87      | 1,174 | 2,05 | < 0,005         |
| 11. Finansal okuryazarlık dzeyi ęrencilerin birikim yapma davranıřlarına gre farklılık gstermektedir.   | 1,73      | 1,268 | 3,60 | < 0,005         |
| 12. Finansal teknoloji dzeyi kamu alıřanlarının ikamet ettikleri yere gre farklılık gstermektedir.  | 3,63      | 1,021 | 2,14 | < 0,042         |
| 13. Finansal teknoloji dzeyi kamu alıřanlarının gelir dzeylerine gre farklılık gstermektedir.  | 4,39      | 1,357 | 3,12 | < 0,005         |

|   |      |       |      |         |
|---|------|-------|------|---------|
| <b>14. Finansal teknoloji düzeyi kamu çalışanlarının genel çevresine göre farklılık göstermektedir.</b> | 4,44 | 1,314 | 3,00 | < 0,005 |
|---|------|-------|------|---------|

Tablo 10’da Tek Örneklem T-Testi sonuçları sunulmuştur. Tek örneklem testi sonuçlarına göre, hipotezler için ölçekten seçilen maddelerin ortalama faydası, belirlenen ortalamadan yüksek çıktığı için ( ...>2,5) hazırlanan hipotezler istatistiksel olarak anlamlı bulunmuştur. Bu durumun rastlantısal mı yoksa istatistiksel olarak anlamlı olup olmadığını belirlemek için Tek Örneklem t-Testi kullanılmıştır.

Bunun yanı sıra Tablo 9’da yer alan tek örneklem t testi ve p-değerlerine bakıldığında, kriter olarak belirlenen değerin 0,05 olduğu bir araştırmada 0,05’ten küçük bir p-değerinin istatistiksel olarak anlamlı olduğu görülmektedir. Boş hipotezin doğru olma olasılığı %5’ten az olduğundan, sıfır hipotezine karşı güçlü kanıt olduğu görülmektedir. Bu durumlarda sıfır hipotezi reddedilir ve alternatif hipotez doğru kabul edilir. Dolayısıyla, hazırladığımız hipotez olumlu iken sıfır hipotezi olumsuz olarak kabul edilmiştir.

## SONUÇ

Finansal teknolojiler (Fintek), finans sektöründe dijitalleşmenin ve teknolojinin gelişimiyle birlikte hayatımıza girmiş ve sektördeki işlemleri daha hızlı, güvenli ve verimli hale getirmiştir. Fintek uygulamaları, bankacılık işlemleri, mobil ödemeler, dijital cüzdanlar ve yatırım işlemleri gibi birçok alanda değişim oluşturmuştur. Kamu çalışanları, bu yeni finansal teknolojileri kullanarak, finansal işlemleri daha kolay ve hızlı gerçekleştirmekte, iş süreçlerinde zamandan ve maliyetten tasarruf sağlamaktadır. Özellikle dijital bankacılık ve mobil ödemeler, geleneksel bankacılığa göre avantajlar sağlamaktadır. Bu bağlamda, Fintek uygulamalarının kamu çalışanları üzerindeki etkisini ve bu uygulamaların kamu finans sektöründe nasıl bir dönüşüm oluşturduğunu incelemek oldukça önemlidir.

Bu çalışmanın amacı, kamu çalışanlarının finans sektöründe Fintek uygulamalarının etkisini ve katkısını tespit etmektir. 05.02.2025 ile 17.02.2025 tarihleri arasında yapılan online anket, güvenlik, eğitim, sağlık ve idari hizmetler gibi çeşitli kamu sektörlerinde çalışan toplamda 429 katılımcıya uygulanmıştır. Elde edilen verilere göre, kamu çalışanları, finans sektöründeki iş ve işlemlerinde Fintek uygulamalarının önemli katkıları olduğunu belirtmişlerdir. Özellikle maaş yönetimi, yatırım yapma ve mobil ödemeler gibi alanlarda Fintek uygulamalarının büyük bir rol oynadığı gözlemlenmiştir. Kamu çalışanları, bu uygulamaların geleneksel bankacılık işlemlerine göre çok daha hızlı ve pratik olduğunu ifade etmişlerdir.

Fintek uygulamaları, özellikle zaman ve güvenilirlik aısından kamu alıřanları tarafından tercih edilmektedir. Dijital bankacılıęın ve mobil ödeme sistemlerinin sunduęu kolaylıklar sayesinde, kamu alıřanları hem zamandan tasarruf etmekte hem de işlemleri daha güvenli bir şekilde gerçekleřtirmektedirler. Bu noktada, kamu alıřanlarının Fintek tabanlı uygulamalara yönelmesi, hem finansal işlem süreçlerini hem de kamu finansmanını daha etkin bir şekilde yönetmelerini sağlayabilecektir.

Ancak, Fintek uygulamalarının etkinlięinin sürdürülebilir olabilmesi için devletin bu uygulamaları destekleyici politikalar geliřtirmesi gerekmektedir. Devletin Fintek uygulamalarını teşvik etmesi ve kamu alıřanlarına yönelik eğitimler düzenlemesi, uygulamaların daha verimli ve yaygın bir şekilde kullanılmasını sağlayacaktır. Ayrıca, Fintek uygulamalarının yaygınlařması için dijital bankacılıkla ilgili detaylı arařtırmalar yapılması önemlidir. Kamu alıřanlarının Fintek uygulamalarına yönelik daha fazla bilgi edinmesi ve bu uygulamaların devlet politikalarıyla desteklenmesi, kullanıcı sayısının artmasına ve uygulamaların daha etkili bir şekilde kullanılmasına yol açacaktır.

Bu alıřmada farklı yař grupları ve sektörlerde alıřan katılımcıların teknolojik araçları kullanma düzeylerinin Fintek uygulamaları üzerindeki etkileri de incelenmiřtir. Özellikle erken yařta memuriyete bařlamıř ve eğitim seviyeleri farklı olan grupların, Fintek uygulamalarına yaklařımları farklılık göstermektedir. Bu tür bir yaklařım, sabit bir grup yerine farklı demografik özelliklere sahip bireyler üzerinden yapılan analizlerin daha kapsamlı ve özgün bir şekilde sonuçlanmasını sağlamaktadır. Arařtırma, kamu alıřanlarının finans sektöründeki Fintek uygulamalarına katkılarını ele alma fırsatı sunmuřtur.

Sonuç olarak, Fintek tabanlı uygulamalar, finans sektöründeki işlemleri hızlandırırken, kamu alıřanlarının finansal yönetimini daha verimli hale getirmektedir. Bu tür teknolojilerin yaygınlařması ve geliřtirilmesi, finansal sektörün dijitalleřme sürecine büyük katkı sağlayacaktır. Kamu alıřanları, Fintek uygulamalarını kullanarak finansal işlemlerini daha hızlı ve güvenli bir şekilde gerçekleřtirebilecek ve bu sayede verimliliklerini artıracaklardır. Gelecekte, Fintek uygulamaları, kamu finans yönetimini ve genel finansal sistemleri dönüřtürerek sektördeki dijital dönüřümün itici gücü haline gelebilir. Bu bağlamda, gelecekte yapılacak arařtırmalarda, yazarların kamu alıřanlarının Fintek uygulamalarını daha kapsamlı şekilde incelemeleri ve demografik faktörlerin bu uygulamaların kullanımına olan etkilerini detaylı bir biçimde ele almaları tavsiye edilebilir. Ayrıca, Fintek uygulamalarının sürdürülebilirlięini sağlamak için devlet destekli eğitim programları ve politika geliřtirmeleri üzerine alıřmalar yapılması önemlidir. Bu sayede, Fintek tabanlı özümün daha geniř bir kullanıcı kitlesine ulařtırılması ve etkili bir şekilde benimsenmesi sağlanabilir.

## KAYNAKÇA

- Akyol, B., (2021). The Validity and Reliability Study of the Scale of Occupational Professionalism of School Principals. *E-International Journal of Educational Research*, 12.(4).
- Ali, H. M., Mohammed H., Hashmi, H. S. & Hassan, M. (2019). Global Landscape Of The Islamic Fintech: Opportunities, Challenges And Future Ahead. *COMSATS Journal of Islamic Finance*, 4(2).
- Arner, D. W., Barberis, J. & Buckley, R. P. (2016). 150 Years Of Fintech: An Evolutionary Analysis. *Jassa*, (3), 22-29.
- Aziza, N. A. (2024). Finansal Teknolojinin Zekât Kurumlarının Şeffaflığı Üzerindeki Etkileri, Yayınlanmamış Doktora Tezi. *Sakarya Üniversitesi Sosyal Bilimler Enstitüsü*, Sakarya.
- Buchak, G., Matvos, G., Piskorski, T. & Seru, A. (2018). Fintech, Regulatory Arbitrage, And The Rise Of Shadow Banks. *Journal of Financial Economics*, 130(3), 453-483.
- Bulazar, A. R. ve Küçükçolak, R. A. (2021). Finans Sektöründe Fintek Etkisi. Working Paper Series, 2(1), 53-63.
- Büyüköztürk, Ş. (2002). Faktör Analizi: Temel Kavramlar ve Ölçek Geliştirmede Kullanımı. *Kuram ve Uygulamada Eğitim Yönetimi*, 32(32),470-483.
- Canbaz, M. F. ve Erbaş, S. (2021). Katılım Bankacılığında Fintek Eğilimleri Ve Sektöre Katkıları. *Finans Ekonomi ve Sosyal Araştırmalar Dergisi*, 6(3), 477-489.
- Candemir, G. (2020). Bankacılık Sektöründe Yeni Trendler ve Teknolojik Gelişmeler: Fintek Sektörü Üzerine Bir Uygulama. Yayınlanmamış Doktora Tezi. *Marmara Üniversitesi Bankacılık ve Sigortacılık Enstitüsü*, İstanbul.
- Çağıl, G. ve Gozde, C. (2020), Türk Bankacılık Sektörünün Fintek'ler Karşısında A'WOT Analizi. *Maliye ve Finans Yazıları*, 113, 207-238.
- Çetin, M. (2008). Üniversite Öğrenci Harcamalarının Analizi ve Bölge Ekonomilerine Katkılarını Belirlemeye Yönelik Bir Araştırma. *Yönetim ve Ekonomi Dergisi*, 15.(2), 99-113.
- Çınar, Ş. ve Demir, Y. (2010). Toplumdaki Hemşirelik İmajı: Bir Ölçek Geliştirme Çalışması. *Anadolu Hemşirelik ve Sağlık Bilimleri Dergisi*, 12(2), 24-33.
- Dahlquist, J. & Knight, R. (2022). Principles of finance. *OpenStax*.
- Degerli, K. (2019). Regulatory Challenges And Solutions For Fintech In Turkey. *Procedia Computer Science*, 158, 929-937.
- Demirdöğen, Y. (2020). Avrupa'daki İslami fintek ekosisteminin analizi. *Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 25, 469-481.



- Demirdöęen, Y. (2020). İřlami Fintek Ekosistemi Üzerine Bir Deęerlendirme. *Gaziantep Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 2, (1)63-99.
- Erden, B. ve Topal, B. (2021). Türkiye’de ve Dünyada İřlami Fintek sektörünün geliřimi. *Ardahan Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 3(1), 69-75.
- Genç, S. ve Küçükçolak, R. A. (2020). Türkiye’de Fintek Sektörü. *Working Paper Series Dergisi*, 1(1),48-60.
- Gujarati & Damodar N. (2009). Basic Econometrics Mc Graw-Hill International Edition.
- Güven, M. ve Yařar, M. E. (2017). Toplam Kalite Yönetimi ve Teknolojinin İřletmeler İçin Önemi: Van Organize Sanayi Bölgesinde Bir Uygulama. *Bingöl Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 7, 127-142.
- Haddad, C. & Hornuf, L. (2019). The Emergence Of The Global Fintech Market: Economic And Technological Determinants. *Small Business Economics*, 53(1), 81-105.
- Karaçayır, E. ve Afřar, A. (2021). Fintek yatırımlarının belirleyicileri: AB ülkeleri ve Türkiye örneęi. *Bingöl Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 5(2), 171-190.
- Karasar, N. (2006). Bilimsel Arařtırma Yöntemleri. Nobel Yayınevi, Ankara.
- Kim, M., Choi, S. & Lee, J. (2017). Economic System And Financial Literacy: Evidence From North Korean Refugees. *Emerging Markets Finance and Trade*, 53(11), 2505-2527.
- Kömürcüoęlu, Ö. F. ve Akyazı, H. (2020). Finansal Teknolojilerdeki (Fintek) Geliřmeler: Fırsatlar ve Riskler. *Karadeniz Ekonomi Arařtırmaları Dergisi*, 1(1), 35-48.
- Magnuson, W. (2017). Ragulating fintech. What is fintech ?, Texas.
- Ozili, P.K. ( 2020). Theories Of Financial İncclusion. *Uncertainty And Challenges In Contemporary Economic Behaviour*. Emerald Publishing Limited, 89-115.
- Rabbani, M. R., Khan, S. & Thalassinos, E. I. (2020). Fintech, Blockchain And Islamic Finance: An Extensive Literature Review.
- Raj, V. (2020). How Aıl & Machine Learning İř İncfiltrating The Fintech İncdustry. *Online: <https://www.fintechnews.org/how-ai-machinelearning-is-incfiltrating-the-fintech-industry>*.
- Sezal, L. (2020). Fintek Hizmetlerinin Finans Sektörüne Etkileri ve Saęlanan Devlet Teřvikleri. *Ekonomi İřletme ve Maliye Arařtırmaları Dergisi*, 2(3), 233-248.
- Tabachnick, B. G. & Fidell, L. S. (2012). Using multivariate statistics, 6. Baskı, Boston: Pearson.

- Temelkov, Z. (2018). Fintech Firmaları Bankalar İçin Fırsat mı Tehdit mi?, *Uluslararası Bilgi, İşletme ve Yönetim Dergisi*, 10, 138-144.
- Usta, M. E. (2013). Yurtdışına Gitmiş Eğitimcilerin Küreselleşmeye İlişkin Görüşleri. *Van Yüzüncü Yıl Üniversitesi Eğitim Fakültesi Dergisi*, 10(1), 227-247.
- Wooldridge, J. M. (2016), Should Instrumental Variables Be Used As Matching Variables. *Research In Economics*, 70(2), 232-237.

# BÖLÜM 2

## BANKACILIKTA SİBER GÜVENLİK VE RİSK YÖNETİMİ

*İdris ADIGÜZEL<sup>1</sup>*

---

<sup>1</sup> Dr, idris-1987@hotmail.com, ORCID: 0000-0002-6737-4387

## 1. GİRİŞ

Günümüzde siber saldırılar, özellikle bankacılık sektörü için büyük bir tehdit oluşturmaktadır. Bankacılık sistemleri, ülke ekonomisinin temelini oluşturan kritik altyapılar arasında yer alır ve bu sistemlerde yaşanacak bir aksaklık, tüm ekonomiyi olumsuz etkilemektedir. Bu tür kesintiler, ciddi mali kayıplara, operasyonel aksaklıklara ve müşteri güveninin sarsılmasına neden olabilir. Bankacılık sektörü, siber saldırıların yol açabileceği riskleri bünyesinde barındırmakta ve bu risklerin etkili bir şekilde yönetilmesi büyük önem taşımaktadır. Bu nedenle, bankaların siber güvenlik önlemlerini sürekli olarak güncellemesi, proaktif bir yaklaşım benimsemesi ve güvenlik stratejilerini geliştirmesi gerekmektedir.

Bankacılık sektöründe siber güvenlik, finans kuruluşlarını siber tehditlere karşı korumak, hassas verilerin güvenliğini sağlamak, operasyonel sürekliliği desteklemek ve müşteri güvenini korumak amacıyla tasarlanmış uygulamalar, teknolojiler ve süreçler bütünüdür. Bu kapsamda, siber saldırılar, veri ihlalleri, dolandırıcılık ve yetkisiz erişim gibi riskleri en aza indirmek için çeşitli güvenlik önlemleri uygulanmaktadır. Siber güvenlik, bankacılık sistemlerinin ve müşteri bilgilerinin bütünlüğünü, gizliliğini ve erişilebilirliğini korumak için hayati bir rol oynamaktadır. Özellikle yapay zeka destekli tehdit tespiti, çok faktörlü kimlik doğrulama, şifreleme ve gerçek zamanlı izleme gibi teknolojiler, bankaların siber tehditlere karşı daha dirençli olmasını sağlamaktadır. Ayrıca, bankaların siber güvenlik konusunda çalışanlarını ve müşterilerini bilinçlendirmesi büyük önem taşımaktadır. Düzenli eğitimler ve farkındalık programları, çalışanların ve müşterilerin siber tehditlere karşı daha bilinçli olmasını sağlamaktadır. Bu tür eğitimler, kimlik avı saldırıları, kötü amaçlı yazılımlar ve diğer siber tehditler konusunda farkındalık yaratarak, olası saldırıların önlenmesine yardımcı olur. Sonuç olarak, bankacılık sektöründe siber güvenlik hem kurumların hem de müşterilerin güvenliğini sağlamak için vazgeçilmez bir unsurdur ve bu alanda yapılan yatırımlar, bankaların gelecekteki tehditlere karşı daha hazırlıklı olmasını sağlayacaktır.

## 2. BANKACILIK SEKTÖRÜNDE SİBER GÜVENLİK

Bankalar, siber tehditler karşısında en savunmasız kurumlar arasında yer almaktadır. Her gün büyük miktarda hassas veri işlemleri ve finansal işlemler gerçekleştirmeleri, onları siber suçlular için oldukça cazip bir hedef haline getirmektedir. Siber güvenlik, bankaların operasyonel süreçlerini koruyarak müşterilerinin gizliliğini ve güvenini de sağlamaktadır. Bankaların güçlü siber güvenlik önlemlerine ihtiyaç duymasının temel nedenleri arasında, veri ihlallerini önleme, finansal dolandırıcılıkları engelleme, müşteri bilgilerini koruma ve yasal düzenlemelere uyum sağlama

gibi faktörler bulunur. Bu önlemler, bankaların itibarını korumak ve siber saldırıların yol açabileceęi mali kayıpları en aza indirmek için kritik öneme sahiptir.

### **2.1. Müşteri Bilgilerinin Gizlilięinin Sağlanması**

Müşteri verileri, bankacılık faaliyetlerinin temelini oluşturmaktadır. Sosyal Güvenlik numaraları, adresler ve finansal bilgiler gibi kişisel veriler, bankaların elinde büyük bir deęer taşımaktadır. Bu bilgilerin ele geçirilmesi, kimlik hırsızlığı, dolandırıcılık ve bireyler için ciddi mali kayıplara yol açabilir. Bu nedenle, siber güvenlik, müşteri verilerini yetkisiz erişimden korumak için hayati bir rol oynar. Bankalar, bu verileri korumak için şifreleme, güvenlik duvarları, güvenli erişim kontrolleri gibi çeşitli önlemler almaktadır. Bu tür güvenlik önlemleri uygulanmadığında, bankalar finansal kayıplar, müşteri güveninin sarsılması ve itibar zedelenmesi gibi ciddi sonuçlarla karşı karşıya kalabilmektedir.

### **2.2. Müşteri Memnuniyeti ve İtibarın Korunması**

Güven, bankacılık ilişkilerinin temelini oluşturan en önemli unsurdur. Müşteriler, finansal kuruluşlarının kişisel ve mali bilgilerini güvenli bir şekilde koruyacağına inanır. Herhangi bir veri ihlali veya siber saldırı, bu güveni zedeleyerek müşteri kaybına ve uzun vadeli itibar zararına neden olabilmektedir. Siber saldırılar, medyada hızla yer bulabilir ve bir bankanın imajını kısa sürede olumsuz etkileyebilir. Bu nedenle, güçlü siber güvenlik önlemleri, müşterilerin bankalarına olan güvenini korumak ve onların hassas bilgilerini paylaşırken kendilerini güvende hissetmelerini sağlamak için büyük önem taşımaktadır. Bu önlemler, bankaların itibarını korumanın yanı sıra müşteri bağlılığını da artırır.

### **2.3. Yasal Düzenlemelere Uyum Sağlama**

Bankalar, finans sektöründe katı veri koruma ve siber güvenlik uyumluluk standartlarına uymak zorundadır. Avrupa'daki Genel Veri Koruma Yönetmelięi (GDPR) ve ABD'deki Kaliforniya Tüketici Gizlilik Yasası (CCPA) gibi yasal düzenlemeler, bankaların müşteri verilerini nasıl yönetmesi ve koruması gerektięi konusunda kesin kurallar belirler. Bu yönetmeliklere uyulmaması durumunda, ağır para cezaları, yasal yaptırımlar ve hatta işletme lisanslarının iptali gibi ciddi sonuçlar ortaya çıkabilir. Bankalar, güçlü siber güvenlik önlemleri olarak hem siber tehditlere karşı korunur hem de bu önemli düzenleyici gereklilikleri yerine getirmiş olurlar.

## 2.4. Mali Zararların Engellenmesi

Başarılı bir siber saldırı, bankalar için ciddi mali kayıplara neden olabilir. Bu kayıplar, hesaplardan çalınan paralar, sistem kesintilerinden kaynaklanan maliyetler veya zarar gören altyapıyı onarma masrafları gibi çeşitli şekillerde ortaya çıkabilmektedir. Bankalar, siber ihlal sonucu dolandırıcılık veya kimlik hırsızlığına uğrayan müşterilere tazminat ödemek zorunda kalabilir. Bankalar, gelişmiş siber güvenlik çözümlerine yatırım yaparak bu tür finansal riskleri azaltabilir. Gerçek zamanlı tehdit izleme, çok faktörlü kimlik doğrulama ve yapay zeka destekli tehdit tespiti gibi proaktif önlemler, saldırıların yol açabileceği maliyetli sonuçları engellemede etkili bir rol oynamaktadır.

## 2.5. Temel Sistem ve Altyapının Güvenliği

Çevrimiçi bankacılık platformları, ATM'ler ve ödeme işlem sistemleri gibi bankacılık altyapısı, siber suçlular için öncelikli hedefler arasında yer almaktadır. Bu sistemlere yönelik başarılı bir saldırı, operasyonel aksaklıklara neden olarak müşterilerin hesaplarına erişememesi veya işlem yapamaması gibi ciddi sorunlara yol açabilmektedir. Siber güvenlik önlemleri, bankaların yetkisiz erişimleri engellemesine, anormal aktiviteleri tespit etmesine ve potansiyel tehditleri minimize etmesine yardımcı olmaktadır. Sürekli izleme ve düzenli güvenlik testleri, bu kritik hizmetlerin güvenli ve kesintisiz bir şekilde çalışmasını sağlayarak, bankaların itibarını ve finansal istikrarını korumaktadır.

## 2.6. Kesintisiz İş Operasyonlarının Garanti Altına Alınması

Siber saldırılar, bir bankanın operasyonlarında ciddi aksaklıklara neden olabilir. Bankaların sistem kesintileri, veri kayıpları ve hatta hizmetlerin tamamen durması gibi sonuçlar doğurabilir. Bu tür kesintiler hem finansal kayıplara yol açabilir hem de müşteri deneyimini olumsuz etkileyebilir. Kapsamlı siber güvenlik önlemleri almak, bankaların bu tür operasyonel aksaklıklara karşı korunmasına yardımcı olur. Güçlü bir olay müdahale planına sahip olmak, düzenli veri yedeklemeleri yapmak ve felaket kurtarma çözümlerini kullanmak, bankaların bir saldırı sonrası hızla toparlanmasını ve müşterilerine kesintisiz hizmet sunmaya devam etmesini sağlamaktadır.

## 3. BANKACILIK SEKTÖRÜNDE SİBER GÜVENLİK TEHDİTLERİ

Siber güvenlik olaylarının önemli bir kısmı, çalışanların dikkatsiz davranışları veya siber güvenlik politikaları ve prosedürleri hakkında ye-

terli bilgiye sahip olmamaları nedeniyle ortaya çıkmaktadır. Özellikle, fiziksel varlıkların, veri depolama cihazlarının ve herkese açık internet bağlantılarının güvenlięi konusunda çalışanların yeterince bilinçli olmaması, siber saldırılar için zemin hazırlayabilmektedir. Bu nedenle, çalışanların siber tehditlerin farkında olması ve bu tehditlere karşı nasıl önlem alınacağı konusunda eğitilmesi büyük önem taşımaktadır.

Kurumlar, siber güvenlik politikalarını net bir şekilde belirlemeli ve bu politikaların tüm çalışanlar tarafından anlaşılmasını sağlamalıdır. Ayrıca, güvenlik protokollerinin sürekli güncellenmesi ve çalışanların bu konuda bilgilendirilmesi, siber saldırıların önlenmesinde etkili bir strateji olabilir. Sonuç olarak, çalışanların siber güvenlik konusunda bilinçlendirilmesi ve eğitilmesi, kurumların siber tehditlere karşı daha dirençli hale gelmesini sağlayacaktır. Bu adımlar hem veri güvenliğini koruyacak hem de kurumların itibarını güçlendirecektir (Hansce, 2001).

Bankacılık sektörü, siber suçluların sürekli olarak zafiyetleri istismar etmek için yeni yöntemler geliřtirmesi nedeniyle sürekli ve karmaşık siber tehditlerle mücadele etmek zorundadır. Büyük miktarda hassas finansal veri ve müşteri bilgisi barındıran bankalar, siber saldırganlar için öncelikli hedefler arasında yer alır. Bu nedenle, finansal kuruluşların siber güvenlik önlemlerini sürekli güncellemesi ve proaktif bir yaklaşım benimsemesi büyük önem taşımaktadır. Aşağıda, bankacılık sektörünün karşı karşıya olduęu en yaygın siber güvenlik tehditleri detaylı bir şekilde ele alınmaktadır.

### 3.1. Kimlik Avı Saldırıları

Kimlik hırsızlığı, bir kişinin vatandaşlık numarası, sosyal güvenlik numarası, doğum tarihi, anne veya baba adı gibi kişisel bilgilerine izinsiz erişilerek, bu bilgilerin mal veya hizmet satın almak gibi ekonomik çıkar sağlamak amacıyla kullanılmasıdır (Berg, 2009a, s. 91).

Kimlik avı, bankacılık sektöründe en sık karşılaşılan siber tehditlerden biri olarak öne çıkmaktadır. Siber suçlular, müşterileri veya çalışanları, hesap bilgileri, şifreler veya kişisel veriler gibi hassas bilgilerini paylaşmaya ikna etmek için sahte e-postalar, SMS mesajları veya gerçek gibi görünen web siteleri kullanır. Bu bilgilere erişim sağladıklarında, para çalma, kimlik hırsızlığı yapma veya bankanın iç sistemlerine sızma gibi eylemler gerçekleştirebilmektedirler. Kimlik avı saldırıları, özellikle finans sektörünü hedef alan dolandırıcılıkların başında gelir ve bankacılık sektörü için büyük bir tehdit oluşturmaktadır. Yaygın kimlik avı taktiklerinden biri aciliet veya panik duygusu yaratmaktır. Saldırganlar, bir alıcının hesabının şüpheli bir etkinlikle karşılaştığını veya bilgilerinin hemen güncellenmesi gerektiğini belirtir. Amaç, kullanıcıların eleştirel düşünmeden hareket etmesini sağlamaktır.

### 3.2. Kötü Amaçlı Yazılım

Kötü amaçlı yazılımlar veya zararlı yazılımlar, özellikle bankacılık sektöründe hesap numaraları, şifreler ve diğer hassas finansal bilgileri ele geçirmeyi hedefleyen ciddi bir siber tehdit oluşturmaktadır. Bu yazılımlar, finansal işlemleri manipüle etmek veya verilere yetkisiz erişim sağlamak amacıyla kullanılır. Güvenlik önlemlerini atlatma ve cihazları etkileme konusunda oldukça yetenekli olan kötü amaçlı yazılımlar, bankalar için büyük bir risk kaynağıdır. Bu tür yazılımlar, genellikle e-posta ekleri, sahte web siteleri veya güvenli olmayan indirmeler gibi çeşitli yollarla yayılmaktadır. Bankalar, bu tehditlere karşı korunmak için güçlü antivirüs programları, düzenli sistem güncellemeleri ve çalışanların siber güvenlik farkındalığını artıracak eğitimler gibi önlemler almalıdır. Ayrıca, çok faktörlü kimlik doğrulama ve şifreleme gibi teknolojiler, hassas verilerin korunmasına yardımcı olabilmektedir. Bu adımlar, kötü amaçlı yazılımların neden olabileceği zararları en aza indirmek için kritik öneme sahiptir.

### 3.3. Truva Atları ve Tuş Kaydediciler

Truva atı, bir tür zararlı yazılım olarak kullanıcıların bilgisayarlarına bulaştıktan sonra fark edilmeden faaliyet gösterebilir. Bu yazılım, veri sızdırma, tuş kaydetme ve ağ trafiğini izleme gibi gizli işlemler gerçekleştirebilmekte. Genellikle kullanışlı gibi görünen programların içine gizlenerek yüklendiği için, kullanıcılar tarafından varlığı uzun süre fark edilmemektedir. Günümüzde oldukça yaygın olan Truva atları, tüm bilgisayar kötü amaçlı yazılımlarının yaklaşık %58'ini oluşturarak siber güvenlik açısından büyük bir tehdit oluşturmaktadır. Bu tür yazılımlar, kullanıcıların farkında olmadan sistemlerine zarar verebilir ve hassas bilgileri riske atabilir (Özkaya, 2019).

Truva atı, kullanıcı tarafından kurulum gerektiren ve genellikle yararlı, yasal bir uygulama gibi görünen ancak arka planda kötü amaçlı faaliyetler gerçekleştiren bir zararlı yazılım türüdür. Bu tür yazılımlar, kullanıcıların dikkatini çekmek için hediye, indirim veya benzeri vaatler sunarak kurulum yapmalarını sağlamaya çalışır. Kullanıcılar, bu tuzaklara düşerek farkında olmadan zararlı yazılımı sistemlerine yükleyebilir. Truva atları, bu şekilde kurulduktan sonra gizlice kötü niyetli işlemler yapmaya başlar ve kullanıcıların güvenliğini tehlikeye atar. Bu nedenle, kullanıcıların indirdikleri uygulamalara karşı dikkatli olmaları ve güvenilir kaynaklardan yazılım temin etmeleri büyük önem taşımaktadır (Jackson, 2018).

Bankacılık trojanları, sisteme bulaştıktan sonra hızla finansal verileri toplamaya başlar. Genellikle, kullanıcı adları, şifreler ve tek kullanımlık kodlar gibi tüm bilgileri kaydeden tuş kaydı (keylogging) tekniğini kullanır. Bu şekilde, kullanıcıların girdiği tüm verileri ele geçirir ve siber



suçluların hesaplara yetkisiz erişim sağlamasına olanak tanır. Bu nedenle, kullanıcıların çevrimiçi bankacılık işlemleri sırasında dikkatli olmaları ve güvenlik önlemlerini artırmaları büyük önem taşır.

Tuş kaydedici (keylogger), kullanıcının klavyede yaptığı her türlü tuş vuruşunu izleyen ve bu bilgileri kaydeden bir kötü amaçlı yazılım türüdür. Bu yazılım, kullanıcı adları, şifreler, sosyal güvenlik numaraları, kimlik numaraları, banka hesap bilgileri gibi kişisel ve hassas verileri toplamaktadır. Toplanan bu bilgiler, siber suçlular tarafından yetkisiz erişim veya dolandırıcılık amacıyla kullanılır. Tuş kaydediciler, genellikle kullanıcıların farkında olmadan sistemlerine bulaşır ve uzun süre fark edilmeden faaliyet gösterebilir. Bu nedenle, kullanıcıların güvenlik yazılımlarını güncel tutmaları ve şüpheli aktivitelere karşı dikkatli olmaları büyük önem taşımaktadır (Marrion ve Twede, 2020, s. 252; Kaspersky, 2021a).

### 3.4. Fidyeye Yazılımı

Fidyeye yazılımı, kullanıcının bilgisayarını veya belirli dosyalarını erişime kapatarak, erişimi geri vermek için fidye talep eden bir kötü amaçlı yazılım türüdür. Bu yazılım, kullanıcıları fidye ödenmediği takdirde sistemlerine zarar vermek, verileri silmek veya özel belgeleri kamuya açmakla tehdit eder. Fidyeye yazılımcıları, genellikle kullanıcıların paniklemesini ve taleplerini yerine getirmesini hedefler. Bu tür saldırılar hem bireysel kullanıcılar hem de kurumlar için ciddi bir tehdit oluşturur. Bu nedenle, düzenli yedekleme yapmak ve güvenlik önlemlerini artırmak, fidye yazılımı saldırılarına karşı korunmak için kritik öneme sahiptir (Kharraz, 2018; Marion & Twede, 2020).

Bankacılık sektöründe, fidye yazılımı saldırıları özellikle tehlikelidir çünkü finansal işlemleri sektöre uğratar ve gizli finansal bilgileri riske atar. Bu tür yazılımlar, müşteri bilgileri, finansal kayıtlar ve işlem detayları gibi kritik verileri şifreleyerek erişilemez hale getirir. Bu durum, bankaların kendi verilerine ulaşmasını engeller ve iş sürekliliğini ciddi şekilde tehdit etmektedir. Kilitlenen veriler nedeniyle, işlemleri işleme, müşteri hesaplarına erişim ve hatta iç iletişim gibi temel operasyonlar durma noktasına gelebilir. Bu tür saldırılar, bankaların itibarını zedeleyebilir ve büyük mali kayıplara yol açabilir. Bu nedenle, bankalar genellikle faaliyetlerini hızla eski haline getirmek için fidye ödemeye zorlanır. Ancak, fidye ödemek her zaman bir çözüm değildir ve saldırganların taleplerini yerine getirmek, gelecekteki saldırıları teşvik edebilir. Bu nedenle, bankaların fidye yazılımı saldırılarına karşı proaktif önlemler alması, düzenli yedekleme yapması ve güvenlik altyapısını sürekli güncellemesi büyük önem taşır.

### 3.5. Üçüncü Taraf Riski

Üçüncü taraf entegrasyonları, bankacılık kuruluşlarına verimlilik ve iş süreçlerinde kolaylık sağlarken, beraberinde önemli siber güvenlik risklerini de getirmektedir. Bir bankanın entegre olduğu her üçüncü taraf sistem, siber saldırganlar için potansiyel bir giriş noktası haline gelebilir. Bu sistemlerdeki güvenlik açıkları, finansal kuruluşların ağlarına veya hassas verilerine yetkisiz erişim sağlanmasına yol açabilmektedir. Özellikle, üçüncü tarafların güvenlik standartlarının yetersiz olması, bankaların siber saldırılara karşı savunmasız kalmasına neden olabilmektedir. Bu nedenle, bankaların üçüncü taraf entegrasyonlarında sıkı güvenlik protokolleri uygulaması, düzenli denetimler yapması ve tedarikçilerin güvenlik önlemlerini sürekli izlemesi büyük önem taşımaktadır. Ayrıca, veri şifreleme, erişim kontrolleri ve siber güvenlik eğitimleri gibi önlemlerle riskler en aza indirilebilir.

### 3.6. Yapay Zeka ile İlgili Siber Tehditler

Yapay zeka (AI), bankacılık sektöründe dolandırıcılık tespiti, risk yönetimi ve müşteri hizmetleri gibi alanlarda önemli ilerlemeler kaydetmektedir. Ancak, bu teknolojilerin getirdiği yeniliklerle birlikte yeni güvenlik riskleri de ortaya çıkmaktadır. Özellikle, AI'nin deepfake olarak bilinen gerçekçi sahte videolar veya ses kayıtları oluşturma yeteneği, siber saldırganlar için etkili bir araç haline gelmiştir. Bu tür sentetik medya, sosyal mühendislik saldırılarında kullanılarak, banka çalışanları gibi davranıp kişisel ve finansal bilgilerin ele geçirilmesine neden olabilmektedir. Bireysel kullanıcılar ve kurumlar için ciddi bir tehdit oluşturmaktadır. Bu nedenle, AI'nin sunduğu fırsatların yanı sıra, bu teknolojinin yol açabileceği risklere karşı da önlem almak büyük önem taşımaktadır. Bankalar, AI tabanlı çözümlerin güvenliğini artırmak ve olası tehditlere karşı hazırlıklı olmak için sürekli çalışmalıdır.

### 3.7. Uzaktan Çalışan İşgücü

Uzaktan çalışma modeli, bankacılık sektörü de dahil olmak üzere birçok alanda yaygın bir şekilde benimsenmiştir. Dijitalleşmenin hızlanmasıyla birlikte, bu çalışma şekli hem esneklik sunmakta hem de operasyonel maliyetleri azaltmaktadır. Ancak, uzaktan çalışanların kritik veya hassas verilere erişmesi, veri güvenliği ihlalleriyle ilişkili ek riskleri de beraberinde getirmektedir. Bu riskler, güvenli olmayan ağ bağlantıları, yetersiz uç cihaz güvenliği ve fiziksel güvenlik açıkları gibi çeşitli siber tehditlere yol açabilmektedir. Özellikle, ev ağlarının güvenlik standartlarının düşük olması veya kişisel cihazların kullanılması, siber saldırganlar için kolay hedefler oluşturabilmektedir. Bu nedenle, bankaların uzaktan çalışma sü-

reçlerinde güçlü güvenlik protokolleri uygulaması, çalışanların bilinçlendirilmesi ve güvenli iletişim kanallarının kullanılması büyük önem taşımaktadır.

### 3.8. Dağıtılmış Hizmet Reddi

Dağıtık hizmet engelleme (DDoS) saldırıları, bir hizmet engelleme saldırısının aynı anda birden fazla kaynaktan ve farklı ağlar üzerinden gerçekleştirilmesidir. Bu tür saldırılar, hedef sistemin kaynaklarını aşırı yükleyerek hizmetlerin kullanılamaz hale gelmesine neden olmaktadır (Lepkowski, 2009). Saldırganlar, genellikle botnet adı verilen ve birbirine bağlı birçok cihazdan oluşan ağları kullanarak, hedefe yoğun bir trafik yükü gönderir. Bu, sistemin kapasitesini aşarak hizmetlerin durmasına veya yavaşlamasına yol açmaktadır. DDoS saldırıları, özellikle bankacılık ve finans sektörü gibi kesintisiz hizmet gerektiren alanlarda ciddi sorunlara neden olabilmektedir. Bu nedenle, kurumların bu tür saldırılara karşı etkili savunma mekanizmaları geliřtirmesi büyük önem taşımaktadır (Mirkovic, 2018, s. 250)

Bir web sitesi, e-posta sunucusu veya benzer bir hedef, maruz kaldığı internet trafięi arttıkça çalışamaz duruma gelmektedir. Dağıtık hizmet engelleme (DDoS) saldırıları, çeşitli yöntemlerle gerçekleştirilebilir. Bu saldırılar, hedef sistemin aşırı yüklenmesine, ağdaki zayıf noktaların istismar edilmesine veya hedefin veritabanlarının yoğun isteklerle boęulmasına neden olabilir. Tüm bu yöntemlerin ortak amacı, hedef siteyi veya hizmeti çevrimdışı hale getirmektir. Bu tür saldırılar, özellikle bankacılık ve finans sektörü gibi kesintisiz hizmet gerektiren alanlarda ciddi sorunlara yol açabilir. Bu nedenle, kurumların DDoS saldırılarına karşı etkili savunma stratejileri geliřtirmesi büyük önem taşımaktadır (Marrion ve Twede, 2020).

### 3.9. Veri İhlalleri

Veri ihlalleri, bankaların cihazlarında şifrelenmemiş halde depolanan bilgiler nedeniyle büyük bir tehdit oluşturmaktadır. Eğer veriler şifrelenmemişse, siber saldırganlar bir ihlal durumunda bu bilgilere kolayca erişebilir ve bunları kurumların aleyhine kullanabilir. Bu durum hem bankaların itibarını zedeleyebilir hem de müşterilerin güvenini sarsabilir. Veri şifreleme, hassas bilgilerin yetkisiz erişime karşı korunmasını sağlayarak, ihlal durumlarında bile verilerin okunamaz hale gelmesini garanti etmektedir. Bu nedenle, bankaların veri güvenliğini artırmak için şifreleme teknolojilerini etkin bir şekilde kullanması büyük önem taşımaktadır. Şifreleme, siber tehditlere karşı güçlü bir savunma mekanizması sunmaktadır.

## 4. BANKACILIKTA SİBER GÜVENLİK ÇÖZÜMLERİ

Gelişmiş siber güvenlik çözümleri, bankaların güçlü ve etkili bir güvenlik altyapısı oluşturmalarına önemli ölçüde katkı sağlamaktadır. Bu çözümler, siber tehditlere karşı proaktif bir savunma mekanizması sunarak, bankaların veri güvenliğini artırır ve olası riskleri en aza indirmektedir. Özellikle yapay zeka destekli tehdit tespiti, çok faktörlü kimlik doğrulama, gerçek zamanlı izleme ve şifreleme gibi teknolojiler, bankaların siber saldırılara karşı daha dirençli olmasını sağlar. Bu tür çözümler siber saldırıları önleyerek ihlal durumlarında hızlı müdahale imkanı sunmaktadır.

Ayrıca, gelişmiş siber güvenlik önlemleri, yasal düzenlemelere uyum sağlamak ve müşteri güvenini korumak için de kritik bir rol oynar. Güçlü güvenlik politikaları ve teknolojiler, bankaların operasyonel sürekliliğini sağlayarak banka itibarını güçlendirmektedir. Bu nedenle, bankaların bu tür çözümlere yatırım yapması ve siber güvenlik stratejilerini sürekli güncellemesi büyük önem taşımaktadır. Siber güvenlik çözümleri, bankaların hem finansal kayıpları önlemesini hem de müşterilerine güvenli bir hizmet sunmasını sağlamaktadır.

### 4.1. Çok Faktörlü Kimlik Doğrulama (MFA)

Geleneksel şifrelerin ötesine geçerek kullanıcıların kimliklerini birden fazla yöntemle doğrulamasını sağlayan bir güvenlik mekanizmasıdır. Bu sistem, biyometrik veriler (parmak izi, yüz tanıma gibi) veya tek kullanımlık şifreler gibi ek doğrulama adımları içermektedir. MFA, şifre kullanımına kıyasla çok daha güçlü bir koruma sağlar ve yetkisiz erişim riskini büyük ölçüde azaltır. Özellikle bankacılık ve finans sektöründe, hassas verilerin korunması için kritik bir rol oynamaktadır. MFA, siber saldırganların hesaplara erişimini zorlaştırarak, kullanıcı hesaplarının güvenliğini artırır ve veri ihlallerini önlemeye yardımcı olmaktadır. Bu yöntem bireysel kullanıcılar ve kurumlar için güvenilir bir çözüm sunmaktadır.

### 4.2. Uçtan Uca Şifreleme

Veri şifreleme, siber saldırganlar hassas bilgilere erişim sağlasa bile bu verileri okuma veya kullanma imkanı bulamayacakları bir koruma sağlar. Veri şifreleme özellikle bankacılık sektöründe depolanan (hareketsiz) ve iletilen (hareket halindeki) verilerin güvenliğini sağlamak için kritik bir rol oynamaktadır. Bankalar, güçlü şifreleme algoritmaları kullanarak müşteri bilgileri, finansal işlemler ve diğer kritik verileri korumalıdır. Bu, veri ihlali durumlarında bile bilgilerin yetkisiz kişiler tarafından kullanılmasını engellemektedir. Şifreleme teknolojileri, yasal düzenlemelere uyum sağlamak ve müşteri güvenini artırmak için de önemli bir araçtır. Bu neden-

le, bankaların gncel ve etkili Őifreleme yntemlerini benimsemesi byk nem tařımadır.

### 4.3. AI Destekli Tehdit Algılama

Yapay zeka (AI), byk veri kmelerini analiz ederek anormal davranıř kalıplarını tespit etme ve bu tehditlere anında mdahale etme yeteneęi sayesinde siber gvenlik alanında nemli bir rol oynar. zellikle kimlik avı, dolandırıcılık ve dięer siber saldırıların nlenmesinde etkili bir ara olarak kullanılır. AI, Őpheli aktiviteleri gerek zamanlı olarak izleyerek, geleneksel yntemlerle fark edilmesi zor olan tehditleri hızlı bir Őekilde belirleyebilir. Bu, bankalar ve finans kuruluřları iin hem gvenlięi artırır hem de mřteri bilgilerinin korunmasını saęlamaktadır. AI'nin bu yetenekleri, siber suluların yntemlerini nceden tahmin edip engellemeye yardımcı olarak, kurumların gvenlik stratejilerini glendirmektedir.

### 4.4. Sıfır Gven Mimarisi

Sıfır gven modeli, tm kullanıcıların, cihazların ve aęların varsayılan olarak gvenilir olmadığı prensibine dayanmaktadır. Bankalar, bu modeli benimseyerek her eriřim talebini ayrıntılı bir Őekilde doęrulayabilir ve yetkisiz eriřim ile veri ihlali risklerini en aza indirebilmektedir. Bu yaklařımın başarılı bir Őekilde uygulanabilmesi iin, saęlam bir aę gvenlik altyapısına ihtiya duyulur. Sistemdeki her eriřim noktasının ve baęlantının gvenlięinin saęlanması, bu modelin temel gerekliliklerinden biridir. Srekli izleme ve eriřim kontrolleri, sıfır gven modelinin etkinlięini artırarak kurumların siber gvenlik seviyesini ykseltir. Bu sayede, bankalar hem i hem de dıř tehditlere karřı daha direnli hale gelmektedir.

### 4.5. Gvenlik Olayı ve Olay Ynetimi (SIEM) Sistemleri

Gvenlik Olayı ve Olay Ynetimi (SIEM) Sistemleri, eřitli kaynaklardan gelen gvenlik verilerini toplayarak analiz eder ve potansiyel tehditler hakkında anında uyarılar sunmaktadır. Bu sistemler, siber saldırıların erken tespit edilmesini saęlayarak, kurumların hızlı ve etkili bir Őekilde mdahale etmesine olanak tanır. Bylece, siber tehditlerin neden olabileceęi zararlar en aza indirilir. SIEM sistemleri, gvenlik ekiplerinin Őpheli aktiviteleri gerek zamanlı olarak izlemesine ve gerekli nlemleri almasına yardımcı olmaktadır. SIEM sistemleri, zellikle bankacılık sektr gibi yksek riskli alanlarda, veri gvenlięini artırmak ve olası ihlalleri nlemek iin kritik bir aratır.

#### 4.6. Mevzuata Uygunluk

Tüketicileri korumak ve bankacılık sistemindeki güvenlik açıklarını en aza indirmek amacıyla bir düzenleme sistemi oluşturulmuştur. Finansal kuruluşlar, yasalara uygun ve güvenli bir şekilde faaliyet gösterebilmek için bu önemli gerekliliklerin bilincinde olmalıdır. Siber güvenlik düzenlemelerine ve standartlarına uymak, sadece cezalardan kaçınmak anlamına gelmez; aynı zamanda bir bankanın müşteri verilerini koruma ve güvenli bir ortam sunma konusundaki taahhüdünü de göstermektedir. Güçlü siber güvenlik uygulamaları müşteriler ve düzenleyici kurumlar nezdinde güven inşa ederek daha güvenli ve istikrarlı bir finansal sistemin oluşmasına katkıda bulunmaktadır.

#### 4.7. Devlet düzenlemeleri

Küresel olarak, hükümetler bankaların belirli siber güvenlik uygulamalarını benimsemesini zorunlu kılan yasalar çıkararak harekete geçmektedir. Bu düzenlemeler, korunması gereken verilerin türünü, ihlal durumlarında izlenecek prosedürleri ve kişisel olarak tanımlanabilir bilgilerin gizliliğinin nasıl sağlanacağını belirlemektedir. Bu tür yasalar, bankaların veri güvenliği konusunda daha titiz ve proaktif olmalarını sağlamaktadır. Ayrıca, müşteri bilgilerinin korunması ve siber tehditlere karşı etkili bir savunma oluşturulması için gerekli standartları ortaya koyar. Bu düzenlemelere uyum, bankaların hem yasal gereklilikleri yerine getirmesini hem de müşteri güvenliğini korumasını sağlamaktadır.

### 5. BANKACILIKTA SİBER GÜVENLİK FARKINDALIĞI VE EĞİTİM

Bankalar, siber tehditlere karşı etkili bir savunma oluşturmak amacıyla çalışanlarının ve müşterilerinin siber güvenlik konusunda bilinçlendirilmesine büyük önem vermelidir. Düzenli olarak düzenlenen eğitimler, çalışanların kimlik avı saldırıları, kötü amaçlı yazılımlar, fidye yazılımları ve diğer siber tehditleri tanımasını ve bu tehditlere karşı nasıl önlem alınacağını öğrenmesini sağlar. Ayrıca, müşterilerin güvenli şifre oluşturma, iki faktörlü kimlik doğrulama, şüpheli e-postalara karşı dikkatli olma ve kişisel bilgilerini koruma gibi konularda bilgilendirilmesi, veri güvenliğini artırır.

Siber güvenlik farkındalığı, bankaların hem iç hem de dış tehditlere karşı daha hazırlıklı olmasını sağlamaktadır. Çalışanların ve müşterilerin siber güvenlik konusunda bilinçli olması, olası saldırıların önlenmesine ve veri ihlallerinin en aza indirilmesine yardımcı olur. Bu tür eğitim ve farkındalık programları, bankaların yasal düzenlemelere uyum sağlamasını

ve müşteri güvenini korumasını kolaylaştırır. Ayrıca, siber güvenlik kültürünün kurum içinde yaygınlaştırılması, bankaların itibarını güçlendirir ve operasyonel süreklilięi desteklemektedir. Bu nedenle, siber güvenlik eğitimleri ve farkındalık çalışmalarını, bankacılık sektöründe vazgeçilmez bir unsurdur.

### 5.1. Düzenli Çalışan Eğitimi

Çalışanlar, siber tehditlere karşı ilk savunma hattını oluşturur ve bu nedenle düzenli eğitim büyük önem taşımaktadır. Personelin, kimlik avı girişimlerini tanıma, şüpheli aktiviteleri raporlama ve güvenlik protokollerine uyma konularında bilinçlendirilmesi gerekir. Siber suçla mücadele, bankalarda çalışanların bu tür tehditleri erken aşamada fark edip önlemeyle başlar. Düzenli eğitimler, çalışanların sahte e-postaları, kötü amaçlı yazılımları ve diğer siber tehditleri tespit etme becerilerini geliştirerek olası zararların önlenmesine yardımcı olmaktadır.

Eğitimler sayesinde çalışanlar güçlü şifreler kullanma, verileri güvenli bir şekilde yönetme ve şüpheli durumları zamanında bildirme konusunda daha bilinçli hale gelir. Bu, kurum içinde güvenlik odaklı bir kültür oluşturur. Çalışanların en yeni siber tehditler hakkında bilgilendirilmesi, insan kaynaklı hataları azaltır ve müşteri bilgilerinin korunmasını sağlar. Dolayısıyla, çalışan farkındalığına yapılan yatırım, bankaları siber saldırılara karşı daha dirençli hale getirir ve güvenli bir iş ortamını sağlar.

### 5.2. Düzenli Güvenlik Denetimleri

Bankaların sistemlerinde ve iş süreçlerinde bulunan potansiyel açıkları belirlemelerine yardımcı olur. Bu denetimler, siber saldırganların bu zafiyetleri istismar etmesini önlemek için gerekli önlemlerin zamanında alınmasını olanak sağlar. Güvenlik açıklarının erken tespiti, bankaların sistemlerini güçlendirerek veri ihlali riskini en aza indirmektedir. Düzenli denetimler, kurumların yasal düzenlemelere uyum sağlamasına ve müşteri güvenini korumasına katkıda bulunur. Bu süreç, siber güvenlik stratejilerinin sürekli olarak iyileştirilmesini sağlar ve bankaların tehditlere karşı daha hazırlıklı olmasını desteklemektedir.

### 5.3. Yazılımların Güncel Tutulması

Siber güvenliğin temel unsurlarından biridir. Eski veya güncellenmemiş yazılımlar, siber saldırganların sistemlere sızması için kolay bir hedef haline gelir. Bankalar, bilinen güvenlik açıklarını kapatmak ve olası tehditleri önlemek için tüm yazılımlarını, özellikle güvenlik yamalarını, düzenli olarak güncellemelidir. Bu, sistemlerin

güvenliğini artırır ve siber saldırılara karşı koruma sağlar. Ayrıca, güncel yazılımlar, yasal düzenlemelere uyum sağlamak ve müşteri verilerinin gizliliğini korumak için de kritik öneme sahiptir. Bu nedenle, bankaların yazılım güncellemelerini önceliklendirmesi, siber güvenlik stratejilerinin vazgeçilmez bir parçasıdır.

#### **5.4. Güçlü ve Benzersiz Parolalar Kullanmak**

Siber güvenliğin temel taşlarından biridir. Bankalar, çalışanlarını ve müşterilerini karmaşık parolalar oluşturmaya ve bu parolaları düzenli aralıklarla güncellemeye teşvik etmelidir. Bu uygulama, kaba kuvvet saldırılarının başarı şansını önemli ölçüde azaltır. Çok faktörlü kimlik doğrulama gibi ek güvenlik önlemleriyle birleştirildiğinde, hesap güvenliği daha da artmaktadır. Güçlü parola politikaları, siber tehditlere karşı etkili bir koruma sağlar.

#### **5.5. Olay Müdahale Planı Geliştirme**

Bankaların, siber saldırılar sırasında ortaya çıkabilecek zararları en aza indirmek ve hizmetleri hızlı bir şekilde yeniden başlatmak için kapsamlı bir olay müdahale planı oluşturması kritik öneme sahiptir. Bu plan, olası tehditlere hızlı ve etkili bir şekilde yanıt vermeyi, operasyonel sürekliliği sağlamayı ve müşteri güvenini korumayı hedefler. Düzenli olarak yapılan tatbikatlar ve planın sürekli güncellenmesi, bankaların siber tehditlere karşı daha hazırlıklı olmasını sağlamaktadır. Bu tür tatbikatlar, çalışanların olası bir saldırı durumunda nasıl hareket etmesi gerektiği konusunda bilinçlenmesine yardımcı olur ve müdahale süreçlerinin daha verimli bir şekilde işlenmesini sağlar. Aynı zamanda, planın güncellenmesi, yeni tehditlere karşı önlemlerin alınmasını ve güvenlik stratejilerinin sürekli olarak iyileştirilmesini mümkün kılar.

### **6. SONUÇ**

Bankacılık sektöründe siber güvenlik, finansal kuruluşları siber tehditlere karşı korumak, hassas verilerin güvenliğini sağlamak, operasyonel sürekliliği desteklemek ve müşteri güvenini korumak amacıyla tasarlanmış uygulamalar, teknolojiler ve süreçlerin tamamını kapsamaktadır. Bu kapsamda, siber saldırılar, veri ihlalleri, dolandırıcılık ve yetkisiz erişim gibi riskleri en aza indirmek için çeşitli güvenlik önlemleri uygulanmaktadır. Siber güvenlik, bankacılık sistemlerinin ve müşteri bilgilerinin bütünlüğünü, gizliliğini ve erişilebilirliğini korumak için hayati bir rol oynamaktadır. Giderek dijitalleşen ve birbirine bağlı hale gelen bir dünyada, bankacılık sektörü siber güvenliği olmazsa olmaz bir gereklilik haline getirmiştir. Fi-



nansal iřlemlerin gvenlięi ve mřteri verilerinin korunması, bankaların itibarını ve iř sreklilięini saęlamak iin kritik neme sahiptir.

Siber tehditlerin srekli olarak geliřmesi ve karmařık hale gelmesi, bankacılık sektrnde hassas finansal verilerin korunmasını ve sistemlerin operasyonel btnlęnn srdrlmesini en nemli nceliklerden biri haline getirmektedir. Siber sulların yntemleri her geen gn daha sofistike bir hal alırken, bankaların da bu tehditlere karřı savunma mekanizmalarını srekli olarak gncellemesi gerekmektedir. Bu srete, geliřmiř siber gvenlik zmlerini benimsemek, sıklı gvenlik protokollerini uygulamak ve en iyi uygulamalara baęlı kalmak byk nem tařımaktadır.

Teknolojik geliřmelerin yanı sıra, bankalar zerindeki dzenleyici baskı da artmaktadır. Hkmetler ve uluslararası kuruluřlar, kresel siber tehditlerin artması nedeniyle daha katı kurallar ve standartlar getirmektedir. Bu dzenlemeler, bankaların siber gvenlik seviyelerini srekli olarak ykseltmelerini ve veri koruma stratejilerini gncel tutmalarını gerektirmektedir. zellikle, mřteri verilerinin gizlilięi ve finansal iřlemlerin gvenlięi konusunda sıklı denetimler yapılmaktadır. Bankalar, bu dzenleyici gerekliliklere uyum saęlamak iin teknolojik altyapılarını glendirmeli ve alıřanlarının siber gvenlik farkındalıęını artıracak eęitimler dzenlemelidir.

Ayrıca, kresel iř birlięi ve bilgi paylařımı, siber gvenlięin geleceęi iin hayati neme sahiptir. Bankalar, siber saldırılara karřı daha etkili bir savunma oluřturmak iin birbirleriyle ve uluslararası gvenlik kuruluřlarıyla iř birlięi yapmalıdır. Bu tr iř birlikleri, yeni tehditlerin hızlı bir Őekilde tespit edilmesine ve ortak zmler geliřtirilmesine yardımcı olabilir. Aynı zamanda, siber gvenlik alanında yapılan Ar-Ge alıřmalarına yatırım yapmak, bankaların gelecekteki tehditlere karřı daha hazırlıklı olmasını saęlayacaktır.

Bankacılık sektrnde siber gvenlięin geleceęi, teknolojik yeniliklerin hızlı evrimi ve giderek sıklılařan dzenleyici erveler tarafından Őekillenecektir. Siber saldırıların giderek daha karmařık ve sofistike hale gelmesi, bankaları savunma mekanizmalarını glendirmek iin yapay zeka (AI), blok zinciri (blockchain) ve kuantum biliřim gibi ileri teknolojilere ynelmeye zorlamaktadır. Yapay zeka ve makine ęrenimi, byk veri kmelerini analiz ederek anormal davranıř kalıplarını tespit etme ve tehditlere gerek zamanlı mdahale etme konusunda kritik bir rol oynayacaktır. Bu teknolojiler, geleneksel yntemlerin fark edemeyeceęi saldırıları nceden belirleyerek, bankaların siber gvenlik stratejilerini daha proaktif hale getirecektir.

Sonuç olarak, teknolojik yenilikler ve dzenleyici gerekliliklerin bir araya gelmesiyle Őekillenecektir. Yapay zeka, blok zinciri ve kuantum bili-

şim gibi teknolojiler, bankaların savunma mekanizmalarını güçlendirirken, düzenleyici kurumların getirdiği sıkı standartlar da kurumların güvenlik seviyelerini yükseltmelerini zorunlu kılmaktadır. Bu süreçte, bankaların hem teknolojik altyapılarını hem de insan kaynaklarını sürekli olarak geliştirmesi, siber tehditlere karşı daha dirençli bir yapı oluşturmalarını sağlayacaktır. Bu kombinasyon, bankacılık sektöründe siber güvenliğin geleceğini tanımlayacak ve müşteri güvenini koruyarak sektörün büyümesine katkıda bulunacaktır.

**KAYNAKÇA**

- Alsayed, A. O. & Bilgrami, A. (2017). "E-Banking Security: Internet Hacking, Phishing Attacks, Analysis and Prevention of Fraudulent Activities", International Journal of Emerging Technology and Advanced Engineering, 7(1), 109-115.
- Amit, S. (2023). Bankacılıkta Siber Gvenlik: Tehditler ve Gvenlik Czmleri <https://www.aquasec.com/cloud-native-academy/application-security/cybersecurity-in-banking/>
- Berg, S. E. (2009a). Identity theft. S. McQuado (Ed.). Encyclopedia of cybercrime. Greenwood Publishing Group. 90-93.
- Boeke, S. (2018). National cyber crisis management: Different Europe Approaches. Governance, 449-464.
- Eren, M. (2023). Bankacılık deme Sistemlerinde Siber Gvenlik Farkındalıęı: Trk Bankacılık Sektrnde Farkındalıęın Belirleyicileri zerine Bir Uygulama. Doktora Tezi, Marmara niversitesi, Bankacılık ve Sigortacılık Enstits.
- Golandsky, Y. (2016). Cyber Crisis Management, Survival or Extinction. Las Vegas: Information Institute Conferences.
- Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. ACM Transactions on Information and System Security, 5(4), 438-457.
- Hansche, S. (2001). "Designing A Security Awareness Program: Part 1", Information Systems Security, 9(6), 1-9.
- IBM. (2015). IBM security services 2015 cyber security intelligence index. Eriřim tarihi: 05.3.2025, <https://securityintelligence.com/media/cyber-security-intelligence-index2015/>.
- IBM.(2019). What are security controls? Eriřim tarihi: 05.3.2025, <https://www.ibm.com/cloud/learn/security-controls>
- Jackson, L. A. (2018). Malware. B. Warf. (Ed.). The sage encyclopedia of the internet. Sage Publications. 619-624.
- Johnson, A. L. (2016). Cybersecurity for financial institutions: The integral role of information sharing in cyber attack mitigation. N.C. Banking Inst., 20(1), 277-310.
- Kaspersky. (2021a). What is keystroke logging and keyloggers? Eriřim tarihi: 04.3.2025, <https://www.kaspersky.com/resource-center/definitions/keylogger>.
- Kerr, G. (2018). "Cybersecurity in Banking and Payments in the United Kingdom", The Visio Journal Sayı 3, 39-48.
- Kharraz, A. (2018). Ransomware. B. Warf. (Ed.). The sage encyclopedia of the internet Sage publications. 720-724

- Lepkowski, P. (2009). Denial of service attacks. S. McQuado (Ed.). Encyclopedia of cybercrime. Greenwood Publishing Group. 63-64
- Marion, N. E., & Twede, J. (2020). Cybercrime: An encyclopedia of digital crime. ABCCLIO.
- Mirkovic, J. (2018). Malware. B. Warf. (Ed.). The sage encyclopedia of the internet. Sage Publications. 250-253.
- Özkaya, E., Sarıca, R. & Durmaz, Ş. (2019). Siber Güvenlik Saldırı ve Savunma Stratejileri, Ankara: Buzdağı Yayınevi
- Von Solms, B., & Von Solms, R. (2018). Cybersecurity and information security-what goes where? Information and Computer Security, 26(1), 2-9.

# BÖLÜM 3

ENDÜSTRİ 4.0 İLE DİJİTALLEŞME DÖNEMİNDEN  
ENDÜSTRİ 5.0 KİŞİSELLEŞTİRME SÜRECİNE

*Emel ABA ŞENBAYRAM*

## Giriş

Teknolojik gelişmelerin işletme ve toplum hayatına hızlı entegrasyonu ile başlayan dijitalleşme süreci, geleneksel iş süreçlerinin, hizmetlerin ve ürünlerin dijital teknolojiler aracılığı ile dönüştürülmesi ve işletmelerin bu teknolojilere uyum sağlamasıdır. Dijitalleşme, işletmelerin ve toplumun dijital dünyaya geçiş sürecidir ve internet, mobil cihazlar, yapay zekâ, bulut bilişim gibi teknolojilerin kullanımını içerir. Dijitalleşme ile bilgi, veri, hizmetler ve ürünler dijital olarak işlenir, depolanır ve paylaşılır.

Endüstrileşme bir ülkede gelişen teknoloji kullanımını neticesinde artan verimliliğin ülkenin GSYH'na olan etkisini ifade ederken aynı zamanda söz konusu ülkenin ekonomik refaha paralel olarak sosyal refahının da gelişmesini ifade etmektedir. Toplumların sosyo ekonomik açıdan gelişimini temsil eden endüstrileşme, zaman içerisinde ortaya çıkan mekanik ve elektronik gelişmeler neticesinde evrilirken yeni bir dönemin de kapısını aralamaktadır.

Dördüncü dönemini yaşamakta olan endüstrileşme ilk olarak buharlı makinaların kullanılmaya başlandığı Endüstri 1.0 ile başlamıştır. Petrolün yaygın kullanımı ve üretim bandı sistemlerinin işgücü ile birleşmesi ile birlikte üretimde verimlilik artmış ve bu dönem Endüstri 2.0 olarak ifade edilmiştir. Zaman içerisinde internetin sektör içerisinde kullanımının artması, elektrik-elektronik ve bilgisayar alanındaki hızlı gelişmeler, sektörleri informatik evrime yönlendirmiş ve bu şekilde Endüstri 3.0 dönemi yaşanmıştır. Hali hazırda yaşanmakta olan Endüstri 4.0 dönemi nesnelerin interneti ve siber-fiziksel sistemler gibi teknolojiler üretim sürecine dahil edilerek üretimde otonom robotların yer aldığı ve sürecin akıllı fabrikalar tarafından takip edildiği bir süreçtir. Ancak dijitalleşme sonrasında bilişim ve iletişim teknolojilerindeki gelişmeler, ülkeler arası siyasi, ekonomik ve politik rekabet ile birleşince endüstrinin de farklı bir boyuta evrilebileceği öngörüsünü doğurmaktadır. Endüstri 5.0 olarak ifade edilen bu dönemde refah düzeyi yüksek akıllı toplumların oluşturulması hedeflenmektedir. Endüstri 5.0'ı Endüstri 4.0'dan ayıran en önemli özellik teknolojinin işgücü ile birlikte kullanılmasından ziyade bilgi ve teknolojinin yapay zekâ aracılığı ile insanların hizmetine sunulmasıdır. İnsanlığı her açıdan köklü bir değişime sürükleyen bu sürecin araştırılması ve farklı perspektiflerden değerlendirilmesi oldukça önemlidir. Bu noktadan hareketle yapılan bu çalışma ile Endüstri 5.0

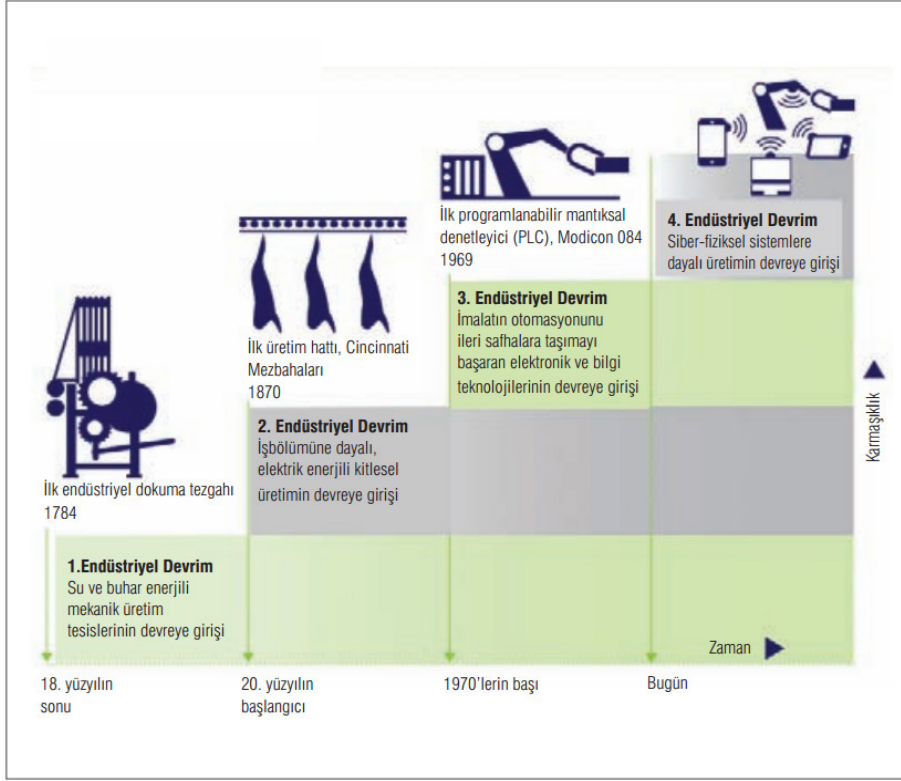
öngörüsünün mevcut şartlar altında dünyadaki durumunun deęerlendirilmesi amaçlanmıřtır.

### 1. Dijitalleşme ve Endüstri 4.0 Süreci

Dijitalleşme, bilgi, iş süreçleri ve hizmetlerin dijital teknolojiler kullanılarak dönüřtürülmesi sürecini ifade etmektedir. Kâğıt, analog ve manuel sistemlerden dijital sistemlere geçiři ifade eder. Günümüzde eğitim, saęlık, finans, sanayi ve ticarete aktif bir şekilde kullanılan dijitalleşme, verilerin işlenmesi ve saklanması, iş süreçlerinin etkinlik ve verimliliklerinin artırılması, toplumsal iletişim ile ve sanayinin gelişimine önemli rol oynamaktadır. Pandemi sonrasında günümüz dünyasında kaçınılmaz bir dönüřüm olan dijitalleşme iş dünyasından günlük yaşama kadar her alanda verimlilięi artırmakta, maliyetleri düşürmekte ve sürdürülebilirlięi desteklemektedir. Genel çerçevede dijitalleşme, iş süreçlerinin kâğıt tabanlı ve manuel sistemlerden, dijital ve otomatik sistemlere geçiřini ifade ederken Endüstri 4.0 ise bu dijital dönüřüm sürecinin üretim sektörüne uygulanmış hali şeklinde tanımlanabilmektedir.

İlk olarak Almanya'nın Hannover Fuar'ında ifade edilen Endüstri 4.0 kavramı aslında gelişen teknolojilerin entegrasyonundan kaynaklı olarak sanayinin radikal dönüřümünü temsil etmektedir (Menendez vd., 2020). Siber fiziksel sistemler, nesnelerin interneti, internet servisleri ve akıllı fabrikalar şeklinde dört ana bileşenden oluşan Endüstri 4.0 için kompleks yapısı sebebiyle net bir tanımlama yapılamamaktadır.

18. Yüzyılın sonlarında başlayan endüstrileşme, zaman içerisinde teknolojik gelişmelere paralel olarak gelişim göstererek dört temel dönemde şekillenmektedir. Endüstrileşmenin tarihsel süreci Şekil 1'de yer almaktadır.



Kaynak: [Endüstri Tarihine Kısa Bir Yolculuk](#), (04.02.2025)

Endüstri 4.0 dönemini diğer endüstriyel dönemlerden ayıran birtakım farklılıklar bulunmaktadır (Bayram ve Karadağ, 2023; Fırat ve Fırat, 2017; Bulut ve Akçacı, 2017; Verl, 2017). Bunlar;

**Hız:** Endüstri 4.0 dönemindeki gelişmeler önceki dönemlerin aksine doğrusal değil istikrarlı ve olumlu yönde gelişim gösteren bir hızlar ilerlemektedir.

**Genişlik ve Derinlik:** Endüstri 4.0 dönemine ait gelişmeler dijital teknoloji alt yapısı üzerine kurulurken toplumu ve toplumu doğrudan etkileyen tüm tarafların gelişime açık paradigmalara donatarak sürdürülebilirliğine olanak tanımaktadır.

**Sistem Etkisi:** Endüstri 4.0 tüm yönetim bilişim sistemlerine ek olarak üretime doğrudan katılı ve etkisi olan tüm tarafların ağ sistemi üzerinden birbirleri ile bağlantıda olduğu bütünleşik bir dönüşümü kapsamaktadır.

Endüstri 4.0'ın önceki endüstri dönemlerinden ayıran en önemli fark ise Endüstri 4.0'ın devrimsel niteliğinin yanında aynı zamanda evrimsel de olmasıdır. Diğer bir ifade ile Endüstri 1.0 ve Endüstri 2.0 teknolojik



geliřmelere paralel olarak üretim sürecinde yařanan devrim nitelięinde deęiřimlerin sonucunda son bulmaktadır. Ancak Endüstri 3.0 dönemi için bir devrin kapandıęını söylemek doęru olmayacaktır. Çünkü her dönemin sona eriřinde üretimde kullanılan teknolojilerde meydana gelen deęiřimlerin neden olduęu dikkate alındıęında, Endüstri 3.0 döneminde bilgisayar ve mikro-iřlemcilerle kontrol edilen üretim sistemleri otomasyona dayandırılırken Endüstri 4.0 'da söz konusu üretim mantıęı devam ederken süreç insanlar yerine akıllı sistemlere baęlı makine ve robotlarla yürütölmektedir.

### ***Endüstri 4.0'ın Temel Hedefleri***

Endüstri 4.0'ın temel hedefi, verimlilięi ve üretim kapasitesini artırırken iřletmelerin daha sürdürölebilir ve rekabetçi hale gelmesini saęlamaktır. Bu doęrultuda ařaęıda verilmekte olan görevlerin geręekleřtirilmesi gerekmektedir.

#### ***Otomasyonu Artırmak***

- Üretim süreçlerini insan müdahalesine gerek kalmadan sürdüröbilmek.
- Robotlar ve yapay zekâ destekli sistemlerle verimlilięi artırmak.

#### ***Akıllı Fabrikalar Kurmak***

- Siber-fiziksel sistemler (CPS) ile makinelerin birbiriyle iletiřim kurmasını saęlamak.
- Üretimi geręek zamanlı veri analizi ile yönetmek.

#### ***Veri Odaklı Karar Alma Mekanizmaları Geliřtirmek***

- Büyük veri (Big Data) analizleriyle iřletme süreçlerini optimize etmek.
- Makine öęrenmesi ile arıza tahminleri yaparak bakım süreçlerini iyileřtirmek.

#### ***Esnek ve Kiřiselleřtirilmiř Üretime Geęmek***

- Tüketici taleplerine göre özelleřtirilmiř ürünler üretmek (kitlesele özelleřtirme).
- Talebe dayalı üretim modelleriyle stok maliyetlerini azaltmak.

### ***Enerji ve Kaynak Verimliliğini Artırmak***

- Üretimde çevre dostu malzemeler ve düşük enerji tüketen sistemler kullanmak.
- Döngüsel ekonomi prensiplerine uygun geri dönüşüm süreçlerini teşvik etmek.

### ***İnsan ve Robot İş Birliğini Geliştirmek***

- İnsansı robotlar ile çalışanları destekleyerek iş güvenliğini artırmak.
- İnsanın yaratıcı gücünü yapay zekâ ile birleştirerek üretim süreçlerini iyileştirmek.

### ***Tedarik Zinciri ve Lojistiği Dijitalleştirmek***

- Blockchain ve IoT teknolojileri ile tedarik zincirini daha şeffaf ve güvenilir hale getirmek.
- Otonom lojistik sistemleri ile teslimat süreçlerini optimize etmek.

### ***Üretim Maliyetlerini Düşürmek***

- Yapay zekâ ve sensör teknolojileriyle hataları azaltarak fire oranlarını düşürmek.
- Öngörülebilir bakım ile makinelerin kullanım ömrünü uzatmak.

Günümüzde insanlar arasında iletişimi sağlayan internet, Endüstri 4.0 ile birlikte nesnelere ile nesnelere, nesnelere ile insanlar hatta hizmetler arasında da iletişimi sağlayan bir araç haline gelmiştir. Bu sürecin en dikkat çeken özelliği insandan nesneye, fabrikadan tüketiciye hayatın her bir alanını bir tür ağla birbirine bağlamayı hedeflemesidir. Büyük veri ve analitiği, bulut bilişim sistemleri, siber güvenlik, akıllı robotlar, yapay zekâ gibi pek çok yeni teknolojiyi barındıran Endüstri 4.0 önümüzdeki dönemde ekonomiden sağlığa, eğitimden güvenliğe, istihdamdan yatırıma birçok alanda değiştirici ve dönüştürücü etki gösterecektir (TBMM, 2023, 15) Bu noktada Endüstri 4.0'ın aslında imalat sanayiini yani üretim süreçlerini ve üretimle ilgili tüm hizmetleri ifade ettiğini belirtmek gerekmektedir. Bir zaman sonra Endüstri 4.0'a yön veren tüm etken ve teknolojilerin çeşitli sektörler kapsamında ele alınarak “Tarım 4.0, Lojistik 4.0, İnşaat 4.0, Enerji 4.0, İnovasyon 4.0, İş 4.0, Eğitim 4.0, Sağlık 4.0 vb.” yeni terimlerin ortaya çıkması muhtemeldir. Söz konusu öngörülerin gerçekleşme-

si iin ihtiya duyulan surenin ok da uzun olmadıęını Dnya Ekonomi Formu'nun hazırlamıř olduęu 2015 Arařtırma Raporu kanıtlar niteliktedir. Raporda 2025 yılı itibariyle dnyada gerekleřmiř olması muhtemel geliřmeler řu Őekilde sıralanmaktadır (World Economic Forum, 2015, 7):

- İnsanların % 10'unun internete baęlanabilen giysiler giymesi
- İnsanların % 90'ının sınırsız ve cretsiz (reklam destekli) depolama alanına sahip olması
- 1 trilyon sensrn internete baęlanması
- Okuma gzlklerinin % 10'unun internete baęlanması
- İnsanların % 80'inin dijital bir varlıęa sahip olması
- retimdeki ilk 3D baskılı otomobilin retilmesi
- Nfus sayımının byk veri kaynaklarıyla gerekleřmesi
- Vcuda yerleřtirilebilir ilk telefonun satıřa sunulması
- Tketicilern rnlerinin yzde 5'inin 3D basılı olması
- Nfusun % 90'ının internete dzenli eriřebilmesi
- Nfusunun % 90'ının akıllı telefon kullanması
- Amerika'da kullanılan otomobillerin % 10'unun srcsz olması
- 3D baskılı ilk karacięer nakli
- Őirket denetimlerinin % 30'unun yapay zeka ile denetlenmesi
- Vergisini blockchain ile toplayan ilk devletin olması
- İnternet kullanımının %50'sinden fazlasının ev aletleri ve cihazlar iin kullanılması
- 50.000'den fazla nfusu olan ve trafik ıřıęı olmayan ilk Őehir
- Kresel gayri safi yurt ii hasılanın %10'unun blockchain teknolojisinde depolanması

Gnmzde Endstri 4.0 ve dijital dnřm performansı en yksek olan lkeler ierisinde ilk sırada ABD, Japonya, Gney Kore ve Almanya yer alırken geliřmiř ekonomiye sahip bu lkeleri Danimarka, İsve, Fransa, İsvire, Finlandiya, İngiltere gibi Avrupa'nın nde gelen lkeleri takip etmektedirler. Slovenya, İspanya, Slovakya, Trkiye ve Meksika gibi ekonomik geliřim sreci devam eden lkeler OECD yesi lkeler ierisinde son sıralarda yer almaktadırlar (Eřiyok ve Demircioęlu, 2022: 394). Genel olarak, Endstri 4.0 seviyesi, teknolojik altyapı, eęitim, yatırım ve politika desteęi gibi faktrlere baęlı olarak farklılık gstermektedir. Bu nedenle, dnya genelinde Endstri 4.0'ın benimsenme oranı ve seviyesi olduka e-

Őitlidir. Endüstri 4.0 ile baŐta Almanya olmak üzere geliŐmiŐ ekonomilere sahip batılı ölkelerin hedefinde, dőnyanın doĐusuna kayan üretim hacmi, verimlilik ve rekabet avantajını yüksek teknolojiye dayalı sanayi aracılıĐı ile elde etmek yer almaktadır (Aba Őenbayram, 2024:1439). Bu stratejinin Almanya'da ortaya ıkmasında ise dőnyanın en rekabeti imalat sanayilerinden birine sahip olması, imalat sanayiinde küresel lider olarak görölmesi, güçlü makine ve imalat endüstrisine, bilgi ve iletişim teknolojileri altyapısına, gömölü sistemler ve otomasyon mühendisliĐindeki bilgi birikimine sahip olması gibi avantajları etkili olmaktadır (Bartodziej, 2017, s. 32)

### Küresel Ölçekte Endüstri 4.0 Stratejileri

Dőnya genelinde birçok ölkede Endüstri 4.0 sürecine uyum saĐlamak ve sanayilerini dijitalleŐtirmek için çeŐitli stratejiler geliŐtirmektedir. Endüstri 4.0, ölkeler için teknolojik üstünlük, verimlilik ve rekabet avantajı saĐlayan kritik bir dönüŐümdür. DijitalleŐmeye hızlı uyum saĐlayan ölkeler, sanayilerini daha verimli ve sürdürülebilir hale getirerek küresel ekonomide güçlü bir konum elde etmektedir. Ölkeler Endüstri 4.0 stratejilerini genellikle aŐaĐıdaki unsurlar etrafında Őekillendirir:

- 1. Dijital DönüŐüm:** Ölkeler, sanayi tesislerinin dijitalleŐmesini teŐvik ederek verimliliĐi artırmayı hedefler. Bu, IoT (Nesnelerin İnterneti), büyük veri analitiĐi ve yapay zeka gibi teknolojilerin entegrasyonunu içerir.
- 2. EĐitim ve Yetenek GeliŐimi:** Endüstri 4.0'a uyum saĐlamak için nitelikli iŐ gücüne ihtiya vardır. Bu nedenle, ölkeler eĐitim sistemlerini güncelleyerek STEM (bilim, teknoloji, mühendislik ve matematik) alanlarına odaklanır.
- 3. AraŐtırma ve GeliŐtirme (Ar-Ge):** Yeniliki teknolojilerin geliŐtirilmesi için Ar-Ge yatırımlarını artırmak, ölkelerin stratejilerinin önemli bir parasıdır. Bu hem özel sektör hem de kamu sektörü iŐ birliĐi ile gerçekleştirilir.
- 4. Altyapı GeliŐimi:** GeliŐmiŐ dijital altyapı, Endüstri 4.0 uygulamaları için kritik öneme sahiptir. Ölkeler, hızlı internet baĐlantıları ve veri merkezleri gibi altyapı projelerine yatırım yapar.
- 5. Politika ve Regölasyon:** Endüstri 4.0'ın etkili bir Őekilde uygulanabilmesi için uygun politikaların ve regölasyonların oluŐturulması gerekmektedir. Bu, veri güvenliĐi, siber güvenlik ve etik konularını da kapsar.

- 6. Uluslararası İř Birlięi:** Ülkeler, Endüstri 4.0 stratejilerini geliřtirmek için uluslararası iř birliklerine önem verir. Bu, bilgi paylařımını ve en iyi uygulamaların benimsenmesini saęlar.

Her ülkenin Endüstri 4.0 stratejisi, kendi ekonomik ve sosyal kořullarına göre farklılık gösterebilir. Ancak genel olarak, bu unsurların çoęu, ülkelerin sanayi ve teknoloji alanında rekabetçi kalmalarını saęlamak için kritik öneme sahiptir.

## 2. Endüstri 5.0 Öngörüsü

Endüstri 5.0, sanayi devrimlerinin en yeni ařamalarından biri olup Endüstri 4.0'ın devamı niteliğindedir. Bu kavram, insan ve makine iř birlięini merkeze alarak daha sürdürülebilir, insan odaklı ve dayanıklı üretim sistemleri geliřtirmeyi amaçlamaktadır. Bu amacın gerçeřtirilmesi için öncelikle insani etik ve ahlaki deęerlerin bilincinde olan akıllı makinelerin geliřtirilmesi gerekmektedir. İnsana özgü bu deęer ve sorumlulukların yapay zekâ destekli makinelere hangi durumlarda, ne amaçla ve nasıl verileceęi ise hala belirsizlięini korumaktadır (Baum, 2020; Ryan & Stahl, 2020; Bostrom & Yudkowsky, 2014). 2017 Biliřim Fuarı CeBIT de Japonya Bařbakanı Shinzo Abe tarafından Endüstri 5.0'in felsefesi ile anlařılması gerektięini vurgulamaktadır. Geliřen teknolojinin, tehdit olarak deęil, toplumlara bir yardımcı olarak düşünülmesi gerektięi belirtilmektedir. Endüstri 5.0'ın temel birtakım özelliklere sahiptir. Bunlar:

**İnsan-Makine İř birlięi:** Endüstri 4.0'daki otomasyon ve yapay zekâ (AI) çözümlerine ek olarak, Endüstri 5.0 insanlarla makinelerin birlikte çalıřmasını vurgular. Robotlar ve otomasyon, insanların yerini almak yerine onlara yardımcı olur.

**Özelleřtirilmiř Üretim:** Seri üretim yerine kiřiselleřtirilmiř, müşteri odaklı üretim ön plandadır. Yapay zekâ ve robot teknolojileri, müşteri ihtiyaçlarına göre uyarlanabilir üretim yapmayı mümkün kılar.

**Sürdürülebilirlik:** Yeřil teknolojiler, geri dönüřtürülebilir malzemeler ve çevre dostu üretim süreçleriyle, sanayinin doęaya zarar vermeden büyümesini hedefler.

**Dayanıklılık ve Esneklik:** Krizlere karřı daha dayanıklı üretim sistemleri geliřtirilir. Tedarik zincirlerinde esneklik artırılarak, küre-

sel krizler (örneğin pandemi veya savaşlar) karşısında sanayi sistemlerinin ayakta kalması sağlanır.

**İnsanı Merkeze Koyma:** İş gücünü tamamen otomasyona bırakmak yerine, insanların daha yaratıcı ve problem çözme yeteneklerini kullanabileceği bir çalışma ortamı yaratmak hedeflenir.

Endüstri 4.0'ın devamı niteliğinde olan Endüstri 5.0, birey ve toplumu merkeze alması bakımından Endüstri 4.0'dan ayrılmaktadır. Bu, söz konusu iki dönem arasındaki en temel farklılıktır. Endüstri 4.0 ve Endüstri 5.0 arasındaki farklar Tablo 1'de yer almaktadır.

Tablo 1. Endüstri 4.0 ve Endüstri 5.0 Arasındaki Farklar

| Kriter                     | Endüstri 4.0                                     | Endüstri 5.0                                    |
|----------------------------|--|---|
| <b>Odağı</b>               | Otomasyon, dijitalleşme, yapay zekâ              | İnsan-makine iş birliği, sürdürülebilirlik      |
| <b>Teknoloji Kullanımı</b> | Robotik, IoT, büyük veri, yapay zekâ             | Akıllı üretim, yeşil teknoloji, etik yapay zekâ |
| <b>İnsan Rolü</b>          | İnsan gücü yerine otomasyon                      | İnsan ve makine birlikte çalışır                |
| <b>Üretim Modeli</b>       | Verimlilik ve karlılık odaklı                    | Çevreye duyarlı, sürdürülebilir, esnek üretim   |
| <b>Toplumsal Etki</b>      | Dijital dönüşüm, otomasyon kaynaklı iş kayıpları | İnsan odaklı ekonomi, yeni iş alanları          |

Endüstri 5.0, endüstriyel otomasyonu insan zekasıyla birleştirerek hız ve hassasiyeti optimize etmektedir. Dayanıklı ve çevre dostu politikalar, minimum atık oluşumu ve daha etkili bir organizasyon sağlamaktadır (Elangovan, 2021). Endüstri 5.0, insan faktörünü üretim sürecinin dışına itmek yerine, onu makinelerle iş birliği içinde çalışabilecek şekilde geliştirmeyi amaçlamaktadır. Endüstri 5.0, ilk düşüncelerin aksine, insan gücünün ihtiyaç duyulmadığı, artık personel istihdamın sağlanmayacağı anlamına gelmemektedir (Günther ve ark., 2022: 2-3; Nahavandi, 2019: 10). Aksine Endüstri 5.0 ile iş gücünün daha yaratıcı ve değerli hale gelmesi hedeflenmektedir. Bu noktada işgücü piyasasının çağın gereklerine uygun plan ve stratejilerle ilerleme kaydetmesi gerekmektedir. Şöyle ki ulusal ve uluslararası alanda ilgili otoritelerin, Endüstri 5.0 süreci ve sonrasında başta işgücü piyasası olmak üzere tüm sektörlerde olması kayıp ve fırsatların önceden belirlenerek bu doğrultuda gerekli yaptırımların

hayata geirilmesi gerekmektedir. Endüstri 5.0 geleceğinde işgücünde maksimum fayda olanađına saęlayabilmek için otomasyon teknolojilerine hâkim olmak için yapay zekâ ve otomasyon eğitimleri önem arz etmektedir. Öte yandan bireylerin büyük veri ve analitik becerilere sahip kariyer fırsatlarını yakalayabilmeleri için veri okuryazarlığı rekabet avantajı saęlayacaktır. İş görenlerin söz konusu rekabet avantajını elde etmeleri ve gerekli yetkinliğe sahip olmaları ancak teknolojik gelişmeler karşısında gösterecekleri esneklik ve adaptasyon performansları etkili olacaktır. Endüstri 5.0 ile otomasyonun yaygınlaşması bazı geleneksel işlerin kaybolmasına neden olabilecektir ancak aynı zamanda yeni meslekler ve istihdam fırsatlarına da imkân tanıyacaktır. Bu noktada en makul çözümün eğitim sistemlerinin bireyleri dijital ve sürdürülebilir ekonomiye uygun becerilerle donatmasıdır. Endüstri 5.0 geleceğin olası mesleklerinden bazıları şöyle sıralanabilmektedir:

#### *Robotik ve Yapay Zekâ Uzmanları*

- **İş Tanımı:** İnsanlarla birlikte çalışabilen cobot'ları (işbirlikçi robotlar) programlama, yapay zekâ destekli üretim süreçlerini geliştirme.
- **Gereken Beceriler:** Yapay zekâ, makine öğrenmesi, veri analitiđi, robotik kodlama.

#### *Dijital İkiz Uzmanları*

- **İş Tanımı:** Fabrika ve makinelerin dijital kopyalarını (dijital ikizler) oluşturup simülasyonlar yapmak, verimlilik analizleri gerçekleştirmek.
- **Gereken Beceriler:** Nesnelerin İnterneti (IoT), büyük veri analizi, sanal modelleme.

#### *Sürdürülebilirlik ve Yeşil Mühendisler*

- **İş Tanımı:** Üretim süreçlerinde karbon ayak izini azaltmak, yenilenebilir enerji ve çevre dostu teknolojiler geliştirmek.
- **Gereken Beceriler:** Çevre mühendisliği, enerji yönetimi, sürdürülebilir malzeme bilimi.

### *İnsan-Makine Etkileşim Uzmanları*

- **İş Tanımı:** Robotların ve akıllı sistemlerin insanlarla nasıl daha iyi etkileşime girebileceğini tasarlamak ve geliştirmek.
- **Gereken Beceriler:** Kullanıcı deneyimi (UX), insan-makine arayüzleri (HMI), biyomekanik.

### *3D Baskı ve Üretim Teknolojileri Uzmanları*

- **İş Tanımı:** Üç boyutlu yazıcılarla üretim süreçlerini optimize etmek, kişiselleştirilmiş üretim yapmak.
- **Gereken Beceriler:** 3D modelleme, malzeme bilimi, üretim mühendisliği.

### *Siber Güvenlik Uzmanları*

- **İş Tanımı:** Endüstriyel sistemleri siber tehditlere karşı korumak, veri güvenliğini sağlamak.
- **Gereken Beceriler:** Etik hackerlik, ağ güvenliği, veri şifreleme.

### *Veri Analistleri ve Yapay Zekâ Mühendisleri*

- **İş Tanımı:** Üretim süreçlerinden gelen büyük veriyi analiz ederek verimliliği artırmak ve karar alma süreçlerine destek olmak.
- **Gereken Beceriler:** Büyük veri analitiği, makine öğrenmesi, veri madenciliği.

### *Biyo-Mühendisler ve Nöro teknoloji Uzmanları*

- **İş Tanımı:** İnsan vücudu ile makineler arasındaki etkileşimi geliştirmek, beyin-makine arayüzleri tasarlamak.
- **Gereken Beceriler:** Sinirbilim, biyoteknoloji, nöro-mühendislik.



### *Döngüsel Ekonomi Uzmanları*

- **İř Tanımı:** Üretimde geri dönüşümü artırmak, atık yönetimi sistemleri geliřtirmek, sürdürülebilir iř modelleri oluşturmak.
- **Gereken Beceriler:** Ekoloji, malzeme bilimi, endüstriyel tasarım.

### *Artırılmış Gerçeklik (AR) ve Sanal Gerçeklik (VR) Uzmanları*

- **İř Tanımı:** Eğitim, tasarım ve üretim süreçlerinde sanal gerçeklik ve artırılmış gerçeklik teknolojilerini kullanmak.
- **Gereken Beceriler:** 3D modelleme, yazılım geliřtirme, görsel tasarım.

## **3. Dünyada Endüstri 5.0 Dönemi**

Endüstri 5.0 dönemine geçen veya bu alanda önemli adımlar atan ülkeler, gelişmiş dijital altyapıya, güçlü sanayi sektörlerine ve ileri teknolojiye sahip ülkelerden oluşmaktadır. Endüstri 5.0'a öncülük eden ülkelerin başında Japonya, Almanya, ABD, Çin, Güney Kore ve AB ülkeleri gelmektedir. Bu ülkeler, insan-makine iş birliği, sürdürülebilir üretim ve yapay zekâ tabanlı sistemler üzerine yoğunlaşmakta ve bu doğrultuda strateji oluşturmaktadırlar. Aşağıda Endüstri 5.0'a öncülük eden ülkeler ve yaptıkları çalışmaların özeti yer almaktadır.

### *Japonya*

◆ **Teknoloji Odaklı Sanayi Politikaları:** Japonya, "Toplum 5.0" kavramıyla Endüstri 5.0'ın temelini öncü ülkelerden biridir. İnsan ve makine iş birliğini artırmak için yapay zekâ (AI) ve robot teknolojilerini geliřtirmektedir. Ayrıca hibrit çalışma ortamları yaratmak için cobotlar (insanlarla çalışan robotlar) yaygın olarak kullanılmaktadır.

### *Almanya*

◆ **Endüstri 4.0'ın Lideri, 5.0'a Geçiş Ařaması:** Almanya, Endüstri 4.0'ın öncüsü olduęu gibi Endüstri 5.0'ın da gelişimine öncülük etmektedir. "Made in Germany 2030" stratejisi ile akıllı fabri-

kalar kurumakta ve sürdürülebilir üretim ve çevreci sanayi politikalarına ağırlık vermektedir.

### *Güney Kore*

◆ **Dijitalleşme ve Robot Teknolojileri:** Güney Kore, akıllı üretim sistemleri ve otomatikleştirilmiş fabrikalar konusunda önde gelen ülkelerden biridir. Yapay zekâ tabanlı iş süreçleri ile üretimde kişiselleştirmeye odaklanmaktadır.

### *Amerika Birleşik Devletleri*

◆ **Endüstri 5.0 ile İnsan Odaklı Üretim:** ABD, Tesla, Apple ve Google gibi teknoloji devleri, robot-insan iş birliği projelerine yatırım yapmakta ve sürdürülebilir üretim ve yenilenebilir enerji sistemleri Endüstri 5.0 ile entegre edilmektedir.

### *Çin*

◆ **Akıllı Fabrikalar ve IoT Çözümleri:** Çin, Endüstri 5.0 için dijital fabrikalar inşa ederek en hızlı gelişen ülkelerden biridir. “Made in China 2025” stratejisi kapsamında, yapay zekâ, büyük veri ve IoT teknolojilerini üretim süreçlerine entegre etmektedir.

### *Avrupa Birliği Ülkeleri*

◆ **Sürdürülebilirlik Odaklı Endüstri 5.0:** AB ülkeleri, yeşil enerji ve sürdürülebilir sanayi alanında öncü adımlar atarken, döngüsel ekonomi prensiplerine dayalı üretim sistemleri geliştirmektedir. Hollanda ve İsveç gibi refah düzeyi yüksek ülkeler karbon nötr üretim sistemlerine yönelik politikalara yönelirken, Fransa ve İtalya için akıllı şehir ve sanayi entegrasyonu öncelik oluşturmaktadır.

Görüldüğü üzere ülkelerin Endüstri 5.0 politikalarının odağında sürdürülebilir kalkınma yer almaktadır. Çevreye duyarlı yeşil teknolojilerin kullanıldığı Endüstri 5.0, sadece ekonomik büyümeyi değil, aynı zamanda çevresel ve sosyal sürdürülebilirliği de amaçlayan bir yaklaşımdır. Yeşil üretim, akıllı teknolojiler ve insan merkezli inovasyon ile sürdürülebilir kalkınmayı desteklenmektedir. Endüstri 4.0 ile zaman içerisinde ekonomik gelişmeler, teknoloji ve küreselleşmenin de etkisiyle ekonomik büyüme yerini kalkınmaya, kalkınma ise yerini daha uzun vadeli yerel bazlı girişimleri de kapsayan ve en önemlisi sürdürülebilir çevre ve toplumsal değerleri önemseyen bir kavram olan sürdürülebilir kalkınmaya bırakmış-

tır. Sürdürülebilir kalkınma ile vurgulanmak istenen konu, salt ekonomik büyümenin tek başına yeterli olmayacağıdır. Temel hedef dinamik ve istikrarlı bir ekonomik büyüme sağlarken, elde edilen katma değerin toplumlar arası dengeli dağılımı sağlamaktır (Aba Şenbayram, 2022:400).

## SONUÇ

Endüstri, bir ülkenin ekonomik kalkınmasının temel taşlarından biri olup, üretim süreçlerinin sistematik hale getirilmesiyle mal ve hizmetlerin büyük ölçekte üretilmesini sağlamaktadır. Tarım ve el işçiliğine dayalı ekonomilerden modern ve yüksek teknolojiye üretime geçiş, sanayi devrimleriyle mümkün olmuştur. Sanayi devrimleri ise her dönem insan hayatını, ekonomiyi ve toplumsal yapıyı derinden değiştirirken aynı zamanda da söz konusu faktörlerden etkilenerek ihtiyaçlar doğrultusunda gelişim göstermiştir. Dijitalleşme ile birlikte siber-fiziksel sistemler, nesnelerin interneti (IoT), bulut bilişim, yapay zekâ ve büyük veri analitiği gibi ileri teknolojileri kullanarak geleneksel üretim yaklaşımlarını kökten değiştiren Endüstri 4.0 devrimi aynı zamanda endüstrinin evrilmesini de ifade etmektedir. Endüstri 4.0'ın temel prensibini oluşturan tam otomasyon ve yapay zekâ birçok sektörde insan faktörünü ikinci planda bırakmaktadır. İnsan ve makine arasındaki iş birliği eksikliği, kişiselleştirilmiş üretim ihtiyacı ve çevre odaklı sürdürülebilir üretim anlayışı Endüstri 5.0 a olan ihtiyacı doğurmuştur. Pandemi ve sonrasında yaşanan sosyo-ekonomik krizler küresel tedarik zincirindeki kırılabilirliği kanıtlarken, küresel ölçekte ekonomik esnekliğin olması gerektiğini ortaya koymuştur. Endüstri 5.0 ile yerel üretimi artırarak tedarik zincirine olan bağımlılığın azalması öngörülmektedir. Ayrıca insan merkezli üretim ile olası kriz durumlarında daha esnek üretim modelleri sürekliliği sağlayacaktır. Özellikle esnek üretim hatları ani talep değişikliklerini ve olası kriz senaryolarına karşı avantaj sağlayacaktır. Endüstri 5.0 İş gücünün makinelerle birlikte daha verimli çalışmasını sağlayacak iş modelleri oluşturarak daha kısa çalışma saatleri ve iş-yaşam dengesini destekleyecektir. Bu durum toplumsal refahın gelişimine katkı sağlayacaktır. Bu noktada vurgulamak gereken en önemli husus, söz konusu gelişmelere paralel olarak geliştirilmesi gereken altyapı imkanlarının yanı sıra gerekli bilgi ve beceriye sahip nitelikli işgücünün sağlanması için eğitim sistemlerinin revize edilerek geliştirilmesidir. Bu durum akabinde olası toplumsal sorunların yaşanmaması noktasında önem arz etmektedir.

## KAYNAKÇA

- Aba Şenbayram E. (2024). BRICS Ülkelerinde Endüstri 4.0 Döneminin Ekonomik Büyümeye Yansımaları. *KMÜ Sosyal ve Ekonomik Araştırmalar Dergisi*, 26(47), 1435-1454.
- A. Şenbayram, E. (2022). Sürdürülebilir Kalkınma Perspektifinden Yeşil Finans. *Social Sciences Research Journal*, 11 (3), 399-409.
- Bartodziej C.J., (2017). The Concept Industry 4.0-An Empirical Analysis of Technologies and Applications in Production Logistics, *Springer Gabler*.
- Baum, S. D. (2020). Social choice ethics in artificial intelligence. *AI & SOCIETY*, 35(1), 165-176
- Bayram, F. Ç. ve Karadaş, H. A. (2023). Endüstri 4.0 Teknolojilerinin Sürdürülebilir Ekonomi Üzerine Etkisi: Seçili OECD Ülkeleri Üzerine Bir Analiz, *Journal of Social, Humanities and Administrative Sciences*, 9(67), 3343-3352.
- Bostrom, N., Yudkowsky, E. (2014). The Ethics of Artificial Intelligence. *The Cambridge Handbook of Artificial Intelligence*, 1, 316-334.
- Bulut, E., ve Akçacı, T. (2017). Endüstri 4.0 ve İnovasyon Göstergeleri Kapsamında Türkiye Analizi. *ASSAM Uluslararası Hakemli Dergi*, 4(7), 55-77.
- Dünya Ekonomik Forumu (WEF), (2015). Readiness for the Future of Production Report, FOP\_Readiness\_Report\_2018.pdf (weforum.org), (Erişim Tarihi: 04.02.2025)
- Eşiyok, S., ve Demircioğlu, M. (2022). OECD ülkelerinin endüstri 4.0 düzeylerinin Critic ve Coda yöntemleri ile değerlendirilmesi. **İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi**, 21(43)
- Fırat, O. Z., ve Fırat, S. Ü. (2017). Endüstri 4.0 Yolculuğunda Trendler ve Robotlar, **İstanbul Üniversitesi İşletme Fakültesi Dergisi**, 46(2), 211-223.
- Günther, N., Prell B., Stephan, J. R. (2022). Industrie 5.0- von der Vision des menschenzentrierten Ansatzes zu soziocyberphysischen Produktionssystemen <https://doi.org/10.33968/2022.26>
- Elangovan, U. (2021). *Industry 5.0: The Future of the Industrial Economy*. USA: CRC Press. <https://doi.org/10.1201/9781003190677>
- Mustafa Ş. (2023) Endüstri 4.0 Kavramsal Çerçeve ve Ülke Uygulamaları, TBMM Araştırma Hizmetleri Başkanlığı Yayınları, 16, 4bc0f960-acbf-4a-bc-a366-2271f6cca948.pdf (tbmm.gov.tr) (Erişim tarihi 04.02.2025)
- Menendez, M. H., Menendez, R. M., Escobar, C. A. ve MCGovern, M. (2020). Competencies For Industry 4.0. *International Journal on Interactive Design and Manufacturing (IJIDEM)*, 14, 1511-1524.
- Nahavandi, S. (2019). Industry 5.0—A Human-Centric Solution. *Sustainability*, 11(16), 1-13. <https://doi.org/10.3390/su11164371>

Ryan, M., Stahl, B. C. (2020). Artificial Intelligence Ethics Guidelines For Developers And Users: Clarifying Their Content And Normative Implications. Journal of Information, Communication and Ethics in Society.

Verl, A. (2017). Robotics & Industrie 4.0. IFR- International Federation of Robotics



# BÖLÜM 4

## BORSA İSTANBUL'DA İŞLEM GÖREN ENERJİ ŞİRKETLERİNİN FİNANSAL DURUMLARININ TOPSIS YÖNTEMİYLE İNCELENMESİ

*Samet BÜYÜKYILMAZ<sup>1</sup>*

*Ayşegül AK<sup>2</sup>*

1 "Bu çalışma, Başkent Üniversitesi Sosyal Bilimler Enstitüsü İşletme Anabilim Dalı'nda yürütülen ve danışmanlığını Dr. Öğretim Üyesi Ayşegül Ak'ın yaptığı "BİST'TE İŞLEM GÖREN ENERJİ ŞİRKETLERİNİN FİNANSAL PERFORMANSLARININ İNCELENMESİ VE SÜRDÜRÜLEBİLİRLİK AÇISINDAN BORSA PERFORMANSLARININ DEĞERLENDİRİLMESİ" başlıklı tez çalışmasından faydalanılarak oluşturulmuştur."

Uzman, Ankara Ticaret Odası, Orcid: 0009-0001-4830-9344, sametbuyukyilmaz@outlook.com.tr

2 Dr. Öğretim Üyesi, Başkent Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, İşletme Bölümü, Orcid: 0000-0003-1434-3103, aysegulak@baskent.edu.tr

## 1. GİRİŞ

Şirketlerin etkili kaynak yönetimi, stratejik karar alma ve rekabetçi unsurları sağlamlaları için finansal performansı ölçmek esastır. Bir şirketin finansal sağlığının kapsamlı bir görünümünü sağlayarak risk tanımlamasına ve uzun vadeli büyümeye yardımcı olan finansal performans ölçümü, şirketler için finansal sağlıklarına ilişkin öngörüler sağladığı, karar almaya rehberlik ettiği ve stratejik hedeflere ulaşmalarına yardımcı olduğu için hayati önem taşır. Finansal performans ölçümü, bir şirketin kaynakları etkili bir şekilde yönetme ve karlılık elde etme yeteneğini değerlendirmek için çeşitli finansal metrikleri değerlendirmeyi içerir. Şirketlerin finansal tablolarından alınan bilançolar ve gelir tabloları genellikle finansal performansı ölçmek için kullanılır. Finansal performans, şirketler tarafından ölçülmesi ve değerlendirilmesi gereken bir unsurdur. Şirketlerin finansal performansını incelemek için cari oranları, hisse başına kazançları, net kar marjları ve hisse senedi devir oranları finansal veriler kullanılarak hesaplanır.

Bu çalışmada, Borsa İstanbul Elektrik Endeksi'nde (BIST XELKT) yer alan 30 enerji şirketinin finansal performanslarının çok kriterli karar alma yöntemlerinden biri olan TOPSIS yöntemi ile ölçülmesi amaçlanmıştır. Mali performans ve faaliyet sonuçlarının analiz edilebilmesi ve şirketlerin hedefleri ile uyumlu olacak kararların alınabilmesi için karar veren kişilerin elinde bu durumu değerlendirebilmesini sağlayacak analitik enstrümanlar gereklidir ve bu amaçla oluşturulan yöntemlerden birinin uygulamaya aktarılması sağlanmış olmaktadır.

## 2. VERİ SETİ ve YÖNTEM

Aralık 2023 tarihinde Borsa İstanbul Elektrik Endeksinde (BİST XELKT) yer alan 30 adet enerji şirketinin finansal performanslarının çok kriterli karar verme yöntemlerinden TOPSIS yöntemiyle ölçülüp karşılaştırılması amacı doğrultusunda şirketlerin 2020 dönemini içeren yıllık verilerden oluşan Uluslararası Finansal Raporlama Standartları'na uyumlu bilanço ve gelir tablolarındaki finansal verileri kullanılarak "Cari Oran, Asit-Test Oranı, Finansman Oranı, Aktif Devir Hızı, Alacak Devir Hızı, Aktif Karlılığı, Öz Kaynak Karlılığı, Finansal Kaldıraç Oranı, KVKYK / Aktif Toplamı, Finansman Giderleri / Net Satışlar" oranları hesaplanmış ve TOPSIS tekniği kullanılmıştır. Bu yöntemin ağırlıklı standart karar matrisinin oluşturulması aşamasında kullanılan performans kriterlerinin ağırlık değerleri, CRITIC ağırlıklandırma yöntemi ile hesaplanmıştır. Sonrasında bu oranlar, şirketlerin performansını belirten bir puana dönüştürülmüştür. Bu puanlarla şirketlerin sıralaması ve derecelendirmesi bulu-



arak karřılařtırma yapılmıřtır. Halka aık řirketler mali verilerini Kamuyu Aydınlatma Platformu (KAP) üzerinden yayınladıęı iin bu alıřmada mali veriler KAP'tan alınmıřtır. Verilerin toplanması ve analizi ařamalarında Microsoft Office 365 Excel programı kullanılmıřtır.

*Tablo1: Arařtırmaya Dahil Edilen řirketler*

| NO | ENDEKS | BİST KODU | řİRKET İSİMİ  |
|----|--------|-----------|---|
| 1  | XELKT  | AHGAZ     | Ahlatıcı Doęal Gaz Daęıtım Enerji ve Yatırım A.ř.                 |
| 2  | XELKT  | AKENR     | Akenerji Elektrik Üretim A.ř.                                     |
| 3  | XELKT  | AKFYE     | Akfen Yenilenebilir Enerji A.ř.                                   |
| 4  | XELKT  | AKSEN     | Aksa Enerji Üretim A.ř.   |
| 5  | XELKT  | AKSUE     | Aksu Enerji ve Ticaret A.ř.                                       |
| 6  | XELKT  | ALFAS     | Alfa Solar Enerji San. ve Tic. A.ř.                               |
| 7  | XELKT  | ARASE     | Doęu Aras Enerji Yatırımları A.ř.                                 |
| 8  | XELKT  | AYDEM     | Aydem Yenilenebilir Enerji A.ř.                                   |
| 9  | XELKT  | AYEN      | Ayen Enerji A.ř.  |
| 10 | XELKT  | BIOEN     | Biotrend Çevre ve Enerji Yatırımları A.ř.                         |
| 11 | XELKT  | CANTE     | an2 Termik A.ř.  |
| 12 | XELKT  | CATES     | ates Elektrik Üretim A.ř.  |
| 13 | XELKT  | CONSE     | Consus Enerji İřletmecilięi ve Hizmetleri A.ř.                    |
| 14 | XELKT  | CWENE     | Cw Enerji Mühendislik Tic. ve San. A.ř.                           |
| 15 | XELKT  | ENERY     | Enerya Enerji A.ř.  |
| 16 | XELKT  | ENJSA     | Enerjisa Enerji A.ř.  |
| 17 | XELKT  | ESEN      | Esenboęa Elektrik Üretim A.ř.                                     |
| 18 | XELKT  | GWIND     | Galata Wind Enerji A.ř.   |
| 19 | XELKT  | HUNER     | Hun Yenilenebilir Enerji Üretim A.ř.                              |
| 20 | XELKT  | IZENR     | İzdemir Enerji Elektrik Üretim A.ř.                               |
| 21 | XELKT  | KARYE     | Kartal Yenilenebilir Enerji Üretim A.ř.                           |
| 22 | XELKT  | MAGEN     | Margün Enerji Üretim San. ve Tic. A.ř.                            |
| 23 | XELKT  | NATEN     | Naturel Yenilenebilir Enerji A.ř.                                 |
| 24 | XELKT  | NTGAZ     | Naturel gaz Sanayi ve Ticaret A.ř.                                |
| 25 | XELKT  | ODAS      | Odař Elektrik Üretim San. Tic. A.ř.                               |
| 26 | XELKT  | PAMEL     | Pamukova Yenilenebilir Elektrik Üretimi A.ř.                      |
| 27 | XELKT  | SMRTG     | Smart Güneř Enerjisi Teknolojileri Ar-Ge Üretim San. ve Tic. A.ř. |
| 28 | XELKT  | TATEN     | Tatlıpınar Enerji Üretim A.ř.                                     |
| 29 | XELKT  | ZEDUR     | Zedur Enerji Elektrik Üretim A.ř.                                 |
| 30 | XELKT  | ZOREN     | Zorlu Enerji Elektrik Üretim A.ř.                                 |

## 2.1. Finansal Oran Analizi

Finansal oran analizi, řirketlerin finansal tablolarındaki hesaplar arasındaki iliřkileri inceleyerek, faaliyetlerini ve mali durumlarını deęerlendirmelerini saęlayan bir yöntemdir. řirketlerin benzer sektörlerdeki dięer

şirketlerle kıyaslanmasına ve geleceğe yönelik stratejik hedefler belirlemesine yardımcı olur (Çiftçi ve Yıldırım, 2020).

- Cari Oran: Şirketin kısa vadeli borçlarını karşılama gücünü gösterir.  $\text{Cari Oran} = \frac{\text{Dönen Varlıklar}}{\text{Kısa Vadeli Yabancı Kaynaklar}}$  (Akdoğan ve Tenker, 2010).
- Asit-Test Oranı: Cari oranı tamamlar.  $\text{Cari Varlıklar} - \text{Stoklar} / \text{Kısa Vadeli Yabancı Kaynaklar}$  formülü ile hesaplanır. Genellikle 1'in üzeri kabul edilir (Çabuk ve Lazol, 2014).
- Finansman Oranı:  $\text{Hazır Değerler} + \text{Menkul Kıymetler} / \text{Kısa Vadeli Yabancı Kaynaklar}$  formülü ile hesaplanır. Kısa vadeli borçların ne kadarının nakit değerlerle karşılanabileceğini gösterir. Genellikle 0.20 seviyesinin yeterli olduğu kabul edilir (Çabuk ve Lazol, 2014).
- Aktif Devir Hızı:  $\text{Net Satışlar} / \text{Toplam Aktifler}$  formülü ile hesaplanır. Şirketin varlıklarını ne kadar etkin kullandığını gösterir (Bülbül ve Köse, 2012).
- Alacak Devir Hızı:  $\text{Net Satışlar} / \text{Ortalama Ticari Alacaklar}$  formülü ile hesaplanır. Yüksek bir oran, alacakların likiditesinin iyi olduğunu gösterir.
- Aktif Karlılığı:  $\text{Net Kâr} / \text{Toplam Aktifler}$  ile hesaplanır. Şirketin varlıklarını ne kadar verimli kullandığını gösterir.
- Özsermaye Karlılığı:  $\text{Net Kâr} / \text{Özsermaye}$  formülü ile hesaplanır. Şirketin yatırımcılarının sermayesini ne kadar kârlı kullandığını gösterir (Onocak, 2023).
- Finansal Kaldıraç Oranı:  $\text{Toplam Yabancı Kaynaklar} / \text{Toplam Aktifler}$  ile hesaplanır. Şirketin ne kadar borçla finanse edildiğini gösterir. %50 oranı genellikle yeterli kabul edilir (Çabuk ve Lazol, 2014).
- STFR / Toplam Aktifler: Kısa vadeli borçların toplam borçlara oranını gösterir.
- Finansman Giderleri / Net Satışlar: Şirketin borçlanma maliyetini göstermektedir.

## 2.2. CRITIC Ağırlıklandırma Yöntemi

CRITIC yöntemi, farklı kriterlerin ağırlıklarını belirlemek için 1995 yılında Diakoulaki ve arkadaşları tarafından geliştirilmiştir. Bu yöntem, kriterlerin varyasyonlarını ve birbirleriyle olan korelasyonlarını değerlendirir.

CRITIC yöntemi řu 5 adımdan oluşur:

1. Karar matrisinin oluşturulması
2. Normalizasyon işlemi
3. Korelasyon katsayılarının hesaplanması
4. Bilgi miktarının hesaplanması
5. Kriter aęırlıklarının belirlenmesi

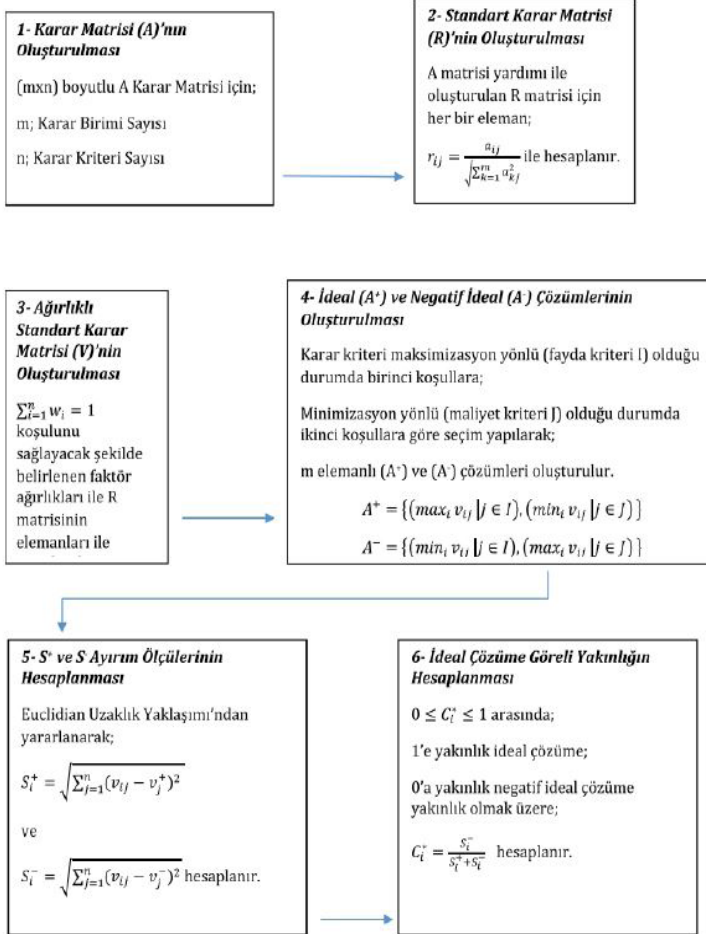
### 2.3. TOPSIS Yöntemi

TOPSIS yöntemi, en iyi ve en kötü alternatifleri belirleyerek řirketleri sıralamaya yarayan bir karar verme yöntemidir. En iyi seçenek pozitif ideal çözüme (PIC) en yakın, negatif ideal çözüme (NIC) en uzak olan seçenektir.

TOPSIS yöntemi 6 aşamadan oluşur:

1. Karar matrisinin oluşturulması
2. Matrisin normalize edilmesi
3. Aęırlıklı karar matrisinin hesaplanması
4. Pozitif ve negatif ideal çözümlerin belirlenmesi
5. Euclidean mesafelerinin hesaplanması
6. řirketlerin sıralanması

TOPSIS yöntemine göre performans deęerlemesi 6 aşamadan oluşmaktadır. řekil 1'de bu adımlar gösterilmiştir ((Durmuşkaya ve Kavas, 2019; Onocak, 2023; Sakarya vd., 2015;Yükçü ve Ataęan, 2010).



Şekil 16. TOPSIS Tekniğinin İşlem Aşamaları

Bu yöntem pozitif ideal çözüm (PİÇ) ve negatif ideal çözüm (NİÇ) olmak üzere iki temel noktaya dayanmaktadır. Yöntem, PİÇ'e en kısa mesafe ve NİÇ'e en uzak mesafedeki seçeneği belirlemeyi amaçlamaktadır. Bu yöntemle aslında tüm seçeneklerin PİÇ ve NİÇ'e olan uzaklıkları hesaplanmaktadır. PİÇ'e en yakın ve NİÇ'e en uzak mesafede olan seçenek en iyi karar seçeneği olarak kabul edilmektedir (Hwang ve Yoon, 1981; Cheng vd., 2002).

İdeal ya da PİÇ olarak ifade edilen en iyi çözüm; maliyet kriterini minimize, fayda kriterini ise maksimize eden çözümdür. İdeal olmayan ya da negatif çözüm ise; fayda kriterini minimize, maliyet kriterini ise maksimize eden çözümdür (Özden, 2011; Wang ve Elhag, 2006). TOPSIS ile tüm karar seçeneklerinin, PİÇ ve NİÇ'den olan görecek uzaklıkları öklid

uzaklıęı ile yardımıyla hesaplanır ve her bir kriterin sıradan bir řekilde azalan ya da artan fayda eğilimine sahip olduęu kabul edilir(Özden, 2011).

Kriterlerin aęırlıklarının belirlenebilmesi için bu yöntemde bir uygulama yoktur(Janic, 2003). Bu işlem için daha çok 1'den 5'e kadar veya 1'den 9'a kadar ya da daha farklı puan cetveli veya SWARA, AHS, ENTROPY, DEMATEL veya AAS gibi yöntemleri kullanmak mümkün olmaktadır(Özbek, 2021:228). Ayrıca literatürde CRITIC yöntemi de kullanılmaktadır.

Bu yöntem çoęu sektör için kullanılabileceęi gibi finans alanında da kullanılmaktadır(Sakarya ve Yıldırım, 2016). Çok amaçlı karar verme yöntemlerinden en yaygın kullanılan TOPSIS yöntemi ile sektörün mali performansı analiz edilerek, BİST'te işlem gören enerji řirketleri derecelendirilmektedir (Sakarya vd., 2015). İşletmelerin performanslarının deęerlendirilmesi, işletmelerin hem kendi performans durumlarını görmeleri hem de sektördeki yerlerini bilmeleri açısından önemlidir. TOPSIS yöntemi bu anlamda řirketlerin gerçek durumlarını görmelerine olanak veren ve performans deęerlemede sıklıkla kullanılan bir yöntemdir (Durmuşkaya ve Kavas, 2019).

### 3. ANALİZ

Analiz yapılırken CRITIC ve TOPSIS teknikleri birlikte kullanılmıştır. TOPSIS yönteminin aęırlıklı standart karar matrisinin oluşturulması aşamasında kullanılan performans kriterlerinin aęırlık deęerleri, CRITIC yöntemi ile hesaplanmıştır.

2020 verileri kullanılarak, CRITIC yönteminin işlem adımları olan karar matrisi, normalize matris, korelasyon katsayısı matrisinin oluşturulması,  $C_j$  ve  $W_j$  deęerlerinin sonuçlarına ařaęıda yer verilmiştir. Tablo 2'de, CRITIC yönteminin 1. adımı olan karar matrisi (30x10) oluşturulmuştur

Tablo 2: Karar Matrisinin Oluşturulması

|    |       | P1     | P2     | P3      | P4     | P5      | P6      | P7      | P8     | P9     | P10    |
|----|-------|--------|--------|---------|--------|---------|---------|---------|--------|--------|--------|
| 1  | AHGZ  | 0,4336 | 0,4263 | -0,1853 | 1,2227 | 6,0887  | 0,0181  | -0,0797 | 1,2274 | 0,7861 | 0,0867 |
| 2  | AKENR | 0,5982 | 0,5888 | -0,0187 | 0,3248 | 22,2693 | -0,1611 | -8,4346 | 1,0191 | 0,0906 | 0,5950 |
| 3  | AKFYE | 0,7936 | 0,7925 | 0,4869  | 0,1214 | 9,7891  | -0,0361 | -0,1101 | 0,6725 | 0,0993 | 0,8189 |
| 4  | AKSEN | 1,0504 | 1,0084 | 0,9483  | 0,7609 | 2,6724  | 0,0587  | 0,1206  | 0,5133 | 0,3470 | 0,0943 |
| 5  | AKSUE | 0,1925 | 0,1751 | 0,2538  | 0,1992 | 6,5621  | -0,1116 | -0,5516 | 0,7976 | 0,2309 | 1,4081 |
| 6  | ALFAS | 1,4490 | 1,1661 | 0,4685  | 1,2858 | 4,4329  | 0,2139  | 0,6704  | 0,6810 | 0,6412 | 0,0455 |
| 7  | ARASE | 1,1817 | 1,1374 | 1,0026  | 1,2429 | 11,6006 | 0,2076  | 0,4147  | 0,4993 | 0,4404 | 0,0460 |
| 8  | AYDEM | 0,3585 | 0,3493 | 0,8959  | 0,1075 | 24,3988 | -0,0455 | -0,0963 | 0,5275 | 0,0728 | 1,0769 |
| 9  | AYEN  | 0,3436 | 0,3436 | 0,3550  | 0,1710 | 10,0850 | -0,0300 | -0,1146 | 0,7380 | 0,1782 | 0,5790 |
| 10 | BIOEN | 1,0694 | 1,0495 | 0,3253  | 0,3011 | 8,1221  | 0,0613  | 0,2496  | 0,7545 | 0,2718 | 0,2597 |
| 11 | CANTE | 0,4879 | 0,2936 | 0,4036  | 0,2683 | 7,3389  | 0,0136  | 0,0471  | 0,7125 | 0,2387 | 0,9493 |
| 12 | CATES | 0,0797 | 0,0701 | -0,6990 | 0,6099 | 7,8730  | -0,4403 | -0,1896 | 3,3221 | 3,1485 | 0,7759 |
| 13 | CONSE | 0,4268 | 0,2688 | 0,3676  | 0,3529 | 11,3577 | 0,0019  | 0,0070  | 0,7312 | 0,3638 | 0,2539 |
| 14 | CWENE | 1,2889 | 0,8283 | 0,6957  | 0,9841 | 7,5707  | 0,0564  | 0,1375  | 0,5897 | 0,3798 | 0,0856 |
| 15 | ENERY | 0,4365 | 0,4292 | -0,1843 | 1,2213 | 6,0888  | 0,0184  | -0,0813 | 1,2259 | 0,7851 | 0,0867 |
| 16 | ENJSA | 0,8269 | 0,8064 | 0,4082  | 0,8817 | 7,3912  | 0,0441  | 0,1521  | 0,7101 | 0,3359 | 0,0639 |
| 17 | ESEN  | 1,3398 | 1,2278 | 0,9189  | 0,1167 | 11,3864 | 0,0662  | 0,1381  | 0,5211 | 0,1602 | 0,6790 |
| 18 | GWIND | 0,5669 | 0,5614 | 1,3373  | 0,2051 | 9,5494  | 0,0965  | 0,1686  | 0,4278 | 0,1867 | 0,2274 |
| 19 | HUNER | 0,1503 | 0,1474 | 0,4956  | 0,0790 | 8,5170  | 0,0039  | 0,0118  | 0,6686 | 0,1634 | 1,7455 |
| 20 | IZENR | 0,2846 | 0,0419 | 0,4475  | 0,4454 | 30,8082 | -0,0659 | -0,2131 | 0,6908 | 0,4785 | 0,2954 |
| 21 | KARYE | 0,4090 | 0,4090 | 1,1533  | 0,0994 | 7,6687  | 0,0453  | 0,0845  | 0,4644 | 0,0337 | 1,2276 |
| 22 | MAGEN | 0,7082 | 0,6985 | 0,7305  | 0,0806 | 12,4582 | 0,0696  | 0,1649  | 0,5779 | 0,1754 | 0,9339 |
| 23 | NATEN | 2,4714 | 2,2909 | 1,2262  | 0,1059 | 10,2744 | 0,0749  | 0,1359  | 0,4492 | 0,0909 | 0,7086 |
| 24 | NTGAZ | 0,9079 | 0,8147 | 1,3956  | 1,1291 | 6,3017  | 0,2246  | 0,3856  | 0,4174 | 0,3223 | 0,0768 |
| 25 | ODAS  | 0,4676 | 0,2921 | 0,3011  | 0,2863 | 6,1058  | -0,0731 | -0,3161 | 0,7686 | 0,3240 | 0,8730 |
| 26 | PAMEL | 1,8087 | 1,8087 | 1,4929  | 0,1245 | 34,0789 | 0,0583  | 0,0973  | 0,4011 | 0,0170 | 1,2566 |
| 27 | SMRTG | 1,1403 | 0,9514 | 0,1469  | 1,0028 | 2,8877  | 0,0999  | 0,7800  | 0,8719 | 0,7599 | 0,0305 |
| 28 | TATEN | 5,1472 | 5,1472 | 0,1258  | 0,0441 | 3,5685  | -0,0679 | -0,7375 | 0,7320 | 0,0197 | 1,6591 |
| 29 | ZEDUR | 0,9139 | 0,9139 | 0,1477  | 0,1246 | 64,0650 | -0,1134 | -0,8813 | 0,8713 | 0,8592 | 1,9115 |
| 30 | ZOREN | 0,4938 | 0,4851 | 0,1202  | 0,4008 | 5,8470  | 0,0018  | 0,0166  | 0,8927 | 0,3751 | 0,3099 |

CRITIC yönteminin 2. adımı olan fayda yönlü ve maliyet yönlü kriterlere göre normalize edilmiş matrise Tablo 3'te yer verilmiştir.

Tablo 3: Normalize Matrisin Oluřturulması

|    | P1    | P2     | P3     | P4     | P5     | P6     | P7     | P8     | P9     | P10    |        |
|----|-------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|
| 1  | AHGAZ | 0,0698 | 0,0753 | 0,2344 | 0,9491 | 0,0556 | 0,6894 | 0,9067 | 0,7171 | 0,7544 | 0,9701 |
| 2  | AKENR | 0,1023 | 0,1071 | 0,3103 | 0,2261 | 0,3192 | 0,4200 | 0,0000 | 0,7884 | 0,9765 | 0,6999 |
| 3  | AKFYE | 0,1409 | 0,1470 | 0,5410 | 0,0622 | 0,1159 | 0,6080 | 0,9034 | 0,9071 | 0,9737 | 0,5809 |
| 4  | AKSEN | 0,1915 | 0,1893 | 0,7515 | 0,5772 | 0,0000 | 0,7505 | 0,9284 | 0,9616 | 0,8946 | 0,9661 |
| 5  | AKSUE | 0,0223 | 0,0261 | 0,4347 | 0,1249 | 0,0634 | 0,4943 | 0,8555 | 0,8643 | 0,9317 | 0,2676 |
| 6  | ALFAS | 0,2702 | 0,2202 | 0,5326 | 1,0000 | 0,0287 | 0,9838 | 0,9881 | 0,9042 | 0,8007 | 0,9920 |
| 7  | ARASE | 0,2175 | 0,2146 | 0,7763 | 0,9655 | 0,1454 | 0,9745 | 0,9604 | 0,9664 | 0,8648 | 0,9918 |
| 8  | AYDEM | 0,0550 | 0,0602 | 0,7276 | 0,0510 | 0,3539 | 0,5938 | 0,9049 | 0,9568 | 0,9822 | 0,4437 |
| 9  | AYEN  | 0,0521 | 0,0591 | 0,4809 | 0,1022 | 0,1207 | 0,6170 | 0,9029 | 0,8847 | 0,9485 | 0,7084 |
| 10 | BIOEN | 0,1953 | 0,1974 | 0,4673 | 0,2069 | 0,0888 | 0,7544 | 0,9424 | 0,8790 | 0,9186 | 0,8781 |
| 11 | CANTE | 0,0806 | 0,0493 | 0,5030 | 0,1806 | 0,0760 | 0,6826 | 0,9205 | 0,8934 | 0,9292 | 0,5115 |
| 12 | CATES | 0,0000 | 0,0055 | 0,0000 | 0,4556 | 0,0847 | 0,0000 | 0,8948 | 0,0000 | 0,0000 | 0,6037 |
| 13 | CONSE | 0,0685 | 0,0444 | 0,4866 | 0,2487 | 0,1415 | 0,6651 | 0,9161 | 0,8870 | 0,8893 | 0,8812 |
| 14 | CWENE | 0,2386 | 0,1540 | 0,6363 | 0,7570 | 0,0798 | 0,7470 | 0,9303 | 0,9354 | 0,8841 | 0,9707 |
| 15 | ENERY | 0,0704 | 0,0759 | 0,2348 | 0,9480 | 0,0556 | 0,6898 | 0,9065 | 0,7176 | 0,7547 | 0,9701 |
| 16 | ENJSA | 0,1474 | 0,1497 | 0,5051 | 0,6746 | 0,0769 | 0,7285 | 0,9319 | 0,8942 | 0,8982 | 0,9823 |
| 17 | ESEN  | 0,2487 | 0,2323 | 0,7381 | 0,0584 | 0,1419 | 0,7617 | 0,9303 | 0,9589 | 0,9543 | 0,6552 |
| 18 | GWIND | 0,0961 | 0,1018 | 0,9290 | 0,1297 | 0,1120 | 0,8073 | 0,9337 | 0,9909 | 0,9458 | 0,8953 |
| 19 | HUNER | 0,0139 | 0,0207 | 0,5450 | 0,0281 | 0,0952 | 0,6681 | 0,9166 | 0,9084 | 0,9533 | 0,0882 |
| 20 | IZENR | 0,0404 | 0,0000 | 0,5231 | 0,3232 | 0,4583 | 0,5631 | 0,8922 | 0,9008 | 0,8526 | 0,8592 |
| 21 | KARYE | 0,0650 | 0,0719 | 0,8451 | 0,0445 | 0,0814 | 0,7303 | 0,9245 | 0,9783 | 0,9947 | 0,3636 |
| 22 | MAGEN | 0,1240 | 0,1286 | 0,6521 | 0,0294 | 0,1594 | 0,7669 | 0,9332 | 0,9395 | 0,9494 | 0,5197 |
| 23 | NATEN | 0,4720 | 0,4405 | 0,8783 | 0,0498 | 0,1238 | 0,7748 | 0,9301 | 0,9835 | 0,9764 | 0,6395 |
| 24 | NTGAZ | 0,1634 | 0,1514 | 0,9556 | 0,8737 | 0,0591 | 1,0000 | 0,9572 | 0,9944 | 0,9025 | 0,9754 |
| 25 | ODAS  | 0,0766 | 0,0490 | 0,4562 | 0,1950 | 0,0559 | 0,5522 | 0,8811 | 0,8742 | 0,9019 | 0,5521 |
| 26 | PAMEL | 0,3412 | 0,3461 | 1,0000 | 0,0648 | 0,5116 | 0,7499 | 0,9259 | 1,0000 | 1,0000 | 0,3482 |
| 27 | SMRTG | 0,2093 | 0,1781 | 0,3859 | 0,7721 | 0,0035 | 0,8124 | 1,0000 | 0,8388 | 0,7628 | 1,0000 |
| 28 | TATEN | 1,0000 | 1,0000 | 0,3763 | 0,0000 | 0,0146 | 0,5600 | 0,8353 | 0,8867 | 0,9991 | 0,1342 |
| 29 | ZEDUR | 0,1646 | 0,1708 | 0,3863 | 0,0648 | 1,0000 | 0,4916 | 0,8197 | 0,8390 | 0,7311 | 0,0000 |
| 30 | ZOREN | 0,0817 | 0,0868 | 0,3737 | 0,2873 | 0,0517 | 0,6649 | 0,9172 | 0,8317 | 0,8856 | 0,8514 |

CRITIC ynteminin 3.adımı olan kriterler arasındaki iliřkinin de-  
recesini lmek iin kullanılan korelasyon katsayı matrisi Tablo 4'te  
gsterilmiřtir.

Tablo 4: Korelasyon Katsayı Matrisinin Oluşturulması

|     | P1      | P2      | P3      | P4      | P5      | P6      | P7      | P8      | P9      | P10     |
|-----|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|
| P1  | 1,0000  | 0,9932  | 0,1638  | -0,0966 | -0,0662 | 0,1882  | 0,0367  | 0,2313  | 0,2454  | -0,1897 |
| P2  | 0,9932  | 1,0000  | 0,1531  | -0,1354 | -0,0503 | 0,1580  | 0,0154  | 0,2133  | 0,2454  | -0,2330 |
| P3  | 0,1638  | 0,1531  | 1,0000  | -0,1700 | 0,0641  | 0,6590  | 0,2712  | 0,7454  | 0,5948  | 0,0147  |
| P4  | -0,0966 | -0,1354 | -0,1700 | 1,0000  | -0,3204 | 0,3735  | 0,1742  | -0,1710 | -0,3417 | 0,7449  |
| P5  | -0,0662 | -0,0503 | 0,0641  | -0,3204 | 1,0000  | -0,2356 | -0,2458 | 0,0653  | -0,0024 | -0,4440 |
| P6  | 0,1882  | 0,1580  | 0,6590  | 0,3735  | -0,2356 | 1,0000  | 0,3954  | 0,7569  | 0,5705  | 0,4294  |
| P7  | 0,0367  | 0,0154  | 0,2712  | 0,1742  | -0,2458 | 0,3954  | 1,0000  | 0,1293  | -0,0897 | 0,1331  |
| P8  | 0,2313  | 0,2133  | 0,7454  | -0,1710 | 0,0653  | 0,7569  | 0,1293  | 1,0000  | 0,9308  | -0,0036 |
| P9  | 0,2454  | 0,2454  | 0,5948  | -0,3417 | -0,0024 | 0,5705  | -0,0897 | 0,9308  | 1,0000  | -0,1245 |
| P10 | -0,1897 | -0,2330 | 0,0147  | 0,7449  | -0,4440 | 0,4294  | 0,1331  | -0,0036 | -0,1245 | 1,0000  |

CRITIC yönteminin 4.adımı olan her bir kriterde bulunan toplam bilgi miktarını ifade eden  $C_j$  değerini hesaplamak için öncelikle Tablo 3'ta yer alan değerler 1'den çıkarılır. Normalize matristeki değerler kullanılarak standart sapma değerleri bulunur ve 4.adımda yer alan denklem kullanılır. Sonuçlara Tablo 5'te yer verilmiştir.

( $\sigma_j$ : Standart Sapma)

Tablo 5:  $C_j$  Değerinin Hesaplanması

|            | P1     | P2     | P3     | P4     | P5     | P6     | P7     | P8     | P9     | P10    |
|------------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|
| P1         | 0,0000 | 0,0068 | 0,8362 | 1,0966 | 1,0662 | 0,8118 | 0,9633 | 0,7687 | 0,7546 | 1,1897 |
| P2         | 0,0068 | 0,0000 | 0,8469 | 1,1354 | 1,0503 | 0,8420 | 0,9846 | 0,7867 | 0,7546 | 1,2330 |
| P3         | 0,8362 | 0,8469 | 0,0000 | 1,1700 | 0,9359 | 0,3410 | 0,7288 | 0,2546 | 0,4052 | 0,9853 |
| P4         | 1,0966 | 1,1354 | 1,1700 | 0,0000 | 1,3204 | 0,6265 | 0,8258 | 1,1710 | 1,3417 | 0,2551 |
| P5         | 1,0662 | 1,0503 | 0,9359 | 1,3204 | 0,0000 | 1,2356 | 1,2458 | 0,9347 | 1,0024 | 1,4440 |
| P6         | 0,8118 | 0,8420 | 0,3410 | 0,6265 | 1,2356 | 0,0000 | 0,6046 | 0,2431 | 0,4295 | 0,5706 |
| P7         | 0,9633 | 0,9846 | 0,7288 | 0,8258 | 1,2458 | 0,6046 | 0,0000 | 0,8707 | 1,0897 | 0,8669 |
| P8         | 0,7687 | 0,7867 | 0,2546 | 1,1710 | 0,9347 | 0,2431 | 0,8707 | 0,0000 | 0,0692 | 1,0036 |
| P9         | 0,7546 | 0,7546 | 0,4052 | 1,3417 | 1,0024 | 0,4295 | 1,0897 | 0,0692 | 0,0000 | 1,1245 |
| P10        | 1,1897 | 1,2330 | 0,9853 | 0,2551 | 1,4440 | 0,5706 | 0,8669 | 1,0036 | 1,1245 | 0,0000 |
|            |        |        |        |        |        |        |        |        |        |        |
|            |        |        |        |        |        |        |        |        |        |        |
| $\sigma_j$ | 0,1888 | 0,1869 | 0,2347 | 0,3474 | 0,2019 | 0,1880 | 0,1715 | 0,1795 | 0,1820 | 0,3014 |
|            |        |        |        |        |        |        |        |        |        |        |
| $C_j$      | 1,4146 | 1,4281 | 1,5268 | 3,1069 | 2,0667 | 1,0723 | 1,4033 | 1,0954 | 1,2687 | 2,6136 |

CRITIC yönteminin 5.adımı olan analiz için kullanılacak kriterlere ait ağırlıkları( $W_j$ ) hesaplamak için ilgili denklem kullanılır. Kriter ağırlıkları Tablo 6'da yer almaktadır.

Tablo 6: Kriter Ağırlıklarının Hesaplanması

| $W_j$ | 0,0832 | 0,0840 | 0,0898 | 0,1828 | 0,1216 | 0,0631 | 0,0826 | 0,0644 | 0,0746 | 0,1538 |
|-------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|
|-------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|



2020 verileri kullanılarak TOPSIS ynteminin iřlem adımları olan karar matrisi, standart karar matrisi, aęırlıklı standart karar matrisi, ideal ve negatif ideal zmlerin oluřturulması, ayırım llerinin hesaplanması ve ideal zme gre yakınlıęına ait sonulara ařaęıda yer verilmiřtir.

Tablo 7: Karar Matrisinin Oluřturulması

|    |       | P1     | P2     | P3      | P4     | P5      | P6      | P7      | P8     | P9     | P10    |
|----|-------|--------|--------|---------|--------|---------|---------|---------|--------|--------|--------|
| 1  | AHGAZ | 0,4336 | 0,4263 | -0,1853 | 1,2227 | 6,0887  | 0,0181  | -0,0797 | 1,2274 | 0,7861 | 0,0867 |
| 2  | AKENR | 0,5982 | 0,5888 | -0,0187 | 0,3248 | 22,2693 | -0,1611 | -8,4346 | 1,0191 | 0,0906 | 0,5950 |
| 3  | AKFYE | 0,7936 | 0,7925 | 0,4869  | 0,1214 | 9,7891  | -0,0361 | -0,1101 | 0,6725 | 0,0993 | 0,8189 |
| 4  | AKSEN | 1,0504 | 1,0084 | 0,9483  | 0,7609 | 2,6724  | 0,0587  | 0,1206  | 0,5133 | 0,3470 | 0,0943 |
| 5  | AKSUE | 0,1925 | 0,1751 | 0,2538  | 0,1992 | 6,5621  | -0,1116 | -0,5516 | 0,7976 | 0,2309 | 1,4081 |
| 6  | ALFAS | 1,4490 | 1,1661 | 0,4685  | 1,2858 | 4,4329  | 0,2139  | 0,6704  | 0,6810 | 0,6412 | 0,0455 |
| 7  | ARASE | 1,1817 | 1,1374 | 1,0026  | 1,2429 | 11,6006 | 0,2076  | 0,4147  | 0,4993 | 0,4404 | 0,0460 |
| 8  | AYDEM | 0,3585 | 0,3493 | 0,8959  | 0,1075 | 24,3988 | -0,0455 | -0,0963 | 0,5275 | 0,0728 | 1,0769 |
| 9  | AYEN  | 0,3436 | 0,3436 | 0,3550  | 0,1710 | 10,0850 | -0,0300 | -0,1146 | 0,7380 | 0,1782 | 0,5790 |
| 10 | BIOEN | 1,0694 | 1,0495 | 0,3253  | 0,3011 | 8,1221  | 0,0613  | 0,2496  | 0,7545 | 0,2718 | 0,2597 |
| 11 | CANTE | 0,4879 | 0,2936 | 0,4036  | 0,2683 | 7,3389  | 0,0136  | 0,0471  | 0,7125 | 0,2387 | 0,9493 |
| 12 | CATES | 0,0797 | 0,0701 | -0,6990 | 0,6099 | 7,8730  | -0,4403 | -0,1896 | 3,3221 | 3,1485 | 0,7759 |
| 13 | CONSE | 0,4268 | 0,2688 | 0,3676  | 0,3529 | 11,3577 | 0,0019  | 0,0070  | 0,7312 | 0,3638 | 0,2539 |
| 14 | CWENE | 1,2889 | 0,8283 | 0,6957  | 0,9841 | 7,5707  | 0,0564  | 0,1375  | 0,5897 | 0,3798 | 0,0856 |
| 15 | ENERY | 0,4365 | 0,4292 | -0,1843 | 1,2213 | 6,0888  | 0,0184  | -0,0813 | 1,2259 | 0,7851 | 0,0867 |
| 16 | ENJSA | 0,8269 | 0,8064 | 0,4082  | 0,8817 | 7,3912  | 0,0441  | 0,1521  | 0,7101 | 0,3359 | 0,0639 |
| 17 | ESEN  | 1,3398 | 1,2278 | 0,9189  | 0,1167 | 11,3864 | 0,0662  | 0,1381  | 0,5211 | 0,1602 | 0,6790 |
| 18 | GWIND | 0,5669 | 0,5614 | 1,3373  | 0,2051 | 9,5494  | 0,0965  | 0,1686  | 0,4278 | 0,1867 | 0,2274 |
| 19 | HUNER | 0,1503 | 0,1474 | 0,4956  | 0,0790 | 8,5170  | 0,0039  | 0,0118  | 0,6686 | 0,1634 | 1,7455 |
| 20 | IZENR | 0,2846 | 0,0419 | 0,4475  | 0,4454 | 30,8082 | -0,0659 | -0,2131 | 0,6908 | 0,4785 | 0,2954 |
| 21 | KARYE | 0,4090 | 0,4090 | 1,1533  | 0,0994 | 7,6687  | 0,0453  | 0,0845  | 0,4644 | 0,0337 | 1,2276 |
| 22 | MAGEN | 0,7082 | 0,6985 | 0,7305  | 0,0806 | 12,4582 | 0,0696  | 0,1649  | 0,5779 | 0,1754 | 0,9339 |
| 23 | NATEN | 2,4714 | 2,2909 | 1,2262  | 0,1059 | 10,2744 | 0,0749  | 0,1359  | 0,4492 | 0,0909 | 0,7086 |
| 24 | NTGAZ | 0,9079 | 0,8147 | 1,3956  | 1,1291 | 6,3017  | 0,2246  | 0,3856  | 0,4174 | 0,3223 | 0,0768 |
| 25 | ODAS  | 0,4676 | 0,2921 | 0,3011  | 0,2863 | 6,1058  | -0,0731 | -0,3161 | 0,7686 | 0,3240 | 0,8730 |
| 26 | PAMEL | 1,8087 | 1,8087 | 1,4929  | 0,1245 | 34,0789 | 0,0583  | 0,0973  | 0,4011 | 0,0170 | 1,2566 |
| 27 | SMRTG | 1,1403 | 0,9514 | 0,1469  | 1,0028 | 2,8877  | 0,0999  | 0,7800  | 0,8719 | 0,7599 | 0,0305 |
| 28 | TATEN | 5,1472 | 5,1472 | 0,1258  | 0,0441 | 3,5685  | -0,0679 | -0,7375 | 0,7320 | 0,0197 | 1,6591 |
| 29 | ZEDUR | 0,9139 | 0,9139 | 0,1477  | 0,1246 | 64,0650 | -0,1134 | -0,8813 | 0,8713 | 0,8592 | 1,9115 |
| 30 | ZOREN | 0,4938 | 0,4851 | 0,1202  | 0,4008 | 5,8470  | 0,0018  | 0,0166  | 0,8927 | 0,3751 | 0,3099 |

TOPSIS ynteminin 2. Adımı ile standart karar matrisi oluřturulmuř ve Tablo 8'de gsterilmiřtir.

Tablo 8: TOPSIS Yöntemi ile Standart Karar Matrisinin Oluşturulması

|    |       | P1     | P2     | P3      | P4     | P5     | P6      | P7      | P8     | P9     | P10    |
|----|-------|--------|--------|---------|--------|--------|---------|---------|--------|--------|--------|
| 1  | AHGAZ | 0,0599 | 0,0614 | -0,0467 | 0,3499 | 0,0644 | 0,0268  | -0,0092 | 0,2391 | 0,2063 | 0,0187 |
| 2  | AKENR | 0,0827 | 0,0849 | -0,0047 | 0,0929 | 0,2354 | -0,2386 | -0,9765 | 0,1986 | 0,0238 | 0,1281 |
| 3  | AKFYE | 0,1097 | 0,1142 | 0,1227  | 0,0347 | 0,1035 | -0,0534 | -0,0128 | 0,1310 | 0,0261 | 0,1764 |
| 4  | AKSEN | 0,1452 | 0,1454 | 0,2389  | 0,2177 | 0,0282 | 0,0870  | 0,0140  | 0,1000 | 0,0911 | 0,0203 |
| 5  | AKSUE | 0,0266 | 0,0252 | 0,0639  | 0,0570 | 0,0694 | -0,1653 | -0,0639 | 0,1554 | 0,0606 | 0,3033 |
| 6  | ALFAS | 0,2003 | 0,1681 | 0,1180  | 0,3679 | 0,0469 | 0,3168  | 0,0776  | 0,1327 | 0,1682 | 0,0098 |
| 7  | ARASE | 0,1633 | 0,1640 | 0,2526  | 0,3557 | 0,1226 | 0,3076  | 0,0480  | 0,0973 | 0,1156 | 0,0099 |
| 8  | AYDEM | 0,0495 | 0,0504 | 0,2257  | 0,0308 | 0,2579 | -0,0674 | -0,0111 | 0,1028 | 0,0191 | 0,2320 |
| 9  | AYEN  | 0,0475 | 0,0495 | 0,0894  | 0,0489 | 0,1066 | -0,0445 | -0,0133 | 0,1438 | 0,0467 | 0,1247 |
| 10 | BIOEN | 0,1478 | 0,1513 | 0,0820  | 0,0862 | 0,0859 | 0,0908  | 0,0289  | 0,1470 | 0,0713 | 0,0559 |
| 11 | CANTE | 0,0674 | 0,0423 | 0,1017  | 0,0768 | 0,0776 | 0,0201  | 0,0055  | 0,1388 | 0,0626 | 0,2045 |
| 12 | CATES | 0,0110 | 0,0101 | -0,1761 | 0,1745 | 0,0832 | -0,6522 | -0,0220 | 0,6472 | 0,8262 | 0,1671 |
| 13 | CONSE | 0,0590 | 0,0387 | 0,0926  | 0,1010 | 0,1201 | 0,0028  | 0,0008  | 0,1425 | 0,0955 | 0,0547 |
| 14 | CWENE | 0,1781 | 0,1194 | 0,1753  | 0,2816 | 0,0800 | 0,0836  | 0,0159  | 0,1149 | 0,0997 | 0,0184 |
| 15 | ENERY | 0,0603 | 0,0619 | -0,0464 | 0,3495 | 0,0644 | 0,0272  | -0,0094 | 0,2388 | 0,2060 | 0,0187 |
| 16 | ENJSA | 0,1143 | 0,1162 | 0,1029  | 0,2523 | 0,0781 | 0,0653  | 0,0176  | 0,1384 | 0,0881 | 0,0138 |
| 17 | ESEN  | 0,1852 | 0,1770 | 0,2315  | 0,0334 | 0,1204 | 0,0980  | 0,0160  | 0,1015 | 0,0420 | 0,1463 |
| 18 | GWIND | 0,0784 | 0,0809 | 0,3369  | 0,0587 | 0,1009 | 0,1429  | 0,0195  | 0,0834 | 0,0490 | 0,0490 |
| 19 | HUNER | 0,0208 | 0,0213 | 0,1249  | 0,0226 | 0,0900 | 0,0058  | 0,0014  | 0,1303 | 0,0429 | 0,3760 |
| 20 | IZENR | 0,0393 | 0,0060 | 0,1128  | 0,1274 | 0,3257 | -0,0976 | -0,0247 | 0,1346 | 0,1255 | 0,0636 |
| 21 | KARYE | 0,0565 | 0,0590 | 0,2906  | 0,0284 | 0,0811 | 0,0670  | 0,0098  | 0,0905 | 0,0088 | 0,2644 |
| 22 | MAGEN | 0,0979 | 0,1007 | 0,1840  | 0,0231 | 0,1317 | 0,1031  | 0,0191  | 0,1126 | 0,0460 | 0,2012 |
| 23 | NATEN | 0,3416 | 0,3302 | 0,3089  | 0,0303 | 0,1086 | 0,1109  | 0,0157  | 0,0875 | 0,0239 | 0,1526 |
| 24 | NTGAZ | 0,1255 | 0,1174 | 0,3516  | 0,3231 | 0,0666 | 0,3327  | 0,0446  | 0,0813 | 0,0846 | 0,0165 |
| 25 | ODAS  | 0,0646 | 0,0421 | 0,0759  | 0,0819 | 0,0645 | -0,1083 | -0,0366 | 0,1497 | 0,0850 | 0,1880 |
| 26 | PAMEL | 0,2500 | 0,2607 | 0,3762  | 0,0356 | 0,3602 | 0,0864  | 0,0113  | 0,0782 | 0,0045 | 0,2706 |
| 27 | SMRTG | 0,1576 | 0,1372 | 0,0370  | 0,2870 | 0,0305 | 0,1480  | 0,0903  | 0,1699 | 0,1994 | 0,0066 |
| 28 | TATEN | 0,7114 | 0,7420 | 0,0317  | 0,0126 | 0,0377 | -0,1006 | -0,0854 | 0,1426 | 0,0052 | 0,3573 |
| 29 | ZEDUR | 0,1263 | 0,1317 | 0,0372  | 0,0357 | 0,6772 | -0,1680 | -0,1020 | 0,1698 | 0,2254 | 0,4117 |
| 30 | ZOREN | 0,0682 | 0,0699 | 0,0303  | 0,1147 | 0,0618 | 0,0026  | 0,0019  | 0,1739 | 0,0984 | 0,0668 |

TOPSIS yönteminin 3. adımında ise Tablo 8’te yer alan değerlerle kriter ağırlık değerleri( $W_j$ ) çarpılarak Tablo 9’da yer alan ağırlıklandırılmış standart karar matrisi hesaplanmıştır

Tablo 9: Aęırlıklı Standart Karar Matrisinin Oluřturulması

| Wj |       | 0,0832 | 0,0840 | 0,0898  | 0,1828 | 0,1216 | 0,0631  | 0,0826  | 0,0644 | 0,0746 | 0,1538 |
|----|-------|--------|--------|---------|--------|--------|---------|---------|--------|--------|--------|
|    |       | P1     | P2     | P3      | P4     | P5     | P6      | P7      | P8     | P9     | P10    |
| 1  | AHGAZ | 0,0050 | 0,0052 | -0,0042 | 0,0640 | 0,0078 | 0,0017  | -0,0008 | 0,0154 | 0,0154 | 0,0029 |
| 2  | AKENR | 0,0069 | 0,0071 | -0,0004 | 0,0170 | 0,0286 | -0,0151 | -0,0806 | 0,0128 | 0,0018 | 0,0197 |
| 3  | AKFYE | 0,0091 | 0,0096 | 0,0110  | 0,0063 | 0,0126 | -0,0034 | -0,0011 | 0,0084 | 0,0019 | 0,0271 |
| 4  | AKSEN | 0,0121 | 0,0122 | 0,0215  | 0,0398 | 0,0034 | 0,0055  | 0,0012  | 0,0064 | 0,0068 | 0,0031 |
| 5  | AKSUE | 0,0022 | 0,0021 | 0,0057  | 0,0104 | 0,0084 | -0,0104 | -0,0053 | 0,0100 | 0,0045 | 0,0466 |
| 6  | ALFAS | 0,0167 | 0,0141 | 0,0106  | 0,0673 | 0,0057 | 0,0200  | 0,0064  | 0,0086 | 0,0126 | 0,0015 |
| 7  | ARASE | 0,0136 | 0,0138 | 0,0227  | 0,0650 | 0,0149 | 0,0194  | 0,0040  | 0,0063 | 0,0086 | 0,0015 |
| 8  | AYDEM | 0,0041 | 0,0042 | 0,0203  | 0,0056 | 0,0314 | -0,0043 | -0,0009 | 0,0066 | 0,0014 | 0,0357 |
| 9  | AYEN  | 0,0040 | 0,0042 | 0,0080  | 0,0089 | 0,0130 | -0,0028 | -0,0011 | 0,0093 | 0,0035 | 0,0192 |
| 10 | BIOEN | 0,0123 | 0,0127 | 0,0074  | 0,0157 | 0,0104 | 0,0057  | 0,0024  | 0,0095 | 0,0053 | 0,0086 |
| 11 | CANTE | 0,0056 | 0,0036 | 0,0091  | 0,0140 | 0,0094 | 0,0013  | 0,0005  | 0,0089 | 0,0047 | 0,0314 |
| 12 | CATES | 0,0009 | 0,0008 | -0,0158 | 0,0319 | 0,0101 | -0,0411 | -0,0018 | 0,0417 | 0,0617 | 0,0257 |
| 13 | CONSE | 0,0049 | 0,0033 | 0,0083  | 0,0185 | 0,0146 | 0,0002  | 0,0001  | 0,0092 | 0,0071 | 0,0084 |
| 14 | CWENE | 0,0148 | 0,0100 | 0,0157  | 0,0515 | 0,0097 | 0,0053  | 0,0013  | 0,0074 | 0,0074 | 0,0028 |
| 15 | ENERY | 0,0050 | 0,0052 | -0,0042 | 0,0639 | 0,0078 | 0,0017  | -0,0008 | 0,0154 | 0,0154 | 0,0029 |
| 16 | ENJSA | 0,0095 | 0,0098 | 0,0092  | 0,0461 | 0,0095 | 0,0041  | 0,0015  | 0,0089 | 0,0066 | 0,0021 |
| 17 | ESEN  | 0,0154 | 0,0149 | 0,0208  | 0,0061 | 0,0146 | 0,0062  | 0,0013  | 0,0065 | 0,0031 | 0,0225 |
| 18 | GWIND | 0,0065 | 0,0068 | 0,0303  | 0,0107 | 0,0123 | 0,0090  | 0,0016  | 0,0054 | 0,0037 | 0,0075 |
| 19 | HUNER | 0,0017 | 0,0018 | 0,0112  | 0,0041 | 0,0109 | 0,0004  | 0,0001  | 0,0084 | 0,0032 | 0,0578 |
| 20 | IZENR | 0,0033 | 0,0005 | 0,0101  | 0,0233 | 0,0396 | -0,0062 | -0,0020 | 0,0087 | 0,0094 | 0,0098 |
| 21 | KARYE | 0,0047 | 0,0050 | 0,0261  | 0,0052 | 0,0099 | 0,0042  | 0,0008  | 0,0058 | 0,0007 | 0,0407 |
| 22 | MAGEN | 0,0081 | 0,0085 | 0,0165  | 0,0042 | 0,0160 | 0,0065  | 0,0016  | 0,0073 | 0,0034 | 0,0309 |
| 23 | NATEN | 0,0284 | 0,0277 | 0,0278  | 0,0055 | 0,0132 | 0,0070  | 0,0013  | 0,0056 | 0,0018 | 0,0235 |
| 24 | NTGAZ | 0,0104 | 0,0099 | 0,0316  | 0,0591 | 0,0081 | 0,0210  | 0,0037  | 0,0052 | 0,0063 | 0,0025 |
| 25 | ODAS  | 0,0054 | 0,0035 | 0,0068  | 0,0150 | 0,0078 | -0,0068 | -0,0030 | 0,0097 | 0,0063 | 0,0289 |
| 26 | PAMEL | 0,0208 | 0,0219 | 0,0338  | 0,0065 | 0,0438 | 0,0054  | 0,0009  | 0,0050 | 0,0003 | 0,0416 |
| 27 | SMRTG | 0,0131 | 0,0115 | 0,0033  | 0,0525 | 0,0037 | 0,0093  | 0,0075  | 0,0109 | 0,0149 | 0,0010 |
| 28 | TATEN | 0,0592 | 0,0623 | 0,0028  | 0,0023 | 0,0046 | -0,0063 | -0,0070 | 0,0092 | 0,0004 | 0,0550 |
| 29 | ZEDUR | 0,0105 | 0,0111 | 0,0033  | 0,0065 | 0,0823 | -0,0106 | -0,0084 | 0,0109 | 0,0168 | 0,0633 |
| 30 | ZOREN | 0,0057 | 0,0059 | 0,0027  | 0,0210 | 0,0075 | 0,0002  | 0,0002  | 0,0112 | 0,0073 | 0,0103 |

Daha sonra performans kriterleri maksimum(fayda) ve minimum(maliyet) yönlü olarak TOPSIS yönteminin 4. Adımı ile ideal(A+) ve negatif ideal (A-) çözümler bulunarak Tablo 10'da gösterilmiştir

Tablo 10: İdeal(A+) ve Negatif İdeal (A-) Çözümlerin Oluşturulması

|           |        |        |         |        |        |         |         |        |        |        |
|-----------|--------|--------|---------|--------|--------|---------|---------|--------|--------|--------|
| <b>A+</b> | 0,0592 | 0,0623 | 0,0338  | 0,0673 | 0,0823 | 0,0210  | 0,0075  | 0,0050 | 0,0003 | 0,0010 |
| <b>A-</b> | 0,0009 | 0,0005 | -0,0158 | 0,0023 | 0,0034 | -0,0411 | -0,0806 | 0,0417 | 0,0617 | 0,0633 |

Euclidian Uzaklık Yaklaşımı'ndan faydalanılarak  $Si^+$  ve  $Si^-$  değerleri hesaplanmış ve Tablo 11'de gösterilmiştir.

Tablo 11:  $Si^+$  ve  $Si^-$  Ayırım Ölçülerinin Hesaplanması

|           |              | <b>Si+</b> | <b>Si-</b> |
|-----------|--------------|------------|------------|
| <b>1</b>  | <b>AHGAZ</b> | 0,1183     | 0,1367     |
| <b>2</b>  | <b>AKENR</b> | 0,1478     | 0,0904     |
| <b>3</b>  | <b>AKFYE</b> | 0,1255     | 0,1213     |
| <b>4</b>  | <b>AKSEN</b> | 0,1104     | 0,1407     |
| <b>5</b>  | <b>AKSUE</b> | 0,1401     | 0,1083     |
| <b>6</b>  | <b>ALFAS</b> | 0,1035     | 0,1549     |
| <b>7</b>  | <b>ARASE</b> | 0,0959     | 0,1568     |
| <b>8</b>  | <b>AYDEM</b> | 0,1221     | 0,1243     |
| <b>9</b>  | <b>AYEN</b>  | 0,1277     | 0,1221     |
| <b>10</b> | <b>BIOEN</b> | 0,1164     | 0,1317     |
| <b>11</b> | <b>CANTE</b> | 0,1284     | 0,1206     |
| <b>12</b> | <b>CATES</b> | 0,1605     | 0,0924     |
| <b>13</b> | <b>CONSE</b> | 0,1211     | 0,1275     |
| <b>14</b> | <b>CWENE</b> | 0,1044     | 0,1428     |
| <b>15</b> | <b>ENERY</b> | 0,1183     | 0,1367     |
| <b>16</b> | <b>ENJSA</b> | 0,1094     | 0,1392     |
| <b>17</b> | <b>ESEN</b>  | 0,1157     | 0,1311     |
| <b>18</b> | <b>GWIND</b> | 0,1192     | 0,1394     |
| <b>19</b> | <b>HUNER</b> | 0,1424     | 0,1166     |
| <b>20</b> | <b>IZENR</b> | 0,1108     | 0,1285     |
| <b>21</b> | <b>KARYE</b> | 0,1316     | 0,1267     |
| <b>22</b> | <b>MAGEN</b> | 0,1238     | 0,1264     |
| <b>23</b> | <b>NATEN</b> | 0,1073     | 0,1379     |
| <b>24</b> | <b>NTGAZ</b> | 0,1038     | 0,1572     |
| <b>25</b> | <b>ODAS</b>  | 0,1307     | 0,1149     |
| <b>26</b> | <b>PAMEL</b> | 0,1011     | 0,1391     |
| <b>27</b> | <b>SMRTG</b> | 0,1114     | 0,1431     |
| <b>28</b> | <b>TATEN</b> | 0,1229     | 0,1381     |
| <b>29</b> | <b>ZEDUR</b> | 0,1227     | 0,1262     |
| <b>30</b> | <b>ZOREN</b> | 0,1242     | 0,1253     |

TOPSIS yönteminin son adımı olan ideal çözüme görelî yakınlığı gösteren  $C_i^*$  değeri ile řirketlerin ideal çözüme yakınlığı bulunur. Bu değerler Tablo 12’de gösterilmiştir.

Tablo 12: İdeal Çözüme Görelî Yakınlığın Hesaplanması

|    |       | $C_i^*$ |    |       | $C_i^*$ |    |       | $C_i^*$ |
|----|-------|---------|----|-------|---------|----|-------|---------|
| 1  | AHGAZ | 0,5361  | 11 | CANTE | 0,4843  | 21 | KARYE | 0,4905  |
| 2  | AKENR | 0,3796  | 12 | CATES | 0,3654  | 22 | MAGEN | 0,5051  |
| 3  | AKFYE | 0,4915  | 13 | CONSE | 0,5129  | 23 | NATEN | 0,5624  |
| 4  | AKSEN | 0,5603  | 14 | CWENE | 0,5776  | 24 | NTGAZ | 0,6024  |
| 5  | AKSUE | 0,4360  | 15 | ENERY | 0,5362  | 25 | ODAS  | 0,4677  |
| 6  | ALFAS | 0,5995  | 16 | ENJSA | 0,5600  | 26 | PAMEL | 0,5792  |
| 7  | ARASE | 0,6205  | 17 | ESEN  | 0,5311  | 27 | SMRTG | 0,5622  |
| 8  | AYDEM | 0,5045  | 18 | GWIND | 0,5390  | 28 | TATEN | 0,5292  |
| 9  | AYEN  | 0,4887  | 19 | HUNER | 0,4501  | 29 | ZEDUR | 0,5070  |
| 10 | BIOEN | 0,5308  | 20 | IZENR | 0,5371  | 30 | ZOREN | 0,5021  |

Tablo 12’den hareketle ilgili řirketleri ideal çözüme en yakın olandan en uzak olana göre sıraladığımızda Tablo 13’teki sıralamaya ulařılmaktadır.

Tablo 13: İlgili Şirketlerin İdeal Çözüme Yakınlığa Göre Sıralanması (2020)

|    |       | $C_i^*$ |    |       | $C_i^*$ |    |       | $C_i^*$ |
|----|-------|---------|----|-------|---------|----|-------|---------|
| 1  | ARASE | 0,6205  | 11 | IZENR | 0,5371  | 21 | ZOREN | 0,5021  |
| 2  | NTGAZ | 0,6024  | 12 | ENERY | 0,5362  | 22 | AKFYE | 0,4915  |
| 3  | ALFAS | 0,5995  | 13 | AHGAZ | 0,5361  | 23 | KARYE | 0,4905  |
| 4  | PAMEL | 0,5792  | 14 | ESEN  | 0,5311  | 24 | AYEN  | 0,4887  |
| 5  | CWENE | 0,5776  | 15 | BIOEN | 0,5308  | 25 | CANTE | 0,4843  |
| 6  | NATEN | 0,5624  | 16 | TATEN | 0,5292  | 26 | ODAS  | 0,4677  |
| 7  | SMRTG | 0,5622  | 17 | CONSE | 0,5129  | 27 | HUNER | 0,4501  |
| 8  | AKSEN | 0,5603  | 18 | ZEDUR | 0,5070  | 28 | AKSUE | 0,4360  |
| 9  | ENJSA | 0,5600  | 19 | MAGEN | 0,5051  | 29 | AKENR | 0,3796  |
| 10 | GWIND | 0,5390  | 20 | AYDEM | 0,5045  | 30 | CATES | 0,3654  |

#### 4. SONUÇ

TOPSIS Performans kriteri olarak kullanılan 10 adet finansal oranın ağırlık(önem) derecelerini CRITIC yöntemi ile hesapladığımızda, 2020 yılı için aktif devir hızının önem düzeyinin en yüksek olduğunu bu oranı, finansman giderleri / net satışlar oranının izlediği görülmektedir. En düşük önem düzeyine sahip oran ise aktif karlılığıdır. BİST XELK endeksinde yer alan 30 adet enerji řirketinin 10 adet finansal oranı temel alınarak oluş-

turulan performans kriterlerine göre TOPSIS yöntemiyle yapılan analiz sonucunda 2020 yılında ideal çözüme en yakın(finansal performans olarak en yüksek) şirket ARASE olurken negatif ideal çözüme en yakın(finansal performans olarak en düşük) şirket CATES olmuştur.

Gelecekteki performans analizi çalışmalarında, farklı metodolojilere dayalı sonuçlardaki varyasyon potansiyelini göz önünde bulundurmak ve karşılaştırma amaçlı kullanmak önemli olacaktır. Örneğin, performans kriteri olarak alternatif finansal oranlar kullanmak, CRITIC yöntemi yerine farklı ağırlıklandırma yöntemleri benimsemek ve TOPSIS yöntemi dışında farklı Çok Kriterli Karar Verme yöntemleri kullanmak, performans kriterleri için farklı önem düzeylerine ve farklı performans sıralaması sonuçlarına yol açabilir. Benzer şekilde, ilgili endeksin dışındaki çeşitli şirketlerden veya endekslerden örnekler seçmek analize ek değişkenlik getirebilir. Performans analizi çalışmaları yürütürken bu farklılıkları gözeterek karar mekanizmalarını oluşturmak gereklidir.

**KAYNAKÇA:**

- Akdoęan, Nalan., ve Tenker, Nejat. (2010). *Finansal tablolar ve mali analiz teknikleri* (13. baskı). Ankara: Gazi Kitabevi.
- Arsu, T. (2021). Finansal performansın Entropi tabanlı ARAS yöntemi ile deęerlendirilmesi: BİST elektrik, gaz ve buhar sektöründeki řletmeler üzerine bir uygulama. *Hacettepe Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 39(1), 15-32.
- Baęcı, H., ve Yüksel Yięiter, ř. (2019). BİST'te yer alan enerji řirketlerinin finansal performansının SD ve WASPAS yöntemleriyle ölçülmesi. *Bingöl Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 9(18), 877-898.
- Bülbül, S., ve Köse, A. (2012). Türk gıda řirketlerinin finansal performansının çok amaçlı karar verme yöntemleriyle deęerlendirilmesi. *Atatürk Üniversitesi İktisadi ve İdari Bilimler Dergisi Ekonometri ve İstatistik Sempozyumu Özel Sayısı*, 25, 71-97.
- Cheung, A. W. K., Roca, E. (2013). The effect on price, liquidity and risk when stocks are added to and deleted from a sustainability index: Evidence from the Asia Pacific context. *Journal of Asian Economics*, 24, 51-65.
- Quick, A., Lazol, I. (2014). *Financial statement analysis* (14th ed.). Ankara: Ekin Publishing House.
- Farmer, H. N., Yildirim, B. F. (2020). Examination of the financial performances of the enterprises operating in the BIST energy sector: An example of a time section based on gray numbers. *Journal of Accounting Science*, 22(3), 384-404.
- Diakoulaki, D., Mavrotas, G. Papayannakis, L. (1995) Determining Objective Weights in Multiple Criteria Problems: The CRITIC Method. *Computers & Operations Research*, 22, 763-770.
- Durmuşkaya, S., ve Kavas, Y. B. (2019). TOPSIS ile finansal performans ölçümü: Turizm sektörü üzerine bir uygulama. *I. Uluslararası İktisat, İşletme ve Sosyal Bilimler Kongresi*, 310-315.
- Kayahan Karakul, A., ve Özeydin, G. (2019). TOPSIS ve VIKOR yöntemleri ile finansal performans deęerlendirmesi: XELKT üzerinde bir uygulama. *Dumlupınar Üniversitesi Sosyal Bilimler Dergisi*, 60, 68-86.
- Metin, S., Yaman, S., ve Korkmaz, T. (2017). Finansal performansın TOPSIS ve MOORA yöntemleri ile belirlenmesi: BİST enerji firmaları üzerine karşılařtırılmalı bir uygulama. *Kahramanmaraş Sütçü İmam Üniversitesi Sosyal Bilimler Dergisi*, 14(2), 371-394.
- Onocak, D. (2023). BİST'te işlem gören konaklama řletmelerinin finansal performanslarının CRITIC aęırlıklandırılmalı TOPSIS yöntemine göre deęerlendirilmesi. *Muhasebe ve Finansman Dergisi*, 97, 79-98.

- Orçun, Ç. (2019). Enerji sektöründe WASPAS yöntemiyle performans analizi. *Bolu Abant İzzet Baysal Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 19(2), 439-453.
- Özden, Ü. H. (2011). TOPSIS yöntemi ile Avrupa Birliğine üye ve aday ülkelerin ekonomik göstergelere göre sıralanması. *Trakya Üniversitesi Sosyal Bilimler Dergisi*, 13(2), 215-236.
- Quick, A., Lazol, I. (2014). Financial statement analysis (14th ed.). Ankara: Ekin Publishing House.
- Sakarya, Ş., Yildirim, H. H., ve Akkus, H. T. (2015). BİST'te işlem gören enerji şirketlerinin finansal performanslarının TOPSIS çok kriterli karar verme yöntemi ile belirlenmesi içinde (s. 601-616). 19. *Finans Sempozyumu, sunulmuş bildiri*, Çorum.
- Türkiye Cumhuriyet Merkez Bankası (b.t.). Elektronik Veri Dağıtım Sistemi. [https://evds2.tcmb.gov.tr/index.php?evds/serieMarket/collapse\\_36/5091/DataGroup/turkish/bie\\_hariccariacik/](https://evds2.tcmb.gov.tr/index.php?evds/serieMarket/collapse_36/5091/DataGroup/turkish/bie_hariccariacik/)
- Wang, T. C., Hsu, J. C. (2004). Evaluation of the business operation performance of the listing companies by applying the TOPSIS method. *Conference Proceedings - IEEE International Conference on Systems, Man and Cybernetics*, 2, 1286-1291.
- Wang, Y. M., ve Elhag, T. M. S. (2006). Fuzzy TOPSIS method based on alpha level sets with an application to bridge risk assessment. *Expert Systems with Applications*, 31(2), 309-319.
- Yükçü, S., ve Atağan, G. (2010). TOPSIS yöntemine göre performans değerlendirme. *Muhasebe ve Finansman Dergisi*, 45, 28-35.