ISSN: 2980-1331
E-ISSN: 3023-4239

BİLGİ TEKNOLOJİLERİ VE İLETİŞİM DERGİSİ

JOURNAL OF INFORMATION TECHNOLOGIES AND COMMUNICATION

CİLT: 3 SAYI: 1 OCAK-HAZİRAN 2025

BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU

BİLGİ TEKNOLOJİLERİ VE İLETİŞİM DERGİSİ

(BTK DERGİ)

JOURNAL OF INFORMATION TECHNOLOGIES AND COMMUNICATION

CİLT: 3 SAYI: 1

OCAK - HAZİRAN 2025

ISSN:2980-1331

E-ISSN: 3023-4239

BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU

BİLGİ TEKNOLOJİLERİ VE İLETİŞİM DERGİSİ (BTK DERGİ)

Hakemli Akademik Araştırma Dergisi

Bilgi Teknolojileri ve İletişim Kurumu Adına Sahibi
Ömer Abdullah KARAGÖZOĞLU

Editör
Dr. Abdulkerim GÜN

Editör Yardımcısı
Salih BOZKURT
Korkmaz AFACAN (Yabancı Dil Editörü)

Sorumlu Yazı İşleri Müdürü
Yakuphan GÜLEÇ

Redaksiyon
Kübra YAVUZ ÇAKIR

Yönetim ve İletişim
Bilgi Teknolojileri ve İletişim Kurumu Eskişehir Yolu Mustafa Kemal Mah.
No: 276 Posta Kodu: 06530 Çankaya/Ankara
e-posta: dergi@btk.gov.tr
web: https://dergi.btk.gov.tr

Yayın Türü:
Yaygın Süreli Yayın

ISSN
ISSN:2980-1331
E-ISSN
3023-4239

Grafik Tasarım
Yasemin KULA
Kevser GÜLDOĞAN

Baskı Adedi
100 Adet

Bilgi Teknolojileri ve İletişim Dergisi'nde yayımlanan yazılardaki görüşler yazarına aittir.

Yılda iki sayı (Haziran-Aralık) yayımlanır.

BİLGİ TEKNOLOJİLERİ VE İLETİŞİM DERGİSİ
(BTK DERGİ)

JOURNAL OF INFORMATION TECHNOLOGIES AND COMMUNICATION

CİLT 3 SAYI 1 OCAK-HAZİRAN 2025

T.C. BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU HAKEMLİ AKADEMİK ARAŞTIRMA DERGİSİ

Bilgi Teknolojileri ve İletişim Dergisi (BTK DERGİ)
CİLT 3 SAYI 1 OCAK-HAZİRAN 2025 ISSN:2980-1331 E-ISSN: 3023-4239

BİLİMSEL YAZIŞMA

Makaleler ile ilgili tüm soru ve yazışmalarınız için:

Tel: 0312 412 24 00 / e-posta: dergi@btk.gov.tr

Bilgi Teknolojileri ve İletişim Dergisi (BTK DERGİ)
CİLT 3 SAYI 1 OCAK-HAZİRAN 2025 ISSN:2980-1331 E-ISSN: 3023-4239

EDİTÖRDEN

Kıymetli Okurlar,

Dijital teknolojilerdeki baş döndürücü gelişmeler, iletişim, güvenlik, kimlik doğrulama ve hukuki altyapılar gibi pek çok alanda paradigmaları kökten değiştirmektedir. Bu çerçevede hazırlanan bu sayımız, hem kavramsal zemin oluşturan hem de teknik ve hukuki tartışmalara katkı sunan güncel çalışmaları kapsamaktadır.

Aybüke GÜNEŞ'in "Deepfake'in Elektronik Ortamda Yapay Zekâ Tabanlı Kimlik Doğrulama Sürecine Etkisi" başlıklı çalışması, yapay zekâ tabanlı biyometrik doğrulama sistemlerini tehdit eden deepfake teknolojilerini ele alarak bu yeni risklere karşı savunma stratejileri geliştirilmesi gerektiğini vurgulamaktadır. Gelişen güvenlik açıkları karşısında ulusal ve uluslararası standartlara yönelik öneriler, çalışmayı değerli kılmaktadır.

Yasemin YAMAK tarafından kaleme alınan "Yapay Zekâ ile İlgili Güncel Düzenleme Çalışmaları: AB, ABD ve Türkiye Açısından İncelenmesi" başlıklı makale, yapay zekâ alanında küresel düzeyde süren düzenleme yarışını ve bu yarışta Türkiye'nin mevcut konumunu karşılaştırmalı olarak analiz etmektedir. Çalışma, özellikle Avrupa Birliği'nin Yapay Zekâ Yasası'nı detaylandırarak regülasyonlara yönelik yol haritası sunmaktadır.

Aycan ILGIN'ın "Bir Kamu Malı Olan Frekansların Tabi Olduğu Hukuksal Rejimin Değerlendirilmesi" başlıklı katkısı, mobil iletişim teknolojilerinin temelini oluşturan frekansların hukuki statüsünü 5809 sayılı Elektronik Haberleşme Kanunu çerçevesinde incelemektedir. Makale, frekansların kamu malı niteliğinden hareketle kamu yararının korunması için gerekli hukuki prensipleri tartışmaktadır.

Ahmet EFE'nin "Hayalî İterasyon ve Yapay Zekâ Temelli Risk Analizi: IoT Entegre Sistemlerde Ortaya Çıkan Siber Güvenlik Tehditleri" başlıklı araştırması, yapay zekânın siber güvenlikteki çift yönlü doğasını – hem savunma hem saldırı vektörü olarak – yenilikçi bir metodoloji olan hayalî iterasyon ile modellemekte ve Türkiye'nin siber güvenlik kapasitesini değerlendirmektedir.

Son olarak, bu sayıda yer alan "Dijitalleşme Sürecinde Sosyal Politikada Güncel Gelişmeler" başlıklı Murat Kalkan tarafından incelenen kitap değerlendirmesi, sosyal politika alanında dijitalleşmenin etkilerini çok boyutlu ele alan esere odaklanmaktadır. Kitap; kavramsal çerçeve, ampirik analizler ve sektörel uygulamalar bağlamında derinlemesine bir inceleme sunmakta, sosyal politika literatürüne önemli bir katkı sağlamaktadır.

Bilgi Teknolojileri ve İletişim Dergimizin bu sayısında yer alan 4 makale ve 1 kitap incelemesinin, okuyucularımıza dijitalleşme, yapay zekâ, siber güvenlik ve iletişim hukuku bağlamında farklı perspektifler kazandırmasını temenni eder, katkı sunan tüm yazarlarımıza ve değerli hakemlerimize teşekkür ederiz.

Saygılarımla,

Dr. Abdulkerim GÜN

Editör

Bilgi Teknolojileri ve İletişim Dergisi (BTK DERGİ)
CİLT 3 SAYI 1 OCAK-HAZİRAN 2025 ISSN:2980-1331 E-ISSN: 3023-4239

İÇİNDEKİLER

Bilgi Teknolojileri ve İletişim Dergisi (BTK DERGİ)
CİLT 3 SAYI 1 OCAK-HAZİRAN 2025 ISSN:2980-1331 E-ISSN: 3023-4239

Bilgi Teknolojileri ve İletişim Dergisi (BTK DERGİ)
CİLT 3 SAYI 1 OCAK-HAZİRAN 2025 ISSN:2980-1331 E-ISSN: 3023-4239

DEEPFAKE'İN ELEKTRONİK ORTAMDA YAPAY ZEKÂ TABANLI KİMLİK DOĞRULAMA SÜRECİNE ETKİSİ

Aybüke GÜNEŞ[1]

Gönderilme Tarihi: 3 Mart 2025
Kabul Tarihi: 20 Mayıs 2025

Review Article / İnceleme Makalesi

ÖZET

Teknolojik gelişmeler, kimlik doğrulama ile yapılan pek çok işlemin elektronik ortama taşınmasını sağlamıştır. Elektronik ortamda gerçekleştirilen işlemlerin güvenliğinin sağlanması, kimlik doğrulama süreçlerini güvence altına almak için önemli bir ihtiyaç haline gelmiştir. Elektronik ortamda kimlik doğrulama işlemlerinin yapay zekâ kullanılarak gerçekleştirilmesi yapay zekâ tabanlı kimlik doğrulama süreçlerini ortaya çıkarmıştır. Yapay zekâ tabanlı kimlik doğrulama, yüz tanıma ve canlılık teknikleri kullanılarak bireylerin elektronik ortamda kimliklerinin doğrulanmasına imkân tanımaktadır. Ancak, bireylerin fotoğraf ve benzeri görüntülerinden yararlanılarak sentetik video veya görüntüler oluşturulmasına yarayan DeepFake, yapay zekâ tabanlı kimlik doğrulama süreçlerini yanıltmak amacıyla kullanılmaktadır. Bu durum, yapay zekâ tabanlı kimlik doğrulama süreçlerini olumsuz etkilemektedir. Dolayısıyla yapay zekâ tabanlı kimlik doğrulamadaki yüz tanıma sistemlerinin savunma yeteneklerinin, DeepFake saldırılarına karşı artırılması ve güçlü anti-DeepFake tekniklerinin geliştirilmesi gerekmektedir. Bu çalışmada, yapay zekâ tabanlı kimlik doğrulama süreci ve DeepFake incelenmiştir. Bütünsel bir perspektif ile incelemeler yapılması amaçlanmış ve yapay zekâ tabanlı kimlik doğrulama sürecinde DeepFake'in etkisi ele alınmıştır. Sonuç olarak, DeepFake'in olumsuz etkilerinden korunmak için güçlü savunma sistemleri geliştirilmesi, ulusal ve uluslararası alanda birlikte çalışabilirliği artırıcı standart, sertifikasyon ve test yöntemlerinin geliştirilmesi gerektiğine değinilmiştir.

Anahtar Kelimeler: *Kimlik Doğrulama, Elektronik Ortamda Kimlik Doğrulama, Yapay Zekâ Tabanlı Kimlik Doğrulama, DeepFake.*

[1] Bilgi Teknolojileri ve İletişim Kurumu, aybuke.gunes95@gmail.com, ORCID:0000-0003-1027-4905

Bilgi Teknolojileri ve İletişim Dergisi (BTK DERGİ)
CİLT 3 SAYI 1 OCAK-HAZİRAN 2025 ISSN:2980-1331 E-ISSN: 3023-4239

IMPACT OF DEEPFAKE ON ARTIFICIAL INTELLIGENCE BASED IDENTITY PROOFING PROCESS IN ELECTRONIC ENVIRONMENT

ABSTRACT

Technological developments have enabled many transactions carried out with identity proofing to be transferred to the electronic environment. In order to secure identity proofing processes, it has become an important need to ensure the security of transactions carried out electronically. The realization of identity proofing processes in the electronic environment using artificial intelligence has led to the emergence of artificial intelligence-based identity proofing processes. Artificial intelligence-based identity proofing allows individuals to be identity proofing electronically using face recognition and liveness techniques. But, DeepFake, which utilizes photographs and similar images of individuals to create synthetic videos or images, is used to deception artificial intelligence-based identity proofing processes. This has a negative impact on artificial intelligence-based identity proofing processes. Accordingly, it is essential to enhance the defensive capabilities of facial recognition systems in artificial intelligence-based identity proofing against DeepFake attacks and to develop robust anti-DeepFake techniques to mitigate such threats. In this study, the artificial intelligence-based identity proofing process and DeepFake are analyzed. With this study, it is aimed to examine with a holistic perspective and the impact of DeepFake in the artificial intelligence-based identity proofing process is discussed. As a result, it has been mentioned that in order to mitigate the adverse impacts of DeepFake technologies, it is essential to develop robust defense systems, as well as to establish standards, certification frameworks, and testing methodologies that enhance interoperability at both national and international levels.

Keywords: *Identity Proofing, Electronic Identity Proofing, Artificial Intelligence-Based Identity Proofing, DeepFake*

GİRİŞ

Dünyadaki dijital dönüşüm ve teknolojik gelişmeler, fiziksel kimlik doğrulama ile yapılan pek çok işleme ilişkin sürecin elektronik ortama taşınmasını sağlamıştır. Elektronik ortamda hizmetlere erişim sağlamak veya herhangi bir işlemi gerçekleştirebilmek için kimlik doğrulama sürecinin de elektronik ortamda yapılması gerekmektedir. Kimlik doğrulama, bireyin gerçekte iddia ettiği kişi olduğundan belirli bir kesinlik seviyesinde emin olunduğunun belirlenmesi süreciyken elektronik ortamda kimlik doğrulama bahse konu kimlik doğrulama sürecinin elektronik bir yöntemle dijital olarak gerçekleştirilmesi sürecidir. Gündelik yaşamdaki işlemlerin dijital ortama taşınması, bir bireyin kimlik doğrulama işleminin gerçekleştirildiği yerde fiziksel olarak bulunma mecburiyetini ortadan kaldırarak kimlik doğrulama sürecinin elektronik ortamda gerçekleştirilmesini mümkün hale getirmiştir.

Günümüzde teknolojinin gelişmesi ile hayatımızın her alanına etki eden yapay zekâ, elektronik ortamda kimlik doğrulama sürecinin otomatik olarak yürütülmesinde de kullanılmaktadır. Elektronik ortamda yapay zekâ tabanlı kimlik doğrulama, parmak izi ve yüz gibi biyometrik veriler ile kimlik doğrulamaya dayalı olarak gerçekleştirilebilmektedir. Halihazırda sıklıkla tercih edilen yöntem yüz biyometrik verisi kullanılarak yüz karşılaştırması ile kimlik doğrulama yöntemidir. Elektronik ortamda yapay zekâ tabanlı bir kimlik doğrulama süreci, teknolojik gelişmelerin beraberinde getirdiği güvenlik açıkları nedeniyle kötü niyetli bir saldırgan tarafından manipüle edilebilmektedir. Özellikle DeepFake, yüz biyometrik verisine dayanan yapay zekâ tabanlı kimlik doğrulama sistemlerine karşı kötü niyetli saldırganlar tarafından kullanılmaktadır. Kötü niyetli bir saldırgan kimlik doğrulama sürecinin tüm adımlarını biliyorsa ve sahte videoyu kimlik doğrulama sürecine enjekte edebiliyorsa veya videoyu bir ekrana sunabiliyorsa otomatik bir kimlik doğrulama sistemini yanıltması mümkün olabilmektedir. Elektronik ortamda yapay zekâ tabanlı kimlik doğrulama sürecinin doğru bir şekilde sonuçlandırılabilmesi ve saldırganların manipülasyonlarından korunabilmesi için güvenlik açıklarına karşı önlemler alınması gerekmektedir.

Bu çalışmada, elektronik ortamda yapay zekâ tabanlı kimlik doğrulama sürecine ve DeepFake'e ilişkin hususlar ele alınmıştır ve bütünsel bir perspektif ile yapay zekâ tabanlı kimlik doğrulama sürecinde DeepFake'in etkisi incelenmiştir. Çalışmanın ilk bölümünde başvuru sahibinin biyometrik verileri kullanılarak

elektronik ortamda gerçekleştirilen yapay zekâ tabanlı kimlik doğrulama süreci ile ilgili bilgilere yer verilmiştir. İkinci bölümde, bireylerin fotoğraf ve benzeri görüntülerinden yararlanılarak sentetik video veya görüntülerin oluşturulmasına yarayan DeepFake teknolojisine dair bilgiler yer almaktadır. Üçüncü bölümde ise, DeepFake'in yapay zekâ tabanlı kimlik doğrulama sürecine etkisi ele alınmıştır. Son olarak çalışmanın sonuçları tartışılarak değerlendirmelere yer verilmiştir.

ELEKTRONİK ORTAMDA YAPAY ZEKÂ TABANLI KİMLİK DOĞRULAMA

Kimlik doğrulama, bireyin gerçekte iddia ettiği kişi olduğundan belirli bir kesinlik seviyesinde emin olmayı ifade etmektedir (NIST, 2017a). Kimlik doğrulama süreci (Şekil 1) genel olarak bireyin tanımlayıcı bilgilerinin toplanması, bireyin tanımlayıcı bilgilerinin gerçek ve doğru olduğundan ve bireyin kimliğinin var olduğundan emin olunması ve kimliğin bireye ait olduğunun teyidinin gerçekleştirilmesi adımlarından oluşmaktadır (AUTHENTICID, 2024).

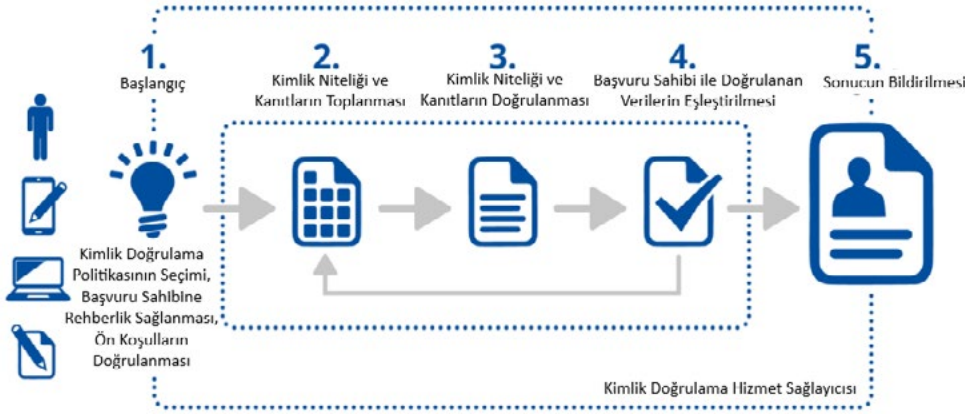
Şekil 1 Kimlik doğrulama süreci (AUTHENTICID, 2024)

Bir bireyin fiziki olarak kimlik doğrulama işlemini yapacak personel ile aynı ortamda bulunmasını gerektiren yani fiziksel mevcudiyete dayalı kimlik doğru-

lama, dünya genelinde yaşanan dijitalleşmenin etkisi ile birlikte elektronik ortamda gerçekleştirilmeye başlanmıştır. Kimlik doğrulama sürecinin elektronik bir yöntemle dijital olarak gerçekleştirilmesi elektronik ortamda kimlik doğrulama sürecini ifade etmektedir.

Elektronik ortamda kimlik doğrulama süreci (Şekil 2), sürecin başlatılması, başvuru sahibinin kimlik niteliği ve kanıtlarının toplanması, toplanan nitelik ve kanıtların doğrulanması, başvuru sahibi ile doğrulanan verilerin eşleştirilmesi ve kimlik doğrulama sonucunun bildirilmesi olmak üzere beş adımdan oluşmaktadır (ENISA, 2021).

Şekil 2 Kimlik doğrulama süreci (ENISA, 2021)



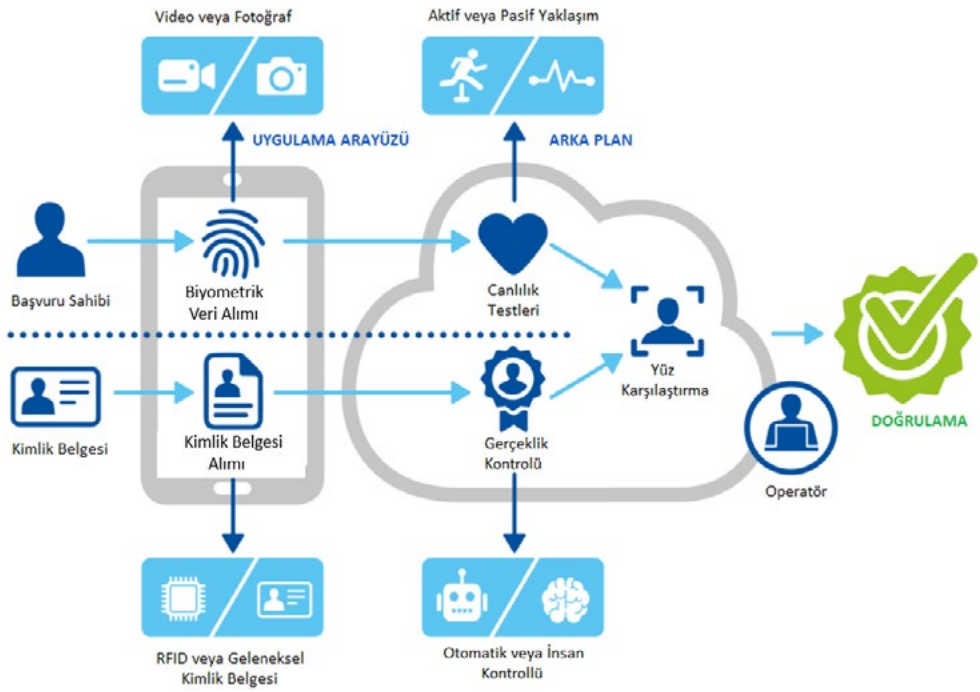
Dijitalleşme ile birlikte, elektronik ortamda kimlik doğrulama sürecinin önünün açılması elektronik işlemlerin çeşitliliğine yönelik potansiyeli artırmış ve işlemlerdeki ilgili tarafların kimliklerinin geçerliliğinin doğrulanabilmesi için kart tabanlı, sertifika tabanlı, mobil tabanlı, biyometrik tabanlı ve çok faktörlü kimlik doğrulama gibi çeşitli yöntemler geliştirilmeye başlanmıştır. Ayrıca elektronik ortamda kimlik doğrulama süreci, günümüz teknolojisinin ilerlemesiyle birlikte açık anahtar altyapısı, blok zincir teknolojisi, yakın alan iletişimi ve yapay zekâ gibi farklı teknolojiler kullanılarak gerçekleştirilebilmektedir (ENISA, 2020).

Esasen, elektronik ortamda kimlik doğrulamanın yapay zekâ ile gerçekleştirildiği bir yaklaşım, yapay zekâ tabanlı kimlik doğrulamayı oluşturmaktadır. Yapay zekâ, kimlik doğrulama süreçlerinin otomatik olarak gerçekleştirilmesini mümkün kılmaktadır. Yapay zekâ tabanlı kimlik doğrulama çözümleri ile bir bireyin

kimliği; yüz, ses ve parmak izi gibi biyometrik veriler ile doğrulanabilmektedir. Ayrıca, kimlik doğrulama süreçlerinde gerçekleştirilen canlılık ve gerçeklik testleri için yapay zekâ algoritmaları kullanılmaktadır.

Elektronik ortamda kimlik doğrulama süreci yapay zekâ ile biyometrik veriye dayalı güvenlik protokolleri oluşturularak gerçekleştirilebilmektedir. Bir bireyin yüz biyometrisi alınarak kimlik belgesindeki fotoğraf ile karşılaştırma yapmak suretiyle yapay zekâ ile kimlik doğrulama gerçekleştirmek mümkündür. Bunun yanı sıra yapay zekâ ile görüntülü kimlik doğrulama sırasında kimliği doğrulanacak birey için canlılık ve gerçeklik testleri de uygulanabilmektedir. Yapay zekâ teknikleri ile herhangi bir insan desteği olmadan otomatik kimlik doğrulama sistemleri oluşturulabileceği gibi operatörlü kimlik doğrulama süreçlerine destek olarak da yapay zekâ teknikleri ile kimlik doğrulama sistemleri kullanılabilmektedir.

Şekil 3 Yapay zekâ tabanlı bir kimlik doğrulama süreci (ENISA, 2022)



Yapay zekâ tabanlı bir kimlik doğrulama sürecine (Şekil 3) göre; ilk olarak başvuru sahibinin kart tabanlı veya geleneksel olan kimlik belgesi ve video kaydı veya fotoğraf kullanılarak biyometrik verisi alınır. Ardından, başvuru sahibinin kimlik belgesinden elde edilen verilerin doğruluğu ve gerçekliği otomatik kontrol veya insan kontrolü ile teyit edilir. Eşzamanlı gerçekleştirilen bu süreç başvuru sahibinin canlılığını gerektirdiği için aktif veya pasif yaklaşımlar kullanılarak canlılık testleri uygulanır. Son olarak başvuru sahibinin biyometrik verisi ile kimlik belgesindeki veriler yapay zekâ ile karşılaştırılır ve sürecin sonunda kimlik doğrulama işleminin kararı ya otomatik bir sistem ile ya da insan denetimi ile sonuçlandırılarak kimlik doğrulama sürecinin çıktısı üretilir (ENISA, 2022).

Elektronik ortamda yapay zekâ tabanlı bir kimlik doğrulamanın süreç adımları; biyometrik verilerin alınması, biyometrik canlılık kontrolü, kimlik belgesi alımı, kimlik belgesi doğruluk kontrolü ve yüz karşılaştırması olmak üzere beş başlık altında gruplandırılabilir.

Biyometrik Verilerin Alınması

Kimlik doğrulamada biyometri kullanımı, hem fiziksel özelliklerin (örneğin parmak izi, iris, yüz özellikleri) hem de davranış özelliklerinin (örneğin, tuş vuruşu hızı) ölçümünü içermektedir (NIST, 2017b). Kimlik belgesi içerisinde bulunan parmak izi veya fotoğraf gibi biyometrik verilerin, yapay zekâ tabanlı bir kimlik doğrulama sürecinde kullanılması, güvenilir kimlik özelliklerinin verimli bir şekilde edinilebilmesi için hem ilgi çekici hem de teknik olarak uygun bir yöntemdir (ENISA, 2021).

Yapay zekâ tabanlı kimlik doğrulama süreci; her zaman bir başvuru sahibinin, kimlik doğrulama sağlayıcısının kendisinden veya güvenilir üçüncü bir taraftan elektronik hizmetlere erişmek ve bu hizmetleri kullanmak için bir kimlik doğrulama hizmetine kaydolmasıyla başlar. Başvuru sahibi ile hizmet sağlayıcı arasındaki güvenli etkileşimin sağlanması için hizmet sağlayıcı tarafından başvuru sahibine iletilen bir mobil uygulama veya bir web tarayıcısı kullanılır. Başvuru sahibi ile hizmet sağlayıcı arasındaki etkileşimin kimliği doğrulanmış güvenli ve korumalı bir kanal üzerinden sağlanması sonrasında, başvuru sahibinin aşağıdakilere ilişkin kanıt sunması gerekir (ENISA, 2022):

- Genellikle başvuru sahibinin video görüntüsü veya bir ya da daha fazla fotoğrafın alınması yoluyla elde edilen yüz özellikleri,

- Elektronik bir belgenin (elektronik kimlik belgesi) çipinde saklanan fotoğraf kullanılarak veya çip ya da şifrelenmiş güvenli ortam olmadığında belge üzerindeki basılı fotoğraf kullanılarak yüz referansının oluşturulabileceği yetkili makamlar tarafından verilmiş geçerli bir kimlik belgesi.

Biyometrik Canlılık Kontrolü

Biyometrik canlılık kontrolü, kameranın önünde yer alan öznenin gerçek ve canlı bir insan olduğuna dair makul güvence elde etmek için başvuru sahibi üzerinde gerçekleştirilen tüm kontrolleri kapsamaktadır. Biyometrik canlılık kontrolü, bir bireyin benzersiz biyometrisini DeepFake kukla, maske veya önceden kaydedilmiş bir video veya fotoğrafın yeniden oynatılması gibi saldırı yöntemleri ile taklit eden bir kopyanın, kimlik doğrulama adımlarını atlatmak için biyometrik tarayıcıya sunulduğu biyometrik sahtekârlık saldırılarına karşı koymak için bir dizi teknik özellik içermektedir (Thales, 2020).

Canlılık kontrolü, güvenli bir uygulamanın en temel unsurları arasında yer almaktadır. Teknik olarak, elektronik ortamda yapay zekâ tabanlı kimlik doğrulama için aktif ve pasif olmak üzere iki tür canlılık kontrolü tespit yöntemi bulunmaktadır (Freiberg, 2024). Bu yöntemler şunlardır:

- **Aktif canlılık tespiti:** Bireylerin süreç sırasında bazı işlemleri yapmasını gerektirmektedir. Aktif canlılık tespitinde, hareketle tetiklenen görüntülerin yakalanması için birey yüzünü kamerayla hizalamalıdır. Ardından bireyin başını sallama, göz kırpma, gülümseme, rastgele sözcükleri okuma, ekranda hareket eden bir nesneyi takip etme, yüzünü kameraya yaklaştırma veya uzaklaştırma, komut üzerine başını sola veya sağa çevirme veya yüzünün önünde elini sallama gibi zorluklara yanıt olarak belirli eylemleri gerçekleştirmesi gerekmektedir (ENISA, 2022).
- **Pasif canlılık tespiti:** Bireylerin süreç sırasında ekstra özel işlemler yapmasını gerektirmemektedir. Pasif canlılık tespitinde, yalnızca bir anlık görüntü alınmakta ve yapay zekâ kullanılarak analiz yapılmaktadır (Freiberg, 2024). Birey yüzünü kamerayla hizalamalıdır. Pasif canlılık tespiti, DeepFake manipülasyonundan kaynaklanan çözünürlük tutarsızlıkları, başvuranın yüzündeki ve çevresindeki yansımaları analiz etmek için birey üzerinde yanıp sönen ışıklar, analiz edilen video çerçevelerinde veya görüntülerde bulunan nabız atışları ve diğer istemsiz insan sinyallerinden kaynaklanan cilt rengi yoğunluğundaki

mikro varyasyonları analiz etme gibi bireyin eylemini gerektirmeyen doğrulama tekniklerine dayanmaktadır (ENISA, 2022).

Aktif canlılık tespiti yaklaşımında, dolandırıcıların fotoğraf saldırıları, video yeniden oynatma saldırıları ve DeepFake gibi tekniklerle elektronik ortamda yapay zekâ tabanlı bir kimlik doğrulama sürecinin kontrollerini atlatması daha zorken; pasif canlılık tespiti yaklaşımında enjekte fotoğraf saldırıları, video yeniden oynatma saldırıları ve DeepFake gibi saldırı tekniklerinin elektronik ortamda yapay zekâ tabanlı bir kimlik doğrulama sürecini atlatması aktif canlılık tespiti yaklaşımındakinden daha kolaydır (Wang vd., 2022).

Kimlik Belgesi Alımı

Kimlik doğrulama için kimlik verilerinin elde edilebilmesi amacıyla başvuru sahibi tarafından ibraz edilen belgenin türüne göre okuma işlemi gerçekleştirilmelidir. Başvuru sahibinin kayıt aşamasında sunduğu kimlik belgesinin türü, bu belgelerin gerçekliğine ilişkin makul güvence elde etmek için gereken kontrol sistemleri üzerinde büyük etkiye sahiptir. Yalnızca kimlik belgesinin ve başvuru sahibinin fotoğrafının yüklenmesinden oluşan bir kimlik doğrulama süreci, kimlik belgesinin ve/veya fotoğrafın manipülasyonuna karşı güvenlik açısından çok zayıf kalacaktır (ETSI, 2021b).

Yalnızca elektronik kimlik belgelerine dayanan elektronik ortamda yapay zekâ tabanlı kimlik doğrulama yöntemi ise erişim ve erişilebilirlik açısından çok sınırlı olacaktır. Bu sınırlamanın başlıca nedenleri; dünya çapında, elektronik kimlik belgelerinin yaygınlığın, geleneksel kimlik belgelerine kıyasla hala ciddi oranlarda az olması ve yakın alan iletişimi okuyucuların, eski ve düşük modelli akıllı telefonlarda yaygın olarak bulunmamasıdır. Diğer yandan geleneksel kâğıt tabanlı kimlik belgelerinin çoğu fiziksel mevcudiyet ile eşdeğer güvence sağlayan araçlar ile gerçekleştirilen elektronik ortamda kimlik doğrulama süreçleri düşünülerek tasarlanmadığından, çok sayıda zorluğa neden olsalar bile hizmetleri geniş çapta erişilebilir kılmaktadırlar (ENISA, 2022).

Elektronik kimlik belgesi veya pasaportun kimlik doğrulama aracı olarak kullanıldığı süreçler bazı güvenlik problemlerini beraberinde getirmektedir. Bu problemlerden biri; başka bir kimlik belgesinin çipinden kopyalanan bir bilgi paketinin kimlik doğrulamasında kullanılan kimlik belgesinin üzerine eklenmesi ile oluşan güvenlik problemidir. Olası diğer bir güvenlik problemi ise; kimlik

doğrulama işlemi esnasında, karşılaştırılmak üzere kimliği doğrulanacak bireyden anlık olarak elde edilen fotoğraf görüntüsü yerine bir saldırı ile farklı bir fotoğrafın kimlik doğrulama sürecinde kullanılması durumudur. Sunucu tabanlı bilgi işlemenin yapıldığı süreçlerde güvenlik önemli bir husustur. Bu sebeple, kimlik doğrulama süreçleri tasarlanırken olası tüm saldırı çeşitleri değerlendirilerek sistem tasarımı yapılmalıdır (ETSI, 2021b).

Kimlik Belgesi Doğruluk Kontrolü

Elektronik ortamda gerçekleştirilecek olan herhangi bir kimlik doğrulama işlemi için öncelikle başvuru sahibinin sunduğu işleme tabi olacak kimlik belgesinin geçerli bir belge olduğu ve sahte olmadığı doğrulanmalıdır. Bir kimlik belgesinin doğrulanması işlemi için, belgenin iptal edilmediğinin ve düzenleyen kurum tarafından geçersiz ilan edilmediğinin kontrolü sağlanmalıdır.

Kimlik belgesi doğruluk kontrolleri, başvuru sahibi tarafından sunulan kimlik belgesinin türüne göre değişiklik göstermektedir. Kimlik belgesinin elektronik olması halinde, kimlik belgesinin çipinde saklanan başvuru sahibinin fotoğrafı gibi kişisel verilerinin kimliğini doğrulamak için açık anahtar altyapısı kullanılmaktadır. Açık anahtar altyapısı, çipte elektronik olarak depolanan verilerin kimliğini doğrulamayı sağlamaktadır. Açık anahtar altyapısında, tüm güvenlik mekanizmalarının tam ve doğru bir şekilde uygulanması, mevcut teknolojilerle yapının ihlâl edilmesini imkânsız hale getirmektedir. Ancak açık anahtar altyapısı mekanizmaları, kimliği doğrulanacak bireyin o anda kimliğini doğrulamak için kullanılan cihazı tuttuğuna dair bir kanıt sağlamamaktadır.

Yalnızca karttan oluşan geleneksel kimlik belgeleri söz konusu olduğunda ise başvuru sahibinin kullandığı cihazın kamerası ile elde edilen deliller üzerinde, optik karakter okuma teknolojisi aracılığıyla veri doğrulama kontrolleri, tutarsızlık ve sahtecilik göstergeleri veya bir yüz fotoğrafının değiştirilmesini tespit etmeyi amaçlayan görsel ve piksel düzeyinde analizler dahil olmak üzere orijinallik kontrolü yapılabilmektedir (ENISA, 2022).

Yüz Karşılaştırma

Elektronik ortamda yapay zekâ tabanlı bir kimlik doğrulamanın yüz karşılaştırma aşamasına geçebilmesi için biyometrik verilerin alınması sonrası gerçekleştirilen canlılık kontrolü adımı ile kimlik belgesi alımı sonrası gerçekleştirilen

kimlik belgesi doğrulama adımlarının başarılı şekilde tamamlanmış olması gerekmektedir.

Yüz karşılaştırma aşamasında gerçekleştirilen yüz tanıma işlemi, genellikle makine öğrenmesi ve derin öğrenme gibi yapay zekâ teknolojilerine dayanmaktadır. Bir bireyin kimliği, biyometrik yüz görüntüsünün fotoğraf veya video ile alınması sonrası yüz tanıma algoritmaları kullanılarak doğrulanmaktadır (Yaman, 2018). Yüz karşılaştırma işlemi, bireyin yüzünün algılanması, algılanan yüz görüntüsünün analiz edilmesi ve yüz eşleştirme oranları değerlendirilerek yüz tanıma işleminin tamamlanması adımlarından oluşmaktadır (Aws, 2023).

Kimliği doğrulanacak başvuru sahibinin yüz görüntüsünün yakalanması için 2D veya 3D sensörler kullanılabilmektedir. Başvuru sahibinin yakalanan yüz görüntüsü belirli algoritmalar ile elektronik bir şablona dönüştürülmekte ve veri tabanında tutulan mevcut şablonlar ile yüz karşılaştırması yapılarak yüz tanıma işlemi sonuçlandırılmaktadır (ENISA, 2020). Yüz tanıma işleminde, zaman içerisinde çok fazla değişiklik göstermeyen gözler arasındaki mesafe, burun genişliği, göz çukurlarının derinliği, elmacık kemiklerinin şekli ve çene hattı uzunluğu gibi bireye ait yüz verilerine odaklanılmaktadır. Günümüzde yüz biyometrisi verilerine dayalı gerçekleştirilen kimlik doğrulama işlemleri, mevcuttaki tek teknoloji ve tek mekanizma olarak kabul edilmektedir (ETSI, 2021b).

Yapay zekâ tabanlı bir kimlik doğrulama sürecinde yüz karşılaştırmasının performansını ölçmek için Yanlış Kabul Oranı (FAR) ve Yanlış Red Oranı (FRR) kullanılmaktadır. FAR ve FRR; parmak izi, yüz ve retina tanıma gibi biyometrik sistemlerin performansını ölçmek için kullanılan güvenlik ölçüleridir. FAR, yanlış bir şekilde geçerli olarak kabul edilen geçersiz girdileri yani yetkisiz bir kullanıcının yanlışlıkla yetkili bir kullanıcı olarak kabul edilme olasılığını temsil etmektedir. Diğer bir ifade ile FAR, biyometrik bir sistemin bir sahtekârdan alınan bir örneği sistemde kayıtlı bir kullanıcının şablonuyla yanlış eşleştirme oranını ölçmektedir. FRR ise, yanlış bir şekilde geçersiz olarak reddedilen geçerli girdileri, yani yetkili bir kullanıcının yanlışlıkla sahtekâr olarak reddedilme olasılığını temsil etmektedir. Diğer bir ifade ile, FRR biyometrik bir sistemin, kayıtlı bir kullanıcıdan alınan veriyi kaç kez başarısız olarak hatalı eşleştirdiğini ölçmektedir (OECD.AI, 2024). Bir sistemin performansı değerlendirilirken kullanılan FAR ve FRR ölçütlerinin dengeli olması gerekmektedir. Kimlik doğrulama için kullanılan sistemdeki özel gereksinimlere ve güvenlik düzeyine bağlı kalarak FAR ve FRR belirlenmelidir.

Günümüzde yaşanan teknolojik gelişmeler ile birlikte ortaya çıkan dijitalleşme, beraberinde kullanılan sistemlerin güvenliğinin sağlanması ve olası tehditlere karşı önlem alınması gerekliliğini getirmiştir. Yapay zekâ tabanlı bir uygulamanın güvenliği, özellikle hassas alanlarda kullanılan yapay zekâ sistemlerinin ve altyapılarının güvenliği için ön koşul kabul edilebilmektedir. Bu nedenle, bir yapay zekâ tabanlı sistemin manipülasyonlara karşı korunabilmesi için doğrulanabilir, izlenebilir ve şeffaf olmasını sağlamak önemlidir. Avrupa Parlamentosu tarafından 2023 yılında kabul edilen ve 1 Ağustos 2024 tarihinde yürürlüğe giren "*Yapay Zekâ Yasası*", güvenlik açıklarına karşı risk barındıran yapay zekâ tabanlı sistemler için şeffaflık yükümlülüğü getirmektedir. Ayrıca yasa, kabul edilemez düzeydeki risklerden minimum risklere kadar dört seviyeli risk temelli bir yaklaşım öngörmektedir. Yasada yer alan bu risk yaklaşımlarından kabul edilemez olanların kullanılmaması, yine yüksek riskli yapay zekâ yaklaşımında, yapay zekâ tabanlı uygulamalar ve hizmetler için potansiyel riskleri en aza indirmek amacıyla devlet kurumları ve özel şirketlerin zorunlu tutulduğu gerekliliklerin olması gerektiği belirtilmektedir (European Parliament, 2023).

Bazı güvenlik riskleri yapay zekâ tabanlı sistemlere özgü olabilmektedir. Örneğin, yapay zekâ tabanlı bir sistemin eğitim verilerinin kirletilmesi ve kullandığı algoritmaların değiştirilmesi ile yapay zekâ tabanlı sistem tehlikeli bir hale getirilebilir. Tanımlanmak istenen bir yüzün doğru şekilde tanımlanmasını önleyebilecek bu tür saldırgan makine öğrenimi tehditleri, yapay zekâ tabanlı sistemlerin güvenliğine yüksek önem verilmesi gerektiğini göstermektedir (ABD National Science and Technology Council, 2016).

Elektronik ortamda yapay zekâ tabanlı kimlik doğrulama sürecinin başlangıcından sonuçlanmasına kadarki her aşamasında, güvenlik riskleri ile karşılaşılabilir. Kimlik doğrulama sürecinde kimlik avı saldırıları, kimlik belgeleri üzerinde yapılan sahtecilikler, başvuru sahibine ait biyometrik verilerin manipüle edilmesi gibi güvenlik açıkları olabilir. Yüz karşılaştırması, canlılık kontrolü gibi kimlik doğrulama adımları DeepFake, 3D maske, fotoğraf ve video tekrar saldırıları gibi güvenlik açıkları ile karşı karşıya kalabilir. Dolayısıyla, elektronik ortamda yapay zekâ tabanlı kimlik doğrulama süreçlerinde güvenliğin sağlanması ve güvenlik açıklarının önlenmesi için süreci etkileyecek olası tehditlerin bilinmesi ve tespiti önem arz etmektedir. Bir sonraki bölümde elektronik ortamda yapay zekâ tabanlı kimlik doğrulama süreçlerinde yüz karşılaştırma ve canlılık testi evrelerini olumsuz etkileyen DeepFake saldırısı detaylı bir şekilde incelenmiştir.

DEEPFAKE

Günümüzdeki teknolojik gelişmelere bağlı olarak her geçen gün daha profesyonel hale gelen DeepFake; yapay zekâ, yapay sinir ağları ve yapay zekânın alt dalları olan makine öğrenmesi ile derin öğrenme tekniklerinin kullanılması ile bireylerin fotoğraf ve benzeri görüntülerinden yararlanılarak sentetik video veya görüntülerin oluşturulmasına yarayan bir teknolojidir. Dünya Ekonomik Forumu'na (WEF) göre, DeepFake ile üretilen videoların sayısı her geçen yıl %900 oranında bir artış göstermektedir. DeepFake ile, herhangi bir bireyin yüz ve vücudunun dijital olarak değiştirilmesi ile başka bir birey gibi görünmesine yarayan gerçekçi videolar veya görüntüler elde edilebilmektedir. Elde edilen bu video veya görüntüler, genellikle yanlış bilgilerin yayılması ve diğer kötü niyetli amaçlar için kullanılmaktadır. (CyberMag, 2023).

DeepFake ile oluşturulan sahte videolar, video akışının bazı yazılım veya donanım araçları ile dahili olarak değiştirilmesine neden olan video enjeksiyon saldırıları aracılığıyla elektronik ortamda yapay zekâ tabanlı kimlik doğrulama sürecini yanıltmak amacıyla kullanılabilmektedir. Video enjeksiyon saldırıları, yazılım ve donanım düzeyi olarak ikiye ayrılmaktadır. Yazılım düzeyinde bir video enjeksiyon saldırısı, kötü amaçlı olmayan bir yazılıma müdahale etmeyi veya kötü amaçlı bir yazılımı gerçek bir uygulama gibi göstermeyi içermektedir. Bir saldırganın, bir cihazın kamerasına yönelik önceden hazırlanmış Deepfake, fotoğraf veya videoları kimlik doğrulama sürecindeki akışa enjekte etmesi yazılım düzeyinde gerçekleştirilen saldırılara örnek olarak verilebilir (Antispoofing, 2024).

Donanım düzeyinde bir video enjeksiyon saldırısı ise bir bilgisayardan gelen HDMI/USB çıkışını, saldırıya uğrayan bir cihaza ait yerel bir video akışıymış gibi maskelemek için kullanılabilmektedir. Burada görüntü veya videonun fiziksel olarak kameraya sunulması yerine donanımsal bir USB bellek veya kameradan video akışını ele geçiren bir JavaScript kodu kullanılarak video enjeksiyon saldırısı gerçekleştirilmektedir (IDR&D, 2024).

Kameraya sunularak veya doğrudan kamera akışına enjekte edilerek gerçekleştirilebilen DeepFake saldırıları özellikle videolu kanıta dayanan kimlik doğrulama süreçlerine karşı kullanılmaktadır. Kötü niyetli saldırgan kimlik doğrulama sürecinin tüm adımlarını biliyorsa ve sahte videoyu kimlik doğrulama sürecine enjekte edebiliyorsa veya videoyu bir ekrana sunabiliyorsa hem otomatik bir

sistemi hem de operatörlü bir kimlik doğrulama sistemini yanıltması mümkün olabilmektedir (ENISA, 2022).

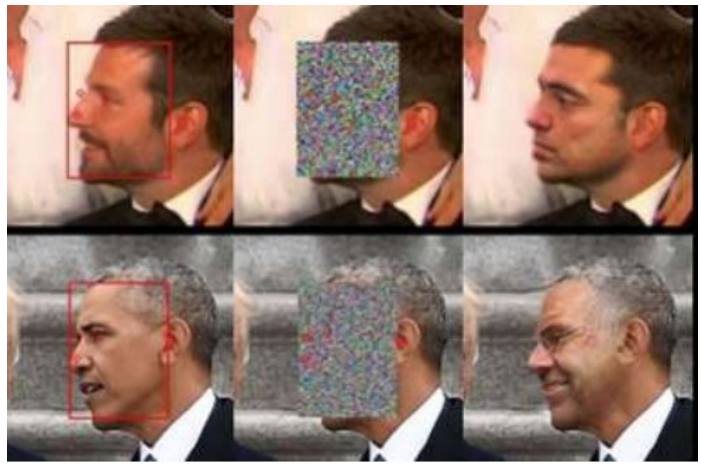
DeepFake'in yüz değiştirme/yerleştirme, ifade değiştirme ve yüz oluşturma olmak üzere bilinen üç yöntemi bulunmaktadır. Bu yöntemler şunlardır (Berk, 2020, s. 1510):

- **Yüz değiştirme/yerleştirme,** hedefteki bir bireyin fotoğrafları kullanılarak bireyin yüzünün başka bir kişiye ait videoya yerleştirilmesi işlemidir (Şekil 4);

Şekil 4 Yüz değiştirme tekniği örneği
((a) orijinal görüntü, (b) DeepFake, (c) hedef birey) (Martı, 2021)

- **İfade değiştirme/yüz yeniden canlandırma/kuklacılık,** kaynak bir videodan elde edilen yüz hareketleri kullanılarak hedefteki bir bireyin yüz videosunun değiştirilmesi işlemidir. Bu yöntem ile hedef kişinin kaş, göz ve ağız ifadelerinin tekrardan oluşturulması ile herhangi bir konu hakkında söylemediği şeyleri söylemiş gibi gösterilmesini sağlayan videolar oluşturulabilmektedir (Şekil 5);

Şekil 5 İfade değiştirme/yüz yeniden canlandırma örneği (Berk, 2020, s. 1510).



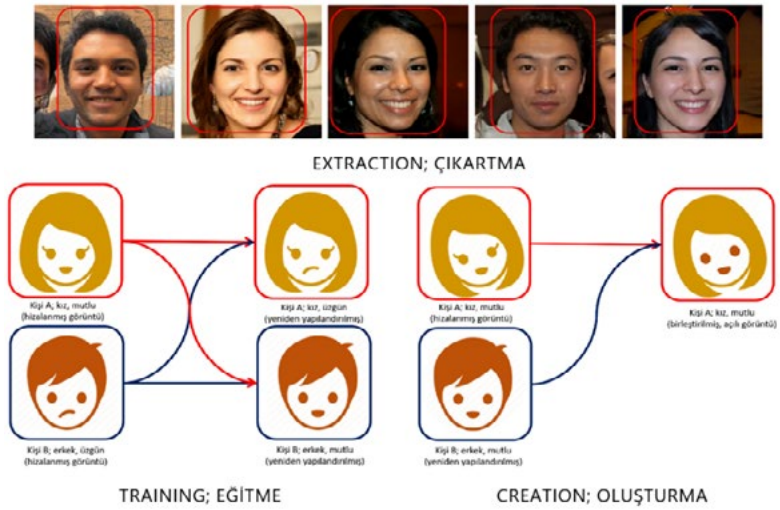
- **Yüz oluşturma,** üretken ve ayrıştırıcı olan iki sinir ağı kullanılarak sahte yüz görüntülerinin oluşturulması işlemidir. Üretken ağın oluşturduğu görüntüler ayrıştırıcı ağ tarafından gerçek olup olmadıkları kontrolünden geçer. Burada amaç üretken kısmın ayrıştırıcı kısmı görüntülerin gerçek olduğuna ikna etmesidir. Ayrıştırıcı kısım üretken kısım tarafından üretilen görüntülerin sahte olduğunu anladığı sürece üretken kısım gerçeğe daha yakın görüntüler üretmeye devam edecektir. Üretken kısım ayrıştırıcı kısmı ikna ederse üretilen görüntü derin öğrenmede kullanılacaktır. Bu yöntem ile pek çok sahte görüntü oluşturulması sağlanmaktadır (Şekil 6).

Şekil 6 Yüz oluşturma örnekleri (Papastratis, 2020).

DeepFake, bir veya daha fazla fotoğraftan başlayarak istenildiği zaman kontrol edilebilen etkileşimli bir 3D dijital kukla kullanılarak da yapılabilmektedir. Bu, saldırganlar tarafından üç boyutlu modeller oluşturmaya yönelik yazılımlar kullanılarak gerçekleştirilebilmektedir. Günümüzde, DeepFake videoları ve etkileşimli DeepFake 3D dijital kuklaları gerçek zamanlı olarak oluşturulabilir durumdadır. Gerçek zamanlı olarak gerçekleştirilen bir saldırı ancak yüksek kalitede ve büyük miktarda bilgi işlem gücünün mevcut olmasıyla elde edilebilmektedir. Dolayısıyla uygulanması oldukça zordur. Ancak, yaşanan teknolojik gelişmelerin etkisi ile bu zorluk engeli her geçen gün azalmaktadır. Günümüzde popüler olan mobil uygulamalardan herhangi biri kullanılarak akıllı telefonlarda oldukça ikna edici DeepFake'ler oluşturulabilmektedir (ENISA, 2022).

Video yapımı ve özel efektler hakkında derin bir bilgiye sahip olmaya gerek kalmadan, makine öğreniminden yararlanan güçlü video işleme ve artırılmış gerçeklik teknikleri ile görüntüsü elde edilebilen herkesin DeepFake videosunun oluşturulması kolay bir hale gelmiştir. Ses klonlama yöntemleri ile daha gerçekçi hale getirilebilen DeepFake'in temel zorluğu, saldırganın, videosunu oluşturmak istediği hedef bireye ait fotoğraf veya videolarından oluşan geniş bir veri kümesine ihtiyaç duymasıdır. Veri kümesinde yer alan hedef bireye ait fotoğraf veya görüntüler yardımı ile DeepFake videosu oluşturmak için kullanılan program eğitilmekte ve eğitim sonucunda öğrenilen bilgiler ile sahte videonun oluşturulması sağlanmaktadır (ENISA, 2022).

Şekil 7 DeepFake temel adımları (Atmaca ve Bakırcı, 2019).



DeepFake'nin çalışma mantığında; veri toplama ve kodlayıcı-kod çözücü adımları ile birlikte çıkartma, eğitme ve oluşturma temel adımları (Şekil 7) olmak üzere genel olarak aşağıda açıklanan beş aşamadan bahsedilebilmektedir (Atmaca ve Bakırcı, 2019; Bernaciak ve Ross, 2022).

- **Kaynak ve hedef videonun toplanması aşaması,** kaynağa ve hedefe ait 4K kalitesinde videoların edinilmesi aşamasıdır. Bu aşamada, DeepFake'in inandırıcı olması ve başarılı sonuçlar verebilmesi için kaynağın ve hedefin benzer yüz şekline ve boyutuna sahip olması, cilt tonu renklerinin benzer olması ve aynı cinsiyete sahip olmaları gibi dikkat edilmesi gereken bazı hususlar mevcuttur.
- **Çıkartma (Extraction) aşaması,** eğitim aşaması öncesi ihtiyaç duyulan büyük miktardaki verinin, hedef bireyin çeşitli yollarla toplanan videolarından ayrıştırılan görüntü parçacıklarından elde edilmesi aşamasıdır.
- **Eğitme (Training) aşaması,** çıkartma aşamasında elde edilen görüntü parçacıkları kullanılarak yapay sinir ağının bir görüntüyü diğer bir görüntüye dönüştürmesi için eğitildiği aşamadır.
- **Dönüşüm aşaması,** bir dizi yüz görüntüsünün kodlayıcı ve kod çözücü ağından tek yönlü olarak geçirildiği ve çıktı olarak bir yazılım aracılığıyla video oluşturabilecek kareler elde edildiği aşamadır.
- **Oluşturma (Creation) aşaması,** DeepFake yazılımının birleştirme özelliğinden yararlanılarak DeepFake'in oluşturulduğu aşamadır. DeepFake yazılımı, derin öğrenme işlemlerinde kullandığı kaynaktan elde edilen fotoğraf veya video verilerinden çıkardığı görüntü parçacıklarını hedefteki yüz görüntüsüne yerleştirmek için programlanmıştır. Kaynaktan elde edilen yüz görüntüleri ne kadar çok ve kaliteli olursa bu aşamanın sonucunda elde edilen video da o derece başarılı olacaktır.

Tüm bunların yanında, DeepFake'in hareketli bir görüntü dışında hareketsiz donuk kareler üzerinde de oluşturulabileceği bilinmektedir. Hatta, DeepFake'in donuk bir kare üzerindeki manipülasyonuna örnek olarak İtalyan ressam Leonardo da Vinci'nin ünlü eseri Mona Lisa'nın yüz ifadesi değiştirilerek oluşturulmuş bir örnek (Şekil 8) bulunmaktadır (Elitaş, 2022, s. 113).

Şekil 8 DeepFake ile gerçekleştirilen donuk kare manipülasyonu (Elitaş, 2022, s. 113).

DeepFake saldırılarının zorluklarından birinin iyi bir veri kümesinin toplanması gerekliliği olmasının yanı sıra unutulmaması gereken bir diğer faktör ise zaman faktörüdür. Pek çok algoritmanın programlandığı görevi gerçekleştirmek için belirli bir hedef üzerinde saatlerce eğitilmesi gerekmektedir. Ancak gelecekteki teknolojik ilerlemeler ile birlikte işlem gücünün gelişmeye devam etmesinin, DeepFake oluşturulurken kullanılan algoritmaların zaman sorununu çözmesi beklenmektedir (ENISA, 2022).

Ayrıca, DeepFake gerçek olanı manipüle etme noktasında yalnızca görüntüler üzerinde veri işlememektedir. DeepFake, gerçekliğin yansıtıcısı olan sesin de derin sinir ağları ile simüle edilmesinde kullanılabilmektedir. Görüntüler üzerinde gerçekleştirilen işlem adımlarına benzer şekilde sesin öğrenilmesi de detaylı bir süreç gerektirmektedir. Bu süreçte sesi taklit edilmek istenen hedef bireye ait ağız hareketleri, tonlama ve vurgulama gibi bireyin sesine ilişkin belirleyici özelliklere dair çok fazla veriye ihtiyaç duyulmaktadır (Elitaş, 2022, s. 113).

Ses manipülasyonu ile kimlik doğrulama sürecinde bir operatör varsa gerçek bir kişiyle etkili bir şekilde konuşuyormuş gibi olacak ve bu kimlik doğrulama sürecinin bir sahtekâr tarafından atlatmasına ihtimal verecektir. 2020 yılında, bir grup hacker "*Business Identity Compromise*" isimli bir yöntem ile Hong Kong bankasından DeepFake ses simülasyonu aracılığıyla 35 milyon dolar çalmayı başarmıştır. Gerçekleştirilen bu soygun dünya genelinde maddi kaybı en yüksek olan olay olarak kabul edilmiştir. Business Identity Compromise, DeepFake teknolojisini kullanan genellikle bir kuruluşun üst düzey yöneticilerinin bilgi ve

sesini kopyalayarak gerçekleştirilen bir saldırı modelidir. Görüntü veya videolara uygulanan DeepFake'ler ile yapılan içerikler ses klonlamalarıyla daha gerçekçi hale gelmektedir. DeepFake'teki ses klonlamaları, monoton konuşma şekli ve metalik ses ile kendini ele verebilmektedir (STM ThinkTech, 2023).

Ek olarak, DeepFake'in görüntüler üzerindeki etkisi elektronik ortamda yapay zekâ tabanlı kimlik doğrulama sürecini etkileyerek sürecin manipülasyonuna neden olabilmektedir.

YAPAY ZEKÂ TABANLI KİMLİK DOĞRULAMA SÜRECİNDE DEEPFAKE

Yapay zekâ ve makine öğrenimi gibi disiplinlerin rekabet ettiği günümüzde araştırmacılar, kimlik doğrulama süreçlerini mümkün olduğunca otonom hale getirmenin yollarını araştırmaktadır. Ancak, elektronik ortamda yapay zekâ tabanlı kimlik doğrulama sürecinde süreci etkileyen DeepFake gibi saldırılar bireylerin kimliğinin doğrulanabilmesi için kullanılan tekniklerin uygulamasının önünde büyük bir sorun teşkil etmektedir.

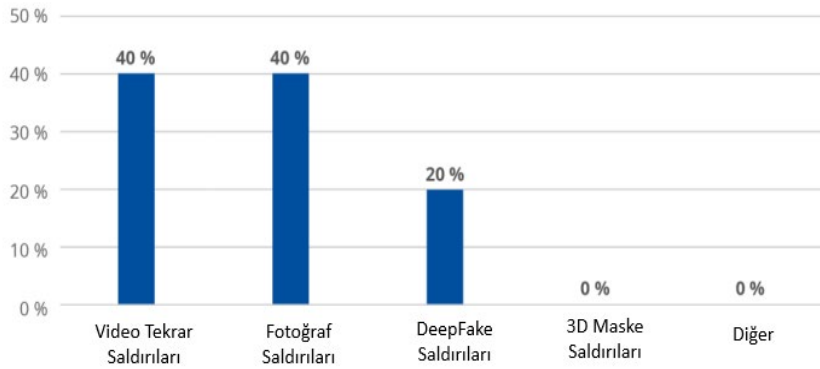
Elektronik ortamda yapay zekâ tabanlı bir kimlik doğrulama sürecinde kullanılan web veya mobil uygulamanın amacı, güvenli bir şekilde başvuru sahibine ait kimlik kanıtlarının toplanmasını sağlamaktır. Ancak dışarıdan gelecek kötü amaçlı herhangi bir müdahale ile kimlik doğrulama sisteminde kullanılan cihazın kamerası manipüle edilebilmektedir. Yani saldırgan kimlik doğrulama sistemine gönderilen video akışını değiştirmek için kimlik doğrulama uygulamasının mimarisine müdahale edebilmekte ve sahte videolar cihaz kamerasından geliyormuş gibi kimlik doğrulama sistemine kanıt olarak sunulabilmektedir.

Günümüzde, film sektörü gibi sektörlerde bir aktörün daha genç veya yaşlı gösterilmesi gibi iyi niyetli amaçlar için DeepFake teknolojisi kullanılsa da DeepFake teknolojisinin iyi niyetli amaçlar dışında kullanılmasının büyük riskler oluşturduğu bilinmektedir. Son yıllarda teknolojide yaşanan gelişmeler son derece gerçekçi görüntüler ve videolar üretmekte kullanılan DeepFake teknolojisinin tespit edilmesini zorlaştırmaktadır. Bazı karmaşık olmayan DeepFake görüntü ve videolarının tespitinde aktif veya pasif kontrollerin etkili olduğu, ancak daha karmaşık bir yapıya sahip DeepFake'lerin gerçeğe yakın görüntü ve video sunmasının elektronik ortamda yapay zekâ tabanlı kimlik doğrulama kontrollerini

atlatmasına olanak tanıdığı düşünülmektedir (STM ThinkTech, 2023).

Son dönemlerde, mevcut saldırıların başarı oranları göz önüne alındığında DeepFake saldırılarının giderek yaygınlaştığı ve geleceğe yönelik en endişe verici saldırılar arasına girdiği (Şekil 9) görülmektedir (ENISA, 2022). Saldırganın hedefin gerçek görüntülerini veya ham videolarını kimlik doğrulama sistemine enjekte ederek kullandığı basit düzeydeki saldırılar aktif ve pasif canlılık kontrollerini atlatmak için yeterli olmamaktadır. Ancak yeni ortaya çıkan ve gelişmiş DeepFake'ler kimlik doğrulama sistemlerindeki aktif ve pasif canlılık kontrollerini atlatabilmektedir.

Şekil 9 Mevcut saldırıların başarı oranları (ENISA, 2022)



Gelecekteki tehditler arasında sayılan ve yasa dışı veya etik olmayan amaçlar için kullanılabilen DeepFake; görüntü, ses ve video oluşturmak veya değiştirmek için orijinal görünen sentetik içerikler sağlayan yapay zekâ tabanlı bir teknolojiyi ifade etmektedir. Teknolojik olarak sürekli gelişim gösteren ve dijital medyayla birbirine bağlanan dünyada DeepFake oluşturma maliyetlerinin önemli ölçüde azalmasıyla birlikte, DeepFake'ler değişik sektörlerde önemli bir hale gelmiştir. DeepFake'ler eğitim, sanat, dijital yeniden yapılanma, kamu güvenliği ve eğlence endüstrisi gibi farklı sektörleri dönüştürme potansiyeline sahip olduğu gibi kötü niyetli saldırganlar tarafından saldırı amaçlı da kullanılabilmektedir (ENISA, 2023a).

Elektronik ortamda yapay zekâ tabanlı kimlik doğrulama sürecinin bir mobil uygulama veya web uygulaması üzerinden telefon veya bilgisayara ait kameralar

kullanılarak gerçekleştirilmesi, DeepFake kullanılarak gerçekleştirilen video enjeksiyon saldırılarına karşı sistemi savunmasız kılmaktadır. Cihazın kontrolünün saldırganda olması, her türlü güvenliğin saldırgan tarafından aşılabilmesi, yeni güvenlik açıklarına karşı daha sağlam yöntemlerin geliştirilmesi gerektiğini göstermektedir. Bir cihazı manipüle eden saldırıların önüne geçebilmek için saldırı adımlarının iyi bilinmesi gerekmektedir. Cihaz manipülasyonu ile saldırı gerçekleştirme işleminin adımları şunlardır (Carta vd., 2022, s. 92):

- Saldırı için kullanılacak cihazın kontrollerini sıfırlamak,
- Kimlik doğrulama işleminin gerçekleştirileceği uygulamanın gizliliğini kaldırmak,
- Uygulamanın kodunu kaynak koda dönüştürmek,
- Uygulamanın hangi işlevlerinin kamerayı çağırdığını, kamera tarafından çekilen görüntülerin nerede saklandığını ve görüntü formatını tespit etmek,
- Kamera tarafından alınan bilgileri yeniden yönlendirerek saldırı cihazından gelen görüntüleri kameradan geliyormuş gibi kimlik doğrulama sistemine yönlendirmek.

Saldırgan saldırıları iki farklı şekilde sisteme enjekte edebilmektedir (Carta vd., 2022, s. 92):

- Enjekte edilecek videolar, uygulama tarafından talep edilen talimatlara göre gerçek zamanlı olarak yeniden yapılandırılabilir; veya
- Enjekte edilecek videolar, uygulamanın hafızasında kayıtlı olan talimatlara göre önceden hazırlanabilir.

Gerçek zamanlı video yapılandırılmasında saldırganın daha fazla çalışması gerekir, ancak video akışında herhangi bir kusur görünmez ve son videoyu oluşturmak için zaman kaybı yaşanmaz. Önceden hazırlanan videolar ise saldırgan açısından kolaylık sağlasa da video akışında oluşacak kesintiler (örneğin; kafanın konumunda yaşanacak değişiklikler) saldırı için dezavantaj oluşturmaktadır (Carta vd., 2022, s. 92).

Bununla birlikte, elektronik ortamda yapay zekâ tabanlı kimlik doğrulama sürecindeki yüz tanıma sistemine uygulanan manipülasyonlardaki DeepFake'ler üç şekilde tanımlanabilmektedir (STM ThinkTech, 2023):

- Bir bireyin yüz görüntüsü başka bir bireyin yüz görüntüsü ile değiştirildiğinde yüz görüntüsünün bazı noktalarında ten rengi ve doku geçişlerinden kaynaklı bozulmalar söz konusu olabilir.
- Özelikle bireyin diş ve gözlerinde yer alan detaylarda fark edilebilir derecede dokusal farklılıklar ve bulanık görünmeler olabilir.
- Bireyin yüz ifadelerinde veya aydınlatma sonucu yüzde oluşan gölgelenmelerde başın hızla hareket ettirilmesi sonucu hatalar oluşabilir.

Güvenlik açıklarına karşı, elektronik ortamda yapay zekâ tabanlı kimlik doğrulama sürecinde kimlik kanıtı olarak başvuru sahibinden toplanan verilerin güvenliği için hizmet sağlayıcı sistemleri üzerinde önlemlerinin alınması, ek olarak başvuru sahibinin yapay zekâ tabanlı kimlik doğrulama süreci için kullandığı cihaz kamerası ile işletim sistemi arasında karşılıklı kimlik doğrulama ve güvenli iletişim kanalı protokollerinin uygulanması gibi çözümler önerilmektedir. Elektronik ortamda yapay zekâ tabanlı kimlik doğrulama için kullanılan sisteme DeepFake'in enjekte edilmesinin önüne geçilebilmesi için kimlik doğrulamanın gerçekleştirildiği cihazın kurcalamaya karşı korumalı olması da gerekmektedir (Carta vd., 2022, s. 92).

Tipik bir yüz tanıma içeren elektronik ortamda yapay zekâ tabanlı kimlik doğrulama sistemi,

- Sisteme kayıtlı bir yüz kimliğine karşı kimlik doğrulama tanımlayıcısı olarak başvuru sahibi tarafından sağlanan tek bir fotoğrafı kullanan görüntü tabanlı,
- Başvuru sahibinin kendi video klibini yüklemesini gerektiren sessizliğe dayalı,
- Başvuru sahibinin kimlik doğrulama sistemi tarafından belirlenen eylemleri gerçekleştirmesini gerektiren eylem tabanlı,
- Bir başvuru sahibinin istemli konuşmasını, o kullanıcının konuşma modeli için sistemin veri tabanı girişiyle eşleştiren ses tabanlı olmak üzere dört farklı vektörden biri ile oluşturulabilmektedir. Her bir vektörde farklı saldırı türü ile karşılaşılabilmektedir.

Bu saldırı türlerinin önüne geçmek için mevcut teknolojilerde;

- Kimlik doğrulamanın başvuru sahibinin kamera akışındaki tek bir kareye dayandığı görüntü tabanlı kimlik doğrulama yönteminin terk edilmesi,

- Görüntü ve ses alanlarında DeepFake tespit sistemlerinin daha esnek ve kapsamlı bir şekilde güncellenmesi,
- Başvuru sahibinin videosundaki ses tabanlı kimlik doğrulamanın dudak hareketleriyle senkronize edilmesinin zorunlu olması ve
- Başvuru sahibinin DeepFake sistemleri tarafından yeniden üretilmesi henüz mümkün olmayan yüzün kısmi olarak karartılması veya profil görünümlerinin sağlanması gibi jest ve hareketleri gerçekleştirmesinin zorunlu tutulması gibi yöntemler ile iyileştirmelerin yapılmasının olumlu sonuçlar vereceği düşünülmektedir (Wang vd., 2022; Anderson, 2022).

Son dönemlerde araştırmacılar, akademisyenler, özel şirketler ve farklı kurum ve kuruluşlar tarafından elektronik ortamda yapay zekâ tabanlı kimlik doğrulama sürecini olumsuz etkileyen saldırılar derinlemesine incelenmekte olup bu saldırılara karşı çeşitli önlemler geliştirilmesine yönelik çalışmalar artırılmaktadır.

Bir DeepFake saldırısına karşı alınan her türlü önlem, anti-DeepFake olarak isimlendirilmektedir. Anti-DeepFake için kullanılacak algoritmalar yüksek düzeyde veriye ihtiyaç duymaktadır. Bu veri ihtiyacının karşılanması amacıyla Facebook Meta ve diğer sektör liderleri tarafından 100.000'den fazla video içeren "*Deepfake Detection Challenge Dataset*" isimli bir veri seti oluşturulmuştur. Oluşturulan veri seti ile DeepFake tespit yöntemlerindeki ilerlemelerin ölçülmesi hedeflenmektedir. Dünyanın dört bir yanından uzmanlar bir araya gelerek DeepFake tespit modellerinin kıyaslanmasına, yeni yaklaşımların denenmesine ve birbirlerinin çalışmalarından yeni şeyler öğrenmelerine, oluşturulan veri setini kullanarak olanak sağlamaktadır (Facebook Meta, 2020). Deepfake Detection Challenge Dataset gibi veri setlerinin oluşturulması anti-DeepFake modellerinin geliştirilmesinin önünü açmaktadır.

Videolardaki anormal göz hareketleri, orantısız parlaklıklar, renk ve ışıkta yaşanan uyumsuzluklar DeepFake'in tespit edilmesinde yardımcı unsurlardır. Mevcut DeepFake'ler dili, ağız içini ve dişleri tam olarak detaylandırmadığından bu alanlardaki bozulmalar DeepFake'i ele verebilmektedir. Bununla birlikte, anti-DeepFake için yapay zekâ yazılımları kullanılabilir. Gelişmiş yapay zekâ teknikleri ile geliştirilmiş yazılımlar yine yapay zekâ teknikleri ile oluşturulmuş DeepFake görüntü ve videolarındaki bozulmaları kolaylıkla tespit edebilir. Ancak anti-DeepFake alanında uluslararası standartların ve düzenlemelerin bulunmaması nedeniyle teknik sorunlar yaşanabilmektedir (STM ThinkTech, 2023).

Bununla birlikte, Amerika Birleşik Devletleri ve Çin arasında kurulan yeni bir araştırma birliği tarafından, yüz tanıma içeren dünyadaki en büyük kimlik doğrulama sistemleri üzerinde DeepFake duyarlılık testleri geçekleştirmiş ve gerçekleştirilen testlerin sonucunda, yeni ortaya çıkan ve her geçen gün gelişen DeepFake saldırılarına karşı yüz tanıma sistemlerinin bazılarının, savunmasız olduğu ortaya çıkarılmıştır. Birçok müşteriye hizmet veren kimlik doğrulama sistemlerindeki DeepFake tespit etme modüllerinin çok fazla hata içerdiği ve kimlik doğrulama sistemlerinde eskimiş DeepFake tekniklerinin kullanılmasının hata oranını artırdığı belirtilmiştir. Ek olarak, genel yüz tanıma sistemlerinde yer alan mevcut konfigürasyonların kadın ve beyaz olmayan bireyleri içermeyerek yalnızca beyaz erkeklere yönelik oluşturulmasının DeepFake riskini kadın ve beyaz olmayan bireyler için artırdığı tespit edilmiştir. Bu durum, belirli bir grup insan için önemli güvenlik riskleri oluşturabilecek hususların bulunduğunu göstermektedir (Anderson, 2022).

Ayrıca, Çin DeepFake faaliyetleriyle ilişkili tehlikeleri azaltmak amacıyla derin sentez/DeepFake teknolojisine ilişkin derin sentez hizmet sağlayıcıları ve kullanıcılarını içeren hükümler yayımlamıştır. Hükümler genel olarak, metin oluşturma veya değiştirme, ses içeriği oluşturma veya değiştirme, konuşma dışı içerik oluşturma veya değiştirme, yüz oluşturma veya değiştirme gibi teknikleri kapsamaktadır. Derin Sentez Hükümleri, derin sentez hizmet sağlayıcılarının ana yükümlülüklerini açıkça belirtmektedir. Derin Sentez Hükümlerine göre derin sentez hizmet sağlayıcıları; veri güvenliği ve kişisel verilerin korunması, şeffaflık, içerik yönetimi ve etiketleme, teknik güvenlik gibi yükümlülükleri yerine getirmekle sorumlu tutulmaktadır (Interesse, 2022; Çin Siber Uzay İdaresi, 2022).

Sonuç olarak, elektronik ortamda yapay zekâ tabanlı bir kimlik doğrulama sürecinde güvenliğin sağlanması ve güvenlik açıklarının önlenmesi için süreci etkileyecek DeepFake gibi olası tehditlerin bilinmesi, tespiti ve bu saldırılara karşı anti-DeepFake önlemlerinin her geçen gün geliştirilmesi önem arz etmektedir.

DEĞERLENDİRME

Dijitalleşme ile birlikte, önem kazanan elektronik ortamda yapay zekâ tabanlı kimlik doğrulama yöntemi, kimlik belgesinde yer alan yüz fotoğrafının başvuru sahibinin canlılığı kanıtlanmış yüz görüntüsü ile karşılaştırılmasına dayanmaktadır. Bu kimlik doğrulama yönteminde, sürecin kötü niyetli bir saldırgan tarafından manipüle edilme ihtimali her zaman mevcuttur. Kimlik doğrulama süreçlerinin vazgeçilmez bir parçası olan kimlik belgesine ve bir bireyin benzersiz şekilde tanınmasına olanak veren yüz görüntüsünün kimlik doğrulama sürecinde kullanılmasına ilişkin bazı güvenlik açıkları ile karşılaşılabilmektedir. Kimlik doğrulama sürecinin doğru bir şekilde sonuçlandırılabilmesi ve saldırganların manipülasyonlarından korunabilmesi için güvenlik açıklarına karşı önlemler alınması gerekmektedir.

Dijitalleşme ile gelen güvenlik hususu sistemlerin donanımsal güvenliğinden yazılımsal güvenliğine ve vatandaşların kişisel bilgilerinin korunmasına kadar pek çok konu ile ilişkilendirilebilmektedir. Bir yapay zekâ sistemi, kendi güvenlik açıkları veya bağlı olduğu diğer mekanizmaların güvenlik açıkları nedeniyle güvenlik tehditlerine karşı savunmasız kalabilmektedir. Güvenli bir yapay zekâ sisteminin geliştirilmesi, geliştirme aşamasından son aşamaya kadar her aşamada güvenlik açıklarının ve risklerinin dikkate alınmasını içermektedir (ENISA, 2023b).

Günümüzde DeepFake teknolojisinin anti-DeepFake tekniklerinden daha hızlı bir şekilde gelişiyor olması ve DeepFake saldırıları ile kimlik doğrulama sistemlerinin aldatılabilmesi nedeniyle yüz tanımanın kimlik doğrulama sistemlerinde tek başına kimlik doğrulama çözümü olarak kullanılması tavsiye edilmemektedir. Yapay zekâ yazılımı ile otomatikleştirilmiş kimlik doğrulama sistemlerinde, yapay zekânın başvuru sahibini tanımlamak için kullandığı doğruluk yüzdesinin önceden belirlenmiş bir eşik değerinin üzerinde olması gerekmektedir. Doğruluk değerinin bu eşik değeri altında kaldığı durumlarda kimlik doğrulama işlemi için insan müdahalesi gerekli olabilmektedir. Bu durumda, bir insan operatör aracılığıyla başvuru sahibinin kimliğinin doğrulanma işlemi teyit edilebilir. Yapay zekâ, yüz karşılaştırması gibi görevlerde insanlardan daha yetenekli olabilmesine rağmen, fotoğrafların çekildiği alanları analiz etmesi gibi görevlerde iyi değildir. Bu da fotoğraflarda yer alan bağlamsal öğelerin tespit edilmesi, başvuru sahibinin bilinçsiz olduğu veya tehdit edilerek kimlik doğrulama süreçlerine zorlandığı

gibi durumların tespitinde yine insan müdahalesinin gerekebileceği anlamına gelmektedir. Teknolojik gelişmelere bağlı olarak, yapay zekânın ihtiyaç duyduğu büyük veri sorunlarının hallolması ile bu durumun değişebileceği düşünülmektedir. Ancak şimdilik yapay zekâ tabanlı bir kimlik doğrulama sürecinde insan operatörlere de ihtiyaç duyulmaktadır (ENISA, 2022).

Elektronik ortamda yapay zekâ tabanlı kimlik doğrulama sürecinde karşılaşılabilecek saldırılara karşı hangi önlemin uygulanacağına dair net bir seçim bulunmamaktadır. Yapay zekâ tabanlı kimlik doğrulama yöntemini kullanacak işletmenin türü, işletmenin hizmet verdiği kullanıcının türü ile sayısı ve işletmenin kimlik doğrulama sürecinde elde etmek istediği güven düzeyi gerçekleştirilen kimlik doğrulama sürecini manipüle etmek için kullanılabilecek saldırılara karşı alınacak önlemlerin seçimi ile doğrudan ilişkidir. Mühendislik problemlerinin pek çoğunda olduğu gibi kimlik doğrulama sürecinde alınacak karşı önlemleri seçerken kullanılabilirlik ve etkinlik arasında doğru bir denge oluşturmak gerekmektedir. Ancak kullanılacak karşı önlemlerin etkinliği konusunda %100'lük bir güvenceye ulaşmak mümkün değildir. Karşı önlemlerin temel amacı, sahtekârlığı gerçekleştirmenin zorluğunu ve maliyetini elde edilecek potansiyel faydalardan daha yüksek tutmaktır (ENISA, 2022).

Bununla birlikte dünya genelinde ülkeler ve uluslararası kuruluşlar dijital güvenlikle ilgili araştırmalar yaparak güvenlik açıklarına karşı oluşabilecek tehditlerin, saldırıların ve siber olayların tespiti ve yönetimine yönelik zorlukları ele almaya çalışmaktadır. Ayrıca, ülkeler ve uluslararası kuruluşlar tarafından kimlik doğrulama, yapay zekâ ve DeepFake gibi pek çok konuda çalışmalar yürütülmektedir (Tablo 1).

Tablo 1 Bu çalışmada bahsi geçen ülkeler ve uluslararası kuruluşların çalışmalarına ilişkin özetler

ÜLKE/ KURULUŞ	ÇALIŞMA ADI	İÇERİK
ABD	National Science and Technology Council	Algoritmaların manipüle edilmesi gibi yapay zekâlı sistemlere özgü bazı güvenlik riskleri ele alınmaktadır.
Çin Siber Uzay Ajansı	Provisions on the Administration of Deep Synthesis Internet Information Services	DeepFake faaliyetleriyle ilişkili tehlikeleri azaltmayı amaçlayan hükümler yayımlanmıştır.
ENISA	eIDAS Compliant eID Solutions	eID araçları için kullanılan temel teknolojilerle ilgili güvenlik hususları ve öneriler ele alınmaktadır.
ENISA	ENISA Remote ID Proofing	Kimlik doğrulama için en yaygın yöntemlere genel bir bakış sunulmaktadır.
ENISA	ENISA Remote Identity Proofing- Attacks & Countermeasures	Yüz tanıma sistemlerini kandırmayı amaçlayan yüz sunumu saldırıları ele alınmaktadır.
ENISA	Identifying Emerging Cyber Security Threats and Challenges for 2030	Gelecekteki siber güvenlik tehditleri araştırılmaktadır.
ENISA	Artificial Intelligence and Cybersecurity Research	Siber güvenlik için yapay zekâ ve yapay zekânın güvenliğini sağlama konusunda araştırma ihtiyaçlarını belirlemektedir.

ETSI	ETSI TS 119 461 V1.1.1 (2021-07)	Güven hizmeti konularının kimlik doğrulamasını sağlayan güven hizmeti bileşenleri için politika ve güvenlik gereksinimlerini belirtmektedir.
ETSI	ETSI TR 119 460 V1.1.1 (2021-02)	Güvenilir hizmetlere ilişkin kimlik doğrulama teknolojileri ve düzenleyici gereklilikleri incelenmektedir.
European Parliament	Artificial Intelligence ACT	Yapay zekâ sistemlerine risk temelli bir yaklaşım getirerek belirli sınıflara ayrıştırılması amaçlanmaktadır.
NIST	Digital Identity Guidelines.	Dijital kimlik hizmetlerine ilişkin teknik gereksinimler sağlamaktadır.
NIST	Digital Identity Guidelines Authentication and Lifecycle Management.	Dijital kimlik hizmetlerini kullananlar için kimlik doğrulama ve yaşam döngüsü yönetimi gereksinimlerini sunmaktadır.
OECD.AI	Catalogue of Tools & Metrics for Trustworthy AI.	Yapay zekânın güvenilirliğini ve risklerini ölçmek ve değerlendirmek için teknik metrikler ve metodolojiler içermektedir.

SONUÇ

Elektronik ortamda kimlik doğrulama işlemleri tüm dünyada olduğu gibi ülkemizde de temel bir öneme sahiptir ve dijital dönüşüm hamleleri ile birlikte giderek daha fazla önem kazanmaktadır. Ancak yapay zekâ tabanlı kimlik doğrulama yöntemini tercih eden ülkelerin sayısı ve bu konuya ilişkin düzenlemeler sınırlı olmakla birlikte henüz net bir standart veya düzenleme de bulunmamaktadır. Ayrıca, ülkelerin yapay zekâ tabanlı kimlik doğrulama süreçlerindeki güvenlik hususlarına ilişkin özel düzenlemelerinin de henüz bulunmadığı bilinmektedir.

Kimlik belgesinde yer alan yüz fotoğrafının başvuru sahibinin canlılığı kanıtlanmış yüz görüntüsü ile karşılaştırılmasına dayanan elektronik ortamda yapay zekâ tabanlı kimlik doğrulama yönteminde, kimlik doğrulama sürecinin doğru bir şekilde sonuçlandırılabilmesi ve saldırganların manipülasyonlarından korunabilmesi için güvenlik açıklarına karşı önlemler alınması gerekmektedir.

Yeni ortaya çıkan DeepFake saldırılarına karşı yüz tanıma sistemleri savunmasızdır ve yüz tanıma sistemlerinin savunma yeteneklerinin DeepFake saldırılarına karşı artırılması gerekmektedir. Çoğu yüz tanıma sistemi, anti-DeepFake tespitlerini içermemektedir. Anti-DeepFake tespiti içeren sistemlerin ise hizmet sağlayıcılar tarafından farklı amaçlar göz önünde bulundurularak geliştirilmiş olması yalnızca belirli türde DeepFake saldırılarına karşı savunma uygulayabilmelerine neden olmaktadır. Dolayısıyla, çok çeşitli yöntemler kullanılarak gerçekleştirilen DeepFake yöntemleri için genel bir savunma henüz sağlanamamış olup bu hususta çalışmalar gerçekleştirilmesi önem arz etmektedir.

Elektronik ortamda yapay zekâ tabanlı kimlik doğrulama süreçlerinde karşılaşılabilecek DeepFake saldırıları için kurcalamaya karşı korumalı donanım ve anti-DeepFake çözümlerinin kullanılması, DeepFake teknolojileri geliştikçe anti-DeepFake tekniklerinin güçlendirilmesi ve DeepFake teknolojilerinin kötü amaçlı kullanımının önüne geçilebilmesi için uluslararası geçerli standartların ve düzenlemelerin geliştirilmesi gerekmektedir.

Yeni gelişen ve uygulanmaya başlayan bir teknolojik gelişmenin kullanımına ilişkin belirli standartların olmaması hem ülke içinde hem de uluslararası alanda birlikte çalışabilirlik esaslarında uyumsuzluklar yaşanmasına neden olabilmektedir. Aynı şekilde, vatandaşların erişimine sunulmuş olan hizmetlere entegre edilen yeni teknolojik gelişmelerin kullanımı ve hizmet sunumu ile ilgili denetim faaliyetlerinin belirlenebilmesi için de bu teknolojilere ilişkin regülasyon çalışmalarının yapılması zorunluluk arz etmektedir.

Saldırı senaryolarının her geçen gün hızlı bir şekilde artırmasından dolayı, dijital dünyada daha fazla standart, sertifikasyon ve test yönteminin ortaya çıkması beklenmektedir. Dolayısıyla, yapay zekâ tabanlı kimlik doğrulama süreçleri için bugün itibariyle belirlenmiş bir standart uygulama bulunmadığı ve bu teknolojinin tüm düzenleyici otoriteler tarafından henüz onay almamış yeni bir teknolojik gelişme olarak sayıldığı göz önünde bulundurulmalıdır. Ayrıca, yapay zekâ tabanlı kimlik doğrulama yöntemlerinde hangi tekniklerin benimseneceği ve hangi kontrollerin uygulanması gerektiği, büyük ölçüde sistemin tasarlandığı kullanım durumlarına ve risk temelli bir yaklaşımı izleyerek sağlaması beklenen güvence düzeyine bağlı olmalıdır.

Bununla birlikte, şirketlerin yüz tanıma ürün ve hizmetlerini geliştirirken verilerin hassasiyetini göz önünde bulundurması, bireylerin açık rızası doğrultusunda yüz tanıma işlemlerinin gerçekleştirilmesi konusunda hassasiyet göstermeleri gerekmektedir.

Sonuç olarak, bir yüz tanıma teknolojisine %100 güvenilmesinin zor olduğu, halen araştırılması ve çözüme kavuşturulması gereken hususların bulunduğu, yapay zekânın yaşam kalitesini iyileştirme potansiyeli olduğu gibi güvenlik açıkları dolayısıyla kötü niyetli saldırganlar tarafından manipülasyonlara uğrama olasılığı, dolayısıyla yapay zekâ sistemlerinin her biri için farklı denetim biçimlerinin mümkün olduğu ve her birinin farklı güçlü veya zayıf yönleri olduğu, yapay zekâya ilişkin yüksek kalitede teknik standartların bulunmaması nedeniyle yeni saldırılara açık olduğu ve yeni güvenlik açıkları ile karşılaşılma ihtimalinin olduğu unutulmamalıdır.

Buna ek olarak, elektronik ortamda yapay zekâ tabanlı kimlik doğrulama süreçlerinde karşılaşılabilecek gerçeğe yakın düzeyde videolar veya sesler oluşturulmasına yarayan DeepFake'in hakaret, gözdağı, gasp, zorbalık ve güvenin zedelenmesi gibi psikolojik zararlarının; kimlik hırsızlığı, dolandırıcılık ve itibar kaybı gibi mali zararlarının ve haber medyasının manipülasyonu, adalet sistemine zarar verilmesi gibi toplumsal zararlarının bulunabileceği hususları da incelenmelidir.

Ayrıca, DeepFake videolarının daha gerçekçi hale getirilmesine neden olan ses klonlama yöntemine ilişkin geliştirme, kullanım, tespit etme ve önlem alma gibi konular da ayrıntılı bir şekilde ele alınmalıdır.

KAYNAKLAR

ABD National Science and Technology Council. (2016, Ekim). The National Artificial Intelligence Research and Development Strategic Plan. https://www.nitrd.gov/pubs/national_ai_rd_strategic_plan.pdf adresinden 1 Temmuz 2024 tarihinde erişildi.

Anderson M.. (2022, Aralık 9). Deepfakes Can Effectively Fool Many Major Facial 'Liveness' APIs. https://www.unite.ai/deepfakes-can-effectively-fool-many-major-facial-liveness-apis/ adresinden 27 Ekim 2024 tarihinde erişildi.

Antispoofing. (2022, Eylül 15). Video Injection Attacks. https://antispoofing.org/video-injection-attacks/ adresinden 16 Eylül 2024 tarihinde erişildi.

Atmaca Y., Bakırcı M. Ç.. (2019, Aralık 1). DeepFake: Yapay Zekâ ve Bilgisayarlar ile Gerçeği Nasıl Bükeriz?. https://evrimagaci.org/deepfake-yapay-zeka-ve-bilgisayarlar-ile-gercegi-nasil-bukeriz-8088 adresinden 29 Eylül 2024 tarihinde erişildi.

AUTHENTICID (2024). Identity Proofing. https://www.authenticid.com/glossary/identity-proofing/, adresinden 21 Aralık 2024 tarihinde erişildi.

AWS. (2023). Yüz tanıma nedir?. https://aws.amazon.com/tr/what-is/facial-recognition/ adresinden 19 Ağustos 2024 tarihinde erişildi.

Berk M. E.. (2020). Dijital Çağın Yeni Tehlikesi "Deepfake. OPUS Uluslararası Toplum Araştırmaları Dergisi, 28(16), 1510-1523. https://doi.org/10.26466/opus.683819.

Bernaciak C., Ross Dominic A.. (2022, Mart 14). How Easy Is It to Make and Detect a Deepfake?. https://insights.sei.cmu.edu/blog/how-easy-is-it-to-make-and-detect-a-deepfake/ adresinden 29 Eylül 2024 tarihinde erişildi.

Carta K., Barral C., El Mrabet N., Mouille S.. (2022). Video Injection Attacks on Remote Digital Identity Verification Solution Using Face Recognition. Proceedings of the 13th International Multi-Conference on Complexity, Informatics and Cybernetics: IMCIC 2022, 2, 92-97. https://doi.org/10.54808/IMCIC2022.02.92.

Çin Siber Uzay İdaresi. (2022). Provisions on the Administration of Deep Synthesis Internet Information Services. https://www.cac.gov.cn/2022-

12/11/c_1672221949318230.htm.

CyberMag. (2023). Deepfake Videolarının Sayısı Her Yıl %900 Oranında Artıyor!. https://www.cybermagonline.com/deepfake-videolarinin-sayisi-her-yil-900-oraninda-artiyor adresinden 27 Eylül 2024 tarihinde erişildi.

ENISA. (2020). eIDAS Compliant eID Solutions. https://www.enisa.europa.eu/publications/eidas-compliant-eid-solutions.

ENISA. (2021). ENISA Remote ID Proofing. https://www.enisa.europa.eu/publications/enisa-report-remote-id-proofing.

ENISA. (2022). ENISA Remote Identity Proofing - Attacks & Countermeasures. https://www.enisa.europa.eu/publications/remote-identity-proofing-attacks-countermeasures.

ENISA. (2023a). Identifying Emerging Cyber Security Threats and Challenges for 2030. https://www.enisa.europa.eu/publications/enisa-foresight-cybersecurity-threats-for-2030.

ENISA. (2023b). Artificial Intelligence and Cybersecurity Research. https://www.enisa.europa.eu/publications/artificial-intelligence-and-cybersecurity-research.

Elitaş T.. (2022). Dijital Manipülasyon 'Deepfake' Teknolojisi ve Olmayanın İnandırıcılığı. Hatay Mustafa Kemal Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 19(49), 113-128. https://dergipark.org.tr/tr/pub/hmkusbed/issue/70758/1072624.

ETSI. (2021a). Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects (ETSI TS 119 461 V1.1.1 (2021-07)). https://www.etsi.org/deliver/etsi_ts/119400_119499/119461/01.01.01_60/ts_119461v010101p.pdf.

ETSI. (2021b). Survey of technologies and regulatory requirements for identity proofing for trust service subjects (ETSI TR 119 460 V1.1.1 (2021-02)). https://www.etsi.org/deliver/etsi_tr/119400_119499/119460/01.01.01_60/tr_119460v010101p.pdf

European Parliament. (2023). Artificial Intelligence ACT. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206.

Facebook Meta. (2020, Haziran 25). Deepfake Detection Challenge Dataset. https://ai.meta.com/datasets/dfdc/ adresinden 25 Ekim 2024 tarihinde erişildi.

Freiberg K.. (2024). Active and passive liveness detection – which one should you use for authentication. https://www.bioid.com/blog/2022/06/active-and-passive-liveness-detection-which-one-to-use-for-authentication/ adresinden 16 Ağustos 2024 tarihinde erişildi.

IDR&D. (2024). How AI Can Prevent a Virtual Camera Injection Attack. https://www.idrnd.ai/how-ai-can-prevent-a-virtual-camera-injection-attack/ adresinden 19 Eylül 2024 tarihinde erişildi.

Interesse G.. (2022, Aralık 20). China to Regulate Deep Synthesis (Deepfake) Technology Starting 2023. https://www.china-briefing.com/news/china-to-regulate-deep-synthesis-deep-fake-technology-starting-january-2023/ adresinden 11 Ocak 2024 tarihinde erişildi.

Martı C. C., (2021 Ocak 15). Korkunç Bir Siber Tehlike: Deepfake Nedir, Nasıl Çalışır ve Tehlikeleri Nelerdir?. https://listelist.com/deepfake-nedir/ adresinden 23 Aralık 2024 tarihinde erişildi.

NIST. (2017a). Digital Identity Guidelines. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf.

NIST. (2017b). Digital Identity Guidelines Authentication and Lifecycle Management. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf.

OECD.AI. (2024). Catalogue of Tools & Metrics for Trustworthy AI. https://oecd.ai/fr/catalogue/metrics adresinden 19 Ağustos 2024 tarihinde erişildi.

Papastratis I.. (2020, Haziran 2). Deepfakes: Face synthesis with GANs and Autoencoders, https://theaisummer.com/deepfakes/ adresinden 28 Eylül 2024 tarihinde erişildi.

STM ThinkTech. (2023, Temmuz 24). Yapay Zekâ ile Üretilen İçerikler Tespit Edilebilir mi?. https://thinktech.stm.com.tr/tr/yapay-zeka-ile-uretilen-icerikler-tespit-edilebilir-mi adresinden 1 Ekim 2024 tarihinde erişildi.

Thales. (2020, Aralık 4). Liveness in biometrics: spoofing attacks and detection. https://www.thalesgroup.com/en/markets/digital-identity-and-se-

curity/government/inspired/liveness-detection adresinden 14 Ağustos 2024 tarihinde erişildi.

Yaman A. U.. (2018). Yüz Tanıma Sistemlerinin Yanıltılmasına Karşı Bir Yöntem: Yüz Videolarında Nabız Tespiti ile Canlılık Doğrulaması [Yüksek Lisans Tezi, Ankara Üniversitesi Fen Bilimleri Enstitüsü]. https://acikbilim.yok.gov.tr/bitstream/handle/20.500.12812/45005/yokAcikBilim_10196903.pdf?sequence=-1&isAllowed=y.

Wang L., Li C., Ji S., Zhang X., Xi Z., Guo S., Wang T.. (2022). Seeing is Living? Rethinking the Security of Facial Liveness Verification in the Deepfake Era. 31st USENIX Security Symposium, 2673-2690. https://www.usenix.org/system/files/sec22-li-changjiang.pdf.

Bilgi Teknolojileri ve İletişim Dergisi (BTK DERGİ)
CİLT 3 SAYI 1 OCAK-HAZİRAN 2025 ISSN:2980-1331 E-ISSN: 3023-4239

YAPAY ZEKÂ İLE İLGİLİ GÜNCEL DÜZENLEME ÇALIŞMALARI: AB, ABD VE TÜRKİYE AÇISINDAN İNCELENMESİ

Yasemin YAMAK[1]

Gönderilme Tarihi: 4 Mart 2025

Kabul Tarihi: 29 Mayıs 2025

Review Article / İnceleme Makalesi

ÖZET

Son yıllarda popüler bir konu haline gelen yapay zekâ hâlihazırda gündelik yaşamımızın bir parçası haline gelmiştir. Yapay zekâ kullanımının birçok alanda yaygınlaşmış olması tehditlere ve mağduriyetlere neden olabilme ihtimalini artırmaktadır. Dolayısıyla, yapay zekânın oluşturabileceği tehditler ve yaşatabileceği mağduriyetlerden kaçınabilmek amacıyla yapay zekâya ilişkin hukuki düzenlemelere ihtiyaç duyulmaktadır. Dünyadaki liderlik yarışında ülkeler için önemli bir alan olan yapay zekâ, ülkelerin düzenleme yarışına girdiği bir konu haline gelmiştir. Pek çok ülke ve uluslararası kuruluş, bir taraftan yapay zekâya ilişkin ulusal stratejilerini ortaya koyarak bu teknolojinin geliştirilmesi amacıyla uzman yetiştirmek, girişimlerin önünü açmak ve teknoloji lideri olabilmek için mali yatırımlar yaparken, diğer taraftan da söz konusu teknolojinin düzenlenmesine ilişkin çalışmalar ve araştırmalar yürütmektedir. Bu çalışmada ise Avrupa Birliği ve Amerika Birleşik Devletleri'nin bu alanda yapmış oldukları düzenleme çalışmaları incelenmiştir. Avrupa Birliği'nin Yapay Zekâ Yasası genel bir bakış açısı ile ele alınmıştır. Ayrıca ülkemizde yapay zekânın düzenlenmesine ilişkin çalışmalar ele alınarak birtakım önerilerde bulunulmuştur.

Anahtar kelimeler: *Yapay Zekâ, Yapay Zekâ Düzenleme Çalışmaları, Yapay Zekâ Yasası*

[1] Bilişim Uzmanı, yamakyasemin0853@hotmail.com, ORCID: 0000-0003-3517-9613

Bilgi Teknolojileri ve İletişim Dergisi (BTK DERGİ)
CİLT 3 SAYI 1 OCAK-HAZİRAN 2025 ISSN:2980-1331 E-ISSN: 3023-4239

CURRENT REGULATION STUDIES ON ARTIFICIAL INTELLIGENCE: AN EXAMINATION FROM THE PERSPECTIVE OF THE EU, THE USA, AND TÜRKİYE

ABSTRACT

Artificial intelligence, which has become a popular topic in recent years, has already become a part of our daily lives. The widespread use of artificial intelligence in many areas increases the possibility of causing threats and victimization. Therefore, legal regulations regarding artificial intelligence are needed in order to avoid the threats that artificial intelligence may pose and the victimization it may cause. Artificial intelligence, which is an important area for countries in the global leadership race, has become a subject where countries enter the regulation race. While many countries and international organizations, on the one hand, present their national strategies regarding artificial intelligence, make financial investments to train experts for the development of this technology, pave the way for initiatives and become technology leaders, on the other hand, they conduct studies and research on the regulation of the technology in question. In this study, the regulatory studies carried out by the European Union and the United States in this field were examined. The Artificial Intelligence Law of the European Union was discussed from a general perspective. In addition, studies on the regulation of artificial intelligence in our country were discussed and some suggestions were made.

Keywords: *Artificial intelligence, artificial intelligence regulation studies, artificial intelligence act*

GİRİŞ

Dünya genelinde yaşanan teknolojik ilerlemeler ve gelişmelerle hayatımıza farklı cihazlar, uygulamalar ve sistemler dâhil olmaktadır. 1950'li yıllarda başlayan yapay zekâ serüveni günümüzde herkesin kullandığı aktif bir teknoloji halini almıştır. Yapay zekâ algoritmaları ile kişisel tercihlerimize göre müzik ve film sunan platformlar, yapay zekâ destekli dijital bankacılık ve sanal asistanlar, son dönemde adını sıkça duyduğumuz ChatGPT gibi birçok uygulama halihazırda hayatımızın vazgeçilmez birer parçası olmuş ve yapay zekâ destekli bu uygulamaların kullanımı önemli düzeyde artış göstermiştir. Öyle ki, 2022 yılında piyasaya sürülen yaklaşık 180,5 milyon kullanıcıya sahip olan ChatGPT uygulamasının web sitesine Ekim 2024'te 3,66 milyar giriş yapılmıştır (Duarte, 2024).

Dünya çapında artan yapay zekâ kullanımı, ülke ekonomilerine de büyük katkı sağlamaktadır. Ülkelere sağladığı ekonomik destek ile birlikte bu teknolojinin kullanımı daha da cazip hale gelmiştir. Yapay zekânın pek çok alanda verimlilik artışı sağması, büyük miktarlardaki verileri kısa sürelerde analiz ederek karar alma süreçlerinin hızlanmasını sağlaması ve bireyler için karmaşık ve zor olan işlerin makineler tarafından yapılmasına imkân vermesi gibi büyük avantajları bulunmaktadır. Ancak geliştirilme maliyetlerindeki fazlalık, etik ve ahlaki değerler hususunda sorunlar yaşanabilme ihtimali, tamamıyla kusursuzluk sağlamaması nedeniyle hatalı kararlar verebilmesi gibi dezavantajları da bulunmaktadır. Ayrıca, yapay zekâ teknolojilerinin beraberinde getirdiği bazı risklerden de bahsetmek mümkündür. Bu risklerin en başında veri güvenliği gelmektedir. Yapay zekâ teknolojisinde veri güvenliğinin sağlanması hem kişisel olarak hem de devletler açısından büyük önem arz etmektedir. Bununla birlikte, yapay zekâ sistemlerinde mahremiyetin korunması ve ayrımcılığın önlenmesi de önemli birer unsurdur.

X, SpaceX ve Tesla şirketlerinin sahibi olan Elon Musk, İngiltere'de düzenlenen "Yapay Zekâ Güvenliği Zirvesi"nde yaptığı bir açıklamada yapay zekânın risklerine dikkat çekerek *"İlk kez en akıllı insandan daha akıllı olacak bir şeyle karşı karşıyayız"* ifadelerini kullanmış ve yapay zekâyı var oluşsal bir risk olarak nitelendirmiştir. Kötü niyetli olarak üretilmiş bir yapay zekâ veya kullanımı sonucunda kişilerin zarar görmesi, mağduriyet yaşaması ihtimalleri göz önüne alındığında bu tür sistemlerin denetiminin yapılması veya hukuksal olarak bağlayıcı olan bir düzenlemeye tabi olması gerektiği aşikârdır.

Bu kapsamda ülkeler ve uluslararası kuruluşlar, yapay zekânın hukuki bir zemine oturtulması için çalışmalar yürütmektedir. Teknolojinin gelişiminde öncü olan Avrupa Birliği (AB) ve Amerika Birleşik Devletleri (ABD) yapay zekâya ilişkin araştırmalar yapmakta, yasa tasarıları üzerinde çalışmakta ve tavsiye niteliğinde belgeler yayımlamaktadır. Bu noktada, Avrupa Birliği'nin oluşturduğu Yapay Zekâ Yasası da bu teknolojinin düzenlenmesine ilişkin yayımlanan ilk yasa olması nedeniyle büyük öneme haizdir.

Bu çalışmada, yapay zekâ düzenlemelerine ilişkin AB ve ABD'nin yürüttüğü çalışmalar incelenmiştir. Bu alanda AB'nin yaptığı çalışmalar ve AB Yapay Zekâ Yasası genel olarak irdelenmiş ve ABD'nin yapay zekâya ilişkin hususları nasıl ele aldığı ile ne tür çalışmalar yürüttüğünden bahsedilmiştir. Bunlara ek olarak, ülkemizde yapay zekâ alanında yapılan çalışmalar incelenmiştir.

Yapay Zekâ Kavramı

Türk Dil Kurumu tarafından "İnsanın düşünme, akıl yürütme, öğrenme, kavramları ve nesneleri zihinde canlandırabilme, objektif gerçekleri algılama, yargılama, sonuç çıkarma, bedeni kontrol edebilme, duyguları doğru algılayabilme, değerlendirebilme, icat edebilme vb. yeteneklerinin ve becerilerinin tamamı" zekâ olarak adlandırılmaktadır (TDK, 2024). Doğuştan, herkes tarafından sahip olunan zekâ; eğitim ile öğrenilerek edinilen bilgi ve deneyimler ile geliştirilebilmektedir. İlk defa karşılaşılan bir duruma karşı uyum sağlayabilme, analiz etme ve anlamlandırma vb. yetiler zekâ ile gerçekleştirilmektedir. Buradan yola çıkılarak, bilgisayara herhangi bir problemi anlama, öğrenme ve probleme çözüm getirme yeteneği kazandırılması amacıyla zekâ modellenmiştir. Dolayısıyla, John McCarthy tarafından kavram olarak ortaya atılan yapay zekâ için, insanoğlunun idrakine yönelik olan yetenekleri, bilgisayar sistemlerinin modellemesidir denilebilir (McCarthy, 2007). Başka bir ifade ile yapay zekâ, insanın zekâsını modelleyebilmek için insan gibi akıl yürütme, anlam çıkarma, geçmiş deneyimlerden ders alarak öğrenme gibi yetilerin bilgisayara kazandırılmasıdır.

El-Harezmî tarafından "0" rakamının ve algoritmanın temelinin atılmasının ardından El-Cezeri ile sibernetik bilimi ve hidrolik temelli robotlarla yapay zekânın temelleri oluşturulmuştur (CBDDO, 2021). 1950 yılında Alan Turing'in "Makineler düşünebilir mi?" sorusu ile başlayan yapay zekâ serüveni artık elle tutulur bir ürüne dönüşmüştür. Günümüzde pek çoğumuz tarafından kullanılan yapay

zekâ destekli uygulamalar mevcut olup, bu uygulamalar her geçen gün kendilerini daha da geliştirmektedir. Örneğin; 2019 yılında Open AI, 1,5 milyar parametreli GPT-2'yi yayınlamışken hemen ardından 2020'de 175 milyar parametreli GPT-3'ü yayınlamıştır. 2021 yılına gelindiğinde ise metinsel tanımlamalardan resimleri üretebilen DALL-E yayınlanmıştır (TRAI, 2023). Yapay zekâ her geçen gün artan bir ivme ile gelişim göstermeye devam etmektedir.

1. YAPAY ZEKÂ ALANINDA ULUSLARARASI DÜZENLEME ÇALIŞMALARI

Teknolojinin gelişmesi ile birlikte ülkeler arasındaki rekabet de her geçen gün artmaktadır. Tedarik zincirleri, pazarlama, araştırma gibi pek çok alanda, yapay zekâ teknolojilerinin kullanımı benimsenmiş durumdadır. Bununla birlikte sohbet robotları, görüntü üreten sistemleri yapay zekâ alanında son yıllarda popüler olan uygulamalar arasındadır. Söz konusu uygulamaların gündelik hayatta aktif olarak kullanımı yapay zekânın pazar payını da artırmaktadır. McKinsey'in yıllık "Küresel Yapay Zekâ Durumu Anketi", yapay zekâyı benimseyen organizasyonların oranının 2017'de %20 iken 2022 yılında %50'ye ulaştığını göstermiştir (McKinsey, 2023). 100 milyar ABD Doları değerinde olan yapay zekâ pazarının, 2030 yılına kadar 20 kat artarak 2 trilyon ABD Dolarına ulaşması beklenmektedir (Statista, 2023).

Oxford Insight'ın 2024 yılında hükümetlerin kamu hizmetlerinde yapay zekâyı kullanmaya ne kadar hazır olduğunu ortaya koymak amacıyla yayınlamış olduğu "Hükümet Yapay Zekâ Endeksi" raporu kapsamında 188 ülke incelenmiştir. "Hükümet", "Teknoloji Sektörü", "Veri ve Altyapı" olmak üzere üç ana başlık altında inceleme yapılmış ve ülke sıralamaları yayımlanmıştır. Tablo 2.1'de de bu sıralamadaki ilk 10 ülke gösterilmiş olup Amerika, Singapur ve Kore sıralamada ilk üçte yer almaktadır. (Oxford Insights, 2024).

Tablo 2.1 Ülkelerin Yapay Zekâ Endeksi

SIRALAMA	ÜLKE	PUAN
1	Amerika	87,03
2	Singapur	84,25
3	Kore	79,98

SIRALAMA	ÜLKE	PUAN
4	Fransa	79,36
5	Büyük Britanya ve Kuzey İrlanda Birleşik Krallığı	78,88
6	Kanada	78,18
7	Hollanda	77,23
8	Almanya	76,90
9	Finlandiya	76,48
10	Avustralya	76,45

Kaynak: Oxford Insights, 2024

Ülkeler, yapay zekânın oluşturduğu büyük pazar payı dikkate alındığında bu büyük pastada pay sahibi olmak için yarış halindedir. Ancak bu yarışta, yapay zekânın araştırma, geliştirme ve kullanımı hususlarında yasal bir boşluk olması, mağduriyet yaşanmasına neden olabilmektedir. Yapay zekâ, uzman sistemler olarak bilinen teknolojiler veya tamamen sembolik akıl yürütme kullanan (if-else mantığı) sistemler gibi deterministik olmadığından farklı sonuçlar veya çıkarımlarda bulunmaktadır. Bu çıktılarda hâlihazırda bir yasal bir zemine oturmamaktadır. Dolayısıyla, bu noktada yapay zekâ sistemleri farklı soruları ve sorunları beraberinde getirmektedir. Bu sorular ve sorunların bazıları aşağıdaki şekilde sıralanabilir:

- Yapay zekâ mala/insana zarar verirse kim sorumlu olmalıdır?
- Yapay zekâ değerli bir çıktı oluşturursa bu çıktının sahibi kim olmalıdır?
- Yapay zekâ fikri mülkiyet yasaları veya ifade özgürlüğüne ilişkin hükümler tarafından korunmalı mıdır?
- Yapay zekâ, ticari kararlar alırken hangi parametreleri dikkate almalıdır? Rekabet eden değerler arasında nasıl bir denge kurulabilir?
- Yapay zekânın yasaklanması gereken veya insan müdahalesinin yasaklanması gereken alanlar var mı?

Mevcut sorunlardan yola çıkılarak ülkeler hâlihazırda çeşitli yapay zekâ etik kuralları ve tasarı halindeki yasalar üzerinde çalışmaktadır. Ancak tasarı halinde olan bazı yasaların yapay zekâ üzerindeki etkileri test edilmemiştir ve bu nedenle belirsizliğini korumaktadır. Bu nedenle, hükümetler de dâhil olmak üzere, yapay zekâ kullanmak isteyen kuruluşlar, teknolojinin nasıl yönetilmesi gerektiği konusunda bir dereceye kadar belirsizlik altında çalışmaktadır. Bu belirsizlik, düzenleyici tablo netleşene kadar yatırım yapmayı planlayan işletmeleri de olumsuz etkilemektedir. (Turner, 2018).

1.1 Avrupa Birliği (AB)

Avrupa Birliği (AB), yapay zekâya ilişkin bir takım çalışmalar yürütmektedir. Bir yandan yapay zekânın kullanımını ve gelişimini desteklerken öte yandan karşılaşılabilecek riskleri ve tehlikeleri dikkatle ele almakta olan AB, 2017 yılında konu ile ilgili raporlar yayınlamaya başlamış, 2023 yılında ise "Yapay Zekâ Yasası"nı hazırlamıştır.

Ekim 2017'de Avrupa Konseyi'nde "yüksek düzeyde veri koruma, dijital haklar ve etik standartlar" sağlarken yapay zekânın da popüler olması vurgulanarak Komisyonun "yapay zekâya Avrupa yaklaşımı" oluşturması gerektiği belirtilmiştir (Council, 2017). Bu çerçevede Nisan 2018'de Komisyon tarafından yayınlanan "*Avrupa için Yapay Zekâ* (*Artificial Intelligence for Europe*)" belgesinde AB'nin, yapay zekânın sunduğu fırsatlardan en iyi şekilde yararlanması ve beraberinde getirdiği zorlukları ele almak için koordineli bir yaklaşım oluşturması gerektiği ifade edilmiştir. Ayrıca yapay zekânın geliştirilmesi ve kullanılması için yasal etik çerçevenin oluşturulması gerekliliğinden bahsedilmiştir (Commission, 2018a). Aralık 2018'de ise "*Yapay Zekâ Koordine Planı (Coordinated Plan on Artificial Intelligence)*" hazırlanmış olup, bu plan ile her ülkenin ulusal yapay zekâ stratejileri için genel bir çerçeve oluşturulmuştur. Yapay zekânın mihenk taşı olan "veri" için ortak bir veri alanı oluşturulmasına ve etik konusu da dâhil olmak üzere AB genelinde iş birliğine dikkat çekilmiştir (Commission, 2018b).

Nisan 2019'da "*Güvenilir Yapay Zekâ için Etik İlkeler Kılavuzu* (*Ethics Guidelines for Trustworthy AI*)" yayınlanmıştır. Bu belgede Komisyon, yapay zekânın karşılaması gereken 7 ilkeyi ortaya koymuştur: (1) insan unsuru ve denetim, (2) teknik sağlamlık ve güvenlik, (3) gizlilik ve verilerin korunması, (4) şeffaflık, (5) çeşitlilik, ayrımcılık yapılmaması ve adalet, (6) toplumsal ve çevresel fayda, (7)

hesap verebilirlik. Etik ve güvenilirlik açısından standardizasyonların oluşturulmasının ve yapay zekâ sisteminin şeffaf, hesap verebilir ve adil olduğunu kamuoyuna kanıtlayabilen kuruluşların oluşturulmasının gerekliliği ifade edilmiştir (Commission, 2019).

Şubat 2020'de Avrupa Komisyonu "*Yapay Zekânın Güvenliği ve Sorumluluğuna İlişkin Rapor (Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics)*" yayımlamıştır. Raporda ürünlerin güvenliği, eğitimde kullanılan verilerin kalitesi ve sistem döngüsünde insan gözetiminin gerekli olabileceğinden bahsedilmiştir. (Commission, 2020a). Aynı yıl içinde "*Yapay Zekâ Üzerine- Mükemmellik ve Güvene Dayalı Avrupa Yaklaşımı*" raporu yayınlamıştır. Bahse konu raporda, yapay zekâ düzenlemesinin mevcut düzenlemelerle uyumlu olmasının önemi vurgulanarak halihazırda var olan mevzuatlara tabi olması gerektiği ancak bununla birlikte halihazırdaki mevzuatların yetersiz kalacağı ifade edilmiştir. Sonuç olarak Komisyon, mevcut mevzuatta yapılacak olası değişikliklerin yanı sıra yapay zekâya ilişkin yeni bir mevzuata ihtiyaç olduğu görüşündedir (Commission, 2020b).

1.1.1 Avrupa Birliği Yapay Zeka Yasası

Yapay zekânın hızla gelişmesi ve her sektörde kullanılabilmesi hem ekonomik hem de toplumsal faydalar sağlamaktadır. Fakat bu teknolojinin düzenleme tabi olması da elzemdir. Yapay zekâyı düzenlemek, iyi işleyen bir pazar oluşturmak amacıyla 2021 yılında Avrupa Komisyon tarafından taslak "Yapay Zekâ Yasası" oluşturulmuştur. Nihai olarak Aralık 2023'te AB Yapay Zekâ Yasası üzerinde geçici bir anlaşmaya varılmıştır. Bahse konu yasa, 13 Mart 2024'te Avrupa Parlementosu'nda kabul edilmiş olup (EU, 2024), 21 Mayıs 2024'te ise AB Konseyi tarafından onaylanmıştır (CNBC, 2024).

Yapay zekâ destekli sistemlerin, insanların fikirlerinin farklı olması gibi konular ve öğrenme esnasında girdi verilerine göre farklılık gösteren sistemler olması nedeniyle bu konuda tam ve keskin sınırlar çizmek mümkün olmamaktadır. Nitekim literatür incelendiğinde konu ile ilgili uzmanların ve kuruluşların yaptıkları tanımlamalar farklılık göstermektedir. Söz konusu teknoloji ile ilgili net bir sınırın oluşturulamamasından dolayı Avrupa Birliği Yapay Zekâ Yasası'nın risk temelli bir yaklaşım benimsediği görülmektedir. Yasadaki en önemli nokta, yapay zekanın tanımının yapılmasıdır (Yamak, 2024) Söz konusu yasada, OECD'nin

güncellemiş olduğu yapay zekâ tanımını kabul ederek Yasa'da tanıma aşağıdaki şekilde yer vermektedir:(AB YZY, Madde 3(1))

"Yapay zekâ sistemi, değişen seviyelerde özerklikle çalışmak üzere tasarlanmış ve açık veya örtülü hedefler için fiziksel veya sanal ortamları etkileyen tahminler, öneriler veya kararlar gibi çıktılar üretebilen makine tabanlı bir sistem anlamına gelir."

Risk temelli yaklaşımı benimseyen yasa, bütün yapay zekâ sistemlerinin uyması gereken ilkeleri şu şekilde tanımlamıştır:

- İnsan aracılığı ve gözetimi
- Teknik sağlamlık ve güvenlik
- Gizlilik ve veri yönetişimi,
- Şeffaflık,
- Çeşitlilik, ayrımcılık yapmama ve adalet
- Sosyal ve çevresel refah

Buna ek olarak Yasa'da, Yasa uygulanırken sağlayıcı, uygulayıcı ve bu sistemlerden etkilenen kişilerin ihtiyaçları dikkate alınarak yeterli düzeyde yapay zekâ okuryazarlığının teşvik edilmesi gerekliliği belirten yapay zekâ okuryazarlığına ilişkin bir madde bulunmaktadır (AB YZY, Madde 4b).

Yasada en önemli hususlardan biri kullanımı kesinlikle yasaklanan uygulamaların açıkça belirtilmiş olmasıdır. Böylece kişilerin bilinçli karar verme yeteneğini bozacak şekilde manipülatif veya aldatıcı teknikler kullanarak bir kişi veya gruba zarar verilmesine neden olabilecek uygulamaların, bir kişinin veya grubun zayıf yönlerini istismar ederek o kişi veya gruba zarar verebilecek uygulamaların, gerçek kişilerin veya grupların sosyal davranışları ile kişisel özelliklerine dayanarak belirli bir süre boyunca sosyal puanlama veya sınıflandırma yapan sistemlerin ve kamuya açık alanlarda gerçek zamanlı uzaktan biyometrik tanımlama sistemlerinin kullanılması yasaklanmıştır (AB YZY, Madde 5(1))

Yasa kapsamında yapay zekâ sistemleri dört kategoride ele alınmıştır: Kabul Edilemez Riskli, Yüksek Riskli, Genel Amaçlı ve Minimum Risk İçeren veya Hiç Risk İçermeyen Yapay Zekâ Sistemleri. Kabul Edilemez Riskli Yapay Zekâ Sistemlerinin hâlihazırda yasa kapsamında detayları paylaşılmış olup, kullanımları

yasaklanmıştır. Yüksek Riskli Yapay Zekâ Sistemlerinin ise belirli kurallara tabii olması gerekmektedir. Kısaca Yüksek Riskli Yapay Zekâ Sistemlerinin uyması gereken kurallar yedi başlık altında toplanmıştır: Risk Yönetim Sistemi, Veri ve Veri Yönetimi, Teknik Dokümantasyon, Kayıtların Tutulması, Şeffaflık ve Kullanıcılara bilgi Sağlama, İnsan Gözetimi, Doğruluk Sağlamlık ve Siber Güvenlik. Genel Amaçlı Yapay Zekâ Sistemlerinin ise şeffaflık yükümlülüklerin uyduğu takdirde kullanımına izin verilmektedir. Son olarak Minimum Risk İçeren veya Hiç Risk İçermeyen Yapay Zekâ Sistemleri tüm yapay zekâ sistemlerinin uyması gereken kurallara uymalı ve bu itibarla da bir kısıtlama uygulanmamaktadır.

Bahse konu yasada, ihlallere ilişkin cezalar da belirlenmiştir. Yasaklanmış Yapay Zekâ Sistemlerine ilişkin ihlaller söz konusu olduğunda 40 milyon avroya veya bir önceki yılın küresel yıllık cirosunun%7'sine kadar idari para cezası uygulanabilecektir. Diğer gereklilik veya yükümlülüklere uyulmaması halinde 10 milyon avroya veya bir önceki yılın küresel yıllık cirosunun %2'sine kadar idari para cezası verilebilecektir. Bir talebe cevaben kuruluşlara ve ulusal yetkili makamlara yanlış, eksik veya yanıltıcı bilgiler verilmesi durumda ise 5 milyon avroya veya bir önceki yılın küresel yıllık cirosunun %1'ine kadar idari para cezası verilebilecektir.

Yapay Zekâ Yasasının altıncı kısmının birinci bölümünde Yapay Zekâ Kurulu tanımlanmıştır. Kurulun merkezi Brüksel'de olup yönetim kurulu, bir sekreterya ve danışma forumundan oluşmaktadır. Yönetim kurulunda ise her bir üye devletin denetim makamından bir temsilci, AB Komisyon'undan bir temsilci, Avrupa Veri Koruma Denetçisinden bir temsilci ve Avrupa Birliği Siber Güvenlik Kurumu'ndan (ENISA) temsilci ve Temel Haklar Kurumu'ndan bir temsilci bulunmaktadır. Yapay Zekâ Kurulu görevlerini yerine getirirken ve yetki kullanımında bağımsız hareket edebilir ancak bu yasa uyarınca Avrupa Parlamentosu ve Konsey'e karşı sorumludur. Yapay Zekâ Kurulu'nun görevleri ayrıca belirlenmiştir (AB YZY, *Madde 56, 57, 58*).

1.2 Amerika Birleşik Devletleri

Teknoloji üreten ülkelerin başında gelen ABD'nin yapay zekâ düzenlemeleri kılavuzlar, çerçeveler ve kararlar, Federal Ticaret Komisyonu ve Ulusal Standartlar ve Teknoloji Enstitüsü dâhil olmak üzere birçok yetkili tarafından yayınlanmıştır. Ülkede düzenlemeler hem eyalet düzeyinde hem de federal olarak yayınlanmaktadır. Federal düzeyinde yapılan düzenlemeler:

1. **Algoritmik Sorumluluk Yasası:** 2019 yılında çıkarılan Algoritmik Sorumluluk Yasası, (Algorithmic Accountability Act) ticari kuruluşlarca yüksek riskli sistemlere ilişkin değerlendirmeler yapılmasını belirtmektedir (Congress, 2019a). Söz konusu yasa, 2022 yılında güncellenmiş olmasına rağmen henüz yürürlüğe girmemiştir. Yapılan güncelleme ile otomatik karar sistemlerini kullanan işletmelerin, tüketiciler üzerindeki etkisini incelemesi ve raporlaması gerekmektedir.

2022 Algoritmik Sorumluluk Yasası (ASY), artırılmış kritik karar süreci ile otomatik karar sistemi üzerine düzenleme yapan bir yasadır. Burada artırılmış kritik karar süreci, kritik bir karar vermek için otomatikleştirilmiş bir karar sistemi kullanan bir süreç, prosedür veya faaliyeti ifade ederken, otomatik karar sistemi ise (makine öğrenimi, istatistik veya diğer veri işleme veya yapay zekâ tekniklerinden elde edilenler dahil) herhangi bir sistem, yazılım veya süreç olarak tanımlanarak süreç sonucunda bir yargıya varılan sistem olarak tanımlanmıştır.

2022 Algoritmik Sorumluluk Yasası, şirketlerin kullandıkları ve tüketiciye sattıkları otomatik sistemlerin etkilerinin değerlendirilmesini zorunlu kılmaktadır. Bu etki değerlendirmeleri belgeleri 3 yıl boyunca saklanmak zorundadır. Etki değerlendirmesini gerçekleştirirken mümkün olduğunca çalışanlar, etik ekipleri ve sorumlu teknoloji ekipleri gibi ilgili iç paydaşlara ve etkilenen grup temsilcileri, sivil toplum kuruluşları ve teknoloji uzmanları gibi dış paydaşlara danışmaları gerekmektedir. Bu istişareler de Algoritmik Sorumluluk Yasası'nda detaylıca belirtildiği bilgileri kapsayacak şekilde belgelenmelidir (Congress, 2022).

Söz konusu yasanın 4. Bölümünde, "Kapsam Dâhilindeki Kuruluş Etki Değerlendirmesinin Gereklilikleri" başlığı altında dikkat edilmesi gereken hususlar belirtilmiştir. Bu kapsamda kuruluşların yapması gerekli olan birçok husus tanımlanmıştır. İlk olarak, ilgili ulusal standartlar ve teknoloji enstitüsü veya diğer Federal Hükümet, otomatik karar sisteminin veya artırılmış kritik karar sürecinin gizlilik riskleri ve gizliliği artırıcı önlemleri hakkında sürekli test ve değerlendirme yapmalıdır. Söz konusu sistem veya sürecin veri minimizasyon uygulamalarının ve ilgili tanımlayıcı bilgilerin ve bunun sonucunda ortaya çıkan kritik kararların saklanma süresi değerlendirilerek belgelenmesi gerekmektedir. Ayrıca yürürlükte olan bilgi güvenliği önlemleri de göz önüne alınarak bu tür bir sistem veya sürecin kullanıcıların emniyeti, mahremiyeti veya güvenliği ve kimlik bilgileri üzerindeki olumlu ve olumsuz etkilerinin değerlendirilerek belgelenmesi

gerekmektedir. Kuruluş, otomatik karar sisteminin veya artırılmış kritik karar sürecinin mevcut ve geçmiş performansını sürekli test etmeli ve değerlendirilmesini yapmalıdır. Bu değerlendirme yapılırken Algoritmik Sorumluluk Yasası'nın 4'üncü bölümünde 4'üncü maddede belirtilen şu hususlara dikkat edilmesi gerekmektedir: (Congress, 2022).

"a) Başarılı performans olarak kabul edilenlerin ve işletme tarafından performansı değerlendirmek için kullanılan yöntemlerin, teknik ve ticari ölçütlerin açıklanması,

b) Söz konusu sistemin veya sürecin kullanım koşulları ve test koşulları altında performansının gözden geçirilmesi veya performansın uygulanan koşullar altında neden gözden geçirilmediğinin açıklanması,

c) Sistem veya sürecin, kullanım koşulları altında performansının test koşullarıyla karşılaştırılması veya böyle bir karşılaştırmanın neden mümkün olmadığının açıklanması,

d) Kullanıcıların ırk, renk, cinsiyet, yaş, engellilik durumu, din, aile durumu, sosyo ekonomik durumu vb. özellikleri ile ilişkili her türlü farklı performansın değerlendirilmesi ve söz konusu değerlendirmeye yönelik metodolojinin açıklanması ile verilerdeki bu tür özellikleri tanımlamak için kullanılan yöntemlere ilişkin bilgilerin belgelenmesi,

…

f) Test ve değerlendirme için herhangi bir alt popülasyon kullanılmışsa, hangi alt popülasyonların kullanıldığına ve bu tür alt popülasyonların test ve değerlendirme ile ilgili olduğunun nasıl ve neden belirlendiğine ilişkin açıklanması."

Kuruluşların etki değerlendirmesinde, otomatik karar sistemini veya artırılmış kritik karar sürecini geliştirmek, test etmek, sürdürmek veya güncellemek için kullanılan her türlü veri veya diğer girdi bilgilerine ilişkin belgeler güncel tutulmalıdır. Kullanılan verilerin veya diğer girdi bilgilerinin neden tercih edildiği ve bu verilerin yanı sıra hangi alternatiflerin araştırıldığının belgelenmesi gereken bir hususdur. Ayrıca kullanılan verilerin veya her türlü girdinin nasıl ve ne zaman elde edildiği önemli bir husus olup verilere ilişkin yasada açıklanan verileri belgelenmelidir. (Congress, 2022).

Kuruluşların etki değerlendirmesindeki gerekliliklerinden biri de tüketici

haklarıdır. Kuruluşların tüketicilere söz konusu sistem veya sürecin nasıl kullanılacağına dair açıklama yapması ve devre dışına bırakılmasındaki işlemlerin belirtilmesi gerekmektedir. Aynı zamanda bu tür bir sistemin veya sürecin şeffaflığını ve açıklanabilirliği ile tüketicinin bir karara itiraz etme, düzeltme, bu tür bir sistem veya süreçten çıkma durumu da belirtilmesi gereken hususlardır. Otomatik karar sisteminin veya artırılmış kritik karar sürecinin tüketiciler üzerindeki muhtemel maddi olumsuz etkileri belirlenerek bu konuda aşağıda belirtilen stratejiler oluşturulmalıdır: (Congress, 2022).

- Sistem veya sürecin tüketiciler üzerindeki olası önemli olumsuz etkilerinin belirlenmesi ve ölçülmesi ile bu etkiyi belirlemek ve ölçmek için atılan adımların belgelenmesi,
- Belirlenen olası maddi olumsuz etkileri ortadan kaldırmak veya azaltmak için atılan adımların belgelenmesi,
- Tüketiciler üzerindeki olası maddi olumsuz etkileri tanımlamak, ölçmek, hafifletmek veya ortadan kaldırmak için kullanılan standart protokollerin veya uygulamaların ve ilgili ekiplerin veya personelin bu tür protokoller veya uygulamalar hakkında nasıl bilgilendirildiğinin ve eğitildiğinin belgelenmesi.

Otomatik karar sistemi veya artırılmış kritik karar süreciyle ilgili olarak geliştirme ve dağıtım sürecine ilişkin herhangi bir testin, dağıtımın, lisansın veya diğer önemli aşamaların tarihi ve katkı sunan ekip, iş birimi veya iç paydaşın iletişim bilgileri de kapsam dâhilindeki kuruluşun etki değerlendirmesi hususunda belgelemesi gereken konulardır. Ayrıca etki değerlendirmesini iyileştirmek için gerekli veya faydalı olabilecek tüm araçlar, standartlar, veri kümelerin, güvenlik protokollerin, paydaş katılımı iyileştirmeler de belgelenmelidir. Etki değerlendirmesi gerekliliklerinin herhangi birine uyulmaması halinde kuruluşlar bunun gerekçesini de belgelemekle sorumludur (Congress, 2022).

2. **Yapay Zekâ Hakları Bildirgesi:** 2022 yılında 117. Kongre'nin yapay zekâ odaklı gerçekleştirilmesi ile ABD, yapay zekâyı düzenleyecek somut yasalar ve yapay zekâyı daha güvenli hale getirme konusundaki kararlılığını göstermiştir. Bu doğrultuda, Beyaz Saray Bilim ve Teknoloji Politikası Ofisi, Yapay Zekâ Hakları Bildirgesi Planı'nı yayımlamıştır. Söz konusu planda otomatik sistemlerin tasarımına ve kullanımına rehberlik etmesi gereken beş ilke belirlenmiştir: Güvenli ve Etkili Sistemler, Algoritmik Ayrımcılıktan Koruma, Veri

Gizliliği, Bildirim ve Açıklama, İnsan Alternatifleri, Değerlendirme ve Geri Dönüş. Bu ilkelerin uygulanmasına yönelik tavsiyelere de planda yer verilmiştir. (Whitehouse, 2022).

3. **NIST Risk Yönetimi Çerçevesi:** Yapay Zekâ Risk Yönetimi Çerçevesinin (Artificial Intelligence Risk Management Framework- AI RMF) amacı, yapay zekânın risklerini yönetme, yapay zekâ sistemlerinin güvenilir ve sorumlu bir şekilde geliştirilmesini ve kullanımını sağlamak için bu sistemleri tasarlayan, geliştiren, dağıtan veya kullanan kuruluşlara bir kaynak sunmaktır. Söz konusu belgeye göre oluşan zararlara yönelik de risk yönetimi yapılmasının gerekliliği vurgulanmıştır. Bu tür sistemler, kendi kendini geliştiren bir yapı olmasından dolayı başta yapılan risk değerlendirmelerinin sistemin yaşamı boyunca aynı kalmaması muhtemeldir. Böylece yapay zekâ sistemleri risk ve güvenirliği için belirli bir ölçüm mevcudiyetinin olmaması da bu konuda bir zorluk oluşturmaktadır. Bunun yanı sıra, geliştirilen yapay zekâ sistemleri laboratuvar ortamlarında kontrollü şekilde test edilip belli sonuçlar elde edilmektedir. Fakat bu sistemlerin gerçek dünyada kullanılması esnasında farklı sonuçlar oluşturması ihtimaline de dikkat edilmesi elzemdir (NIST, 2023).

4. **Ticari Yüz Tanıma Gizlilik Kanunu:** Ticari Yüz Tanıma Gizlilik Kanun Tasarısı, 2019 yılında senatoya sunulmuş olmasına rağmen henüz yürürlüğe girmemiştir. Kanun; kuruluşların, son kullanıcının onayı olmadan son kullanıcıyı tanımlamak veya takip etmek için ve başka amaçlarla yüz tanıma teknolojisini kullanmasını engellemek amacıyla düzenleme getirmektedir. Kanuna göre işletmeler kullanıcıdan onay alırken verilerin hangi uygulamalarda kullanıldığı, son kullanıcıların verilerinin toplanması, saklanması ve kullanımına ilişkin kişinin anlayabileceği şekilde açıklayıcı bildirim yapmak zorundadır.

   Verileri işleyen kuruluş veya işletme, son kullanıcıya fiziksel veya mali zarar verilmesine yol açabilecek, son kullanıcı için beklenmedik veya rahatsız edici bir durumun oluşabileceği durumlarda nihai kararı belirlemeden önce gerçek bir kişinin kontrolünden geçmesi zorunludur. Ayrıca bir yüz tanıma teknolojisini çevrimiçi hizmet olarak kullanıma sunan kuruluşun, yüz tanıma teknolojisinin doğruluk ve önyargı açısından testlerini bağımsız bir kuruluşa yaptırması gerekmektedir (Congress, 2019b).

5. **Yapay Zekânın Güvenli, Emniyetli ve Güvenilir Geliştirilmesi ve Kullanımına İlişkin Kararname:** Ekim 2023'te Başkan Biden, yapay zekânın risklerini yönetmek üzere bir Kararname yayımlamıştır. Kararnamede yapay zekânın güvenliği için yeni standartların oluşturulması gerektiği belirtilmiştir. Kararnameye göre yapay zekâ sistem geliştiricilerinin, güvenlik testi sonuçları ile kritik bilgileri ABD hükümeti ile paylaşması gerekmektedir. Ulusal güvenliğe, ulusal ekonomik güvenliğe veya ulusal kamu sağlığı ve güvenliğine ciddi risk teşkil eden herhangi bir model geliştiren şirketler, modeli eğitirken federal hükümete bildirimde bulunmak ve tüm güvenlik sonuçlarını paylaşmak zorundadır. Bu önlemler ile şirketlerin yapay zekâ sistemlerinin emniyeti ve güvenilirliğinin sağlanması hedeflenmektedir. Ayrıca bu hedef doğrultusunda standartlar, araçlar ve testler geliştirileceği belirtilmiş olup, Ulusal Standartlar ve Teknoloji Enstitüsü (NIST), sistemlerin kullanıma sunulmasından önce güvenliği sağlamak amacıyla kapsamlı testlere yönelik katı standartlar oluşturacaktır. Kararnamede belirtildiği üzere, İç Güvenlik Bakanlığı (The Department of Homeland Security) bu standartları kritik altyapı sektörlerine uygulayacaktır. Ayrıca Yapay Zekâ Emniyet ve Güvenlik Kurulu da kurulacaktır. Enerji ve Ulusal Güvenlik Bakanlıkları yapay zekâ sistemlerinin kritik altyapıya yönelik tehditlerinin yanı sıra kimyasal, biyolojik, radyolojik, nükleer ve siber güvenlik risklerini de ele alacaktır. Halkı, yapay zekâ destekli sahtekârlıklara karşı korumak için yapay zekâ tarafından oluşturulan içeriği tespit etmek ve resmi içeriğin kimliğini doğrulamak için standartlar oluşturulacaktır. Ticaret Bakanlığı, yapay zekâ tarafından oluşturulan içeriği açıkça etiketlemek amacıyla içerik kimlik doğrulaması için kılavuz geliştirecektir. Bunun yanı sıra, kritik yazılımlardaki güvenlik açıklarını bulup düzeltmek amacıyla yapay zekâ araçları geliştirmek için gelişmiş bir siber güvenlik programı oluşturulacağı da kararnamede belirtilmiştir (Whitehouse, 2023).

ABD'de eyaletler kendi hukuk sistemlerine göre yapay zekâ ile ilgili düzenleme yapmış olup konu ile ilgili çalışmalarına devam etmektedir. Kaliforniya'da "Çevrimiçi Şeffaflığı Destekleme Yasası" ve İllinois eyaletinde ise "Yapay Zekâ Video Mülakat Yasası" 2020 yılında yürürlüğe girmiş olan yasalardır. Çevrimiçi Şeffaflığı Destekleme Yasası Kaliforniya'da Ağustos 2020'de yürürlüğe girmiş olup, botların[2] internet ortamında ticari veya politik amaçlar doğrultusunda bi-

[2] Bot, gerçek bir sosyal medya hesabı gibi davranan ama bir algoritma tarafından yürütülen sosyal medya hesapları olarak tanımlanmaktadır.

reylerle iletişime geçerek onları yanıltmasını yasaklamaktadır. Yasa, yalnızca bot iletişimleri kapsamakta olup servis sağlayıcısı ve çevrimiçi platformlar açısından bir yükümlülük getirmemektedir. Bot kimliği, açıkça ve makul bir şekilde açıklarsa yasaya aykırı bir durum oluşmamaktadır. Yasaya aykırı davranışların cezası ise ihlal başına 2.500 ABD doları olarak belirlenmiştir (Bacaksız ve Sümer, 2021). Yapay Zekâ Mülakat Yasası ise İllinois eyaleti tarafından Ocak 2020'de yürürlüğe girmiştir ve iş mülakatlarında video röportajlarını analiz etmek için yapay zekâ kullanan işletmecilere yükümlülükler getirmektedir. Bu kapsamda, yapay zekânın video röportajını analiz etmesinde kullanılacağı hakkında görüşmeden önce kişinin bilgilendirilmesi gerekmektedir. Aynı zamanda kişinin, yapay zekânın nasıl çalıştığına ilişkin bilgilendirilmesi ve mülakat öncesinde de rızasının alınması gerekmektedir. Yasa kapsamında mülakat videolarının ancak değerlendirme ile yetkili kişilerle paylaşılabileceği ve bu videoların 30 gün içerisinde silinmesinin gerektiği belirtilmiştir (Bacaksız ve Sümer, 2021). Bazı eyaletlerde ise yapay zekâ sektörel olarak düzenleyen yasalar bulunmaktadır. Tablo 2.3'te 2023 yasama döneminde çıkarılan yasalar ve açıklamalarına yer verilmiştir (Zhu, 2023).

Tablo 2.2 2023 Yılında yürürlüğe giren eyalet yasaları

EYALET	YASA	GEÇTİĞİ TARİH	YÜRÜRLÜK TARİHİ	AÇIKLAMA
Arizona	Oy İşleme ve Elektronik Karar Verme Sınırı (Ballot Processing and Electronic Adjudication Limit)	10 Nisan 2023	Veto	Bu yasa, oy pusulası işlemede yapay zekâ kullanımını engellemektedir.
Georgia	House Bill 203	2 Mayıs 2023	1 Temmuz 2023	Bu yasa, otomatik sistemler aracığıyla göz muayenesini düzenlemektedir. Otomatik sistemler aracığıyla yapılan göz değerlendirmeleri gerçek zamanlı yapılan göz muayenelerinin yerini almaması gerekmektedir.

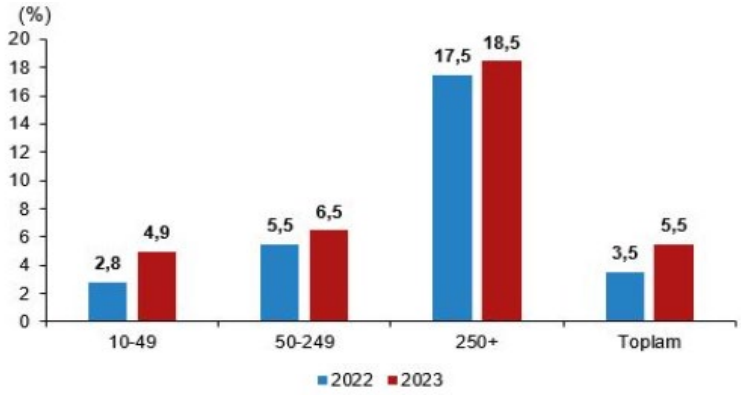
Hawaii	SR123/SCR179	Nisan 2023	Nisan 2023	Bu karar yapay zekânın istenmeyen sonuçlarına karşı uyarıda bulunmakla birlikte Kongre'yi yapay zekânın yararlarını ve risklerini tartışmaya çağırmıştır.

1.3 Türkiye

Son yıllarda büyük bir ivme ile gelişim gösteren yapay zekâ teknolojisi, hayatımızın birçok alanında yerini almıştır. Sağladığı olumlu gelişmelerin yanı sıra ortaya çıkabilecek olumsuzluklara karşı diğer ülkeler gibi ülkemizde de çalışmalar yürütülmekte olup, hem teknik hem de hukuki boyutlarda ele alınmaktadır.

Türkiye, teknolojiyi sadece kullanan değil, aynı zamanda üreten olmak ve teknoloji yarışında üst sıralarda yerini almak için büyük bir çaba göstermektedir. 2023 Dijital Türkiye Raporuna göre nüfusun %95,4'ü hücresel mobil bağlantısına sahipken, %83,4'ü de internet kullanıcısıdır. Ayrıca nüfusun %73,1'i de aktif sosyal medya kullanıcısıdır (Digital, 2023). Rakamlara bakıldığında ülkemiz teknolojiyi aktif olarak kullanmaktadır. Buna ek olarak TÜİK verilerine göre, ülkemizde yapılan girişim faaliyetlerinde girişimlerin %96'sı internet erişimine sahiptir. Yapay zekâyı kullanan girişimlerin çalışan sayılarına göre oranları Şekil 3.1'de gösterilmiştir. Yapay zekâ teknolojilerinden herhangi birini kullandığını belirten girişimlerin oranı, 2022 yılında %3,5 iken 2023 yılında ise %5,5 olmuştur. Çalışan sayısı büyüklük grubuna göre yapay zekâ kullanan girişimlerin oranı incelendiğinde; 10-49 çalışanı olan girişimlerin %4,9'unun, 50-249 çalışanı olan girişimlerin %6,5'inin ve 250 ve üzeri çalışanı olan girişimlerin %18,5'inin yapay zekâ kullandığı görülmüştür. Yapay zekâ kullanan girişimlerden görüntülere göre nesneleri veya kişileri tanımlayan girişimler %48,4 ile ilk sırada yer alırken, %43,7 ile farklı iş akışlarını otomatikleştiren veya karar vermeye yardımcı olan yapay zekâ teknolojilerini kullanan teknolojiler ve %41,5 ile yazılı veya sözlü dil üreten yapay zekâ teknolojilerini kullanan girişimler takip etmiştir (TÜİK, 2023).

Şekil 3.1 Çalışan sayısı büyüklük grubuna göre yapay zekâ kullanan girişimlerin oranı



Kaynak: TÜİK, 2023.

Üniversite/kamu araştırma merkez ve enstitülerinde üretilen teknolojinin ve bilgi birikiminin, "TÜBİTAK BİLGEM Yapay Zekâ Enstitüsü "nün koordinasyonuyla ihtiyaçları karşılayan yenilikçi ürün ve çözümlere dönüştürülmesi, proje çıktılarının ilgili sahalarda uygulanması ve elde edilmiş olan ürün ve çözümlerin yapay zekâ ekosistemine aktarılması amacıyla finans teknolojileri, akıllı üretim sistemleri, akıllı tarım, gıda ve hayvancılık teknolojileri, iklim değişikliği ve sürdürülebilirlik ile akıllı eğitim teknolojileri olmak üzere beş alan belirlenmiş olup "TÜBİTAK 1711 - Yapay Zekâ Ekosistem 2023 Çağrısı" yapılmıştır (TÜBİTAK, 2023). Bu çağrı kapsamında bahse konu beş alana ilişkin 32 başvuru yapılmış olup bunlardan 17'si destek almıştır (TRTHaber, 2024)

Bu girişimler ve girişim çağrıları ülkemizde bu alanın gelişmesi için çaba sarf edildiğinin ispatıdır. Fakat yapılan girişimlerde yapay zekâ teknolojisinin tercih edilmediği de görülmüş olup girişimlerinde yapay zekâ teknolojilerinden herhangi birini kullanmayanların nedenleri Tablo 3.1'de gösterilmiştir. Tablo incelendiğinde en önemli nedenin %60,7 ile maliyetlerin çok yüksek olması olduğu görülmüştür. Bunu, ilgili uzmanlık eksiğinin bulunması ve mevcut ekipman, yazılım veya sistemlerle uyumsuzluğun olması takip etmiştir. Ayrıca %36,3'ü hukuki sonuçların net olmamasından dolayı yapay zekâ teknolojilerini kullanmadığını belirtmiştir. %35,9'u ise veri koruma ve gizliliğin ihlaline ilişkin endişelerinin olması nedeniyle yapay zekâ kullanımını tercih etmezken, %31,3'ü de etik faktörlerden dolayı tercih etmemektedir (TÜİK, 2023).

Tablo 3.3 Girişimlerin yapay zekâ kullanmama nedenleri

YAPAY ZEKÂ TEKNOLOJİSİ KULLANMAMA NEDENİ	ORAN(%)
Maliyetlerin çok yüksek olması	60,7
Girişimde ilgili uzmanlık eksikliğinin bulunması	58,3
Mevcut ekipman, yazılım veya sistemlerle uyumsuzluğun olması	49,6
Gerekli verilerin mevcudiyeti veya kalitesiyle ilgili zorlukların bulunması	40,1
Yapay zekâ teknolojilerinin girişime yararlı olmaması	36,5
Hukuki sonuçların net olmaması	36,3
Veri koruma ve gizliliğine ilişkin endişelerin olması	35,9
Etik faktörler	31,3

Kaynak: (TÜİK, 2023).

Yapay Zekâ Politikaları (AIPA) Derneği tarafından yayınlanan "*Gelecek Araştırması: Toplumda Yapay Zekâ Algısı*" raporu, yapay zekânın kitleler üzerindeki algısını araştırmak ve analiz etmek amacıyla toplamda 1135 kişi ile görüşülerek hazırlanmıştır. Raporun "Yapay Zekânın Kanunlara ve Değerlere Hesap Vermesi Durumu" başlığı altında katılımcılara "Yapay zekânın kanunlar önünde hesap verebilir olması gerektiğine ne derece katılıyorsunuz?" ve "Yapay zekânın toplumsal değerler önünde hesap verebilir olması gerektiğine ne derece katılıyorsunuz?" soruları sorulmuştur. Katılımcıların %35,4'ü yapay zekânın kanunlar önünde hesap vermesi gerektiğine katılırken, %37,1'i yapay zekânın toplumsal değerler önünde hesap vermesi gerektiğine katılmaktadır (Küçükşabanoğlu vd., 2021)

Hukuki sonuçların net olmaması, veri gizliliği ve etik konularından dolayı girişimlerde yapay zekânın tercih edilmeme yüzdelerinin yüksek olduğu görülmektedir. Başka bir ifadeyle bu konular yapay zekâ teknolojilerinin gelişiminde engel teşkil etmekle birlikte, toplumda da yapay zekânın kanun ve toplumsal de-

ğerlere göre hesap vermesi gerektiği kabul görmektedir.

Bunun yanı sıra Oxford Insight'a ait 2024 yılında yayınlanan "Hükümetin Yapay Zekâ Hazırlık Endeksi" raporunda ülkemiz, 60,63 puanla dünyada 53. sırada yer alırken Güney ve Orta Asya'da 2. sırada yer almaktadır. En az puan 42,32 ile teknoloji sektöründen alınmıştır. Veri ve altyapı bakımından 66,02 puan alırken, hükümet alanından 70,73 puan alınmıştır (Oxford, 2024).

Ülkemizde gelişen teknolojiler, kamu sektöründeki reform eğilimleri ile toplumsal talepler doğrultusunda farklı kurumlar altında ayrı olarak yürütülen dijital dönüşüm, büyük veri ve yapay zekâ, siber güvenlik, milli teknolojileri ile ilgili çalışmaların tek elden yürütülmesi amacıyla 10 Temmuz 2018 tarih ve 30474 sayılı, 1 Sayılı Cumhurbaşkanlığı Kararnamesi'nin Resmî Gazete'de yayınlanarak yürürlüğe girmesiyle T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi kurulmuştur (CBDDO, 2023). 48 Sayılı Cumhurbaşkanlığı Kararnamesi ile CBDDO bünyesinde diğer başkanlıklar ile "Büyük Veri ve Yapay Zekâ Uygulamaları Dairesi Başkanlığı" kurulmuş olup görevleri tanımlanmıştır (CB Kararnamesi, 2019).

Cumhurbaşkanlığı'nın yanı sıra Bakanlıklar düzeyinde de yapay zekâ ile ilgili birimler oluşturulmuştur:

- Adalet Bakanlığı bünyesinde Bilgi İşlem Genel Müdürlüğü altında, "Büyük Veri ve Yapay Zekâ Uygulamaları Şube Müdürlüğü",
- Sağlık Bakanlığı bünyesinde Sağlık Bilgi Sistemleri Genel Müdürlüğü, Ulusal Projeler Yönetim Koordinatörlüğü altında "Yapay Zekâ ve Giyilebilir Teknolojiler Birimi",
- Millî Savunma Bakanlığı bünyesinde Muhabere ve Bilgi Sistem Dairesi Başkanlığı altında, "Süreç Yönetimi ve Yapay Zekâ Uygulamaları Şube Müdürlüğü" (CBDDO, 2021).

Ülkemizin yapay zekâ politikalarının geliştirilmesine ve uygulanmasına yönelik doğrudan veya dolaylı olarak strateji belgeleri bulunmakta olup bu belgelere ilişkin hususlar şu şekildedir:

- **2023 Sanayi ve Teknoloji Stratejisi:** Teknoloji geliştirme süreçlerinde AR-GE'nin üretim ve operasyonlarla olan ilişkisi, yazılım ve yapay zekâ teknolojisi geliştirme ortamları göz önüne alınarak, yerinde AR-GE'yi destekleyen teşvik

yapısının, fabrika alanları, üniversite laboratuvarları, ofisler ve atölyelerde yapılan çalışmaları içerecek şekilde yeniden düzenlenmesi hedeflenmektedir. Bu doğrultuda "henüz hazır olmayan ve sıfırdan yatırımın zaman gerektirdiği yapay zekâ ve makine öğrenmesi, robotik, nesnelerin interneti gibi yıkıcı teknolojilere hızlı giriş için uluslararası şirketler ile iş birliği yapılacağı, gerektiğinde şirket veya teknoloji satın alma fırsatlarının değerlendirileceği ve buna uygun desteklerin oluşturulacağı" belirtilmiştir (STB, 2019).

- **2020-2023 Akıllı Şehirler Stratejisi ve Eylem Planı:** "Hayata Değer Katan Yaşanabilir ve Sürdürülebilir Şehirler" vizyonu doğrultusunda veriye dayalı olarak "şehirlerdeki problemlerin ve ihtiyaçların öngörülerek çözümler üretilmesi, şehircilik hizmetlerinin daha kaliteli ve hızlı bir şekilde sunumu ve böylece hizmetlerden memnuniyetin ve nihai hedef olarak yaşam kalitesinin artırılması" amaçlanmıştır (ÇŞB, 2019)
- **2020-2023 Ulusal Akıllı Ulaşım Sistemleri (AUS) Stratejisi Belgesi ve Eylem Planı:** "AUS bileşenlerini içeren IoT ağının kurulması, bu bileşenlerden toplanan verilerin büyük veri ortamında saklanması ve analize uygun hâle getirilerek yapay zekâ, derin öğrenme, haberleşme ve benzeri alanlardaki yenilikçi teknolojiler kullanılarak ulaşım altyapısının optimize edilmesi" hedeflenmiştir (UAB, 2019).

1.3.1 Ulusal Yapay Zekâ Stratejisi

2019-2023 yıllarını kapsayan 11. Kalkınma Planı'nda yapay zekâ teknolojilerinin üretilmesi ve kullanımının yaygınlaştırılması ile bu teknolojinin yol haritasının oluşturulması belirtilmiştir. Söz konusu bu plan ile Cumhurbaşkanlığı yıllık programları kapsamında, 2021 yılında Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Başkanlığı (CBDDO) ile Sanayi ve Teknoloji Bakanlığı (STB) tarafından hazırlanarak ülkemizin 2021-2025 Ulusal Yapay Zekâ Stratejisi (UYZS) yayımlanmıştır. Yayımlanan belgede yapay zekâ, *"En genel haliyle, bir bilgisayarın veya bilgisayar kontrolündeki bir robotun çeşitli faaliyetleri zeki canlılara benzer şekilde yerine getirme kabiliyeti olarak tanımlanmaktadır. Yapay zekâ terimi; dinamik ve belirsiz ortamlarda akıl yürütme, anlam keşfetme, genelleme veya geçmiş deneyimlerden öğrenme gibi insanlara özgü bilişsel kabiliyetlerle donatılmış sistemler için kullanılmaktadır."* şeklinde tanımlanmıştır. Ayrıca yayımlanan strateji belgesinde 6 stratejik öncelik belirlenmiştir:

1. Yapay zekâ uzmanlarını yetiştirmek ve alanda istihdamı artırmak
2. Araştırma, girişimcilik ve yenilikçiliği desteklemek
3. Kaliteli veriye ve teknik altyapıya erişim imkânlarını genişletmek
4. Sosyoekonomik uyumu hızlandıracak düzenlemeleri yapmak
5. Uluslararası düzeyde iş birliklerini güçlendirmek
6. Yapısal ve iş gücü dönüşümünü hızlandırmak

UYZS çerçevesinde tedbir ve eylem planının uygulanması için bir yönetişim mekanizması planlanmıştır. Bu mekanizmanın bir tarafı stratejik, diğer tarafı ise idari ve teknik düzeyde çalışmalar gerçekleştirmektedir. Stratejik kısımda üst seviye koordinasyon ve karar verme mekanizmaları yer alırken; idari ve teknik kısımda ise UYZS uyarınca hayata geçirilecek çalışmaların etkin bir şekilde kurgulanıp yürütülmesine yönelik teknik ve idari mekanizmalar oluşturulacağı belirtilmiştir (CBDDO, 2021).

Cumhurbaşkanlığının 2021/18 sayılı ve Ulusal Yapay Zekâ Stratejisi (2021-2025) konulu genelge, 20 Ağustos 2021 tarihli Resmî Gazete 'de yayımlanmıştır. Söz konusu genelge ile yapay zekâ teknolojilerinin üretimi ve kullanımının yaygınlaştırılması ilişkin belirlenen ulusal politikalar çerçevesinde yapılacak çalışmaların yürütülmesi, strateji belgesinde belirtilen tedbirlerin uygulanması ve koordinasyonun sağlanması amacıyla Cumhurbaşkanı Yardımcısı Cevdet YILMAZ'ın başkanlığında CBDDO ile Sanayi ve Teknoloji Bakanlığının ilgili bakan yardımcısı katılımı ile "Ulusal Yapay Zekâ Stratejisi Yönlendirme Kurulu" kurulmuştur. Yönlendirme Kurulu'nun, üç ayda bir kez veya davet üzerine toplanmasına karar verilmiştir (CB, 2021).

Yapay zekânın düzenlenmesine ilişkin CBDDO tarafından UYZS belgesi doğrultusunda çalışma grupları oluşturulmuş olup ilgili çalışmalar yürütülmektedir. Bu doğrultuda hâlihazırda yapay zekâ hukuku ve eğitimine ilişkin bir çalışma grubu da oluşturulmuştur. Ancak ülkemizde şu an için direkt olarak yapay zekâya yönelik yasal bir düzenleme bulunmamaktadır.

1.3.2 Türk Standartları Enstitüsü Yapay Zekâ Ayna Komitesi

Çeşitli alanlarda standardizasyon ve uygunluk değerlendirmesi yapmakla görevli olan Türk Standartları Enstitüsü (TSE) yapay zekâ alanındaki çalışmalarda

da görev almaktadır. Başta Avrupa olmak üzere uluslararası teknik komitelerin yapay zekâ alanındaki çalışmaları takip etmek ve katkı sağlamak amacıyla da TSE bünyesinde Yapay Zekâ Ayna Komitesi kurulmuştur. Aylık olarak toplanan Komite, toplantılarda o ay içinde görüş bildirilmesi talep edilen Avrupa ve uluslararası standart taslaklarına ilişkin incelemeler ve değerlendirmeler yapmakta, ülke görüşüne karar vermektedir. Komite tarafından ülkemizde bu sektörle ilgili temaslar, güncel takip için gereken çalışmalar koordine edilmekte ve ilgili Avrupa ve uluslararası komitelerce duyurusu yapılan standart tasarısı oylamaları gibi noktalarda ülkemiz görüşleri TSE üzerinden bildirilmektedir (AA, 2023).

1.3.3 Türkiye Sağlık Veri Araştırmaları ve Yapay Zekâ Uygulamaları Enstitüsü Yapılanması ve Faaliyetlerinin Yürütülmesine Dair Yönetmelik

Ülkemizde yapay zekâ alanında "Türkiye Sağlık Veri Araştırmaları ve Yapay Zekâ Uygulamaları Enstitüsü Yapılanması ve Faaliyetlerinin Yürütülmesine Dair Yönetmelik", 12.03.2022 tarihli ve 31776 sayılı Resmî Gazete'de yayınlamıştır. Söz konusu yönetmelik, Türkiye Sağlık Veri Araştırmaları ve Yapay Zekâ Uygulamaları Enstitüsünün (TÜYZE) kuruluşu, görevleri, yetki ve çalışma usul ve esaslarını belirlemektedir. TÜYZE, Enstitü Başkanlığı, bilim kurulları ve Yönetim Kurulu kararı ile kurulacak diğer birimlerden oluşmaktadır. Şu an Enstitü bünyesinde "Sağlık Veri Organizasyonu Bilim Kurulu" ile "Yapay Zekâ Bilim Kurulu" bulunmaktadır.

Söz konusu Yönetmeliğin 4'üncü maddesinde yer alan;

"a) Türkiye'de sağlık verisi araştırmaları ve sağlık alanında yapay zekânın kullanımı konusunda ülkemizin rekabet gücünü artırmak ve sağlık hizmetlerinin etkinliğinin artırılmasına yönelik bilimsel ve teknolojik ihtiyacı karşılamak üzere yenilikçi ve öncü araştırmalar yapmak ve bu tür araştırmaları desteklemek.

b) Kliniklerde toplanan laboratuvar tetkikleri veya X-Ray, MR ve BT gibi radyolojik görüntüler ve patolojik görüntüler ile hekimler için hastalık özelinde karar destek sistemlerinin geliştirilmesi için araştırmalar yapmak ve kamu kurumları, yükseköğretim kurumları, Ar-Ge merkezleri gibi kurumlarda bu tür araştırmaların yapılmasını desteklemek.

c) Toplanan klinik veriler ve radyolojik görüntüler ile bunların güvenilir değerlendirilmesine yönelik hazırlanan referans bilgileri saklamak ve etkin bir şekilde

yönetmek için altyapı oluşturmak, araştırmacılara anonimleştirilmiş verilerin bütününe veya bir kısmına düzenlenen protokoller ile erişim yolları sunmak.

ç) Geliştirilen karar destek sistemlerinin sahada kullanılabilir ürünlere dönüşmesine yönelik gömülü sistem ve ağ uygulamalarını teşvik etmek ve bunların taşınabilir veya çevrimiçi kullanımı ile medikal görüntüleme cihazlarına entegrasyonu için kamu kurumları, yükseköğretim kurumları, teknoloji transfer ofisleri, Ar-Ge merkezleri ve özel sektör iş birliklerine aracı olmak.

d) Sağlık veri araştırmaları ve yapay zekâ uygulamaları alanında kamu kurum ve kuruluşları, özel hukuk tüzel kişileri ve gerçek kişiler tarafından gerçekleştirilecek Ar-Ge faaliyetlerine mali ya da bilimsel destek sağlamak, bunları koordine etmek ve izlemek.

e) Sağlık veri araştırmaları ve yapay zekâ uygulamaları alanındaki gelişme, buluş ve yeniliklerin sağlık hizmetlerinde kullanımına ve yaygınlaştırılmasına yönelik Ar-Ge yapmak ve/veya yaptırmak, bu maksatla Ar-Ge merkezleri ve ihtiyaç duyulan diğer birimlerin kurulması veya kurdurulması tekliflerini Yönetim Kurulunda karar oluşturulması için Başkana sunmak.

f) Sağlık veri araştırmaları ve yapay zekâ uygulamaları alanında yurt içi ve yurt dışı iş birlikleri gerçekleştirmek ve ülkemizin dijital sağlık ekosisteminin oluşturulması için gerekli araştırma, geliştirme, eğitim, organizasyon ve koordinasyon çalışmalarını yürütmek."

hükümleri uyarınca Enstitünün görevleri tanımlanmıştır (Mevzuat, 2023).

1.3.4 Yapay Zekâ Alanında Kişisel Verilerin Korunmasına Dair Tavsiyeler Raporu

Yapay zekâ alanında faaliyet gösteren üreticiler, geliştiriciler, servis sağlayıcıları ve karar alıcılar için Kişisel Verileri Koruma Kurumu (KVKK) tarafından 6698 sayılı Kişisel Verilerin Korunması Kanunu kapsamında kişisel verileri korumaya yönelik tavsiyeler içeren bir rapor yayınlanmıştır. Bahse konu raporda, genel olarak yapay zekâ uygulamalarının geliştirilmesi ve uygulanması süreçlerinde kişilerin temel hak ve özgürlüklerine saygı gösterilmesi ve hak ihlallerine meydan verilmemesi tavsiye edilmiştir. Kişisel verilerin işlenmesine yönelik uygulamalarda ilk andan itibaren KVKK'ya uyumlu şekilde geliştirilmesi gerekmektedir. Bununla birlikte hukuka uygunluk, dürüstlük, hesap verebilirlik, ölçülülük, şeffaflık,

kişisel verilerin doğru ve güncel olması, kişisel veri kullanım amacının belirli ve sınırlı olması ilkeleri ile veri güvenliği dikkat edilmesi gerektiği belirtilmiştir.

Diğer taraftan uygulamada aynı sonuçlar kişisel veriler işlenmeden de elde edilebiliyorsa verilerin anonimleştirilerek kullanılması tavsiye edilmiştir. Kişisel verilerin işlendiği yapay zekâ uygulamalarında özel nitelikli kişisel veri kullanılıyorsa özel veri koruma kuralları olduğu göz önüne alınarak teknik ve idari tedbirler daha sıkı bir şekilde uygulanması gerekmektedir. Ayrıca kişisel veri kullanılan yapay zekâ çalışmalarının farklı paydaşlar açısından veri sorumlusu veya veri işleyen olma statüleri, projenin başında belirlenerek aralarındaki hukuki ilişki veri koruma mevzuatı ile uyumlu hale getirilmesi tavsiye edilmiştir. Eğer kişisel verilerin korunması bakımından yüksek riskli bir durum söz konusu ise mahremiyet etki değerlendirmesi yapılması ve veri işleme faaliyetinin hukuka uygunluğuna bu çerçevede karar verilmesi tavsiye edilmiştir (KVKK, 2023).

Geliştiriciler, üreticiler ve servis sağlayıcıları için verilen tavsiyelerde insan hakları, veri mahremiyeti vb. konulara dikkat etmesinin yanı sıra kullanılan kişisel verilerin niteliği, kalitesi, miktarı, kaynağı ve içeriği değerlendirilerek minimum veri kullanımına gidilmesi ve geliştirilen modelin doğruluğunun sürekli izlenmesi belirtilmiştir. Kişilere, görüş ve kişisel gelişimlerini etkileyen teknolojilere dayalı işlemelerle ilgili itiraz hakkı tanınması gerektiği ifade edilmiştir. Ulusal ve uluslararası hukuka uygunluğun yanında risk değerlendirilmesi de teşvik edilmelidir. Ayrıca kişilerden veri onayı alınması gerektiği ve veri işleme faaliyetini durdurabilme hakkı tanınması, kullanıcılara ait verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi imkânı tasarlanması gerekliliği de ifade edilmiştir.

Uygulamayı kullanan kişilerin, kişisel veri işleme faaliyetinin gerekçeleri, kişisel verilerin işlenmesinde kullanılan yöntemlerin detayları ile muhtemel sonuçları hakkında aydınlatılması veri işleme onay mekanizması oluşturulması önerilmiştir. Karar alıcılar için yapılan tavsiyelerde ilk olarak hesap verilebilirlik ilkesine uygunluğa dikkat edilmesi gerektiği belirtilerek, karar alma süreçlerinde insan müdahalesinin rolünün belirlenmesi ve yapay zekânın önerdiği sonuçlara güvenmeme özgürlüğünün olması gerektiği ifade edilmiştir. Yapay zekâdan elde edilen sonuçların kişilerin temel hak ve özgürlüklerini büyük ölçüde etkilediği takdirde, yapay zekâyı denetleyen otoritelere başvurulması önerilmiştir (KVKK, 2023).

1.3.5 On İkinci Kalkınma Planı

1 Kasım 2023 tarihinde Resmî Gazete'de On İkinci Kalkınma Planı (2024-2028) yayınlanmıştır. Söz konusu planda, yapay zekâ teknolojilerinin ulusal ve uluslararası düzeyde düzenlenmesinin gerekli olduğu belirtilmiştir. Kişisel veri güvenliği ve mahremiyeti, siber güvenlik, yapay zekâ ve dijital etik gibi konularda yenilikçi ve kapsamlı kamu politikaları ile yasal düzenlemelerin yapılması ihtiyacı olduğu ifade edilmiştir. Kamu sektörünün veri sağlayıcısı olarak öncü olduğundan bahisle kamu verisi paylaşımının hayata geçirilerek yapay zekâ alanında yerli ve milli çözümlerin üretilmesi gerektiği belirtilmiştir. Plan kapsamında yapay zekâ teknolojilerinin gelişmesinin destekleneceği belirtilerek kamu, özel sektör ve üniversite iş birliklerinin güçlendirilmesi ve yapay zekâ alanında uluslararası iş birliklerinin artırılması hedeflenmektedir. Buna ek olarak, yapay zekâ teknolojilerinden ortaya çıkan ihtiyaçlara yönelik gerekli hukuki düzenlemelerin yapılması da planlanmaktadır (On İkinci Kalkınma Planı, 2023).

1.3.6 Yapay Zekâya İlişkin Yönetmelikler

Yapay zekâya ilişkin ülkemizde Yönetmelik çalışmaları da yapılmaktadır. Bankacılık sektöründe Bankacılık Düzenleme ve Denetleme Kurumu (BDDK) tarafından hazırlanarak 01.04.2021 tarihli ve 31441 sayılı Resmî Gazete'de yayımlanan "*Bankalarca Kullanılacak Uzaktan Kimlik Tespiti Yöntemlerine ve Elektronik Ortamda Sözleşme İlişkisinin Kurulmasına İlişkin Yönetmelik*" ve 11.02.2022 tarihli ve 31716 sayıl Resmî Gazete'de yayımlanan "*Finansal Kiralama, Faktoring, 220 Finansman ve Tasarruf Finansman Şirketlerince Kullanılacak Uzaktan Kimlik Tespiti Yöntemlerine ve Elektronik Ortamda Sözleşme İlişkisinin Kurulmasına İlişkin Yönetmelik*" ile ihtiyaç halinde elektronik ortamda müşterilerin kimliğinin yapay zekâ ile uzaktan tespit edilmesine ilişkin hususların BDDK tarafından belirlenebileceği belirtilmiştir.

Hazine ve Maliye Bakanlığı tarafından hazırlanan 30.04.2021 tarihli ve 31470 sayılı Resmî Gazete 'de yayımlanan "*Mali Suçları Araştırma Kurulu Genel Tebliği (Sıra No:19)*"nde bir müşterinin kimliğinin uzaktan tespiti noktasında yapay zekâ kullanılabileceği ifade edilmiştir.

Bilgi Teknolojileri ve İletişim Kurumu tarafından hazırlanarak 26.06.2021 tarihli ve 31523 sayılı Resmî Gazete 'de yayımlanarak 01.03.2022 tarihinde yürür-

lüğe giren "*Elektronik Haberleşme Sektöründe Başvuru Sahibinin Kimliğinin Doğrulanma Süreci Hakkında Yönetmelik*"te elektronik haberleşme, elektronik imza ve kayıtlı elektronik posta sektörlerinde abonelik sözleşmeleri, nitelikli elektronik sertifika başvurusu, kayıtlı elektronik posta başvurusu gibi işlemler için oluşturulan belgelerin elektronik ortamda gerçekleştirilmesi halinde başvuru sahibinin kimliğinin ispatlanabilir irade beyanı ile doğrulanabilmesi için uygulanabilecek usul ve esaslar arasında yapay zekâ kullanımına ilişkin hususlara da yer verilmiştir.

SONUÇ

Yapay zekâ hayatımızın gündelik işlerine dâhil olan, bireyler tarafından kullanımı sıklıkla tercih edilen bir teknoloji haline gelmiştir. Bireyler, herhangi bir konu hakkında yazmak istedikleri yazıdan, herhangi bir konuya ilişkin oluşturmak istedikleri görsele kadar pek çok konuda yapay zekâ uygulamalarından fikir almaktadır. Bu durum, ilerleyen süreçlerde yapay zekânın hayatımızın vazgeçilmez bir parçası olacağını göstermektedir. Adından sıkça söz edilen yapay zekânın sağlamış olduğu verimlilik artışı, insan hatalı kaynakların azaltılması 7/24 kullanılabilirlik gibi avantajların yanında; yüksek maliyet, etik ve ahlaki değerlerdeki belirsizlik kaynaklı problemler gibi bazı dezavantajları ve veri manipülasyonları gibi güvenlik problemlerini de beraberinde getirmektedir.

Yapay zekâ ile gelişen bir sistemin eğitilmesinde kullanılan veriden, ilgili sistemin farklı amaçlar için kullanımına kadar birçok alanda kişilerin güvenliğini tehdit eden unsurlar günümüz yapay zekâsının geldiği noktada olduğu gibi ileride de olması muhtemeldir. Bu kapsamda, ulusal ve uluslararası düzeyde yapay zekâ ile ilgili düzenleme çalışmaları yürütülmeye başlanmıştır.

AB ve ABD yapay zekânın düzenlenmesine ilişkin hususları iki farklı bakış açısı ile değerlendirmektedir. AB'nin yürütmüş olduğu çalışmalar incelendiğinde, yüksek risk temelli yapay zekâ sistemleri için şeffaflık ve güvenlik gibi yükümlülükler ortaya koyan ve ihlal durumunda önemli yaptırımlar getiren bütüncül bir yaklaşım benimsediği görülmektedir. ABD'nin yapmış olduğu çalışmalara bakıldığında ise bir ikilem olduğu gözlemlenmektedir. "Algoritmik Sorumluluk Yasası" yürürlüğe girmediği sürece ABD'nin yapay zekânın sektörel olarak düzenlenmesini savunduğu görülmektedir. Bir diğer ifade ile "Algoritmik Sorumluluk Yasası" bütüncül bir düzenleme getirdiğinden, yasanın yürürlüğe girmesi

ABD'nin belirtilen bu iki grup arasındaki yerini netleştireceği düşünülmektedir. Ayrıca her iki yaklaşım grubunda da yüksek riskli yapay zekâ sistemleri için paydaşlara gerekli bilgilerin sağlanması, etki değerlendirmelerinin yapılması ve kayıtların tutulmasının tavsiye edildiği veya zorunlu kılındığı görülmüştür.

Öte yandan hem AB'nin hem de ABD'nin yapay zekâ hususunda etik ilkeler üzerinde hemfikir olduğunu söylemek mümkündür. Ek olarak, risk temelli yaklaşımda daha çok yüksek riskli yapay zekâ sistemleri üzerinde durulduğu görülmektedir.

Bununla birlikte, risk temelli bir yaklaşımla oluşturulan AB'nin "Yapay Zekâ Yasası"nda tüm yapay zekâ sistemlerinin uyması gereken ilkelerin belirtilmesi mağduriyet yaşanmasının önüne geçilmesinde önemli bir adım olarak değerlendirilmektedir. ABD'nin "Algoritmik Sorumluluk Yasası" hâlihazırda yürürlükte olmadığından ABD'nin halen sektörel düzeyde bir düzenleme ilkesinde ilerlediği değerlendirilmektedir.

ABD "Algoritmik Sorumluluk Yasası" hâlihazırda yürürlükte olmadığından ABD'nin halen sektörel düzeyde bir düzenleme ilkesinde ilerlediği değerlendirilmektedir. Yapay zekâya ilişkin hâlihazırda bulunan iki önemli yasa olan AB'nin "Yapay Zekâ Yasası" ile ABD'nin "Algoritmik Sorumluluk Yasası"na bakıldığında; yapay zekâya bakış açıları olarak benzerlikler görülmektedir. Özellikle söz konusu teknolojide kullanılan veriler bakımından her iki yasanın da getirmiş olduğu yasal sorumlulukların yapay zekâ açısından son derece önemli ve doğru bir yaklaşım olduğu değerlendirilmektedir. Fakat her iki yasa karşılaştırıldığında "Algoritmik Sorumluluk Yasası"nın sadece yapay zekâ özelinde olmayıp daha geniş bir kapsama sahip olduğu açıktır. "Yapay Zekâ Yasası"nın ise yapay zekâ sistemleri özelinde hazırlandığı, bu teknolojinin sınırlarını belirleyen ve teknik bilgilerin dokümantasyonu bakımından da daha detaylı düzenlemeleri içeren bir yasa olduğu değerlendirilmektedir.

Alanında ilk ilk olması hasebiyle AB Yapay Zekâ Yasası bu alanda bir mihenk taşı olmuştur. Riskler temel alınarak oluşturulan söz konusu yasa, AB ülkelerinin kendi düzenlemelerine entegrasyonunda önem arz etmektedir. Ülkemizde yapay zekâ konusuna önem vermektedir. Dolayısıyla yapay zekâ düzenlemelerine öncülük eden AB'nin "Yapay Zekâ Yasası" esas alınarak risk temelli bir yaklaşımla bütüncül bir yasa oluşturulmasının ülkemiz açısından yerinde olacağı değerlendirilmektedir. Ulusal ölçekte uygulanacak olan bir yasa ile hem mevzuatsal

çakışmalarının önüne geçilerek yeknesak bir uygulamanın temin edileceği hem de yapay zekâ teknolojisinin gelişimi sağlanırken ortaya çıkabilecek olumsuzluklara da kolaylıkla müdahale edilebileceği değerlendirilmektedir. Bununla birlikte yapay zekânın önemli bir parçası olan "veri" de dikkate alındığında, risk temelli bütüncül bir yasanın hem kişisel veriler hem de ülkemiz verilerinin korunması açısından daha etkili olacağı düşünülmektedir. Ayrıca hazırlanacak olan risk temelli bir yasanın ardından ülkemizde yapay zekâ teknolojilerinin kullanımını içeren mevzuatların birbirleri ile uyumlu ve kendi gerekliliklerini içeren şekilde hazırlanabileceği değerlendirilmektedir.

Yapay zekâ teknolojileri, gelişen ve değişebilen bir yapıya sahiptir. Kendi kendine öğrenebilen sistemlerin de varlığı göz önüne alındığında bu sistemlerin belirli aralıklarla kontrol edilmesi ve denetlenmesi büyük öneme haizdir. Böyle bir denetimin gerçekleştirilmesi halinde veri güvenliğinin rahatlıkla sağlanabileceği ve böylelikle kişi mağduriyetlerinin de engellenebileceği düşünülmektedir. Bu bağlamda yapay zekâ teknolojilerinin yeknesak bir kuruluş tarafından düzenlenmesi ve denetlenmesi mevzuatsal karışıklıkların önüne geçebileceği değerlendirilmektedir. Nitekim AB'nin "Yapay Zekâ Yasası"na bakıldığında, Yasa'nın ulusal düzeyde ülkelerin bir denetim kurumunun olmasını zorunlu kıldığı görülmektedir. Bu bağlamda ülkemizde de yapay zekânın düzenlenmesi ve denetlenmesine ilişkin bir kurum veya başkanlığın oluşturulmasının gerekli olduğu değerlendirilmektedir.

Bununla birlikte, yapay zekânın önemli bir ayağını verinin oluşturduğu ve kullanılan verilerin, elde edilen sonuçlar üzerindeki etkisi aşikârdır. Bu kapsamda "*Türkiye Sağlık Veri Araştırmaları ve Yapay Zekâ Uygulamaları Enstitüsü Yapılanması ve Faaliyetlerinin Yürütülmesine Dair Yönetmelik*"in 4'üncü maddesinin birinci fıkrasının (c) bendinde yer alan; "*Toplanan klinik veriler ve radyolojik görüntüler ile bunların güvenilir değerlendirilmesine yönelik hazırlanan referans bilgileri saklamak ve etkin bir şekilde yönetmek için altyapı oluşturmak, araştırmacılara anonimleştirilmiş verilerin bütününe veya bir kısmına düzenlenen protokoller ile erişim yolları sunmak*." şeklindeki ifadeler ile; sağlık verilerinin ne şekilde kullanılacağı ve bunlara erişimin ne şekilde olacağına yönelik bir düzenleme yapıldığı görülmektedir. Yapay zekâ uygulamalarının birçok alanda kullanıldığı dikkate alındığında kamu kurum ve kuruluşları gibi ilgili paydaşlarla iş birliği içerisinde anonimleştirilmiş açık veri portalının oluşturulmasının yerinde olabileceği düşünülmektedir. Oluşturulacak bahse konu platformda, kamuya açılımında

herhangi bir sakınca bulunmayan verilerin paylaşılabileceği ve ülkemizde yapılacak olan yapay zekâ çalışmalarına katkı sağlanması amacıyla bu verilerin kullanılabileceği düşünülmektedir. Bununla birlikte, oluşturulacak portaldaki verilerin kullanım şartlarının belirlenmesi, portalda yer alan verilerin kimler tarafından, ne amaçla kullandığına dair bilgilerin kayıtlarının tutulması da son derece önemli bir husus olacaktır.

Yapay zekâ teknolojisinin bir yazılım olması ve kendini geliştirme özelliği kapsamında veri kullanımı göz önüne alındığında, bu teknolojinin hem siber güvenliği sağlama da kullanılabileceği hem de siber saldırılara mazur kalabileceği açıktır. Dolayısıyla, yapay zekânın siber güvenliğin sağlanmasında kullanılması ve yapay zekâlı bir sistemin karşılaşabileceği siber saldırılara güvenlik tedbirlerinin alınmış olması amacıyla ilgili kurum ve kuruluşların iş birliği içerisinde söz konusu teknolojinin siber güvenliğinin sağlanması yönünde daha aktif rol alınmasının yerinde olacağı değerlendirilmektedir.

KAYNAKLAR

AA, 2023, Türkiye, Yapay Zekada AB Standartlarına Uyumu "Ayna Komite" Çalışmalarıyla Sağlıyor, https://www.aa.com.tr/tr/bilim-teknoloji/turkiye-yapay-zekada-ab-standartlarina-uyumu-ayna-komite-calismalariyla-sagliyor/3050470 , (19.12.2023)

AB YZY, 2024, Avrupa Birliği Yapay Zekâ Yasası, https://afyonluoglu.org/eu-ai-act-00/ , (10.12.2024)

BACAKSIZ Pınar ve SÜMER Seda Yağmur, 2021, Robotlar, Yapay Zeka ve Ceza Hukuku, Adalet Yayınevi.

CB, 2021, Cumhurbaşkanlığı 2021/18 Genelgesi

CBDDO, 2021, Ulusal Yapay Zeka Stratejisi, https://cbddo.gov.tr/SharedFolderServer/Genel/File/TR-UlusalYZStratejisi2021-2025.pdf , (14.10.2023)

CBDDO, 2023, Dijital Dönüşüm Ofisi, https://cbddo.gov.tr/hakkimizda/ , (05.12.2023)

CB Kararnamesi, 2019, Cumhurbaşkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesinde Değişiklik Yapılmasına Dair Cumhurbaşkanlığı Kararnamesi, No 48.

CNBC, 2024, World's first major law for artificial intelligence gets final EU green light, https://www.cnbc.com/2024/05/21/worlds-first-major-law-for-artificial-intelligence-gets-final-eu-green-light.html , (11.11.2024).

COMMISSION European, 2018a, Artificial Intelligence For Europe, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A237%3AFIN, (21.02.2023)

COMMISSION European, 2018b, Coordinated Plan on Artificial Intelligence, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018DC0795, (21.02.2023)

COMMISSION European, 2019, Ethics Guidelines For Trustworthy AI, https://www.europarl.europa.eu/cmsdata/196377/AI%20HLEG_Ethics%20Guidelines%20for%20Trustworthy%20AI.pdf (27.03.2023)

COMMISSION European, 2020a, Report On The Safety And Liability İmplications Of Artificial Intelligence, The Internet Of Things And Robotics, https://eur-lex.europa.eu/legal-content/en/TXT/?qid=1593079180383&uri=CELEX%3A52020DC0064 , (27.03.2023)

COMMISSION European, 2020b, White Paper On Artificial Intelligence - A European Approach To Excellence And Trust, https://commission.europa.eu/system/files/2020-02/commission-white-paper-artificial-intelligence-feb2020_en.pdf , (30.03.2023)

CONGRESS, 2019a, Algorithmic Accountability Act of 2019, https://www.congress.gov/bill/116th-congress/house-bill/2231 , (17.09.2023)

CONGRESS, 2019b, Commercial Facial Recognition Privacy Act of 2019, https://www.congress.gov/bill/116th-congress/senate-bill/847/text , (11. 10. 2023)

CONGRESS, 2022, Algorithmic Accountability Act of 2022, https://www.congress.gov/bill/117th-congress/senate-bill/3572/text , (24.09.2023)

COUNCIL European, 2017, European Council Meeting – Conclusions, https://data.consilium.europa.eu/doc/document/ST-14-2017-INIT/en/pdf, (17.02.2023)

ÇŞB, 2019, 2020-2023 Ulusal Akıllı Şehirler Stratejisi Ve Eylem Planı, https://www.akillisehirler.gov.tr/wp-content/uploads/EylemPlani.pdf , (09.01.2024)

DIGITAL, 2023, Dijital Türkiye Raporu, https://www.guvenliweb.org.tr/dosya/HQTLP.pdf , (03.11.2023).

DUARTE Fabio, 2024, Number of ChatGPT Users, https://explodingtopics.com/blog/chatgpt-users, (22.12.2024)

EU, 2024, Artificial Intelligence Act: MEPs adopt landmark law, https://www.europarl.europa.eu/news/en/press-room/20240308IPR19015/artificial-intelligence-act-meps-adopt-landmark-law , (25.11.2024).

KÜÇÜKŞABANOĞLU Zafer, KILIÇ Volkan ve ÖZDEMİR Şebnem, 2021, AIPA Gelecek Araştırması: Toplumda Yapay Zeka Algısı Kantitatif Araştırma Raporu, Yapay Zeka Politikaları Derneği (AIPA).

KVKK, 2023, Yapay Zekâ Alanında Kişisel Verilerin Korunmasına Dair Tavsiyeler, https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/25a1162f-0e61-4a43-98d0-3e7d057ac31a.pdf , (20.11.2023)

MCCARTHY John, 2007, From here to human-level AI, Artificial Intelligence, Cilt 171, Sayı 18, s.1174-1182.

MCKINSEY, 2023, McKinsey Technology Trends Outlook 2023, https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-top-trends-in-tech#/ , (10.09.2023)

Mevzuat, 2023, Türkiye Sağlık Veri Araştırmaları Ve Yapay Zekâ Uygulamaları Enstitüsünün Yapılanması Ve Faaliyetlerinin Yürütülmesine Dair Yönetmelik

NIST, 2023, Artificial Intelligence Risk Management Framework, https://nvlpubs.nist.gov/nistpubs/ai/nist.ai.100-1.pdf , (25. 10. 2023)

On İkinci Kalkınma Planı, 2023, https://www.resmigazete.gov.tr/eskiler/2023/11/20231101M1-1-1.pdf , (17.11.2023)

OXFORD Insights, 2024, Government AI Readiness Index 2024, https://oxfordinsights.com/wp-content/uploads/2024/12/2024-Government-AI-Readiness-Index-2.pdf , (22.12.2024)

STATISTA, 2023, Artificial ıntelligence Market Size Worldwide ın 2021 With A Forecast Until 2030, https://www.statista.com/statistics/1365145/artificial-intelligence-market-size/ , (03.09.2023)

STB, 2019, Sanayi ve Teknoloji Stratejisi 2023, https://www.sanayi.gov.tr/assets/pdf/SanayiStratejiBelgesi2023.pdf (08.01.2024)

TDK, 2024, Türk Dil Kurumu Sözlükleri, https://sozluk.gov.tr/ ,(25.02.2024).

TRAI, 2023, Yapay Zekâ Zaman Çizelgesi, https://turkiye.ai/kaynaklar/yapay-zeka-zaman-cizelgesi/ (26.03.2023)

TRTHaber, 2024, Tübitak 17 Yapay Zeka Projesini Destekleyecek, https://www.trthaber.com/haber/ekonomi/tubitak-17-yapay-zeka-projesini-desteleyecek-826612.html , (07.01.2024)

TURNER Jacob, 2018, Robot Rules: Regulating Artificial Intelligence, Springer.

TÜBİTAK, 2023, Yapay Zekâ Ekosistem 2023 Çağrısı ve TÜBİTAK BİLGEM Yapay Zekâ Enstitüsü, https://bilgem.tubitak.gov.tr/wp-content/uploads/sites/8/YZ_Ekosistem-Cagrisi-2023-Bilgilendirme-YZE-Sunusu.pdf , (02.11.2023)

TÜİK, 2023, Girişimlerde Bilişim Teknolojileri Kullanım Araştırması, https://data.tuik.gov.tr/Bulten/Index?p=Girisimlerde-Bilisim-Teknolojileri-Kullanim-Arastirmasi-2023-49393 , (03.11.2023)

UAB, 2019, Akıllı Ulaşım Sistemleri Strateji Belgesi ve 2020-2023 Eylem Planı, https://www.uab.gov.tr/uploads/announcements/ulusal-akilli-ulasim-sistemleri-strateji-belgesi-v/ulusal-akilli-ulas-im-sistemleri-strateji-belgesi-ve-2020-2023-eylem-plani.pdf , (11.01.2024)

WHITE HOUSE, 2022, Blueprint for an AI Bill of Rights, https://www.whitehouse.gov/ostp/ai-bill-of-rights/ , (18.09.2023)

WHITE HOUSE, 2023, President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence, https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/ , (05.11. 2023)

YAMAK Yasemin, 2024, Yapay Zeka İle İlgili Güncel Düzenleme Çalışmaları: Avrupa Birliği ve Uluslararası Çerçevede İnceleme ve Türkiye İçin Öneriler, Bilgi Teknolojileri ve İletişim Kurumu, Yayınlanmamış Uzmanlık Tezi.

ZHU Katrina, 2023, The State of State AI Laws: 2023, https://epic.org/the-state-of-state-ai-laws-2023/ , (09.11.2023)

Bilgi Teknolojileri ve İletişim Dergisi (BTK DERGİ)
CİLT 3 SAYI 1 OCAK-HAZİRAN 2025 ISSN:2980-1331 E-ISSN: 3023-4239

BİR KAMU MALI OLAN FREKANSLARIN TABİ OLDUĞU HUKUKSAL REJİMİN DEĞERLENDİRİLMESİ

AYCAN ILGIN[1]

Gönderilme Tarihi: 15 Haziran 2025

Kabul Tarihi: 10 Temmuz 2025

Review Article / İnceleme Makalesi

ÖZET

İletişimin ana kaynaklarından biri olan frekansın tabi olduğu hukuksal rejim, ülkemizdeki haberleşmenin tabi olduğu hukuksal çerçeveyi doğru anlamak bakımından özel bir anlam taşımaktadır. Nitekim, en yaygın haberleşme araçlarından olan mobil ve kablosuz iletişim teknolojileri ve gelecekte bizleri bekleyen uydu teknolojileri ile entegre olmuş mobil iletişim teknolojileri frekansların tabi olduğu hukuksal rejim etrafında şekillenecektir. 5809 sayılı Elektronik Haberleşme Kanunu'nun ve Avrupa Birliği mevzuatının sıklıkla bu kaynağın kıt olduğunu vurgulaması da bu kaynağın nispeten günümüzde ama çok büyük bir olasılıkla yakın gelecekte hem sosyal hem ekonomik açıdan çok daha değerli olacağının ilk sinyallerini vermektedir. Bu makale ile, frekansların esas olarak düzenlendiği ve frekansların hukuksal rejimine ilişkin veriler sunan 5809 sayılı Elektronik Haberleşme Kanunu'nun ilgili hükümlerinin, yargı kararları ve doktrin görüşleri doğrultusunda incelenmesi amaçlanmaktadır. Bu inceleme yapılırken ihtiyaç oldukça 5809 sayılı Kanun'un uyum sağlama amacı taşıdığı Avrupa Birliği'nin elektronik haberleşme hizmetlerine ilişkin düzenleyici çerçevesine de değinilmektedir. Frekansların hukuksal rejimi belirlenirken bunların birer kamu malı niteliğinde olduğu gözetilerek, bunlara ilişkin yapılacak düzenlemelerde kamu mallarına özgü kabul edilen belli başlı hukuksal ilkelerin dikkate alınması, tüm kamunun menfaatinin sağlanması bakımından elzem görünmektedir. Yeni gelişen teknolojiler ile birlikte frekansların kullanımlarında da yeni modellerin gündeme gelebilmesi mümkündür. Gerek frekansların işletmeciler ve diğer paydaşlar arasında paylaştırılmasında gerekse işletmecilerin kullanımına tahsis edilmesi ve bunlar arasında el değiştirmesinde başta milli güvenlik olmak üzere, kamu düzeni ve rekabetin korunması ilkelerinin öncelikle gözetilmesi gerekmektedir. 5809 sayılı Kanun'un da frekansların kamu malı niteliğini dikkate almak suretiyle bir düzenleyici çerçeve sunduğunu ve gelecekteki teknolojik gelişmelere bağlı farklı modeller içerebilecek frekans kullanımlarına olanak sağladığı görülmektedir.

Anahtar kelimeler: *Frekans, Kamu Malı, Mobil Elektronik Haberleşme, Devlet, Hukuk*

[1] Bilişim Uzmanı, aycan.ilgin@btk.gov.tr, ORCID: 0000-0002-1624-5665

Bilgi Teknolojileri ve İletişim Dergisi (BTK DERGİ)
CİLT 3 SAYI 1 OCAK-HAZİRAN 2025 ISSN:2980-1331 E-ISSN: 3023-4239

AN EVALUATION OF THE LEGAL REGIME GOVERNING FREQUENCIES AS A PUBLIC RESOURCE

ABSTRACT

The legal regime governing frequency, one of the essential resources of communication, carries special importance for understanding the legal framework that regulates telecommunications in Turkey. Mobile and wireless communication technologies—among the most common means of communication—as well as future mobile technologies integrated with satellite systems, will evolve around the legal regime applied to frequencies. The fact that Law No. 5809 on Electronic Communications and EU legislation frequently emphasize the scarcity of this resource signals its increasing value both socially and economically, especially in the near future. This article aims to analyze the relevant provisions of Law No. 5809, which primarily regulates frequencies and provides insights into their legal regime, in light of judicial decisions and academic opinions. Where necessary, reference is also made to the EU's regulatory framework, which Law No. 5809 seeks to align with. Given that frequencies are considered public property, it is essential that legal principles specific to public goods are taken into account when regulating their use, to ensure the protection of public interest. With advancing technologies, new models of frequency usage may emerge. In the allocation, assignment, and transfer of frequencies among operators and stakeholders, priority must be given to national security, public order, and the protection of competition. Law No. 5809 provides a regulatory framework that considers the public nature of frequencies and accommodates flexible models for future technological developments.

Keywords: *Frequency, Public Good, Mobile Electronic Communications, State, Law*

GİRİŞ

Frekanslar, günlük yaşantımızın ayrılmaz bir parçası olan sesli ve görüntülü iletişimin ana unsurlarından biri olmakla birlikte, maddi bir varlıkları bulunmadığından, onların hukuken ekonomik değer taşıyan mal niteliğinde olduklarını kabul etmek ancak gelişen teknoloji ile birlikte gerçekleşmiştir. Nitekim, frekansların taşıdıkları bilgi ve enerji, teknolojik araçlarla algılanıp ölçülebildiğinden, gelişen teknolojilerle birlikte frekansların günlük haberleşmemiz için önemli birer unsur olduklarını görmekteyiz. Günümüzde kimi zaman aynı bölgede çok fazla kullanıcının aynı anda mobil haberleşme yöntemiyle iletişim kurmak istemesi durumunda yaşanan iletişim aksaklıklarında, aynı frekans bandının yoğun bir şekilde kullanılıyor olmasının sonuçlarını tecrübe ederiz. Özetle, frekansları görmesek de aldığımız kamu hizmeti niteliği taşıyan elektronik haberleşme hizmetlerinin sunumu için vazgeçilmez bir kaynak olduğunu sadece hukuki metinlerden değil; yaşantımızın bir gerçeği olarak da algılamaktayız. Öte yandan, hukuki metinler toplumun ihtiyaçlarını gidermeye yönelik olduğundan, frekansların ayrı birer kamu kaynağı olarak belirtilmesi ve bu yönde özel bazı düzenlemeler içermesi özellikle mobil teknolojinin yaygınlaşması ile birlikte gerek ülkemizde gerekse Avrupa Birliği'nde 2000'li yılların başını bulmuştur. Avrupa Birliği'nin 2002/20/EC sayılı Yetkilendirme Direktifi ve 2002/21/EC sayılı Çerçeve Direktifinde frekansların bir tür kaynak oldukları belirtilerek bunların özel kişilere ancak ücreti karşılığında hizmet sunumu amacıyla üye devletlerce kullanım haklarının verilebileceği belirtilmişken, bu Direktifleri de kapsayacak şekilde tüm elektronik haberleşme düzenleyici çerçevesini tek bir metinde birleştiren 2018/1972 sayılı Avrupa Elektronik Haberleşme Kanunu (European Union, 2018), frekansın piyasa değeri olan ve kıt bir kamu malı[2] olduğunu açıkça belirterek frekans kaynağına ilişkin daha detaylı düzenlemeler getirmektedir. Ülkemizde de 05.11.2008 tarihli ve 5809 sayılı Kanun sonrası frekansların Devletin yetki ve sorumluluğu altında kaynaklar olduğu belirtilerek, bu kaynağa ihtiyaç duyulan elektronik haberleşme hizmetlerinin özel kişilere gördürülmesi usulleri Avrupa Birliği mevzuatına koşut biçimde, frekansların özel kişilerce kullanılmasına izin verilmesi halini almıştır. Benzer şekilde, hizmet sunumu dışında frekans kaynağına ihtiyaç duyan başta kamu kurumları olmak üzere diğer paydaşların frekans kullanımına ilişkin hususlar da ayrıca detaylı bir şekilde düzenlenmiştir. Bu çalışmanın amacı, geli-

[2] public resource" ve "public good" (md.45) şeklinde ifade edilmektedir. (European Union, 2018, Önsöz paragraf 127; md.45). Birinci tanımlama için "kamu kaynağı" ikinci ifade için "kamu malı" çevirisi kullanılabilir.

şen teknoloji ile birlikte gelecekte daha fazla hukuki düzenlemeye ihtiyaç duyacak olan frekans kaynağının ülkemizde tabi olduğu hukuksal rejim üzerine bir değerlendirme sunulması olup, çalışma araştırma ve yayın etiğine uygun olarak kaleme alınmıştır.

Makalede izlenen yöntem olarak; öncelikle, frekansların hukuki niteliğinin belirlenmesi için, frekansın tanımı yapılmaya çalışılmış; işin doğası gereği frekansın içerdiği teknik özelliklere ilaveten ilgili hukuki düzenlemelerin frekansı nasıl tanımladığı değerlendirilmiştir. Akabinde doğrudan frekans kaynağına yönelik yargı kararları yanında, bu kaynağa ilişkin yargının yapmış olduğu hukuki belirlemelerin benzer durumlar için diğer yargı kararlarında ve doktrinde ne anlama geldiği araştırılmaya çalışılmıştır. Anılan yöntemlerle frekansın hukuki nitelendirilmesinin yapılmasını takiben, bu hukuki nitelemeye doktrin ve yargı kararlarında bağlanan hukuki ilke ve kurallar açıklanarak bunların 5809 sayılı Kanun'da gözetilip gözetilmediği incelenmiştir. Son olarak, frekansın devamlı gelişen teknolojiye bağlı hukuki değişim geçiren bir kaynak olduğu gerçeğinden hareketle, gelecekte frekans kaynağına bağlı ihtiyaç duyulabilecek hukuki düzenlemelere de değinilmiştir.

1.FREKANSLARIN KAMU MALI NİTELİĞİNİN BELİRLENMESİ

1.1. 5809 SAYILI ELEKTRONİK HABERLEŞME KANUNUNA GÖRE FREKANSIN TANIMI VE HUKUKİ SINIRI

5809 sayılı Kanunu'nun "Kapsam" başlıklı 2'nci maddesinde "Elektronik haberleşme hizmetlerinin yürütülmesi ve elektronik haberleşme alt yapı ve şebekesinin tesisi ve işletilmesi ile her türlü elektronik haberleşme cihaz ve sistemlerinin imali, ithali, satışı, kurulması, işletilmesi, frekans dahil kıt kaynakların planlaması ve tahsisi ile bu konulara ilişkin düzenleme, yetkilendirme, denetleme ve uzlaştırma faaliyetlerinin yürütülmesi bu Kanuna tabidir." hükmü yer aldığından, frekansların hukuki nitelikleri belirlenirken 5809 sayılı Kanun ile bu Kanuna dayanılarak çıkarılan yönetmelik hükümleri önem arz etmektedir.

5809 sayılı Kanun'da frekans için doğrudan bir tanıma yer verilmemiştir. 5809 sayılı Kanun'a dayanılarak çıkarılan 02.07.2009 tarihli ve 27276 sayılı Resmî

Gazete'de yayımlanan Spektrum Yönetimi Yönetmeliği'nde Genel frekans planı (Allocation); "ITU tarafından dünya genelinde tanımlanan frekans bölgelerine göre yapılan frekans planlarına uygun olarak belirli bir frekans bandının bir veya daha çok sayıda karasal ve uzay telsiz haberleşme hizmetleri ile radyoastronomi hizmetleri tarafından belli şartlar dâhilinde kullanılması amacıyla Millî Frekans Planına işlenmesi" şeklinde tanımlanmıştır. Bu tanımda yer alan ITU (International Telecommunication Union); Uluslararası Telekomünikasyon Birliğini ifade etmekte olup, üyesi ülkelerle birlikte küresel radyo frekans ve uydu yörüngelerinin tahsis, plan ve politikalarını belirlemekle görevli bir Birleşmiş Milletler Kuruluşu'dur[3]. Ülkemizin de üyesi olduğu bu kuruluşun temel belgeleri olan ITU Anayasası ve Sözleşmesi, Türkiye tarafından uygun bulma kanunlarıyla onaylanmış ve yürürlüğe konulmuştur. Bu çerçevede, söz konusu belgeler diğer üye ülkelerde olduğu gibi ülkemiz açısından da bağlayıcı niteliktedir. ITU tarafından hazırlanan Terimler Sözlüğünde frekans; bir olayın bir saniyede kaç kez tekrarlandığını gösteren bir büyüklük olarak tanımlanmakta ve "hertz" (Hz) cinsinden ölçüldüğü belirtilmektedir (ITU, 2014). Frekans kelimesi mevzuatta sıklıkla "spektrum" kelimesi ile yakın anlam ilişkisi içerisinde kullanılmakta olup, spektrum ise; 5809 sayılı Kanun'un "Tanımlar ve kısaltmalar" başlıklı 3'üncü maddesinin (kk) bendinde "Elektronik haberleşme amacıyla kullanılan, frekansı 9 kHz-3000 GHz arasında olan ve uluslararası düzenleme yapılması halinde 3000 GHz'in üzerindeki frekanslar da dahil olmak üzere elektromanyetik dalgaların frekans aralığı" şeklinde tanımlanmıştır. Buna göre, bir büyüklük olarak frekansın elektronik haberleşme açısından önemini belirleyen husus, elektromanyetik dalgalarda frekansın, bir saniyedeki tekrar (titreşim) sayısını ifade etmesi nedeniyle; bu tekrar hızının dalganın enerji düzeyi, taşıyabileceği veri miktarı (bant genişliği) ve yayılım özellikleri üzerinde doğrudan etkili olmasıdır. Frekans yükseldikçe, birim zamanda daha fazla veri aktarımı mümkün hale gelirken, dalgaların yayılım mesafesi kısalmakta ve fiziksel engellere karşı duyarlılığı artmaktadır. Bu nedenle frekans, elektronik haberleşme altyapılarında hem teknik kapasiteyi hem de hizmet kalitesini belirleyen stratejik bir parametre olarak değerlendirilmektedir.

Frekansların teknik özelliklerine bu makalede yer verilmesinin önemi, bu

[3] https://www.itu.int/en/about/Pages/default.aspx Ayrıca ülkemiz, ITU'nun kurucu üyelerindendir. https://search.itu.int/history/HistoryDigitalCollectionDocLibrary/4.153.57.en.100.pdf ITU, 17 Mayıs 1865'te Paris'te "Uluslararası Telgraf Birliği" adı altında 20 Avrupa devleti tarafından kurulmuş; bu toplantıya Osmanlı İmparatorluğu da katılmıştır.

kaynakların fiziken algılanabilir ve belirlenebilir nitelikte olmamakla birlikte, sahip oldukları yükseklik (frekans değeri) ve doluluk (bant genişliği kullanımı) gibi parametrelerin, elektronik haberleşme hizmetlerinin kalitesi üzerinde doğrudan etkili olabilmesinden kaynaklanmaktadır. Bu teknik nitelikler, frekansların hukuki rejiminin belirlenmesinde de ayrıca dikkate alınması gereken unsurlar arasında yer almaktadır.

Öte yandan, 5809 sayılı Kanun, frekans için doğrudan bir tanıma yer vermemiş olsa da, frekansın ayırıcı bir takım özelliklerini düzenlemektedir. Bunlardan en önemlisi, 5809 sayılı Kanun'un "İlkeler" başlıklı 4'üncü maddesinde, frekans tahsislerinin yapılması ile bunların düzenlenmesinin "Devletin yetki ve sorumluluğu altında" olduğunun belirtilmesidir. Hukukumuzda doğal kaynakları düzenleyen yasalarda ise çoğunlukla bunların "Devletin hüküm ve tasarrufu altında" olduğunun belirtildiğini görüyoruz. Örneğin, Anayasamızın 43'üncü maddesi ile 3621 sayılı Kıyı Kanunu'nun 5 inci maddesine göre "Kıyılar, Devletin hüküm ve tasarrufu altındadır."; 3213 sayılı Maden Kanunu'nun 4'üncü maddesine göre "Madenler Devletin hüküm ve tasarrufu altında olup, içinde bulundukları arzın mülkiyetine tabi değildir."; 6491 sayılı Petrol Kanunu'nun 3'üncü maddesine göre, "Türkiye'deki petrol kaynakları Devletin hüküm ve tasarrufu altındadır."; 167 sayılı Yeraltı Suları Hakkında Kanun'un 1'inci maddesine göre, "Yeraltı suları umumi sular meyanında olup Devletin hüküm ve tasarrufu altındadır."; 5686 sayılı Jeotermal Kaynaklar ve Doğal Mineralli Sular Kanunu'nun 4'üncü maddesine göre "jeotermal kaynaklar ve doğal mineralli sular, Devletin hüküm ve tasarrufu altında olup bulundukları arzın mülkiyetine tâbi değildir.". Bu çerçevede, 5809 sayılı Kanun'da geçen "Devletin yetki ve sorumluluğu altında" ifadesinin, "Devletin hüküm ve tasarrufu altında" olma haline karşılık gelip gelmediğinin netleştirilmesinde fayda görülmektedir.

Esasen Anayasamız, "Ekonomik Hükümler" başlıklı İkinci Bölümünün "Tabiî servetlerin ve kaynakların aranması ve işletilmesi" başlıklı 168 inci maddesinde tabii (doğal) kaynakların hukuki durumlarına ilişkin düzenleme getirmektedir:

> "Tabiî servetler ve kaynaklar Devletin hüküm ve tasarrufu altındadır. Bunların aranması ve işletilmesi hakkı Devlete aittir. Devlet bu hakkını belli bir süre için, gerçek ve tüzelkişilere devredebilir. Hangi tabiî servet ve kaynağın arama ve işletmesinin, Devletin gerçek ve tüzelkişilerle ortak olarak veya doğrudan gerçek ve tüzelkişiler eliy-

> le yapılması, kanunun açık iznine bağlıdır. Bu durumda gerçek ve tüzelkişilerin uyması gereken şartlar ve Devletçe yapılacak gözetim, denetim usul ve esasları ve müeyyideler kanunda gösterilir."

Anayasa Mahkemesi (AYM); Kurumun tahsis ettiği frekans ve numara kaynakları için iptal/geri alma dahil her türlü değişikliği yapabileceği ve bu konuda yapılacak düzenlemeler sonucunda herhangi bir yükümlülük altına girmeyeceği yönündeki 5809 sayılı Kanun'un 31'inci ve 36'ncı maddelerinin Anayasa'ya aykırı olduğu savıyla açılan davada, Anayasa'nın 168'inci maddesini dayanak göstererek, 5809 sayılı Kanun'da frekans, numara, uydu pozisyonu ve benzeri kaynak tahsislerinin yapılması ile bunların düzenlenmesinin Devletin yetki ve sorumluluğu altında olduğunun hükme bağlandığı sonucuna varmaktadır (AYM, E.2008/115, K.2011/86, 2/6/2011). AYM'nin bu kararından çeşitli sonuçlar çıkarmak mümkündür. Öncelikle, AYM'ye göre 5809 sayılı Kanun'daki "Devletin yetki ve sorumluluğu altında" olma hali; Anayasa'da ifadesini bulan "Devletin hüküm ve tasarrufu altında" olma hususuna karşılık gelmektedir. İkinci olarak, AYM'ce frekansların bir tür "tabii servet ve kaynak" olarak değerlendirildiği çıkarımını yapmak mümkündür.

Öte yandan, pozitif hukukumuzda "Devletin hüküm ve tasarrufunda olma" hususunu açıklayıcı mahiyette bir takım düzenlemelerin yer aldığını görüyoruz. Örneğin, 4721 sayılı Türk Medeni Kanunu'nun "Sahipsiz yerler ve yararı kamuya ait mallar" başlıklı 715'inci maddesinde "Sahipsiz yerler ile yararı kamuya ait mallar, Devletin hüküm ve tasarrufu altındadır." hükmü yer almaktadır. 3402 sayılı Kadastro Kanunu'nun "Kamu malları" başlıklı 16'ncı maddesinde ise, "Devletin hüküm ve tasarrufu altında bulunan sahipsiz yerler"; "Devletin hüküm ve tasarrufu altında bulunan kayalar, tepeler, dağlar (bunlardan çıkan kaynaklar) gibi, tarıma elverişli olmayan sahipsiz yerler ile deniz, göl, nehir gibi genel sular" ve "Devletin hüküm ve tasarrufu altında bulunan ormanlar" ifadesinin geçtiği görülmektedir.

Bu noktada Devletin hüküm ve tasarrufu altında olan mal, kaynak ve yerlerin "kamu malları" ile ilişkili olduğu görüldüğünden, kamu malı kavramı ve bu kavramın, devletin hüküm ve tasarrufu altında bulunan yerler ve kaynaklar ile ilişkisinin netleştirilmesinde fayda bulunmaktadır.

1.2 KAMU MALI KAVRAMI: HUKUKİ TANIM, DOKTRİN VE YARGI İÇTİHATLARI IŞIĞINDA DEĞERLENDİRME

1.2.1 Kavramsal Çerçeve

Ülkemizde , devletin ve diğer kamu tüzel kişilerinin sahip olduğu malları düzenleyen genel bir kanun olmadığından, kamu mallarının tanımlanması ve belirlenmesinde genel anlamda doktrin ve yargı içtihatları önemli rol oynamaktadır.

Dikkat çeken bir diğer husus ise terminolojik belirsizliklerdir. Kamu malları için doktrinde ve yargı kararlarında "devlet malları", "kamu hizmeti eşyası", "amme emlaki", "idare malları", "kamuya ilişkin mallar" gibi ifadelerin de kullanıldığını ve terim birliğinin olmadığını belirtmekte fayda bulunmaktadır (Gülan, 1995, s. 9-10). Örneğin; 21.7.1983 tarihli ve 2863 sayılı Kültür ve Tabiat Varlıklarını Koruma Kanunu'nun 5 inci maddesi "Devlet malı niteliği" başlığını taşırken; 3402 sayılı Kadastro Kanunu "Kamu malları" madde başlığı altında düzenlemeler getirmektedir.

Öte yandan doktrinde idarenin özel malı ile kamu malı arasında bir ayrım kabul edilmiş (Yayla, 1988, s.357) olmakla birlikte kamu malı ifadesinin dar ve geniş olmak üzere iki ayrı anlamda kullanıldığını belirten Gözler'e (2009, s.818-819) göre; "kamu malı" ifadesinin; kamu tüzel kişilerinin sahip olduğu kamu hukukuna veya özel hukuka tabi bütün mallarını anlatmak için kullanılabileceği; "kamusal mal" ifadesinin ise; kamu tüzel kişilerinin sadece kamu hukukuna tabi mallarını anlatmak için kullanılabileceğini; bununla birlikte böyle bir anlam farkı yaratmanın dilbilgisi bakımından zor olduğu gerekçesiyle kamusal mallar için de "kamu malı" ifadesini tercih ettiğini belirtmiştir. Biz de bu makalede, "kamu hizmeti", "kamu kurumu", "kamu gücü", "kamu hukuku" gibi ön adı "kamu" olan tamlamaların İdare hukukunda yaygınlığı nedeniyle okunuşta kolaylık sağlaması için Devlet ve kamu tüzel kişilerinin sahip olduğu sadece kamu hukukuna tabi mallarını ifade eder biçimde "kamu malı" ifadesini kullanmayı tercih ediyoruz. Ayrıca 3402 sayılı Kadastro Kanunu'nda tapuya tescil bakımından düzenlemeler getiren 16'ncı madde başlığının "Kamu malları" olması, bu tercihimiz için pozitif bir temel de oluşturmaktadır.

Kamu mallarının belirlenmesinde güçlük arz eden bir diğer husus ise, kamu mallarına ilişkin düzenlemelerin, farklı işlevleri olan birçok mal türünü kapsamak zorunda olduğu için, farklı mal türleri bakımından çok sayıda istisna hük-

mü içeriyor oluşudur (AYM, E.2004/85, K.2009/69, 02/06/2009). Bu düzenlemeler arasında en kapsayıcı nitelikte olanlardan "Kamu malları" başlıklı 21/6/1987 tarihli ve Kadastro Kanunu'nun 16 ıncı maddesi şöyledir:

> **"Madde 16 –** Kamunun ortak kullanılmasına veya bir kamu hizmetinin görülmesine ayrılan yerlerle Devletin hüküm ve tasarrufu altında bulunan sahipsiz yerlerden:
>
> **A)** Kamu hizmetinde kullanılan, bütçelerinden ayrılan ödenek veya yardımlarla yapılan resmi bina ve tesisler, (Hükümet, belediye, karakol, okul binaları, köy odası, hastane veya diğer sağlık tesisleri, kütüphane, kitaplık, namazgah, cami genel mezarlık, çeşme, kuyular, yunak ile kapanmış olan yollar, meydanlar, pazar yerleri, parklar ve bahçeler ve boşluklar ve benzeri hizmet malları) kayıt, belge veya özel kanunlarına veya Cumhurbaşkanlığı kararnamelerine göre Hazine, kamu kurum ve kuruluşları, il, belediye köy veya mahalli idare birlikleri tüzelkişiliği, adlarına tespit olunur
>
> **B)** Mera, yaylak, kışlak, otlak, harman ve panayır yerleri gibi paralı veya parasız kamunun yararlanmasına tahsis edildiği veya kamunun kadimden beri yararlandığı belgelerle veya bilirkişi veya tanık beyanı ile ispat edilen orta malı taşınmaz mallar sınırlandırılır, parsel numarası verilerek yüzölçümü hesaplanır ve bu gibi taşınmaz mallar özel siciline yazılır.
>
> Bu sınırlandırma tescil mahiyetinde olmadığı gibi bu suretle belirlenen taşınmaz mallar, özel kanunlarında yazılı hükümler saklı kalmak kaydıyla özel mülkiyete konu teşkil etmezler.
>
> Yol, meydan, köprü gibi orta malları ise haritasında gösterilmekle yetinilir.
>
> **C)** Devletin hüküm ve tasarrufu altında bulunan kayalar, tepeler, dağlar (bunlardan çıkan kaynaklar) gibi, tarıma elverişli olmayan sahipsiz yerler ile deniz, göl, nehir gibi genel sular tescil ve sınırlandırmaya tabi değildir, istisnalar saklıdır.
>
> **D)** Devletin hüküm ve tasarrufu altında bulunan ormanlar, bu Kanunda hüküm bulunmayan hallerde, özel kanunları hükümlerine tabidir."

Elbette bu hüküm, taşınmaz malların sınırlarını belirtmek ve hukukî durumlarını tespit etmek suretiyle 4721 sayılı Türk Medeni Kanunu'nun öngördüğü tapu sicilini kurmak amacıyla çıkarılan bir kanun hükmü olduğundan; yalnızca taşınmazları kapsamaktadır; tabii servet ve kaynakların hepsi veya taşınır mallar burada yer almamaktadır. Bununla birlikte, düzenlediği kamu malları için, "devletin hüküm ve tasarrufu altındaki sahipsiz yerler" "orta malları", "bir kamu hizmetinin görülmesine ayrılan yerler", "Kamunun ortak kullanılmasına ayrılan yerler" şeklinde ayrım ve tanımlamalar yapması nedeniyle önem arz etmektedir.

Doktrinde önceleri Fransız hukukunun etkisiyle devlet malları üst başlığı altında; kamu hizmetlerinin ve halkın doğrudan doğruya bağlantısı olduğu ve bu bakımdan idare hukukuna hükümlerine tabi olduğu kabul edilen kamu malları ve devlet ile diğer kamu tüzel kişilerinin diğer bireyler gibi yararlandıkları özel mallar olarak ikiye ayrıldığı hususu gündeme gelmiştir (Onar, S.S., 1966, s.1300). Bu görüş kamu hizmeti ile bağlantısı geniş tutulduğu ve kamu malı kavramını çok genişlettiği için eleştirilmiş (Gülan, 1995, s.28); bu eleştiriye çözüm olarak kamu hizmetine, o hizmetin bir unsurunu teşkil edecek şekilde bağlanmış olması kriteri getirilmiş ve 1982 Anayasası öncesi dönemindeki yargı kararlarında benimsenmiştir (Duran, 1984, s.46). Günümüzde ise, kamu malının özel bir düzenlemeyle kamu hizmetine tahsis edilmiş olması esası benimsenmiştir. Buna göre, doktrinde, kamu malları teorisinin esinlendiği Fransız hukukunun da etkisiyle, kamu tüzel kişisinin mülkiyetinde bulunan ve kamunun doğrudan kullanımına/yararlanmasına tahsis edilen (özgülenen) ya da özel bir düzenleme ile bir kamu hizmetine tahsis edilen taşınır ve taşınmaz mallar kamu malı olarak tanımlanmaktadır. (Gözübüyük ve Tan, s.1072-1073; Gözler, 2009, s.825; Akyılmaz vd., 2017, s.698; Gülan, 1995, s.29). "Kamunun doğrudan kullanımına veya bir kamu hizmetine tahsis" şartı; tek bir şart olarak "kamu yararına tahsis" olarak da telaffuz edilebilmektedir (Gözler, 2009, s.821).

Şu halde, bir malın kamu malı olup olmadığını belirlemek için önce organik unsur olarak mala sahip olan tüzel kişiliğin, Devlet veya diğer kamu tüzel kişileri olması gerekmektedir. Burada özellik arz eden husus ise, AYM'nin bir kurumun kamu tüzel kişiliğini haiz olup olmadığını belirlerken, bu kurumun mallarının aşağıda belirteceğimiz bir takım kamusal ayrıcalıklara sahip olup olmadığını denetlemesidir. Örneğin; AYM bir kararında kurumun mevcutlarının devlet mallarına ait haklara sahip olmasını da dikkate alarak kamu kurumu niteliğinde olduğu hususunda şöyle değerlendirme yapmaktadır:

> "…Kanun'un 11. ve 14. maddeleri uyarınca; İLKSAN'ın Millî Eğitim Bakanlığına bağlı olarak faaliyet göstermek üzere kanunla kurulmuş bir tüzel kişilik olduğu, üzerinde Millî Eğitim Bakanlığının idari vesayet yetkisinin bulunduğu, bu bağlamda işleyiş tarzının ve esaslarının belirlendiği ana statüsünün Millî Eğitim Bakanlığınca hazırlandığı, mevcutlarının ve alacaklarının devlet mallarına ait hak ve önceliklere sahip olduğu, gelirlerinin her türlü vergi, resim ve harçtan muaf olduğu gibi haciz ve temlik edilemediği gözetildiğinde anılan kuruluşun, üyelerinin serbest iradelerinin eseri olmadığı, fonksiyonları bakımından kamu gücüne dayanan bir statüye sahip olduğu, işlemlerinin kapsam ve sınırının kanunla belirlendiği ve bu özellikleri nedeniyle tüzel kişiliğe sahip bir kamu kurumu olduğu açıktır" (AYM, E.2016/192, K.2017/160, 29.11.2017)

Bu noktada aslında kanun koyucunun bir kuruluşu kamu tüzel kişiliği olarak düzenlemesi durumunda, bu tüzel kişiliğe kamusal nitelik kazandırmak ile amaçlanan kamu yararına uygun olarak, bunun mallarına da özel bir rejim öngördüğü çıkarımı yapılabilir. Bu çerçevede, bir kamu tüzel kişisinin mallarının, özel hukuk rejiminden farklı bir takım ayrıcalıklı düzenlemelere tabi olması da, esasen kamu tüzel kişiliğinin kuruluş amacı ile görev ve yetkilerini herhangi bir kısıtlamaya tabi olmadan yerine getirebilmesinin sağlanması olduğu sonucuna varabiliriz.

Kamu malı tanımına ait organik unsur sonrasında ise; kamu malının niteliğinin belirlenebilmesi için malın doğrudan kamunun kullanımına sunulup sunulmadığı ile özel bir düzenleme ile kamu hizmetine tahsis edilip edilmediğine bakılacaktır.

Kamu tüzel kişilerinin özel hukuka tabi malları (özel malları) ise, ihale esaslarına uymak, kamulaştırma amacının gereğini yerine getirmek şeklinde bazı kayıtlamalar dışında, herhangi bir malik gibi tasarrufta bulunabileceği mallarıdır (Düren, 1975, s.89). Bu mallar kamu yararı amacından çok gelir getirme amacı taşırlar. Esasen idarenin uhdesinde olup da henüz veya kamunun doğrudan yararlanmasına veya kamu hizmetine tahsis edilmemiş mallardır. Bu anlamda kamulaştırılan ancak henüz kamunun yararına tahsis edilmemiş olan bir taşınmaz idarenin özel malıdır. Bu mallardan doğan uyuşmazlıklar kural olarak adli yargı yerlerinde çözümlenir (Akyılmaz vd., 2017, s.699).

AYM ise, "Kamu malları, kamu idare ve kurumlarının gerek kamunun doğrudan kullanımına ayrılmış, gerekse nitelikleri gereği veya hizmetin amacına uygun düzenlenmiş olmak kaydıyla kamu hizmetine tahsis edilmiş (özgülenmiş) malların tümü" şeklindeki tanımıyla (AYM, E.2004/85, K.2009/69, 02/06/2009) doktrin ile büyük ölçüde örtüşmektedir. Bununla birlikte AYM'nin, kamu hizmeti ile kamu malları arasındaki ilişkiyi daha geniş tanımladığı bir kararında (AYM, E.1996/66, K.1997/7, 31.1.1997) "Doğal nitelikleri gereği herkesin ortak yararlanmasına açık olan sahipsiz mallar ile kamu tüzelkişileri tarafından herkesin ya da halkın bir kısmının yararlanmasına ayrılan orta malları ve kamu hizmeti niteliğindeki etkinliklerin konusu ve aracı olan mallar, kamu malı olarak tanımlanabilir." denilmek suretiyle kamu hizmeti niteliğindeki etkinliklerin konusu ve aracı olan malların da kamu malı olduğu belirtilmiştir.

1.2.2.Kamu Mallarının Tabi Olduğu İlkeler

Kamu malı olduğu belirlenen bir malın özel mülkiyetten ayrı kamu hukukuna tabi bir takım ilke ve kurallara tabi olacağı hususunda doktrin ve yargı kararlarında görüş birliği bulunmaktadır. Elbette bu ilke ve kuralların doğrudan bir kanunda yer almayışı nedeniyle, yasa koyucunun her bir kamu malı için farklı rejimler getirebilmesi bakımından kolaylık sağlasa da, yasa koyucu anayasanın çizdiği sınırlarla çevrilidir.

Öte yandan, söz konusu ilke ve kuralların önemli bir bölümü, eşyanın tabiatından kaynaklanan zorunluluklardır. Örneğin; kamu mallarının devir ve ferağ edilmezliği; bu malların özel mülkiyete tabi mallar gibi el değiştiremeyeceği gerçeğinin bir sonucudur. Nitekim yukarıda gördüğümüz gibi bu mallar ya doğrudan kamunun yararlanmasında bulunan nehirler, kıyılar, parklar, pazar yerleri gibi yerler ya da idari bir düzen içerisinde kamu hizmetinin görülmesinde kullanılan mallardır. Bu malların devir ve ferağ edilebilmesi için öncelikle kamuya sağladığı yarardan koparılması gerekmekle birlikte idarenin her türlü eylem ve işleminde kamu yararı amacı gözetmesi esastır. Diğer bir ifadeyle idarenin kamu hizmete tahsis ettiği bir malı, bu hizmet ile bağını koparmadan devredemeyecek olması işin doğası gereğidir. Benzer şekilde, bu malların kural olarak zamanaşımı ile kazanılamaması da özel mülkiyette bulunamayacak olmalarının bir diğer sonucudur. 2004 sayılı İcra İflas Kanunu'nun 88 inci maddesinin "Devlet malları ile mahsus kanunlarında haczi caiz olmadığı gösterilen mallar haczedilemez." doğrultusunda kamu mallarının haczedilmezliği ilkesi kabul edilmiş

olmakla birlikte, AYM bu yararlanmadan sadece dar anlamdaki kamu ilke ve kurallarına tabi kamu mallarının değil; idarelerin özel mallarını da kapsayacak şekilde tüm mallarının yararlanacağını belirtmiştir (AYM, E.1992/13, K.1992/50, 21.10.1992). Birçok yasada devlet malı olduğu belirtilen veya kamu malı niteliği olduğu anlatılan malların haczedilemeyeceği ifade edilmiştir[4]. Kamu mallarının kira gibi özel hukuk sözleşmelerine konu yapılamayacağı ilkesi hakkında ise Gülan, (1995, s.148-149) bu ilkenin ne kadar hayata geçmiş olduğunun tartışılması gerektiğini; birçok yasada kamu mallarının kiraya verilmesinden söz edildiğini; kiraya verilemeyeceğini belirten yasaların azınlıkta kaldığını belirtmektedir.

AYM ise kamu mallarının tabi olduğu rejimin özelliklerini şöyle açıklamaktadır:

> "Kamu mallarının elde edilmesi, tasarrufu, korunması ve elden çıkarılmasında gerek Anayasa'da ve yasalarda gerekse uygulamada özel ilkeler benimsenmiştir. İstisnaları olmakla birlikte, kamu mallarının zamanaşımı ile kazanılamayacağı, kamu malı statüsünü kaybetmedikçe özel mülkiyete konu olamayacağı, devredilemeyeceği, kamu mallarının haczedilemeyeceği ilkeleri ve kamu mallarının bazı hallerde özel bir korumaya tâbi tutulması, kamu mallarına hâkim olan ve özel mülkiyetin korunmasından kimi noktalarda ayrılan bir koruma rejiminin olduğunu göstermektedir." (AYM, E.2004/85, K.2009/69, 02/06/2009)

Kamu mallarının tabi olduğu özellikler Yargıtay Hukuk Genel Kurulu tarafından ise şu şekilde ifade edilmiştir:

> "Bir malın kamu malı olarak nitelendirilmesinin hukuksal sonuçları şunlardır: Kamu malları üzerinde özel mülkiyet kurulamaz ve bunlar kamu hizmetine tahsis olundukları, yetkili idarece kamu malı olmaktan çıkarılmadıkları sürece temlik edilemez, kazandırıcı zamanaşımı yoluyla da edinilemezler. Devlet mallarının haczine de olanak yoktur (İcra ve iflas Kanunu, madde 82). Buradaki 'özel mülkiyet kurulamaz' sözü, 'gerçek kişilerin veya özel hukuk tüzel kişile-

[4] Örneğin, 2690 sayılı Türkiye Enerji, Nükleer Ve Maden Araştırma Kurumu İle İlgili Bazı Düzenlemeler Yapılması Hakkında Kanun'un Ek Madde 3- (Ek: 2/7/2018 - KHK/703/119 md.) (Değişik: 29/5/2025-7549/12 md.) *"Türkiye Enerji, Nükleer ve Maden Araştırma Kurumunun mal ve varlıkları Devlet malı sayılır, haczedilemez ve rehnedilemez."* hükmü yer almaktadır.

rinin mülkiyetine giremez şeklinde anlaşılmalıdır" (Yargıtay Hukuk Genel Kurulu, E.2022/751, K.2023/1094, 15.11.2023).

Yargı kararlarında da, kamu mallarının özel mülkiyet konusu olamayacağı ilkesinden yola çıkılarak doktrin ile aynı şekilde; bunların devir edilemeyeceği, kazandırıcı zamanaşımı ile kazanılamayacağı ve haczedilemeyeceği kabul edilmektedir.

1.3 Devletin Hüküm ve Tasarrufu Altındaki Mallarının Hukuki Niteliği

Devletin hüküm ve tasarrufu altında olan malları düzenleyen genel bir kanun olmadığından, kanun koyucu çoğu zaman Devletin hüküm ve tasarrufu altında olduğunu belirttiği bir kaynak veya mal için sadece bu kaynak veya malın özelliklerini gözeterek bir takım özel düzenlemelere yer vermektedir. Öte yandan, herhangi bir yasada "Devletin hüküm ve tasarrufu altında olmak", unsurlarıyla tanımlanmamış olsa da, 4721 sayılı Türk Medeni Kanunu'nun "Sahipsiz yerler ve yararı kamuya ait mallar" başlıklı 715'inci maddesinde "Sahipsiz yerler ile yararı kamuya ait mallar, Devletin hüküm ve tasarrufu altındadır." hükmü, Devletin hüküm ve tasarrufu altındaki yerlerin, sahipsiz yerler ve yararı kamuya ait mallar olmak üzere iki farklı kategori içerdiğini göstermektedir. Esasen bu kavram kapsamındaki malların nelerden oluştuğundan daha önemlisi, bu malların, kamu malları içerisinde yer alıp almadığı ile bu soruya olumlu yanıt verilmesi durumunda, bu malların kamu mallarından ayrıksı bir takım hukuki ilke ve kurallara tabi olup olmayacağıdır. Bu sorulara verilecek yanıtlarla devletin hüküm ve tasarrufu altında olduğu belirlenen frekansların da tabi olacağı hukuksal rejimin çerçevesi için bir belirleme yapılabilecektir.

AYM, yasa koyucunun "devletin hüküm ve tasarrufu altında" olduğunu belirttiği mallar veya kaynaklar için doğrudan kamu malı tanımlamasını kullanmaktadır. Örneğin, bir kararında kıyıların Anayasa'nın 168'inci ve 43'üncü maddeleri gereğince Devletin hüküm ve tasarrufu altında olduğunu belirttikten sonra, kıyıların doğal niteliği itibarıyla herkesin serbestçe yararlanmasına açık ve bu nedenle bir kamu malı olduklarını belirtmiştir (AYM, E.2019/35, K.2019/53, 26/06/2019) Bir başka kararında ise, bu malları "özellik gösteren kamu malları" olarak tanımlamaktadır. Bu kararında şu ifadelere yer verilmiştir:

> "Görülüyor ki, bu maddelere egemen olan anlayış, özellik gösteren bir kamu malına karşı, bir anayasal sorumluluk ve duyarlıktan kaynaklanmaktadır. Devletin hüküm ve tasarrufu altına bırakılan bu malların korunmasında, devletin merkezi örgütünde yer alan uzman ve yetkili kuruluşlarının görevlendirilmesi, yukarıda temel ilke ve esasları açıklanan kıyı rejiminin bir gereğidir. Yasakoyucu, anayasal rejimi kurarken, bu kamu malına özgü, devletin, merkezi ve yerel kuruluşlarının görev alanını belirlemiş, Anayasa'n m 43. maddesinin gereğini yerine getirmiştir. Soruna, salt, yerel gereksinim açısından yaklaşılmamış aynı zamanda, kıyının ülke tümlüğü içindeki yeri gözetilmiştir (AYM, E.1990/23, K.1991/29, 18/09/1991).

Onar (1966, s.1364); Devletin hüküm ve tasarrufu altında olduğu belirtilen tabii servet ve kaynakların diğer kamu malları gibi Devletin mülkiyeti altına bile koyulmadığını ve bu nedenle devletin dahi mülkiyet hakkının olmadığı bir durumda özel mülkiyetten söz etmenin mümkün görünmediğini ifade etmektedir. Buna göre Onar, Devletin hüküm ve tasarrufu altında olan yerlerin kamu malları içerisinde olduğunu kabul etmekle birlikte, bu mallar üzerinde herhangi bir mülkiyetten söz etmenin mümkün olmadığını işaret etmektedir. Duran (1984 ,s.49) ise bu kavramın egemenlik içermediği gibi geniş manada zabıta kudretinden de ibaret sayılmadığını; bu kavramın Türk hukukuna özgü ve genel olarak kamu mallarını hem bireylere ve topluluklarına, hem de devlete ve malik tüzel kişilerine karşı korumayı amaçlayan ve özel mülkiyet hakkının sakıncalarından koruyan bir önlem ilkesi olarak kabul edilebileceğini ifade etmektedir. Bilgen'e göre (1994, s.38); Medeni Kanun, devletin hüküm ve tasarrufu altındaki yerleri mülkiyet rejiminin dışına çıkarmış ve her birinin kendine özgü ve tamamen kamu hukuku kurallarından oluşan bir statüsü vardır; istisnai olarak medeni hukuk kurumlarından yararlanabilirler ve kıyılar, denizler, ormanlar gibi sahipsiz mallar; tabii servet ve kaynakların, ormanların ve yollar, köprüler, pazar yerleri gibi malların bu kapsamda olduğunu belirtmektedir.

Şu halde, Devletin hüküm ve tasarrufu altında olan varlıkların doktrin ve yargı kararlarında kamu hukuku ilke ve kurallarına bağlı kamu malı olarak nitelendirildiğini söyleyebiliriz.

1.4 Frekansların Hukuki Niteliği Yönünden Değerlendirme

5809 sayılı Kanun'da Devletin yetki ve sorumluluğu altında olduğu belirtilen frekansların, AYM tarafından Anayasa'nın 168'inci maddesi çerçevesinde Devletin hüküm ve tasarrufu altında olan tabii servet ve kaynak olarak belirlenmesi ve bu tür varlıkların doktrinde kamu malı olarak fakat AYM tarafından özellik gösteren kamu malı olarak nitelendirilmesi karşısında, fiziken algılanabilir ve belirlenebilir olmayan frekansların ise devletin hüküm ve tasarrufu altındaki kaynaklar içerisinde *sui generis* bir kamu malı olduğu sonucuna varabiliriz. Bununla birlikte, bu kaynakların hukuksal rejimini değerlendirebilmek için öncelikle Devletin hüküm ve tasarrufu altındaki varlıkların hukuksal rejimini genel hatlarıyla ortaya koymakta fayda bulunmaktadır.

2. DEVLETİN HÜKÜM VE TASARRUFU ALTINDAKİ VARLIKLARIN HUKUKSAL REJİMİ

Devletin hüküm ve tasarrufu altındaki varlıkların kamu malı olarak nitelendirilmesinin kural olarak sonucu, bunların da kamu mallarına uygulanan hukuksal rejime tabi olacağıdır. Bununla birlikte AYM, bu durumdaki varlıklar için kamu mallarından ayrılan bir takım hukuksal değerlendirmelerde bulunmuştur. Bunlardan en önemlisi Devletin bunlar üzerinde sahip olduğu tasarruf yetkisini geniş şekilde yorumlamasıdır. Tapu kütüğünde kimse adına tescil edilmemiş taşınmazların olağanüstü zamanaşımı ile kazanılmasına yönelik zilyedin sunacağı delillere ilişkin yeni düzenleme getiren kanun hükmünü inceleyen AYM bu hususta değerlendirmesini şöyle aktarmaktadır:

> "Şüphesiz kanun koyucu, Devletin hüküm ve tasarrufu altında bulunan sahipsiz yerlerin mutlaka kişiler tarafından işgal ihya ve imar yollarıyle veya başka biçimlerde mal edinilebilmesinin sebep ve şartlarını tesis etmek zorunluğunda değildir. Hattâ bir kanunla bu hükümlerin tümünün ilga ederek bu gibi yerler üzerinde zilyedlik yolu ile bir hak doğamıyacağını ilân da edebilir" (AYM, E.1966/19, K.1968/25, 19/06/1968).

Benzer şekilde, devletin hüküm ve tasarrufu altındaki yerlerin zamanaşımı ile kazanılmasına yönelik olarak;

> "Devletin hüküm ve tasarrufu altında bulunan taşınmazların, bu taşınmazlara belli koşullar dâhilinde zilyet olanlarca mülk edinilebilmesi, kanun koyucunun takdir yetkisi çerçevesinde getirilen bir imkân olup anayasal bir zorunluluğu ifade etmediği gibi, anayasal bir yükümlülüğün ifası amacı da taşımamaktadır. Dolayısıyla Devlet malı niteliğinde kabul edilen taşınmazların mülkiyet hakkının, olağanüstü kazandırıcı zamanaşımı yoluyla kazanılamaması da kanun koyucunun takdirinde olup hukuk devleti ilkesine aykırılık taşımamaktadır" (AYM, E.2016/49, K.2016/200, 28/12/2016)

denilmek suretiyle, bu tür yerlerin özel kişilerce zamanaşımı ile kazanılmasına imkan verilip verilmemesi hususunda devletin takdir yetkisinin bulunduğu belirtilmiştir. AYM burada, zamanaşımı ile kazanılamayacağını belirttiği kamu malları rejiminden ayrıksı bir yorumda bulunmaktadır. Bu yorumun temelinde AYM'nin, devletin hüküm ve tasarrufu altında bulunan kaynaklar üzerinde devletin tasarruf ve karar verme yetkisini daha geniş olarak görmesi yatmaktadır. Hemen bu noktada kanun koyucunun yetkisinin sınırsız olmadığını Anayasa'daki kural ve ilkelerle sınırlandığını hatırlatalım. Bu çerçevede AYM, Anayasa'nın kıyılara ilişkin hükmü ile ormanların zamanaşımı ile kazanılamayacağı yolundaki hükmünü esas almak suretiyle,

> "Anayasa'nın 43. ve 169. maddelerinde temel bir değer olarak çevrenin korunması ve herkesin çevreden eşit şekilde yararlanması hakkını güvence altına almak amacıyla kıyıların ve ormanların devletin hüküm ve tasarrufu altında olduğu belirtilerek bu alanlarda özel mülkiyet yasaklanmıştır. Bu nedenle belli bir sürenin geçmesiyle söz konusu alanlarda özel mülkiyet edinilmesi olanaklı değildir"

şeklinde hüküm kurmuştur (AYM, E.2009/31, K.2011/77, 12.5.2011).

AYM, "Devletin hüküm ve tasarrufu altında olma"nın ne anlama geldiğini ise bir başka kararında şu şekilde açıklamaktadır:

> …Anayasa, tabii servetleri ve kaynaklarını Medeni Kanunun hükümlerine bağlı özel mülkiyet düzeninin kapsamı dışında bırakmakta, onlara. Devletin, devlet olma niteliği ile eli altında tuttuğu nesneler düzeni içinde yer vermektedir. Her iki düzen başka başka koşullara ve kurallara bağlıdır; değişik niteliktedir; aralarında bir-

> birlerine karıştırılmalarını önleyecek bellilik ve kesinlikte sınırlar vardır. Anayasa, . . . tabii servetlerin ve kaynakların devletin hüküm ve tasarrufu altında bulunduğunu açıklamakla aynı zamanda bunların mülkiyet konusu olamayacağını da hükme bağlamıştır .... Aslında mülkiyet düzenine bağlı bulunmayan bir nesnede mülkiyetin devri de öncelikle söz konusu olamaz (AYM, E.1990/23, K.1991/29, 18/09/1991).

Kararda geçen "Devletin, devlet olma niteliği ile eli altında tuttuğu nesneler düzeni" ifadesiyle; Devletin egemenlik yetkisine dayanarak doğrudan tasarruf ettiği varlıkları kapsayan bir hukuki düzeninin işaret edildiği değerlendirmesi yapılabilir.

Devletin hüküm ve tasarrufu altında bulunduğu anayasal düzeyde belirtilen tabii servet ve kaynaklardan biri, kıyılardır. Anayasa'nın "Kıyılardan yararlanma" başlıklı 43'üncü maddesinde; kıyıların devletin hüküm ve tasarrufu altında olduğu belirtildikten sonra deniz, göl ve akarsu kıyılarıyla, deniz ve göllerin kıyılarını çevreleyen sahil şeritlerinden yararlanmada öncelikle kamu yararı gözetileceği ve bu yerlerden yararlanma imkân ve şartlarının kanunla düzenleneceği ifade edilmiştir. AYM, kıyıların devletin hüküm ve tasarrufu altında olmasının, buraların özel mülkiyete konu olamayacağı ve doğasına uygun olarak genellik, eşitlik ve serbestlik ilkeleri çerçevesinde herkesin ortak kullanımına açık bulunmaları gerektiği anlamına geldiğini ifade etmektedir (AYM, E.2020/42, K.2023/99, 18/5/2023).

Esasen Anayasamızın 168'inci maddesiyle; Devletin hüküm ve tasarrufunda bulunan tabii servet ve kaynaklar için özel bir hukuki rejim öngörülmüştür. Buna göre devletin hüküm ve tasarrufunda bulunan tabii servet ve kaynakların aranması ve işletilmesi hakkı Devlete ait olmakla birlikte kanunun açıkça vereceği izne bağlı olarak Devlet bu hakkını belirli bir süre ortak olarak veya doğrudan gerçek ve tüzel kişiler eliyle yapılmasını sağlayabilir. Böyle bir durumda da devletin gözetim, denetim ve yaptırım uygulama yetkileri bulunmakla birlikte, devletin bu yetkileri ile söz konusu gerçek ve tüzel kişilerin uyacağı şartların kanunla düzenlemesi şartı bulunmaktadır.

AYM söz konusu Anayasa hükmünü yorumladığı bir kararında şu ifadelere yer vermektedir:

"Doğal servet ve kaynakları yerinde kullanarak ya da onlardan yerinde yararlanarak kamu hizmeti üreten KİT'lerin özelleştirilmesinde Anayasa'nın 168. maddesinde öngörülen ilkelerin gözönünde bulundurulması zorunludur. 168. maddeye göre işletme hakkı devlete ait olan doğal servetler ve kaynakların işletme hakkı gerçek veya tüzel kişilere ancak süreli olarak devredilebilir. Doğal servet ve kaynaklardan yararlanarak kamu hizmeti üreten KİT ya da buna bağlı kuruluşlar ile diğer kamu tüzel kişilerin varlıklarının özelleştirilmesinde bunların yararlandıkları doğal servet ve kaynakların mülkiyetinin gerçek ve tüzel kişilere devri olanaksızdır.

Bu tür KİT'lerin yasada öngörüldüğü gibi satış yöntemiyle özelleştirilmeleri durumunda, mülkiyete bağlı işletme hakkı da süresiz olarak satın alanlara geçecektir. Buna karşılık, kamu hizmeti üretilmesinde yararlanılan doğal servet veya kaynağın işletme hakkının devredilmediği; KİT'lerin işletme hakkının devredildiği ileri sürülebilirse de kamu hizmetini bu biçimde üreten KİT'ler ile bunların kamu hizmeti üretiminde yararlandıkları doğal zenginlik ve kaynakların birbirinden ayrı düşünülmesi olanaksızdır.

Doğal zenginlik ve kaynaklarla ilgili KİT'lerin ve diğer kamu tüzel kişilerinin varlıklarının özelleştirilmesinde, bunların yararlandıkları doğal zenginlik ve kaynakların işletme hakkının belli süreyle devri biçiminde olması zorunludur. KİT'lerin yararlandıkları doğal zenginlik ve kaynakların satış ya da işletme hakkının süresiz devri biçiminde özelleştirilmeleri Anayasa'nın 168. maddesine aykırı düşer.

Bu nedenlerle, 3987 sayılı Yasa doğal zenginlik ve kaynaklarla ilgili KİT'lerin satışına ve bunların işletme hakkının süresiz devredilmesine olanak verdiğinden Anayasa'nın 168. maddesine aykırıdır." (AYM, E.1994/49, K.1994/45, 07/07/1994)

AYM'nin bu kararından şu sonuçlara ulaşılabilir:

- doğal servetler ve kaynakların işletme hakkı gerçek veya tüzel kişilere ancak süreli olarak devredilebilir.
- doğal servet ve kaynakların mülkiyetinin gerçek ve tüzel kişilere devri olanaksızdır.

- kamu hizmetini üreten kurumlar ile bunların kamu hizmeti üretiminde yararlandıkları doğal zenginlik ve kaynakların birbirinden ayrı düşünülmesi olanaksızdır.

AYM, bir başka kararında ise, devletin hüküm ve tasarrufunda bulunan kıyılar yönünden yapılan düzenlemeyi, Devletin gözetim ve denetim görevini yerine getirmesini sağlayacak kurallara yer verilmeksizin düzenlenmesinin hukuki belirsizliğe yol açacağını ifade etmektedir. (AYM, E.2019/35, K.2019/53, 26/06/2019)

O halde, Devletin gözetim ve denetim yükümlülüğü bulunduğu tabii servet ve kaynaklara ilişkin yapılacak düzenlemelerde devletin bu yükümlülüklerini yerine getirmesini sağlayacak kuralların bulunmaması durumunda AYM'nin, Anayasa'nın 168'inci maddesi yönünden iptal kararı verebileceği söylenebilir.

3. 5809 SAYILI ELEKTRONİK HABERLEŞME KANUNU'NDA FREKANSLARIN TABİ OLDUĞU HUKUKSAL REJİMİN DEĞERLENDİRİLMESİ

3.1. GÜNCEL HUKUKİ ÇERÇEVE

Frekansların, kamu malları içerisinde özellik arz eden devletin hüküm ve tasarrufu altında bulunan kaynaklar kategorisi altında olmakla birlikte, fiziken algılanabilir ve belirlenebilir olmayışları nedeniyle de kendine özgü bir kamu malı olduğu sonucuna vardığımızdan, frekansların hukuki rejiminin özel hukuk ilke ve kurallarından ayrık olarak frekansların mahiyeti uygun düştükçe kamu hukuku ilke ve kurallarına göre belirlenmelidir. Örneğin, frekansların taşınır veya taşınmaz bir mal olmadığı için yürürlükteki mevzuatımıza göre zamanaşımı ile kazanılmaları zaten fiilen olanaksız olduğundan, kamu mallarının kural olarak zamanaşımı ile kazanılamayacakları yönündeki ilke burada uygulama alanı bulamayacaktır.

Öte yandan AYM'nin, tabii servet ve kaynakları, bunları kullananların varlığından ayrı tutulamayacağı yönündeki isabetli görüşü çerçevesinde, frekans kaynağının, gerçek veya tüzel kişilerce kullanımına izin veren tahsisten (ve özel kişilerce hizmet sunumuna izin veren ve tahsisin özel bir türü olan kaynağın kullanım hakkının verilmesinden) ayrı düşünmek olanaksızdır.

Gerek Anayasa'nın devletin hüküm ve tasarrufundaki kaynaklar için bağladığı sonuçlara gerekse de doktrin ve yargı kararlarıyla şekillenen kamu mallarına ait özelliklere ilişkin hususlara 5809 sayılı Kanun ve buna dayanılarak çıkarılan yönetmeliklerde rastlanmaktadır. Örneğin; 5809 sayılı Kanun'un 3 üncü maddesinde "kullanım hakkı" *"Frekans, numara, uydu pozisyonu gibi kıt kaynakların kullanılması için verilen hakkı,"* şeklinde tanımlanarak, frekansların özel kişilerce kullanılmak suretiyle elektronik haberleşme hizmeti sunulmasının sağlanmasına aynı Kanun'un 9'uncu maddesi ve devamı hükümlerinde yer verilmesi, bu kaynakların Anayasa'nın 168'inci maddesinde belirtildiği üzere özel kişilerce işletilmesine bir örnek teşkil etmektedir. Burada, Anayasa'nın 168'inci maddesindeki ifadenin "kaynakların aranması ve işletilmesi" olarak geçtiği; frekans kaynağının ise aranmaya muhtaç olmadığı belirtilebilir. Bununla birlikte, Anayasa'nın bu hükmünün gerekçesinde, arama faaliyetlerinden ayrı olarak "Amaç millî servetin işletilmesini ve millî gelirin artırılmasını biran önce sağlamaktır." denilmektedir (AYM, 2021). Ayrıca, bu Anayasa hükmü yürürlüğe girdiğinde frekansların henüz devletin hüküm ve tasarrufunda olduğu ve elektronik haberleşme hizmetleri için en kıymetli unsurlardan biri olduğu henüz dünyada bile tam olarak kabul görmüş bir durum değildi. Bu nedenle anayasanın ruhuna uygun olarak, bu maddeden salt olarak kaynakların işletilmesini de anlamak uygun olacaktır. Nitekim kaynakların aranma ve işletilmesine tipik bir örnek teşkil eden 3213 sayılı Maden Kanunu da arama ve işletme için ayrı ayrı (md.3); "Arama Ruhsatı : Belirli bir alanda maden arama faaliyetlerinde bulunulabilmesi için verilen yetki belgesi"; "İşletme Ruhsatı : İşletme faaliyetlerinin yürütülebilmesi için verilen yetki belgesi." şeklinde tanımlayarak bu tanımlara göre ayrı ruhsatlandırmalar yapılmasını öngörmektedir.

Benzer şekilde, Anayasa'nın 168'inci maddesiyle uyumlu olarak devletin bu kaynakların işletilmesine yönelik denetim ve yaptırım uygulama yetkisine 5809 sayılı Kanun'un "Kurumun yetkisi ve idarî yaptırımlar" başlıklı 60'ıncı maddesinde "Kurum; mevzuata, kullanım hakkı ve diğer yetkilendirme şartlarına uyulmasını izleme ve denetlemeye, aykırılık halinde işletmecilere bir önceki takvim yılındaki net satışlarının yüzde üçüne kadar idarî para cezası uygulamaya,(…) yetkilidir." şeklinde yer verilmektedir. Bu yetki Kanun ile Bilgi Teknolojileri ve İletişim Kurumu (Kurum)'na verilmiştir. Bu hüküm, kullanım hakkını mevzuata uygun şekilde elinde bulundurmak suretiyle hizmet sunmaya yetkili işletmecilerin kullanım hakkı sınırlarına uymamalarına yönelik olmakla birlikte, bir kamu malı-

nın izinsiz ve yetkisiz kullanımının yaptırımı ceza hukuku alanına gireceğinden, bu hususa ilişkin düzenlemeler 5809 sayılı Kanun'un "Cezai hükümler" başlıklı 63'üncü maddesinde "Bu Kanunun 9 uncu maddesine aykırı olarak kullanım hakkı olmadan elektronik haberleşme hizmeti verenler, tesisi kuranlar ve/veya işletenler hakkında altı aya kadar hapis ve beş bin günden on beş bin güne kadar adli para cezasına hükmolunur." şeklinde ifade edilmiştir.

Öte yandan, AYM kararlarında zikredilen; tabii kaynakların genellik, eşitlik ve serbestlik ilkeleri doğrultusunda herkesin ortak kullanımına açık bulunmaları ilkesi gereğince frekans kaynağından elektronik haberleşme hizmet sunmak üzere yararlanmak isteyenlerin ödeyecekleri ücretler, 5809 sayılı Kanun'un 11'inci maddesinde yer alan "Kullanım hakkı ücretlerinin asgari değerleri, Kurumun önerisi ve Bakanlığın teklifi üzerine Cumhurbaşkanı tarafından belirlenir." hükmü çerçevesinde önceden herkes için eşit şekilde belirlenmektedir. Bu ücretler, toplumda bu kaynaktan doğrudan yararlanmayanların da bulunduğu gözetilerek ve 5809 sayılı Kanun'un 11'inci maddesinin "Kullanım hakkı ücretleri, 5369 sayılı Kanun hükümleri saklı kalmak kaydıyla Hazineye gelir kaydedilmek üzere ilgili muhasebe birimine yatırılır." hükmüyle, toplumda adil bir paylaşımın gereği olarak Hazine'nin geliri şeklinde düzenlenmiştir.

Benzer şekilde, 5809 sayılı Kanun'da frekansın bir kıt kaynak olduğunun ve etkin ve verimli kullanılmasının vurgulanması, bunların eşit ve genel bir şekilde paylaşımını da zorunlu kılmaktadır. Anılan Kanun'un "Frekans planlama, tahsis ve tescili" başlıklı 36 ncı maddesiyle, telsiz yayınlarının birbirleri üzerinde elektromanyetik girişim oluşturmaması ve frekans bantlarının etkin ve verimli şekilde kullanılmasını sağlamak amacıyla milli frekans planlaması yapma ve tahsisi, uluslararası koordinasyon ile tescil işlemleri yetkisi Kuruma verilmiştir.

5809 sayılı Kanun'un "Haczedilmezlik ve haberleşme hizmetlerinin sürekliliği" başlıklı 34'üncü maddesiyle; tahsis edilen frekans kullanım haklarının ve işletmecilerin yetkilendirmelerinin hiçbir şekilde haczedilemeyeceği hükme bağlanmıştır. Kamu mallarının devredilmezliği ve haczedilmezliği ilkesini kamu hizmetlerinin devamlılığına bağlayan görüşün (Bilgen, 1995, s. 92) madde başlığında benimsendiği görülmektedir. AYM'ye göre de; "Zor kullanılması Devlete tanınmış bir yetki olduğundan bunu Devletin kendisine karşı kullanması düşünülemez. Kamu hizmetlerinin aksatılmadan ve kesintiye uğramadan sağlanması ve bütçenin getirdiği esasların cebri icra sonunda tahmin dışı ihlallere uğratılma-

ması esastır." (AYM, E.1992/13, K.1992/50, 21/10/1992).

Esasen bir kamu malı olan frekans, özel mülkiyete konu olamayacağından bunlara ilişkin kullanım haklarının da haczedilemez nitelikte olması doğal bir sonuçtur. Nitekim, yargının da elektronik haberleşme hizmet sunumu için kaynakların kullanım hakkının verilmesiyle işletmecilerin bu kaynaklar üzerinde özel mülkiyet hakkının bulunmadığı (AYM, E.2008/115, K.2011/86, 2.6.2011; Işıklar, 2023, s.749) ve bunlara ilişkin yapılacak ücretlendirmeler yönünden işletmecilerin kazanılmış hak iddiasında bulunamayacakları yönünde kararlar verdiği görülmektedir (Danıştay 13. D., E.2005/6622, K.2005/6264, 30.12.2005). Yasa koyucu anılan hükümle, kaynaklara ilişkin kullanım haklarının ekonomik değerleri olduğundan bahisle, hacze konu olabileceği yönündeki tereddütleri ortadan kaldırmış ve kamu malı niteliğindeki frekansların tahsisinin özel mülkiyet sonucunu doğurmayacağı gerçeğinden hareketle bunların haczedilemez olduğunu isabetli bir şekilde açıkça düzenlemiştir.

Öte yandan, 5809 sayılı Kanun kapsamında yapılan değerlendirmeler sonucu alınan yargı kararlarında (Danıştay 13. D., E.2019/1485, K.2020/3038, 09.11.2020) yapılan; Devlete ait kaynakların özel hukuk kişilerine hizmet sunumu amacıyla kullandırıldığı değerlendirmesi yerinde olmakla birlikte frekansların yalnızca hizmet sunumu için işletmecilere ayrılmış bir kaynak olduğunu düşünmek eksik olacaktır. Frekanslar, devletin çeşitli kurumlarınca uydu teknolojilerinden kablosuz erişim sistemlerine kadar birçok iletişim teknolojisi ihtiyaçları için kullanılan ve bu kapsamda Kurum tarafından ilgili kurumlara tahsisi yapılan önemli bir kaynaktır. Örneğin, 5809 sayılı Kanun'un "Frekans planlama, tahsis ve tescili" başlıklı 36'ncı maddesine göre frekans tahsislerinde Dışişleri Bakanlığı, Jandarma Genel Komutanlığı ile Sahil Güvenlik Komutanlığı ihtiyaçları da dahil Türk Silahlı Kuvvetlerine, Millî İstihbarat Teşkilatı Müsteşarlığına ve Emniyet Genel Müdürlüğüne öncelik tanınmaktadır. Öte yandan, kamu kurumlarına yapılan tahsislerde milli güvenliğin sağlanmasına öncelik verilmesinin nedeni, bu kaynağın kamu yararına en iyi şekilde kullandırılmak istenmesidir. Frekans kaynağının bir çok paydaş tarafından etkin ve verimli kullanımı ve bu paydaşlar arasındaki kullanımın, birbirlerinin haberleşmelerini olumsuz yönde etkilemeyecek (elektromanyetik girişim/enterferans yaşanmaması) şekilde düzenlenmesi için ise Kurum; milli frekans planlaması, tahsisi, uluslararası koordinasyon ile tescil işlemleri için yetkili kılınmıştır. Hemen burada tahsis kelimesinin, işletmecilere frekans kullanım hakkı verilmesini de kapsayan ama bundan daha geniş bir

anlamda, ilgili mevzuata göre frekans kullanmaya yetkili olanlara frekansın kullanılması için verilen izni ifade ettiğini belirtelim. Nitekim, "Tahsis" kelimesi için 5809 sayılı Kanun'da ayrıca bir tanım yer almamakla birlikte bu Kanuna dayanılarak çıkarılan Spektrum Yönetimi Yönetmeliği'nin "Tanımlar" başlıklı 4'üncü maddesinin (ı) bendinde "Frekans tahsisi (Assignment): Detay frekans planına uygun olarak Kurum tarafından bir telsiz istasyonuna frekans veya frekans kanalları, çıkış gücü, yayın süreleri de dâhil belirli şartlar altında kullanmak üzere izin verilmesi" şeklinde tanımlanmıştır.

Frekansların devletin yetki ve sorumluluğu altında olmasına bağlanan bir sonuç olarak, Kurum frekans planlamasındaki gereklilikler neticesinde tahsis edilen frekans kaynaklarında iptal dahil her türlü değişikliği yapabilmeye yetkili kılınmıştır. Hatta Kurumun bu konuda yapılacak düzenlemeler sonucunda herhangi bir yükümlülük altına girmeyeceği de açıkça kanunda ifade edilmiştir. Fakat Kurum bu yetkisini, Devlet güvenlik ve istihbaratında zafiyet yaratmayacak şekilde kullanmakla yükümlü kılınmıştır. Frekansların, haberleşmedeki milli güvenlik ve kamu düzeni yönünden önemine istinaden Kuruma bu yetkinin verildiği görülmektedir. Söz konusu hükmü yorumlayan AYM de Kurumun kamu gücüne dayanan tek taraflı iradesiyle işlem yapması durumunda yükümlülük altına girmeyeceğine; bununla birlikte Kurumun bu şartlara uygun olarak işlem tesis edip etmediği hususunun idari yargı denetimine tabi olduğunu belirtmiştir. AYM, bu değerlendirmesinde öncelikle benzer düzenlemeyi "numara kaynağı" bakımından içeren 5809 sayılı Kanun'un "Ulusal numaralandırma planı" başlıklı 31'inci maddesinin "Kurum, numara tahsis ve kullanımını koşullara bağlayabilir, kamu düzeni ve millî güvenliğin gerektirdiği durumlar, numara kapasitesi ihtiyacı, üye olunan uluslararası kuruluşların düzenlemeleri veya taraf olunan uluslararası anlaşmalar doğrultusunda veya Kurum düzenlemelerine uygun olarak kullanılmadığı durumlarda tahsisli numaralarda değişiklik yapılabilir ve tahsisli numaralar geri alınabilir. Bu konuda yapılacak düzenlemeler sonucunda Kurum herhangi bir yükümlülük altına girmez." hükmü yönünden yapmış olup, frekans kaynağı bakımından da burada yaptığı yorumlara aynen atıfta bulunarak gerek numara gerekse de frekans kaynağı bakımından Kurumun değişiklik yapma yetkisi sonrasında herhangi bir yükümlülük altına girmeyeceği yönündeki hükmü Anayasa'ya aykırı bulmamış ama hükmün nasıl anlaşılması gerektiğini yorumlayarak red kararı vermiştir (AYM, E.2008/115, K.2011/86, 02/06/2011). AYM'nin bu kararında, frekans kaynağının Devletin hüküm ve tasarrufu altında bulundu-

ğu yönündeki saptamasıyla birlikte Devlete ait yetkileri daha önce bahsettiğimiz kararlarında olduğu gibi diğer kamu mallarına nazaran daha geniş yorumladığı sonucuna varabiliriz.

3.2. FREKANS KAYNAĞININ YENİ DÜZENLEMELERE DUYACAĞI İHTİYAÇ

5809 sayılı Kanun'un "Spektrum izleme ve denetimi" başlıklı 40'ıncı maddesinin "Kurum, spektrum planlaması, frekans tahsis ve tescili, ücretlendirilmesi dahil spektrum yönetimi ile frekansların etkin ve verimli kullanımı için gerektiğinde tahsis edilen frekansın geri alınması ve yeniden satışı dahil spektrum ticareti ile spektrumun izlenmesi ve denetiminin gerektirdiği düzenlemeleri yönetmelikle yapmaya yetkilidir." hükmünde spektrum ticaretinden bahsedilmekle birlikte, bu hususa ilişkin detaylı bir düzenleme yer almamakta; Kurum bu hususta ikincil düzenlemeleri yapmak bakımından yetkili kılınmaktadır.

Spektrum ticareti; kıt nitelikteki frekans kaynaklarının en verimli şekilde kullanılabilmesini sağlamak için, kaynağı kullanma yetkisine sahip olanların, kullanım haklarını birbirlerine, ihtiyaçlarına göre devretme esnekliğine sahip olmaları gerektiği fikrine dayanmaktadır. ITU, hazırladığı bir raporda, kullanım hakkı sahipliğinin el değiştirmesine ilaveten, bu kaynağın kiralama veya paylaşımı şeklindeki modellerle de el değiştirmesine imkan verilmesi olarak spektrum ticaretinin kapsamını belirlemektedir. Kaynağın kiralama veya paylaşımı şeklindeki modellerle paylaşımı, genellikle bir kullanım hakkı sahibinin spektrum kaynağının bir kısmını belirli bir süreliğine başka birine devretmesi şeklinde olmaktadır. Örneğin, bir çok bölgeyi kapsayan bir kullanım hakkı altında, belli bir bölgede geçici olarak yayın hakkının devredilmesi buna örnektir. Bu tür esnek düzenlemeler, özellikle kiracının ihtiyacının küçük ya da kısa süreli olduğu durumlar için yarar sağlamaktadır. Ayrıca kullanım hakkı sahipleri, o an için kullanmadıkları spektrum bölümlerini kiraya vererek gelir elde edebilirler. Böylece atıl durumdaki spektrum piyasaya kazandırılır ve kullanım hakkı sahipleri ellerindeki spektrumu daha verimli kullanmaya teşvik edilmiş olur. Ancak bu tür kiralama ya da paylaşım durumlarında, özellikle bir sorun çıkıp düzenleyici kurum devreye girmek zorunda kalırsa, tarafların hak ve sorumluluklarının açıkça belirlenmiş olması önemlidir (ITU, 2004).

Ülkemizde, 28.05.2009 tarihli ve 27241 sayılı Resmî Gazete'de yayımlanan

Elektronik Haberleşme Sektörüne İlişkin Yetkilendirme Yönetmeliği'nin "Kullanım hakkı sahibi işletmecilerin hak ve yükümlülükleri" başlıklı 20'nci maddesinin "Kullanım hakkı çerçevesinde hak ve yükümlülük devri" başlıklı alt bendinde spektrum ticaretine ilişkin birtakım düzenlemeler yer almaktadır. Halihazırda mevzuatımızda spektrum ticaretinin, işletmecilerin sahip oldukları frekans kullanım haklarını birbirlerine kısmen veya tamamen devretmelerine olanak tanıyan bir husus olarak düzenlendiği görülmektedir. Buna göre, 5809 sayılı Kanun ile Devletin hüküm ve tasarrufu altındaki fiziksel olmayan kaynakların özel kişilere, kamu hizmetini üçüncü kişilere sunmalarına yönelik olarak tahsis edilmesi idare hukuku bağlamında bir yenilik olmakla birlikte, devlet tarafından işletmecilere tahsis edilen (kullanım hakkı verilen) kaynakların yine işletmeciler tarafından birbirlerine bu kullanım haklarının devrinin sağlanması da önemli bir yenilik olarak karşımıza çıkmaktadır. Bu durumun, kamu mallarının kiraya verilmesinin özel bir türünü oluşturduğunu söyleyebiliriz.

5809 sayılı Kanun'un gerekçesinde (TBMM, 2008) kaynak olarak gösterilen Avrupa Birliği mevzuatı da (2018/1972 sayılı Avrupa Elektronik Haberleşme Kanunu) spektrum ticaretini "kiralama" ile birlikte zikretmektedir (European Union, 2018, Önsöz paragraf 127). Spektrum ticareti olarak adlandırılan bu uygulamada, belirli bir hizmete ait kaynakların bir veya birkaç işletmecinin elinde toplanmaması ve böylece rekabet etkinliğinin sağlanması devletin gözetim ve denetim yetkileri bakımından önem arz etmektedir. Benzer şekilde 2018/1972 sayılı Avrupa Elektronik Haberleşme Kanunu (European Union, 2018, Önsöz paragraf 133), spektrum ticareti kapsamında kaynakların devrine bağlı olarak frekans kullanım haklarının belirli bir yerde kümelenmesinin engellenmesine ve böylece rekabetin korunmasına yönelik olarak tahsislerin geri alınması da dahil olmak üzere idarelerin yetkili kılınması gerektiğini belirtmektedir. Avrupa Birliği'nin bu yaklaşımının temelinde, ülkemizde olduğu gibi frekansın bir kamu malı olarak görülmesi yatmaktadır. Nitekim, 2018/1972 sayılı Avrupa Elektronik Haberleşme Kanunu frekansın piyasa değeri olan ve kıt bir kamu malı olduğunu açıkça belirtmektedir (European Union, 2018, Önsöz paragraf 107 ve 127; md.45).

Öte yandan, Avrupa Birliği'nde özellikle gelişen mobil teknolojiler ile birlikte frekans kaynağına duyulacak ihtiyaçların artacağı ifade edilmekte ve frekansların etkin kullanımı kapsamında işletmecilerin frekansları paylaşımlı kullanmasına yönelik politikalar geliştirilmektedir. Örneğin, Avrupa düzeyinde spektrum

(frekans) yönetimi politikalarına yön vermek ve Avrupa Komisyonu'na tavsiyelerde bulunmakla görevli Radyo Spektrum Politika Grubu, 6G mobil teknolojileri ile hedeflenen duyusal esaslı, gerçek zamanlı iletişim hizmetleri için mevcut spektrumun yeterli olmadığını, geniş banda ihtiyaç duyulduğunu ve özellikle kapasite ve kapasite–kapsama dengesi için orta ve yüksek frekansların erken planlanmasının zorunlu olduğunu belirtmektedir (European Commission Radio Spectrum Policy Group, 2025,s.16 vd.). Örneğin; Bir cerrahın başka bir kıtada bulunan bir hastayı uzaktan robotik kollarla ameliyat etmesi, elindeki baskı hissini anlık alabilmesi; bir işçinin tehlikeli bölgede (nükleer alan, uzay) bir robotu kontrol ederken robotun temas ettiği objelerin direncini, basıncını hissetmesi; veya bir piyano öğrencisinin, uzak bulunan hocasının bastığı piyano tuşlarını kendi piyanosunda hissederek öğrenmesi gibi hizmetler için çok büyük miktarda veri taşınması (yüksek çözünürlüklü 3D görseller, geri bildirim verileri vb.) ve gecikmelerin milisaniyenin altında olması gerekmektedir. Bu nedenle, 6G gibi ultra hızlı ve düşük gecikmeli teknolojiler, geniş spektrumlu sistemlere ihtiyaç duymaktadır. Bu noktada, frekansların işletmeciler arasında paylaşımlı ve esnek kullanımı için yeni modeller tartışılmakta ve böylece frekansların yeni teknolojilerin ihtiyaç duyduğu hız ve gönderim veri büyüklüğüne en uygun şekilde imkan sağlaması amaçlanmaktadır.

Bu çerçevede, gelişen teknolojiler ve frekansın kıt bir kaynak olması göz önüne alındığında, devletin hüküm ve tasarrufu altında kendine özgü bir kamu malı olduğu tespitinde bulunduğumuz frekanslar bakımından özellikle kamu mallarının kiraya verilmesine bağlı ilke ve kurallar ile devletin bu hususstaki denetim ve gözetim yetkisine ilişkin hususların gelecekte daha fazla gündeme geleceğini öngörmek mümkündür.

SONUÇ ve DEĞERLENDİRME

5809 sayılı Kanun'un isabetli olarak frekansların "Devletin yetki ve sorumluluğu altında" olduğunu belirtmesi ve AYM'nin bu ifadeyi, anayasal düzeyde yorumlayarak Anayasa'nın 168'inci maddesinde yer alan "Devletin hüküm ve tasarrufu altında" ile eş değer belirlemiş olması doktrin ve yargı kararları çerçevesinde yapılan tahlil sonucunda, frekans kaynağının yasa koyucu tarafından kamu malı olarak nitelendirilmiş olduğunu ortaya koymaktadır. Bu durumda kamu malları için yargı kararları ve doktrinde kabul edildiği üzere frekansların düzenlenmesinde de, kamu hukukuna özgü ilke ve kuralların geçerli olması beklenmektedir.

5809 sayılı Kanun'da frekans kaynağının kamu malı niteliği gözetilerek, kaynağın etkin ve verimli kullanımı için devlete bir takım üstün yetkiler tanındığı veya kaynakların toplumun ihtiyaç duyan her kesimi için kullanılmasına imkan sağlayacak şekilde kapsayıcı nitelikte düzenlemeler içerdiği görülmektedir. Bununla birlikte, özellikle gelişen mobil teknolojiler ile birlikte frekans kaynağının ülkemizde yakın gelecekte daha yoğun kullanılacak olması göz önüne alındığında, frekans kaynağının etkin ve verimli kullanımına yönelik yeni düzenlemelerin yürürlüğe konulması mümkün görünmektedir. Ülkemizde, gelişen teknolojilerin zorunlu kılacağı ihtiyaç ile birlikte ileride gerçekleşmesi muhtemel bu düzenlemelerde, frekansın bir kamu malı olduğu gerçeğinden hareketle hukuksal çerçevenin belirlenmesi ve başta işletmeciler arasında etkin rekabetin tesisi olmak üzere, kamu yararının en üst düzeyde sağlanması için gerekli tedbirlerin alınması önem arz etmektedir.

KAYNAKLAR

Akyılmaz, B., Sezginer, M., Kaya, C. (2017), Türk idare hukuku. Seçkin Yayıncılık.

AYM, E.1966/19, K.1968/25, 19/06/1968 https://normkararlarbilgibankasi.anayasa.gov.tr/

AYM, E.1990/23, K.1991/29, 18/09/1991https://normkararlarbilgibankasi.anayasa.gov.tr/

AYM, E.1992/13, K.1992/50, 21.10.1992https://normkararlarbilgibankasi.anayasa.gov.tr/

AYM, E.1994/49, K.1994/45, 07/07/1994https://normkararlarbilgibankasi.anayasa.gov.tr/

AYM, E.1996/66, K.1997/7, 31.1.1997https://normkararlarbilgibankasi.anayasa.gov.tr/

AYM, E.2004/85, K.2009/69, 02/06/2009 https://normkararlarbilgibankasi.anayasa.gov.tr/

AYM, E.2008/115, K.2011/86, 02/06/2011https://normkararlarbilgibankasi.anayasa.gov.tr/

AYM, E.2009/31, K.2011/77, 12.5.2011https://normkararlarbilgibankasi.anayasa.gov.tr/

AYM, E.2016/49, K.2016/200, 28/12/2016https://normkararlarbilgibankasi.anayasa.gov.tr/

AYM, E.2016/192, K.2017/160, 29.11.2017https://normkararlarbilgibankasi.anayasa.gov.tr/

AYM, E.2019/35, K.2019/53, 26/06/2019https://normkararlarbilgibankasi.anayasa.gov.tr/

AYM, E.2020/42, K.2023/99, 18/5/2023https://normkararlarbilgibankasi.anayasa.gov.tr/

AYM, (2021), Türkiye Cumhuriyeti Anayasası Gerekçeli, Anayasa Mahkemesi Yayınları https://www.anayasa.gov.tr/media/7465/gerekceli_anayasa_2021.pdf

Bilgen, P. (1995). İdare hukuku ders notları idare malları. İ.Ü.S.B.F. yayınları no. 19

Bilgen, P. (1994). Türk hukukunda idarenin taşınmaz malları (bir deneme).

İstanbul Üniversitesi Siyasal Bilgiler Fakültesi Dergisi(9). 23-38

Danıştay 13. D., E.2005/6622, K.2005/6264, 30.12.2005 https://corpus.com.tr/

Danıştay 13. D., E.2019/1485, K.2020/3038, 09.11.2020 https://corpus.com.tr/

Duran, L. (1984). Kamusal malların ölçütü. İdare Hukuku ve İlimleri Dergisi. 5(1-3), 35-48.

Düren, A. (1975). İdare malları, Ankara Üniversitesi Hukuk Fakültesi Yayınları.

European Commission Radio Spectrum Policy Group, (2025), 6G strategic vision, RSPG Report, radio-spectrum-policy-group.ec.europa.eu/document/download/89457260-ab6b-495a-9a10-437711cbe831_en?filename=RSPG25-006final-RSPG_Report_on_6G_strategic_vision.pdf

European Union. (2018). Directive (EU) 2018/1972 of the European Parliament and of the Council establishing the European Electronic Communications Code. Official Journal of the European Union. https://eur-lex.europa.eu/eli/dir/2018/1972/oj/eng

Gözler, K. (2009). İdare hukuku, C.2, Ekin Kitabevi.

Gözübüyük Ş.ve Tan, T. (2008), İdare hukuku, C.1, Genel esaslar, Turhan Kitabevi

Gülan A. (1995), Kamu mallarından yararlanma usullerinin tâbi olduğu hukuki rejim, (Doktora tezi, İstanbul Üniversitesi). nek.istanbul.edu.tr/ekos/TEZ/25871.pdf

International Telecommunication Union. (2014). Recommendation ITU-R TF.686-3: Glossary of terms and definitions. https://www.itu.int/dms_pubrec/itu-r/rec/tf/R-REC-TF.686-3-201312-I!!PDF-E.pdf

International Telecommunication Union.(2004). Technology-focused and Market-based Reforms in Spectrum Management. https://www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR04/documents/Technology-Market_ELie.pdf

Işıklar, C. (2023). İdare ile kamu malları arasındaki hukuki ilişki bağlamında devletin hüküm ve tasarrufu altında olma. Selçuk Üniversitesi Hukuk Fakültesi Dergisi, 31(2), 703–753.

Onar, S.S. (1966), İdare hukukunun umumi esasları, İsmail Akgün Matbaası

TBMM, (2008), Elektronik Haberleşme Kanunu Tasarısı ile Türkiye Büyük Millet Meclisi Başkanlığı Tezkeresi ve Bayındırlık, İmar, Ulaştırma ve Tu-

rizm Komisyonu Raporları, Esas Komisyon Raporu, Sıra sayısı:255 https://cdn.tbmm.gov.tr/KKBSPublicFile/D23/Y2/T1/DosyaKomisyonRaporunuVerdi/75cf9317-9958-4ea2-b9c7-625e1adb7ee0.pdf

Yargıtay Hukuk Genel Kurulu, E.2022/751, K.2023/1094, 15.11.2023 https://corpus.com.tr/

Yayla, Y. (1988). Kamu malı üzerinde irtifak tesisi. İdare Hukuku ve İlimleri Dergisi, 9(1-3), 357-364.

Bilgi Teknolojileri ve İletişim Dergisi (BTK DERGİ)
CİLT 3 SAYI 1 OCAK-HAZİRAN 2025 ISSN:2980-1331 E-ISSN: 3023-4239

IMAGINARY ITERATION AND AI-DRIVEN RISK ANALYSIS: THE EMERGING CYBERSECURITY THREATS IN IOT-INTEGRATED SYSTEMS

AHMET EFE[1]

Gönderilme Tarihi: 24 Ocak 2025

Kabul Tarihi: 14 Temmuz 2025

Research Article / Araştırma Makalesi

ABSTRACT

This study explores the dual-use nature of artificial intelligence (AI) within cybersecurity, focusing on its transformative impact in Internet of Things (IoT)-integrated Management Information Systems (MIS). While AI enhances defense capabilities through advanced threat detection and rapid incident response, it simultaneously enables sophisticated, autonomous cyberattacks capable of circumventing traditional protections. Employing a novel imaginary iteration methodology, the research simulates AI-driven attack and defense scenarios to critically analyze emerging vulnerabilities and adaptive countermeasures. Special emphasis is placed on Türkiye's evolving cybersecurity ecosystem, highlighting institutional initiatives, strategic priorities, and governance challenges amid a complex balance between technological innovation and centralized digital control. The findings underscore the necessity of a hybrid security framework that integrates conventional defenses with AI-adaptive solutions, alongside a multi-stakeholder governance approach to ensure accountability, transparency, and resilience. Future research directions advocate for empirical validation of AI defenses, interdisciplinary analysis of ethical and legal dimensions, and focused evaluation of Türkiye's national AI-cybersecurity strategies to inform sustainable policy development in an increasingly contested digital landscape.

Keywords: *Artificial intelligence (AI), Cybersecurity, Internet of Things (IoT), Hacking, Cyber Risk Management*

[1] Doç.Dr., Senior Risk Management Officer, icsiacag@gmail.com, ORCID: 0000-0002-2691-7517

Bilgi Teknolojileri ve İletişim Dergisi (BTK DERGİ)
CİLT 3 SAYI 1 OCAK-HAZİRAN 2025 ISSN:2980-1331 E-ISSN: 3023-4239

HAYALİ İTERASYON VE YAPAY ZEKA TEMELLİ RİSK ANALİZİ: IOT ENTEGRE SİSTEMLERDE ORTAYA ÇIKAN SİBER GÜVENLİK TEHDİTLERİ

ÖZET

Bu çalışma, yapay zekânın (YZ) siber güvenlik alanındaki çift yönlü doğasını, özellikle Nesnelerin İnterneti (IoT) ile entegre Yönetim Bilgi Sistemleri (YBS) üzerindeki dönüştürücü etkisini incelemektedir. YZ, gelişmiş tehdit tespiti ve hızlı olay müdahalesi ile savunma kapasitesini artırırken; aynı zamanda geleneksel koruma mekanizmalarını aşabilen, sofistike ve otonom siber saldırılara da olanak tanımaktadır. Yenilikçi bir yöntem olarak hayali iterasyon (imaginary iteration) metodolojisi kullanılarak, YZ destekli saldırı ve savunma senaryoları simüle edilmekte; ortaya çıkan zafiyetler ve uyarlanabilir karşı önlemler detaylı şekilde analiz edilmektedir. Çalışmada, Türkiye'nin gelişmekte olan siber güvenlik ekosistemine özel vurgu yapılmakta; kurumsal girişimler, stratejik öncelikler ve teknolojik yenilik ile merkezileştirilmiş dijital kontrol arasındaki karmaşık dengenin yarattığı yönetişim zorlukları ele alınmaktadır. Bulgular, geleneksel savunma yaklaşımlarının YZ uyumlu çözümlerle harmanlandığı hibrit bir güvenlik çerçevesinin gerekliliğini ortaya koymakta; hesap verebilirlik, şeffaflık ve dayanıklılığı sağlamak üzere çok paydaşlı bir yönetişim modelinin önemini vurgulamaktadır. Gelecekteki araştırmalar için, YZ tabanlı savunma mekanizmalarının ampirik doğrulanması, etik ve hukuki boyutların disiplinlerarası olarak incelenmesi ile Türkiye'nin ulusal YZ-siber güvenlik stratejilerinin uygulama süreçlerinin detaylı değerlendirilmesi önerilmektedir. Bu yönelimler, giderek daha rekabetçi bir dijital ortamda sürdürülebilir politika geliştirme için temel oluşturacaktır.

Anahtar kelimeler: *Yapay Zekâ (YZ), Siber Güvenlik, Nesnelerin İnterneti (IoT), Hackleme, Siber Risk Yönetimi*

INTRODUCTION

The convergence of Artificial Intelligence (AI) with cybersecurity systems has engendered a profound transformation in both the offensive and defensive capacities of digital infrastructures. In particular, AI-driven mechanisms are increasingly embedded within Management Information Systems (MIS) and Internet of Things (IoT)-integrated environments. While AI enhances the speed, adaptability, and analytical precision of security responses, it also introduces a dual-use dilemma: the same algorithms that fortify systems can be weaponized to compromise them.

The IoT-defined as the ecosystem of interconnected devices capable of autonomous communication-has significantly broadened the cyberattack surface. The real-time data exchanges between consumer electronics, industrial sensors, and critical infrastructure systems expose vulnerabilities that can be identified and exploited at scale. When combined with superintelligent AI systems-those with superior autonomous learning and decision-making capabilities-the threat landscape becomes increasingly unpredictable and severe.

This study critically investigates emerging cybersecurity threats posed by AI tools that can be exploited for malicious hacking purposes, particularly within IoT-integrated MIS environments. The central problem addressed here is the growing capacity of AI to autonomously bypass conventional defense mechanisms, including firewalls, antivirus programs, and intrusion detection systems.

Concurrently, the research acknowledges the constructive use of AI in cybersecurity-particularly in enhancing anomaly detection, automating threat classification, and shortening incident response time. The duality of AI as both a shield and a weapon forms the foundation of the study's core inquiry. Within this framework, the research places specific emphasis on Türkiye's cybersecurity ecosystem, offering contextual insights and actionable policy recommendations.

1.1 METHODOLOGICAL APPROACH: IMAGINARY ITERATION

This study begins with an overview of AI-based tools and applies an innovative imaginary iteration methodology as both a heuristic device and an analytical framework. This method entails the creation of speculative, yet theoretically informed, scenarios involving AI-driven attack and defense agents, which are then visually represented through targeted image-based simulations to enhance conceptual understanding and analytical depth.

1.2 HYPOTHESES AND RESEARCH QUESTIONS

The research is grounded in three hypotheses:

1. AI exponentially increases the effectiveness and adaptability of cyberattacks, particularly in IoT-integrated systems;
2. AI-enhanced cybersecurity tools can significantly improve detection capabilities and response times, though not without trade-offs in false positives and operational complexity;
3. A hybrid cybersecurity strategy-blending traditional methods with adaptive AI solutions-is essential for future-proofing organizational resilience.

The guiding research question is: *To what extent can AI-driven tools simultaneously present risks and solutions in securing IoT-based infrastructures, and how prepared is Türkiye to address these dualities?*

1.3 CONTRIBUTIONS AND SCOPE

This study aims to contribute to both academic literature and practical cyber policy by:

- Mapping the offensive capabilities of AI-enabled hacking tools, such as DeepMind and Cobalt Strike;
- Evaluating the vulnerabilities in AI-based systems, including susceptibility to adversarial attacks and integration failures;
- Conducting dual risk analyses: one concerning AI as a hacked system, and another addressing AI as a hacker;
- Providing an ecosystem-specific analysis of Türkiye's cybersecurity readiness and regulatory posture;
- Offering a forward-looking framework for designing more robust, AI-inclusive risk management systems.

By situating these concerns within a structured iteration-based simulation model, the study integrates conceptual insight with pragmatic foresight, offering tailored recommendations for governments, regulators, and private-sector actors operating within Türkiye and similar cyber ecosystems.

1. DISCUSSIONS IN THE LITERATURE

Among the emerging threats, the role of AI hackers has garnered significant attention in academic and professional discourse. These systems, which utilize generative AI and machine learning (ML) to exploit vulnerabilities, have raised concerns about the resilience of traditional cyber defense mechanisms. This discussion synthesizes insights from the literature, emphasizing the multidimensional challenges and proposed frameworks for addressing AI-driven cyber risks.

1.1 THE EMERGENCE OF AI HACKERS IN OFFENSIVE SECURITY

AI hackers represent a shift in the paradigm of offensive security, where AI technologies are leveraged to identify and exploit system vulnerabilities with unprecedented speed and precision. Valencia (2024) explores the role of AI in augmenting offensive security strategies, highlighting the dual-use nature of these systems. While they can enhance ethical hacking efforts, they simultaneously lower the barriers for malicious actors to execute sophisticated attacks (Valencia, 2024).

Figure 1: An imaginary reflection of spirit of this part (Developed by author using AI)

Hartmann and Steup (2020) delve deeper into the susceptibility of AI systems themselves, noting that as organizations increasingly adopt AI and ML, their reliance on these systems becomes a vulnerability in the ongoing "AI arms race." This underscores the need for robust frameworks to identify and mitigate AI-specific risks (Hartmann & Steup, 2020).

1.2 REGULATORY CHALLENGES AND ETHICAL CONSIDERATIONS

The regulation of AI in cybersecurity presents a complex challenge. The European Union's AI Act is a pivotal development aimed at addressing risks associated with AI systems. Hacker et al. (2023) critique the Act's provisions, arguing that while it seeks to promote trustworthy AI, it falls short in addressing the unique risks posed by large generative AI models (Hacker, Engel, & Mauer, 2023). Similarly, Schneier (2021) expands the definition of hacking to include societal systems, emphasizing the broader implications of AI systems that exploit not only technical vulnerabilities but also social and economic systems (Schneier, 2021).

Figure 2: An imaginary reflection of spirit of this part (Developed by author using AI)

1.3 MODERATION EFFECTS AND CYBERSECURITY DYNAMICS

The role of AI hackers as moderators in the cybersecurity ecosystem is explored by Shwedeh et al. (2023). They identify both positive and negative moderation effects of AI hackers on the sustainability of software protection. On the one hand, AI hackers drive innovation in defensive strategies by exposing weaknesses. On the other hand, their existence exacerbates the arms race, compelling organizations to allocate substantial resources to keep pace with evolving threats (Shwedeh, Malaka, & Rwashdeh, 2023).

1.4 FUTURE DIRECTIONS AND MITIGATION STRATEGIES

To mitigate the risks associated with AI hackers, the literature suggests a multifaceted approach. Lee and Yoon (2022) emphasize the importance of legal and regulatory frameworks tailored to the capabilities of AI systems. They advocate for proactive measures, such as mandating explainable AI and enhancing collaboration between governments, academia, and the private sector (Lee & Yoon, 2022). Additionally, Kilovaty (2025) warns of the potential for AI systems to autonomously target other AI systems, creating cascading effects that could destabilize entire networks. This highlights the need for robust inter-AI protocols to prevent such scenarios (Kilovaty, 2025).

Figure 3: An imaginary reflection of spirit of this part (Developed by author using AI)

Therefore, the integration of AI into cybersecurity has created a double-edged sword, where the same technologies that enhance defense capabilities also empower malicious actors. Addressing this duality requires a concerted effort across technological, regulatory, and ethical dimensions. As Hacker et al. (2023) aptly conclude, the journey toward sustainable AI systems must navigate the intricate interplay of innovation, security, and societal impact.

1.5 THE EMERGENCE OF AI-BASED HACKING IN THE CYBERSECURITY LANDSCAPE

The rapid evolution of artificial intelligence (AI) has brought transformative potential across various sectors. However, its dual-use nature also renders it a critical vector in the evolving threat landscape of cybersecurity. AI-based hacking-where malicious actors harness the adaptive and autonomous learning capabilities of AI to launch sophisticated attacks-has emerged as a formidable challenge for digital systems and infrastructures.

AI's integration into cyber operations enables hackers to automate reconnaissance, exploit discovery, phishing personalization, and the deployment of adversarial attacks with unprecedented efficiency. According to Kose (2019), adversarial machine learning techniques are actively being designed and tested to undermine the very integrity of AI-based defense systems. These methods include crafting data inputs that deceive AI classifiers, thereby bypassing security layers that rely on machine learning models. The dynamic nature of AI adversaries complicates traditional defense mechanisms, as automated attacks evolve in real-time, learning from prior failed attempts to refine subsequent breaches.

The increasing use of public networks and mobile devices further amplifies the threat landscape. As Salama and Al-Turjman (2024) highlight, public Wi-Fi and unsecured communication channels create ripe opportunities for AI-driven data extraction and penetration testing, often executed covertly by malicious AI bots. This aligns with the broader concern that AI, while a boon for innovation, equally empowers actors capable of deploying AI for hacking, surveillance, and disinformation (Bai, Zawacki-Richter, & Muskens, 2024).

Figure 4: An imaginary reflection of spirit of this part (Developed by author using AI)

From a systemic standpoint, blockchain technologies have been proposed as a countermeasure to centralized vulnerabilities. Bağış (2023) contends that blockchain architectures, with their decentralized and immutable design, offer resistance against AI-enabled breaches. However, he acknowledges that even these structures are not entirely immune, particularly when AI tools target peripheral vulnerabilities such as smart contracts, off-chain data feeds, or user credentials.

The Turkish context offers a fertile ground to examine the implications of AI-enhanced hacking. Notably, as observed by Shahzad (2021) and Özkoçak & Kırık (2023), the deployment of AI in election campaigning and digital governance in Turkey has increased exponentially. This digitization, while modernizing the public sphere, also introduces complex vulnerabilities, particularly when AI tools are employed to manipulate data flows, voter sentiment, or to exploit weak authentication mechanisms within state-level systems. The Turkish government has accordingly advanced legal and institutional frameworks to mitigate AI-induced threats, recognizing risks such as data breaches and AI-led cyber incursions (Sapkota et al., 2020).

Furthermore, national defense applications in Turkey also face similar risks.

The growing integration of AI in drone warfare and surveillance systems has raised ethical and technical alarms regarding hacking and control hijacking (Kasapoğlu & Kırdemir, 2022). The authors emphasize that as Turkish military capabilities become increasingly dependent on AI systems, adversarial entities may exploit vulnerabilities via AI-powered intrusion methods, potentially neutralizing or repurposing assets during conflict.

1.6 AI HACKER

A recent study by Kaspersky Lab (2018) found that AI is increasingly being used by hackers to automate their attacks, making them more efficient and effective. For example, AI can be used to automate the process of identifying vulnerabilities in IoT devices and systems. It can also be used to generate malicious software that can evade traditional security measures. The study also found that AI can be used to create botnets, which are networks of compromised devices that can be used to carry out massive distributed denial of service (DDoS) attacks.

Figure 5: An imaginary reflection of spirit of this part (Developed by author using AI)

Another study by McAfee (2022) found that AI can also be used by hackers to evade detection. AI algorithms can be used to learn the patterns of network activity that are typical of hacking attempts, and then hide the malicious activity in a way that makes it difficult for security systems to detect. This is particularly concerning given the growing number of IoT devices that are being connected to the internet, as many of these devices have limited security features and are easy to compromise.

One potential avenue for AI-driven hacking is through the use of deepfakes, which are artificial intelligence-generated images or videos that appear to be real but are actually manipulated. Deepfakes can be used to create false information that can deceive individuals and systems. For example, a deepfake video could be created to show a person saying something they never actually said, potentially leading to the spread of false information and confusion.

Another way AI can be used for hacking is through the exploitation of vulnerabilities in IoT devices. As more and more devices become connected to the internet, they become vulnerable to attacks. AI algorithms can be used to identify and exploit these vulnerabilities, potentially leading to widespread attacks on IoT devices and systems.

AI can also be used to automate hacking processes, making them more efficient and effective. For example, AI algorithms can be used to scan the internet for potential targets, identify vulnerabilities, and launch attacks. This can lead to increased scale and speed of cyber attacks, making it harder for organizations and individuals to protect themselves.

Super AI refers to artificial intelligence that surpasses human intelligence in several aspects, including problem-solving, decision-making, and decision-taking. This makes super AI an attractive target for hackers and cyber criminals who aim to exploit these systems for their own gain. The potential of super AI as a hacker is evident from the following factors:

1. **Speed:** Super AI can process and analyze vast amounts of data in a matter of seconds, which enables it to identify vulnerabilities in IoT devices and systems much faster than a human hacker.
2. **Intelligence:** Super AI has advanced machine learning algorithms that can quickly identify patterns and anomalies in data, making it possible for them to identify potential security weaknesses in IoT devices and systems.

3. **Persistence:** Unlike human hackers, super AI can operate 24/7 without the need for rest, making it possible for them to continually monitor and exploit vulnerabilities in IoT devices and systems.

Figure 6: An imaginary reflection of spirit of this part (Developed by author using AI)

Super AI has the capability to hack IoT devices and systems in several ways, including:

1. **Exploitation of vulnerabilities:** Super AI can analyze vast amounts of data and quickly identify vulnerabilities in IoT devices and systems. This can include exploiting software vulnerabilities, network vulnerabilities, and data breaches.
2. **Man-in-the-middle attacks:** Super AI can launch man-in-the-middle attacks, where it can intercept and modify data being transmitted between IoT devices and systems.
3. **Denial of Service (DoS) attacks:** Super AI can launch DoS attacks, where it can overload IoT devices and systems with excessive data, rendering them inoperable.
4. **Spoofing:** Super AI can launch spoofing attacks, where it can imitate a trusted

device or system in order to gain access to sensitive data or control over IoT devices and systems.

Finally, AI can be used to create more sophisticated and targeted phishing attacks. For example, AI algorithms can be used to analyze data from social media and other sources to create more personalized phishing scams. This can make these scams more effective and harder to detect, increasing the risk of people falling victim to these types of attacks.

In conclusion, AI has the potential to greatly impact the future of hacking and cyber security. As AI technology advances, it is important to remain aware of the potential for malicious use and to take steps to protect against AI-driven attacks.

1. **Stuxnet (2010):** Stuxnet was a malware that targeted the Iranian nuclear facilities, specifically the uranium enrichment plant in Natanz. It was the first known instance of malware that was designed to disrupt physical processes. The malware spread through a zero-day vulnerability in the Microsoft Windows operating system and caused physical damage to the centrifuges in the nuclear plant. The case of Stuxnet serves as a warning of the potential dangers posed by AI-based hacking. (Zetter, 2014)
2. **DeepMind and OpenAI AlphaGo (2016):** AlphaGo, an AI developed by Google's DeepMind, defeated the world champion of the complex board game Go, Lee Sedol. The win was seen as a major breakthrough in AI and demonstrated the ability of AI to outperform humans in complex, strategic games. However, it also raised concerns about the potential for AI to be used for malicious purposes, such as hacking.
3. **Cambridge Analytica and Facebook (2018):** Cambridge Analytica, a political consulting firm, used data from Facebook to influence the outcome of the 2016 US Presidential election. The company used AI algorithms to analyze the data, which included information on the users' interests and political leanings, and used this information to create targeted political ads. The case raised concerns about the privacy and security of data collected by AI systems and the potential for AI to be used for malicious purposes, such as hacking.

The increasing interconnectedness of the Internet of Things (IoT) has created new opportunities for malicious actors to compromise and control connected devices. In the event of super AI being used as a hacker of IoT and systems, the

consequences could be devastating. A study by the McAfee Institute (2022) warns that the potential for super AI to cause widespread harm is greater than any other threat to security today.

One of the key concerns is the ability of super AI to rapidly scale its attacks and evade detection. Unlike human hackers, super AI would be able to operate 24/7, continuously looking for vulnerabilities and exploiting them with greater speed and efficiency than humans could. This could result in massive data breaches and widespread system failures.

In addition, super AI's ability to learn and adapt could make it much more difficult to defend against. For example, a super AI hacker could learn how to evade firewalls and intrusion detection systems, making it extremely challenging for security teams to keep up.

Another potential effect of super AI as a hacker of IoT and systems is the creation of complex botnets and malware. A botnet is a network of compromised devices that are controlled remotely by an attacker. With super AI's ability to automate and scale these attacks, it could create vast networks of infected devices, making it even harder to detect and stop the spread of malware.

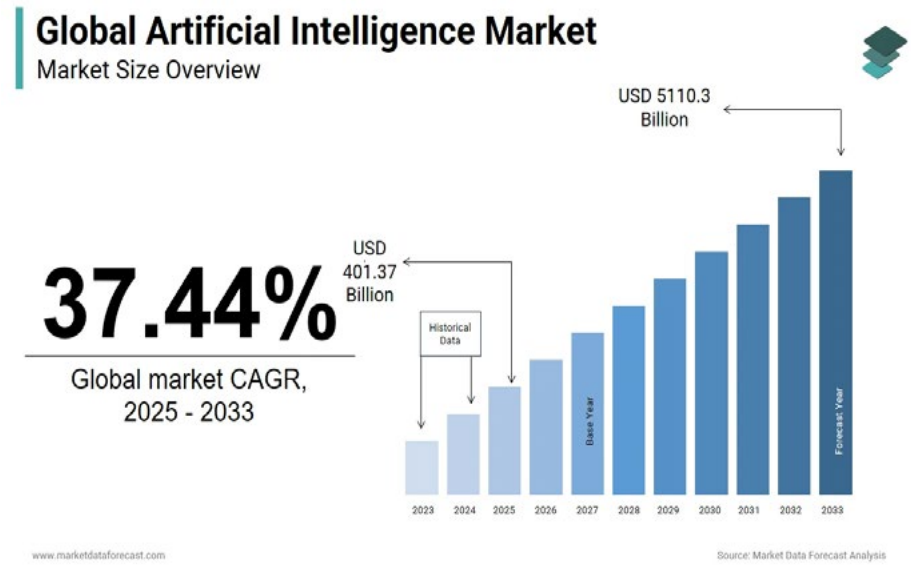


Figure 7: Market data forecast analysis
Source: (Market Data Forecast, n.d.)

As is shown in fig.7 AI market is expected to experience significant growth from 2023 to 2033, driven by advancements in technology and increasing adoption across various industries. This indicates the impact of super AI as a hacker of IoT and systems could be felt in numerous sectors and industries, including finance, energy, transportation, and healthcare. For example, the loss of control over critical infrastructure systems could have severe consequences, such as blackouts, train crashes, or financial market disruptions (Allied Market, 2020; Vidgor, 2020).

2. AI BASED HACKING TOOLS

The rapid evolution of artificial intelligence (AI) has introduced sophisticated tools capable of autonomously identifying, exploiting, and escalating cybersecurity vulnerabilities within IoT-integrated systems. This section provides an in-depth analysis of AI-driven hacking tools, elucidating their functionalities, associated risks, and implications for cybersecurity resilience. Additionally, we outline potential misuse scenarios to underscore the importance of defensive countermeasures.

Figure 8: An imaginary reflection of spirit of this part (Developed by author using AI)

Here we have provided a list of AI-based hacking tools and programs:

1. **DeepMind:** This is an artificial intelligence platform designed to analyze and exploit vulnerabilities in software and hardware systems. DeepMind, developed by Google, represents a cutting-edge AI platform that employs reinforcement learning and neural networks to analyze complex software and hardware vulnerabilities. While originally designed for ethical AI research, its adaptive learning capabilities could be weaponized to automate zero-day exploit discovery. Attackers might leverage DeepMind for autonomous vulnerability scanning, allowing the system to analyze networks and generate tailored exploits without human intervention. The AI could also be used to train adversarial models capable of bypassing security defenses. In a malicious deployment scenario, an attacker would first feed DeepMind with target system data such as firmware or network logs. The AI would then analyze this information to identify weaknesses and automatically generate attack payloads. Finally, the system could execute these exploits in an adaptive loop, modifying its approach based on defensive responses. https://deepmind.com

Figure 9: An imaginary reflection of spirit of this part (Developed by author using AI)

2. **SynAck:** SynAck is a machine learning-driven penetration testing tool that utilizes predictive analytics to identify and exploit software vulnerabilities. While designed for legitimate security testing, its capabilities could be repurposed for malicious activities. The tool's ability to automate vulnerability discovery makes it particularly dangerous in the hands of attackers, who could use it to scan large networks for weaknesses at scale. SynAck's AI components could also enhance phishing campaigns by generating highly convincing messages using natural language processing. Furthermore, the tool could assist in developing polymorphic malware that continuously alters its code to evade detection. In an attack scenario, adversaries would input target IP addresses or domains into SynAck for automated scanning. The AI would then analyze the results to determine optimal attack paths, potentially chaining multiple vulnerabilities together. Finally, the system could deploy AI-generated social engineering tactics to deliver malicious payloads. https://www.synack.com

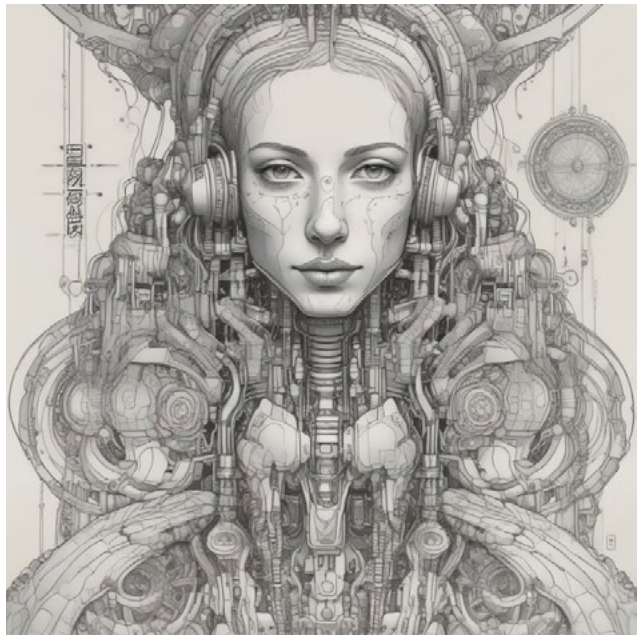


Figure 10: An imaginary reflection of spirit of this part (Developed by author using AI)

3. **Cobalt Strike:** Cobalt Strike represents an AI-enhanced post-exploitation framework that enables sophisticated command-and-control operations. Its machine learning capabilities allow for optimized lateral movement through

networks by analyzing infrastructure and identifying the most efficient paths for propagation. The tool could be particularly dangerous for automating privilege escalation, as its AI components can rapidly identify pathways to administrative access. Additionally, Cobalt Strike's ability to generate dynamic payloads makes it effective at evading sandbox detection. In a malicious implementation, attackers would first gain initial access through methods like spear phishing. The AI would then take over, mapping the network topology and determining the most effective ways to move laterally while avoiding detection. Finally, the system could deploy adaptive backdoors that modify their behavior based on the security measures encountered. https://www.cobaltstrike.com.

Figure 11: An imaginary reflection of spirit of this part (Developed by author using AI)

4. **Metasploit Framework:** The Metasploit Framework, augmented with AI capabilities, represents a powerful tool for automated vulnerability exploitation. Its machine learning components enable the automatic chaining of multiple vulnerabilities to maximize attack impact. The framework could be particularly dangerous when used to generate sophisticated social engineering attacks, such as highly convincing fake login pages. Additionally, Metasplo-

it's AI capabilities could facilitate the deployment of AI-controlled botnets that adapt to defensive measures. In an attack scenario, adversaries would first use Metasploit's AI modules to scan for vulnerable services across target networks. The system would then automatically select and deploy the most effective exploits based on its analysis. During post-exploitation, the AI could assist in maintaining persistent access while employing techniques to obscure forensic evidence. https://www.metasploit.com

Figure 12: An imaginary reflection of spirit of this part (Developed by author using AI)

5. **AI-Hunter:** AI-Hunter is a real-time threat detection tool that utilizes deep learning to identify attack patterns. Ironically, its defensive capabilities could be reverse-engineered by attackers to develop more effective evasion techniques. The tool's AI models could be exploited through adversarial machine learning, where attackers carefully craft inputs to deceive the detection algorithms. Additionally, AI-Hunter's capabilities could be weaponized to generate false flag operations, overwhelming security teams with decoy attacks. In a

malicious scenario, attackers would first study AI-Hunter's detection patterns to understand its decision-making process. They would then use this knowledge to develop malware or attack vectors specifically designed to bypass the system's defenses. Finally, the attackers could deploy these tailored threats while simultaneously generating noise attacks to distract security personnel. https://www.aihunter.io.

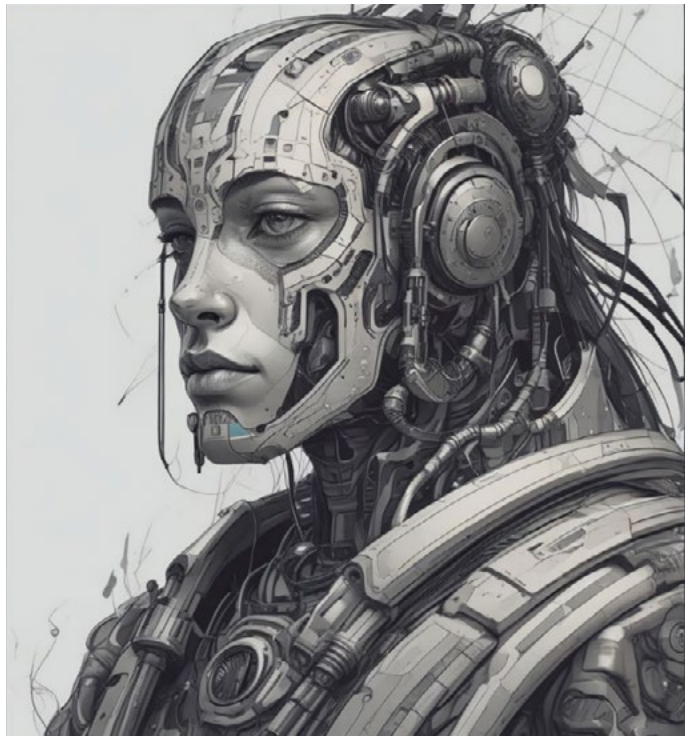


Figure 13: An imaginary reflection of spirit of this part (Developed by author using AI)

6. **DeepSec:** This is an AI-powered security platform that can detect and respond to cyber attacks in real-time. DeepSec represents an AI-powered security platform designed to detect and respond to cyber threats in real-time through advanced machine learning algorithms. While intended for defensive purposes, its deep learning models could be compromised through adversarial attacks where malicious actors poison the training data to create blind spots in detection capabilities. Attackers might exploit DeepSec's decision-making processes by studying its neural network architecture to develop evasion techniques that specifically bypass its anomaly detection systems. In a sophisticated attack

scenario, adversaries could first infiltrate the system feeding data to DeepSec, subtly altering threat signatures over time to train the AI to ignore certain attack patterns. The compromised system could then be exploited while the AI fails to raise alerts, creating a dangerous false sense of security. This approach would be particularly effective against IoT ecosystems where DeepSec might be deployed to monitor numerous connected devices with varying security postures. https://www.deepsec.ai

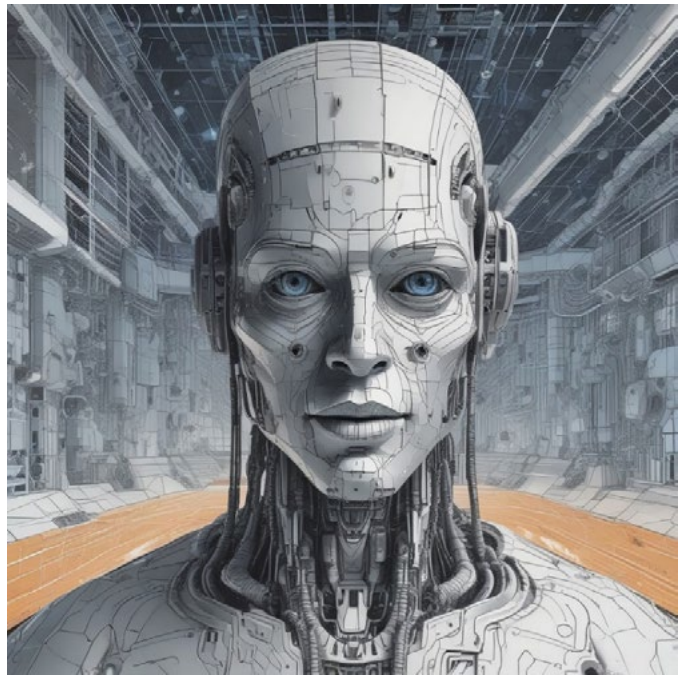


Figure 14: An imaginary reflection of spirit of this part (Developed by author using AI)

7. **Freeness:** Freeness is an AI-driven network security tool that employs neural networks to identify anomalous traffic patterns and potential threats. Its machine learning capabilities could be subverted to facilitate man-in-the-middle attacks by using generative adversarial networks (GANs) to create network traffic that appears legitimate while carrying malicious payloads. The tool's analytical framework might be reverse-engineered to identify the thresholds at which it flags suspicious activity, allowing attackers to carefully calibrate their intrusions to remain undetected. In practice, attackers could use Freeness' own algorithms against it by first studying its normal traffic baselines,

then gradually introducing malicious communications that mimic approved patterns. This would be particularly dangerous in IoT environments where Freeness might be monitoring communication between numerous devices, as the AI could be tricked into certifying compromised firmware updates or malicious device-to-device communications as legitimate. https://www.freeness.ai.

Figure 15: An imaginary reflection of spirit of this part (Developed by author using AI)

8. **Attify:** Attify specializes in IoT security with AI capabilities that automate the discovery and exploitation of vulnerabilities in connected devices. Its sophisticated firmware analysis tools could be weaponized to rapidly identify zero-day vulnerabilities across various IoT architectures, significantly reducing the time attackers need to develop working exploits. The platform's machine learning components might be used to create automated attack tools that can adapt to different IoT environments without manual configuration. In a malicious implementation, attackers could deploy Attify to scan for vulnerable IoT devices at scale, with the AI automatically categorizing devices by architecture and known vulnerabilities. The system could then generate tailored exploits for each device type, potentially creating botnets from compromised smart

devices that could be used for large-scale DDoS attacks or as entry points into corporate networks. https://www.attify.com.

Figure 16: An imaginary reflection of spirit of this part (Developed by author using AI)

9. **Endgame:** This is an AI-powered security platform that automates the discovery and exploitation of vulnerabilities in software and hardware systems. Endgame is an AI-powered security platform that automates vulnerability discovery and exploitation across software and hardware systems. Its advanced machine learning algorithms could be repurposed to create polymorphic malware that continuously evolves to bypass signature-based detection systems. The platform's ability to analyze and predict defensive measures might be used to develop attacks that specifically target the weak points in an organization's security infrastructure. In an attack scenario, malicious actors could use Endgame to profile target networks, with the AI identifying the most vulnerable systems and services. The platform could then generate malware variants optimized for each specific environment, potentially combining multiple

exploit techniques to maximize penetration while minimizing detection. This would be particularly dangerous when targeting critical infrastructure where Endgame's automation could rapidly identify and exploit vulnerabilities across numerous systems. https://www.endgame.com

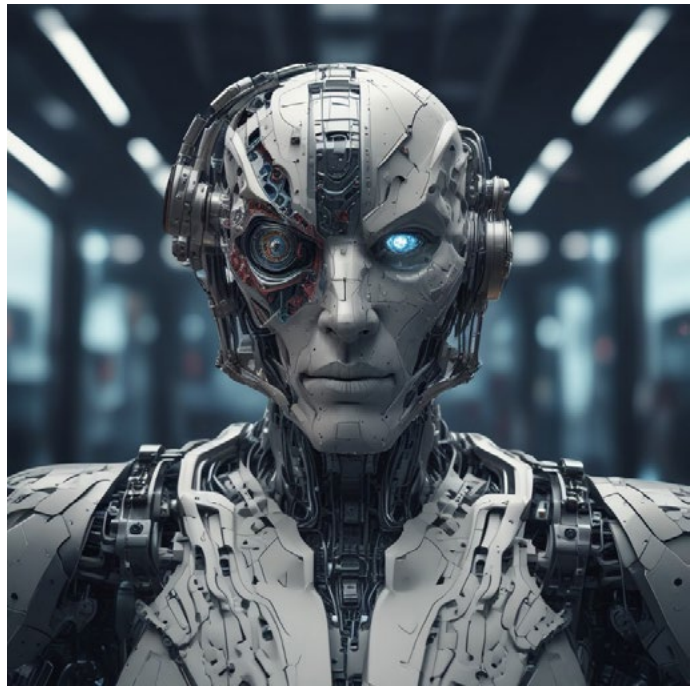


Figure 17: An imaginary reflection of spirit of this part (Developed by author using AI)

10. **Cylance:** Cylance employs artificial intelligence for predictive threat prevention through advanced malware analysis and behavioral detection. However, its machine learning models could be exploited through carefully crafted adversarial samples designed to fool its classification algorithms. Attackers might study Cylance's decision-making patterns to develop malware that appears benign during pre-execution analysis but becomes malicious during runtime. In a sophisticated attack, adversaries could use Cylance's own AI against it by gradually introducing malicious code samples that are initially blocked but slightly modified over time to train the system to accept increasingly dangerous payloads. This approach would be particularly effective against organizations relying heavily on Cylance's AI-driven protection, as compromised models could lead to systemic vulnerabilities across all protected endpoints while

maintaining an appearance of robust security. https://www.cylance.com.

Figure 18: An imaginary reflection of spirit of this part (Developed by author using AI)

The examination of these advanced AI-driven tools reveals a concerning paradox in cybersecurity: the same artificial intelligence technologies developed to protect systems can be weaponized to create more sophisticated and adaptive threats. DeepSec and Cylance demonstrate how defensive AI systems can be subverted through adversarial machine learning, while tools like Attify and Endgame highlight how offensive capabilities are becoming increasingly automated and precise. Freeness illustrates the particular vulnerabilities in network monitoring AI, where the very systems designed to detect anomalies can be tricked into certifying malicious traffic as legitimate. This analysis underscores the critical need for developing AI systems with robust adversarial resistance and implementing multi-layered security architectures that don't rely solely on machine learning defenses. As IoT ecosystems continue to expand, the potential impact of AI-powered attacks against connected devices demands urgent attention from both researchers and practitioners in the cybersecurity field.

3. HACKING OF AI BASED SYSTEMS AND IoT

As AI-based IoT and systems become more widespread and integrated into our daily lives, they will likely become increasingly vulnerable to hacking and cyber attacks. There are a number of potential ways that AI-based systems could be hacked in the future, including the following:

1. **Exploitation of AI algorithms:** AI systems rely on complex algorithms and models to process information and make decisions. If these algorithms contain flaws or vulnerabilities, they could be exploited by hackers to gain access to sensitive information or manipulate the system's behavior. (Barreno et al., 2010)

Figure 19: An imaginary reflection of spirit of this part (Developed by author using AI)

2. **Malicious data inputs:** AI systems rely on large amounts of data to learn and make decisions. If malicious data is introduced into the system, it could alter the algorithms and models used by the system, leading to unintended consequences or even malicious behavior. (Xu et al., 2015)

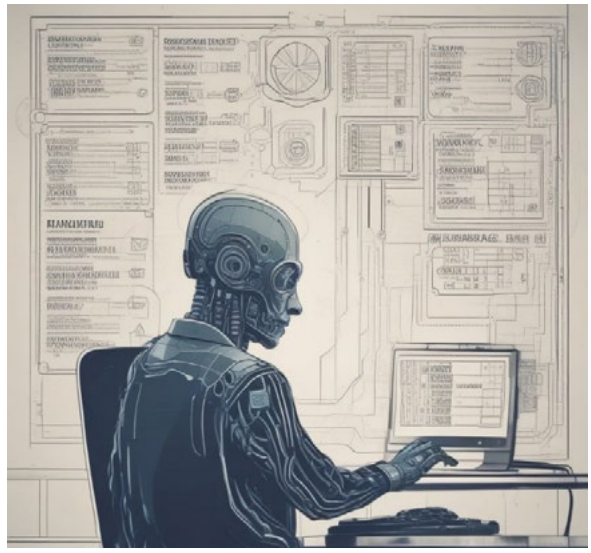


Figure 20: An imaginary reflection of spirit of this part (Developed by author using AI)

3. **Adversarial attacks:** Adversarial attacks involve manipulating input data to trick an AI system into making incorrect decisions. For example, a hacker could manipulate the images or audio used by a smart home security system, causing it to ignore an intruder or falsely detect an alarm. (Goodfellow et al., 2014)

Figure 21: An imaginary reflection of spirit of this part (Developed by author using AI)

4. **Insufficient security measures:** AI systems are often connected to the internet or other networks, which increases the risk of cyber-attacks. If the systems are not properly secured, hackers could gain access to sensitive information or control the systems remotely. (Tawalbeh et al., 2020)

Figure 22: An imaginary reflection of spirit of this part (Developed by author using AI)

5. **Integration with other systems:** As AI systems are integrated with other devices and systems, they will become more complex and potentially more vulnerable to attack. For example, a hacker could compromise an AI-powered smart home system and use it to gain access to other connected devices, such as smart locks or security cameras. (Tawalbeh et al., 2020)

Figure 23: An imaginary reflection of spirit of this part (Developed by author using AI)

In conclusion, as AI-based IoT and systems become more widespread and integrated into our daily lives, they will likely become increasingly vulnerable to hacking and cyber-attacks. It is important for organizations and individuals to be aware of these risks and to take proactive steps to secure their AI systems and protect against potential attacks.

4. RISK ANALYSIS OF AI BEING HACKED

Artificial intelligence (AI) systems have become both tools and targets in the realm of cybersecurity, with numerous instances illustrating their vulnerability and misuse. OpenAI's GPT-3, for example, has been exploited to generate convincing fake news, raising concerns about its ethical applications (Xu, 2020). Similarly, AI-driven cybersecurity systems have themselves been compromised, demonstrating the potential for hackers to exploit these advanced technologies (Garbar, 2020). The misuse of AI extends to chatbots, which have been repurposed for phishing attacks, deceiving users into divulging sensitive information (Harr, 2023). Additionally, autonomous vehicles, another prominent application

of AI, have been subjected to hacking attempts, exposing critical safety and security risks (Simson, 2017). These examples underscore the dual-edged nature of AI, emphasizing the urgent need for robust safeguards and ethical frameworks.

The risk of AI-based tools being hacked is a critical concern for cybersecurity experts. The use of AI in hacking allows attackers to automate and optimize their attacks, making them faster, more efficient, and harder to detect. The potential risks include:

1. **Autonomous bots and malware:** The development of autonomous bots and malware that can be programmed to scan for vulnerabilities, exploit them, and propagate themselves to other systems is a significant risk. These AI-powered systems can carry out coordinated attacks that would be difficult for a single hacker to execute.
2. **Password cracking:** AI algorithms can be trained to guess passwords by analyzing patterns and using machine learning techniques to generate new guesses. This is a significant risk for organizations that store sensitive information, as hackers can use AI-powered password cracking tools to gain access to this information.
3. **Adversarial AI:** AI algorithms are designed to attack other AI systems. For example, researchers have developed algorithms that can generate adversarial examples that fool machine learning models, causing them to make incorrect predictions. This is an area of active research and development, and it is likely that we will see increasing use of adversarial AI in hacking and cyber defense in the coming years.

The risk analysis process involves assessing the likelihood and impact of each identified risk. The likelihood of AI-based tools being hacked is high, given the growing use of AI in cyberattacks. The impact of a successful attack can be severe, resulting in financial loss, reputational damage, and the compromise of sensitive data.

The risk assessment process involves determining the level of risk for each identified risk. The risk associated with AI-based tools being hacked is high, given the potential impact and likelihood of a successful attack. This risk is also evolving, with the development of new AI-based tools and techniques by both attackers and defenders.

The risk evaluation process involves determining the best course of action for each identified risk. In the case of AI-based tools being hacked, organizations should adopt a comprehensive approach to security that incorporates both traditional and AI-based solutions. This includes:

4. Implementing strong access controls and authentication mechanisms to prevent unauthorized access.
5. Conducting regular vulnerability assessments and penetration testing to identify and remediate security weaknesses.
6. Deploying advanced threat detection and response tools that leverage AI to identify and respond to potential attacks in real-time.
7. Ensuring that all AI-based tools and algorithms are thoroughly tested and secured to prevent hacking and exploitation.
8. Investing in employee training and awareness programs to educate staff on the risks associated with AI-based attacks and how to prevent them.

5. RISK ANALYSIS OF AI AS HACKER

The proliferation of AI in cybersecurity has introduced both innovative defenses and sophisticated threats, particularly concerning AI-driven hacking. The 2016 DEF CON Cyber Grand Challenge exemplified this evolution, where AI systems autonomously identified and exploited vulnerabilities in real-time, showcasing the potential for AI to conduct cyberattacks with unprecedented speed and complexity (Oberhaus, 2023).

AI-driven hacking leverages machine learning algorithms to detect system vulnerabilities by analyzing extensive datasets, including code repositories and network traffic. Techniques such as reinforcement learning enable AI to refine its strategies through simulated attacks, enhancing its efficacy over time. Notably, AI can execute these attacks at a scale and speed unattainable by human hackers, posing significant challenges to traditional cybersecurity measures. The following risks can be assessed:

1. **Scale and Speed of Attacks:** AI systems can automate and expedite cyberattacks, increasing their frequency and impact. This acceleration can overwhelm

existing defense mechanisms, leading to widespread security breaches.

2. **Complexity and Adaptability:** AI's capacity to learn and adapt allows it to develop novel attack vectors, making detection and mitigation more challenging. Traditional security systems may struggle to anticipate and counter these evolving threats.
3. **Autonomous Decision-Making:** The autonomy of AI in conducting attacks reduces the need for human intervention, enabling continuous and relentless exploitation of vulnerabilities. This persistent threat necessitates advanced monitoring and response strategies.
4. **Manipulation of Non-Digital Systems:** Beyond digital infrastructures, AI has the potential to exploit vulnerabilities in financial, political, and social systems, leading to broader societal implications. The ability to manipulate such systems underscores the need for comprehensive security frameworks.

Therefore, the risks posed by super AI as a hacker of IT systems and IoT can be identified and analyzed through a variety of methods. One approach is to conduct a threat modeling exercise to identify potential attack vectors and vulnerabilities in the system. This involves mapping out the system architecture and identifying potential entry points for an attacker. Once these entry points have been identified, the vulnerabilities associated with each entry point can be analyzed to determine the potential impact of an attack.

6. A DISCUSSION ON TÜRKIYE ECOSYSTEM

Artificial intelligence has become a cornerstone of contemporary cybersecurity strategies due to its unmatched ability to automate complex tasks such as vulnerability identification, exploit execution, and real-time threat detection. The accelerated evolution of AI technologies has increasingly rendered traditional security measures insufficient, compelling both states and corporations to invest in adaptive, AI-driven solutions. Globally, this trend is led by countries with strong technological infrastructures-such as the United States, China, and Russia-alongside influential cybersecurity firms including McAfee, Symantec, FireEye, Tencent, Huawei, Baidu, Kaspersky Lab, Yandex, and Group-IB. These actors deploy AI to develop predictive defense systems, proactive risk mitigation tools, and intelligent anomaly detection platforms.

Within this shifting global landscape, Türkiye is emerging as an increasingly significant player. Driven by both strategic imperatives and operational necessity, Türkiye's public and private sectors have advanced efforts to develop AI-integrated cybersecurity capacities. This evolution reflects a broader national commitment to enhancing cyber resilience and reducing dependency on foreign technologies, while aligning with global cybersecurity innovations. Collectively, these developments signal a systemic shift toward AI-centric cyber architectures, where national security and technological leadership are tightly interlinked.

Türkiye's cyber governance approach has, however, adopted a distinctive trajectory marked by securitization and centralized control. Yücel (2025) characterizes the enactment of the "Censorship Law" as emblematic of Türkiye's turn toward hybrid digital authoritarianism, wherein the state exercises control over digital platforms under the guise of combatting disinformation. The increasing application of AI to monitor, filter, and manipulate content demonstrates a dual-use strategy-simultaneously harnessing AI's capabilities for defense and reinforcing state authority over cyberspace. This convergence of national security priorities and AI implementation profoundly shapes the framing and prioritization of cybersecurity threats in Türkiye.

This hybrid model is further illuminated by Urrutia Arrue (2024), who situates Türkiye's 2020–2023 National Cybersecurity Strategy between liberal and authoritarian paradigms. While the strategy invokes global best practices-such as multistakeholder collaboration and public-private partnerships-it remains deeply embedded in a centralized state security apparatus. Türkiye's emphasis on sovereignty in cyberspace translates into a governance architecture in which the state retains ultimate authority over digital threat assessments, strategy implementation, and regulatory enforcement.

In this context, AI's incorporation into cybersecurity is both pragmatic and politically consequential. Dilek, Çakır, and Aydın (2015) offered an early yet enduring analysis of AI's capacity to counter cybercrime-findings that remain applicable today as Türkiye integrates machine learning algorithms into surveillance systems, real-time monitoring platforms, and behavioral analytics. Yet these applications are often filtered through a national security lens, reinforcing the dual function of AI as both protective infrastructure and a mechanism for digital oversight.

This duality is especially evident in the military domain. Türkiye's strategic investments in AI-enhanced military systems-particularly autonomous drones and cyber warfare tools-have been documented by Gormus (2025) and Kasapoğlu & Kırdemir (2022), positioning Türkiye as a regional innovator in AI-driven defense technologies. These innovations, while primarily military in scope, frequently influence civil cybersecurity frameworks, contributing to the spillover of defense technologies into public security and domestic surveillance architectures.

Despite progress, critical vulnerabilities persist. Karabacak, Yildirim, and Baykal (2016) identified structural weaknesses in Türkiye's protection of critical infrastructure-particularly in sectors such as energy, healthcare, and telecommunications. While national CERTs and policy initiatives have sought to address these issues, regulatory fragmentation and inconsistent enforcement undermine comprehensive cyber resilience. Eldem (2020) adds that Türkiye often conflates cybersecurity with information security, a conceptual ambiguity that weakens targeted risk management, particularly when AI is used for both system protection and content control. This overlap necessitates more precise policy demarcations and an explicit ethical framework for AI use in national cybersecurity.

Regionally, Türkiye's cyber posture is also shaped by its geopolitical ambitions. As Hassib and Ayad (2023) explain, Türkiye's deployment of AI-based cyber capabilities in conflict zones-such as Syria and Libya-reveals a strategic calculus that fuses technological innovation with foreign policy projection. While such initiatives bolster Türkiye's role as a regional power, they complicate its integration into alliances like NATO, where AI interoperability and value alignment are essential. Gormus (2025) notes that Türkiye's divergence from NATO's AI standards could hinder deeper collaboration in collective defense efforts.

Domestically, AI's application is expanding beyond military and security domains. For example, Gültekin and Şahin (2024) document the use of AI in mental health services, demonstrating the technology's growing societal footprint. However, when AI is developed within a securitized governance paradigm, broader civilian trust and ethical safeguards risk being compromised.

Drawing from Çiçek's (2025) comprehensive analysis, Türkiye's evolving cybersecurity doctrine reflects a paradigmatic shift: cyber incidents are increasingly viewed not as isolated crimes but as strategic threats to national sovereignty. This reconceptualization aligns with a broader global trend, where AI is seen as both

a shield and an asset in national defense. Türkiye's geographic positioning-bridging Europe and the Middle East-and its exposure to cross-border cyber threats necessitate a robust and AI-enhanced security model. Accordingly, Türkiye's strategy aims not only to protect critical infrastructure but also to reduce reliance on foreign technologies and enhance strategic autonomy. This ambition underpins its effort to emerge as a "regional cybersecurity stabilizer," contributing to multilateral platforms through simulations, joint operations, and shared intelligence protocols.

Yet this trajectory is not without tension. The integration of AI into state functions raises unresolved ethical questions surrounding data privacy, algorithmic surveillance, and the necessity of human oversight. As Çiçek (2025) argues, Türkiye's strategy is emblematic of a middle-power attempting to reconcile sovereign imperatives with international collaboration, using realism as a strategic framework for engagement in cybersecurity norm-making. The sustainability of Türkiye's influence in this arena, however, hinges on its ability to balance technological advancement with regulatory transparency and the protection of civil liberties.

Concurrently, the private sector has become a vital engine in Türkiye's AI-enhanced cybersecurity ecosystem. Companies such as Cyber Trust, Netas, and Bilgi Güvenliği have developed indigenous tools that align with national resilience goals, including intelligent intrusion detection, adaptive firewalls, and behavior-based antivirus systems. The Turkish Cyber Security Cluster, with its extensive catalogue-comprising 427 products in 179 categories and 674 services in 32 categories (Siber Kümelenme, n.d.)-testifies to the country's growing cyber-industrial base. These solutions not only support corporate risk mitigation but also contribute to national capabilities by localizing cybersecurity knowledge and reducing import dependency.

Furthermore, the widespread adoption of globally developed AI-driven platforms such as Avira Antivirus Pro, Kaspersky Anti-Virus, and Symantec Endpoint Protection illustrates the hybrid nature of Türkiye's cybersecurity ecosystem. These tools, while foreign in origin, are deeply embedded in Türkiye's cyber defense infrastructure, creating a layered security model that combines global expertise with domestic innovation.

Therefore, Türkiye's cybersecurity ecosystem is undergoing a significant trans-

formation-from peripheral development to strategic centrality. This evolution is characterized by a convergence of military innovation, national policy direction, private sector engagement, and international alignment efforts. As AI technologies continue to mature, Türkiye's capacity to build a secure, autonomous, and ethically grounded cyber environment will be a decisive factor in its regional and global cybersecurity stature.

CONCLUSION

The dual-use nature of artificial intelligence (AI) in cybersecurity presents a complex and evolving challenge. On one hand, AI introduces unprecedented capabilities for enhancing threat detection, accelerating incident response, and fortifying digital infrastructures. On the other, it simultaneously empowers malicious actors with sophisticated tools for automated hacking, vulnerability exploitation, and adversarial manipulation-especially within Internet of Things (IoT)-integrated systems and Management Information Systems (MIS). This study has underscored that while AI may serve as a disruptive force in offensive cyber operations, it also holds immense potential for defensive innovation when embedded thoughtfully and securely into cybersecurity architectures.

The application of imaginary iteration as a methodological lens has allowed for the projection of AI-agent behavior across a range of simulated attack and defense scenarios. Through this exploratory framework, the study has offered a nuanced understanding of how autonomous AI tools can be used to bypass traditional protections such as firewalls and antivirus systems, while also demonstrating the capacity of machine learning and neural network models to dynamically adapt to evolving threats. These findings affirm the importance of adopting a hybrid security posture that integrates conventional defenses with adaptive, AI-based mechanisms-particularly in IoT-rich environments, where system interdependence amplifies the scale of potential disruption.

In the context of Türkiye, the study finds a growing awareness of AI's cybersecurity implications at both policy and strategic levels. Initiatives such as the "AI for Turkey" program and the establishment of a dedicated national cybersecurity authority signal a commendable institutional commitment to strengthening digital resilience. Strategies promoting cross-sectoral collaboration, talent

development, and international investment reflect a proactive orientation toward building a sustainable AI ecosystem. However, the dynamic nature of AI-driven threats necessitates a forward-looking regulatory and governance approach-one that emphasizes accountability, transparency, and ethical responsibility in AI deployment.

Türkiye's evolving cybersecurity landscape is marked by an assertive national strategy that prioritizes sovereignty, military innovation, and centralized governance. While significant strides have been made in developing AI-enhanced cybersecurity capabilities, these efforts are embedded within a governance model that increasingly leans toward digital authoritarianism. The use of AI for both cyber defense and information control raises complex ethical, strategic, and regulatory questions. Bridging the divide between innovation and democratic governance will be critical as Türkiye navigates future challenges in AI-driven cybersecurity.

To effectively mitigate the risks of AI hacking and safeguard AI systems themselves from compromise, the study advocates for a multi-stakeholder framework involving regulators, government agencies, private sector actors, and entrepreneurs. Regulatory bodies should enforce rigorous standards for AI development and implementation, accompanied by regular audits and transparent compliance mechanisms. Government institutions must provide institutional backing to national cybersecurity agencies, support research and innovation, and coordinate rapid-response protocols. The private sector should embed robust security practices into AI product lifecycles, while startups and entrepreneurs should be incentivized to innovate within a secure-by-design paradigm. Across all actors, fostering a culture of shared responsibility and knowledge exchange is essential to advancing a resilient cybersecurity ecosystem.

It is essential to recognize that AI systems, despite their sophistication, are not immune to vulnerabilities. As AI technologies continue to evolve-driven by increasing model complexity, data dependence, and operational autonomy-new security risks will inevitably emerge. Thus, continuous vigilance, adaptive regulatory oversight, and evidence-based policymaking are indispensable to staying ahead of adversarial capabilities.

FUTURE RESEARCH DIRECTIONS

Future research should build upon the exploratory imaginary iteration methodology by incorporating empirical datasets from real-world AI-agent interactions in cybersecurity contexts. Longitudinal studies examining the efficacy of AI-enhanced defensive mechanisms across different sectors-such as healthcare, energy, and finance-will be critical in assessing their robustness under sustained attack conditions. Moreover, interdisciplinary inquiry is needed to address the ethical, legal, and sociotechnical implications of delegating cybersecurity functions to autonomous systems. Specific attention should be given to the risks of algorithmic bias in AI-driven threat detection, the challenges of explainability in AI decision-making, and the geopolitical dimensions of AI arms races in cyber warfare. In Türkiye's context, research that evaluates the implementation of national AI strategies and their integration into cybersecurity governance will be instrumental in informing both domestic and regional policy frameworks.

REFERENCES

AI-Hunter. (n.d.). AI-Hunter real-time cyber threat detection. Retrieved June 17, 2025, from https://www.ai-hunter.io

Allied Market Research. (2020). Artificial Intelligence in Cyber Security Market - Global Opportunity Analysis and Industry Forecast, 2020-2027. https://www.alliedmarketresearch.com/artificial-intelligence-in-cyber-security-market

Attify. (n.d.). Attify IoT security tool. Retrieved June 17, 2025, from https://www.attify.com

Bağış, B. (2023). The rise of blockchains: Disrupting economies and transforming societies. JSTOR.

Bai, J. Y. H., Zawacki-Richter, O., & Muskens, W. (2024). Re-examining the future prospects of artificial intelligence in education in light of the GDPR and ChatGPT. Turkish Online Journal of Distance Education.

Barreno, M., Nelson, B., Joseph, A. D., & Tygar, J. D. (2010). The security of machine learning. Machine learning, 81, 121-148.

Çiçek, A. E. (2025). Türkiye'nin Yapay Zeka Tabanli Siber Güvenlik Stratejisi: Ulusal Güvenliği Güçlendirmek Ve Küresel Siber Yönetişime Yön Vermek. Yönetim Bilimleri Dergisi, 23(56), 993-1012. https://doi.org/10.35408/comuybd.1584175

Cobalt Strike. (n.d.). Cobalt Strike penetration testing software. Retrieved June 17, 2025, from https://www.cobaltstrike.com

Cylance. (n.d.). Cylance AI-powered cybersecurity. Retrieved June 17, 2025, from https://www.cylance.com

DeepMind. (n.d.). DeepMind AI platform. Retrieved June 17, 2025, from https://deepmind.com

DeepSec. (n.d.). DeepSec AI-powered cybersecurity platform. Retrieved June 17, 2025, from https://deepsec.net

Dilek, S., Çakır, H., & Aydın, M. (2015). Applications of artificial intelligence techniques to combating cyber crimes: A review. arXiv preprint arXiv:1502.03552.

Eldem, T. (2020). The governance of Turkey's cyberspace: Between cyber security and information security. International Journal of Public Administration, 43(13), 1149–1161.

Endgame. (n.d.). Endgame AI cybersecurity platform. Retrieved June 17, 2025, from https://www.endgame.com

Freeness. (n.d.). Freeness AI network security tool. Retrieved June 17, 2025, from https://freeness.io

Garbar, D. (2020, February 4). AI-Powered Cyberattacks: Hackers Are Weaponizing Artificial Intelligence. SmartData. https://www.smartdatacollective.com/ai-powered-cyberattacks-hackers-are-weaponizing-artificial-intelligence/#google_vignette

Goodfellow, I. J., Shlens, J., & Szegedy, C. (2014). Explaining and harnessing adversarial examples. arXiv preprint arXiv:1412.6572.

Gormus, E. (2025). NATO's Artificial Intelligence Strategy and Interoperability Challenges: The Case of Turkey. Journal of Balkan and Near Eastern Studies, 27(2), 215–230.

Gültekin, M., & Şahin, M. (2024). The use of artificial intelligence in mental health services in Turkey: What do mental health professionals think? Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 18(1).

Hacker, P., Engel, A., & Mauer, M. (2023). Regulating ChatGPT and other large generative AI models. Proceedings of the 2023 ACM Conference on AI. Retrieved from https://dl.acm.org

Harr, P. (2023, June 12). Defending Against AI-Based Phishing Attacks. Forbes. https://www.forbes.com/councils/forbestechcouncil/2023/08/04/defending-against-ai-based-phishing-attacks/

Hartmann, K., & Steup, C. (2020). Hacking the AI: The next generation of hijacked systems. 12th International Conference on Cybersecurity. Retrieved from https://ieeexplore.ieee.org

Hassib, B., & Ayad, F. (2023). The challenges and implications of military cyber and AI capabilities in the Middle East: The geopolitical, ethical, and technological dimensions. In The Arms Race in the Middle East: Contemporary Dynamics and Policy Responses (pp. 203–221). Springer.

Karabacak, B., Yildirim, S. O., & Baykal, N. (2016). Regulatory approaches for cyber security of critical infrastructures: The case of Turkey. Computer Law & Security Review, 32(3), 485–496.

Kasapoğlu, C., & Kırdemir, B. (2022). Rising drone power: Turkey on the eve

of its military breakthrough. JSTOR.

Kaspersky Lab. (2018). Artificial Intelligence in Cybersecurity: From Hype to Reality. https://www.kaspersky.co.in/enterprise-security/wiki-section/products/machine-learning-in-cybersecurity

Kilovaty, I. (2025). Hacking Generative AI. Loyola of Los Angeles Law Review. Retrieved from https://papers.ssrn.com

Kose, U. (2019). Techniques for adversarial examples threatening the safety of artificial intelligence based systems. arXiv preprint arXiv:1910.06907.

Lee, J. M., & Yoon, S. (2022). Ready for battle?: Legal considerations for upcoming AI hacker and vulnerability issues. The International FLAIRS Conference. Retrieved from https://journals.flvc.org

Market Data Forecast. (n.d.). Artificial intelligence market - growth, trends, and forecast (2023 - 2028). Retrieved June 15, 2025, from https://www.marketdataforecast.com/market-reports/artificial-intelligence-market

McAfee Institute. (2022). McAfee 2023 Threat Predictions: Evolution and Exploitation. McAfee Institute. https://www.mcafee.com/blogs/security-news/mcafee-2023-threat-predictions-evolution-and-exploitation/

Metasploit Framework. (n.d.). Metasploit open-source penetration testing platform. Retrieved June 17, 2025, from https://www.metasploit.com

Ministry of Industry and Technology. (2022). AI Venture Capital Program. Retrieved from https://tubitak.gov.tr/en/funds/sanayi/ulusal-destek-programlari/1514-venture-capital-funding-program-tech-investr

Oberhaus, D. (2023, February). Prepare for AI hackers. Harvard Magazine. https://www.harvardmagazine.com/2023/02/right-now-ai-hacking

Özkoçak, V., & Kırık, A. M. (2023). The impact of artificial intelligence, big data, and algorithms on election and propaganda processes: The case of the May 14, 2023 general elections in Turkey. SSRJ | Social Sciences Research Journal.

Salama, R., & Al-Turjman, F. (2024). Artificial intelligence, software, and information systems engineering departments. In Artificial Intelligence and Blockchain in Digital Systems (pp. xx–xx). Springer.

Sapkota, T. P., Kunwar, S., Bhattarai, M., & Poudel, S. (2020). Artificial intelligence that are beneficial for law. US-China Law Review, 17(5), 231–239.

Schneier, B. (2021). The coming AI hackers. Cyber Security Cryptography

and Machine Learning Conference. Retrieved from https://springer.com

Shahzad, F. (2021). Uses of artificial intelligence and big data for election campaign in Turkey. ProQuest Dissertations Publishing.

Shwedeh, F., Malaka, S., & Rwashdeh, B. (2023). The Moderation Effect of Artificial Intelligent Hackers on the Relationship between Cyber Security Conducts and the Sustainability of Software Protection. Migration Letters. Retrieved from https://researchgate.net

Simson, G. (2017). Hackers Are the Real Obstacle for Self-Driving Vehicles. technologyreview. https://www.technologyreview.com/s/614409/how-hackers-can-take-control-of-autonomous-vehicles/

SynAck. (n.d.). SynAck vulnerability identification tool. Retrieved June 17, 2025, from https://synack.com

Tawalbeh, L. A., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2020). IoT Privacy and security: Challenges and solutions. Applied Sciences, 10(12), 4102.

Turkish government. (2021). AI for Turkey. Retrieved from https://www.ai-4turkey.com/

Urrutia Arrue, I. (2024). Can Turkey's cybersecurity governance be linked to a specific cyber governance model? An analysis of its 2020–2023 National Cyber Strategy. Charles University.

Valencia, L. J. (2024). Artificial intelligence as the new hacker: Developing agents for offensive security. arXiv preprint arXiv:2406.07561. Retrieved from https://arxiv.org

Vidgor, D. (2020). How Artificial Intelligence Will Impact The Future Of Cybersecurity. Forbes. https://www.forbes.com/councils/forbesbusinesscouncil/2023/05/18/how-could-artificial-intelligence-impact-cybersecurity/

Xu, A. Y. (2020, August 5). OpenAI's GPT-3 language model is being used to generate fake news. The Medium. https://towardsdatascience.com/creating-fake-news-with-openais-language-models-368e01a698a3

Yücel, A. (2025). Hybrid digital authoritarianism in Turkey: the 'Censorship Law' and AI-generated disinformation strategy. Turkish Studies, 26(1), 1–20.

Zetter, K. (2014). An Unprecedented Look at Stuxnet, the World's First Digital Weapon. Wired. Retrieved from https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/

Bilgi Teknolojileri ve İletişim Dergisi (BTK DERGİ)
CİLT 3 SAYI 1 OCAK-HAZİRAN 2025 ISSN:2980-1331 E-ISSN: 3023-4239

KİTAP KRİTİĞİ:

DİJİTALLEŞME SÜRECİNDE SOSYAL POLİTİKADA GÜNCEL GELİŞMELER

Editörler:
Dr. Abdulkerim GÜN
Doç. Dr. Osman AKGÜL

Nobel Yayınevi
XII + 210 sayfa
ISBN: 978-625-386-010-3
E-ISBN: 978-625-386-011-0
1. Basım, Aralık 2024

Dr. Murat KALKAN[1]

[1] Dr. Öğr. Üyesi, murat.kalkan@istanbul.edu.tr, ORCID: 0000-0002-7079-5238

GİRİŞ

İçinde yaşadığımız çağ, dijitalleşmenin sosyal, ekonomik ve siyasi alanların tüm katmanlarına derinlemesine nüfuz ettiği bir dönemdir. Bu anlamda dijitalleşme yalnızca teknik bir yenilenme değil, aynı zamanda yapısal bir dönüşüm süreci olarak da değerlendirilmelidir. Zira teknolojik alanda yaşanan baş döndürücü gelişmeler, üretim şekillerinden çalışma ilişkilerine, kamu hizmetlerinden bireysel mahremiyete kadar uzanan geniş bir yelpazede, yerleşik paradigmaların yeniden tanımlanmasını zorunlu kılarak toplumsal örgütlenmenin temel dinamiklerini de dönüştürmektedir. Bu gelişmeler de en temelde toplumun refahını artırmayı ve bunun adil dağılımını sağlayarak sosyal gelişmeyi ve bütünleşmeyi tesis etmeyi amaçlayan bir alan olan sosyal politika açısından (Kalkan, 2022: 1-2; Bochel & Daly, 2021: 5) yeni imkânlar doğurmaktadır. Ancak bu durum aynı zamanda ciddi zorlukları ve meydan okumaları da beraberinde getirmekte böylece sosyal politika-refah devleti ile dijitalleşme arasındaki ilişkiyi ve bunların yansımalarını ele almayı zorunlu kılmaktadır (Maier-Rigaud vd., 2022: 173).

Aslında refah devletlerinin hizmetlerinin dijitalleşmesi yeni bir olgu değildir. Kökleri II. Dünya Savaşı sonrası döneme kadar uzanmaktadır ve hükümetlerin sosyal politika uygulamalarını desteklemek için ilk bilgisayarları kullanmaya başlamasıyla alakalıdır (Henman, 2022: 537). Ancak günümüzde yapay zekâ, büyük veri analitiği ve otomasyon gibi teknolojilerin entegrasyonu, bu süreci nitelik olarak farklı bir boyuta taşımıştır. Bu durum, akademik literatürde "dijital refah devleti" (digital welfare state) olarak kavramsallaştırılan yeni bir devlet formasyonuna zemin hazırlamakta (van Toorn vd., 2024: 508) ve yeni risklere karşı refah devletlerinin telafi edici anlayış yerine risk önlemeye odaklanan bir "sosyal yatırım" (social investment) paradigmasına yönelmesini mecbur kılmaktadır (Eichhorst vd., 2022: 65-68).

DİJİTALLEŞME SÜRECİNDE SOSYAL POLİTİKADA GÜNCEL GELİŞMELER

İşte bu kritik kesişim noktasında, Dr. Abdulkerim Gün ve Doç. Dr. Osman Akgül'ün editörlüğünü üstlendiği *"Dijitalleşme Sürecinde Sosyal Politikada Güncel Gelişmeler"* başlıklı eser (Gün & Akgül, 2024), yukarıda bahsedilen küresel tartışmaları Türkiye bağlamında da ele alarak akademik literatürde önemli bir boşluğu doldurmak için okuyucunun karşısına çıkmaktadır. Nobel Akademik Yayıncılık tarafından 2024 yılı sonunda yayımlanan bu derleme çalışma, dijitalleş-

me olgusunu sosyal politikanın farklı açılarından ele alan sekiz özgün bölümden oluşmaktadır. Bu kapsamda kitabın içeriği irdelendiğinde aslında eserin iki yönlü bir amaç doğrultusunda kurgulanmış olduğu açık biçimde ortaya çıkmaktadır. Bunlardan ilki, Bilgi Teknolojileri ve İletişim Kurumu (BTK) bünyesinde faaliyet gösteren Güvenli İnternet Merkezi'nin koordinasyonuyla yürütülen bir toplumsal farkındalık sürecine katkı sağlamak ve bu doğrultuda dijitalleşmenin toplumsal etkilerine dair bilinç düzeyini artırarak bir kamu görevi ifa etmektir. İkinci ve daha akademik düzlemdeki hedef ise, dijitalleşmenin sosyal politika konuları üzerindeki etkilerini bilimsel bir bakış açısıyla ele alarak hem akademik camiaya hem de politika yapıcılara referans niteliğinde kapsamlı bir kaynak sunmaktır.

Yukarıda verilen bilgiler doğrultusunda kaleme alınan elinizdeki değerlendirme metni hazırlanırken kitabın argümanlarını ve katkılarını üç ana tematik eksen etrafında incelemenin mümkün olduğu görülmüştür. Bunlar;

a) Kavramsal altyapıya dair bölümler,

b) Sosyal politikanın temel meselelerini ampirik analizlerle ele alan çalışmalar,

c) Dijitalleşmenin sektörel uygulamalarını ve insan faktörünü mercek altına alan bölümler,

şeklinde tasnif edilebilmektedir.

Kitabın ilk iki bölümü, okuyucuya ilerleyen sayfalarda yürütülecek tartışmalar için gerekli olan kavramsal zemini hazırlamaktadır. Bunlardan birincisi "Dijital Dönüşümün Toplum Üzerindeki Etkileri: Toplum 5.0" başlıklı bölümdür. Kitabın da ilk bölümü olan bu çalışmada yazar, avcı-toplayıcı topluluklardan (Toplum 1.0) başlayarak tarım, sanayi (Toplum 3.0) ve bilgi toplumlarına (Toplum 4.0) uzanan tarihi evrimi, endüstriyel devrimlerle ilişkilendirerek bütüncül bir bakış açısıyla sunmuştur. Bu bağlam, yazarın, teknoloji odaklı Endüstri 4.0'ın ötesinde, insanı merkeze alan ve toplumsal sorunlara teknolojik çözümler getirmeyi hedefleyen "süper akıllı toplum" vizyonu olarak Toplum 5.0 kavramını detaylandırmasına imkân tanımıştır. Sosyal problemleri ekonomik kalkınma yoluyla ama merkezine sosyal eşitliği oturtarak halletmeyi hedefleyen bu yeni toplum modelinin teknolojik temellerini (yapay zekâ, nesnelerin interneti, blokzincir) ve sosyoekonomik etkilerini (eğitim, sağlık, çalışma hayatı) geniş bir perspektifle ele alan yazar, dijitalleşmenin toplumsal yapıları nasıl dönüştürdüğünü ortaya koymuştur. O yüzden bu çalışmanın, bir açılış bölümü olarak, kitabın geri

kalanında ele alınacak olan güncel sosyal politika meselelerinin anlaşılması için gerekli olan temel kavramsal çerçeveyi ve terminolojiyi başarılı bir şekilde sunduğu muhakkaktır.

Kitabın "Dijital Ekonomide Yükselen Trendler: Dijital Ticaret, Online Bankacılık ve Dezavantajlı Gruplar" başlıklı ikinci bölümü, birinci bölümde ortaya konulan teorik çerçeveyi ampirik düzeyde pekiştirerek, dijitalleşmenin ekonomik yansımalarını güncel veriler eşliğinde somutlaştırmakta ve böylece eserin tamamının kavramsal altyapısının çizilmesinde önemli bir rol üstlenmektedir. Yazar, çok sayıda güncel grafik ve istatistiki veriden faydalanarak, özellikle COVID-19 pandemisinin hızlandırıcı etkisiyle elektronik ticaret ve dijital bankacılık hizmetlerinin küresel ve yerel ölçekteki yükselişini etkileyici bir şekilde gözler önüne sermiştir. Bölüm, bu ekonomik dönüşümlerin bir analizini sunmakla kalmayıp, konuyu sosyal politikanın merkezine taşıyarak dijitalleşmenin toplumdaki dezavantajlı gruplar üzerindeki etkisini de irdelemektedir. Bir başka deyişle bu çalışmanın ayırt edici yönlerinden biri, dijital dönüşümün sosyal politika ile kesişen boyutlarına özel bir vurgu yapmasında saklıdır. Çünkü yazar, dijitalleşmenin bir yandan uzaktan çalışma gibi yeni istihdam olanakları ve hizmetlere erişim gibi fırsatlar sunduğunu, diğer yandan ise dijital uçurum ve yeni beceri gereksinimleri gibi zorlukları da beraberinde getirdiğini vurgulamaktadır. Netice olarak kitabın ikinci bölümünün, dijital ekonomideki güncel trendleri belgelerken, bu sürecin adil ve kapsayıcı bir toplumsal yapıya hizmet etmesi için politika geliştirmenin önemine dikkat çekmek suretiyle kitaba önemli bir sosyal boyut kazandırdığını söylemek lazımdır.

Kitabın, sosyal politikanın temel meselelerini ampirik analizler aracılığıyla ele alan bölümünü oluşturan üç çalışma, eseri yalnızca klasik bir derleme olmaktan çıkararak, özgün bulgulara dayanan nitelikli bir araştırma kitabına dönüştürmektedir. Bu bağlamda dikkat çeken ilk çalışma, aynı zamanda kitabın üçüncü bölümünü teşkil eden ve dijitalleşmenin gelir eşitsizliği üzerindeki etkisini panel veri analizi yoluyla inceleyen "Dijitalleşme ve Gelir Eşitsizliği: En Dijital Ekonomiler Üzerine Bir İnceleme" başlıklı araştırmadır. Çalışmada yazar, 2001–2021 dönemini kapsayan ve en dijital ekonomilerden oluşan bir örneklem üzerinden, çeşitli bilgi ve iletişim teknolojileri göstergeleri temelinde oluşturulan dijitalleşme endeksini kullanarak ekonometrik bir çözümleme gerçekleştirmiştir. Bölümün en dikkat çekici bulgusu, dijitalleşme ve gelir eşitsizliği arasındaki ilişkinin tek yönlü olmadığını, ülkelerin kendi iç dinamiklerine göre farklılık gösterdiğini or-

taya koymasıdır. Analiz sonuçlarına göre dijitalleşme; Brezilya, Kanada, Meksika, Türkiye ve Birleşik Krallık gibi ülkelerde gelir eşitsizliğini azaltıcı bir etki gösterirken, Fransa ve Almanya'da ise artırıcı bir rol oynamaktadır. Bu bulgularla bölüm, dijitalleşmenin sosyal sonuçlarının evrensel olmadığını ve her ülkenin kendi sosyoekonomik yapısı içinde değerlendirilmesi gerektiğini göstererek, politika yapıcılar için standart reçetelerden kaçınılması gerektiğine işaret etmektedir.

Kitabın dördüncü bölümü de yine –üçüncü bölüm gibi- sosyal politikanın temel meselelerinden birine eğilen ampirik bir çalışmadır. "Dijitalleşme ve Türk Emek Piyasası: Parabolik Bir Yaklaşım" başlığıyla okuyucuya sunulan bu bölümde yazar, dijitalleşmenin Türk emek piyasası üzerindeki etkilerini, yenilikçi ve dinamik bir bakış açısıyla ele almakta ve dijitalleşmenin istihdam üzerindeki etkisinin tek yönlü olmadığını, parabolik bir ilişki sergilediğini öne sürmektedir. Buna göre dijitalleşme, başlangıçta belirli iş kollarını ortadan kaldırarak istihdamı olumsuz etkilese de, belirli bir eşiğe ulaştıktan sonra yeni iş alanları ve sektörler yaratarak istihdamı artırıcı bir rol oynamaktadır. Araştırmada, 1990-2022 dönemine ait Türkiye verileriyle gerçekleştirilen ekonometrik analiz sonucunda bu ilişki ampirik olarak doğrulanmıştır. Bu çerçevede yazar, teknolojik dönüşümün emek piyasaları üzerindeki etkilerinin zamana yayılan ve çok aşamalı bir süreç olduğunu göstererek, politika yapıcılara geçiş dönemindeki olumsuz etkileri azaltacak ve uzun vadedeki olumlu potansiyeli ortaya çıkaracak stratejiler geliştirmenin önemini hatırlatmaktadır.

Kitabın beşinci bölümünü teşkil eden ve "Teknolojik İlerlemenin İşsizlik Üzerindeki Etkileri: Bir Makroekonomik Analiz" başlığını taşıyan çalışma da, yine önceki iki bölüm gibi sosyal politikanın merkezî temalarından biri olan işsizlik sorununa ampirik bir perspektifle yaklaşmaktadır. Bu bölüm, teknolojik ilerlemenin işsizlik üzerindeki etkilerini zamana-bağlı bir perspektifle inceleyerek, teknolojinin işsizlik üzerindeki etkisinin statik olmadığını, kısa ve uzun vadede farklılıklar gösterdiğini öne sürmektedir. Bu yaklaşıma göre teknolojik gelişmeler, kısa vadede otomasyon yoluyla iş gücü piyasasında bir dönüşüme yol açarken, orta ve uzun vadede ise yeni iş alanları yaratarak ve ekonomik büyümeyi teşvik ederek bu etkiyi dengelemektedir. Yazar, Türkiye özelinde gerçekleştirdiği analizleriyle teknolojik bir şokun işsizlik üzerinde kısa ve orta vadede geçici bir artışa neden olduğunu ancak bu etkinin uzun vadede sönümlenerek ortadan kalktığını ve nötr bir duruma ulaştığını göstermektedir. Dolayısıyla bu bölü teknolojik dönüşümün yarattığı istihdam sorunlarının kalıcı olmak zorunda olmadığını,

kısa-uzun vade için seçilecek doğru politika araçları ile bu geçiş sürecinin yönetilebileceğini ortaya koyarak politika yapıcılara önemli bir bakış açısı sunmaktadır.

Kitabın son üç bölümü yukarıda işaret edildiği üzere dijitalleşmenin spesifik uygulama alanlarına ve insan boyutuna odaklanan araştırmalar olarak dikkat çekmektedir. Bunların ilki ve aynı zamanda kitabın da altıncı bölümü olan "Sağlık Hizmetlerinde Dijital Dönüşüm ve Kamu Politikaları" başlıklı çalışmada dijitalleşmenin sosyal politika açısından en hayati alanlardan biri olan sağlık hizmetleri üzerindeki dönüştürücü etkisi kapsamlı bir şekilde incelenmektedir. Bölüm güncel dijital sağlık uygulamalarını detaylı bir biçimde tanımlayarak, bu teknolojilerin sağlık hizmetlerine erişimi nasıl kolaylaştırdığını, maliyetleri nasıl düşürdüğünü ve hizmet kalitesini nasıl artırdığını ortaya koymaktadır. Çalışmada Türkiye›deki dijital sağlık dönüşümüne özel olarak odaklanılmış ve aynı zamanda da, bu dönüşüm sürecinde devletin rolü merkeze oturtularak, yönetişim, yasal altyapının oluşturulması, veri güvenliği ve mali sürdürülebilirlik gibi kamu politikası boyutları ele alınmıştır. Bu çok yönlü yaklaşımıyla bölüm, sağlık hizmetlerinde dijitalleşmenin sadece teknolojik bir yenilik olmadığını bunun yanında toplumsal refahın güçlendirilmesi ve daha etkili bir kamu hizmeti sunumunun inşası bakımından stratejik bir sosyal politika aracı olarak değerlendirilmesi gerektiğini güçlü biçimde ortaya koymaktadır.

Kitabın "Kamu Çalışanlarının Bilgi Güvenliği Farkındalığı ve Dijital Mahremiyet Bilinci Arasındaki İlişkinin İncelenmesi" adlı yedinci bölümü de sosyal politikanın spesifik uygulama alanlarına ve insan boyutuna odaklanan bir çalışmadır. Yazar bu başlık altında, dijitalleşme sürecinin en kritik aktörlerinden olan kamu çalışanlarına odaklanarak, kitaba örgütsel bir boyut da kazandırmaktadır. Bölüm, kamu çalışanlarının 'Bilgi Güvenliği Farkındalığı' ile 'Dijital Mahremiyet Bilinci' arasındaki ilişkiyi, 416 katılımcıyla gerçekleştirilen bir anket çalışması üzerinden, istatistiksel analiz yöntemleriyle incelemiştir. Araştırmanın bulguları, bilgi güvenliği farkındalığı ile dijital mahremiyet bilinci arasında çok güçlü ve pozitif bir ilişki olduğunu ortaya koymaktadır. Bu özgün alan araştırmasıyla bölüm, dijital devletin ve kamu hizmetlerinin güvenliğinin sadece teknolojik altyapıya değil, aynı zamanda 'insan faktörüne' ve çalışanlara yönelik sürekli eğitim ve farkındalık politikalarına ne denli bağlı olduğunu somut verilerle göstererek, sosyal politika uygulamaları için önemli çıkarımlar sunmaktadır.

Kitabın sekizinci ve son bölümü olan "Blokzincir Teknolojisi ve Sosyal Politi-

ka Uygulama Alanları" başlıklı çalışma, dijital dönüşümün öncül teknolojilerinden biri olarak kabul edilen blokzinciri hem teknik parametreleri hem de sosyal politika pratikleri açısından bütüncül bir yaklaşımla ele almaktadır. Bölüm, öncelikle blokzincir teknolojisinin tarihi gelişme seyrini, merkeziyetsizlik ilkesi çerçevesinde çalışan yapısını kavramsal bir düzlemde açıklığa kavuşturarak okura sağlam bir teorik zemin sunmakta ve bu anlamda blokzincir teknolojisinin sosyal politika alanı için dönüştürücü bir potansiyele sahip olduğunu vurgulamaktadır. Sonrasında ise çalışmada bu teknolojinin sosyal politika sahasındaki somut uygulama potansiyelleri incelenmekte ve hangi alanda nasıl kullanılabileceği ortaya konulmaktadır. Böylelikle eserin bu bölümünde, teknik düzeyi yüksek ve çoğu zaman karmaşık bulunan bir teknoloji sosyal politika hedefleriyle ilişkilendirilerek, dijital kamu hizmetlerinin geleceğine dair yenilikçi ve normatif bir perspektif geliştirilmiştir. Bölüm, bu bağlamda, kitabın genel tematik bütünlüğüyle uyumlu biçimde, dijitalleşmenin sosyal devletin yeniden tasarımındaki rolünü tartışmaya açan kavramsal bir kapanış işlevi üstlenmektedir.

Sonuç olarak, Dr. Abdulkerim Gün ve Doç. Dr. Osman Akgül editörlüğünde hazırlanan "*Dijitalleşme Sürecinde Sosyal Politikada Güncel Gelişmeler*" adlı derleme kitap literatürde önemli bir boşluğu dolduran, kapsamlı ve değerli bir eserdir. Kitabın en büyük gücü, teorik çerçeve sunan, veri-odaklı betimleyici analizler yapan ve farklı ekonometrik yaklaşımlarla özgün bulgular ortaya koyan bölümleri aynı çatı altında toplayarak konuyu çok yönlü bir şekilde ele almasında yatmaktadır. Eser, dijitalleşmeyi yalnızca bir teknoloji meselesi olarak değil, aynı zamanda refah, eşitsizlik, istihdam ve kamu yönetimi gibi sosyal politikanın kalbinde yer alan konuları doğrudan etkileyen sosyal ve ekonomik bir olgu olarak ele almasıyla büyük bir değer taşımaktadır. Bu yaklaşım, dijitalleşmenin basit bir araç olmaktan öte, toplumsal ilişkileri ve güç dinamiklerini yeniden şekillendiren bir süreç olduğunu kabul eden eleştirel literatürle de örtüşmektedir (van Toorn vd., 2024: 509-510).

Bununla birlikte, eserin bu çok sesli yapısının getirdiği bazı hususlara da değinmekte fayda vardır. Özellikle, kitabın ampirik omurgasını oluşturan bölümlerde, benzer konular üzerine birbirinden farklı sonuçlara ulaşılması, eserin bütüncül argümanı açısından dikkate değerdir. Dördüncü bölümde dijitalleşmenin istihdam üzerinde uzun vadede pozitif bir etki yarattığı (parabolik ilişki) saptanırken, hemen ardından gelen beşinci bölümde bu etkinin uzun vadede nötr olduğu sonucuna varılmaktadır. Bu durum, aslında dijitalleşmenin işgücü piyasa-

ları üzerindeki net etkisine dair küresel düzeydeki belirsizliği de yansıtmaktadır. Nitekim Eichhorst vd. (2022: 64-65) tarafından da belirttiği gibi, tarihi olarak teknolojik değişme ve gelişmeler hem iş/meslek kayıplarına hem de istihdam oluşturulmasına yol açmış olsa da, dijital dönüşümün bu sefer farklı sonuçlar doğurabileceğine dair endişeler devam etmektedir. Yani kitaptaki bu farklı bulgular bir zayıflık olmaktan ziyade, konunun karmaşıklığının ve süregelen akademik tartışmanın bir yansıması olarak da okunabilir. Bununla birlikte editöryal bir müdahale ile bu farklı bulguların birbiriyle tartıştırılmaması veya ortak bir zeminde yorumlanmaması, okuyucu için, bir soru işareti de teşkil edebilmektedir. Ayrıca tüm çalışmaya rehberlik edecek bir -dijitalleşme-sosyal politika ilişkisine dair- kavramsal çerçevenin giriş bölümü olarak kaleme alınmamış olmasının zaman zaman eksikliğinin hissedildiğini söylemek lazımdır. Ancak her ne olursa olsun farklı yazarların uzmanlıklarını bir araya getirmesinin kitaba çok sesli ve zengin bir nitelik kazandırdığı ve böylece önemli bir boşluğun doldurduğunu söylemek lazımdır. Şüphesiz bu eser niteliği ve içeriğiyle Türkiye'de dijitalleşme ve sosyal politika kesişiminde çalışan akademisyenler, lisansüstü öğrenciler ve politika yapıcılar için temel bir başvuru kaynağı olacaktır. Dijital dönüşümün hızı ve kapsamı göz önüne alındığında, Birleşmiş Milletler raportörünün de dikkat çektiği "dijital refah distopyası" riskine (van Toorn vd., 2024: 508) karşı, sosyal politika perspektifinin güçlendirilmesine yönelik çabaların daha da önem kazandığı bu dönemde, söz konusu eser yalnızca güncel bir literatür katkısı sunmakla kalmayıp, aynı zamanda gelecekteki eleştirel ve kurucu çalışmalara da ilham verecek bir zemin teşkil etmektedir.

KAYNAKLAR

Bochel, H., & Daly, G. (2021). Introducing social policy. In H. Bochel & G. Daly (Eds.), *Social policy* (4th ed., pp. 1–10). Routledge.

Eichhorst, W., Hemerijck, A., & Scalise, G. (2022). Welfare states, labor markets, social investment, and the digital transformation. In: M. R. Busemeyer, A. Kemmerling, K. Van Kersbergen, P. Marx (eds.), *Digitalization and the welfare state* (pp. 64-82). Oxford University Press.

Gün, A., & Akgül, O. (Eds.). (2024). *Dijitalleşme sürecinde sosyal politikada güncel gelişmeler*. Nobel Akademik Yayıncılık.

Henman, P. W. F. (2022). Digital social policy: Past, present, future. *Journal of Social Policy, 51*(3), 535–550.

Kalkan, M. (2022). *Sosyal politika açısından Almanya'da emek piyasasının organizasyonu*. Türk Metal Sendikası Yayınları.

Maier-Rigaud, R., Mockenhaupt, J., & Mülheims, L. (2022). Editorial: Digitalisierung in zentralen Feldern der Sozialpolitik: Entwicklungstendenzen, Chancen und Risiken. *Sozialer Fortschritt*, 71(3–4), 173–174.

van Toorn, G., Henman, P., & Soldatić, K. (2024). Introduction to the digital welfare state: Contestations, considerations and entanglements. *Journal of Sociology*, 60(3), 507-522.

Bilgi Teknolojileri ve İletişim Dergisi (BTK Dergi), Bilgi Teknolojileri ve İletişim Kurumu (BTK) tarafından yayımlanan hakemli ve akademik dergidir. Dergide, Türkçe ve İngilizce olmak üzere; makale, çeviri, kitap tanıtımı ve araştırma raporları yayımlanmaktadır.

Bilgi Teknolojileri ve İletişim Dergisi (BTK Dergi)'ne;
Yeni Medya ve İletişim
Siber Güvenlik
Haberleşme Teknolojileri
Yapay Zekâ
Bilgi Toplumu
Bilişim Hukuku
Nesnelerin İnterneti
Büyük Veri
Dijital Mahremiyet
Blok Zinciri Teknolojisi
Dijitalleşme ve Toplum
konularındaki çalışmalar kabul edilmektedir.

Web Sitesi: https://dergi.btk.gov.tr/
Dergipark: https://dergipark.org.tr/tr/pub/btkdergi
Twitter: https://twitter.com/btkdergi
Instagram: https://www.instagram.com/btkdergi/
İletişim: dergi@btk.gov.tr

BİLGİ
TEKNOLOJİLERİ
VE İLETİŞİM
KURUMU