KVKK
KİŞİSEL VERİLERİ KORUMA KURUMU

YAPAY ZEKÂ TEKNOLOJİLERİNE AKADEMİK BAKIŞ

KVKK
KİŞİSEL VERİLERİ KORUMA KURUMU

adalet

KVKK
KİŞİSEL VERİLERİ KORUMA KURUMU

Yapay Zekâ Teknolojilerine

AKADEMİK BAKIŞ

Bu çalışmada yer alan fikir ve görüşler Kurumumuz görüşünü yansıtmamakta olup yazarların görüşlerini yansıtmaktadır.

KVKK
KİŞİSEL VERİLERİ KORUMA KURUMU

Yapay Zekâ Teknolojilerine

AKADEMİK BAKIŞ

Kişisel Verileri Koruma Kurumunun akademik alanda konunun derinlemesine analizinin yapılmasına katkı sunması, akademinin konuya duyarlılığının artırılması ve yeni gelişmeler konusunda akademi ile irtibatlı olunmasını sağlamayı amaçlamaktadır.

Adres:
Nasuh Akar Mahallesi 1407. Sokak
No:4 Balgat Çankaya/ANKARA

ADALET YAYINEVİ
Ankara - 2025

Editör
Prof. Dr. Faruk BİLİR

Düzenleyen
Beste EKİN

KVKK Yayınları No
64

ISBN: 978-625-377-212-3

Mart, 2025

Tasarım & Mizanpaj

Adalet Yayınevi

Strazburg Caddesi No: 10/B Sıhhiye-Ankara
Tel: (0312) 231 17 00 Fax: (0312) 231 17 10
www.adalet.com.tr – www.adaletyayinevi.com

Basım Yeri

Dedemat Ambalaj Matbaacılık San. ve Dış Tic.Ltd.Şti.
Fidanlık Mah. Mithatpaşa Cd. 31/12 Çankaya/Ankara
Sertifika No: 70086

SUNUŞ

Teknolojinin insan hayatına kattığı yenilikler, geçmişte hayal bile edilemeyecek imkânları günümüzde gerçeğe dönüştürmektedir. Yapay zekâ, bu dönüşümün merkezinde yer alarak en karmaşık problemlere çözümler sunabilen, karar alma süreçlerini destekleyen ve hayatı kolaylaştıran bir teknoloji olarak öne çıkmaktadır. Ancak yapay zekânın gücünü, faydalı ve sürdürülebilir bir şekilde kullanabilmek için bu teknolojinin etik ve hukuki ilkeler çerçevesinde ele alınması önem taşımaktadır.

Yapay zekâya dair tartışmalar, aşırı iyimser beklentiler ile olumsuz gelecek senaryoları arasında sıkışıp kalmamalıdır. Bu alana gerçekçi bir perspektifle yaklaşmak ve yapay zekâyı insan odaklı bir anlayışla geliştirmek esastır. Yapay zekâ, bilinçli ve sorumlu bir şekilde kullanıldığı sürece insanlığın en büyük yardımcılarından biri olabilir. Ancak bu süreçte mahremiyet, şeffaflık ve hesap verebilirlik gibi temel etik ilkeler göz ardı edilmemelidir.

Teknoloji ile mahremiyet arasında sağlanacak dengeli bir ilişki, yalnızca bireylerin hak ve özgürlüklerinin korunmasını temin etmekle kalmayacak, aynı zamanda toplumun teknolojiye duyduğu güveni de pekiştirecektir. Bu bağlamda, yapay zekâ sistemlerinin insan merkezli bir yaklaşımla geliştirilmesi ve kullanılması büyük önem taşımaktadır. Ülkemizin 2021-2025 Ulusal Yapay Zekâ Stratejisi'nde de vurgulandığı üzere; yapay zekâ sistemleri kişisel verilerin korunmasına halel getirmeyecek bir şekilde geliştirilmelidir. Kişisel veriye dayalı olarak alınan kararların bireyler üzerindeki etkileri her zaman denetime açık ve izlenebilir olmalıdır. 2021 yılında Kurumumuz tarafından yayımlanan "Yapay Zekâ Alanında Kişisel Verilerin Korunmasına Dair Tavsiyeler" çalışmasında da kişisel veri işlemenin her aşamasında temel hak ve özgürlüklerin gözetilmesi, bireyler üzerinde meydana gelebilecek ayrımcılık riskinin veya diğer olumsuz etkilerin ve ön yargıların önlenmesi gerektiği ifade edilmiştir.

Bu bağlamda, güncel gelişmeler çerçevesinde kişisel verilerin korunmasına yönelik yeni yaklaşımlar geliştirilmesi gerekmektedir. Kişisel verilerin

korunmasının bireyler açısından taşıdığı önem ve yapay zekâ sistemlerinin ortaya çıkardığı yeni hukuki, teknik ve etik sorular, araştırmacıların ve akademisyenlerin bu alandaki çalışmalarını daha da kıymetli bir hale getirmektedir. Akademik araştırmalar ve bilimsel yayınlar, yapay zekâya ilişkin yasal düzenlemelerin daha iyi anlaşılmasına, uluslararası standartların değerlendirilmesine ve güncel gelişmelerin ele alınmasına önemli katkılar sunmaktadır. Aynı zamanda bu tür çalışmalar, veri koruma politikalarının sürdürülebilirliğini sağlama açısından da fayda sağlamaktadır. Hukuk ve bilişim disiplinlerinin kesişim noktasında yer alan kişisel verilerin korunması konusu, akademik alanda giderek artan bir ilgi görmekte, bu alandaki çalışmaların sayısı ve kapsamı sürekli genişlemektedir. Bu akademik üretim süreci, kişisel verilerin korunmasına yönelik farkındalığın artmasında ve daha sağlam bir veri koruma ekosistemi oluşturulmasını sağlamada etkili bir rol oynamaktadır.

Bu doğrultuda, Kurum olarak 2023 yılında yayımladığımız "Kişisel Verilerin Korunmasına Akademik Bakış" başlıklı derleme çalışması ile akademik çalışmalara katkı sunmayı amaçlamıştık. Şimdi ise bu çalışmanın devamı niteliğinde değerlendirilebilecek olan "Yapay Zekâ Teknolojilerine Akademik Bakış" isimli çalışmamızı siz kıymetli okuyucularla buluşturuyoruz.

"Yapay Zekâ ve Makine Öğrenmesine Giriş", "Yapay Zekâ ve Hukuk: Etik İlkeler, Hukuki Çerçeve ve Sorumluluk", "Yapay Zekâ Sistemlerinde Kişisel Verilerin İşlenmesi", "Yapay Zekânın Sektörel Uygulamaları" ile "Yapay Zekâda Yönetişim ve Metodoloji" olmak üzere beş bölümden ve bu bölümler altında toplamda on beş makaleden oluşan bu eserin yapay zekâ konusunda yapılan akademik çalışmalara katkı sağlayacağına inanıyorum.

Çalışmanın hazırlanmasında emeği geçen akademisyenlere ve Kurum personeline teşekkür ediyor, çalışmanın tüm ilgililere faydalı olmasını diliyorum.

Prof. Dr. Faruk BİLİR

Kişisel Verileri Koruma Kurumu Başkanı

MAKALELER VE YAZARLARI LİSTESİ

- **YAPAY ZEKÂ VE MAKİNE ÖĞRENMESİNE GİRİŞ**

  Doç. Dr. Tuncay ÖZCAN

  Dr. Öğr. Üyesi Ebru PEKEL ÖZMEN

- **YAPAY ZEKÂ TEKNOLOJİLERİNE ETİK YAKLAŞIM**

  Doç. Dr. Elif KÜZECİ

  Av. Zeynep ÖĞRETMEN KOTİL

- **KODLAR VE KANUNLAR: YAPAY ZEKÂNIN REGÜLASYON ROTASI VE AB YAPAY ZEKÂ TÜZÜĞÜ**

  Dr. Öğr. Üyesi Osman Gazi GÜÇLÜTÜRK

- **YAPAY ZEKÂNIN YOL AÇTIĞI ZARARLARDAN HUKUKİ SORUMLULUK**

  Doç. Dr. Hüseyin Can AKSOY

- **VERİ KORUMA HUKUKUNUN TEMEL PRENSİPLERİ VE YAPAY ZEKÂ UYGULAMALARI AÇISINDAN DEĞERLENDİRİLMESİ**

  Dr. Öğr. Üyesi Çiçek ERSOY

- **YAPAY ZEKÂ ALGORİTMALARIYLA PROFİLLEME VE KİŞİSEL VERİLERİN KORUNMASI**

  Prof. Dr. E. Eylem AKSOY RETORNAZ

- **YAPAY ZEKÂ VE TEMEL VERİ KORUMA YÖNTEMLERİ**

  Prof. Dr. Yücel SAYGIN

  Doç. Dr. Ali İNAN

  Dr. Öğr. Üyesi Mehmet Emre GÜRSOY

- **HASSAS GRUPLAR (ÇOCUKLAR, YAŞLILAR, ENGELLİ BİREYLER) İÇİN GELİŞTİRİLEN YAPAY ZEKÂ UYGULAMALARINDA DİKKAT EDİLMESİ GEREKEN ETMENLER**

  Prof. Dr. Hatice KÖSE

- **SAĞLIK ALANINDA YAPAY ZEKÂ VE KİŞİSEL VERİLER**

  Prof. Dr. Perihan Elif EKMEKCİ

- **İSTİHDAMDA YAPAY ZEKÂ**

  Dr. Öğr. Üyesi Başak OZAN ÖZPARLAK

- **ÖNERİ MODELLERİNİN KVKK İLE UYUMU**

  Prof. Dr. Şule GÜNDÜZ ÖĞÜDÜCÜ

  Öğr. Gör. Dr. Resul TUGAY

- **ULAŞIM SEKTÖRÜNDE YAPAY ZEKÂ**

  Doç. Dr. Nazım Kemal ÜRE

- **FİNANS SEKTÖRÜNDE YAPAY ZEKÂ KULLANIMI: KİŞİSEL VERİLERİN KORUNMASI ODAĞINDA BİR DEĞERLENDİRME**

  Doç. Dr. Pınar ÇAĞLAYAN AKSOY

- **EĞİTİMDE YAPAY ZEKÂ**

  Doç. Dr. Nursel YALÇIN

  Arş. Gör. Behiye CANBAZ

- **YAPAY ZEKÂDA YÖNETİŞİM VE METODOLOJİ**

  Hâkim İsmet YURTERİ

İÇİNDEKİLER

BİRİNCİ BÖLÜM
YAPAY ZEKÂ VE MAKİNE ÖĞRENMESİNE GİRİŞ

Doç. Dr. Tuncay ÖZCAN - Dr. Öğr. Üyesi Ebru PEKEL ÖZMEN

I. YAPAY ZEKÂ NEDİR? 21
A. YAPAY ZEKÂNIN TARİHÇESİ 21
B. YAPAY ZEKÂNIN UYGULAMA ALANLARI 23
C. YAPAY ZEKÂ VE ETİK 25
II. YAPAY ZEKÂ UYGULAMALARI 26
A. AKILLI ROBOTLAR 26
1. Akıllı Robotların Tanımı ve Temel Bileşenleri 27
2. Akıllı Robotların Tarihçesi ve Gelişimi 28
3. Akıllı Robotların Uygulama Alanları 29
B. DOĞAL DİL İŞLEME: MAKİNE İLE İNSAN DİLİ ARASINDAKİ KÖPRÜ 30
1. Uygulama Alanları 31
C. NESNELERİN İNTERNETİ 32
D. BÜYÜK VERİ ANALİTİĞİ 33
E. MAKİNE ÖĞRENMESİ 33
III. MAKİNE ÖĞRENMESİNİN TEMELLERİ 34
A. BİR MAKİNE NASIL ÖĞRENİR? 34
B. MAKİNE ÖĞRENMESİ TÜRLERİ 36
1. Denetimli Öğrenme 37
a. Sınıflandırma 37
b. Regresyon 40
c. Topluluk Öğrenme 43
2. Denetimsiz Öğrenme 44
a. Kümeleme (Clustering) 45
b. Birliktelik Analizi 46
IV. POPÜLER MAKİNE ÖĞRENİMİ ALGORİTMALARI 47
A. KARAR AĞAÇLARI 47
B. K-EN YAKIN KOMŞU ALGORİTMASI 49
C. K-ORTALAMALAR ALGORİTMASI 50

D. YAPAY SİNİR AĞLARI 50
E. APRIORI ALGORİTMASI 52
KAYNAKÇA 55

İKİNCİ BÖLÜM
YAPAY ZEKÂ VE HUKUK: ETİK İLKELER, HUKUKİ ÇERÇEVE VE SORUMLULUK

YAPAY ZEKÂ TEKNOLOJİLERİNE ETİK YAKLAŞIM

Doç. Dr. Elif KÜZECİ - Av. Zeynep ÖĞRETMEN KOTİL

GİRİŞ 61
I. YAPAY ZEKÂNIN TANIMI VE KAPSAMI 62
A. YAPAY ZEKÂNIN GELİŞİMİ VE TANIMIN DEĞİŞİMİ 63
B. YAPAY ZEKÂ SİSTEMLERİNİN SINIFLANDIRILMASI 68
1. Gelişmişlik Seviyesine Göre Sınıflandırma 68
2. Risk Seviyesine Göre Sınıflandırma 69
3. Sembolik Yapay Zekâ ve Veri Odaklı Yapay Zekâ Ayrımı 71
4. Diğer Sınıflandırmalar 71
C. FARKLI YAKLAŞIMLARIN ORTAK PAYDASI 72
D. ETİK İLKELERE GİDEN YOLDA YAPAY ZEKÂ 73
II. YAPAY ZEKÂ ETİĞİ 74
A. ETİK İLKELER 78
1. İnsan Haklarına Saygılı ve İnsan Odaklı Olma 80
2. Çeşitlilik, Eşitlik, Ayrımcılık Yapmama ve Adalet 81
3. Çevresel ve Toplumsal Refaha Öncelik Verme 83
4. Şeffaflık ve Hesap Verilebilirlik 84
5. Teknik Sağlamlık ve Güvenlik 86
6. Gizlilik ve Veri Yönetimi 87
B. ZAMANA, YAYIMLAYAN KURUMA VE BÖLGEYE BAĞLI YAKLAŞIM FARKLILIKLARI 89
1. Zamansal Yaklaşım Farklılıkları 91
2. Yayımlayan Kuruluşa Bağlı Yaklaşım Farklılıkları 93
3. Bölgesel Yaklaşım Farklılıkları 95
SONUÇ 97
KAYNAKÇA 101

KODLAR VE KANUNLAR: YAPAY ZEKÂNIN REGÜLASYON ROTASI VE AB YAPAY ZEKÂ TÜZÜĞÜ

Dr. Öğr. Üyesi Osman Gazi GÜÇLÜTÜRK

GİRİŞ 109
I. TEKNOLOJİ REGÜLASYONU, HUKUK VE YAPAY ZEKÂ 111
A. REGÜLASYON KAVRAMI 111
B. HUKUKUN TEKNOLOJİ REGÜLASYONUNDAKİ YERİ 115
II. YAPAY ZEKÂNIN HUKUK YOLUYLA REGÜLASYONUNUN GEREKLİLİĞİ ÜZERİNE BİR METODOLOJİ ÖNERİSİ VE DİKKAT EDİLMESİ GEREKEN HUSUSLAR 118
A. TEKNOLOJİ REGÜLASYONUNDA GEREKLİLİK ANALİZİ 118
1. Amaç Tespiti 119
2. Müdahalenin Gerekliliğini İncelemek 122
3. Hukuki Müdahale 124
B. YAPAY ZEKÂNIN HUKUKİ DÜZENLEME YOLUYLA REGÜLASYONUNUN GEREKLİLİĞİ 128
III. BİR HUKUKİ DÜZENLEME NESNESİ OLARAK YAPAY ZEKÂ 131
IV. YAPAY ZEKÂNIN HUKUK YOLUYLA REGÜLASYONUNDA BİR MİHENK TAŞI OLARAK AB YAPAY ZEKÂ TÜZÜĞÜ 136
A. NİTELİĞİ VE YASALAŞMA SÜRECİ 139
B. YZT'NİN KAPSAMI 144
1. Bir yapay zekâ sistemi ya da genel amaçlı bir yapay zekâ modeli bulunmalıdır 144
2. YZT kapsamında sayılan operatörlerden biri bulunmalıdır 145
3. İlgili operatörle bağlantılı olarak YZT'nin öngördüğü coğrafi uygulama şartlarından biri sağlanmalıdır. 148
4. YZT'nin istisnalarından biri uygulanmıyor olmalıdır 149
C. YZT'NİN UYGULANMASI 151
1. YZT'nin Yapay Zekâ Sistemi ve Yapay Zekâ Modellerine Yaklaşımı 151
2. Yapay Zekâ Sistemleri Bakımından 152
a. Risk Temelli Yaklaşım 152
b. Yükümlülüklerin Tespiti 160
c. Uyum Değerlendirmesi ve Yaptırımlar 162
3. Genel Amaçlı Yapay Zekâ Modelleri Bakımından 164
a. Genel Amaçlı Yapay Zekâ Modelleri ile İlgili Yükümlülükler 165

b. Sistemik Risk Taşıyan Genel Amaçlı Yapay Zekâ Modelleri ve İlgili Yükümlülükler 166
c. Genel Amaçlı Yapay Zekâ Modelleri ile İlgili Yükümlülüklere Uyum ve Yaptırımlar 167
D. BİR REGÜLASYON ARACI OLARAK YZT'YE DAİR DEĞERLENDİRMELER 168
SONUÇ 171
KAYNAKÇA 173

YAPAY ZEKÂNIN YOL AÇTIĞI ZARARLARDAN HUKUKİ SORUMLULUK

Doç. Dr. Hüseyin Can AKSOY

GİRİŞ 179
I. YAPAY ZEKÂ SORUMLULUĞU VE HUKUKİ ÇERÇEVE 180
A. YAPAY ZEKÂNIN TEMEL ÖZELLİKLERİ VE DOĞURDUĞU BAŞLICA RİSKLER 180
B. YAPAY ZEKÂNIN YOL AÇTIĞI ZARARLARDAN HUKUKİ SORUMLULUĞA İLİŞKİN TEMEL SORUNLAR 182
C. AVRUPA BİRLİĞİ'NDEKİ YAPAY ZEKÂ DÜZENLEMELERİ BAĞLAMINDA YAPAY ZEKÂNIN YOL AÇTIĞI ZARARLARDAN HUKUKİ SORUMLULUK 184
1. Yapay Zekâ Yasası 184
2. Yapay Zekâ Sorumluluk Direktifi Taslağı 185
a. Zarar Görenin Delillere Erişme Hakkı 185
b. Nedensellik Bağı Karinesi 186
3. Ürün Sorumluluğu Direktifi 188
a. Ürün Tanımının Yapay Zekâ Sistemlerini Kapsar Şekilde Genişletilmesi 189
b. Tazmin Edilebilir Zarar Türlerinin Çoğaltılması 189
c. Ayıp Değerlendirmesinde Dikkate Alınacak Unsurların Yapay Zekâ Sistemleri ile Uyumlu Hale Getirilmesi 190
d. Zarar Görenin Delillere Erişme Hakkı 190
e. İspat Yükünün Zarar Gören Lehine Hafifletilmesi 191
II. KİŞİSEL VERİLERİN KORUNMASI BAĞLAMINDA YAPAY ZEKÂNIN SORUMLULUĞU 191
A. YAPAY ZEKÂ SİSTEMLERİNİN ÇALIŞMASINDA KİŞİSEL VERİLERİN İŞLEVİ 192
B. YAPAY ZEKÂ SİSTEMLERİNİN KİŞİSEL VERİ İHLALLERİNDEN DOĞAN HUKUKİ SORUMLULUK 192
SONUÇ VE ÖNERİLER 194
KAYNAKÇA 196

ÜÇÜNCÜ BÖLÜM
YAPAY ZEKÂ SİSTEMLERİNDE KİŞİSEL VERİLERİN İŞLENMESİ

VERİ KORUMA HUKUKUNUN TEMEL PRENSİPLERİ VE YAPAY ZEKÂ UYGULAMALARI AÇISINDAN DEĞERLENDİRİLMESİ

Dr. Öğr. Üyesi Çiçek ERSOY

GİRİŞ 199
I. HUKUKA UYGUN İŞLEME VE ŞEFFAFLIK 201
II. AMACA UYGUN İŞLEME 204
III. ÖLÇÜLÜLÜK 207
IV. VERİ MİNİMİZASYONU VE GEREKLİ SÜRE KADAR SAKLANMA 208
V. DOĞRULUK VE GEREKTİĞİNDE GÜNCEL OLMA 209
VI. BÜTÜNLÜK, GİZLİLİK VE GÜVENLİK 209
VII. HESAP VERİLEBİLİRLİK 210
KAYNAKÇA 212

YAPAY ZEKÂ ALGORİTMALARIYLA PROFİLLEME VE KİŞİSEL VERİLERİN KORUNMASI

Prof. Dr. E. Eylem AKSOY RETORNAZ

GİRİŞ 215
I. PROFİLLEME KAVRAMINA GENEL BİR BAKIŞ 217
A. TANIM 217
B. PROFİLLEME TÜRLERİ 218
1. Bireysel Profilleme-Grup Profillemesi 219
2. Doğrudan Profilleme-Dolaylı Profilleme 220
3. Profilleme-Yüksek Riskli Profilleme 220
II. KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN ULUSAL VE ULUSLARARASI METİNLERDE PROFİLLEME 222
A. AVRUPA KONSEYİ METİNLERİNDE PROFİLLEME 222
1. Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi (108 sayılı Sözleşme) 222
2. Profil Oluşturma Bağlamında Kişisel Verilerin İşlenmesiyle İlgili Olarak Bireylerin Korunması Tavsiye Kararı - CM/Rec(2021)8 223
3. Avrupa Konseyi Yapay Zekâ, İnsan Hakları, Demokrasi ve Hukukun Üstünlüğü Çerçeve Sözleşmesi 225

B. AVRUPA BİRLİĞİ MEVZUATI ... 226
1. Genel Veri Koruma Tüzüğü (GVKT) ... 226
a. Profilleme Tanımı ... 226
b. Profilleme Türleri ... 227
c. Profillemeye Dayalı Otomatik Münferit Karar Alma ... 229
2. AB Polis ve Yargı Direktifi (2016/80 sayılı Direktif) ... 232
3. AB Yapay Zekâ Tüzüğü ... 233
C. 6698 SAYILI KİŞİSEL VERİLERİN KORUNMASI KANUNU VE PROFİLLEME ... 235
III. KİŞİSEL VERİLERİN KORUNMASI KAPSAMINDA YAPAY ZEKÂ SİSTEMLERİ VE PROFİLLEME ... 236
A. KİŞİSEL VERİ TANIMI VE YAPAY ZEKÂ SİSTEMLERİ ARACILIĞIYLA PROFİLLEME ... 236
B. KİŞİSEL VERİLERİN İŞLENMESİNE İLİŞKİN TEMEL İLKELER VE YAPAY ZEKÂ SİSTEMLERİ ARACILIĞIYLA PROFİLLEME ... 237
1. Aydınlatma Yükümlülüğü ... 237
2. Amaçla Sınırlı İşleme İlkesi ve Veri Minimizasyonu ... 238
C. İLGİLİ KİŞİNİN RIZASI ... 239
D. İLGİLİ KİŞİNİN HAKLARI BAKIMINDAN YAPAY ZEKÂ SİSTEMLERİYLE PROFİLLEME ... 241
E. VERİ KORUMA ETKİ DEĞERLENDİRİLMESİ ... 242
SONUÇ ... 243
KAYNAKÇA ... 244

YAPAY ZEKÂ VE TEMEL VERİ KORUMA YÖNTEMLERİ

Prof. Dr. Yücel SAYGIN - Doç. Dr. Ali İNAN - Dr. Öğr. Üyesi Mehmet Emre GÜRSOY

GİRİŞ ... 249
I. KİŞİSEL GİZLİLİK KORUMA YÖNTEMLERİ ... 254
A. İSTATİSTİKSEL VERİ TABANI KORUMASI ... 254
B. ANONİMLEŞTİRME ... 256
C. DİFERANSİYEL MAHREMİYET ... 262
D. ALTERNATİF TANIMLAR VE FARKLARI ... 265
II. FEDERE ÖĞRENME VE KİŞİSEL GİZLİLİK ETKİLERİ ... 267
A. FEDERE ÖĞRENME ... 267
B. FEDERE ÖĞRENME İLE İLGİLİ ZORLUKLAR ... 270
C. FEDERE ÖĞRENME İLE İLGİLİ RİSKLER VE SALDIRILAR ... 271
D. FEDERE ÖĞRENMEDE KİŞİSEL GİZLİLİK VE GÜVENLİK KORUMA YÖNTEMLERİNİN UYGULANMASI ... 274
KAYNAKÇA ... 276

HASSAS GRUPLAR (ÇOCUKLAR, YAŞLILAR, ENGELLİ BİREYLER) İÇİN GELİŞTİRİLEN YAPAY ZEKÂ UYGULAMALARINDA DİKKAT EDİLMESİ GEREKEN ETMENLER

Prof. Dr. Hatice KÖSE

GİRİŞ 279
I. VERİ TOPLANMASI, SAKLANMASI VE PAYLAŞIMI 283
A. ÖRNEK UYGULAMALAR: İŞİTME ENGELLİ ÇOCUKLAR 283
1. RoboRehab: Yardımcı Odyoloji Rehabilitasyon Robotu 283
B. ÖRNEK UYGULAMALAR: OTİZMLİ ÇOCUKLAR 285
1. EMBOA: Otizmli Çocuklara Yönelik Bir Müdahale Aracı Olarak Sosyal Yardımcı Robotikte Duygusal Döngü 285
a. Etik Onaydan Önce 285
b. Etik Onay Alındıktan Sonra ve Katılımcıların İşe Alımı Sırasında 286
c. Çalışmadan Önce 287
d. Çalışma Sırasında 287
C. ÖRNEK UYGULAMALAR: SEREBRAL PALSİLİ BEBEKLER 288
1. Techtoys: Nörogelişimsel Bozuklukların Erken Tespiti ve İzlenmesi için Sensör Tabanlı Oyuncaklarla Bebeklik Döneminde Dijital Biyobelirteçler Edinimi 288
TARTIŞMA VE SONUÇ 288
KAYNAKÇA 290

DÖRDÜNCÜ BÖLÜM
YAPAY ZEKÂNIN SEKTÖREL UYGULAMALARI

SAĞLIK ALANINDA YAPAY ZEKÂ VE KİŞİSEL VERİLER

Prof. Dr. Perihan Elif EKMEKCİ

SONUÇ VE ÖNERİLER 302
KAYNAKÇA 304

İSTİHDAMDA YAPAY ZEKÂ

Dr. Öğr. Üyesi Başak OZAN ÖZPARLAK

I. İSTİHDAM SÜREÇLERİNDE YAPAY ZEKÂ SİSTEMLERİ 305
A. İSTİHDAMDA ALGORİTMİK DÖNÜŞÜMÜN VERİ KORUMA HUKUKU AÇISINDAN ÖNEMİ 305
1. İstihdamda Yapay Zekâ 305

2. İstihdamda Yapay Zekâ Konusunu Ele Almanın Güncel Önemi 307
B. İSTİHDAM SÜREÇLERİNDE ALGORİTMİK YÖNETİM KAVRAMI 311
1. İşe Alım Sürecinde Kullanılan Yapay Zekâ Sistemleri 313
2. İş İlişkisinin Kurulmasından Sonra YZ Kullanımı 315
II. İSTİHDAMDA YZ KULLANIMININ 6698 SAYILI KANUN'DAKİ DEĞİŞİKLİKLER AÇISINDAN DEĞERLENDİRİLMESİ 322
A. İSTİHDAMDA YAPAY ZEKÂ VE 6698 SAYILI KİŞİSEL VERİLERİN KORUNMASI KANUNU REFORMU 322
B. İSTİHDAMDA YZ KULLANIMINDA İŞLENEN HASSAS VERİLER AÇISINDAN 6698 SAYILI KANUN'UN 6. MADDESİ DEĞİŞİKLİĞİNİN DEĞERLENDİRİLMESİ 325
III. İSTİHDAMDA YZ KULLANIMININ GÜNCEL AB REGÜLASYONLARI AÇISINDAN DEĞERLENDİRİLMESİ 327
A. AB DİJİTAL HİZMETLER KANUNU AÇISINDAN DEĞERLENDİRME 327
B. AB YAPAY ZEKÂ KANUNU AÇISINDAN DEĞERLENDİRME 328
1. İstihdamda Yapay Zekâ Kullanımının AB YZ Kanunundaki Risk Kategorisi Açısından Değerlendirilmesi 328
2. AB YZ Kanunu 13. Maddesi ile Getirilen Şeffaflık Yükümlülükleri 331
3. YZ Kanunu 14. Maddesi: İnsan Gözetimi 333
SONUÇ 334
KAYNAKÇA 336

ÖNERİ MODELLERİNİN KVKK İLE UYUMU

Prof. Dr. Şule GÜNDÜZ ÖĞÜDÜCÜ - Öğr. Gör. Dr. Resul TUGAY

GİRİŞ 341
I. ÖNERİ MODELLERİ 342
A. ÖNERİ SİSTEMLERİ ÇEŞİTLERİ 347
1. İşbirlikçi Filtreleme 348
2. İçerik Tabanlı Filtreleme 349
3. Hibrit Yöntemler 351
B. ÖNERİ MODELLERİNDE KULLANILAN VERİ TÜRLERİ 354
C. RİSKLER 356
1. Öneri Sistemi Kaynaklı Riskler 359
a. Veriye Doğrudan Erişim 359
b. Yetkisiz Veri Depolama 359
c. Diğer (Üçüncü Taraf) Şirketlerle Veri Paylaşımı 360

d. Çalışanlar Tarafından Yetkisiz Erişim 360
e. Kullanıcı Tercih Verilerinden Çıkarım 361
2. Öneri Sistemini Kullanan Diğer Kullanıcılar Tarafından Oluşturulan Riskler 362
3. Öneri Sistemi Kullanıcısı Olmayan Dış Varlıklar Tarafından Oluşturulan Riskler 363
D. ÖNERİ SİSTEMLERİNİN 6698 SAYILI KANUN DÜZENLEMELERİNE UYARLANMASI 363
SONUÇ 365
KAYNAKÇA 367

ULAŞIM SEKTÖRÜNDE YAPAY ZEKÂ

Doç. Dr. Nazım Kemal ÜRE

GİRİŞ 371
I. OTONOM ARAÇLAR 373
II. TRAFİK YÖNETİMİ 379
III. YOL GÜVENLİĞİ 382
IV. HUKUKİ VE ETİK HUSUSLAR 384
SONUÇ 386
KAYNAKÇA 387

FİNANS SEKTÖRÜNDE YAPAY ZEKÂ KULLANIMI: KİŞİSEL VERİLERİN KORUNMASI ODAĞINDA BİR DEĞERLENDİRME

Doç. Dr. Pınar ÇAĞLAYAN AKSOY

GİRİŞ 389
I. FİNANS SEKTÖRÜNDE YAPAY ZEKÂ TEKNOLOJİLERİNİN KULLANILMASI 395
A. BORÇ VERME (CREDIT INTERMEDIATION) 398
B. VARLIK VE SERVET YÖNETİMİ 400
C. ÖDEMELER 403
D. ALGORİTMİK TİCARET 403
E. BLOKZİNCİRİ TEMELLİ FİNANS 404
F. MÜŞTERİ DENEYİMİNİN İYİLEŞTİRİLMESİ 406
G. FİNANSAL SUÇLARIN TESPİTİ VE ÖNLENMESİ 407
II. FİNANS SEKTÖRÜNDE YAPAY ZEKÂ KULLANIMININ KİŞİSEL VERİLERİN VE MAHREMİYETİN KORUNMASI BAKIMINDAN DEĞERLENDİRİLMESİ 409
A. GENEL OLARAK 409

B. GEN-AI MODELLERİNE ÖZGÜ YENİ ZORLUKLAR 414
C. SİBER GÜVENLİK RİSKLERİ 416
D. "ROBO-DANIŞMANLIK" VE KİŞİSEL VERİLER 417
E. FİNANS SEKTÖRÜNDE YAPAY ZEKÂ KULLANILMASI SÜREÇLERİNDE KİŞİSEL VERİLERİN VE MAHREMİYETİN KORUNMASI HAKKINDA GÜNCEL YAKLAŞIMLAR VE ÖNERİLER 419
1. Mahremiyet Artırıcı Teknolojiler (Privacy Enhancing Technologies) 419
2. Finansal Kuruluşlara İlişkin Diğer Öneriler 421

SONUÇ 422

KAYNAKÇA 427

EĞİTİMDE YAPAY ZEKÂ

Doç. Dr. Nursel YALÇIN - Arş. Gör. Behiye CANBAZ

GİRİŞ 431

I. EĞİTİMDE YAPAY ZEKÂ TARİHİ 432

II. EĞİTİMDE YAPAY ZEKÂ TÜRLERİ 442

A. UZMAN SİSTEMLER (EXPERT SYSTEMS) 442
B. AKILLI ÖĞRETİCİ SİSTEMLER 443
C. DİYALOG TABANLI ÖĞRETİCİ SİSTEMLER 445

III. EĞİTİMDE KULLANILAN YAPAY ZEKÂ ARAÇLARI 446

A. ÇEVİRİ ARAÇLARI 447
B. SOHBET ROBOTLARI 448
C. ÖĞRENME ORTAMLARI 449
D. DİJİTAL DERS KİTAPLARI 450
E. SESLİ ASİSTANLAR 452
F. BENZERLİK ORANI KONTROLÜ 453
G. NOT TUTMA 453
H. DİL BİLGİSİ 454
I. GÖRSELLEŞTİRME & GÖRÜNTÜ OLUŞTURMA 455
J. MAKİNE ÖĞRENMESİ VE PROGRAMLAMA 456
K. SUNU OLUŞTURMA 457
L. MÜZİK VE AVATAR OLUŞTURMA 457
M. VİDEO VE SES OLUŞTURMA 457

IV. EĞİTİMDE YAPAY ZEKÂ KULLANIMININ AVANTAJLARI 458
V. EĞİTİMDE YAPAY ZEKÂ KULLANIMININ DEZAVANTAJLARI VE ZORLUKLARI 460
SONUÇ 463
KAYNAKÇA 464

BEŞİNCİ BÖLÜM

YAPAY ZEKÂDA YÖNETİŞİM VE METODOLOJİ

Hâkim İsmet YURTERİ

GİRİŞ 469
I. YAPAY ZEKÂ YÖNETİŞİM İLKELERİ 469
A. EŞİTLİK VE ADALET 469
B. HUKUKUN ÜSTÜNLÜĞÜ 471
C. REGÜLASYON VE DENETİM 472
D. ŞEFFAFLIK VE HESAP VEREBİLİRLİK 473
II. YAPAY ZEKÂ YÖNETİŞİM MEKANİZMALARI 475
A. HEDEF VE STRATEJİK PLANLAMA 475
B. KURUMSAL YAPI VE ORGANİZASYON YAPILANDIRMASI 476
C. HUKUKİ ÇERÇEVE VE DÜZENLEYİCİ MEKANİZMALAR 479
D. MEVZUAT UYUMLULUK SÜREÇ TAKİBİ 480
E. BİLGİ VE İLETİŞİM TEKNOLOJİLERİ ALTYAPISI 481
F. RİSK VE TEKNİK SORUN TESPİT MEKANİZMASI 483
1. Etik 484
2. Veri Gizliliği 485
3. Siber Güvenlik 486
G. YAPAY ZEKÂ ALGORİTMALARININ STANDARDİZASYONU 487
H. YAPAY ZEKÂ YÖNETİŞİM EKOSİSTEMİ 498
III. YAPAY ZEKÂ YÖNETİŞİM METODOLOJİSİNE ETKİ EDEN UNSURLAR 499
A. ULUSAL YAPAY ZEKÂ STRATEJİSİNİN ETKİSİ 499
B. RİSK TEMELLİ YAKLAŞIMIN ETKİSİ 501
C. ÜRETKEN YAPAY ZEKÂ SİSTEMLERİNİN ETKİLERİ 505
D. SÜPER HİZALAMA VE ETKİLERİ 510
E. SİBER GÜVENLİĞİN ETKİSİ 513
F. NESNELERİN VE DAVRANIŞLARIN İNTERNETİNİN ETKİLERİ 516
1. Nesnelerin İnterneti (IoT) 516
2. Davranışların İnterneti (IoB) 518

G. ÇOK DUYULU GENİŞLETİLMİŞ GERÇEKLİK (XR) UYGULAMALARININ VE DİJİTAL İKİZİN ETKİLERİ 519
1. Çok Duyusal Genişletilmiş Gerçeklik (XR) Uygulamaları (Multi - Sensory Extended Reality (XR) Applications) 519
2. Dijital İkiz 520
H. KUANTUM BİLGİSAYAR SİSTEMLERİNİN ETKİLERİ 521
I. 5G VE 6G HÜCRESEL AĞLARIN ETKİLERİ 524
IV. TÜRKİYE'DE YAPAY ZEKÂ YÖNETİŞİMİ VE METODOLOJİSİ 529
SONUÇ 538
KAYNAKÇA 543

YAPAY ZEKÂ VE MAKİNE ÖĞRENMESİNE GİRİŞ

Doç. Dr. Tuncay ÖZCAN*

Dr. Öğr. Üyesi Ebru PEKEL ÖZMEN**

I. YAPAY ZEKÂ NEDİR?

Yapay Zekâ (YZ), insan zekâsını taklit eden, öğrenebilen ve problem çözebilen sistemlerin geliştirilmesini amaçlayan bir bilim dalıdır. Yapay zekâ, bilgisayarların ve diğer makinelerin karmaşık görevleri otonom bir şekilde gerçekleştirmesini sağlar. Yapay zekânın temel amacı, makinelerin insan benzeri zekâ ve becerilere sahip olmasını sağlamaktır.

Yapay zekânın alt dalları arasında makine öğrenmesi, derin öğrenme, doğal dil işleme ve bilgisayarla görme gibi çeşitli alanlar bulunmaktadır. Her bir alt dal, farklı uygulama alanlarına ve problemlere çözüm getirmek için özel teknikler ve algoritmalar kullanır.

A. YAPAY ZEKÂNIN TARİHÇESİ

Yapay Zekâ (YZ) alanı, 20. yüzyılın ortalarından bu yana büyük bir gelişim göstermiştir. Bu alt bölümde, yapay zekânın tarihçesi ve bu alandaki önemli kilometre taşlarını ele alınacaktır.

1950'ler: Başlangıç ve İlk Adımlar

- 1950: Alan Turing, "Computing Machinery and Intelligence" makalesinde, makinelerin düşünebilme yeteneğini tartışarak Turing Testi'ni önermiştir[1]. Bu test, bir makinenin insan benzeri zekâya sahip olup olmadığını belirlemeye yönelik bir kriterdir[2].

* İstanbul Teknik Üniversitesi, İşletme Mühendisliği Bölümü

** Samsun Üniversitesi, Endüstri Mühendisliği Bölümü

1 Alan Mathison Turing, "Mind," *Mind* 59, no. 236 (1950).

2 Francesca Ferrando, "Is the Post-Human a Post-Woman? Cyborgs, Robots, Artificial Intelligence and the Futures of Gender: A Case Study," *European Journal of Futures Research* 2, no. 1 (2014), https://doi.org/10.1007/s40309-014-0043-8.

- 1956: Dartmouth Konferansı, yapay zekânın bir bilim dalı olarak kabul edilmesini sağlamıştır. John McCarthy, Marvin Minsky, Nathaniel Rochester ve Claude Shannon gibi öncüler bu konferansta yapay zekânın temellerini atmışlardır[3].

1960'lar: İlk Çalışmalar ve Uygulamalar

- 1961: İlk endüstriyel robot olan Unimate, General Motors fabrikasında kullanılmaya başlanmıştır.
- 1966: Joseph Weizenbaum, ilk doğal dil işleme programı olan ELIZA'yı geliştirmiştir. ELIZA, belirli anahtar kelimeler kullanarak insanlarla etkileşim kurabiliyordu.
- 1969: Marvin Minsky ve Seymour Papert, "Perceptrons" adlı kitabı yayımlayarak, yapay sinir ağlarının sınırlamaları üzerinde durmuştur. Bu kitap, yapay zekâ araştırmalarında önemli bir dönüm noktası olmuştur.

1970'ler: Yapay Zekâ Kışı ve İlerlemenin Duraklaması

- 1970'ler: Yapay zekâ araştırmalarında ilerleme kaydedilememesi ve yüksek beklentilerin karşılanamaması nedeniyle, fonlamalar azalmış ve araştırmalar yavaşlamıştır. Bu dönem, "Yapay Zekâ Kışı" olarak adlandırılmaktadır.

1980'ler: Uzman Sistemler ve Yeniden Canlanma

- 1980'ler: Yapay zekâ araştırmaları, uzman sistemlerin geliştirilmesiyle yeniden canlanmıştır. Uzman sistemler, belirli bir alandaki uzman bilgilerini kullanarak karmaşık problemleri çözebilen bilgisayar programlarıdır. MYCIN ve DENDRAL gibi sistemler bu dönemin önemli örneklerindendir.
- 1986: Geoffrey Hinton, David Rumelhart ve Ronald Williams, geri yayılım (backpropagation) algoritmasını tanıtmıştır. Bu algoritma, yapay sinir ağlarının eğitilmesinde önemli bir ilerleme sağlamıştır.

---

[3] Michael Haenlein, Andreas Kaplan, "A Brief History of Artificial Intelligence: On the Past, Present, and Future of Artificial Intelligence," *California Management Review* 61, no. 4 (2019), https://doi.org/10.1177/0008125619864925.

1990'lar: Yeni Algoritmalar ve İnternetin Etkisi

- 1997: IBM'in Deep Blue adlı süper bilgisayarı, dünya satranç şampiyonu Garry Kasparov'u yenerek büyük bir başarı elde etmiştir. Bu olay, yapay zekâ alanında önemli bir dönüm noktası olarak nitelendirilmiştir.
- 1990'lar: İnternetin yaygınlaşması, büyük veri setlerinin ve güçlü hesaplama kaynaklarının erişilebilirliğini artırarak yapay zekâ araştırmalarında yeni imkânlar sunmuştur.

2000'ler ve 2010'lar: Derin Öğrenme ve Büyük Veri

- 2006: Geoffrey Hinton ve ekibi, derin öğrenme kavramını tanıtmış ve bu alanda önemli çalışmalar yapmıştır. Derin öğrenme, yapay sinir ağlarının daha derin ve karmaşık yapılarını kullanarak gerçek hayat problemleri için daha yüksek doğrulukla sonuçlar elde etmeyi mümkün kılmıştır.
- 2012: AlexNet adlı derin öğrenme modeli, ImageNet yarışmasında büyük bir başarı elde etmiş ve derin öğrenmenin gücünü göstermiştir[4].
- 2016: Google'ın DeepMind ekibi tarafından geliştirilen AlphaGo, dünya Go şampiyonu Lee Sedol'u yenerek yapay zekânın karmaşık oyunlarda bile üstün performans gösterebileceğini kanıtlamıştır.

Günümüz ve Gelecek

- Günümüz: Yapay zekâ, sağlık, finans, otomotiv, eğitim ve daha birçok alanda devrim niteliğinde uygulamalara sahip olmaya devam etmektedir. Özellikle doğal dil işleme ve üretken yapay zekâ, görüntü tanıma ve otonom sistemler gibi alanlarda önemli ilerlemeler kaydedilmektedir.
- Gelecek: Yapay zekânın geleceği, etik ve güvenlik konularının yanı sıra, insan-makine etkileşimlerinin nasıl şekilleneceği ve yapay zekânın toplum üzerindeki etkilerinin nasıl yönetileceği konularında önemli soruları da beraberinde getirmektedir.

B. YAPAY ZEKÂNIN UYGULAMA ALANLARI

Yapay zekâ, günümüzde sağlık, finans, otomotiv, eğitim ve birçok başka alanda geniş bir kullanım alanına sahiptir. Bu teknolojinin çeşitli sektör-

[4] Alex Krizhevsky, Ilya Sutskever, Geoffrey E. Hinton, "2012 AlexNet," *Adv. Neural Inf. Process. Syst* (2012).

lerdeki uygulama alanları, insan yaşamını kolaylaştırmak ve iş süreçlerini en iyilemek için önemli fırsatlar sunmaktadır. Yapay zekâ alanındaki çalışmaların hızla ilerlemesi ve çeşitli sektörlerde farklı uygulamaların geliştirilmesiyle birlikte insanların iş ve gelecek kaygılarının arttığı vurgulanmaktadır[5]. Özellikle sağlık sektöründe, yapay zekâ hastalık teşhisi, tedavi planlama ve kişiselleştirilmiş tıp gibi alanlarda önemli bir rol oynamaktadır[6]. Sağlık profesyonellerinin yapay zekâ kaygı durumlarının incelenmesi de bu alandaki önemli araştırma konularından biridir[7]. Finans sektöründe ise yapay zekâ, algoritmik ticaret, kredi risk değerlendirmesi ve dolandırıcılık tespiti gibi alanlarda etkin bir şekilde kullanılmaktadır[8]. Finans ve bankacılık sisteminde yapay zekâ kullanımı üzerine yapılan bir çalışmada, kullanıcıların yapay zekâyı kullanma biçimlerinin yaş, cinsiyet, meslek ve gelir dağılımı açısından farklılık gösterdiği belirtilmektedir. Eğitim sektöründe ise yapay zekâ, akıllı eğitim sistemleri ve öğrenci performans analizi gibi alanlarda kullanılmaktadır[9]. Sosyal bilgiler eğitimi alanında lisansüstü eğitimini sürdüren öğrencilerin yapay zekâ hakkındaki görüşlerinin incelenmesi, yapay zekânın eğitim süreçlerindeki potansiyel etkilerini anlamak açısından önemli bir çalışma konusudur[10]. Sonuç olarak, yapay zekânın sağlık, finans, eğitim ve diğer sektörlerdeki uygulama alanları giderek genişlemekte ve bu teknolojinin insan yaşamına olan etkisi ve önemi her geçen gün artmaktadır. Yapay zekâ teknolojilerinin etkin ve verimli bir şekilde kullanılması, iş süreçlerini en iyilemek ve insan yaşamını iyileştirmek için büyük potansiyeller sunmaktadır.

---

5 Bülent Akkaya, Ayşegül T. Özkan, Hasan Özkan, "Yapay Zekâ Kaygı (YZK) Ölçeği: Türkçeye Uyarlama, Geçerlik Ve Güvenirlik Çalışması," *Alanya Akademik Bakış* 5, no. 2 (2021), https://doi.org/10.29023/alanyaakademik.833668.

6 Yusuf K. Yilmaz et al., "Yapay Zekâ Ve Sağlıkta Yapay Zekânın Kullanımına Yönelik Sağlık Bilimleri Fakültesi Öğrencilerinin Görüşleri," *Süleyman Demirel Üniversitesi Sağlık Bilimleri Dergisi* 12, no. 3 (2021), https://doi.org/10.22312/sdusbed.950372.

7 Emel Filiz, Şerife Güzel, Abdurrahman ŞEngÜL, "Sağlık Profesyonellerinin Yapay Zekâ Kaygı Durumlarının İncelenmesi," *International Journal of Academic Value Studies (Javstudies Javs)* 8, no. 8 (2022), https://doi.org/10.29228/javs.57808.

8 Ersin Gümüş, Batuhan Medetoğlu, Salih Tutar, "Finans Ve Bankacılık Sisteminde Yapay Zekâ Kullanımı: Kullanıcılar Üzerine Bir Uygulama," *Bucak İşletme Fakültesi Dergisi* 3, no. 1 (2020), https://doi.org/10.38057/bifd.690982.

9 Emel Gümüş, Ece U. Kasap, "Hemşirelik Mesleğinin Geleceği: Robot Hemşireler," *Journal of Artificial Intelligence in Health Sciences* (2021), https://doi.org/10.52309/jai.2021.10.

10 Sedat Yeşilyurt, "Sosyal Bilgiler Eğitimi Alaninda Lisansüstü Eğitimini Sürdüren Öğrencilerin Yapay Zekâ Hakkindaki Görüşleri," *Asya Studies* 8, no. 27 (2024), https://doi.org/10.31455/asya.1406649.

C. YAPAY ZEKÂ VE ETİK

Yapay zekâ teknolojileri, günümüzde birçok sektörde yaygın olarak kullanılmakta olup, bu kullanımın etik boyutları da önemli bir konu haline gelmiştir. Yapay zekâ uygulamalarının insan hakları, mahremiyet, eşitlik ve ön yargı yapmama gibi temel değerlerle uyumlu olması ve etik standartlara uygun şekilde kullanılması gerekmektedir[11]. Bu bağlamda, yapay zekâ teknolojilerinin kullanımıyla ilgili etik sorunlar ve toplumsal etkileri üzerine yapılan çalışmalar, yapay zekâ alanında önemli bir araştırma alanı oluşturmaktadır.

Sağlık hizmetleri ve yönetiminde yapay zekânın kullanımıyla ilgili yapılan çalışmalar, yapay zekâ uygulamalarının etik boyutunu vurgulamakta ve bu teknolojinin insan sağlığına olan etkilerini değerlendirmektedir[12]. Özellikle perinatal dönemde yapay zekâ teknolojilerinin kullanımıyla ilgili yapılan araştırmalar, etik standartların sağlık alanındaki yapay zekâ uygulamalarında önemli bir rol oynaması gerektiğini vurgulamaktadır[13].

Endüstri 5.0'a doğru ilerlerken, zeki otonom sistemlerde etik ve ahlaki sorumluluklar konusu da önemli bir tartışma konusu haline gelmiştir[14]. Bu bağlamda, yapay zekâ tabanlı sistemlerin kişisel veri gizliliği ve güvenliği konularında belirsizliklerin ortaya çıkması, etik standartların ve yasal düzenlemelerin önemini artırmaktadır[15].

Ayrıca, yapay zekâ teknolojilerinin kullanımıyla ilgili toplumsal cinsiyet kapsamında yapılan araştırmalar, yapay zekâ uygulamalarının mevcut toplumsal cinsiyet algılarında bir değişime neden olup olmayacağı konu-

---

11 Tülay Turan, Gökhan Turan, Ecir U. Küçüksille, "Ethics of Artificial Intelligence: Impact on Society," *Mehmet Akif Ersoy Üniversitesi Fen Bilimleri Enstitüsü Dergisi* 13, no. 2 (2022), https://doi.org/10.29048/makufebed.1058538.

12 Betül Akalin, Ülkü Veranyurt, "Sağlık Hizmetleri Ve Yönetiminde Yapay Zekâ," *Acta Infologica* 5, no. 1 (2021), https://doi.org/10.26650/acin.750857..

13 Ebru C. Ekrem, Zeynep Daşikan, "Perinatal Dönemde Yapay Zekâ Teknolojisinin Kullanımı," *Eurasian Journal of Health Technology Assessment* 5, no. 2 (2021), https://doi.org/10.52148/ehta.980568.

14 Pelin Canbay, Zübeyde Demircioğlu, "Endüstri 5.0'a Doğru: Zeki Otonom Sistemlerde Etik Ve Ahlaki Sorumluluklar," *Ajit-E Online Academic Journal of Information Technology* 12, no. 45 (2021), https://doi.org/10.5824/ajite.2021.02.006.x.

15 Nermin Kişi, "İnsan Kaynakları Yönetiminde Yapay Zekâ Teknolojisinin Benimsenmesi Üzerine Güç Alanı Analizi," *İktisadi Ve İdari Bilimler Fakültesi Dergisi* (2024), https://doi.org/10.33707/akuiibfd.1406096.

sunu ele almaktadır[16]. Bu çalışmalar, yapay zekâ teknolojilerinin toplumsal cinsiyet eşitliği ve adaleti üzerindeki potansiyel etkilerini değerlendirmekte ve yapay zekâ uygulamalarının toplumsal cinsiyet konusundaki duyarlılığını vurgulamaktadır.

Sonuç olarak, yapay zekâ teknolojilerinin etik boyutları üzerine yapılan çalışmalar, bu teknolojilerin insan yaşamına ve topluma olan etkilerini anlamak ve etik standartlara uygun şekilde kullanımını teşvik etmek amacıyla önemli bir rol oynamaktadır. Yapay zekâ uygulamalarının etik ilkelerle uyumlu olması ve toplumsal faydaya odaklanması, bu teknolojinin sürdürülebilir ve güvenilir bir şekilde kullanılmasını sağlayacaktır.

II. YAPAY ZEKÂ UYGULAMALARI

Yapay Zekâ (YZ), çeşitli alanlarda devrim niteliğinde yenilikler getiren geniş bir uygulama yelpazesine sahiptir. Bu bölümde, YZ'nin en dikkat çekici ve etkili beş uygulama alanı incelenecektir.

A. AKILLI ROBOTLAR

Akıllı robotlar, yapay zekâ teknolojilerinin en heyecan verici ve hızla gelişen alanlarından biridir. Bu robotlar, insanlarla etkileşim kurabilme yeteneğine sahiptir. Çeşitli sektörlerde karmaşık görevleri yerine getirebilmekte ve çevrelerine uyum sağlayabilmektedir. Akıllı robotlar, sağlık, endüstri, eğitim ve hatta ev yaşamı gibi çeşitli alanlarda kullanım potansiyeline sahiptir. Sağlık sektöründe, akıllı robotlar cerrahi operasyonlardan hasta bakımına kadar çeşitli görevleri üstlenebilmektedir. Özellikle hassas operasyonları gerçekleştirebilen cerrahi robotlar, cerrahların işini kolaylaştırmakta ve hastaların iyileşme sürecini hızlandırmaktadır[17]. Ayrıca, akıllı robotlar hastanelerde hasta taşıma, ilaç dağıtımı ve hasta takibi gibi rutin görevleri yerine getirebilmektedir[18]. Endüstri sektöründe, akıllı robotlar üretim hatlarında otomasyon sağlayarak üretim verimliliğini artırmakta ve işçilerin güvenliğini sağlamaktadır. Bu robotlar karmaşık montaj operasyonlarını gerçekleştirebilmekte, üretim süreçlerinin verimliliğini arttır-

16 Büşra S. Çifci, Cigdem Basfirinci, "Yapay Zekâ Konusunun Toplumsal Cinsiyet Kapsaminda İncelenmesi: Mesleklere Yönelik Bir Araştirma," *Çukurova Üniversitesi Sosyal Bilimler Enstitüsü Dergisi* 29, no. 4 (2020), https://doi.org/10.35379/cusosbil.819510.

17 Akalin, Veranyurt, "Sağlık Hizmetleri Ve Yönetiminde Yapay Zekâ."

18 Akkaya, Özkan, Özkan, "Yapay Zekâ Kaygı (YZK) Ölçeği: Türkçeye Uyarlama, Geçerlik Ve Güvenirlik Çalışması."

makta ve maliyetleri düşürmektedir. Ayrıca endüstriyel tesislerde çalışan akıllı robotlar, insanların tehlikeli ortamlarda karşılaştığı riskleri azaltmaktadır. Eğitim alanında, akıllı robotlar öğrencilere etkileşimli ve kişiselleştirilmiş öğrenme fırsatları sunmaktadır. Bu robotlar dil öğrenimi, matematik ve fen bilimleri gibi konularda öğrencilere destek olabilmekte, öğrenme sürecini daha eğlenceli hale getirebilmektedir. Ayrıca akıllı robotlar, öğrencilerin problem çözme becerilerini geliştirmelerine ve yaratıcı düşünmelerini teşvik etmelerine yardımcı olmaktadır[19]. Ev yaşamında, akıllı robotlar güvenlik sistemleri ve temizlik robotları gibi çeşitli alanlarda kullanılmaktadır. Ev otomasyon sistemleri aracılığıyla akıllı robotlar ev sahiplerine konfor ve kolaylık sağlarken enerji verimliliğini artırmaktadır[20]. Ayrıca akıllı temizlik robotları evlerde otomatik olarak temizlik görevlerini yerine getirerek ev sahiplerinin zamanlarını daha verimli kullanmalarını sağlamaktadır[21].

1. Akıllı Robotların Tanımı ve Temel Bileşenleri

Akıllı robotlar, belirli görevleri yerine getirmek için programlanmış, insan müdahalesi olmadan kendi başlarına çalışabilen robotlardır. Bu robotların temel bileşenleri şunlardır:

- **Sensörler:** Robotların çevresini algılamasını sağlayan cihazlardır. Görüntü sensörleri, lazer tarayıcılar, ultrasonik sensörler ve dokunma sensörleri gibi çeşitli türleri bulunmaktadır. Bu sensörler, robotların çevresindeki nesneleri, engelleri ve değişiklikleri algılamasına yardımcı olmaktadır[22].
- **Aktüatörler:** Robotların hareket etmesini ve çeşitli görevleri yerine getirmesini sağlayan mekanik bileşenlerdir. Motorlar, pnömatik sistemler ve hidrolik sistemler bu kategoriye girmektedir. Aktüatörler, robotların kollarını, bacaklarını veya tekerleklerini hareket ettirmektedir[23].

---

19 BaŞKaya et al., "The Impact of Artificial Intelligence-Based Systems on Personal Data Privacy: A Study on Chatbots," *Bilişim Teknolojileri Dergisi* 15, no. 4 (2022), https://doi.org/10.17671/gazibtd.1053803.

20 Anas Abou Allaban, Maozhen Wang, Taşkın Padır, "A systematic review of robotics research in support of in-home care for older adults," *Information* 11, no. 2 (2020).

21 Anshu Prakash Murdan, Pawan Kumar Ramkissoon, "A smart autonomous floor cleaner with an Android-based controller" (2020).

22 Abdulkadir Karaci, Mustafa Erdemir, "Arduino Ve Wifi Temelli Çok Sensörlü Robot Tasarımı Ve Denetimi," *Bilişim Teknolojileri Dergisi* (2017), https://doi.org/10.17671/gazibtd.307271.

23 Celal H. Kagnicioglu, Emircan Özdemir, "Evaluation of SMEs in Eskisehir Within the Context of Industry 4.0," *Pressacademia* 3, no. 1 (2017), https://doi.org/10.17261/pressacademia.2017.672.

- **Yapay Zekâ Yazılımları:** Robotların öğrenme, karar verme ve planlama yeteneklerini sağlayan algoritmalar ve yazılımlardır. Makine öğrenmesi, derin öğrenme ve kuvvetli yapay zekâ algoritmaları, robotların görevleri daha etkili bir şekilde yerine getirmesine yardımcı olmaktadır[24].

Bu bileşenlerin bir araya gelmesiyle akıllı robotlar, çeşitli sektörlerde kullanılarak insan hayatını kolaylaştırmakta ve iş süreçlerinin verimliliğini artırmaktadır. Örneğin, endüstriyel robotlar üretim hatlarında otomasyon sağlayarak verimliliği artırırken, sağlık sektöründe cerrahi robotlar hassas operasyonları gerçekleştirerek cerrahların işini kolaylaştırmaktadır.

Bu sayede akıllı robotlar, insanların günlük yaşamlarını kolaylaştırmak ve daha verimli bir gelecek inşa etmek için önemli bir teknolojik gelişme olarak karşımıza çıkmaktadır.

2. Akıllı Robotların Tarihçesi ve Gelişimi

Akıllı robotların tarihçesi ve gelişimi oldukça ilginç ve hızlı bir şekilde ilerleyen bir konudur. Bu robotlar, teknolojinin evrimi ve yapay zekâ alanındaki ilerlemelerle yakından ilişkilidir. İlk robotlar başlangıçta endüstriyel ortamlarda kullanılmak üzere tasarlanmış basit makinelerdir. Ancak, robot teknolojilerinin gelişmesiyle birlikte akıllı robotlar ortaya çıkmıştır. Akıllı robotların tarihçesi 20. yüzyılın ortalarına dayanmaktadır.

Akıllı robotların gelişimi, yapay zekâ teknolojilerinin ilerlemesiyle hız kazanmıştır. Makine öğrenmesi, derin öğrenme ve güçlü yapay zekâ algoritmaları sayesinde robotlar daha akıllı ve etkili hale gelmiştir. Akıllı robotların tarihçesindeki bazı önemli kilometre taşları aşağıdaki gibi sıralanabilir:

- **1950'ler ve 1960'lar:** İlk endüstriyel robotlar, General Motors fabrikalarında kullanılmıştır. Bu robotlar, montaj hattında basit görevleri yerine getirmiştir.
- **1980'ler:** Yapay zekâ araştırmalarındaki ilerlemeler, robotların daha karmaşık görevleri yerine getirmesini sağlamıştır. Uzman sistemler ve makine öğrenmesi algoritmaları, robotlara yeni yetenekler kazandırmıştır.

---

[24] Sinan S. Ozkan et al., "Esnek Algılayıcı Kontrollü Robot El Tasarımı Ve Gerçeklenmesi," *Academic Platform Journal of Engineering and Smart Systems* (2017), https://doi.org/10.21541/apjes.314521.

- **2000'ler:** Otonom araçlar ve hizmet robotları gibi ileri seviye robotlar geliştirilmiştir. Boston Dynamics gibi şirketler, insansı ve hayvansı robotlar üzerinde çalışmıştır.

3. Akıllı Robotların Uygulama Alanları

Akıllı robotlar, montaj hatlarında, malzeme taşıma ve paketleme işlemlerinde yaygın olarak kullanılmaktadır. Otomotiv, elektronik ve gıda endüstrileri akıllı robotların etkin bir şekilde kullanıldığı sektörler arasındadır. Bu robotlar, üretim hızını artırmakta, hata oranını azaltmakta ve işçi güvenliğini sağlamaktadır[25]. Örneğin, otomotiv endüstrisinde kullanılan robotik sistemler, montaj hatlarında büyük verimlilik artışı sağlamış ve insan işçilerin tehlikeli görevlerden uzak tutulmasına yardımcı olmuştur.

Cerrahi robotlar, hassas ameliyatları gerçekleştirebilme yetenekleriyle dikkat çekmektedir. Da Vinci cerrahi sistemi gibi robotlar, minimal invaziv cerrahilerde kullanılmaktadır[26]. Ayrıca, hasta bakımında yardımcı robotlar ve rehabilitasyon robotları da sağlık sektöründe önemli bir rol oynamaktadır[27]. Bu tür robotlar, cerrahlara operasyon sırasında yüksek hassasiyet ve kontrol sağlarken, hastaların iyileşme sürecini hızlandırmaktadır.

Akıllı ev robotları, temizlik, güvenlik ve eğlence gibi alanlarda kullanılmaktadır. Roomba gibi robotik süpürgeler, ev temizliğini otomatikleştirmektedir[28]. Aynı zamanda, yaşlı ve engelli bireylerin günlük yaşam aktivitelerinde yardımcı olan sosyal robotlar da bulunmaktadır[29]. Örneğin, akıllı ev robotları, ev sahiplerine güvenlik sağlamak için hareket algılama ve kamera sistemleri ile donatılmıştır.

Otonom robotlar, tehlikeli veya erişilemeyen alanlarda keşif yapmak için kullanılmaktadır. Mars Rover gibi uzay robotları, uzay keşiflerinde kritik bilgiler toplamaktadır[30]. Denizaltı robotları, okyanusların derinliklerinde

---

25 Mikell P. Groover, *Automation, production systems, and computer-integrated manufacturing* (Pearson Education India, 2016).

26 Richard M. Satava, "Surgical robotics: the early chronicles: a personal historical perspective," *Surgical Laparoscopy Endoscopy & Percutaneous Techniques* 12, no. 1 (2002).

27 Terrence Fong, Illah Nourbakhsh, Kerstin Dautenhahn, "A survey of socially interactive robots," *Robotics and autonomous systems* 42, no. 3-4 (2003).

28 Fong, Nourbakhsh, Dautenhahn, "A survey of socially interactive robots."

29 Fong, Nourbakhsh, Dautenhahn, "A survey of socially interactive robots."

30 James G. Bellingham, Kanna Rajan, "Robotics in remote and hostile environments," *science* 318, no. 5853 (2007).

araştırma yapmaktadır[31].Bu robotlar, insanlı görevlerin mümkün olmadığı veya tehlikeli olduğu durumlarda hayati bilgiler sağlamaktadır.

Tarım robotları, mahsul ekimi, hasadı ve bitki sağlığı izleme gibi görevlerde kullanılmaktadır. Bu robotlar, tarımsal verimliliği artırmak ve iş gücünü optimum kullanmak için tasarlanmıştır[32]. Örneğin, akıllı tarım robotları, bitki sağlığını izlemek için sensörler kullanarak hastalık ve zararlıları erken tespit edebilmekte ve bu sayede verimliliği artırmaktadır.

B. DOĞAL DİL İŞLEME: MAKİNE İLE İNSAN DİLİ ARASINDAKİ KÖPRÜ

Doğal Dil İşleme (NLP), bilgisayarların insan dilini anlaması, yorumlaması ve üretmesiyle ilgilenen bir yapay zekâ alanıdır. NLP uygulamaları, metin ve konuşma verilerini işleyerek anlamlı bilgiler çıkarmakta ve insanlarla etkileşim kurabilen sistemler oluşturmaktadır. Uygulama örnekleri arasında sesli asistanlar (Siri, Alexa), dil çeviri hizmetleri (Google Translate) ve müşteri hizmetleri sohbet robotları (chatbot) bulunmaktadır. NLP, ayrıca büyük veri analitiği ve duygu analizi gibi alanlarda da önemli rol oynamaktadır.

Doğal Dil İşleme (NLP), insan dilini anlamak, işlemek ve üretmek için bilgisayarların ve yazılımların geliştirilmesiyle ilgilenen bir yapay zekâ dalıdır. NLP, dilin karmaşıklığını çözmek amacıyla dilbilgisi kuralları, sözdizimi, anlambilim ve anlam gibi dilsel özellikleri analiz etmektedir. Bu alan, makinelerin insan dilini anlayabilmesi ve anlamlı çıktılar üretebilmesi için gerekli teknikleri ve algoritmaları geliştirmeyi hedeflemektedir.

Doğal Dil İşleme, 1950'lerde Alan Turing'in "Makine Düşünmesi" üzerine yaptığı çalışmalarla temellerini atmıştır. Turing'in "Turing Testi" önerisi, makinelerin insan gibi düşünmesini test etme yolunu açmış, bu da NLP araştırmalarının yolunu belirlemiştir. Ancak, gerçek anlamda ilerlemeler 1980'lerin sonuna doğru başlamıştır. 1990'lar ve 2000'lerde, bilgisayarların işlem gücünün artması ve veri miktarının büyümesiyle NLP'de büyük gelişmeler kaydedilmiştir.

NLP'de kullanılan temel teknikler ve yöntemler aşağıdaki gibi sıralanabilir:

---

31 Bellingham, Rajan, "Robotics in remote and hostile environments."

32 Simon Blackmore et al., "Robotic agriculture-the future of agricultural mechanisation?," in *Precision Agriculture '05* (Wageningen Academic, 2005).

- Sözlük Tabanlı Yaklaşımlar: Bu yaklaşımlar, kelimelerin anlamlarını ve ilişkilerini belirlemek için önceden tanımlanmış sözlük ve kurallara dayanmaktadır. WordNet gibi kelime dağarcığı kaynakları bu tür uygulamalarda sıkça kullanılmaktadır.
- Makine Öğrenimi: 2000'lerin başından itibaren makine öğrenimi algoritmaları NLP'de yaygın olarak kullanılmaya başlanmıştır. Bu yöntemler, dil verilerini analiz ederek örüntüleri tanımlamak ve tahminler yapmak için kullanılmaktadır. Destek vektör makineleri (SVM), karar ağaçları ve rastgele ormanlar gibi algoritmalar, sınıflandırma ve regresyon problemlerinde etkilidir.
- Derin Öğrenme: 2010'ların ortalarında derin öğrenme teknikleri, NLP'de devrim yaratmıştır. Sinir ağları, özellikle de uzun kısa süreli bellek (LSTM) ve dönüştürücülere dayalı modeller, dil modelleme ve doğal dil anlama görevlerinde çığır açmıştır. Google'ın BERT (Bidirectional Encoder Representations from Transformers) ve OpenAI'ın GPT (Generative Pre-trained Transformer) modelleri, bu alandaki en bilinen örneklerdir.
- Doğal Dil Üretimi ve Çeviri: Makine çevirisi, NLP'nin en erken uygulama alanlarından biridir. Google Translate gibi sistemler, derin öğrenme ve büyük veri kullanarak dil çevirisini daha doğru ve akıcı hale getirmiştir. Ayrıca, doğal dil üretimi (NLG) teknikleri, makinelerin anlamlı ve insana yakın metinler oluşturmasını sağlamaktadır.

1. Uygulama Alanları

NLP'nin uygulama alanları oldukça geniştir. Bazı örnekler aşağıdaki gibi sıralanabilir:

Sesli Asistanlar: Siri, Alexa ve Google Assistant gibi sesli asistanlar, kullanıcıların sesli komutlarını anlamak ve yanıtlamak için NLP teknolojilerini kullanmaktadır.

Duygu Analizi: Sosyal medya gönderileri, müşteri yorumları ve haber makaleleri gibi metinlerdeki duygu ve eğilimleri analiz etmek için kullanılmaktadır.

Metin Sınıflandırma ve Etiketleme: E-posta spam filtreleme, haber makalelerini kategoriye ayırma ve sosyal medya gönderilerini sınıflandırma gibi uygulamalarda kullanılmaktadır.

Çeviri Sistemleri: Otomatik çeviri sistemleri, farklı dillerdeki metinleri doğru ve anlamlı bir şekilde çevirmede kullanılmaktadır.

Soru-Cevap Sistemleri: Kullanıcıların sorularını anlamak ve doğru cevapları sunmak için NLP kullanılmaktadır. SQuAD gibi veri setleri üzerinde çalışan sistemler, bu sistemlere örnek olarak verilebilir[33].

C. NESNELERİN İNTERNETİ

Nesnelerin İnterneti (IoT), fiziksel cihazların, araçların, binaların ve diğer nesnelerin birbirleriyle ve kullanıcılarla internet üzerinden iletişim kurmasını sağlayan bir teknoloji ağıdır. Bu nesneler, genellikle gömülü sensörler, yazılımlar ve diğer teknolojilerle donatılarak, veri toplayabilmekte ve paylaşabilmektedir. IoT, günlük yaşamdan sanayiye kadar geniş bir yelpazede devrim niteliğinde değişiklikler getirmektedir.

IoT'nin temel amacı, fiziksel nesneleri dijital dünyaya entegre ederek daha akıllı ve verimli sistemler oluşturmaktır[34]. IoT ekosisteminin temel bileşenleri şunlardır:

- Cihazlar ve Sensörler: IoT'nin temel yapı taşlarıdır. Bu cihazlar, veri toplamak için çeşitli sensörler kullanmaktadır. Örneğin, akıllı termostatlar sıcaklık verilerini toplamakta, akıllı buzdolapları içindeki yiyecekleri izlemekte ve sağlık izleme cihazları vücut aktivitelerini takip etmektedir.
- Bağlantı: IoT cihazlarının birbirleriyle ve merkezi sistemlerle iletişim kurabilmesi için bağlantı gereklidir. Bu, Wi-Fi, Bluetooth, Zigbee, LoRaWAN ve 5G gibi çeşitli kablosuz teknolojiler aracılığıyla sağlanmaktadır.
- Veri İşleme ve Analitik: Toplanan verilerin anlamlı bilgilere dönüştürülmesi gerekmektedir. Bu işlem, veri analitiği ve makine öğrenmesi algoritmaları kullanılarak gerçekleştirilir. Örneğin, bir akıllı şehirde trafik verileri analiz edilerek trafik ışıklarının optimizasyonu sağlanabilir.
- Kullanıcı Arayüzü: IoT sistemlerinin kullanıcılarla etkileşim kurmasını sağlamaktadır. Bu arayüzler, mobil uygulamalar, web arayüzleri veya sesli asistanlar gibi çeşitli şekillerde olabilir. Kullanıcılar, bu arayüzler aracılığıyla IoT cihazlarını kontrol edebilmekte ve izleyebilmektedir.

---

33 Pranav Rajpurkar, Robin Jia, Percy Liang, "Know what you don't know: Unanswerable questions for SQuAD," *arXiv preprint arXiv:1806.03822* (2018).

34 Charith Perera et al., "Context aware computing for the internet of things: A survey," *IEEE communications surveys & tutorials* 16, no. 1 (2013).

5G ve yapay zekâ entegrasyonu ile IoT'nin daha da gelişeceği öngörülmektedir. IoT'nin sürdürülebilirlik ve çevresel yönetim alanlarında önemli katkılar sağlaması beklenmektedir[35].

D. BÜYÜK VERİ ANALİTİĞİ

Büyük Veri Analitiği, büyük ve karmaşık veri setlerinin analiz edilerek anlamlı bilgiler elde edilmesini sağlayan bir süreçtir. Geleneksel veri işleme yöntemleriyle yönetilemeyen veri hacimleri, yüksek hızda ve çeşitli formatlarda üretilir. Büyük veri analitiği, bu verileri toplamak, depolamak ve analiz etmek için ileri düzey algoritmalar ve yapay zekâ teknikleri kullanmaktadır. Örneğin, makine öğrenmesi ve derin öğrenme yöntemleri, büyük veri analitiği süreçlerinde kritik bir rol oynamaktadır. Sağlık sektöründe, hastaların genetik bilgilerini ve sağlık geçmişlerini analiz ederek kişiselleştirilmiş tedavi yöntemleri geliştirmek için büyük veri analitiğinden yararlanılmaktadır. Finansal sektörde ise, dolandırıcılık tespiti ve risk yönetimi gibi alanlarda büyük veri analitiği kullanılarak daha güvenilir ve etkili çözümler üretilmektedir. Perakende sektöründe büyük veri analitiği ile müşteri davranışları analiz edilerek kişiselleştirilmiş pazarlama stratejileri geliştirilmekte ve müşteri memnuniyeti artırılmaktadır. Büyük veri analitiği, işletmelerin stratejik kararlar almasına yardımcı olarak rekabet avantajı sağlamakta ve inovasyonu desteklemektedir.

E. MAKİNE ÖĞRENMESİ

Makine öğrenmesi, bilgisayar sistemlerinin doğrudan programlanmadan veri üzerinden öğrenme yeteneği kazanmasını sağlayan bir yapay zekâ dalıdır. Bu teknoloji, veri analitiği, model oluşturma ve karar verme süreçlerini otomatikleştirir.

Makine öğrenmesi, bilgisayarların belirli görevleri yerine getirmek için verilerden örüntüler ve ilişkiler öğrenmesini sağlamaktadır. Bu süreç, veri toplama, ön işleme, model seçimi, model eğitimi, model değerlendirmesi ve tahmin yapma gibi adımlardan oluşmaktadır. Makine öğrenmesi, insan müdahalesi olmadan sürekli olarak performansını iyileştirmekte ve yeni bilgileri öğrenmektedir. Bu başlık altında konu özetlenmiş olup, detaylı bilgiler sonraki bölümlerde ele alınacaktır.

---

[35] Rolf H. Weber, "Internet of Things–New security and privacy challenges," *Computer law & security review* 26, no. 1 (2010).

III. MAKİNE ÖĞRENMESİNİN TEMELLERİ

Günümüzde teknoloji, veri, bilgi ve enformasyondan oluşur. Veri ve veriden elde edilen bilgiler, sistemlerle ilgili stratejik kararların temelini oluşturur. Güvenilir, güncel, açık ve zamanında erişilebilen veriler, bu kararların etkili ve amaca uygun olabilmesi için gereklidir. Bu kavramlar hayatımızın her alanında karşımıza çıkıyor ve otomasyon, alışveriş ve sağlık gibi alanlarda hızla artan bir veri sayısı var. Sonuç olarak, işletmelerin yeni oluşturulan veri tabanlarının uygun bir şekilde saklanması artık zorunlu hale gelmiştir.

Verilerin depolanması ve korunması sürecinde, veri ambarlarındaki veri miktarı arttıkça bir dizi sorun ortaya çıkmıştır. Araştırmacılar, veri tabanları ve dosya sistemlerindeki yeniliklerle bu sorunları çözmeye çalışmaktadır. Karar destek süreçlerinde bu kadar büyük veri tabanlarını herhangi bir arayüz kullanmadan analiz etmek ve kullanmak artık mümkün değildir. Bu noktada veri tabanlarından bilgi keşfetme fikri ortaya çıkmış ve veri tabanlarından bilgi keşfi olarak bilinen süreç, verilerden faydalı bilgiler elde etme süreci olarak tanımlanabilmektedir.

Bilgi keşfi yapılabilmesi için verilerin, düzenli bir veri tabanı yapısı olan veri ambarlarında bulunması gerekmektedir. Veri ambarları, hem işlemsel hem de işlemsel olmayan verileri barındırır. Bu yapı, veri tabanında bilgi keşfi için gerekli altyapıyı sağlar. Veri ambarlarının düzenli olması, makine öğrenmesi uygulamalarının gerçekleştirilmesini büyük ölçüde kolaylaştırır.

A. BİR MAKİNE NASIL ÖĞRENİR?

Makine öğrenmesi, bilgisayar sistemlerinin veri aracılığıyla öğrenme kabiliyeti kazanmasını sağlayan bir yapay zekâ dalıdır. Bu süreç, sistemlerin belirli görevleri gerçekleştirmek için verilerden kalıplar ve ilişkiler öğrenmesini içerir. Makine öğrenmesi, çeşitli uygulama alanlarında büyük başarılar elde etmiş olup, sağlık, finans, perakende ve otomotiv gibi birçok sektörde köklü değişikliklere yol açmaktadır[36].

Makine öğrenme süreci, veri toplama, veri ön işleme, model seçimi, model eğitimi, model değerlendirmesi ve tahmin yapma olmak üzere bir dizi adımdan oluşur.

---

[36] Christopher M. Bishop, Nasser M. Nasrabadi, *Pattern recognition and machine learning*, vol. 4 (Springer, 2006).

- Veri Toplama: Makine öğrenme sürecinin ilk adımı veri toplamaktır. Veriler, modelin eğitilmesi ve test edilmesi için gerekli temel bilgileri sağlamaktadır. Bu veriler, sensörler, veri tabanları veya internet üzerindeki veri setleri gibi çeşitli kaynaklardan elde edilebilir[37].

- Veri Ön İşleme: Toplanan veriler genellikle ham ve düzensizdir. Veri ön işleme, verilerin temizlenmesi, eksik verilerin doldurulması ve veri formatlarının birleştirilmesini içermektedir. Bu adım, modelin doğru ve etkili bir şekilde çalışabilmesi için kritik öneme sahiptir[38].

- Model Seçimi: Farklı makine öğrenme algoritmaları, farklı türdeki problemler için uygundur. Örneğin, sınıflandırma problemleri için karar ağaçları veya destek vektör makineleri kullanılabilirken, kümeleme problemleri için k-ortalamalar algoritması tercih edilebilir. Model seçimi, problemin doğasına ve veri setinin özelliklerine bağlıdır[39].

- Model Eğitimi: Seçilen model, eğitim verileri kullanılarak eğitilir. Bu süreçte model, verilerdeki örüntüleri ve ilişkileri öğrenir. Modelin parametreleri, eğitim süreci boyunca ayarlanarak optimize edilir. Bu aşama, modelin veriye dayalı olarak öğrenme yeteneğini kazanmasını sağlar[40].

- Model Değerlendirmesi: Eğitilen model, test verileri kullanılarak değerlendirilir. Modelin performansı, problemin yapısına bağlı olarak farklı metrikler kullanılarak ölçülmektedir. Modelin genel performansını değerlendirmek, modelin gerçek dünya verileriyle ne kadar iyi çalışacağını belirlemek için önemlidir[41].

- Tahmin Yapma: Model başarılı bir şekilde eğitildikten ve değerlendirildikten sonra, yeni veriler üzerinde tahminler yapabilir. Bu tahminler, modelin öğrendiği örüntülere ve ilişkilere dayanmaktadır. Örneğin, bir finansal model, gelecekteki hisse senedi fiyatlarını tahmin edebilir veya bir tıbbi model, hastalık teşhisinde kullanılabilir[42].

---

37 Trevor Hastie et al., *The elements of statistical learning: data mining, inference, and prediction*, vol. 2 (Springer, 2009).

38 Salvador García, Julián Luengo, Francisco Herrera, *Data preprocessing in data mining*, vol. 72 (Springer, 2015).

39 Bishop, Nasrabadi, *Pattern recognition and machine learning*, 4.

40 Ian Goodfellow, Yoshua Bengio, Aaron Courville, *Deep learning* (MIT press, 2016).

41 Hastie et al., *The elements of statistical learning: data mining, inference, and prediction*, 2.

42 Kevin P. Murphy, *Machine learning: a probabilistic perspective* (MIT press, 2012).

Makine öğrenmesi; denetimli öğrenme, denetimsiz öğrenme ve pekiştirmeli öğrenme olmak üzere üç ana kategoriye ayrılır.

i. Denetimli Öğrenme: Bu tür öğrenmede, model, girdi ve çıktı verileriyle eğitilir. Amaç, yeni girdi verileri için doğru çıktıları tahmin etmektir. Örneğin, bir e-posta sınıflandırma sistemi, e-postaları spam veya spam değil olarak sınıflandırabilir.

ii. Denetimsiz Öğrenme: Denetimsiz öğrenmede, model yalnızca girdi verileriyle eğitilir. Amaç, veri setindeki gizli örüntüleri ve yapıları keşfetmektir. Örneğin, müşteri segmentasyonu veya veri kümesindeki aykırı değerlerin tespiti.

iii. Pekiştirmeli Öğrenme: Bu öğrenme türünde, bir ajan, ödüller ve cezalar yoluyla çevresiyle etkileşime girerek öğrenir. Ajan, en yüksek ödülü elde etmek için en iyi eylemleri belirler. Bu tür öğrenme, oyun oynama ve robotik gibi alanlarda yaygın olarak kullanılmaktadır.

Makine öğrenmesi, bilgisayar sistemlerine veri üzerinden öğrenme ve tahmin yapma yeteneğini kazandıran güçlü bir teknolojidir. Veri toplama, ön işleme, model seçimi, model eğitimi, model değerlendirmesi ve tahmin yapma adımlarından oluşan bu süreç, çeşitli sektörlerde büyük başarılar elde edilmesini sağlamıştır. Makine öğrenmesinin temellerinin anlaşılması, bu teknolojinin etkin bir şekilde uygulanabilmesi için kritik öneme sahiptir.

B. MAKİNE ÖĞRENMESİ TÜRLERİ

Makine öğrenmesi, analizlerde sonuç tahmin etmek (öngörme) veya belirli bir sonucu tanımlamak (tanımlama) amacıyla kullanılmaktadır. Bu bağlamda, makine öğrenmesi işlevleri öngörücü ve tanımlayıcı olmak üzere iki ana kategoriye ayrılmaktadır.

Öngörücü işlevlerde amaç, bir nesnenin bir özelliğinin diğer özellikler temel alınarak tahmin edilmesidir. Tahmin edilen değer, sürekli bir sayısal değer olabileceği gibi, kategorik bir değer de olabilir. Bu tahmin sürecinde model, geçmiş verilerle eğitilir. Bu nedenle, bu işlevler denetimli öğrenme yöntemleri olarak adlandırılmaktadır.

Tanımlayıcı görevler ise, makine öğrenmesi teknikleri kullanarak özellikler arasındaki ilişkileri ortaya çıkarmayı amaçlar. Bu süreçte model bir eğitim aşamasından geçmez. Bu sebeple, tanımlayıcı görevler denetimsiz öğrenme olarak bilinmektedir.

1. Denetimli Öğrenme

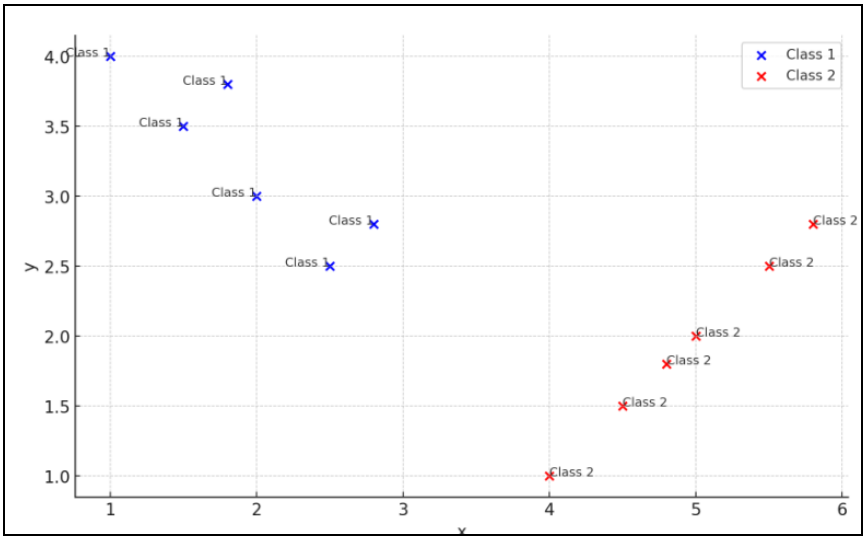
Gelecekteki bir sonucu tahmin etmek için geçmiş verilere dayanan fonksiyonlar kullanılır. Bu süreçte, yeni bir değişkenin niteliklerini analiz etmek ve bu değişkeni belirli bir sınıfa dahil etmek için, geçmişte benzer değişkenlerin hangi sınıflara ait olduğu bilgisi kullanılır. Modellemelerde, olası sonuçları tahmin etmek için gerekli nitelikler ve sonuçlar yer alır. Model oluşturulurken, geçmiş verilerde niteliklerin aldığı değerlere göre edinilen sonuçlar veri olarak kullanılır. Beklenen sonuç, "Evet-Hayır" gibi ikili veya kategorik bir değer ya da sayısal bir değer olabilir.

Tahmin edilen sonuçların performans değeri, tahminin kendisi kadar önemlidir. Genellikle tahmin edilen sonucun doğruluğunu ve güvenilirliğini ölçmek için güven aralığı, olasılık ve doğruluk oranı gibi metrikler kullanılır. Tahmin edici modellerin ana amacı, bilinen sonuçlara dayalı olarak verilerden bir model geliştirip, bu model aracılığıyla sonuçları bilinmeyen veri kümeleri için tahmin etmektir. Tahminleyici fonksiyonların hedefi, veri tabanındaki belirli alanların diğer alanlarla ilişkili olarak tahmin edilmesidir. Tahmin edilecek değişken eğer sayısal (sürekli) bir değişken ise, bu durum bir regresyon problemi olarak adlandırılır. Eğer tahmin edilecek değişken kategorik bir değişken ise, bu bir sınıflama problemidir.

Sınıflandırma ve regresyon problemleri için çok sayıda değişken kullanılabilmektedir. Tahmin edici modellerde, problem; her gözlem için hedef değişkenin değerinin verildiği eğitim veri seti ve problem hakkında önceden sahip olunan bilgileri yansıtan varsayımlar kümesi göz önünde bulundurularak, tahmin edilecek değişkenin alabileceği olası değerin belirlenmesi olarak tanımlanabilir.

a. Sınıflandırma

Sınıflandırma, farklı veri sınıflarını gruplandırabilen bir veri analizi yöntemidir. Bu tür modeller sınıflandırıcı olarak adlandırılır ve kategorik (ayrık, sırasız) sınıf etiketlerini tahmin ederler (Şekil 1). Örneğin, bir sınıflandırma modeli, banka kredi başvurularını güvenli veya riskli olarak kategorize etmek için oluşturulabilir. Bu tür analizler, büyük veri setlerini daha iyi anlamaya katkıda bulunur. Makine öğrenimi, örüntü tanıma ve istatistik alanlarında birçok sınıflandırma yöntemi literatürde önerilmiştir. Çoğu algoritma genellikle küçük veri setleri üzerinde uygulanarak geliştirilmiştir.



Şekil 1. *İki farklı özellik değerlerine göre sınıflandırılmış bir veri*

Son yıllarda, veri madenciliği işlevlerine yönelik daha derinlemesine çalışmalar yapılmış ve büyük miktarda gömülü veriyi işleyebilen ölçeklenebilir sınıflandırma ve tahmin teknikleri geliştirilmiştir. Bu tekniklerin sınıflandırma, sahtekarlık tespiti, pazarlama, performans tahmini, üretim ve tıbbi teşhis gibi çeşitli uygulama alanları bulunmaktadır. Örneğin, bir banka kredi yetkilisi, her kredi başvurusunu "güvenli" veya "riskli" olarak sınıflandırmak için analiz etmelidir. Benzer şekilde, bir teknoloji mağazasının pazarlama müdürü, belirli bir profile sahip bir müşterinin yeni bir bilgisayar satın alıp almayacağını tahmin etmek için sınıflandırma algoritmalarına ihtiyaç duyar. Bir tıbbi araştırmacı ise, meme kanseri verilerini analiz ederek bir hastanın hangi üç özel tedaviden birini alması gerektiğini tahmin etmek isteyebilir.

Sınıflandırma algoritmaları, kredi başvurusu probleminde olduğu gibi "güvenli" veya "riskli" gibi sınıf (kategorik) etiketlerini tahmin eder; pazarlama örneğinde değişkenleri "evet" veya "hayır" olarak sınıflandırmayı amaçlar, hastalık teşhisi örneğinde ise "tedavi A", "tedavi B" veya "tedavi C" olarak sınıflandırır. Bu kategoriler, sıralamada bir anlamı olmayan ayrık değerlerle temsil edilebilir. Örneğin, 1, 2 ve 3 değerleri sırasıyla işlemler A, B ve C'yi temsil edebilir; bu durumda, tedavi sınıflarının nasıl adlandırıldığının bir önemi yoktur43.

43 Jiawei Han, Micheline Kamber, Data Mining, "Concepts and techniques," *Morgan Kaufmann* 340 (2006).

Denetimli öğrenmede, seçilen tekniğe uygun olarak hazırlanan veriler, başlangıç aşamasında temel olarak iki kısma ayrılmakta ve biri modelin eğitilmesi için, diğeri ise modelin performansının test edilmesi için kullanılmaktadır. Modelin eğitilmesi, eğitim verisi üzerinde uygulandıktan sonra, test verisi kullanılarak modelin başarımı belirlenmektedir. Bir modelin performansının test edilmesinde kullanılan en temel tekniklerden biri basit geçerlilik testidir. Bu yöntemde, veri kümesinin yaklaşık %5 ile %33'ü arasındaki bir bölümü test verileri olarak ayrılır ve modelin eğitimi tamamlandıktan sonra kalan veriler üzerinde test işlemi gerçekleştirilir. Bir sınıflandırma tekniğinde, yanlış sınıflanan nesne sayısının tüm nesne sayısına bölünmesi ile hata oranı, doğru sınıflanan nesne sayısının tüm nesne sayısına bölünmesi ile ise doğruluk oranı elde edilir.

Eğer sınırlı miktarda veri mevcutsa, çapraz geçerleme (Cross Validation) testi kullanılabilir. Bu yöntemde, veri kümesi rastgele olarak iki eşit parçaya ayrılır: Öğrenim Kümesi ve Test Kümesi. İlk parça üzerinde model eğitilirken, diğer parça üzerinde test işlemi gerçekleştirilir. Daha sonra parçalar değiştirilerek model tekrar çalıştırılır ve test edilir. Elde edilen iki farklı hata oranının ortalaması kullanılır. Bir diğer doğrulama yöntemi ise, verilerin n gruba ayrıldığı n katlı çapraz geçerleme (N-Fold Cross Validation) yöntemidir. Örneğin; n değerinin 10 olduğu bir çapraz geçerlemede veriler eşit büyüklükte 10 gruba ayrılmaktadır. İlk aşamada birinci grup test için kullanılırken, diğer 9 grup eğitim için kullanılmaktadır. Bu süreç 10 kez tekrarlanarak, her defasında bir grubun test, diğer grupların ise eğitim amacıyla kullanılması ile devam etmektedir. Sonuçta elde edilen on doğruluk ya da hata oranının ortalaması, kurulan modelin tahmini doğruluk ya da hata oranı olarak kabul edilmektedir.

Model oluşturma çalışmaları sonucunda, aynı teknik kullanılarak farklı parametrelerle veya diğer algoritma ve araçlar denenerek çeşitli modeller oluşturulabilir. Hangi tekniğin en uygun olduğunu belirlemek zor olabilir. Bu nedenle, farklı modeller oluşturmak ve doğruluk derecelerine göre en uygun modeli seçmek için birçok deneme gereklidir. Özellikle sınıflandırma çalışmalarında, oluşturulan modellerin performansını değerlendirmek için basit ama önemli bir özet sunan Karmaşıklık Matrisi (Confusion matrix) kullanılır. Karmaşıklık matrisi, bir örneklem setindeki gerçek sınıf etiketi ile tahmin edilen sınıf etiketi sayılarını içerir (Şekil 2).

	Tahmin: Pozitif	Tahmin: Negatif
Gerçek: Pozitif	TP (True Positive)	FN (False Negative)
Gerçek: Negatif	FP (False Positive)	TN (True Negative)

Şekil 2. *Karmaşıklık matrisi*

Doğru pozitif (TP): Modelin doğru bir şekilde pozitif olarak tahmin ettiği durumları,

Yanlış negatif (FN): Modelin yanlış bir şekilde negatif olarak tahmin ettiği, ancak aslında pozitif olan durumları,

Yanlış pozitif (FP): Modelin yanlış bir şekilde pozitif olarak tahmin ettiği, ancak aslında negatif olan durumları,

Doğru negatif (TN): Modelin doğru bir şekilde negatif olarak tahmin ettiği durumları ifade etmektedir.

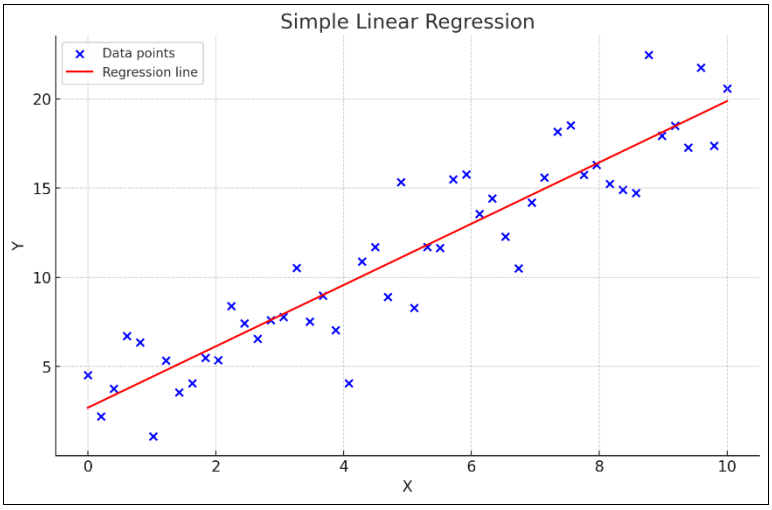
Sınıflandırma modellerinin başarımını değerlendirmek ve karşılaştırmak için karmaşıklık matrisi kullanılarak, doğruluk oranı, hata oranı, kesinlik, anma ve f-ölçüsü gibi metrikler hesaplanabilir.

Makine Öğrenmesi çalışmalarında sınıflandırma problemlerinde yaygın olarak kullanılan başlıca algoritmalar olarak Destek vektör makineleri, karar ağaçları, rastgele ormanlar, naive bayes, k-en yakın komşu, yapay sinir ağları, aşırı gradyan artırma, topluluk öğrenme ve derin öğrenme algoritmaları sayılabilir.

b. Regresyon

Regresyon analizi, bir veya daha fazla değişken arasındaki neden-sonuç ilişkisini belirlemeyi amaçlar. Bu analiz yöntemi, kurulan ilişkiyi kullanarak tahminlerde bulunmak veya öngörüler yapmak için uygulanır. Eğer tahmin aşamasında yalnızca bir değişken kullanılıyorsa bu basit regresyon olarak sınıflandırılır, iki veya daha fazla değişken kullanılıyorsa çoklu regresyon analizi olarak adlandırılır. Buradaki ana amaç, öngörücü değişkenlerin kriter değişken üzerindeki toplam değişime katkısını belirlemek ve bu değişkenlerin doğrusal kombinasyonlarına dayalı olarak kriter değerini tahmin etmektir. Daha genel anlamda, regresyon analizi, neden-sonuç iliş-

kisine sahip iki veya daha fazla değişken arasındaki ilişkiyi belirlemek ve bu ilişkiyi kullanarak ilgili tahminlerde bulunmak için gerçekleştirilir.



Şekil 3. *Basit regresyon modeli*

Bu analiz tekniğinde, bir tek değişken (basit regresyon) veya birden fazla değişken (çoklu regresyon) arasındaki ilişkiyi açıklamak için matematiksel bir model kullanılır ve bu modele "regresyon modeli" denir (Şekil 3). Değişkenler arasındaki desen belirlendikten sonra, bağımsız değişkenlerden elde edilen çıkarımlar kullanılarak bağımlı değişkenin değeri tahmin edilebilir. Regresyon analizinde, açıklanan veya tahmin edilen veri grubu "Bağımlı Değişken" (y) olarak tanımlanır. "Bağımsız Değişken" (x), regresyon modelinde açıklayıcı veri grubu olup, bağımlı değişkenin değerini tahmin etmek için kullanılır. Bağımlı değişkenin bağımsız değişkenle ilişkili olduğu varsayılır. Tek bir bağımsız değişken kullanılarak yapılan regresyon, tek değişkenli regresyon analizi olarak adlandırılır; birden fazla bağımsız değişkenin kullanıldığı regresyon ise çok değişkenli regresyon analizi olarak bilinir.

Tek Değişkenli Regresyon Analizi, bir bağımlı değişken ile bir bağımsız değişken arasındaki ilişkiyi incelerken, Çok Değişkenli Regresyon Analizi, bir bağımlı değişken ile birden fazla bağımsız değişken arasındaki ilişkiyi inceler. Ayrıca, eğer bağımlı ve bağımsız değişkenler arasında eğrisel bir ilişki varsa, bu ilişki doğrusal olmayan regresyon modelleri ile açıklanır.

Regresyon analizinde de modelin performansını değerlendirmek, modelin güvenilirliği ve doğruluğunu belirlemek için kritik öneme sahiptir. Performans ölçümünde kullanılan çeşitli metrikler, modelin ne kadar iyi tahminler yaptığını ve veriye ne kadar iyi uyum sağladığını belirlemeye yardımcı olmaktadır. Bu metrikler, modelin başarımını kantitatif olarak ifade etmekte ve farklı modellerin karşılaştırılmasına olanak tanımaktadır. Kullanılan başlıca metrikler aşağıda verilmiştir.

Ortalama kare hatası (MSE), tahmin edilen değerler ile gerçek değerler arasındaki farkların karelerinin ortalamasını ifade eder. MSE, modelin tahminlerindeki hataların büyüklüğünü ölçer ve Denklem (1.1)'deki gibi hesaplanır:

$$MSE = \frac{1}{n}\sum_{i=1}^{n}(y_i - \hat{y}_i)^2 \qquad \text{Denklem (1.1)}$$

Ortalama mutlak hata (MAE), tahmin edilen değerler ile gerçek değerler arasındaki farkların mutlak değerlerinin ortalamasını ifade eder. MAE, modelin tahminlerindeki hataların büyüklüğünü ölçer ve Denklem (1.2)'deki gibi hesaplanır:

$$MAE = \frac{1}{n}\sum_{i=1}^{n}(|y_i - \hat{y}_i|) \qquad \text{Denklem (1.2)}$$

MAE, MSE'den farklı olarak hataların mutlak değerlerini kullanır, bu da aşırı hataların etkisini azaltır.

R-Kare, modelin açıklama gücünü ölçen bir istatistiktir. Bu metrik, bağımlı değişkendeki toplam varyansın ne kadarının bağımsız değişkenler tarafından açıklandığını gösterir. R^2 değeri 0 ile 1 arasında değişir ve denklem (1.3)'deki hesaplanır:

$$R^2 = 1 - \frac{\sum_{i=1}^{n}(y_i - \hat{y}_i)^2}{\sum_{i=1}^{n}(y_i - \bar{y})^2} \qquad \text{Denklem (1.3)}$$

Burada y_i gerçek değerleri, $\hat{y}_i$ tahmin edilen değerleri ve $\bar{y}$ ise gerçek değerlerin ortalamasını temsil etmektedir. R^2 değerinin 1'e yakın olması, modelin bağımlı değişkendeki varyansın büyük bir kısmını açıkladığını göstermektedir.

c. Topluluk Öğrenme

Topluluk öğrenmesi, denetimli öğrenme algoritmaları arasında yer alır ve eğitilebilir ve öngörücü özellikleriyle dikkat çeker. Topluluk öğrenme yöntemi, diğer öğrenme algoritmaları gibi tek bir hipotezi temsil eder; ancak, diğer yöntemlerden farklı olarak, birden fazla sınıflandırıcı yöntemden oluşur. Topluluk öğrenme ile oluşturulan hipotez, onu oluşturan sınıflandırıcıların hipotezlerini tam olarak yansıtmak zorunda değildir. Bu nedenle, topluluk öğrenme algoritmaları, diğer makine öğrenme algoritmalarına kıyasla daha esnek tahminler üretebilir. Bu esneklik, teorik olarak, eğitim verilerinin tek bir modelde daha hızlı öğrenilmesini sağlar. Ancak, pratikte bazı topluluk öğrenme teknikleri (özellikle torbalama tekniği) eğitim verilerinin aşırı uyum gibi sorunlara yatkın olabilir[44].

Genel olarak, topluluk öğrenme yöntemleri, bileşen modeller arasında anlamlı bir çeşitlilik olduğunda daha iyi performans gösterir. Bu nedenle, birçok topluluk öğrenme yöntemi, birleştirilen modeller arasında çeşitliliği teşvik etmeyi amaçlar. Belki de beklenmedik bir şekilde, daha rastgele algoritmalar (örneğin, rastgele karar ağaçları), daha deterministik algoritmalara (örneğin, entropi azaltıcı karar ağaçları) göre daha güçlü bir öğrenme yapısı oluşturabilir[45].

Topluluk öğrenme yöntemlerinin başarısı, birleştirilen sınıflayıcıların bağımsız ve çeşitliliğe sahip olmasına dayanmaktadır. Bu çeşitlilik, model kombinasyonlarının farklı hata türlerini telafi etmesine olanak tanımakta, böylece genel tahmin doğruluğunu artırmaktadır. Torbalama, arttırma ve istifleme gibi yaygın topluluk öğrenimi teknikleri, bu çeşitliliği sağlamak ve genel model performansını iyileştirmek amacıyla geliştirilmiştir. Örneğin, torbalama, veri örneklemeleri üzerinde birden fazla model eğiterek aşırı öğrenmeyi azaltmayı amaçlarken, arttırma, ardışık modellerin hatalarını düzelterek doğruluğu artırır.

---

44 Leo Breiman, "Bagging Predictors," *Machine Learning* 24, no. 2 (1996), https://doi.org/10.1007/bf00058655.

45 Breiman, "Bagging Predictors."

2. Denetimsiz Öğrenme

Bazı uygulama senaryolarında ve gerçek hayat problemlerinde, bağımlı değişken ya da sınıf etiketi niteliği bulunmamaktadır. Daha açık bir ifadeyle, veri kümesi içerisinde tahmin edilmesi gereken bir veri alanı yoktur. Bu tür durumlarda, denetimsiz bir öğrenme yöntemi kullanılmalıdır. Denetimsiz öğrenme, aykırılık tespiti, kümeleme ve birliktelik kuralları madenciliğinde yaygın olarak kullanılmaktadır.

Denetimsiz aykırılık tespiti yöntemleri belirli bir varsayıma dayanmaktadır: Normal nesneler belirli bir "kümeleşme" eğilimi gösterirler. Diğer bir ifadeyle, denetimsiz bir aykırılık tespiti yöntemi, normal nesnelerin aykırı kalıplardan daha sık izlediği desenleri belirlemeye çalışmaktadır. Normal nesnelerin, yüksek benzerlik gösteren bir grupta yer alması gerekmemektedir. Bunun yerine, belirgin özelliklere sahip çeşitli gruplar oluşturabilirler. Ancak, normal nesnelerin bu gruplarından herhangi birinin dışında kalan özellikler taşıyan bir çıkarımın olması beklenmektedir.

Denetimsiz yöntemler, bu tür aykırı değerleri etkili bir şekilde tespit edemeyebilir. Bazı uygulamalarda, normal nesneler çeşitli şekillerde dağıtılmış olup, birçok nesne belirgin desenler takip etmez. Örneğin, bazı izinsiz giriş tespiti ve bilgisayar virüsü tespiti problemlerinde, normal aktiviteler oldukça çeşitlidir ve çoğu yüksek kaliteli kümelere dahil olmaz. Bu tür senaryolarda, denetimsiz yöntemler yanlış pozitif oranına sahip olabilir; yani, birçok normal nesneyi yanlışlıkla anormal olarak etiketleyebilir ve gerçek aykırı değerleri tespit edemeyebilir. Bu tür durumlarda, saldırılar ve virüsler arasında yüksek benzerlik gösteren nesneleri (örneğin, hedef sistemlerde önemli kaynaklara saldırma eğilimleri) modellemek için denetimli yöntemlerin kullanılması daha etkili olabilir.

Birçok kümeleme yöntemi, denetimsiz öğrenme yöntemleri olarak uyarlanabilir. Bu bağlamda yaygın yaklaşım, önce kümeleri belirlemek ve ardından bu kümelere ait olmayan nesneleri aykırı değerler olarak tespit etmektir. Ancak, bu yöntemlerin iki ana problemi vardır. Birincisi, herhangi bir kümeye ait olmayan bir veri nesnesi, aykırı bir değerden ziyade gürültü verisi olabilir. İkincisi, önce kümeleri belirlemek ve ardından aykırı değerleri tespit etmek, pahalı ve zaman alıcı bir süreç olabilir.

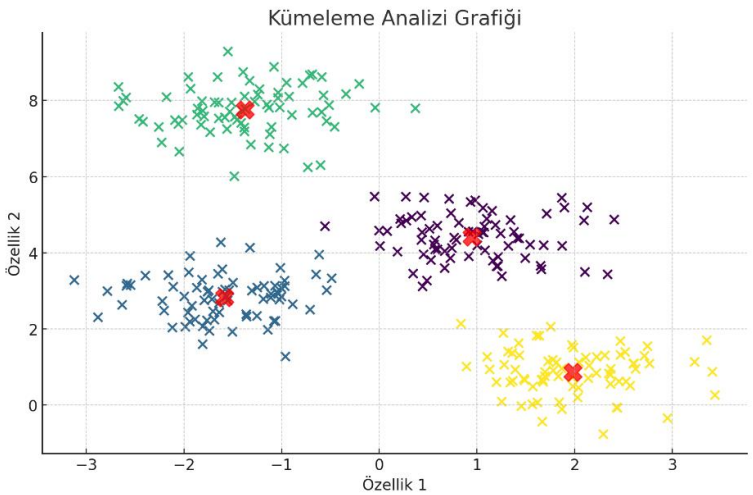
Genellikle, aykırı değerlerin normal nesnelerden daha az sapma gösterdiği varsayılır. Normal nesneler belirlenmeden önce büyük bir veri kümesini işlemek pratik olmayabilir. Literatürde, belirgin ve kesin kümeler bulma-

dan doğrudan aykırı değerleri tespit etmek için denetimsiz aykırı değer tespit yöntemleri geliştirilmiştir[46].

a. Kümeleme (Clustering)

Makine öğreniminde kullanılan önemli tekniklerden biri kümeleme analizidir. Kümeleme analizinin ana amacı, nesneleri temel özelliklerini dikkate alarak gruplara ayırmak ve böylece araştırmacıya özetleyici bilgi sağlamaktır. Kümeleme analizi, araştırmada gözlemlenen birimlerin tüm ölçülen değişkenler üzerindeki değerlerini hesaplayarak benzer birimleri aynı küme içinde sınıflandırır. Analiz, oluşturulacak kümeler ve gruplar üzerinde yoğunlaşır ve ortaya çıkan kümelerin kendi içinde homojen, kendi aralarında ise heterojen bir yapı sergilemesi beklenir.

Kümeleme analizi, birim ve bu birimlere ait değişkenlerin sınıflamaları hakkında kesin bilginin bulunmadığı bir popülasyondan alınan n birimin, p değişkene ilişkin gözlem sonuçları ile ilgilenmektedir. Homojen nesneleri bir araya getirerek heterojen gruplar oluşturma sürecinde, birimler hiyerarşik bir düzene sokulur. Bu sınıflandırma yöntemi, gözlem sonuçlarının minimum bilgi kaybı ile bir araya toplanmasını sağlamaktadır. Şekil 4'te görüldüğü üzere, ortaya çıkacak kümelerin kendi içlerinde homojen, kendi aralarında ise heterojen bir yapıya sahip olmaları beklenmektedir.



Şekil 4. *Kümeleme analizi grafiği örneği*

[46] Han, Kamber, Mining, "Concepts and techniques."

Kümeleme analizinin ana amacı, gözlemlenen bireyler veya nesneler arasındaki benzerlikleri veya uzaklıkları tespit etmektir. Benzerlik, iki nesne veya iki özellik arasındaki ilişkinin gücü olarak açıklanır. Bu nicel değer, ölçeğe veya veri türüne bağlı olarak farklı şekillerde elde edilir. Uzaklık ise, iki nesne arasındaki farkları ölçer ve bir zıtlık veya uyumsuzluk ölçüsüdür. Benzerlik ve uzaklık ölçümleri, gözlemlerin birbirinden ayrılmasını sağlar ve böylece gözlemler gruplara ayrılır. Uzaklık ölçümü, verilerin nicel veya karma veri olup olmamasına bağlı olarak farklılık gösterir. Nicel veriler için uzaklık ölçümü, çeşitli matematiksel mesafe hesaplama yöntemleri ile yapılır.

Kümeleme modellerinde kullanılan başlıca teknikler olarak; Bölme Yöntemleri, Izgara Tabanlı Yöntemler, Hiyerarşik Yöntemler, Yoğunluk Tabanlı Yöntemler örnek gösterilebilir.

b. Birliktelik Analizi

Birliktelik kuralları madenciliği, 1993 yılında Agrawal ve arkadaşları tarafından önerilmiştir[47]. Bağlantı kuralları, büyük veri setleri arasındaki ilişkileri çıkaran ve nesnelerin birlikte gerçekleşme olasılıklarını analiz eden bir denetimsiz öğrenme yöntemidir. Bağlantı kuralları; pazarlama, eğitim, sağlık, ekonomi, telekomünikasyon, e-ticaret ve bilişim gibi birçok alanda yaygın olarak kullanılmaktadır[48].

Birliktelik kuralları için verilen en yaygın örnek çocuk bezi ve bira örneğidir. Walmart ismindeki süpermarket zincirinin yaptığı analiz şu şekildedir; "Yeni çocuk sahibi olan ebeveynler eğlenmek için vakit bulamayıp Cuma günlerini partiye gitmek yerine eve bira alarak evde geçirmek zorunda kalıyorlar. Bu yüzden bebek bezi alan baba çoğunlukla yanında bir de bira alır". Bu analiz, müşteri işlem verileri ile de doğrulanmaktadır. Bu doğrultuda, bir market bebek bezi ve birayı yakın yerlere koyarak çapraz satışlarını arttırmayı hedefleyebilmektedir[49].

---

47 Mohammed J. Zaki, "Scalable Algorithms for Association Mining," *Ieee Transactions on Knowledge and Data Engineering* 12, no. 3 (2000), https://doi.org/10.1109/69.846291.

48 Manpreet Kaur, Shivani Kang, "Market Basket Analysis: Identify the Changing Trends of Market Data Using Association Rule Mining," *Procedia Computer Science* 85 (2016), https://doi.org/10.1016/j.procs.2016.05.180.

49 Marcin Szymkowiak, Tomasz Klimanek, and Tomasz Józefowski, "Applying Market Basket Analysis to Official Statistical Data," *Econometrics* 22, no. 1 (2018), https://doi.org/10.15611/eada.2018.1.03.

Benzer şekilde, internet alışverişlerinde de birliktelik analizi kullanılmaktadır. Müşterinin satın aldığı bir üründen yola çıkarak, o ürünle birlikte satın alınma olasılığı en yüksek olan tamamlayıcı ürünler önerilebilmektedir. Bu tür öneriler, müşteri deneyimini artırmak, ürün önerilerini kişiselleştirmek ve satışları teşvik etmek için kullanılabilmektedir[50].

Birliktelik analizi, pazar sepeti analizi olarak da bilinir ve çeşitli sektörlerde kullanılmaktadır. Örneğin, tıbbi veriler üzerinde yapılan birliktelik analizi çalışmaları, endüstriler için değerli bilgiler sağlamaktadır[51]. Ayrıca, çoklu mağaza ortamlarında pazar sepeti analizi, satın alma alışkanlıklarını anlamak ve müşteri davranışlarını analiz etmek için kullanılmaktadır.

Sonuç olarak, birliktelik analizi, veri madenciliği alanında önemli bir araç olup, çeşitli sektörlerde kullanılmaktadır. Bu analiz yöntemi, ilişkileri belirlemek, satış stratejilerini en iyilemek, müşteri davranışlarını anlamak ve işletmelerin karar alma süreçlerine rehberlik etmek için etkili bir araç olarak karşımıza çıkmaktadır. Birliktelik analizi modellerinde kullanılan başlıca yöntemler; Appriori, FP-Ağacı ve Eclat algoritmalarıdır.

IV. POPÜLER MAKİNE ÖĞRENİMİ ALGORİTMALARI

A. KARAR AĞAÇLARI

Karar Ağaçları (DT), sınıflandırma problemlerinin çözümünde yaygın olarak kullanılan denetimli öğrenme algoritmalarından biridir. Karar ağaçları, eğitim verilerinden öğrenip kendilerini eğitmekte ve yeni verilerin sınıf etiketini tahmin etmektedir. Karar ağaçları hem kategorik hem de sürekli girdi ve çıktı değişkenleri üzerinde çalışmaktadır. Tümevarımsal çıkarım için en yaygın kullanılan ve pratik yöntemlerden biridir[52].

Karar ağaçları, kök düğümden başlayarak, dallara ve yaprak düğümlere doğru ilerleyen bir yapı ile veriyi bölmektedir. Her düğüm, bir özelliğe dayalı olarak veri kümesini iki veya daha fazla alt kümeye ayırmaktadır. Bu süreç, tüm veriler belirli bir kritere göre ayrılana kadar veya belirli bir

50 Srinivas Doddi et al., "Discovery of Association Rules in Medical Data," *Medical Informatics and the Internet in Medicine* 26, no. 1 (2001), https://doi.org/10.1080/14639230010028786.

51 Yen-Liang Chen et al., "Market Basket Analysis in a Multiple Store Environment," *Decision Support Systems* 40, no. 2 (2005), https://doi.org/10.1016/j.dss.2004.04.009.

52 Yunhai Wang et al., "Efficient volume exploration using the gaussian mixture model," *IEEE Transactions on Visualization and Computer Graphics* 17, no. 11 (2011)..

durdurma koşuluna ulaşılana kadar devam etmektedir. Karar ağaçlarının inşasında kullanılan temel algoritmalar arasında ID3, C4.5 ve CART (Sınıflandırma ve Regresyon Ağaçları) bulunmaktadır[53]. Bu bölümde, CART algoritması üzerinde durulmaktadır. CART algoritması, bir karar ağacı oluşturmak için Gini indeksini kullanmaktadır. Bu nedenle, Gini algoritması olarak da adlandırılabilir. CART, her karar düğümünden ağacı iki dala bölme prensibine dayanmaktadır. Ebeveyn düğümü, Gini indeksi değeri göz önünde bulundurularak belirlenmektedir. Gini indeksi değeri, veri setindeki nesnelerin oranı olarak tanımlanabilir. İki nesnenin Gini değeri aynı ise, sonuç dağılımı da aynıdır[54].

Eğitim veri kümesi D olsun, Gini değeri Denklem (1.4)'deki şekilde elde edilir [55].

$$\text{Gini}\ (D) = 1 - \sum_{i=1}^{t} \left[\frac{C_{i,D}}{D}\right]^2 \qquad (1.4)$$

Denklem (1.4)'te, t sınıf etiket sayısını belirtmekte ve $C_{i,D}$ ise veri kümesinde i sınıfına ait olan ögelerin sayısını ifade etmektedir. Eğer veri kümesinde ikili bir bölünme varsa (binary split), her bir özellik A için D_1 ve D_2 olarak adlandırılan iki farklı Gini indeksi olacaktır (Denklem 1.5).

$$\text{Gini}_{A}(D) = \frac{|D_1|}{|D|}\text{Gini}\ (D_1) + \frac{|D_2|}{|D|}\text{Gini}\ (D_2) \qquad (1.5)$$

En yüksek safsızlık azalmış olan özellik, bölme özelliği (bir sonraki ebeveyn düğümü) olarak seçilir. Safsızlık azalması, Denklem (1.6)'dan elde edilir.

$$\Delta\text{Gini}\ (A) = \text{Gini}\ (D) - \text{Gini}_{A}(D) \qquad (1.6)$$

53 J. Ross Quinlan, "Induction of decision trees," *Machine learning* 1, no. 1 (1986).

54 Leszek Rutkowski et al., "The CART decision tree for mining data streams," *Information Sciences* 266 (2014)..

55 Jiawei Han, Jian Pei, Micheline Kamber, *Data mining: concepts and techniques* (Elsevier, 2011).

B. K-EN YAKIN KOMŞU ALGORİTMASI

k-En Yakın Komşu (k-NN) algoritması, denetimli öğrenme yöntemleri arasında yer alan ve özellikle sınıflandırma ve regresyon problemlerinin çözümünde yaygın olarak kullanılan bir algoritmadır. Temel prensibi, yeni bir veri noktasının sınıfını veya değerini belirlerken, eğitim veri kümesindeki en yakın k komşusunu dikkate alarak karar vermektir.

k-NN algoritmasının işleyişi şu adımlardan oluşur:

- Mesafe Hesaplama: Yeni bir veri noktası ile eğitim veri kümesindeki tüm noktalar arasındaki mesafeler hesaplanmaktadır. Bu mesafeler genellikle Öklid uzaklığı ile hesaplanır, ancak Manhattan veya Minkowski gibi diğer mesafe ölçütleri de kullanılabilir.
- Komşuların Seçimi: Hesaplanan mesafelere göre, yeni veri noktasına en yakın k komşu seçilmektedir.
- Sınıf veya Değer Atama: Seçilen k komşunun sınıfları veya değerleri incelenir. Sınıflandırma problemlerinde, yeni veri noktası, en yakın komşularının çoğunluk sınıfına atanır. Regresyon problemlerinde ise, k komşunun ortalama değeri yeni veri noktasının tahmini değeri olarak belirlenir.

k değeri, k-NN algoritmasının performansını önemli ölçüde etkileyen bir parametredir. Çok küçük k değerleri, modelin gürültüye duyarlı olmasına ve aşırı uyum göstermesine neden olabilirken, çok büyük k değerleri ise modelin fazla genelleştirme yapmasına ve yetersiz uyum göstermesine yol açabilmektedir. Bu nedenle, k değeri genellikle çapraz doğrulama yöntemi ile belirlenmektedir.

k-En Yakın Komşu algoritması, basitliği ve esnekliği ile öne çıkan, ancak büyük veri kümelerinde hesaplama ve depolama maliyetleri gibi dezavantajları bulunan etkili bir yöntemdir. Uygun k değerinin seçilmesi ve veri ön işleme adımlarının doğru bir şekilde uygulanması, algoritmanın performansını önemli ölçüde artırabilmektedir. Bu nedenle, k-NN algoritması, makine öğrenmesi ve veri madenciliği projelerinde sıkça tercih edilen yöntemlerden biridir.

C. K-ORTALAMALAR ALGORİTMASI

K-ortalamalar yöntemi, veri setini her veri noktasının yalnızca bir gruba ait olduğu k benzersiz ve örtüşmeyen alt gruplara (kümelere) bölmeye çalışan yinelemeli bir tekniktir. Bu yöntem, küme içi veri noktalarını mümkün olduğunca benzer hale getirirken, kümeler arasındaki farklılıkları en büyüklemeyi amaçlamaktadır. Veri noktaları, veri noktaları ile kümenin ağırlık merkezi arasındaki karesi alınmış mesafenin toplamı (o kümeye ait tüm veri noktalarının aritmetik ortalaması) en küçük olacak şekilde kümelere tahsis edilmektedir. Aynı küme içindeki veri noktaları arasındaki varyans ne kadar azsa, küme o kadar homojendir[56]. Bilinen bir k değeri için k-ortalamalar kümeleme algoritmasının dört aşaması aşağıda açıklanmaktadır:

- **Başlangıç Küme Merkezlerinin Belirlenmesi:** İlk adımda k tane küme merkezi rastgele seçilmektedir. Bu merkezler, başlangıçta mevcut veri noktalarından seçilebileceği gibi rastgele olarak da belirlenebilir.
- **Kümelerin Oluşturulması:** Her veri noktası, en yakın merkez ile olan mesafesine göre bir kümeye atanır. Bu mesafe genellikle Öklid uzaklığı kullanılarak hesaplanır.
- **Merkezlerin Güncellenmesi:** Her kümenin merkezi, o kümeye atanmış veri noktalarının aritmetik ortalaması alınarak yeniden hesaplanır. Bu, mevcut merkezlerin yeni veri noktalarıyla uyumlu hale getirilmesini sağlamaktadır.
- **Yineleme ve Sonlandırma:** Veri noktalarının kümeleri ve merkezlerin güncellenmesi işlemleri, merkezlerin artık değişmediği veya belirli bir sayıda yineleme tamamlandığı ana kadar tekrar edilir.

K-ortalamalar yöntemi, basit ve etkili bir kümeleme algoritmasıdır. Bununla birlikte, başlangıç noktalarına duyarlılığı ve yerel minimumlara takılma riski gibi bazı dezavantajları bulunmaktadır.

D. YAPAY SİNİR AĞLARI

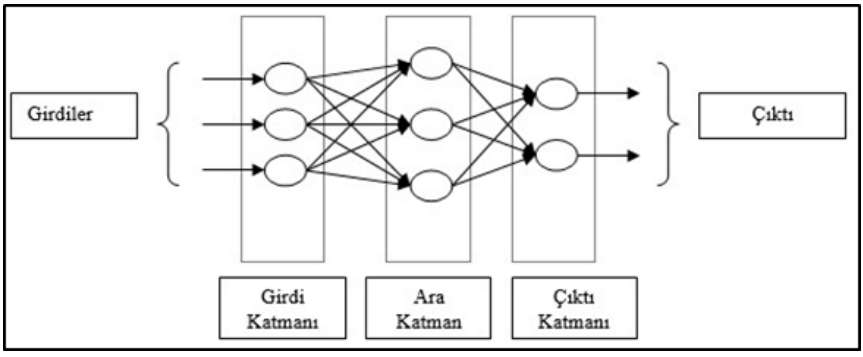
Yapay Sinir Ağları (YSA), insan sinir sisteminin mekanizmalarından ve düşünebilme yeteneğinden esinlenerek geliştirilmiş bir makine öğrenmesi

[56] Kristina P Sinaga, Miin-Shen Yang, "Unsupervised K-means clustering algorithm," *IEEE access* 8 (2020).

tekniğidir. YSA'lar, karmaşık öğrenme kapasiteleri sayesinde, geleneksel makine öğrenmesi yöntemleri ile çözümlenmesi zor veya imkânsız olan problemlere çözüm sunabilmektedir. Öğrenme yetenekleri sayesinde, bilinen örnekleri kullanarak daha önce karşılaşılmamış durumlar hakkında genelleme yapabilme kabiliyetine sahiptirler[57].

Yapay Sinir Ağları, sadece sayısal verilerle çalışmakta olup, geçmiş verilerden öğrenerek gerçekleşmemiş olaylara dair tahminlerde bulunabilmektedir. Bu özellikleri sayesinde, YSA'lar mühendislik, sağlık, sanayi gibi pek çok alanda yaygın olarak kullanılmaktadır. Örneğin, arıza tespiti ve önceden arıza öngörüsü gibi uygulamalarda etkin bir şekilde kullanılmaktadırlar[58]. YSA uygulamaları genellikle tahmin, sınıflandırma ve veri kümeleme işlemlerinde kullanılmaktadır.

Yapay Sinir Ağlarının genel işlem süreci Şekil 5'te gösterildiği gibidir. Girdi verileri, gizli katmanlardaki nöronlara iletilmeden önce ağırlıkları ile çarpılır ve ardından belirlenen aktivasyon fonksiyonları uygulanır. Bu işlemler sonucunda elde edilen veriler, bir sonraki katman için girdi verileri olarak kullanılır ve güncellenen ağırlıklar aracılığıyla çıktı verileri oluşturulur.



Şekil 5. *Örnek bir yapay sinir ağı mimarisi*

57 Onursal Çetin, Feyzullah Temurtaş, Şenol Gülgönül, "An Application of Multilayer Neural Network on Hepatitis Disease Diagnosis Using Approximations of Sigmoid Activation Function," *Dicle Medical Journal / Dicle Tip Dergisi* 42, no. 2 (2015), https://doi.org/10.5798/diclemedj.0921.2015.02.0550.

58 Meltem Karaatli et al., "Yapay Sinir Ağları Yöntemi İle Otomobil Satış Tahmini," *International Journal of Management Economics and Business* 8, no. 17 (2012), https://doi.org/10.11122/ijmeb.2012.8.17.290.

YSA'ların bu karmaşık işlem yetenekleri ve öğrenme kapasiteleri, onları geniş bir uygulama yelpazesinde vazgeçilmez kılmaktadır. Endüstri 4.0 ile birlikte birçok üretme probleminde, tıbbi teşhis, finansal tahmin ve daha birçok alanda YSA'lar, insan karar verme süreçlerini taklit ederek, karmaşık problemleri çözmede önemli bir rol oynamaktadır.

E. APRIORI ALGORİTMASI

Veri madenciliği, büyük veri kümelerinden anlamlı bilgiler çıkarma sürecidir ve bu sürecin önemli bir parçası birliktelik kuralları madenciliğidir. Apriori algoritması, Rakesh Agrawal ve Ramakrishnan Srikant tarafından 1994 yılında geliştirilmiştir. Bu algoritma, genellikle pazar sepeti analizinde kullanılmakta ve belirli ürünlerin birlikte satın alınma olasılıklarını belirlemektedir. Özellikle perakende sektörü gibi büyük veri yığınlarına sahip alanlarda, müşterilerin satın alma davranışlarını analiz etmek için birliktelik kuralları kullanılmaktadır. Bu alanda en yaygın kullanılan algoritmaların başında Apriori algoritması gelmektedir [59].

Apriori algoritması, her bir işlemde müşterinin ziyaretinde satın aldığı öğeler arasındaki ilişkileri belirlemek için kullanılmaktadır. Bu algoritma, büyük veri kümelerinde sıkça tekrarlanan öğe gruplarını tespit ederek ilişkilendirme kurallarını çıkarır. Bu tür analizler, perakende sektöründe müşteri tercihlerini anlamak, ürün ve mağaza yerleşimini optimize etmek ve satış stratejilerini geliştirmek için önemli bir araç haline gelmiştir[60].

Perakende sektöründe, büyük veri analitiği ve ilişkilendirme kuralları, günlük operasyonların ve tedarik zinciri uygulamalarının iyileştirilmesinde özellikle faydalıdır[61]. Bu teknolojiler, müşteri davranışlarını anlamak, trendleri öngörmek ve pazarlama stratejilerini geliştirmek için önemli bir rol oynamaktadır[62]. Ayrıca, bu analizlerde dış verilerin kullanımı da önem-

---

59 Rakesh Agrawal, Tomasz Imieliński, Arun Swami, "Mining Association Rules Between Sets of Items in Large Databases," (1993), https://doi.org/10.1145/170035.170072.

60 Tom Joe, R. Sreejith, Kannan Sekar, "Optimization of Store Layout Using Market Basket Analysis," *International Journal of Recent Technology and Engineering* 8, no. 2 (2019), https://doi.org/10.35940/ijrte.b2207.078219.

61 Sadia Shaikh, Faisal Sultan, Muhammad Asim, "Assortment on the Bases of Big-Data Analytics: A Quantitative Analysis on Retail Industry," *Journal of Independent Studies and Research Management Social Science and Economics* 19, no. 2 (2021), https://doi.org/10.31384/jisrmsse/2021.19.2.9.

62 Mustafa A. Raji, "Real-Time Data Analytics in Retail: A Review of USA and Global Practices," *GSC Advanced Research and Reviews* 18, no. 3 (2024), https://doi.org/10.30574/gscarr.2024.18.3.0089.

lidir. Örneğin, rakiplerin fiyatları ve hava koşulları gibi dış faktörlerin talep tahmini ve fiyatlandırmada kullanılması mümkündür [63].

Apriori algoritması gibi birliktelik kuralları madenciliği teknikleri, perakende sektöründe müşteri ilişkileri yönetimi için de önemli bir rol oynamaktadır. Müşteri şikayetlerinin yönetilmesi, başarılı işletmeler için müşteri ihtiyaçlarını ve davranışları yönetmek açısından kritik bir gerekliliktir[64] (Ngai et al., 2009). Bu tür analizler, müşteri memnuniyetini artırmak, sadakati güçlendirmek ve rekabet avantajı sağlamak için kullanılmaktadır.

Büyük veri analitiği ve ilişkilendirme kuralları, perakende sektöründe mağaza düzenlemesinden ürün seçimine kadar birçok alanda kullanılmaktadır. Mağaza düzeni, müşterileri çekmek ve alışveriş deneyimini iyileştirmek için önemli bir faktördür. Ayrıca, optimal ürün seçimi için veri madenciliği çerçeveleri geliştirilmiştir, bu da perakende süpermarket verilerinde etkili bir şekilde kullanılmaktadır[65].

Perakende sektöründe, büyük veri ve ilişkilendirme kurallarıyla yapılan analizler, şirketlerin karar alma süreçlerini desteklemekte ve stratejik yönlendirmeler yapmalarına yardımcı olmaktadır. Bu analizler, gizli ilişkileri ortaya çıkararak işletmelerin rekabet avantajı elde etmelerine yardımcı olur[66]. Ayrıca, yapay zekâ ve makine öğrenimi algoritmalarının entegrasyonu, perakende sektöründe gelecekteki pazar trendlerini tahmin etme yeteneğini artırmaktadır.

Apriori algoritmasına ilişkin bazı temel kavramlar şu şekildedir:

Destek (Support): Bir ürün kombinasyonunun (örneğin, süt ve ekmek) veri kümesindeki tüm alışveriş sepetlerinde görülme sıklığıdır. Matematiksel olarak, destek Denklem (1.7)'deki şekilde ifade edilir:

---

63 Emel Aktaş, Yuwei Meng, "An Exploration of Big Data Practices in Retail Sector," *Logistics* 1, no. 2 (2017), https://doi.org/10.3390/logistics1020012.

64 Eric W. Ngai, Xiu Li, Dennis Chau, "Application of Data Mining Techniques in Customer Relationship Management: A Literature Review and Classification," *Expert Systems With Applications* 36, no. 2 (2009), https://doi.org/10.1016/j.eswa.2008.02.021.

65 Tom Brijs et al., "A Data Mining Framework for Optimal Product Selection in Retail Supermarket Data," (2000), https://doi.org/10.1145/347090.347156.

66 Monerah Alawadh, "THAPE: A Tunable Hybrid Associative Predictive Engine Approach for Enhancing Rule Interpretability in Association Rule Learning for the Retail Sector," *Computers Materials & Continua* 0, no. 0 (2024), https://doi.org/10.32604/cmc.2024.048762.

$$\text{Support (A)} = \frac{\text{A'nın görülme sayısı}}{\text{Toplam işlem sayısı}} \qquad (1.7)$$

Güven (Confidence): Bir ürün kombinasyonunun diğer bir ürünle birlikte görülme olasılığıdır. Örneğin, A ürününü satın alan müşterilerin B ürününü de satın alma olasılığı. Matematiksel olarak Denklem (1.8)'deki şekilde ifade edilir:

$$\text{Confidence } (A \rightarrow B) = \frac{\text{Support } (A \cup B)}{\text{Support (A)}} \qquad (1.8)$$

Kaldıraç (Lift): İki ürünün birlikte satın alınma olasılığının, bağımsız olarak satın alınma olasılıklarına göre artışını gösterir ve Denklem (1.9)'daki gibi hesaplanır:

$$\text{Lift } (A \rightarrow B) = \frac{\text{Support } (A \cup B)}{\text{Support (A)x Support(B)}} \qquad (1.9)$$

Apriori algoritması, aşağıdaki adımlarla uygulanabilir:

- **Birinci Adım:** Tüm veri kümesi üzerinde tekil ürünlerin destek değerleri hesaplanır ve belirli bir destek eşiğinin (minimum support) üzerinde olanlar seçilir.
- **İkinci Adım:** İlk adımda seçilen ürünler kombinasyonlar oluşturularak destek değerleri tekrar hesaplanır. Yine, destek eşiğinin üzerinde olan kombinasyonlar seçilir.
- **Üçüncü Adım:** Bu süreç, destek eşiğini geçen tüm kombinasyonlar bulunana kadar devam eder. Her bir adımda, bir önceki adımda seçilen kombinasyonlar genişletilir.
- **Dördüncü Adım:** Elde edilen tüm kombinasyonlar üzerinden güven ve kaldıraç değerleri hesaplanarak, anlamlı ilişkilendirme kuralları oluşturulur.

KAYNAKÇA

Abou Allaban, Anas, Maozhen Wang, Taşkın Padır. "A Systematic Review of Robotics Research in Support of in-Home Care for Older Adults." Information 11, no. 2 (2020): 75.

Agrawal, Rakesh, Tomasz Imieliński, Arun Swami. "Mining Association Rules between Sets of Items in Large Databases." (1993). https://doi.org/10.1145/170035.170072.

Akalin, Betül, Ülkü Veranyurt. "Sağlık Hizmetleri Ve Yönetiminde Yapay Zekâ." Acta Infologica 5, no. 1 (2021): 231-40. https://doi.org/10.26650/acin.750857.

Akkaya, Bülent, Ayşegül T. Özkan, Hasan Özkan. "Yapay Zekâ Kaygı (Yzk) Ölçeği: Türkçeye Uyarlama, Geçerlik Ve Güvenirlik Çalışması." Alanya Akademik Bakış 5, no. 2 (2021): 1125-46. https://doi.org/10.29023/alanyaakademik.833668.

Aktaş, Emel, Yuwei Meng. "An Exploration of Big Data Practices in Retail Sector." Logistics 1, no. 2 (2017): 12. https://doi.org/10.3390/logistics1020012.

Alawadh, Monerah. "Thape: A Tunable Hybrid Associative Predictive Engine Approach for Enhancing Rule Interpretability in Association Rule Learning for the Retail Sector." Computers Materials & Continua 0, no. 0 (2024): 1-10. https://doi.org/10.32604/cmc.2024.048762.

Başkaya, gt, Fatma, Hacer Karacan. "The Impact of Artificial Intelligence-Based Systems on Personal Data Privacy: A Study on Chatbots." Bilişim Teknolojileri Dergisi 15, no. 4 (2022): 481-91. https://doi.org/10.17671/gazibtd.1053803.

Bellingham, James G., Kanna Rajan. "Robotics in Remote and Hostile Environments." science 318, no. 5853 (2007): 1098-102.

Bishop, Christopher M., Nasser M. Nasrabadi. Pattern Recognition and Machine Learning. Vol. 4: Springer, 2006.

Blackmore, Simon, Bill Stout, Maohua Wang, Boris Runov. "Robotic Agriculture-the Future of Agricultural Mechanisation?". In Precision Agriculture '05, 621-28: Wageningen Academic, 2005.

Breiman, Leo. "Bagging Predictors." Machine Learning 24, no. 2 (1996): 123-40. https://doi.org/10.1007/bf00058655.

Brijs, Tom, Bart Goethals, Gilbert Swinnen, Koen Vanhoof, Geert Wets. "A Data Mining Framework for Optimal Product Selection in Retail Supermarket Data." (2000). https://doi.org/10.1145/347090.347156.

Canbay, Pelin, Zübeyde Demircioğlu. "Endüstri 5.0'a Doğru: Zeki Otonom Sistemlerde Etik Ve Ahlaki Sorumluluklar." Ajit-E Online Academic Journal of Information Technology 12, no. 45 (2021): 106-23. https://doi.org/10.5824/ajite.2021.02.006.x.

Chen, Yen-Liang, Kwei Tang, Ren-Jie Shen, Ya-Han Hu. "Market Basket Analysis in a Multiple Store Environment." Decision Support Systems 40, no. 2 (2005): 339-54. https://doi.org/10.1016/j.dss.2004.04.009.

Çetin, Onursal, Feyzullah Temurtaş, Şenol Gülgönül. "An Application of Multilayer Neural Network on Hepatitis Disease Diagnosis Using Approximations of Sigmoid Activation Function." Dicle Medical Journal / Dicle Tip Dergisi 42, no. 2 (2015). https://doi.org/10.5798/diclemedj.0921.2015.02.0550.

Çifci, Büşra S., Cigdem Basfirinci. "Yapay Zekâ Konusunun Toplumsal Cİnsİyet Kapsaminda İncelenmesİ: Mesleklere Yönelİk Bir Araştirma." Çukurova Üniversitesi Sosyal Bilimler Enstitüsü Dergisi 29, no. 4 (2020): 183-203. https://doi.org/10.35379/cusosbil.819510.

Doddi, Srinivas, Achla Marathe, S. S. Ravi, David C. Torney. "Discovery of Association Rules in Medical Data." Medical Informatics and the Internet in Medicine 26, no. 1 (2001): 25-33. https://doi.org/10.1080/14639230010028786.

Ekrem, Ebru C., Zeynep Daşikan. "Perinatal Dönemde Yapay Zekâ Teknolojisinin Kullanımı." Eurasian Journal of Health Technology Assessment 5, no. 2 (2021): 147-62. https://doi.org/10.52148/ehta.980568.

Ferrando, Francesca. "Is the Post-Human a Post-Woman? Cyborgs, Robots, Artificial Intelligence and the Futures of Gender: A Case Study." European Journal of Futures Research 2, no. 1 (2014). https://doi.org/10.1007/s40309-014-0043-8.

Fİlİz, Emel, Şerife Güzel, Abdurrahman Şengül. "Sağlık Profesyonellerinin Yapay Zekâ Kaygı Durumlarının İncelenmesi." International Journal of Academic Value Studies (Javstudies Javs) 8, no. 8 (2022): 47-55. https://doi.org/10.29228/javs.57808.

Fong, Terrence, Illah Nourbakhsh, Kerstin Dautenhahn. "A Survey of Socially Interactive Robots." Robotics and autonomous systems 42, no. 3-4 (2003): 143-66.

García, Salvador, Julián Luengo, Francisco Herrera. Data Preprocessing in Data Mining. Vol. 72: Springer, 2015.

Goodfellow, Ian, Yoshua Bengio, Aaron Courville. Deep Learning. MIT press, 2016.

Groover, Mikell P. Automation, Production Systems, and Computer-Integrated Manufacturing. Pearson Education India, 2016.

Gümüş, Emel, Ece U. Kasap. "Hemşirelik Mesleğinin Geleceği: Robot Hemşireler." Journal of Artificial Intelligence in Health Sciences (2021). https://doi.org/10.52309/jai.2021.10.

Gümüş, Ersin, Batuhan Medetoğlu, Salih Tutar. "Finans Ve Bankacılık Sisteminde Yapay Zekâ Kullanımı: Kullanıcılar Üzerine Bir Uygulama." Bucak İşletme Fakültesi Dergisi 3, no. 1 (2020): 28-53. https://doi.org/10.38057/bifd.690982.

Haenlein, Michael, Andreas Kaplan. "A Brief History of Artificial Intelligence: On the Past, Present, and Future of Artificial Intelligence." California Management Review 61, no. 4 (2019): 5-14. https://doi.org/10.1177/0008125619864925.

Han, Jiawei, Jian Pei, Micheline Kamber. Data Mining: Concepts and Techniques. Elsevier, 2011.

Han, Jiawei, Micheline Kamber, Data Mining. "Concepts and Techniques." Morgan Kaufmann 340 (2006): 94104-3205.

Hastie, Trevor, Robert Tibshirani, Jerome H. Friedman, Jerome H. Friedman. The Elements of Statistical Learning: Data Mining, Inference, and Prediction. Vol. 2: Springer, 2009.

Joe, Tom, R. Sreejith, Kannan Sekar. "Optimization of Store Layout Using Market Basket Analysis." International Journal of Recent Technology and Engineering 8, no. 2 (2019): 1459-63. https://doi.org/10.35940/ijrte.b2207.078219.

Kagnicioglu, Celal H., Emircan Özdemir. "Evaluation of Smes in Eskisehir within the Context of Industry 4.0." Pressacademia 3, no. 1 (2017): 900-08. https://doi.org/10.17261/pressacademia.2017.672.

Karaatli, Meltem, Özlem C. Helvacioğlu, Nuri Ömürbek, Gönül Tokgöz. "Yapay Sinir Ağları Yöntemi İle Otomobil Satış Tahmini." International Journal of Management Economics and Business 8, no. 17 (2012). https://doi.org/10.11122/ijmeb.2012.8.17.290.

Karaci, Abdulkadir, Mustafa Erdemir. "Arduino Ve Wifi Temelli Çok Sensörlü Robot Tasarımı Ve Denetimi." Bilişim Teknolojileri Dergisi (2017): 435-49. https://doi.org/10.17671/gazibtd.307271.

Kaur, Manpreet, Shivani Kang. "Market Basket Analysis: Identify the Changing Trends of Market Data Using Association Rule Mining." Procedia Computer Science 85 (2016): 78-85. https://doi.org/10.1016/j.procs.2016.05.180.

Kişi, Nermin. "İnsan Kaynakları Yönetiminde Yapay Zekâ Teknolojisinin Benimsenmesi Üzerine Güç Alanı Analizi." İktisadi Ve İdari Bilimler Fakültesi Dergisi (2024). https://doi.org/10.33707/akuiibfd.1406096.

Krizhevsky, Alex, Ilya Sutskever, Geoffrey E. Hinton. "2012 Alexnet." Adv. Neural Inf. Process. Syst (2012): 1-9.

Murdan, Anshu Prakash, Pawan Kumar Ramkissoon. "A Smart Autonomous Floor Cleaner with an Android-Based Controller." 2020.

Murphy, Kevin P. Machine Learning: A Probabilistic Perspective. MIT press, 2012.

Ngai, Eric W., Xiu Li, Dennis Chau. "Application of Data Mining Techniques in Customer Relationship Management: A Literature Review and Classification." Expert Systems With Applications 36, no. 2 (2009): 2592-602. https://doi.org/10.1016/j.eswa.2008.02.021.

Ozkan, Sinan S., Durmus Karayel, Gökhan Atali, İbrahim Gökbayrak. "Esnek Algılayıcı Kontrollü Robot El Tasarımı Ve Gerçeklenmesi." Academic Platform Journal of Engineering and Smart Systems (2017): 35-40. https://doi.org/10.21541/apjes.314521.

Perera, Charith, Arkady Zaslavsky, Peter Christen, Dimitrios Georgakopoulos. "Context Aware Computing for the Internet of Things: A Survey." IEEE communications surveys & tutorials 16, no. 1 (2013): 414-54.

Quinlan, J. Ross. "Induction of Decision Trees." Machine learning 1, no. 1 (1986): 81-106.

Raji, Mustafa A. "Real-Time Data Analytics in Retail: A Review of USA and Global Practices." GSC Advanced Research and Reviews 18, no. 3 (2024): 059-65. https://doi.org/10.30574/gscarr.2024.18.3.0089.

Rajpurkar, Pranav, Robin Jia, Percy Liang. "Know What You Don't Know: Unanswerable Questions for Squad." arXiv preprint arXiv:1806.03822 (2018).

Rutkowski, Leszek, Maciej Jaworski, Lena Pietruczuk, Piotr Duda. "The Cart Decision Tree for Mining Data Streams." Information Sciences 266 (2014): 1-15.

Satava, Richard M. "Surgical Robotics: The Early Chronicles: A Personal Historical Perspective." Surgical Laparoscopy Endoscopy & Percutaneous Techniques 12, no. 1 (2002): 6-16.

Shaikh, Sadia, Faisal Sultan, Muhammad Asim. "Assortment on the Bases of Big-Data Analytics: A Quantitative Analysis on Retail Industry." Journal of Independent Studies and Research Management Social Science and Economics 19, no. 2 (2021): 154-67. https://doi.org/10.31384/jisrmsse/2021.19.2.9.

Sinaga, Kristina P, Miin-Shen Yang. "Unsupervised K-Means Clustering Algorithm." IEEE access 8 (2020): 80716-27.

Szymkowiak, Marcin, Tomasz Klimanek, Tomasz Józefowski. "Applying Market Basket Analysis to Official Statistical Data." Econometrics 22, no. 1 (2018): 39-57. https://doi.org/10.15611/eada.2018.1.03.

Turan, Tülay, Gökhan Turan, Ecir U. Küçüksille. "Ethics of Artificial Intelligence: Impact on Society." Mehmet Akif Ersoy Üniversitesi Fen Bilimleri Enstitüsü Dergisi 13, no. 2 (2022): 292-99. https://doi.org/10.29048/makufebed.1058538.

Turing, Alan Mathison. "Mind." Mind 59, no. 236 (1950): 433-60.

Wang, Yunhai, Wei Chen, Jian Zhang, Tingxing Dong, Guihua Shan, Xuebin Chi. "Efficient Volume Exploration Using the Gaussian Mixture Model." IEEE Transactions on Visualization and Computer Graphics 17, no. 11 (2011): 1560-73.

Weber, Rolf H. "Internet of Things–New Security and Privacy Challenges." Computer law & security review 26, no. 1 (2010): 23-30.

Yeşilyurt, Sedat. "Sosyal Bilgiler Eğitimi Alanında Lisansüstü Eğitimini Sürdüren Öğrencilerin Yapay Zekâ Hakkindaki Görüşleri." Asya Studies 8, no. 27 (2024): 1-14. https://doi.org/10.31455/asya.1406649.

Yilmaz, Yusuf K., Derya U. Yılmaz, Duygu Yıldırım, Esra A. Korhan, Derya Ö Kaya. "Yapay Zekâ Ve Sağlıkta Yapay Zekânın Kullanımına Yönelik Sağlık Bilimleri Fakültesi Öğrencilerinin Görüşleri." Süleyman Demirel Üniversitesi Sağlık Bilimleri Dergisi 12, no. 3 (2021): 297-308. https://doi.org/10.22312/sdusbed.950372.

Zaki, Mohammed J. "Scalable Algorithms for Association Mining." Ieee Transactions on Knowledge and Data Engineering 12, no. 3 (2000): 372-90. https://doi.org/10.1109/69.846291.

YAPAY ZEKÂ TEKNOLOJİLERİNE ETİK YAKLAŞIM

Doç. Dr. Elif KÜZECİ *

Av. Zeynep ÖĞRETMEN KOTİL

GİRİŞ

Bilişim teknolojileri, 21. yüzyıl insanının yaşamını dönüşüme uğratmaktadır. 1970'li yıllarda bilgisayar sistemlerindeki gelişmeler, 1990'lı yıllarda İnternet'in gelişimi ve son olarak da özellikle 2010'lu yıllardan itibaren Yapay Zekâ (YZ) alanındaki atılım bu dönüşümün mihenk taşları olarak anılabilir. Bilim ve teknolojinin her alanında olduğu gibi sayısal dünyanın bileşenleri de birbirini destekleyerek gelişmektedir. YZ alanında son dönemde gerçekleşen hızlı gelişmelerin de bilgisayar sistemlerinin veri işleme kapasitesindeki artış ve İnternet'in yaygınlaşması ile ilişkisi bulunmaktadır. Özellikle YZ atılımında makine öğrenmesi alanındaki gelişmelerin etkisi düşünüldüğünde bu ilişki açıkça görülebilir.

YZ tabanlı sistemler hâlihazırda yaşamın pek çok alanında etki gücüne kavuşmuştur. Bu etkinin önümüzdeki dönemde artacağı açıktır. Nitekim YZ sistemlerinin günlük yaşamı kolaylaştıran, toplumsal ve ekonomik gelişimi artıran, daha sağlıklı ve güvenli yaşam olanaklarını destekleyen yönü, bu alana yönelik ilgiyi ve yatırımları artırmaktadır. Öte yandan bu gelişmeler, aynı alanlarda pek çok yeni riski de beraberinde getirmektedir. Özellikle çalışma şekline ilişkin belirsizlikler, algoritmik ayrımcılık, veri koruması açısından söz konusu sorunlar gibi konular, YZ'nin geliştirilmesi ve kullanılması açısından önemli sorular ortaya koymaktadır. Bu sorulara yanıt olarak hukuksal düzenlemelerin hazırlanması yönünde girişimler vardır. Ancak nispeten yeni ve fakat hızla gelişen bir teknoloji olarak YZ tabanlı sistemlerin ortaya çıkardığı bireysel, toplumsal, ekonomik ve siyasal risklere karşı etik ilkeler de önemli

* İhsan Doğramacı Bilkent Üniversitesi Hukuk Fakültesi

** Bağımsız yazar.

bir kaynak oluşturmaktadır. Özellikle son yıllarda dünyanın farklı bölgelerinden farklı nitelikteki kuruluş ve oluşumlar, bu bağlamda ilkeler ve bunların uygulanmasına yönelik politikalar geliştirmektedir.

Bu bölüm kapsamında öncelikle yeni gelişen YZ ile neyin ifade edildiğine yoğunlaşılacaktır. Nitekim YZ tabanlı sistemlerin çeşitliliği, farklı alanlarda kullanımı, önümüzdeki dönemde olası gelişim çizgisi tanımlar açısından bazı farklılıklara yol açmaktadır. Bu konudaki tanıtımın YZ etik ilkeleri açısından önemli olduğu kanaatindeyiz. Bu tanıtımın ardından hukuk ve etik ilişkisine kısaca değinilerek YZ etiği kapsamında değerlendirilen ilkelerin öne çıkanları açıklanacak; etik ilkelere ilişkin temel metinler arasında bir karşılaştırma yapılarak bu alandaki genel yaklaşıma ışık tutulmaya çalışılacaktır. Çalışmamızın sonuç bölümünde ise YZ etik ilkelerinin özellikle veri koruması ile ilişkili yönleri ortaya konulacaktır.

I. YAPAY ZEKÂNIN TANIMI VE KAPSAMI

YZ alanındaki kavramsal açıklamalar, çoğunlukla bu alanda uzlaşılmış bir tanım bulunmadığı belirtilerek başlar. Gerçekten de YZ'ye ilişkin genel geçer bir tanımın varlığı şüphelidir[1]. Ancak YZ'nin tanımlanması, bu sistemlere ilişkin tartışmaların sınır ve kapsamının belirlenmesi açısından gereklidir[2]. YZ'ye ilişkin geniş tanım yelpazesi incelendiğinde, rasyonellik ve insan performansına yakınlık fenomenlerinden sıklıkla yararlanıldığı görülür. İnsan performansı yaklaşımı YZ'yi insan gibi davranma ve düşünme yeteneklerine yakınlığı açısından değerlendirirken, rasyonalist yaklaşım matematik ve mühendisliğin birleşimi ile bir sistemin kendisine verilenler ışığında en doğru ve ideal sonuca ulaşma becerisine odaklanır. Bu bağlamda örneğin Russell ve Norvig, YZ tanımlarını dört temel yaklaşıma göre sınıflandırmıştır: "insan gibi düşünen", "insan gibi hareket eden", "rasyonel düşünen", "rasyonel hareket eden". Hangi yaklaşım temel alınarak tanımın yapıldığı, tanımı yapan aktörlerin konumuna ve kullandıkları yönteme bağlı olarak değişkenlik gösterir[3].

Tanımlar arasındaki farklardansa ortaklıklara odaklandığımızda, doğal sistemler tarafından gerçekleştirilen bazı fiziksel ve zihinsel etkinliklerin

---

1 Turner, J.: Robot Rules - Regulating Artificial Intelligence, İsviçre 2019, s. 9-15.

2 Küzeci, E.: Sayısal Fil, 1. Baskı, İstanbul 2021, s. 138-139.

3 Norvig, P./Russell, S.: Artificial Intelligence – A Modern Approach, 3. Baskı, New Jersey 2010, s. 1-5.

makineler aracılığıyla gerçekleştirilmesini sağlayan sistemlerin YZ sistemleri olarak adlandırıldığını söyleyebiliriz[4]. Ancak YZ'yi tanımlama çabalarına ilişkin iki hususa özellikle işaret etmek gerekir. Bunlardan ilki, YZ'nin gelişimiyle YZ tanımlarının da değişmesidir. Bunda YZ'nin teknik açıdan değişmesi ve gelişmesi etkili olmuştur. İkincisi, YZ tanımına ilişkin tartışmaların sürmesinde bu alanın nasıl düzenleneceğine ilişkin yaklaşım farklarının etkisidir. Nitekim tanımın darlığı ya da genişliği, kural ya da ilkelerin hangi sistemlere uygulanacağı konusunda belirleyici olmaktadır. Bu husus, tartışmalarımız bağlamında özellikle önemlidir. Bu nedenle, izleyen başlık altında öncelikle bu konuya ilişkin açıklamalara yer verilecektir.

A. YAPAY ZEKÂNIN GELİŞİMİ VE TANIMIN DEĞİŞİMİ

Düşünebilen ya da "zeki" makineler, insanların zihnini oldukça uzun zamandır meşgul etmektedir. Mitolojik hikayelere, edebiyata ve felsefeye yansıdığı şekliyle bu konuyla ilişkilendirilebilecek tasvirlerin ve tartışmaların, insanların "biyolojik" zihinlerini meşgul ettiği söylenebilir. Homeros'un İlyada'sında geçen mucit Daidalaos'un hareketli heykelleri[5], Thomas Hobbes'un Leviathan'ında otomatlar ile insanlar arasında kurulan analoji[6], robot ifadesinin ilk kez kullanıldığı Karel Capek'in R.U.R.'u[7] bunun örnekleri olarak gösterilebilir. Ancak teknik gelişmeler özellikle 20. yüzyılda hız kazanmıştır. Alan Turing'in 1950 yılında yayımlanan "Bilgisayar ve Zekâ" başlıklı makalesinde ortaya koyduğu "makineler düşünebilir mi" sorusu ve bu soruyu yanıtlayabilmek için geliştirdiği "Taklit Oyunu" (çoğunlukla Turing Testi olarak da anılmaktadır)[8] özellikle anılmaya değerdir.

YZ terimi ilk olarak 1955 yılında John McCarthy ve bir grup bilgisayar programcısının, izleyen yıl bir yaz çalıştayı düzenlemek için sundukları öneride yer almıştır[9]. Terimin isim babası olan McCarthy, yıllar sonra kaleme aldığı bir yazıda, bu terimi icat etmesinin nedenini sibernetik ile

---

4 Delipetrev, B./Kostić, U./Tsinaraki, C.: *"Historical Evolution of Artificial Intelligence"*, (*https://publications.jrc.ec.europa.eu/repository/handle/JRC120469*, E.T.: 09.07.2024), s. 5.

5 Homeros. (çev. Erhat, A./Can, A.K.): İlyada, 24. Baskı, İstanbul 2008, s. 425.

6 Hobbes, T. (Lim, S.): Leviathan veya Bir Din ve Dünya Devletinin İçeriği, Biçimi ve Kudreti, 4. Baskı, İstanbul 2004, s. 17.

7 Capek, K. (çev. Öztürk, P.): R.U.R. Rossum'un Evrensel Robotları, Ankara 2013.

8 Turing, A.M.: *Computing Machinery and Intelligence,* Mind 1950, C. LIX, S. 236, s. 433-460.

9 McCarthy, J./Minsky, M.L./ Rochester, N./Shannon, C.E.: *A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence, August 31, 1955*, AI Magazine 2006, C. 27, S. 4, s. 12-14.

ilişkilendirilmekten ve sibernetik alanının kurucusu olan Norbert Wiener'i bir rehber olarak kabul etmekten (veya onunla tartışmaktan) kaçınmak olarak açıklamıştır[10]. Ancak şurası açıktır ki -ilk nedenler ne olursa olsun- sonraki dönemde YZ terimi genel kabul görmüş ve yaygın bir şekilde kullanılmıştır. "Zekâ"yı tanımlamaktaki güçlük, YZ'nin tanımlanmasındaki güçlüğün nedenlerinden biri olmuştur. Nitekim güncel tartışmalar değerlendirildiğinde YZ ifadesi çoğunlukla düşünen makineleri -ya da zeki makineleri- nitelemek için değil, makine öğrenmesi algoritmasını ve benzer teknolojileri nitelemek için kullanılmaktadır. Hatta kimi uzmanlar, belirtilen hususlar hareketle, YZ'nin güçlü bir markadan öteye geçmediği düşüncesindedir[11].

Gerçekten YZ tanımında yer alan "zekâ" kavramı, ilk başlarda insanlar tarafından gerçekleştirilen basit mekanik eylemlerin makineler tarafından da gerçekleştirilmesi ile ilişkilendirilmiş ve fiziksel boyutu ile gündeme gelmiştir[12]. Mekanik perspektifin yanı sıra mantık boyutuna ilişkin tartışmaları da beraberinde getiren zekâ terimi[13], bir süre sonra makine çıktısı ile insan kararları arasındaki farkın ayırt edilememesi[14], makinelerin önceki deneyimlerinden öğrenebilmesi, akıl yürütebilmesi ve problem çözebilmesi fikri üzerinde şekillenmiştir[15]. Cihaz kapasitesi yetersizliği sorununun giderilmesinin ardından geliştirilen uzman sistemler, belirli bir süre için zekâ tanımının yeni yüzü olmuştur[16]. Ancak günümüzde YZ'ye ilişkin tartışmanın ekseni veri temelli tek-

---

10 McCarthy, J.: *[Review of] Bloomfield, Brian, ed. The Question of Artificial Intelligence: Philosophical and Sociological Perspectives,* Annals of the History of Computing 1988, C. 10, S. 3, s. 227.

11 Solove, D.J.: *Artificial Intelligence and Privacy*, Florida Law Review (forthcoming Jan 2025), (*http://dx.doi.org/10.2139/ssrn.4713111*, E.T.: 09.07.2024), s. 11.

12 Buchanan, B.G.: *A (Very) Brief History of Artificial Intelligence*, AI Magazine 2006, C. 26, S. 4, s. 53-54; Küzeci (Sayısal Fil), s. 139-140; Nilsson, N.J. (çev. Doğan, M.): Yapay Zekâ Geçmişi ve Geleceği, 2. Baskı, İstanbul, 2019, s. 19-23.

13 Nilsson, s. 27-34.

14 Alan Turing tarafından ortaya konulan ve *"Makineler düşünebilir mi?"* sorusu üzerine geliştirilen ve makinelerin insanı taklit yeteneğini ölçen Turing Testi hakkında ayrıntılı bilgi için bkz. Nilsson, s. 65-66; Turing, A.M.: Can Digital Computers Think? (1951), (ed. Copeland, B.J.), "The Essential Turing: Seminal Writings in Computing, Logic, Philosophy, Artificial Intelligence, and Artificial Life: Plus The Secrets of Enigma", New York 2004, s. 482-486; Turing (Computing Machinery), s. 433-434.

15 Buchanan, s. 56-58; Norvig/Russell, s. 16-18.

16 Boucher, P.: *"Artificial intelligence: How does it work, why does it matter, and what can we do about it?",* (*https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641547/EPRS_STU(2020)641547_EN.pdf,* E.T.: 09.07.2024), s. 2-3; Delipetrev/Kostić/Tsinaraki, s. 8-9; Nabiyev, V.: Yapay Zekâ, 6. Baskı, Ankara, 2021, s. 399-404; Nilsson, s. 347-349.

Uzman sistemler hakkında ayrıntılı değerlendirmeler için bkz. Nabiyev, s. 399-418.

nolojilerdir. Büyük Veri'nin yaşamımıza girmesi[17], İnternet'in ve bağlantılı cihazların yaygınlaşması ve cihaz kapasitelerinin artması makine öğrenmesinin, onun bir alt dalı olan derin öğrenmenin, yapay sinir ağlarının ve doğal dil işleme gibi veri odaklı teknolojilerin gelişmesini sağlamış[18]; bu ise YZ tartışmalarının içeriğini belirleyici bir unsur olmuştur.

Teknolojik gelişmeler, içinde bulunduğu ortamı algılayabilen, büyük miktarda veri toplayan ve bu verileri otomatik veya manuel olarak modelleyerek yorumlayan YZ sistemlerini ortaya çıkarmıştır. Bu sistemlerin dikkat çekici bir özelliği, verileri işleyerek geniş bir çözüm kümesi içerisinde makul ve rasyonel çözüme ulaşmaya çalışan modeller ortaya koymalarıdır. Bu noktada üretilen çözüm, YZ sisteminin çıktısı olarak adlandırılmaktadır. Çıktı sayısal, sözel, fiziksel, işitsel gibi çeşitli biçimlerde olabilir. YZ sistemleri, verileri analiz ederek bir anlamda "öğrenmekte"; ayrıca içinde bulunduğu ortamın çıktıdan nasıl etkilendiğini değerlendirerek karar mekanizmasını buna uyarlayabilmektedir[19]. Bu sistemlerin etkin bir biçimde çalışması, YZ kullanımının yaygınlaşmasını sağlamıştır[20]. Ancak bu durum, YZ uygulamalarından kaynaklı hukuk-

---

17 Ahia Quarcoo, J./Aning, J./Kusi Fosu, G./Nti, I.K.: *A mini-review of machine learning in big data analytics: Applications, challenges and prospects*, Big Data Mining and Analytics, 2022, C. 5, S. 2, s. 81-84, 89; Boucher, s. 8; Nabiyev, s. 555.
Büyük Veri kavramının tanımı ve bileşenlerine ilişkin ayrıntılı bir değerlendirme için bkz. Ekin, B.: Kişisel Verilerin Korunması ve Rekabet Hukuku Boyutuyla Büyük Veri, 1. Baskı, İstanbul, 2021, s. 82-96.

18 Alexander, C.A./Wang, L.: *Machine Learning in Big Data*, International Journal of Mathematical, Engineering and Management Sciences 2016, C. 1, S. 2, s. 53-59; Boucher, s. 3-13; Delipetrev/Kostić/Tsinaraki, s. 11-17; Küzeci (Sayısal Fil), s. 159-160; OECD: *"Artificial Intelligence, Machine Learning and Big Data in Finance: Opportunities, Challenges, and Implications for Policy Makers",* (*https://www.oecd-ilibrary.org/finance-and-investment/artificial-intelligence-machine-learning-and-big-data-in-finance_98e761e7-en,* E.T.: 09.07.2024), s. 16-19.
Yapay öğrenme ve doğal dil işleme hakkında ayrıntılı bilgi için bkz. Nilsson, s. 501-570.
Yapay sinir ağları ve derin öğrenme hakkında ayrıntılı bilgi için bkz. Nabiyev, s. 577-621.

19 Delipetrev/Kostić/Tsinaraki, s. 5; European Parliament (2023), *What is artificial intelligence and how is it used?,* (*https://www.europarl.europa.eu/news/en/headlines/society/20200827ST085804/what-is-artificial-intelligence-and-how-is-it-used,* E.T.: 09.07.2024); High-Level Expert Group on Artificial Intelligence: *"A Definition of AI: Main Capabilities and Disciplines",* (*https://ec.europa.eu/futurium/en/system/files/ged/ai_hleg_definition_of_ai_18_december_1.pdf,* E.T.: 09.07.2024), s. 1-6; OECD: "*Artificial Intelligence in Society",* (*https://doi.org/10.1787/eedfee77-en,* E.T.: 09.07.2024), s. 15.

20 Brooks, R./Brynjolfsson, E./Calo, R./Etzioni, O./Hager, G./Hirschberg, J./Kalyanakrishnan, S./Kamar, E./Kraus, S./Leyton-Brown, K./Parkes, D./Press, W./Saxenian, A./Shah, J./Stone, P./Tambe, M./Teller, A.: "*Artificial Intelligence and Life in 2030"*, One Hundred Year Study on Artificial Intelligence, Report of the 2015 Study Panel, (*https://ai100.*

sal, sosyal, etik ve çevresel risklerin de daha güçlü bir şekilde ortaya çıkmasına neden olmuştur[21]. Aşağıda ayrıntılı bir şekilde değerlendirileceği üzere, bu riskleri olanaklı olduğu ölçüde bertaraf etmek ve güvenilir ve sorumlu YZ'nin inşasını sağlamak için etik ilkeler ve hukuksal düzenlemeler üzerinde tartışmalar ve çalışmalar sürmektedir. Ancak ilke ve kuralların ortaya konulması ve uygulama alanının saptanması için öncelikle bunların etki etmesi öngörülen YZ sisteminin tanımlanması gerekir[22]. Nitekim politika yapıcılar, uygulayıcılar ve üreticiler açısından hukuksal öngörülebilirliğin sağlanabilmesi her şeyden önce mevzu bahis sistemin tanımlanmasını gerektirir[23]. Ancak tanımlama çalışmaları, beraberinde çeşitli zorlukları getirir. Bu zorluklar, YZ'nin teknik yapısı, kullanım alanı, tanımın oluşturulma nedeni gibi hususlardan kaynaklanabilmektedir.

Her şeyden önce YZ'nin insan zekâsı ve insanın sorun çözme becerisi temel alınarak tanımlanmaya çalışılması çeşitli sorunlara neden olmaktadır. İnsan zekâsı, öznel ve soyut olduğu gibi biyokimyasal ve psikolojik koşullara bağlı olarak çalışmaktadır. İnsan zekâsını tanımlamadaki zorluk, bundan hareketle YZ tanımı geliştirmeyi de güçleştirmektedir[24]. Bunun yanında belirtilen analoji ile tanımlama çalışmaları yapılması bir yanılgıya da neden olabilir. Nitekim farklı YZ sistemleri zekânın kabul gören farklı unsurlarını yerine getirebilmektedir; ayrıca YZ ifadesinde yer alan "zekâ" terimi, her durumda doğrudan insan zekâsını taklit etmeye yönelen bir yapıyı ifade etmemektedir. Aksi yönde bir kabul, insan zekâsını tanımlamaktan ileri gitmeyecektir[25].

---

stanford.edu/sites/g/files/sbiybj18871/files/media/file/ai100report10032016fnl_singles.pdf, E.T.: 09.07.2024), s. 18-41.

21 Bartneck, C./Lütge, C./Wagner, A./Welsh, S.: An Introduction to Ethics in Robotics and AI, İsviçre 2020, *(https://doi.org/10.1007/978-3-030-51110-4),* s. 45-49; Boucher, s. 18-29; Delipetrev/Kostić/Tsinaraki, s. 24; Martinez, R.: *Artificial Intelligence: Distinguishing Between Types & Definitions*, Nevada Law Journal 2019, C. 19. S. 3, s. 1018-1021.

22 Martinez, s. 1022.

23 Bugingo, G./Huang, K./Katell, M./Krafft, P.M./Young, M.: *Defining AI in Policy versus Practice*, Proceedings of the 2020 AAAAI/ACM Conference on AI, Ethics and Society (AIES'20) 2020, *(https://doi.org/10.1145/3375627.3375835),* s. 1-2; Wang, P.: *On Defining Artificial Intelligence*, Journal of Artificial General Intelligence 2019, C. 10, S. 2, s. 2.

24 Dehmer, M./Emmert-Streib, F./Yli-Harja, O.: *Artificial Intelligence: A Clarification of Misconceptions, Myths and Desired Status*, Frontiers in Artificial Intelligence 2020, C. 3, Makale 524339, s. 2; Küzeci (Sayısal Fil), s. 148-152; McCarthy, J. (2007), *What Is Artificial Intelligence?,* (*http://jmc.stanford.edu/articles/whatisai/whatisai*, E.T.: 09.07.2024), s. 2-4.

25 Martinez, s. 1023-1026; McCarthy (What Is Artificial Intelligence?), s. 2-4; Wang, s. 16.

Günümüzde hukuksal düzenlemelerin ve tartışmaların konusu olan YZ sistemleri, geleneksel olarak anladığımız şekliyle "düşünen sistemler" değildir. Öte yandan YZ, farklı sistemleri ifade edecek şekilde de kullanılabilmektedir. Gerçekten yalnızca basit problemleri kendisine verilen kurallar rehberliğinde çözen sistemler ile veriden "öğrenen" ve karar mekanizmalarını güncelleyebilen makine öğrenmesi temelli sistemlerin YZ çatısı altında buluşması bir kavram karmaşasına neden olabilmektedir. Ayrıca şu soruna da işaret etmek gerekir: Bazen tanım, kavramsal olarak aydınlatıcı ve yol gösterici olabilir. Bir başka anlatımla, konuya yabancı bir kişinin alanı anlamasına yardımcı olabilir. Ancak aynı tanım, YZ uygulamalarını düzenlemeye yönelik bir metinde belirsizlik yaratabilir. Bu bağlamda bazı tanım çalışmalarının, YZ'nin mevcut yeteneklerini ve kapasitesini eksik ele aldıkları ve faydalı olamayacak denli belirsiz oldukları gerekçesiyle eleştirildiği görülmektedir[26]. Ancak bu eleştiriyi göğüsleyecek tanımlar üretebilmek de kolay değildir.

Mevcut YZ teknolojilerinin yanı sıra gelecekte söz konusu olabilecek teknolojik gelişmelere cevapsız kalmayacak düzenlemeler yapma isteği, YZ'nin tanımının da genişlemesine neden olur. Ne var ki YZ'yi tanımlamada benimsenecek geniş bir yaklaşımın, aşırı düzenleme ve inovasyonun engellenmesi gibi sorunlara neden olabileceğine yönelik endişeler bulunmaktadır. Bu bağlamda, inovasyonun ve hukuki belirliliğin desteklenmesi için dar ve kesin bir YZ tanımı önerilmektedir[27].

YZ'nin tanımlanmasını zorlaştıran bir diğer husus, felsefe, matematik, ekonomi, sinir bilimi, psikoloji, dil bilimi gibi farklı disiplinlerden beslenmesi ve nihayetinde bu disiplinlerin kapsamındaki tartışmaları da dönüştürmesidir[28]. Fakat bu farklılıklara rağmen, ortak bir anlayışı yansıtan başlangıç noktasına yönelik gereksinim varlığını korumaktadır[29].

---

26 Bugingo/Huang/Katell/Krafft/Young, s. 2.

27 Colonna, L./Magnusson Sjöberg, C.: *The AI Act – Comprehensive but is it Future-Proof?,* Community Reference Meeting: Challenges and Opportunities of Regulating AI, WASP-HS Research Brief Series, 2022/02, (*https://mau.diva-portal.org/smash/get/diva2:1695574/FULLTEXT01.pdf,* E.T.:09.07.2024), s. 5.

28 Norvig/Russell, s. 5-16.

YZ algısı ve tanımının, kendisini "YZ araştırmacısı" olarak tanımlayan veya YZ ile alakalı belirli konferanslardan en az birinde yayın yapan katılımcılar arasında dahi ne denli farklılık gösterdiğine ilişkin ayrıntılı bir değerlendirme için bkz. Bugingo/Huang/ Katell/Krafft/Young, s. 3-7.

29 Wang, s. 2-6.

YZ'ye ilişkin üzerinde uzlaşılmış, genel geçer bir tanımın bulunmaması, sektörlere veya uzmanlık alanlarına göre farklılaşan tanımların ortaya konulmasına neden olmuştur. Bilimsel araştırma amaçlı yapılan bir tanımın, endüstri amaçlı yapılan bir tanım ile birebir aynı olmasını beklemek makul değildir. Nitekim teknik uzmanlığa sahip kimseler tarafından yapılacak tanımlar da kullanıcılar tarafından yapılacak tanımlardan farklı olacaktır[30]. Yapılan bir çalışmada, araştırmacıların YZ'yi genel anlamda rasyonel bir yaklaşım ile tanımlarken, politika yapıcıların insan gibi düşünme kriteri üzerinden değerlendirme yapma eğiliminde olduğu görülmüştür[31]. Öte yandan, YZ'nin geliştirilmesine ve kullanılmasına ilişkin hukuksal düzenlemeler ve etik ilkeler belirlenirken YZ ile neyin kastedildiğinin açık olarak ortaya konulması elzemdir. Aksi durum, düzenlemelerin ve ilkelerin hangi durumlarda uygulanacağı konusunda belirsizlik yaratır. Bu nedenle, YZ etik ilkelerine ilişkin açıklamalarımıza geçmeden önce, YZ tanımları arasındaki farklılıkları –en azından ana hatları ile- ortaya koymak istemekteyiz.

B. YAPAY ZEKÂ SİSTEMLERİNİN SINIFLANDIRILMASI

Kavram karmaşasını önlemek, ortak bir zemin yaratmak gibi amaçlarla YZ sistemlerinin sınıflandırılması yönünde çeşitli çalışmalar olduğu görülmektedir[32]. Bu sınıflandırmaların belli başlılarına aşağıda yer verilmiştir.

1. Gelişmişlik Seviyesine Göre Sınıflandırma

YZ sistemleri gelişmişlik seviyelerine göre genel olarak üç kategoriye ayrılarak incelenmektedir. Bu kategorilerden ilkini, bir veya birkaç görevi yerine getirebilen, programlandıkları konularda, rutin ve tekrarlayan işlerde insandan hızlı ve doğru sonuçlar ortaya koyabilen, ancak genelleme ve alanlar arası bilgi aktarma yeteneği bulunmadığından programlanma amaç ve konusu dışında insanı ikame etmekten aciz olan Yapay Dar/Zayıf Zekâ (Artificial Narrow Intelligence/Weak AI) oluşturur[33]. Hâlihazırda gelişti-

30 De Prato, G./Delipetrev, B./Gómez, E./López-Cobo, M./Martínez-Plumed, F./Samoili, S.: *"AI Watch. Defining Artificial Intelligence. Towards an operational definition and taxonomy of artificial intelligence",* (*https://publications.jrc.ec.europa.eu/repository/handle/JRC118163,* E.T.: 09.07.2024), s. 7-14.

31 Bugingo/Huang/Katell/Krafft/Young, s. 2-7.

32 De Prato/Delipetrev/Gómez/López-Cobo/Martínez-Plumed/Samoili, s. 9-14.

33 Delipetrev/Kostić/Tsinaraki, s. 5-6.

rilmiş YZ sistemleri bu kategoride yer alır[34]. İkinci kategoride yer alan Yapay Genel Zekâ (Artificial General Intelligence/Strong AI) ise ortalama bir insan kapasitesine sahip kabul edilmektedir. Bu kategorinin içinde yer alan öz farkındalık, sağduyulu muhakeme, amaç belirleme, kavramsal ilişki kurma ve bilginin alanlar arası aktarımı gibi özelliklere sahip YZ sistemleri günümüzde henüz geliştirilememiştir[35]. Üçüncü kategoride yer alan Yapay Süper Zekâ (Artificial Superintelligence) kavramı ise Nick Bostrom tarafından ortaya konulmuştur. Bostrom'un ifadesiyle Yapay Süper Zekâ, "İnsanların bilişsel performansını handiyse her alanda katbekat aşan her türlü zekâ"dır[36]. Bu kategoride yer alan sistemlerin de henüz geliştirilemediği açıktır.

2. Risk Seviyesine Göre Sınıflandırma

YZ sistemleri çeşitli seviyelerde riskler yaratmaktadır[37]. Bu riskler, YZ sistemlerinin kullanım alanlarından kaynaklanabildiği gibi, sistemlerin modellerinden veya çalışma mekanizmalarından da kaynaklanabilir. Risk belirlenirken YZ'nin insan hakları, demokrasi ve hukukun üstünlüğü üzerindeki olumsuz etki potansiyeli, etkinin zamansal ve mekânsal boyutu, potansiyel olumsuz etkilerin telafisinin olanaklı olup olmadığı gibi unsurlar değerlendirilmektedir[38]. Farklı risk seviyeleri, alınması gereken tedbirleri ve risklerle mücadelede benimsenecek yöntemleri de farklılaştırmaktadır[39]. Risk seviyesi gözetilerek yapılan değerlendirmeler, özellikle konuya ilişkin Avrupa Konseyi ve Avrupa Birliği (AB) bünyesindeki gelişmeler ile daha dikkat çekici hale gelmiştir.

---

34 Boucher, s. 13; Delipetrev/Kostić/Tsinaraki, s. 5; Stahl, B.C.: Artificial Intelligence for a Better Future, Springer, İsviçre 2021, *(https://doi.org/10.1007/978-3-030-69978-9),* s. 10-11.

35 Boucher, s. 13, 17; Delipetrev/Kostić/Tsinaraki, s. 6; High-Level Expert Group on Artificial Intelligence (A Definition of AI), s. 5; Stahl, s. 11-12.

36 Bostrom, N.: *How Long Before Superintelligence?,* Linguistic and Philosophical Investigations 2006, C. 5, S. 1, s. 11-30; Bostrom, N. (çev. Aydar, F.B.): Süper Zekâ: Yapay Zekâ Uygulamaları, Tehlikeler ve Stratejiler, 2. Baskı, İstanbul, 2020, s. 39; Boucher, s. 13-14; Delipetrev/Kostić/Tsinaraki, s. 6.

37 Boucher, s. 18-29; Delipetrev/Kostić/Tsinaraki, s. 24.

38 CAHAI: "*Feasibility Study",* (*https://rm.coe.int/cahai-2020-23-final-eng-feasibility-study-/1680a0c6da,* E.T.: 09.07.2024), par. 125-126.

39 CAHAI (Feasibility Study), par. 42-44.

Ayrıntılı bilgi ve risk temelli yaklaşım önerileri için bkz. CAHAI (Feasibility Study), par. 95-128.

Avrupa Konseyi Yapay Zekâya İlişkin Geçici Komitesi (Ad Hoc Committee on Artificial Intelligence – CAHAI) tarafından hazırlanan Yapay Zekâ Sistemlerine Dair Regülasyona Doğru (Towards Regulation of AI Systems) ve Fizibilite Çalışması (Feasibility Study) başlıklı dokümanlarda, "insan hakları, demokrasi veya hukukun üstünlüğü açısından önemli veya bilinmeyen riskler oluşturabilecek ve mevcut yasal çerçevelerde bu riskleri hafifletecek uygun önlemlerin bulunmadığı" yüksek riskli YZ sistemlerinin kullanımlarının sınırlandırılmasına ilişkin "kırmızı çizgiler" ("red lines") belirlenmiştir[40]. Daha sonra Avrupa Birliği Yapay Zekâ Yasası (European Union Artificial Intelligence Act)[41] (YZY) ile bu yaklaşım geliştirilmiştir.

YZY'nin farklı YZ sistemleri için öngördüğü yükümlülükleri içeren hükümlerinin yorumlanması neticesinde, YZ sistemlerinin kullanımlarına bağlı olarak meydana gelebilecek risklerin boyutuyla orantılı dört farklı risk kategorisi benimsenmiştir: Kabul edilemez risk, yüksek risk, sınırlı risk ve minimum risk[42]. Bireyi manipüle etme, savunmasız grupların zayıf noktalarından yararlanarak psikolojik veya fiziksel zarar verme, bireyin özgür seçim haklarını engelleme, kamu otoriteleri veya bu otoriteler adına sosyal puanlama sistemlerinin kullanımı gibi potansiyel kullanımlar, belirli şartlar altında kabul edilemez risk kategorisi olarak yorumlanabilir[43]. Öte yandan kritik altyapıların yönetilmesi ve işletilmesi, istihdam ve işçi yönetimi, kamu hizmetlerine erişim gibi amaçlarla kullanılan YZ sistemleri, yüksek riskli YZ kategorisinde yer alır[44]. Bu kategorinin YZY'de açıkça belirlendiği görülmektedir. Benzer şekilde sohbet robotları gibi YZ sistemlerinin sınırlı risk kategorisinde[45], YZ destekli video oyunları veya spam filtreleri gibi YZ uygulamalarının ise minimum risk kategorisinde yer aldığı söylenebilecektir[46,47].

---

40 CAHAI (Feasibility Study), par. 43; CAHAI: "*Towards Regulation of AI Systems",* (*https://rm.coe.int/prems-107320-gbr-2018-compli-cahai-couv-texte-a4-bat-web/1680a0c17a,* E.T.: 09.07.2024), s. 35-36.

41 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act).

42 YZY, par. 26, 53.

43 YZY, m. 5.

44 YZY, Ek III, m. 6.

45 European Commission (2024), *AI Act,* (*https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai#:~:text=Limited%20risk%20refers%20to%20AI,to%20continue%20or%20step%20back.*, E.T.: 09.07.2024); YZTT, s. 14-15.

46 European Commission (2024), *AI Act;* YZY, par. 53.

3. Sembolik Yapay Zekâ ve Veri Odaklı Yapay Zekâ Ayrımı

Sembolik YZ ve veri odaklı YZ arasındaki ayrım, YZ'nin gelişim süreciyle bağlantılıdır. Sembolik YZ, gerçek dünyanın karmaşıklığını sayısal ortama aktarabilmek ve makinelerin insan benzeri kararlara ulaşmasına yardımcı olmak için ayrıntılı ve anlaşılabilir karar yapılarının insan eliyle oluşturulmasını gerektirir. Bu süreçte sistem, kendisine verilen amaca ulaşmak için daha önceden tanımlanan mantıksal temsilleri kullanır. Sembolik YZ sistemlerinde her türlü komutun insan eli ile girilmesi, her türlü hatanın yine insan müdahalesi ile düzeltilmesi gerekir[48].

Veri odaklı YZ ise temelde makine öğrenmesini ve derin öğrenme, yapay sinir ağları gibi alt dallarını kullanan sistemleri ifade eder. Sembolik YZ'de söz konusu olan, insan eli ile oluşturulmuş talimatlar yerine, büyük miktarda veri içerisindeki örüntü ve bağlantılardan hareketle çıkarımda bulunan veri odaklı YZ, otomatik bir şekilde veri temelli öğrenmeyi olanaklı kılmaktadır. İlgili veriler, sistem tarafından mevcut problemin çözümüne ilişkin matematiksel bir model üretmek için kullanılır. Sembolik YZ ile çözülemeyecek denli karmaşık ve her bir problemin manuel olarak tanımlanmasının olanaklı olmadığı hallerde bu yönteme başvurulmaktadır[49].

Güncel tartışmalara konu olan YZ, genellikle veri odaklı YZ'dir. Ancak sembolik YZ'nin tekrar eden iş ve işlemlerde, planlama ve optimizasyonda kullanımı söz konusudur. Bunun yanı sıra sembolik ve veri odaklı YZ sistemlerini birleştiren uygulamalara da rastlanmaktadır[50].

4. Diğer Sınıflandırmalar

Yukarıda açıklanan sınıflandırmalar yanında YZ sistemlerinin, aktörler üzerindeki çeşitli etkileri (insan hakları, demokrasi, kullanıcı grubu, toplum, çevre vb.), ekonomik düzlemdeki yansımaları (kullanım alanları, kritik etkiler, farklı endüstrilere entegrasyon), veri ve girdiler (veri işleme, işlenen verilerin niteliği ve formatı, veri setlerinin kalitesi), YZ modeli

---

47 Risk sınıflandırmasına ve detaylara ilişkin ayrıntılı bilgi ve değerlendirmeler için bkz. Veale, M./Zuiderveen Borgesius, F.: *Demystifying the Draft EU Artificial Intelligence Act*, Computer Law Review International 2021, C. 22, S. 4, s. 97-112.

48 Boucher, s. 3; OECD (Artificial Intelligence in Society), s. 27.

49 Boucher, s. 3-4; High-Level Expert Group on Artificial Intelligence (A Definition of AI), s. 3; OECD (Artificial Intelligence in Society), s. 27-28.

50 Boucher, s. 3; OECD (Artificial Intelligence in Society), s. 27.

(modelin karakteristik özellikleri, tercih edilen öğrenme yöntemi, insan faktörü ve müdahalesi, şeffaflık ve hesap verilebilirlik), görev ve çıktılar (otonomluk seviyesi, uygulama alanları, sistemin tanımlanan görevleri) gibi farklı başlıklar altında sınıflandırıldığı da görülmektedir[51].

C. FARKLI YAKLAŞIMLARIN ORTAK PAYDASI

Yukarıdaki açıklamalar ışığında YZ tanımlarına ilişkin geçmiş dönem çalışmalarında daha çok teknik özelliklere ve detaylara odaklanılırken güncel çalışmalarda daha çok kavramsal bir yaklaşımın tercih edildiği söylenebilir. Öte yandan pek çok tanımda, YZ sistemlerinin yaşamın karmaşıklığını ve çevreyi algılaması, verilerin işlenmesi, karar verme süreçlerinin işlerliği, farklı otonomluk seviyelerine sahip olma gibi özelliklerine yoğunlaşıldığı görülmektedir[52].

YZ tanımlarına ilişkin geniş bir yelpaze karşımızdadır. AB ve ABD'den uzmanların hazırladığı "AB-ABD Yapay Zekâ Terminolojisi ve Taksonomisi" ("EU-U.S. Terminology and Taxonomy for Artificial Intelligence") belgesi de bu yelpazeyi ortaya koymaktadır[53]. Metnin ilk versiyonunda AB ve ABD'de yayımlanan önemli belgelerde yer alan 65 terim listelenmiştir. Bu metin daha sonra güncellenmiştir. Güncelleme kapsamında 13 yeni terim (örneğin veri sızıntısı, özellik mühendisliği, kayıp/maliyet fonksiyonu) eklenmiş ve 24 terimde (örneğin güvenilir YZ, opaklık, büyük dil modeli) değişiklik yapılmıştır[54]. Kısa sürede metnin güncellenmesi gereksiniminin ortaya çıkması, YZ tanımlarını topluca ortaya koymanın dahi ne kadar güç olduğunu göstermektedir.

---

51 OECD: *"OECD Framework for the Classification of AI Systems",* (*https://www.oecd-ilibrary.org/docserver/cb6d9eca-en.pdf?expires=1705706916&id=id&accname= guest&checksum=17CEFCA23E0FCA0059F51E72FCC5D621,* E.T. 09.07.2024), s. 17-21.

Sınıflandırmaya ilişkin ayrıntılı bilgi için bkz. OECD (OECD Framework), s. 25-54.

52 Bu konuda ayrıca bkz. De Prato/Delipetrev/Gómez/López-Cobo/Martínez-Plumed/ Samoili, s. 8-9; Gulley, A./Hilliard, A. (2023), *Lost in Transl(A)t(I)on: Differing Definitions of AI,* (*https://www.holisticai.com/blog/comparing-definitions-of-ai,* E.T. 09.07.2024).

53 *"EU-U.S. Terminology and Taxonomy for Artificial Intelligence",* (*https://digital-strategy.ec.europa.eu/en/library/eu-us-terminology-and-taxonomy-artificial-intelligence,* E.T.: 09.07.2024).

54 *"EU-U.S. Terminology and Taxonomy for Artificial Intelligence – Second Edition",* (*https://digital-strategy.ec.europa.eu/en/library/eu-us-terminology-and-taxonomy-artificial-intelligence-second-edition,* E.T.: 09.07.2024).

Kanaatimizce ideal bir tanım, yukarıda ayrıntılarıyla açıklanan sınıflandırma yöntemlerini de içerisinde barındırmalıdır. Her bir YZ sistemini kapsayacak yeknesak bir tanım yapma gayreti, zorluğunun yanı sıra etkisizdir. Tutarlı, zamandan, mekândan, sektörden ve kişilerden bağımsız, evrensel, öngörülü ve esnek bir genel tanımın, farklı ekosistemler ve süreçler özelinde, yukarıda bahsi geçen veya başkaca sınıflandırma yöntemleri ile özelleştirilerek kullanılması daha etkili olacaktır.

Bunun yanında kanaatimizce, düzenlemelerde riske dayalı sonuçları ve diğer parametreleri de göz önünde bulunduran bir yaklaşıma öncelik vermek, belirtilen sorunun çözümü açısından yararlı olacaktır. YZ'nin tanımlanması ile YZ'den ne anlaşılması gerektiğinin açıklığa kavuşturulması hedeflenmektedir. Ancak tanımın yanlış yaklaşım ve yöntemlerle yapılmasının yaratabileceği olumsuz sonuçlar göz ardı edilmemelidir[55]. Ayrıca farklı yapıda, farklı kaynaklar ile beslenen ve farklı hedefler için geliştirilen YZ sistemlerinin bulunduğu unutulmamalıdır. Bu bağlamda YZ'ye ilişkin metinlerde, metinlerin kapsamını tam ve doğru bir şekilde ortaya koyabilmek için o metne özgü tanımı açıklamak gerekir. Aşağıda –yukarıdaki açıklamalar ışığında- bu bölümde esas alınan YZ tanımına ilişkin açıklamada bulunulacaktır.

D. ETİK İLKELERE GİDEN YOLDA YAPAY ZEKÂ

Çağımızın en dikkat çeken teknolojik gelişmeleri arasında yer alan YZ sistemlerinin, insanların yararına sunulan araçlar olduğu unutulmamalıdır. YZ, insanın gereksinimlerinden ve merakından doğmuş bir teknoloji ürünüdür[56]. Kanımızca bu bakış açısı, YZ'ye mucizevi değerler atfetmekten ya da gerçekçi olmayan distopik senaryolar üretmekten kaçınmamıza yardımcı olabilir. Potansiyel faydalar ve riskler, pek çok teknolojik üründe olduğu gibi YZ sistemleri açısından da karşımıza çıkmaktadır[57]. Yetersiz kullanım veya kullanımdan gereksiz yere kaçınma sonucunda fırsat maliyetleri oluşabilir[58]. Öte yandan aşırı veya muhteviyatına uygun olmayan

55 Martinez, s. 1034-1035.

56 Boucher, s. 60; Floridi, L.: Introduction – The Importance of an Ethics-First Approach to the Development of AI, (ed. Floridi, L.), "Ethics, Governance, and Policies in Artificial Intelligence", Philosophical Studies Series, C. 144, 2021, s. 2-3.

57 AI4People: "*AI4People's Ethical Framework for a Good AI Society: Opportunities, Risks, Principles and Recommendations",* (https://eismd.eu/wp-content/uploads/2019/11/AI4People's-Ethical-Framework-for-a-Good-AI-Society_compressed.pdf, E.T.: 09.07.2024), s. 9; Buchanan, s. 60.

58 Boucher, s. 18-19.

kullanım da pek çok soruna neden olabilir[59]. Bu açıdan faydayı artıran, riskleri azaltan ve süreçleri optimize eden kullanım standartları belirlenmesinin yararları bulunmaktadır.

YZ sistemlerinin kullanım alanlarının ve risk seviyelerinin çeşitliliği yeknesak tanımları zorlaştırsa da bu sistemlerin geliştirilmesine ve kullanımına rehberlik edebilecek esnek, zamansız, mekândan bağımsız, inovasyonu teşvik eden etik çerçeveler geliştirmek, YZ serüveninin toplumsal değerler ve normlarla uyumlu olmasını sağlamaya yardımcı olabilecek bir başlangıç noktası ve tamamlayıcı unsur olabilir. Şimdiye dek ortaya konan etik ilkeler, yorum ve uygulamada sağladığı esneklik ve uyumluluğun gönüllülük esasına dayalı olması sayesinde üzerinde uzlaşıya varabilmeyi kolaylaştırmıştır. Genel çerçeve çizmeyi sağlayan etik ilkelerden özel düzenlemelere giden yolda bu uzlaşıyı korumak güç olabilecek ise de[60] düzenlemeler hazırlanır ve geliştirilirken etik ilkelerin göz önünde bulundurulması kanımızca olumlu bir etki yaratacaktır.

Güvenilir YZ'ye ilişkin etik ilkeleri tanımlayabilmek ve uygulayabilmek, anlamlı bir tartışma ortamını sağlayabilmek, belirliliği tesis etmekten ve uzlaşıya varmaktan geçmektedir. Herhangi bir kavram karmaşasından kaçınabilmek için çalışmamızın devamında YZ terimini kullanırken -metne esas alınan etik ilke metinlerinde de benimsendiği şekilde-, sınırlı sayıda görevi insandan daha hızlı ve doğru yerine getirebilen ancak genelleme yeteneği bulunmayan Yapay Dar Zekâ kapsamında yer alan, makine öğrenmesi ve alt dallarını kullanarak büyük miktarda veri içerisindeki örüntü ve bağlantılardan çıkarımda bulunan veri odaklı YZ uygulamalarını ifade ettiğimizi belirtmek isteriz. Bu kapsamda, aşağıda "düşünen" ya da "zeki" makinelerden değil, belirli bir teknik sistem içinde veri temelli çalışan ve bunlardan sonuç üreten YZ örneklerine odaklanacağız ve bu sistemlere ilişkin günümüzde kabul edilen etik ilkeleri inceleyeceğiz.

II. YAPAY ZEKÂ ETİĞİ

Modern bir hukuk sisteminde, uyulması zorunlu kurallar benimsenmiştir. Bu kurallar toplumsal ilişkileri ve gündelik yaşamı etkiler. Hukuk kurallarının devletin yaptırım gücü ile desteklenmesi, onu toplumsal yaşamı düzenleyen diğer kurallardan ayıran önemli özelliklerden biridir. Etik dahil

[59] AI4People, s. 9; Boucher, s. 28-29.

[60] Aynı yönde bkz. Boucher, s. 51-52.

olmak üzere diğer ilke ve kurallar da hukuk ile etkileşim içindedir. Bu ilkelerin hukuksal bağlayıcılığı, pozitif hukuk tarafından ne oranda tanındıkları ile ilişkilidir[61]. Ancak hukuk kuralları, toplumsal yaşamın dinamizmi karşısında her zaman en etkili ve tek başına yeterli çözüm olamamaktadır[62]. Bu husus, etik ilkelerin uygulamadaki önemini ortaya koyar. Nitekim etik ilkeler, doğru uygulamalar geliştirebilmek için daha dinamik bir kaynak olabilmektedir.

Bu çalışma kapsamındaki kullanımı açısından etik, olay, olgu ve eylemlerin iyi veya kötü, doğru veya yanlış olarak değerlendirilmesi ile ilgilenen bir disiplin olarak tanımlanabilir[63]. Bu açıdan etik, belirli bir amaca ulaşmada yararlanılan, geniş uygulama alanı olan ve üzerinde uzlaşıya varılmış soyut, genel nitelikte; eylem ve kararların iyiye, doğruya ve ideale yönelmesini amaçlayan ilkeleri içerir. Özellikle normatif etik, öznel değerlendirmeleri değil, genel geçerliliği olan ve herkes için kabul edilebilir yargı ve normları ifade etmektedir[64]. Etik ilkeler, kişisel çıkarlardan ziyade iyi, doğru ve anlamlı sonuçlara giden yolda referans noktası görevi görerek tutarlı kararlar vermeye yardımcı olabilir[65].

Etik değerler, ilkeler aracılığıyla ifade ve idealize edilir[66]. Etik ilkelere yansıyan adalet, eşitlik, insan haklarına ve hukukun üstünlüğüne saygı, dürüstlük kuralına uygunluk, insan onuru gibi değerler, hukuk ile ilişkisi bağlamında özellikle dikkat çekmektedir[67]. İlkeler, etiğin ortaya koyduğu ve adalet, eşitlik gibi hukukun temelinde de yer alan değerlerin korunmasında önemli bir etkiye sahiptir. Ancak bu ilkelerin, hukuk kurallarından ayrılan yönlerini belirlemek önem arz eder. Nitekim pozitif hukuk, yürürlüğe konulmuş kurallara uymayı ve uyulmadığı takdirde yaptırımlar aracılığıyla uyuma zorlamayı öngörür. Etik ise bireyin, ortaya konan değer ve ilkelere

---

61 Yüksel, M.: *Modernleşme Bağlamında Hukuk ve Etik İlişkisine Sosyolojik Bir Bakış*, Ankara Üniversitesi SBF Dergisi, C. 57, S. 1, s. 179-180.

62 Yüksel (Modernleşme), s. 190.

63 Xhemajli, H.: *The Role of Ethics and Morality in Law: Similarities and Differences,* Ohio Northern University Law Review 2021, C. 48, s. 82-83.

64 Bartneck/Lütge/Wagner/Welsh, s. 17-19.

65 Kuçuradi, İ: *Etik ve "Etikler",* Türkiye Mühendislik Haberleri 2003, S. 423, s. 7-9; The Ethics Center (2016), *Ethics Explainer: Ethics, morality & law*, (*https://ethics.org.au/ethics- explainer-ethics-morality-law/,* E.T.: 09.07.2024).

66 Yüksel (Modernleşme), s. 181.

67 Özel, K.C.: *Etik ve Etik.- Hukuk Arasındaki İlişki*, TAAD 2019, S. 33, Y. 9, s. 696-699.

uyumun "doğru ve iyi olan" olduğuna inanmasını, bu inanç doğrultusunda hareket etmesini, ilkelerin bir durumu değerlendirirken yol göstermesini ve referans noktası işlevi görmesini hedefler[68].

Etik ilke ve değerler zamanla, gereksinimden, bireysel ve toplumsal bilinçten doğarlar. Bu sebeple, hukuk kuralları gibi belirli bir anda yürürlükten kaldırılmaları ve etkilerinin de aynı şekilde kısa sürede ortadan kalkması olanaklı değildir. Etiğin ortaya koyduğu ilke ve değerler, nesiller boyu etkisini sürdürmeye devam eder[69].

Etik değerler her ne kadar benzer deneyimler, etkileşimler ve olayların sonucu olarak ortaya çıkmakta ise de "etik ilke" formuna büründüklerinde dışsal ve müdahaleci bir ilkeler bütünü haline gelerek hukuk kurallarına yaklaşmaktadırlar[70]. Bu yönüyle etik, hukukun meydana gelmesinde, gelişmesinde ve şekillenmesinde de önemli bir kaynaktır. Etiğin yapı taşlarını oluşturan değer ve ilkeler, hukuksal süreçlere uygun bir şekilde düzenlemelere yansıtıldığında pozitif hukuk kuralı haline gelebilir. Ancak bu durum, etik ilke ve değerlerin her zaman hukuk kuralına evrileceğini ifade etmediği gibi, hukuk kurallarının da her zaman etik ilke ve değerlerle uyumlu olduğunu söylemek olanaklı değildir. Etik değerler ve hukuk kuralları bazen belirli bir hususta kesişmekte, bazen birbirini tamamlayıcı ve yol gösterici nitelikte olmakta, bazen ise birbirinden ayrışmaktadır[71]. Öte yandan, etik ilkelerin hukuksal olarak bağlayıcı olmamasına karşın çeşitli aktörler tarafından adeta bağlayıcı bir hukuk kuralı gibi uygulandığı da görülebilmektedir.

Etik ilkeler, bazı durumlarda hukuksal alanda düzenlenmemiş konulara ilişkin sorunlarla mücadeleye destek sunmaktadır[72]. Örneğin kişisel verilerin korunmasına ilişkin hukuksal düzenlemeler bağlayıcı niteliktedir. Ancak bu düzenlemelerin yetersiz kaldığı bazı durumlarda, konuya ilişkin benimsenmiş etik ilkeler yorumlama ve gerekçelendirme açısından önemli kaynaklar haline gelmektedir[73]. Belirtilen husus YZ teknolojilerinin yarattığı riskler açısından da gözlemlenebilir. Nitekim YZ sitemlerinin ortaya

---

68 Karacan, O.: *Hukukçuların Etik Sorumlulukları ve İlkelerin Rolü*, TBB Dergisi 2022, S. 160, s. 253-257; Özel, s. 699-701; Yüksel, M.: *Etik Kodlar, Ahlak ve Hukuk*, Hacettepe HFD 2015, C. 5, S. 1, s. 21-22.

69 Karakoç, Yusuf: *Hukuk – Etik İlişkisi*, HFSA 2012, S. 24, s. 93-94.

70 Yüksel (Etik Kodlar), s. 19-20.

71 Özel, s. 698-700.

72 Yüksel (Modernleşme), s. 178-179.

73 Karacan, s. 253-254; Özel, s. 699-700; Yüksel (Modernleşme), s. 178-179, 193.

koyduğu risklerle mücadeleye odaklanan uluslararası ve yasal olarak bağlayıcı bir aracın yokluğunda, YZ'nin yaygın kullanımından önce yürürlüğe konan yasal düzenlemelerin YZ ekseninde yorumlanması, bağlamsal değerlendirmelerin yapılması bakımından YZ etiği gibi bağlayıcı olmayan ilkeler yardımcı olabilir[74].

Uygulamalı etiğin bir alt dalı olarak belirlenebilecek YZ etiği, bu teknolojinin insan odaklı, topluma faydalı ve güvenli olabilmesini konu edinmektedir. Bu açıdan YZ etiği, YZ sistemlerinin düzenlenmesi için gereksinim duyulan kuralların oluşturulmasında, yorumlanmasında ve uygulanmasında, kısaca güvenilir YZ'ye ulaşmada önemli bir işlev kazanmaktadır[75]. Bizim de katıldığımız bir görüşe göre, YZ etiğinin bağlamı yalnızca YZ'nin algoritmik karar süreçleri olmamalıdır. Karar mekanizmalarını şekillendiren maddi, sosyal, ekonomik ve ekolojik etmenler ve kararların sonuçlarının yarattığı etkiler bir bütün olarak YZ etiğinin konusunu oluşturmalıdır[76]. Nitekim YZ'nin tasarımı, geliştirilmesi ve kullanılması da YZ etiğinin bir parçasıdır[77].

Öte yandan YZ etiğine, etiğin diğer alanlarında olduğu gibi yalnızca regülasyonların oluşturulmasında ve uyumun sağlanmasında değil, uygulamalar ve karşılaşılan zorluklarla mücadele, toplumun faydasını gözetecek çözümlerin aranmaya devam edilmesi, mevcut hükümlerin yorumlanması, sosyal normlara ve toplumsal değerlere aykırı unsurların belirlenmesi gibi konular açısından da gereksinim duyulmaktadır[78]. YZ etiği, YZ'nin sağladığı avantajları tespit etmeyi ve bunlardan faydalanmayı olanaklı kılarken mevcut ve potansiyel riskleri belirleyerek onlarla mücadele etmeyi ve riske dayalı maliyetleri azaltmayı da hedeflemektedir[79]. Böylelikle YZ'nin sürdürülebilir ve sorumlu bir şekilde geliştirilmesi hedeflenmektir. Bu açıdan ilkeler, her somut olay karşısında tek başına yeterli olmayabilir.

---

74 CAHAI (Feasibility Study), par. 82.

75 Ayrıca bkz. High-Level Expert Group on Artificial Intelligence: "*Ethics Guidelines for Trustworthy AI",* (*https://op.europa.eu/en/publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1,* E.T.: 09.07.2024), s. 9.

76 Attard-Frost, B./De los Rios, A./Walters, D.R.: *The Ethics of AI business practices: a review of 47 AI ethics guidelines*, AI and Ethics 2023, C. 3, s. 398.

77 Bartneck/Lütge/Wagner/Welsh, s. 103.

78 Floridi, L.: The Ethics of Artificial Intelligence – Principles, Challenges, and Opportunities, Oxford 2023, s. 81-82.

Floridi tarafından ortaya konulan "yumuşak etik" *("soft ethics")* ve "katı etik" *("hard ethics")* yaklaşımına ilişkin detaylı bilgi için bkz. Floridi (The Ethics of AI), s. 82-87.

79 AI4People, s. 14.

Zira öngörülmesi veya genelleştirilmesi olanaklı olmayan olay ve olgular, ilkeler gibi genel düzenlemeler ile ele alınamayabilir. Bu hallerde, bağlamsal ayrıntıların analizini sağlayan etik akıl yürütmeye gereksinim duyulmaktadır[80].

A. ETİK İLKELER

YZ sistemlerindeki gelişmeler, devletler, uluslararası oluşumlar, sivil toplum kuruluşları, endüstri devleri gibi çeşitli aktörlerin, benimsedikleri etik ilkeleri gösteren çeşitli metinler yayımlamalarına neden olmuştur.

AB YZ Üst Düzey Uzman Grubu'nun (High-Level Expert Group on AI) işaret ettiği üzere, etik ilkelerin YZ sistemlerinin yaşam döngüsünü bir bütün olarak kapsaması, bütünsel ve sistematik bir yaklaşımla uygulanması beklenmektedir[81]. Bunun yanında etik ilkeler arasında bir hiyerarşi bulunmadığı belirtilmelidir. Birçok ilke, birbirini tamamlayıcı niteliktedir. Fakat somut olayın özelliklerine göre bir ilkenin diğerinden daha öncelikli olması söz konusu olabilir. Bu durumda dahi ilkeler bütünsel bir şekilde düşünülmeli, yorumlamada ilkeler arası tutarlılığa dikkat edilmelidir[82]. UNESCO, etik ilkeler arası gerilimlerin, ölçülü, temel hak ve özgürlüklere saygılı bir yaklaşımla ele alınması gerektiğini vurgulamaktadır[83]. Montréal Deklarasyonunda ise ilkelerin, geliştirildikleri toplumların kültür, politika ve değer yargılarını yansıtsalar da kültürlerarası ve uluslararası bir konuma sahip olmalarının amaçlandığı belirtilmiştir[84]. Öte yandan etik ilkelerin, YZ sistemlerinin yaşam döngüsü boyunca ve döngüye dâhil olan tüm aktörler tarafından göz önünde bulundurulması beklenir. İlkelerin değerlendirilmesi ve yorumlanması, ulusal ve uluslararası hukukta kabul edilmiş düzenlemelerle uyumlu olmalıdır[85]. Ayrıca etik ilkelerin kapsamlı bir etki

---

80 High-Level Expert Group on Artificial Intelligence (Ethics Guidelines), s. 9.

81 High-Level Expert Group on Artificial Intelligence (Ethics Guidelines), s. 5.

82 High-Level Expert Group on Artificial Intelligence (Ethics Guidelines), s. 13-14.

83 UNESCO: "*Recommendation on the Ethics of Artificial Intelligence"*, (*https://unesdoc.unesco.org/ark:/48223/pf0000381137?posInSet=2&queryId=0f338b37-d696-4b9c-9962-251f99ba628f,* E.T.: 09.07.2024), s. 18.

84 University of Montréal: "*Montréal Declaration for a Responsible Development of Artificial Intelligence"*, (*https://declarationmontreal-iaresponsable.com/wp-content/uploads/2023/04/UdeM_Decl-IA-Resp_LA-Declaration-ENG_WEB_09-07-19.pdf,* E.T.: 09.07.2024), s. 5.

85 High-Level Expert Group on Artificial Intelligence (Ethics Guidelines), s. 5-6; The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems: "*Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems, Ver-*

yaratabilmesi, çok paydaşlı ve uluslararası iş birliğini sağlamayı gerektirir[86].

Çalışmamız kapsamında etik ilkelere ilişkin değerlendirmelerimizde AB YZ Üst Düzey Uzman Grubu'nun "Güvenilir YZ için Etik İlkeler"[87] ("Ethics Guidelines for Trustworthy AI") isimli kılavuzu temel alınmıştır. İncelenen ve çalışmamıza kaynak teşkil eden kaynaklar içerisinde Elektrik ve Elektronik Mühendisleri Enstitüsü'nün (Institute of Electrical and Electronics Engineers – IEEE) "Etik Açıdan Uyumlu Tasarım"[88] ("Ethically Aligned Design") isimli vizyon metnine, UNESCO'nun "Yapay Zekâ Etiği Üzerine Tavsiye Kararı"na[89] ("Recommendation on the Ethics of Artificial Intelligence") ve Montréal Deklarasyonu'na[90] (Montréal Declaration for a Responsible Development of Artificial Intelligence) sıklıkla başvurulmuştur. Bu bağlamda aşağıda, belirtilen metinlerde öne çıkan etik ilkelere ilişkin açıklamalara yer verilecektir. Bu etik ilkeler şu başlıklar altında toplanabilir:

i. İnsan Haklarına Saygılı ve İnsan Odaklı Olma

ii. Çeşitlilik, Ayrımcılık Yapmama ve Adalet

iii. Çevresel ve Toplumsal Refaha Öncelik Verme

iv. Şeffaflık ve Hesap Verilebilirlik

v. Teknik Sağlamlık ve Güvenlik

vi. Gizlilik ve Veri Yönetimi.

---

sion 2", (*https://standards.ieee.org/wp-content/uploads/import/documents/other/ead_v2.pdf,* E.T.: 09.07.2024), s. 150.

86 UNESCO (Recommendation), s. 30.

87 *High-Level Expert Group on Artificial Intelligence: "Ethics Guidelines for Trustworthy AI",* (*https://op.europa.eu/en/publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1,* E.T.: 09.07.2024).

88 *The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems: "Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems, Version 2", (https://standards.ieee.org/wp-content/uploads/import/documents/other/ead_v2.pdf, E.T.: 09.07.2024).*

89 UNESCO: "*Recommendation on the Ethics of Artificial Intelligence",* (*https://unesdoc.unesco.org/ark:/48223/pf0000381137?posInSet=2&queryId=0f338b37-d696-4b9c-9962-251f99ba628f,* E.T.: 09.07.2024).

90 University of Montréal: "*Montréal Declaration for a Responsible Development of Artificial Intelligence",* (*https://declarationmontreal-iaresponsable.com/wp-content/uploads/2023/04/UdeM_Decl-IA-Resp_LA-Declaration-ENG_WEB_09-07-19.pdf,* E.T.: 09.07.2024).

Farklı metinlerin ilkeleri ele alış biçimlerindeki zamansal, sektörel ve bölgesel farklılıklar, çalışmanın ilerleyen bölümlerinde ayrıca değerlendirilecektir.

1. İnsan Haklarına Saygılı ve İnsan Odaklı Olma

Diğer pek çok teknoloji gibi YZ sistemlerinin de insan haklarını koruyup geliştirme kadar ihlal etme, mevcut ihlalleri güçlendirme veya kolaylaştırma potansiyeli bulunur. Özgürlüklere müdahale, ayrımcılığın derinleşmesi, sosyal ve ekonomik haklardan gereği gibi yararlanamama, demokrasi ve hukukun üstünlüğünün zedelenmesi bu riskler arasındadır[91]. Risklerle mücadelede ve güvenilir YZ'nin inşasında insan haklarına saygılı bir yaklaşım elzemdir. Bu yaklaşımın temelinde ise insan onuruna saygı yer alır. YZ etiği kapsamında insan onuru, karşılığını insan odaklı yaklaşımda bulmaktadır[92]. Bu ilke, insan haklarının ve insan onurunun korunmasına ilişkin yerleşmiş uygulamaların ve benimsenen değerlerin YZ sistemlerine entegre edilmesine, bireyin temel hak ve özgürlüklere aykırı uygulamalar karşısında etkili koruma mekanizmalarına sahip olabilmesine yardımcı olabilir[93] .

Bu ilke kapsamında YZ sistemleri, insanlığın yararını gözeten ve önceleyen, insanlara zarar vermeyen, insan haklarına, hukukun üstünlüğüne ve demokratik değerlere saygılı, kapsayıcı, barışçıl, adil, katılımcı ve kolaylaştırıcı nitelikte tasarlanmalıdır[94]. Temel amaç, YZ'nin bireyin zihinsel ve fizik-

---

91 Konuya ilişkin ayrıntılı değerlendirmeler için bkz. CAHAI (Towards Regulation of AI Systems), s. 23-32.

92 High-Level Expert Group on Artificial Intelligence (Ethics Guidelines), s. 9-10.

93 Access Now: "*Human Rights in the Age of Artificial Intelligence",* (*https://www.accessnow.org/wp-content/uploads/2018/11/AI-and-Human-Rights.pdf,* E.T.: 09.07.2024), s. 6, 37.

94 CAHAI (Feasibility Study), s. 27-29; European Commission for the Efficiency of Justice (CEPEJ) of the Council of Europe: "*European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment",* (*https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c*, E.T.: 09.07.2024), s. 8; High-Level Expert Group on Artificial Intelligence (Ethics Guidelines for Trustworthy AI), s. 10-11; OECD: *"Recommendation of the Council on Artificial Intelligence",* OECD/LEGAL/0449, (*https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449#backgroundInformation,* E.T.: 09.07.2024), s. 8; T.C. Sanayi ve Teknoloji Bakanlığı/Türkiye Cumhuriyeti Cumhurbaşkanlığı Dijital Dönüşüm Ofisi: "*Ulusal Yapay Zekâ Stratejisi 2021-2025",* (*https://cbddo.gov.tr/SharedFolderServer/Genel/File/TR-UlusalYZ Stratejisi2021-2025.pdf,* E.T.: 09.07.2024), s. 59; The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems, s. 22-23; UNESCO (Recommendation), s. 18-20.

sel kapasitelerinin geliştirilmesine, sosyal ve kültürel becerilerinin artırılmasına olanak tanıması ve katkı sunması, insan özerkliğine ve bireyin kendi kaderini tayin hakkına zarar vermemesidir. Ayrıca YZ'nin bireyi manipüle etmesi, şartlandırması, nesneleştirmesi veya ikincilleştirmesi de bu ilke kapsamında önlenmeye çalışılmaktadır[95].

İnsanı döngünün dışına çıkarmak, potansiyel risklerin tespitini, denetlenmesini ve bu risklerle mücadeleyi zorlaştırabilir. Bu kapsamda insan denetimi önemli bir rol oynamaktadır. Birey, hangi kararların insan tarafından alınacağını seçme özgürlüğüne sahip olmalı ve bu özgürlüğü YZ sistemlerine devretmemelidir[96]. İnsan denetimi, insan özerkliğinin teminatıdır[97].

Toplum, YZ sistemlerinin yaygınlaşması ile yaşanan dönüşüme hazırlıklı hale getirilmelidir. Bilgi ve güç asimetrisinin önüne geçebilmek için bireyin YZ okuryazarlığının teşvik edilmesi, gerekli becerilerle donatılması, YZ'nin potansiyel kullanımları, sınırları ve riskleri konusunda kamuoyu farkındalığının artırılması bir gereksinim durumuna gelmektedir[98]. Bunun yanında, IEEE'nin de işaret ettiği üzere, bireyi YZ'nin yarattığı dönüşüme hazırlamak kadar, YZ tarafından ikame edilen ya da edilebilecek olan iş kollarına karşılık yeni iş alanları tesis ederek ekonomik hayata katılımın sürekliliğini sağlamak da konunun önemli bir boyutunu oluşturur[99]. YZ alanındaki gelişmelerin bireysel, toplumsal ve ekonomik yönleri bulunduğu dikkatten kaçmamalıdır.

2. Çeşitlilik, Eşitlik, Ayrımcılık Yapmama ve Adalet

YZ sistemlerinin yarattığı önemli sakıncaların başında çeşitlilik, eşitlik, ayrımcılık yapmama ve adalet ilkelerine yönelik potansiyel riskler barındırması gelmektedir. Gerçekten bu sistemlerin kullanımı, ayrımcılığa ve ön

---

95 High-Level Expert Group on Artificial Intelligence (Ethics Guidelines), s. 10-12; The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems, s. 25; UNESCO (Recommendation), s. 18, 20; University of Montréal, s. 8-11.

96 AI4People, s. 12, 18-19; Floridi (The Ethics of AI), s. 62.

97 High-Level Expert Group on Artificial Intelligence (Ethics Guidelines), s. 12; The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems, s. 152.

98 European Commission for the Efficiency of Justice (CEPEJ) of the Council of Europe, s. 12; High-Level Expert Group on Artificial Intelligence (Ethics Guidelines), s. 23; T.C. Sanayi ve Teknoloji Bakanlığı/Türkiye Cumhuriyeti Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, s. 59.

99 The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems, s. 136-140.

yargıya neden olabilir, bunları pekiştirebilir, çeşitliliği zedeleyebilir, bireyin sınıflandırılmasına ve eşitliğe aykırı uygulamalara maruz kalmasına neden olabilir[100]. Temel hak ve özgürlüklere karşı bu tehditlerin tek kaynağı YZ olmasa da ayırt edici unsur, YZ sistemlerinin bu risklerin boyutunu ve yaygınlığını, etkilenen insan sayısını artırması ve bu etkilerin tespitini zorlaştırmasıdır[101]. Bu etkiler genel anlamda sistemlerin eğitildikleri veri setlerinden kaynaklansa da tasarım tercihleri, erişim imkânları, toplumun farklı kesimlerinin süreçlere dâhil edilmesi de etki eden faktörler arasındadır[102]. Bu etik ilke ile risklere ilişkin farkındalığın artırılması; eşit, adil, kapsayıcı ve ayrımcılık yapmayan uygulamalar için etkili mekanizmaların oluşturulması hedeflenmektedir.

YZ sistemleri bireyi çeşitli etiketlerle tanımlayabilir ve sınıflandırabilir. Algoritmik ön yargıları destekleyen bu tarz uygulamalar, bireyin temel hak ve özgürlüklerden gereği gibi yararlanamamasına, potansiyel veya mevcut dezavantajların pekiştirilmesine, eşitliğe aykırı muameleye maruz kalmasına sebebiyet verebilir[103]. Benzer analiz yöntemleri, "yankı odaları" veya "filter bubble effect" oluşturarak toplumda homojenleşmeye neden olabilir. Bu durum bireyin radikalleşmesine sebep olurken farklı fikir ve tercihlere erişimi zorlaştırarak çeşitliliği engellemektedir[104]. Toplumun farklı kesimlerinin, YZ inovasyonunun yaşam döngüsüne dahil edilmesi ve çok paydaşlı katılımın ilke olarak benimsenmesi kültürel, sosyal, etnik, dini ve cinsel çeşitliliği sağlamada etkili yöntemlerdir[105]. Katılımda çeşitliliğin

---

100 Access Now, s. 24-25; CAHAI (Towards Regulation of AI Systems), s. 28; High-Level Expert Group on Artificial Intelligence (Ethics Guidelines), s. 18-19.

101 CAHAI (Towards Regulation of AI Systems), s. 28.

102 CAHAI (Towards Regulation of AI Systems), s. 28; High-Level Expert Group on Artificial Intelligence (Ethics Guidelines), s. 18-19; Zuiderveen Borgesius, F.: *"Discrimination, Artificial Intelligence, and Algoritmic Desicion-Making"*, (*https://rm.coe.int/discrimination-artificial-intelligence-and-algorithmic-decision-making/1680925d73,* E.T.: 09.07.2024), s. 15-23.

103 Zuiderveen Borgesius, s. 16-18.

104 Access Now, s. 23; CAHAI (Feasibility Study), par. 27; CAHAI (Towards Regulation of AI Systems), s. 27.

105 Access Now/Amnesty International: "*The Toronto Declaration: Protecting the right to equality and non-discrimination in machine learning systems",* (*https://www.torontodeclaration.org/wp-content/uploads/2019/12/Toronto_Declaration_English.pdf,* E.T.: 09.07.2024), s. 6; High-Level Expert Group on Artificial Intelligence (Ethics Guidelines), s. 11; T.C. Sanayi ve Teknoloji Bakanlığı/Türkiye Cumhuriyeti Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, s. 59-61; University of Montréal, s. 14; UNESCO (Recommendation), s. 19.

sağlanması, veri setlerinde de çeşitliliği artırır. Ancak bu ilkenin tesisi için veri setinin çeşitliliği ve kapsayıcılığı kadar kalitesi de önem arz eder[106].

Bu ilke kapsamında, bireyin maddi ve manevi olarak kendisini var edebilmesine engel olan, sosyal ilişkilerini zedeleyen, fiziksel ve zihinsel refahını olumsuz etkileyen, adaleti ve demokratik süreçleri tehdit eden, nefret söylemleri oluşturan[107], yanlış bilgi üreten ve yayan, doğru bilgiye erişimi güçleştiren, toplumsal infiale sebep olabilecek[108] her türlü uygulama dikkatle değerlendirilmelidir[109].

Bu ilke uyarınca YZ sistemlerine erişim ve bu sistemlerden yararlanma olanakları toplumun her kesimine adil ve eşit şekilde dağıtılmalı, sağlanan faydaların dağıtımı da benzer şekilde planlanmalıdır[110]. Evrensel tasarım ilkelerinin ve sistemin aktörlerinin anlamlı istişareleri sonucu elde edilen geri bildirimlerin sistemlerin yaşam döngüsüne dâhil edilmesi, çeşitlilik, katılım, eşitlik, temel hak ve özgürlüklere saygı gibi unsurlar bakımından anlamlıdır[111].

3. Çevresel ve Toplumsal Refaha Öncelik Verme

Çevre ve toplum, YZ sistemlerinin yaşam döngüsünde yer alan sessiz paydaşlardır[112]. Bireysel tecrübeler, toplumsal ölçekte etkilere zemin hazırlamaktadır. Nitekim bireysel veya toplumsal uygulamalar birtakım çevresel etkiler doğurmaktadır. Bu ilke, YZ'nin etkilerinin daha geniş bir perspektiften ele alınmasını sağlamaktadır.

---

106 Achten, N./Fjeld, J./Hilligoss, H./Nagy, A.C./Srikumar, M: *Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-based Approaches to Principles for AI*, Berkman Klein Center for Internet & Society 2020, Research Publication No 2020-1, s. 49.

107 Konuya ilişkin örnek olay için bkz. Schwartz, O. (2019), *In 2016, Microsoft's Racist Chatbot Revealed the Dangers of Online Conversation*, (*https://spectrum.ieee.org/in-2016-microsofts-racist-chatbot-revealed-the-dangers-of-online-conversation,* E.T.: 09.07.2024).

108 European Parliament: *"Tackling deepfakes in European policy"*, (*https://www.europarl.europa.eu/RegData/etudes/STUD/2021/690039/EPRS_STU(2021)690039_EN.pdf,* E.T.: 09.07.2024), s. 24-25, 29-34.

109 Floridi, L./Taddeo, M.: *How AI can be a force for good*, Science 2018, C. 361, S. 6404, s. 752; High-Level Expert Group on Artificial Intelligence (Ethics Guidelines), s. 19.

110 OECD (Recommendation), s. 10; UNI Global Union: "*Top 10 Principles for Ethical Artificial Intelligence",* (*https://uniglobalunion.org/wp-content/uploads/uni_ethical_ai.pdf,* E.T.: 09.07.2024), s. 8.

111 Access Now/Amnesty International, s. 6; High-Level Expert Group on Artificial Intelligence (Ethics Guidelines), s. 18-19.

112 High-Level Expert Group on Artificial Intelligence (Ethics Guidelines), s. 19.

Çevresel ve toplumsal refaha öncelik verme, çevre ve toplum faydasını hedeflemeyi, sosyal ve doğal yaşamda yer alan risk ve olumsuzluklarla anlamlı mücadeleyi, sürdürülebilir ve sorumlu yaklaşımların benimsenmesini gerektirir[113]. Ekosistemin ve biyolojik çeşitliliğin korunması ve geliştirmesi, çevresel ve toplumsal refaha katkı sağlar. YZ sistemleri, sürdürülebilir kalkınmanın yanı sıra kaynakların etkili kullanımı, geri dönüşüm süreçlerinin yaygınlaştırılması, iklim değişikliyle mücadele, sürdürülebilir tüketim ve üretim modellerinin oluşturulması, doğal afetlerle mücadele, eğitimde fırsat eşitliğinin sağlanması, salgın hastalıklarla mücadele gibi süreçlerde etkili bir araç olarak kullanılabilir[114].

YZ sistemlerinin yaşam döngüsünün doğrudan ve dolaylı çevresel etkileri değerlendirilmeksizin geliştirilmesi ve kullanımı ciddi riskleri barındırır. Bu bağlamda olumsuz çevresel etkileri azaltacak çevre dostu politikalar benimsenmelidir[115]. Bunun yanında YZ'nin birey ve toplum üzerinde dönüştürücü ve uzun vadeli etkilerinin olabileceği, sürdürülebilirliğe ilişkin değerlendirmelerde göz önünde bulundurulmalıdır[116]. Belirtmek gerekir ki toplumsal refaha ilişkin başlıklar, kültürel mirasın korunması ve zenginleştirilmesinden[117] sosyal ve demokratik etkilere kadar geniş bir yelpazeden oluşmaktadır.

4. Şeffaflık ve Hesap Verilebilirlik

Şeffaflık ve hesap verilebilirlik ilkesi, birbirini tamamlayan iki bileşendir[118]. Şeffaflık, YZ süreçlerinin izlenebilir ve açıklanabilir olmasını; sistemlerin yetenekleri, sınırlamaları ve amaçları hakkında anlamlı bilgilerin sağlanmasını gerektirir[119]. Hesap verilebilirlik ise sistemlerin yaşam dön-

113 Achten/Fjeld/Hilligoss/Nagy/Srikumar, s. 31.

114 High-Level Expert Group on Artificial Intelligence (Ethics Guidelines), s. 32-33; The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems, s. 131-135; UNESCO (Recommendation), s. 30-31; UNI Global Union, s. 7; United Nations: "*Interim Report: Governing AI for Humanity",* (*https://www.un.org/sites/un2.un.org/files/un_ai_advisory_body_governing_ai_for_humanity_interim_report.pdf*, E.T.: 09.07.2024), s. 6-7; University of Montréal, s. 17.

115 UNESCO (Recommendation), s. 19, 30-31.

116 Leslie, D.: "*Understanding artificial intelligence ethics and safety: A guide for the responsible design and implementation of AI systems in the public sector*", The Alan Turing Institute 2019, (*https://doi.org/10.5281/zenodo.3240529,* E.T.: 09.07.2024), s. 26.

117 UNESCO (Recommendation), s. 32-33.

118 The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems, s. 27, 29.

119 The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems, s. 29.

güsünün belgelenmesini, açıklanmasını, denetlenebilmesini ve sorumluların belirlenebilmesini sağlamaktadır[120]. Şeffaflık ve hesap verilebilirlik, temel hak ve özgürlükler ile diğer etik ilkelere uyum, güvenilir YZ için öngörülen güvencelerin mevcudiyeti, risklerin saptanması ve denetlenebilmesi, sorumluların belirlenebilmesi, etkili telafi mekanizmalarının oluşturulması için bir ön koşuldur. Bu ilkeler, güvenilir YZ inşasında anahtar ilkelerdir[121].

AB YZ Üst Düzey Uzman Grubu, şeffaflık ilkesini üç ana başlık altında incelemektedir: İzlenebilirlik, açıklanabilirlik ve iletişim. İzlenebilirlik, YZ süreçlerinin (veri toplama, veri etiketleme, kullanılan algoritmalar, kararlar) belli standartlarda belgelenmesini gerektirir. Böylelikle YZ sistemlerinin kararları açıklanabilir veya hatalı kararları, nedenleri ile birlikte saptanabilir ve denetlenebilir. İzlenebilirlik, potansiyel hataların önlenmesine yönelir. Açıklanabilirlik ise bir sistemin teknik süreçlerinin yanı sıra iş modellerinin ve insanlar tarafından alınan kararların açıklanabilmesini ifade eder. Nitekim YZ kararlarının toplumun farklı kesimleri tarafından anlaşılabilmesi, YZ çıktısının belli bir kararı ne ölçüde etkilediğinin anlaşılmasını sağlar. Bireyin YZ ile etkileşimde olduğunu veya bir kararın YZ tarafından alındığını bilme hakkı ise iletişim açısından önemlidir. Sistemlerin yetenekleri ve sınırlamaları hakkında bireye öz ve anlaşılır açıklamalar yapmak, YZ kararlarına itiraz etme hakkı sağlamak, gereksinim halinde insan unsurunun sürece dahil edilmesini talep edebilmek[122] de bu kapsamda değerlendirilir[123].

Bu ilke açısından önemli bir husus, şeffaflığın ne düzeyde sağlanacağına karar vermektir. Asgari şeffaflık ve açıklanabilirlik seviyesi, bağlam ve etkiye uygun şekilde değerlendirilmelidir[124]. Örneğin bireyin yaşamı üzerinde etki doğuran kararların YZ kullanılarak verilmesi durumunda bireye, kararı şekillendiren faktör ve parametreleri ortaya koyan gerekçeli bir açıklama yapılmalıdır[125].

---

120 The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems, s. 27-28.

121 Floridi (The Ethics of AI), s. 63; The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems, s. 27-29; UNESCO (Recommendation), s. 22.

122 Future of Life Institute (2017), *Asilomar AI Principles*, (*https://futureoflife.org/open-letter/ai-principles/*, E.T.: 09.07.2024); OECD (Recommendations), s. 8-9; UNI Global Union, s. 6-7.

123 High-Level Expert Group on Artificial Intelligence (Ethics Guidelines), s. 18.

124 High-Level Expert Group on Artificial Intelligence (Ethics Guidelines), s. 13; UNESCO (Recommendation), s. 22.

125 High-Level Expert Group on Artificial Intelligence (Ethics Guidelines), s. 18; University of Montréal, s. 12.

AB YZ Üst Düzey Uzman Grubu, şeffaflık ilkesine benzer şekilde hesap verilebilirliği de alt başlıklar altında incelemiştir. Bu ilkenin adalet ilkesiyle doğrudan bağlantısına da işaret eden Grubun belirlediği alt başlıklar şöyledir: Denetlenebilirlik, olumsuz etkilerin azaltılması ve raporlanması, ödünleşmeler ve telafi. Denetlenebilirlik uyarınca YZ'nin yaşam döngüsünün farklı unsurları (veri, tasarım süreçleri, algoritmalar) değerlendirilmeli, belgelendirilmeli, doğrulanabilmeli ve denetlenebilmelidir. Olumsuz etkilerin azaltılması ve raporlanması, risklerin saptanmasını, değerlendirilmesini ve risklerle mücadeleyi destekler. Ödünleşmeler (trade-offs) ise etik ilkeler kapsamında öngörülen gereklilikler uygulanırken ilkeler arasında ortaya çıkabilecek gerilimi hafifletmeyi hedefler. İlkeler arası çatışmaların bulunduğu ve ödünleşmenin kaçınılmaz olduğu durumlarda, YZ kullanımı neticesinde etkilenen menfaat ve değerler arası dengenin nasıl kurulduğu belgelendirilmeli, gerekçeli şekilde açıklanabilmeli ve uygunluğu periyodik olarak denetlenmelidir. Telafi başlığı altında ise etkili ve erişilebilir telafi mekanizmalarının varlığı öngörülür. Bu unsur, güveni sağlamada etkilidir[126].

5. Teknik Sağlamlık ve Güvenlik

Teknik sağlamlık ve güvenlik ilkesi, zararın önlenmesine yönelerek güvenilir YZ sistemlerinin geliştirilmesini destekler. Güvenilir YZ sistemlerinin, her şeyden önce canlılara ve çevreye zarar vermemesi gerekir[127]. Teknik sağlamlık, sistemlerin olağan veya olağan dışı kullanımlarından kaynaklanabilecek riskleri belirleyebilmeyi, bu risklerle mücadeleye hazırlıklı olmayı, makul olmayan güvenlik risklerinin oluşmamasını, risklerle mücadelede önleyici bir yaklaşımın benimsenmesini gerektirir. Bu ilke aynı zamanda sistemlerin sınırlarının belirlenebilmesini sağlar[128].

YZ sistemlerinin güvenliği iki yönlüdür: Sistemler dışarıdan gelebilecek saldırılara karşı dayanıklı olmalı ve sistemlerin iç güvenliği sağlanmalıdır. Nitekim yetersiz güvenlik önlemleri ve sistem açıkları, sisteme karşı saldırıların karar mekanizmasında değişiklik yapmasına, sistemin gereği gibi işlememesine veya hiç yanıt vermemesine sebep olabilir. Bu durum, hatalı

126 High-Level Expert Group on Artificial Intelligence (Ethics Guidelines), s. 19-20.

127 Achten/Fjeld/Hilligoss/Nagy/Srikumar, s. 37-39.

128 Access Now/Amnesty International, s. 9; High-Level Expert Group on Artificial Intelligence (Ethics Guidelines for Trustworthy AI), s. 16-17; University of Montréal, s. 12; OECD (Recommendation), s. 9.

karar riskinin yanı sıra fiziksel zarara da neden olabilir. Bunun yanında kötü niyetli kullanıma açık sistemlerin, siber saldırılarda hem bir hedef hem de bir araç olabileceği unutulmamalıdır[129]. Bu gibi tehlikelerin önüne geçmek için uygun güvenlik önlemleri belirlenirken sistemin risk seviyesi gözetilmeli, periyodik risk değerlendirmeleri yapılmalı ve güvenlik önlemleri test edilmelidir[130].

AB YZ Üst Düzey Uzman Grubu, sistemlerin karar mekanizmalarının doğruluğunu ve öngörülebilirliğini de bu ilke kapsamında değerlendirir. Doğru girdiler ile yanlış çıktılar üreten, girdileri ve çıktıları arasında uyumsuzluk bulunan, aynı girdiler ile aynı parametrelerde farklı ve tutarsız çıktılar oluşturan YZ sistemleri doğru ve öngörülebilir değildir. Açık ve iyi tasarlanmış bir değerlendirme, geliştirme ve geri bildirim süreci, olası hataların azaltılmasını sağlar. Doğruluğu ve öngörülebilirliği destekleyen önlemler, sistemlerin sonuçlarının güvenilir ve tutarlı olmasına olumlu etki etmektedir[131].

6. Gizlilik ve Veri Yönetimi

YZ sistemlerinden kaynaklı gizliliğe ilişkin endişeler özellikle kişisel verilerin korunmasına, bireyin fiziksel, zihinsel ve ahlaki bütünlüğüne, bireyin kendini var edebilme hakkına ve bireysel özerkliğe yönelik olası ihlalleri kapsar[132]. YZ sistemlerinin, gözetim etkinliklerini kolaylaştırma, yaygınlaştırma, çeşitlendirme ve bu etkinlikler neticesinde elde edilen verilerin analizinden başkaca anlamlı sonuçlar elde edilebilmesini sağlama potansiyeli bulunur. Nitekim bireyin kişisel verilerinin YZ sistemlerinde işlenmesi, hedefe yönelik performans artışı sağlayabilse de manipülasyon, profilleme, özgür iradeyi ve bireysel özerkliği zedeleme, bireyin nesneleşmesi veya verileri üzerindeki denetimini kaybetmesi gibi birçok riski barındırmaktadır[133]. Bu riskler, gizlilik ve veri yönetimi ilkesini güvenilir YZ için vazgeçilmez hale getirmektedir.

---

129 High-Level Expert Group on Artificial Intelligence (Ethics Guidelines), s. 16; University of Montréal, s. 15.

130 Access Now/Amnesty International, s. 8-9; High-Level Expert Group on Artificial Intelligence (Ethics Guidelines), s. 17; OECD (Recommendation), s. 9.

131 High-Level Expert Group on Artificial Intelligence (Ethics Guidelines), s. 16-17; Leslie, s. 30-31.

132 Bartneck/Lütge/Wagner/Welsh, s. 68-69; CAHAI (Towards Regulation of AI Systems), s. 24-26; Küzeci, E.: Kişisel Verilerin Korunması, 4. Baskı, İstanbul 2020, s. 41-47.

133 Bartneck/Lütge/Wagner/Welsh, s. 67; Küzeci (Kişisel Verilerin Korunması), s. 61-66; Küzeci (Sayısal Fil), s. 217-220, 223-224.

Gizlilik ve kişisel verilerin koruması, YZ'nin yaşam döngüsünü bütünüyle kapsayacak şekilde sistemin aktörleri tarafından garanti edilmelidir[134]. YZ'ye girdi olarak sunulan veriler kadar çıktıları da bu korumanın bir parçası olmalıdır[135]. Birey, verileri üzerindeki denetimini kaybetmemeli ve bu denetimden vazgeçmek, bireyin YZ sistemlerine erişimi için bir koşul olarak belirlenmemelidir[136]. Güçlü ve dinamik veri koruma yasaları ve veri yönetişimi modelleri, insan hakları ihlalleri başta olmak üzere YZ'nin meydana getirdiği birçok riskin öngörülmesi, azaltılması ve denetlenmesinde etkili araçlardır[137]. Bu bağlamda, veri koruma ilke ve kurallarını içeren ulusal ve uluslararası düzenlemelerin dikkate alınması, süreçlerin bu düzenlemelere uygun tasarlanması önerilmektedir[138].

Ayrıca bu ilkenin yaşama geçirilebilmesi için birey, verilerinin YZ sistemleri kullanılarak işlendiğinden haberdar olabilmeli, bu işleme faaliyetlerine itiraz edebilmeli veya bu faaliyetleri sınırlandırabilmelidir[139]. Bu kapsamda UNESCO ve IEEE tarafından, ilgili kişilerin haklarını kullanabilmelerini ve verileri üzerindeki denetimlerini sağlayacak erişilebilir, kullanıcı dostu ve etkili mekanizmaların sisteme entegre edilmesi önerilmektedir[140].

Son olarak belirtmek gerekir ki bireyin verileri üzerinde denetim hakkını kullanmasının, insan hakları açısından gerekli olması yanında sistemin kendisi için de olumlu yönleri bulunur. Zira yanlış veri setleri sistem performansını olumsuz etkiler. Bu kapsamda, verilerin doğruluğunu, bütünlüğünü ve erişilebilirliğini sağlamak için periyodik denetimi içeren veri yönetişimi stratejileri geliştirilmelidir[141]. Bireyin haklarını YZ sistemlerinde kullanabilmesi, kişisel verilerin korunması hukukunda yer bulan, bilgilerin doğru ve güncel olması ilkesinin sağlanmasına katkı sunacaktır.

---

134 Achten/Fjeld/Hilligoss/Nagy/Srikumar, s. 25; UNESCO (Recommendation), s. 21-22.

135 High-Level Expert Group on Artificial Intelligence (Ethics Guidelines), s. 17.

136 Achten/Fjeld/Hilligoss/Nagy/Srikumar, s. 22-23; University of Montréal, s. 10.

137 Access Now, s. 30-31.

138 UNESCO (Recommendation), s. 21-23.

139 Achten/Fjeld/Hilligoss/Nagy/Srikumar, s. 23-24.

140 The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems, s. 88-112; UNESCO (Recommendation), s. 29.

141 UNESCO (Recommendation), s. 29.

B. ZAMANA, YAYIMLAYAN KURUMA VE BÖLGEYE BAĞLI YAKLAŞIM FARKLILIKLARI

YZ sistemlerinde etik ilkelerin özellikle son dönemde artan oranda ilgi çektiği, hatta YZ etiği başlıklı yeni bir inceleme alanının geliştiği görülmektedir. Bu ilginin bir göstergesi olarak pek çok kurum, kuruluş ve oluşum konuya ilişkin etik ilkeler yayımlamıştır. Bu metinlerin niteliğine ve içeriğine ilişkin derli toplu bir tablo sunmanın YZ etiği çalışmaları açısından yararlı olacağı kanaatindeyiz. Bu düşünceyle çalışmamız kapsamında incelediğimiz ve öğretide atıf alan belli başlı metinlere ilişkin bazı hususları aşağıda yer alan tabloda (bkz. Tablo 1) derledik. Bu tablo, metinlerin kimin tarafından yayımlandığını, yayım tarihini ve metinlerde yer verilen temel ilkeler ile bazı önemli konuları listelemektedir. Belirtmek gerekir ki listede esas alınan metinlerde ilkelerin detaylandırılması, ele alınış şekli ve terminolojisi arasında farklılıklar bulunmaktadır. Ancak etik ilkelerin belirlendiği metinler arasındaki ortaklıkları ortaya koyabilmek amacıyla, metinlerde ayrıca bir başlık olarak yer alan etik ilkeler siyah, metin içeriğinde yer alan ancak açıkça bir başlık olarak belirtilmemiş ilkeler ise gri renk ile tabloda işaretlenmiştir. Bazı metinlerde yalnızca gri işaretlemelerin yapılması, bu metinlerde etik ilkelere ilişkin doğrudan bir başlıklandırmaya yer verilmemesinden kaynaklanmaktadır. Bu doğrultuda -konuya ilişkin yapılan kısa değerlendirmeler dâhil olmak üzere- metinlerde yer alan her açıklamayı dikkate alınarak tabloda işaretleme yaptığımızı dikkate sunmak isteriz. Bunun yanında, aşağıdaki tabloda yer alan metinlerin tüketici nitelikte olmadığı, öğretide yer verilme ve kaynak gösterilme sıklığı dikkate alınarak yalnızca bir örneklem oluşturulduğu belirtilmelidir.

Tablo 1

YZ Etik Metinlerine ve Yaklaşımlarına Genel Bakış

Metin Başlığı	Hazırlayan	Tarih	Metin İçeriği																		
			İnsan Hakları	İnsan Odaklı Olma	Çeşitlilik, Eşitlik, Ayrımcılık Yapmama ve Adalet	İnsan Denetimi	Şeffaflık	Hesap Verilebilirlik ve Açıklanabilirlik	Teknik Sağlamlık ve Güvenlik	Çevresel ve Toplumsal Refah	Sürdürülebilirlik	Gizlilik ve Veri Gizliliği, Veri Yönetimi	Toplum Farkındalığı	Sorumluluk	Politika ve Uygulama Tavsiyeleri	Riskler ve Risk Temelli Yaklaşım	Kaynak Planlama ve Yatırım	İnsanlığın Geleceği ve İşçi Hakları	YZ'nin Askeri Amaçlı Kullanımı	
Tenets	Partnership on AI	Eylül 2016	X	X	**X**		**X**	**X**	**X**	**X**	X	X	X		X	X		**X**			
Preparing for the Future of Artificial Intelligence	Executive Office of the President - National Science and Technology Council Committee on Technology (US)	Ekim 2016			X	X		X	X	X	X	X	X	X	X	X	X	X	X		

Metin Başlığı	Hazırlayan	Tarih	Metin İçeriği																		
			İnsan Hakları	İnsan Odaklı Olma	Çeşitlilik, Eşitlik, Ayrımcılık Yapmama ve Adalet	İnsan Denetimi	Şeffaflık	Hesap Verilebilirlik ve Açıklanabilirlik	Teknik Sağlamlık ve Güvenlik	Çevresel ve Toplumsal Refah	Sürdürülebilirlik	Gizlilik ve Veri Gizliliği, Veri Yönetimi	Toplum Farkındalığı	Sorumluluk	Politika ve Uygulama Tavsiyeleri	Riskler ve Risk Temelli Yaklaşım	Kaynak Planlama ve Yatırım	İstihdamın Geleceği ve İşçi Hakları	YZ'nin Askeri Amaçlı Kullanımı
Asilomar AI Principles	Future of Life Institute	Ocak 2017	X	X	X	X	X	X	X	X		X		X	X	X	X		X
Report with Recommendations on the Commission on Civil Rules on Robotics	European Parliament (EU)	Ocak 2017	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Top 10 Principles for Ethical Artificial Intelligence	UNI Global Union	Aralık 2017	X	X	X	X	X	X		X		X		X	X			X	X
Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems, Version 2	The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems	2017	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Statement on Artificial Intelligence, Robotics and 'Autonomous' Systems	European Commission, Directorate-General for Research and Innovation, European Group on Ethics in Science and New Technologies (EU)	Mart 2018	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X		X
AI in the UK: ready, willing and able?	The Authority of the House of Lords (UK)	Nisan 2018		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
The Toronto Declaration: Protecting the right to equality and non-discrimination in machine learning systems	Access Now & Amnesty International	Mayıs 2018	X		X		X	X				X		X	X	X	X		
AI4People's Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations	AI4People (EU)	Kasım 2018		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Human Rights in the Age of Artificial Intelligence	Access Now	Kasım 2018	X		X	X	X	X				X	X	X	X	X	X	X	X
European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment	European Commission for the Efficiency of Justice (CEPEJ) of the Council of Europe (EU)	Aralık 2018	X		X	X	X	X	X			X	X		X				
Montréal Declaration for a Responsible Development of Artificial Intelligende	University of Montréal	Aralık 2018	X	X	X	X	X	X	X	X	X	X	X	X	X	X		X	
Preliminary Study on the Ethics of Artificial Intelligence	COMEST & UNESCO	Şubat 2019	X		X	X	X	X		X	X	X	X	X	X	X		X	X
Social Principles of Human-Centric AI	Government of Japan (Japan)	Mart 2019	X	X	X		X	X	X	X	X	X	X	X	X	X	X	X	
Ethics Guidelines for Trustworthy AI	High-Level Expert Group on Artificial Intelligence (EU)	Nisan 2019	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Beijing Artificial Intelligence Principles	Beijing Academy of AI (China)	Mayıs 2019	X	X	X	X	X	X	X	X	X	X	X	X	X	X		X	
Understanding artificial intelligence ethics and safety: A guide for the responsible design and implementation of AI systems in the public sector	David Leslie – The Alan Turing Institute	Haziran 2019	X	X	X	X	X	X	X	X	X	X	X	X	X	X			
Governance Principles for New Generation AI: Developing Responsible AI	National Governance Committe for the New Generation Artificial Intelligence (China)	Haziran 2019	X	X	X		X	X	X	X	X	X	X	X	X	X			
Everyday Ethics for Artificial Intelligence	IBM	Ekim 2019		X	X	X	X	X	X			X	X	X	X				
Executive Order on Promoting the Use of Trustworthy AI in Federal Government	The White House (USA)	Aralık 2020	X				X	X	X	X		X		X	X	X			
Ethics and Governance of Artificial Intelligence for Health	World Health Organization	Haziran 2021	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
Ulusal Yapay Zekâ Stratejisi 2021-2025	T.C. Sanayi ve Teknoloji Bakanlığı & Türkiye Cumhuriyeti Cumhurbaşkanlığı Dijital Dönüşüm Ofisi (Turkey)	Ağustos 2021	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	

Metin Başlığı	Hazırlayan	Tarih	Metin İçeriği																		
			İnsan Hakları	İnsan Odaklı Olma	Çeşitlilik, Eşitlik, Ayrımcılık Yapmama ve Adalet	İnsan Denetimi	Şeffaflık	Hesap Verilebilirlik ve Açıklanabilirlik	Teknik Sağlamlık ve Güvenlik	Çevresel ve Toplumsal Refah	Sürdürülebilirlik	Gizlilik ve Veri Gizliliği, Veri Yönetimi	Toplum Farkındalığı	Sorumluluk	Politika ve Uygulama Tavsiyeleri	Riskler ve Risk Temelli Yaklaşım	Kaynak Planlama ve Yatırım	İstihdamın Geleceği ve İşçi Hakları	YZ'nin Askeri Amaçlı Kullanımı
Ethical Norms for the New Generation Artificial Intelligence	National Governance Committe for the New Generation Artificial Intelligence (China)	Eylül 2021	x	x	**x**	x	**x**	x	**x**	x	x	**x**	x	x	x	**x**			
Recommendation on the Ethics of Artificial Intelligence	UNESCO	Kasım 2021	x	x	**x**	**x**	**x**	**x**	**x**	x	**x**	**x**	**x**	**x**	x	x	x	x	
Microsoft Responsible AI Standard, v2 – General Requirements	Microsoft	Haziran 2022			**x**	x	**x**	**x**	**x**			**x**		x	x	x	x		
AI Principles Progess Update	Google	2023	x	x	**x**	x	x	**x**	**x**	**x**	x	**x**	x	x	x	x	x	x	x
National Artificial Intelligence Research and Development Strategic Plan	Select Committee on Artificial Intelligence of the National Science and Technology Council (US)	Kabul Tarihi: 2016 İlk Güncellenme tarihi: 2019 Son güncellenme tarihi: Mayıs 2023	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	
Interim Report: Governing AI for Humanity	United Nations	Aralık 2023	**x**	x	**x**		x	x	x	**x**	**x**	**x**	x	x	x	x	x	x	x
Recommendation of the Council on Artificial Intelligence	OECD	Kabul tarihi: Mayıs 2019 İlk güncellenme tarihi: Kasım 2023 Son güncellenme tarihi: Mayıs 2024	**x**	x	**x**	x	**x**	**x**	**x**	**x**	**x**	**x**	x	x	x	x	x	x	

Tablo 1 incelendiğinde dikkat çeken bir husus, pek çok etik ilkenin birden fazla metinde yer aldığı, bu bağlamda farklılıklardansa ortaklıkların daha açık bir şekilde görünür olduğudur. Bu bağlamda etik ilkelerin, YZ'nin güvenilir şekilde kullanılmasını sağlamaya yöneldiği söylenebilir. Nitekim şeffaflık, eşitlik, adalet, zarar vermeme, sorumluluk ve gizlilik ilkelerine yönelik uzlaşının geliştiği görülmektedir[142]. Ancak bu, her konuda bir uzlaşının sağlandığı anlamına gelmez. İlkelere yaklaşım, ilkelerin ele alınış şekilleri, anlamsal ve kavramsal açıklamalar zamana, yayımlayan kuruma (ya da oluşuma) ve bölgeye bağlı olarak farklılık göstermektedir. Aşağıda bu husus daha yakından incelenecektir.

1. Zamansal Yaklaşım Farklılıkları

YZ etik ilkelerinin yer verildiği metinlerde zaman içinde bazı değişiklikler olduğu görülmektedir. Örneğin OECD tarafından 2019 yılında yayımlanan tavsiye ilkeler, 2023 yılında güncellenmiştir. Bu güncellemede, kavram karmaşasının önüne geçmek için YZ tanımı ve tanımda yer alan ifadeler güncellenmiş, üretken YZ (generative AI) sistemlerine vurgu yapılarak bu sistemler de tanıma dâhil edilmiştir. Bu husus, toplumsal yaşama etki eden yeni gelişmelerin metinlere yansımasının bir göstergesi olarak değerlendi-

142 CAHAI (Towards Regulation of AI Systems), s. 39.

rilebilir. Bunun yanında güncellemeler kapsamında YZ sistemlerinin örtülü ve açık amaçlarının olabileceğine dikkat çekilerek sistemlerin tasarım ve kullanıma hazır hale getirme evresinden sonra da gelişip değişebileceği gerçeğine vurgu yapılmıştır[143].

Aynı metin 2024 yılında ilgi ve bağlantının korunması, uygulanmasının kolaylaşması amacıyla yeniden güncellenmiştir. Bu kez dezenformasyonla mücadele, üretken YZ bağlamında bilgi bütünlüğünün korunması, sistemlerin amaç dışı veya kötüye kullanımları, YZ aktörlerinin sağlaması gereken bilgilerin açıklığa kavuşturulması hususlarına değinilmiştir. Geri döndürülemez zararlara sebep olan veya istenmeyen davranışlar sergileyen YZ sistemlerine ilişkin güvenlik kaygılarına ve bunlara karşı insan etkileşimine yer verilmiştir. İlk versiyondan bu yana önemi bariz bir şekilde artan çevresel sürdürülebilirlik konusuna açıkça vurgu yapılmıştır. Dünya çapında YZ politikası girişimlerinin artışı karşısında birlikte çalışabilir yönetişim ve politika ortamlarının teşvik edilmesi için birlikte çalışmanın öneminin altı çizilmiştir. Bunun yanı sıra izlenebilirlik ve risk yönetimi başta olmak üzere metnin bir kısmında daha detaylı açıklamalara yer verilmiştir[144]. İlgili metinde 2019 yılından bu yana yapılan değişiklikler ve metnin güncellenme sayısı, alanın gelişim hızını ve zamana bağlı değişimleri açıkça göstermektedir.

Tablo 1'de de görüleceği üzere YZ etik ilkelerine ilişkin metinlerin önemli bir bölümü, 2017 ve 2019 yılları arasında yayımlanmıştır. Zaman içerisinde YZ uygulamalarının çeşitlenmesi, potansiyel risklerin gerçekleşmesi neticesinde metinlerde yer alan risk örneklerinin de artırıldığı görülmektedir. Bu bağlamda özellikle üretken YZ'ye ilişkin örnek ve değerlendirmelerin nispeten yakın tarihli metinlerde yer aldığını da belirtmek gerekir.

Tabloda yer alan metinlerin yayımlanma zamanı açısından dikkat çeken bir diğer husus, ilk dönem metinlerinde riske ilişkin değerlendirmelerin daha çok "zarar" kavramı ile ilişki kurularak yapılmasıdır. Buna karşın daha yakın tarihli metinlerde "zarar" kavramına vurgu azalarak risk kategorilerinin tanımlanması ve risk temelli yaklaşımın benimsenmesi yoluna gidilmiştir. Aynı doğrultuda ilk metinlerde daha çok mevcut risklerin tanımlanması ile yetinilirken zaman içerisinde risk değerlendirmesi, riskleri önleme, risklerle mücadelede başvurulabilecek teknik ve idari yöntemler

143 OECD (Recommendation), s. 4.

144 OECD (Recommendation), s. 4-5.

tanımlanmaya başlanmış, bu önlemler sistemle bütünleştirilmesi gereken unsurlar olarak benimsenmiştir.

Benzer bir değişim istihdamın geleceği ve işçi hakları konularında da görülmektedir. Önceki tarihli metinlerde daha çok YZ'nin istihdamın geleceğinde yaratacağı sorunların tanımlandığı görülürken, ilerleyen dönemde risklerle mücadele için işçilerin YZ dönüşümüne hazır hale getirilmesine ilişkin çözüm önerileri sıralanmıştır. YZ'nin askeri kullanımına ilişkin endişeler de ilk metinlerde kısaca dile getirilip kullanımın yasaklanması tavsiye edilmiştir. Sonrasında askeri amaçlı kullanımın çeşitlerine, kullanımdan kaynaklanan risklere ve alınması gereken önlemlere de yer verilmeye başlandığı görülmektedir. Bu değişimin, YZ kullanımının çeşitliliği ve yaygınlaşması ile ilişkili olduğu düşünülebilir.

Şeffaflık ilkesine yapılan vurgular, zaman içerisinde yerini hesap verilebilirlik, denetlenebilirlik, izlenebilirlik ve açıklanabilirliğe bırakmıştır. Bu dört unsurun arasındaki bağ kuvvetlendirilmiştir. Sistemlerin yalnızca karar mekanizmalarını açıklamaya ilişkin yaklaşım, yerini daha katmanlı ve YZ'nin tüm yaşam döngüsünü içeren kapsamlı bir anlayışa bırakmıştır. Bu değişim, sorumluluğa ilişkin yaklaşımları da dönüştürmüştür. Sorumluluğa ilişkin ilk değerlendirmeler çoğunlukla insanın sorumluluğu ve YZ'nin kişilik sahibi olmaması gerekliliğini içermektedir. Yakın tarihli metinlerde ise sistemin aktörlerinin sorumlulukları, denetlenebilirlik ve hesap verilebilirlik değerlendirmeleri daha geniş yer kaplamaya başlamıştır. İnsan denetiminin tanımının da zaman içerisinde daha kapsamlı bir biçim aldığı belirtilmelidir. Kavram, özerklik ile ilişkilendirilmiş ve somutlaştırılmıştır. Benzer şekilde sürdürülebilirliğe ilişkin değerlendirmelerde YZ ekosisteminin enerji tüketimi, karbon salınımı gibi olumsuz yönlerinin yakın tarihli metinlerde daha somut bir şekilde ortaya konulduğu görülmektedir. Bu bağlamda inovasyonun ve entegrasyonun sürdürülebilir ve çevre dostu olmasına ilişkin önerilere yer verilmiştir.

2. Yayımlayan Kuruluşa Bağlı Yaklaşım Farklılıkları

Tablo 1'de yer verilen metinler, farklı kamu kurum ve kuruluşları, uluslararası kuruluşlar, sivil toplum örgütleri ile çeşitli sektörlerde etkinlik gösteren şirketler tarafından hazırlanmıştır. Farklı nitelikteki kuruluşların YZ etiğine ilişkin metinler yayımlaması, bu teknolojinin etkilerinin yaygınlığına işaret etmektedir. Öte yandan farklı kuruluşlar ve sektörler bünyesinde üretilen metinler arasında dikkat çeken bazı farklar bulunduğu belirtilmelidir.

Özel sektörde etkinlik gösteren kuruluşlarca hazırlanan metinlerin, etik ilkeleri daha genel bir şekilde açıkladığı ve örneklere daha sık başvurduğu söylenebilir. Hatta bazı örneklerde ilgili ilkenin başlığına yer vermekle yetinildiği belirtilmelidir[145]. Öte yandan konuya ilişkin hukuksal düzenlemelere uyum, en iyi uygulamaları geliştirme, şirket içi uygulamalar, potansiyel müşterilerin ve hedef kitlelerin bilgilendirilmesi, teknik çözümlerin geliştirilmesi gerekliliklerine vurgu yapıldığı görülmektedir. Bunun, YZ'nin kullanımına ilişkin olumlu bir kamu algısı yaratma çabası ile ilişkili olduğu düşünülebilir.

Belirtilen metinlerde çoğunlukla müşteri ve kullanıcı odaklı bir yaklaşım benimsendiği söylenebilir. Katılımcı süreçlere, YZ'nin düzenlenmesine ilişkin yasama faaliyetlerine dair esaslı tartışmalara, özel sektörde etkinlik gösteren kuruluşlar tarafından hazırlanan metinlerde daha sınırlı bir şekilde yer verilmiştir. Bu değerlendirmeye şeffaflık, gizlilik ve insan haklarına ilişkin ilkeler de eklenebilir. Bu doğrultuda incelenen özel sektör metinlerinin daha çok uygulamaya ilişkin değerlendirmeler ve güçlükler karşısında atılacak adımları açıklayan metinler izlenimi verdiği söylenebilecektir.

Öte yandan sivil toplum kuruluşlarının, hükümetler arası organizasyonların ve kamu kurumlarının etik ilkelere yaklaşımının özel sektörden farklılık gösterdiği söylenebilir. Bu metinlerde açıklamalar daha detaylıdır ve gelecekteki düzenlemelere de zemin hazırlama çabası dikkat çekmektedir. Kamu sektörünün ekonomik büyümeye ve istihdama ilişkin vurgusu, sivil toplum kuruluşlarında yerini özel sektörün hesap verilebilirliğine bırakmaktadır.

Hükümetler arası kuruluşlarca yayımlanan metinlerin etik ilke yelpazesinin daha geniş olduğunu söylemek yanlış olmayacaktır. Bu metinlerde hesap verilebilirlik, farklı sektörlerin YZ'nin inovasyonu ve sürdürülebilirliği için koordine şekilde çalışması gerekliliği, çok paydaşlı ve çok disiplinli yaklaşım öne çıkmaktadır.

---

145 Örneğin Microsoft tarafından hazırlanan metinde ilkeler, sorumlu YZ kullanımı için hedefler olarak belirlenmiştir. Bu kapsamda her bir hedef altında alt başlıklar, gereklilikler ve kullanılabilecek araçlar sıralanmışsa da kavramın tanımı ve içeriğine ilişkin bir açıklama yapılmamıştır. Bkz. Microsoft: *"Microsoft Responsible AI Standard, v2 – General Requirements"*, (*https://blogs.microsoft.com/wp-content/uploads/prod/sites/5/2022/06/Microsoft-Responsible-AI-Standard-v2-General-Requirements-3.pdf,* E.T.: 09.07.2024).

Nitekim IBM tarafından hazırlanan metinde de benimsenen etik ilkeler liste olarak sıralanmış, ilkeler altında ayrıca bir açıklamaya yer verilmemiştir. Devam eden kısımda yapılan açıklamalar, örnek uygulama pratiklerini ve tavsiyeleri içermektedir. Bkz. IBM: *"Everyday Ethics for Artificial Intelligence"*, (*https://www.ibm.com/watson/assets/duo/pdf/ everydayethics.pdf,* E.T.: 09.07.2024).

3. Bölgesel Yaklaşım Farklılıkları

YZ konulu araştırma ve geliştirme çalışmalarının, etik ilkeler ve yasal düzenlemeler konulu metinlerin büyük bölümü Kuzey Amerika, Kanada, Birleşik Krallık, AB kurumları ve AB ülkeleri menşeilidir[146]. Bu bölgelerin kültür, felsefe ve yaklaşımının aşırı temsilinin, YZ'nin inovasyonunda uluslararası yönetişimin sağlanmasını, çeşitlilik ve genel kabul edilebilirliği olumsuz etkileyeceği, yerel etik bakış açıları ile uyumsuzluklar yaratabileceği ve bunun da potansiyel küresel faydaların gerçekleşmesini engelleyeceği, kapsayıcı olma idealine zarar vereceği yönünde endişeler mevcuttur. Nitekim YZ etik çerçevelerinin, güvenilirliği artırarak toplumun her kesimine hitap edebilecek, genel kabul edilebilirliği haiz nitelikte olması gerekir[147]. Bahsi geçen bölgelerin YZ yönetişimindeki aşırı temsiline karşılık Çin Halk Cumhuriyeti gibi farklı ülkelerin de konuya yönelik çalışmalarının arttığı belirtilmelidir[148].

Bölgesel yaklaşım farklılıklarının, zamana ve metni yayımlayan kuruluşa bağlı farklılıklar kadar açık olmadığı söylenebilir. Genel yaklaşım ve ilkeler bağlamında bölgeler arasında benzerlik olduğu belirtilmelidir. İlkesel anlamda özellikle AB yaklaşımına uyumluluk göze çarpmaktadır.

Tablo 1'de yer alan metinleri, bölgesel olarak Asya, ABD ve AB olarak üçe ayırarak incelemek olanaklıdır. Bu metinlerden AB menşeili olanlarda insan odaklı yaklaşıma vurgu yapıldığı görülmektedir. Bu kapsamda insan haklarına, YZ'nin demokrasi, adalet ve toplum üzerindeki olumsuz etkilerine, temel hak ve özgürlüklere ilişkin detaylı değerlendirmelere ve örneklere yer verilmiştir. AB metinlerinin tamamına yakınında, YZ'nin uluslararası yönetişiminde ve yaşam döngüsünde insan hakları temelli bir yaklaşımın öncelendiği açıkça ifade edilmektedir. İnsan denetimine ilişkin en detaylı açıklamalara yine bu metinlerde rastlanmaktadır.

---

146 Barbosa, C./Corrêa, N.K./De Oliveira, N./Del Pino, C./Galvão, C./Galvão, L./Mambrini, R./Massmann, D./Pinto, E.P./Santos, J.W./Terem, E.: *Worldwide AI ethics: A review of 200 guidelines and recommendations for AI governance,* Patterns 2023 C. 4, S. 10, 100857, s. 7.

147 Ienca, M./Jobin, A./Vayena, E.: *The global landscape of AI ethics guidelines*, Nature Machine Intelligence 2019, S. 1, s. 391; Lewis, D./Roche, C./Wall, P. J.: *Ethics and diversity in artificial intelligence policies, strategies and initiatives*, AI and Ethics 2023, C. 3, s. 1096.

148 CAHAI (Towards Regulation of AI Systems), s. 54.

ABD ve Asya bölgesinden kamu kurumları tarafından yayımlanan metinlerde[149], YZ sistemlerinin kısa sürede toplumsal ve gündelik hayata entegrasyonu ve kullanımına odaklanıldığı söylenebilir. İnovasyonu teşvik ederek olanaklı olan en kısa sürede entegrasyonu sağlama ve bunu yaparken maksimum faydayı elde etme düşüncesi metinlere yansımıştır. Etik kaygılar daha çok araştırma ve geliştirme, yatırım, sistemi uygulama, kullanım gibi konularda yoğunlaşmaktadır. Sistemlerin kullanımının, toplumun her kesimi tarafından benimsenmesinin yanı sıra çok paydaşlı katılım ve devletin farklı aktörlerle iş birliğini teşvikine ilişkin değerlendirmeler de göze çarpmaktadır. Asya metinlerinde YZ'nin toplumun geliştirilmesini ve kalkınmayı desteklemesi odak noktalar iken ABD metinlerinde YZ temalı araştırma ve geliştirme faaliyetlerine ağırlık verilmiştir.

ABD'de kamu kurumları tarafından yayımlanan metinlerde[150] uzun vadeli araştırma ihtiyacına ve toplumsal entegrasyona odaklanılmakta, düzenleyici role ilişkin görece daha sınırlı açıklama bulunmaktadır. Bu bağlamda inovasyonun devamlılığına ve artışına yönelik vurgu göze çarpmaktadır. Birey ve toplumun YZ sistemlerine güveninin sağlanması, YZ'nin potansiyel kullanımının ve faydalarının artmasında anahtar olarak görülmüştür. Entegrasyon sürecinde temel Amerikan değerlerinin korunmasına ilişkin hassasiyet de dile getirilmiştir.

---

149 Örneğin bkz. Executive Office of the President National Science and Technology Council Committee on Technology: *"Preparing for the Future of Artificial Intelligence"*, (*https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf*, E.T.: 09.07.2024); Government of Japan: *"Social Principles of Human-Centric AI"*, (*https://www.cas.go.jp/jp/seisaku/jinkouchinou/pdf/humancentricai.pdf*, E.T.: 09.07.2024); National Governance Committee for the New Generation Artificial Intelligence: *"Governance Principles for a New Generation of Artificial Intelligence: Develop Responsible Artificial Intelligence"*, (*https://perma.cc/V9FL-H6J7*, E.T.: 09.07.2024).

150 Örneğin bkz. Executive Office of the President - National Science and Technology Council Committee on Technology: *"Preparing for the Future of Artificial Intelligence"*, (*https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf,* E.T.: 09.07.2024); The White House: "*Executive Order on Promoting the Use of Trustworthy AI in Federal Government*", (*https://www.govinfo.gov/content/pkg/FR-2020-12-08/pdf/2020-27065.pdf*, E.T.: 09.07.2024); Select Committee on Artificial Intelligence of the National Science and Technology Council: "*National Artificial Intelligence Research and Development Strategic Plan*", 2023 Update, (*https://www.whitehouse.gov/wp-content/uploads/2023/05/ National-Artificial-Intelligence-Research-and-Development-Strategic-Plan-2023-Update.pdf*, E.T.: 09.07.2024).

SONUÇ

YZ etik ilkeleri, gelişen sistemlerin yaratabileceği risklerin en düşük düzeye indirilmesini hedefler. Etiğin yaptırım gücü olmaması, bu ilkelerin hedeflenen amaçları gerçekleştirmesi konusunda şüphelere neden olmaktadır. Ancak etik ilkelerin benimsenmesinin, hukuksal olarak düzenlenmiş ve yaptırıma bağlanmış kuralların eksik kaldığı noktalarda yol gösterici olacağı ve ayrıca gelecekteki olası hukuksal düzenlemelere kaynak oluşturabileceği unutulmamalıdır. Bu açıdan, bu bölümün kapanışını yaparken, kitabımızın hedefleri ve kapsamı da dikkate alınarak, yukarıda aktardığımız ilkelerin kişisel verilerin korunması düzenlemeleri ile ilişkisini ana hatlarıyla ortaya koymak isteriz.

YZ sistemlerinin ortaya çıkardığı riskler arasında kişisel verilerin korunması ile ilişkili olanlar özellikle dikkat çekicidir. Her şeyden önce bu sistemlerin gözetim (surveillance) etkinliklerini derinleştirme potansiyeli bulunur. Gözetim, bireyin sürekli ve sistemli bir şekilde izlenmesine ve bunun yaşamını çeşitli biçimlerde etkilemesine neden olmaktadır. Bununla ilişkili olarak gözetim, bireysel özerkliğin ve toplumsal çeşitliliğin zarar görmesi ve hatta yitirilmesi tehlikesini barındırır. YZ sistemlerinin veri işleme potansiyeli, bu risklerin katlanarak artmasına neden olabilir. Riskleri en az seviyeye indirebilmek için kişisel verilerin korunmasına ilişkin ilke ve kuralların YZ sistemleri üzerinde etkin bir şekilde uygulanması önemlidir. Ancak bu ilke ve kuralların YZ sistemlerinde uygulanmasını zorlaştıran bazı hususlar dikkat çekmektedir. Bunlar, hangi verilerin kişisel veri niteliğinde olduğunun saptanması aşamasında dahi görülebilir. Nitekim YZ'nin Büyük Veri kümelerine erişimi ve bu verilerden başkaca veriler türetmesi, kişisel veri tanımını genişletmekte ve bunun sonucunda kişisel veriler ile kişisel veri niteliğini haiz olmayan veriler arasındaki fark giderek bulanıklaşmaktadır[151].

Bu bölüm kapsamında açıklanan YZ etik ilkeleri, kişisel verilerin korunmasına ilişkin düzenlemelerin uygulamasını desteklemektedir. Bunu en açık şekilde "gizlilik ve veri yönetimi" ilkesi açısından saptayabiliriz. Nitekim bu ilke, YZ'nin yaşam döngüsü boyunca temas ettiği, yalnızca girdileri değil çıktıları da içeren verilerin güvenliğini ve gizliliğini sağlamayı amaçlamaktadır. Gizlilik ve veri yönetimi ilkesi, bir bütün olarak kişisel verilerin korunması yaklaşımını YZ uygulamalarına yansıtmaktadır. Nitekim kişisel

[151] CAHAI (Feasibility Study), s. 35-36.

verilerin korunmasına ilişkin düzenlemeler, YZ sistemlerinin gizlilikle ilişkili ortaya koyduğu sorunlar değerlendirilirken, ilkeler ve önlemler tasarlanırken de etkili olmuştur[152]. Öte yandan, YZ sistemleri dolayısıyla ortaya çıkan yeni sorunlar, kişisel verilerin korunmasına ilişkin düzenlemelerin yeniden değerlendirilmesini gerekli kılan bazı hususlar da barındırmaktadır. Bu açıdan YZ etiğine ilişkin çeşitli metinlerde yer bulan gizlilik ve veri yönetimi ilkesi, kişisel verilerin korunması alanında etkili teknik ve idari çözümlerin geliştirilmesinde destek olabilecektir.

"Gizlilik ve veri yönetimi" ilkesi yanında başka pek çok YZ etik ilkesi de kişisel verilerin korunması hakkı ile ilişkilidir. Örneğin, "insan haklarına saygılı ve insan odaklı olma" ilkesi, kişisel verilerin korunması hakkının koruduğu temel değerler ve düzenlemelerde yer bulan çeşitli haklar ile doğrudan ilişkilidir. Bunlar arasında otomatik kararlara konu edilmemeyi talep hakkı özellikle dikkat çekicidir. Yaşamı üzerinde önemli etkiler doğuran kararların YZ kullanılarak verilmesi halinde ilgili kişi, sistemin karar mekanizması hakkında bilgilendirilmelidir. Kararı şekillendiren faktör ve parametreler ortaya konarak gerekçelendirilmiş bir açıklama sağlanmalıdır. Bu husus, kişisel verilerin korunması hakkının bir gereği olduğu gibi gizlilik ve veri yönetimi ilkesi yanında şeffaflık gibi YZ etiği kapsamındaki başka ilkelerin de bir gereğidir.

Etik ilkeler arasında yer alan şeffaflık ve hesap verilebilirlik ise veri koruma düzenlemeleri için vazgeçilmez unsurlar arasındadır. YZ etiğinin temel yapı taşlarını oluşturan bu ilkeler, ilgili düzenlemelerde de doğrudan yer almakta ve çeşitli ilke ve yükümlülüklerde karşılığını bulmaktadır. Örneğin şeffaflık ilkesi aydınlatma yükümlülüğü, bilgilendirmeye dayalı rıza, belirli, açık ve meşru amaçlarla veri işleme gerekliliği, tasarımda ve varsayılanlarda gizlilik, bilgiye erişim hakkı ile doğrudan bağlantılıdır. Hesap verilebilirlik ilkesi ise zararın giderilmesini talep hakkı, başvuru ve şikâyet hakları, tasarımda gizlilik, bilgiye erişim hakkı, veri güvenliğinin tesis edilmesi ile ilişkilidir. Bununla birlikte, veri koruma düzenlemelerinde yer alan veri koruma etki değerlendirmesi, veri koruma görevlisi atanması, davranış kuralları ve sertifikasyon gibi yöntem ve araçlar ise bu ilkenin gereklerini yerine getirmek için öngörülen etkili mekanizmalardır. YZ sistemlerinin temel hak ve özgürlükler üzerinde olumsuz etkilerinin olduğu senaryolarda, tamamlayıcı bir unsur olarak temel haklar etki değerlendirmesi yapıl-

[152] Achten/Fjeld/Hilligoss/Nagy/Srikumar, s. 21.

ması yönündeki öneriler[153], veri koruma ilke ve kuralları ile YZ etik ilkeleri arasındaki karşılıklı ve tamamlayıcı etkiye örnek niteliğindedir.

Aynı şekilde "çeşitlilik, eşitlik, ayrımcılık yapmama ve adalet" ilkesi de kişisel verilerin korunması hakkının koruduğu temel değere işaret etmektedir. Örneğin kişisel verilerin korunmasına ilişkin pek çok düzenlemede özel nitelikli kişisel verilerin ayrı bir kategori olarak belirlenmesinin temel nedenlerinden biri, bu türdeki verilerin ayrımcılık yaratma olasılığıdır. Bu önemli riskin bertaraf edilebilmesi için ilgili kişinin sağlığı, biyometrik ve genetik verileri, siyasal düşünceleri, dinsel inançları gibi konulara ilişkin kişisel veriler daha güçlü bir koruma rejimine tabi tutulmaktadır. Dolayısıyla, ayrımcılığın önlenmesinin kişisel verilerin korunması düzenlemelerinin amaçları arasında yer aldığını rahatlıkla söyleyebiliriz. Bu durumun, kişisel verilerin YZ sistemleri tarafından işlendiği durumlar için de geçerli olacağı şüphesizdir. Zira ayrımcılık, bu sistemlerin yaratabileceği önemli riskler arasındadır. Sistemlerin kullanımının güç veya bilgi asimetrisi yaratma riskinin yanı sıra mevcut asimetriyi derinleştirmesi potansiyeli[154], bilhassa savunmasız bireylerin veya grupların YZ karşısındaki konumunun ayrıca değerlendirilmesini gerektirir[155]. Bahsi geçen risklerle mücadele için sistemlerin amaçlarını, yöntemlerini ve potansiyel etkilerini şeffaf ve anlaşılır şekilde ortaya koyabilecek etki değerlendirmeleri ve gözetim mekanizmaları önerilmektedir[156]. Bu noktada her ne kadar veri koruma düzenlemelerinde yer alan mekanizmalar uygulama alanı bulabilecek ise de yetersiz veya cevapsız kaldıkları durumlarda YZ etik ilkeleri aracılığıyla bu riskin bertaraf edilmesi beklenebilir.

Öte yandan "çevresel ve toplumsal refaha öncelik verme" ilkesi, veri koruma ilke ve kuralları ile de korunması amaçlanan bireyin kendisini toplum içerisinde özgürce var edebilmesine hizmet etmektedir. Bu ilkenin, bireyin maruz kaldığı olumsuz toplumsal etkileri bertaraf etmek için unutulma hakkından faydalanabilmesi ile ilişkisi kurulabilir. "Teknik sağlamlık ve güvenlik" ilkesi ise kişisel verilerin korunması açısından özellikle veri güvenliğinin sağlanması ilke ve kurallarını destekleyici niteliktedir. YZ sis-

153 High-Level Expert Group on Artificial Intelligence (Ethics Guidelines), s. 15.

154 United Nations, s. 8.

155 European Commission for the Efficiency of Justice (CEPEJ) of the Council of Europe, s. 9; High-Level Expert Group on Artificial Intelligence (Ethics Guidelines), s. 12; The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems, s. 52.

156 High-Level Expert Group on Artificial Intelligence (Ethics Guidelines), s. 18.

temleri, muhteviyatları gereği birçok teknik riski bünyesinde barındırmaktadır. Bu teknik riskler, veri işleme faaliyetlerinde kullanılan YZ sistemlerinin güvenliğine ilişkin endişeler doğurmaktadır. Bahsi geçen risklerin bir bölümü mevcut ilke ve kurallar aracılığıyla çözümlenebilir ancak bu düzenlemeler, gelişen ve değişen teknoloji karşısında yetersiz kalabilir. Bu durumda etik ilkeler dinamik çözümler sunabilir, güncel teknik gelişmelere cevap verebilecek nitelikte uygulamalar geliştirilmesine yardımcı olabilir.

Belirtilen hususlar yanında etik ilkeler ve veri koruma ilke ve kuralları arasındaki bir benzerliğe dikkat çekmek gerekir. Yukarıda yapılan açıklamalarda görüleceği üzere, etik ilkelerdeki birbirini tamamlayıcı olma unsuru, veri koruma düzenlemelerinde yer alan ilke ve kurallarda da varlığını göstermektedir. Bu durum, bir veri koruma ilke veya kuralının birden fazla etik ilkeyle veya bir etik ilkenin birçok veri koruma kuralıyla doğrudan bağlantılı olmasının sebebini oluşturur.

Etik ilkelere ilişkin değerlendirmelerimizi noktalarken, güncel duruma ve ilkelerin değerine ilişkin görüşlerimize kısaca yer vermek isteriz. Her ne kadar yayımlanan etik ilke metinlerinin sayısı zaman içerisinde azalmış ve yasama faaliyetlerine yönelim gözlenmişse de etik ilkeler iyi uygulamalar için önemini korumaktadır. Etik ilkeler, bir yandan hukuksal düzenlemelerde yer bulmayan yeni gelişmeler ya da mevcut ayrıksı örnekler bağlamında dikkate değer bir etki yaratabileceği gibi, öte yandan yorum etkinliklerinde bir başvuru kaynağı olmayı da sürdürecektir. YZ etiği ve ortaya koyduğu ilkelerin, zamandan ve mekândan bağımsız olarak YZ serüveninin bir parçası olmaya devam edeceği düşüncesindeyiz.

KAYNAKÇA

Access Now: Human Rights in the Age of Artificial Intelligence, (https://www.accessnow.org/wp-content/uploads/2018/11/AI-and-Human-Rights.pdf, E.T.: 09.07.2024).

Access Now ve Amnesty International: The Toronto Declaration: Protecting the right to equality and non-discrimination in machine learning systems, (https://www.torontodeclaration.org/wp-content/uploads/2019/12/Toronto_Declaration_English.pdf, E.T.: 09.07.2024).

ACHTEN, Nele, FJELD, Jessica, HILLIGOSS, Hannah, NAGY, Adam Christopher ve SRIKUMAR, Madhulika: Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-based Approaches to Principles for AI, Berkman Klein Center for Internet & Society 2020, Research Publication No 2020-1.

AHIA QUARCOO, Juanita, ANING, Justice, KUSI FOSU, Godfred ve NTI, Isaac Kofi: A mini-review of machine learning in big data analytics: Applications, challenges and prospects, Big Data Mining and Analytics 2022, C. 5, S. 2, s. 81-97.

AI4PEOPLE: AI4People's Ethical Framework for a Good AI Society: Opportunities, Risks, Principles and Recommendations, (https://eismd.eu/wp-content/uploads/2019/11/AI4People's-Ethical-Framework-for-a-Good-AI-Society_compressed.pdf, E.T.: 09.07.2024).

ALEXANDER, Cheryl Ann ve WANG, Lidong: Machine Learning in Big Data, International Journal of Mathematical, Engineering and Management Sciences 2016, C. 1, S. 2, s. 52-61.

ATTARD-FROST, Blair, DE LOS RIOS, Andres ve WALTERS, Deneille R.: The Ethics of AI business practices: a review of 47 AI ethics guidelines, AI and Ethics 2023, C. 3, s. 389-406.

BARBOSA, Camila, CORRÊA, Nicholas Kluge, DE OLIVEIRA, Nythamar, DEL PINO, Carolina, GALVÃO, Camila, GALVÃO, Luiza, MAMBRINI, Rodrigo, MASSMANN, Diogo, PINTO, Edson Pontes, SANTOS, James William, TEREM, Edmund: Worldwide AI ethics: A review of 200 guidelines and recommendations for AI governance, Patterns 2023 C. 4, S. 10, Makale No 100857.

BARTNECK, Christoph, LÜTGE, Christoph, WAGNER, Alan ve WELSH, Sean: An Introduction to Ethics in Robotics and AI, İsviçre 2020, (https://doi.org/10.1007/978-3-030-51110-4).

Beijing Academy of AI: Beijing Artificial Intelligence Principles, (https://link.springer.com/content/pdf/10.1007/s11623-019-1183-6.pdf, E.T.: 09.07.2024).

BOSTROM, Nick: How Long Before Superintelligence?, Linguistic and Philosophical Investigations 2006, C. 5, S. 1, s. 11-30.

BOSTROM, Nick. (çev. Aydar, F.B.): Süper Zekâ: Yapay Zekâ Uygulamaları, Tehlikeler ve Stratejiler, 2. Baskı, İstanbul 2020.

BOUCHER, Philip: Artificial intelligence: How does it work, why does it matter, and what can we do about it?, (https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641547/EPRS_STU(2020)641547_EN.pdf, E.T.: 09.07.2024).

BROOKS, Rodney, BRYNJOLFSSON, Erik, CALO, Ryan, ETZIONI, Oren, HAGER, Greg, HIRSCHBERG, Julia, KALYANAKRISHNAN, Shivaram, KAMAR, Ece, KRAUS, Sarit, LEYTON-BROWN, Kevin, PARKES, David, PRESS, William, SAXENIAN, AnnaLee (Anno), SHAH, Julie, STONE, Peter, TAMBE, Milind ve TELLER, Astro: Artificial Intelligence and Life in 2030, One Hundred Year Study on Artificial Intelligence, Report of the 2015 Study Panel, (https://ai100.stanford.edu/sites/g/files/sbiybj18871/files/media/file/ai100report10032016fnl_singles.pdf, E.T.: 09.07.2024).

BUCHANAN, Bruce G.: A (Very) Brief History of Artificial Intelligence, AI Magazine 2006, C. 26, S. 4, s. 53-60.

BUGINGO, Ghislain, HUANG, Karen, KATELL, Michael, KRAFFT, P.M. ve YOUNG, Meg: Defining AI in Policy versus Practice, Proceedings of the 2020 AAAAI/ACM Conference on AI, Ethics and Society (AIES'20) 2020, (https://doi.org/10.1145/3375627.3375835).

CAHAI: Feasibility Study, (https://rm.coe.int/cahai-2020-23-final-eng-feasibility-study-/1680a0c6da, E.T.: 09.07.2024), ("Feasibility Study").

CAHAI: Towards Regulation of AI Systems, (https://rm.coe.int/prems-107320-gbr-2018-compli-cahai-couv-texte-a4-bat-web/1680a0c17a, E.T.: 09.07.2024), ("Towards Regulation of AI Systems").

CAPEK, Karel (çev. Öztürk, P.): R.U.R. Rossum'un Evrensel Robotları, Ankara 2013.

COLONNA, Liane ve MAGNUSSON SJÖBERG, Cecilia: The AI Act – Comprehensive but is it Future-Proof?, Community Reference Meeting: Challenges and Opportunities of Regulating AI, WASP-HS Research Brief Series, 2022/02, (https://mau.diva-portal.org/smash/get/diva2:1695574/FULLTEXT01.pdf, E.T.:09.07.2024), s. 5-6.

COMEST & UNESCO: Preliminary Study on the Ethics of Artificial Intelligence, SHS/COMEST/EXTWG-ETHICS-AI/2019/1,
(https://unesdoc.unesco.org/ark:/48223/pf0000367823, E.T.: 09.07.2024).

DE PRATO, Giuditta, DELIPETREV, Blagoj, GÓMEZ, Emilia, LÓPEZ-COBO, Montserrat, MARTÍNEZ-PLUMED, Fernando ve SAMOILI, Sofia: AI Watch. Defining Artificial Intelligence. Towards an operational definition and taxonomy of artificial intelligence, (https://publications.jrc.ec.europa.eu/repository/handle/JRC118163, E.T.: 09.07.2024).

DEHMER, Matthias, EMMERT-STREIB, Frank ve YLI-HARJA, Olli: Artificial Intelligence: A Clarification of Misconceptions, Myths and Desired Status, Frontiers in Artificial Intelligence 2020, C. 3, Makale 524339.

DELIPETREV, Blagoj, KOSTIĆ, Uroš ve TSINARAKI, Chrisa: Historical Evolution of Artificial Intelligence, (https://publications.jrc.ec.europa.eu/repository/handle/JRC120469, E.T.: 09.07.2024).

EKİN, Beste: Kişisel Verilerin Korunması ve Rekabet Hukuku Boyutuyla Büyük Veri, 1. Baskı, İstanbul 2021.

EU-U.S. Terminology and Taxonomy for Artificial Intelligence, (https://digital-strategy.ec.europa.eu/en/library/eu-us-terminology-and-taxonomy-artificial-intelligence, E.T.: 09.07.2024).

EU-U.S. Terminology and Taxonomy for Artificial Intelligence – Second Edition, (https://digital-strategy.ec.europa.eu/en/library/eu-us-terminology-and-taxonomy-artificial-intelligence-second-edition, E.T.: 09.07.2024).

European Commission (2024), AI Act, (https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai#:~:text=Limited%20risk%20refers%20to%20AI,to%20continue%20or%20step%20back., E.T.: 09.07.2024).

European Commission, Directorate-General for Research and Innovation, European Group on Ethics in Science and New Technologies: Statement on Artificial Intelligence, Robotics and 'Autonomous' Systems, (https://op.europa.eu/en/ publication-detail/-/publication/dfebe62e-4ce9-11e8-be1d-01aa75ed71a1, E.T.: 09.07.2024).

European Commission for the Efficiency of Justice (CEPEJ) of the Council of Europe: European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment, (https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c, E.T.: 09.07.2024).

European Parliament: Report with recommendations on the Commission on Civil Law Rules on Robotics (2015/2103(INL)), A8-0005/2017, (https://www.europarl.europa.eu/doceo/document/A-8-2017-0005_EN.html, E.T.: 09.07.2024).

European Parliament: Tackling deepfakes in European policy, (https://www.europarl.europa.eu/RegData/etudes/STUD/2021/690039/EPRS_STU(2021)690039_EN.pdf, E.T.:09.07.2024).

European Parliament (2023), What is artificial intelligence and how is it used?, (https://www.europarl.europa.eu/news/en/headlines/society/20200827STO85804/what-is-artificial-intelligence-and-how-is-it-used, E.T.: 09.07.2024).

Executive Office of the President - National Science and Technology Council Committee on Technology: Preparing for the Future of Artificial Intelligence, (https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf, E.T.: 09.07.2024).

FLORIDI, Luciano: Introduction – The Importance of an Ethics-First Approach to the Development of AI, (ed. Floridi, L.), "Ethics, Governance, and Policies in Artificial Intelligence", Philosophical Studies Series, C. 144, 2021, s. 1-4.

FLORIDI, Luciano: The Ethics of Artificial Intelligence – Principles, Challenges, and Opportunities, Oxford 2023, ("The Ethics of AI").

FLORIDI, Luciano ve TADDEO, Mariarosaria: How AI can be a force for good, Science 2018, C. 361, S. 6404, s. 751-752.

Future of Life Institute (2017), Asilomar AI Principles, (https://futureoflife.org/open-letter/ai-principles/, E.T.: 09.07.2024).

Google: AI Principles Progress Update 2023, (https://ai.google/static/ documents/ai-principles-2023-progress-update.pdf, E.T.: 09.07.2024).

Government of Japan: Social Principles of Human-Centric AI, (https://www.cas.go.jp/jp/seisaku/jinkouchinou/pdf/humancentricai.pdf, E.T.: 09.07.2024).

GULLEY, Ayesha ve HILLIARD, Airlie (2023), Lost in Transl(A)t(I)on: Differing Definitions of AI, (https://www.holisticai.com/blog/comparing-definitions-of-ai, E.T.: 09.07.2024).

High-Level Expert Group on Artificial Intelligence: A Definition of AI: Main Capabilities and Disciplines, (https://ec.europa.eu/futurium/en/system/ files/ged/ai_hleg_definition_of_ai_18_december_1.pdf, E.T.: 09.07.2024), ("A Definition of AI").

High-Level Expert Group on Artificial Intelligence: Ethics Guidelines for Trustworthy AI, (https://op.europa.eu/en/publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1, E.T.: 09.07.2024), ("Ethics Guidelines").

HOBBES, Thomas. (Lim, S.): Leviathan veya Bir Din ve Dünya Devletinin İçeriği, Biçimi ve Kudreti, 4. Baskı, İstanbul 2004.

HOMEROS. (çev. Erhat, A., Can, A.K.): İlyada, 24. Baskı, İstanbul 2008.

IBM: Everyday Ethics for Artificial Intelligence, (https://www.ibm.com/watson/assets/duo/pdf/everydayethics.pdf, E.T.: 09.07.2024).

IENCA, Marcello, JOBIN, Anna ve VAYENA, Effy: The global landscape of AI ethics guidelines, Nature Machine Intelligence 2019, S. 1, s. 389–399.

KARACAN, Olcay: Hukukçuların Etik Sorumlulukları ve İlkelerin Rolü, TBB Dergisi 2022, S. 160, s. 245-258.

KARAKOÇ, Yusuf: Hukuk – Etik İlişkisi, HFSA 2012, S. 24, s. 91-95.

KUÇURADİ, İoanna: Etik ve "Etikler", Türkiye Mühendislik Haberleri 2003, S. 423, s. 7-9.

KÜZECİ, Elif: Kişisel Verilerin Korunması, 4. Baskı, İstanbul 2020, ("Kişisel Verilerin Korunması").

KÜZECİ, Elif: Sayısal Fil, 1. Baskı, İstanbul 2021, ("Sayısal Fil").

LESLIE, David: Understanding artificial intelligence ethics and safety: A guide for the responsible design and implementation of AI systems in the public sector, The Alan Turing Institute 2019, (https://doi.org/10.5281/zenodo.3240529, E.T.: 09.07.2024).

LEWIS, Dave, ROCHE, Cathy ve WALL, P. J.: Ethics and diversity in artificial intelligence policies, strategies and initiatives, AI and Ethics 2023, C. 3, s. 1095–1115.

MARTINEZ, Rex: Artificial Intelligence: Distinguishing Between Types & Definitions, Nevada Law Journal 2019, C. 19. S. 3, s. 1015-1042.

MCCARTHY, John: [Review of] Bloomfield, Brian, ed. The Question of Artificial Intelligence: Philosophical and Sociological Perspectives, Annals of the History of Computing 1988, C. 10, S. 3, s. 224-229.

MCCARTHY, John (2007), What Is Artificial Intelligence?, (http://jmc.stanford.edu/articles/whatisai/whatisai, E.T.: 09.07.2024).

MCCARTHY, John, MINSKY, Marvin L., ROCHESTER, Nathaniel ve SHANNON, Claude E.: A proposal for the Dartmouth Summer Research Project on Artificial Intelligence, August 31, 1955, AI Magazine 2006, C. 27, S. 4, s. 12-14.

Microsoft: Microsoft Responsible AI Standard, v2 – General Requirements, (https://blogs.microsoft.com/wp-content/uploads/prod/sites/5/2022/06/ Microsoft-Responsible-AI-Standard-v2-General-Requirements-3.pdf, E.T.: 09.07.2024).

NABİYEV, Vasif: Yapay Zekâ, 6. Baskı, Ankara 2021.

National Governance Committee for the New Generation Artificial Intelligence: Governance Principles for a New Generation of Artificial Intelligence: Developing Responsible Artificial Intelligence**,** (https://perma.cc/V9FL-H6J7, E.T.: 09.07.2024).

National Governance Committee for the New Generation Artificial Intelligence: Ethical Norms for the New Generation Artificial Intelligence, (https://ai-ethics-

and-governance.institute/2021/09/27/the-ethical-norms-for-the-new-generation-artificial-intelligence-china/, E.T.: 09.07.2024).

NILSSON, Nils J. (çev. Doğan, M.): Yapay Zekâ Geçmişi ve Geleceği, 2. Baskı, İstanbul 2019.

NORVIG, Peter ve RUSSELL, Stuart: Artificial Intelligence – A Modern Approach, 3. Baskı, New Jersey 2010.

OECD: Artificial Intelligence in Society, (https://doi.org/10.1787/eedfee77-en, E.T.: 09.07.2024), ("Artificial Intelligence in Society").

OECD: Artificial Intelligence, Machine Learning and Big Data in Finance: Opportunities, Challenges, and Implications for Policy Makers, (https://www.oecd-ilibrary.org/finance-and-investment/artificial-intelligence-machine-learning-and-big-data-in-finance_98e761e7-en, E.T.: 09.07.2024).

OECD: OECD Framework for the Classification of AI Systems, (https://www.oecd-ilibrary.org/docserver/cb6d9eca-en.pdf?expires=1705706916&id=id&accname=guest&checksum=17CEFCA23E0FCA0059F51E72FCC5D621, E.T.: 09.07.2024), ("OECD Framework").

OECD: Recommendation of the Council on Artificial Intelligence, OECD/ LEGAL/0449, (https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449#backgroundInformation, E.T.: 09.07.2024), ("OECD Recommendation").

ÖZEL, Kadir Can: Etik ve Etik – Hukuk Arasındaki İlişki, TAAD 2018, S. 33, Y. 9, s. 685-708.

Partnership on AI: Tenets, (https://partnershiponai.org/about/#:~:text=Our%20 Tenets& text=We%20will%20seek%20to%20ensure,as%20many%20people%20as%20possible.&text=We%20will%20educate%20and%20listen,work%2C%20and%20address%20their%20questions, E.T.: 09.07.2024).

Schwartz, Oscar (2019), In 2016, Microsoft's Racist Chatbot Revealed the Dangers of Online Conversation, (https://spectrum.ieee.org/in-2016-microsofts-racist-chatbot-revealed-the-dangers-of-online-conversation, E.T.: 09.07.2024).

Select Committee on Artificial Intelligence of the National Science and Technology Council: National Artificial Intelligence Research and Development Strategic Plan, 2023 Update, (https://www.whitehouse.gov/wp-content/uploads/2023/05/National-Artificial-Intelligence-Research-and-Development-Strategic-Plan-2023-Update.pdf, E.T.: 09.07.2024).

SOLOVE, Daniel J.: Artificial Intelligence and Privacy, Florida Law Review (forthcoming Jan 2025), (http://dx.doi.org/10.2139/ssrn.4713111, E.T.: 09.07.2024).

STAHL, Bernd Carsten: Artificial Intelligence for a Better Future, İsviçre 2021, (https://doi.org/10.1007/978-3-030-69978-9).

T.C. Sanayi ve Teknoloji Bakanlığı ve Türkiye Cumhuriyeti Cumhurbaşkanlığı Dijital Dönüşüm Ofisi: Ulusal Yapay Zekâ Stratejisi 2021-2025, (https://cbddo.gov.tr/SharedFolderServer/Genel/File/TR-UlusalYZStratejisi2021-2025.pdf, E.T.: 09.07.2024).

The Authority of the House of Lords: AI in the UK: ready, willing and able?, (https://publications.parliament.uk/pa/ld201719/ldselect/ldai/100/100.pdf, E.T.: 09.07.2024).

The Ethics Center (2016), Ethics Explainer: Ethics, morality & law, (https://ethics.org.au/ethics-explainer-ethics-morality-law/, E.T.: 09.07.2024).

The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems: Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems, Version 2, (https://standards.ieee.org/wp-content/uploads/import/documents/other/ead_v2.pdf, E.T.: 09.07.2024).

The White House: Executive Order on Promoting the Use of Trustworthy AI in Federal Government, (https://www.govinfo.gov/content/pkg/FR-2020-12-08/pdf/2020-27065.pdf, E.T.: 09.07.2024).

TURING, Alan M.: Can Digital Computers Think? (1951), (ed. Copeland, B.J.), "The Essential Turing: Seminal Writings in Computing, Logic, Philosophy, Artificial Intelligence, and Artificial Life: Plus The Secrets of Enigma", New York 2004, s. 476-486.

TURING, Alan M.: Computing Machinery and Intelligence, Mind 1950, C. LIX, S. 236, s. 433-460, ("Computing Machinery").

TURNER, Jacob: Robot Rules - Regulating Artificial Intelligence, İsviçre 2019.

UNESCO: Ethical Impact Assessment – A Tool of the Recommendation on the Ethics of Artificial Intelligence, (https://unesdoc.unesco.org/ark:/48223/pf0000386276, E.T.: 09.07.2024).

UNESCO: Recommendation on the Ethics of Artificial Intelligence, (https://unesdoc.unesco.org/ark:/48223/pf0000381137?posInSet=2&queryId=0f338b37-d696-4b9c-9962-251f99ba628f, E.T.: 09.07.2024), ("Recommendation").

UNI Global Union: Top 10 Principles for Ethical Artificial Intelligence, (https://uniglobalunion. org/wp-content/uploads/uni_ethical_ai.pdf, E.T.: 09.07.2024).

United Nations: Interim Report: Governing AI for Humanity, (https://www.un.org/sites/un2.un.org/files/un_ai_advisory_body_governing_ai_for_humanity_interim_report.pdf, E.T.: 09.07.2024).

University of Montréal: Montréal Declaration for a Responsible Development of Artificial Intelligence,(https://declarationmontreal-iaresponsable.com/wp-content/uploads/ 2023/ 04/UdeM_Decl-IA-Resp_LA-Declaration-ENG_WEB_09-07-19.pdf, E.T.: 09.07.2024).

VEALE, Michael ve ZUIDERVEEN BORGESIUS, Frederik: Demystifying the Draft EU Artificial Intelligence Act, Computer Law Review International 2021, C. 22, S. 4, s. 97-112.

WANG, Pei: On Defining Artificial Intelligence, Journal of Artificial General Intelligence 2019, C. 10, S. 2, s. 1-37.

World Health Organization: Ethics and governance of artificial intelligence for health, (https://www.who.int/publications/i/item/9789240029200, E.T.: 09.07.2024).

XHEMAJLI, Haxhi: The Role of Ethics and Morality in Law: Similarities and Differences, Ohio Northern University Law Review 2021, C. 48, s. 81-93.

YÜKSEL, Mehmet: Etik Kodlar, Ahlak ve Hukuk, Hacettepe HFD 2015, C. 5, S. 1, s. 9-26, ("Etik Kodlar").

YÜKSEL, Mehmet: Modernleşme Bağlamında Hukuk ve Etik İlişkisine Sosyolojik Bir Bakış, Ankara Üniversitesi SBF Dergisi, C. 57, S. 1, s. 177-195, ("Modernleşme").

ZUIDERVEEN BORGESIUS, Frederick: Discrimination, Artificial Intelligence, and Algoritmic Desicion-Making, (https://rm.coe.int/discrimination-artificial-intelligence-and-algorithmic-decision-making/1680925d73, E.T.: 09.07.2024).

KODLAR VE KANUNLAR: YAPAY ZEKÂNIN REGÜLASYON ROTASI VE AB YAPAY ZEKÂ TÜZÜĞÜ

Dr. Öğr. Üyesi Osman Gazi GÜÇLÜTÜRK*

GİRİŞ

Yapay zekâ olarak adlandırılan teknolojilerin hayatımızdaki etkisinin ne kadar hızlı şekilde arttığı açıktır. Bu etki arttıkça ve bu teknolojilerin kullanımının faydası veya verim artışı kadar olası olumsuz sonuçlarını da gördükçe bu teknolojilerin geliştirilmesinin, kullanımının ve çıktı ya da sonuçlarının da başta hukuki düzenlemeler olmak üzere farklı araçlar yoluyla kontrol edilmesinin gerekli olup olmadığı önemli bir tartışma konusu olarak karşımıza çıkmaktadır.

Yeni teknolojik gelişmelerin zararları ortaya çıkmaya başladığında devlet müdahalesinin talep edilmesi ya da geniş ölçekte "regülasyon" çağrılarının yapılması alışılmadık şeyler değildir. Hukuki düzenlemelerin de teknolojik gelişmeleri hedef alması yeni bir husus olmamakla birlikte özellikle kompleks bir altyapı üzerine kurulu olan, alandaki uzmanların bile bazı detaylarına tam anlamıyla nüfuz edemediği ve kullanımının takip edilmesi oldukça zor olan teknolojik uygulamaların regülasyonunda aslında daha geniş çaplı bir değerlendirme yapılması ve daha etkili araç ve yöntemler mevcut ise hem kamu kaynaklarının israfı anlamına gelebilecek hem de oldukça uzun sürebilecek hukuki müdahale yönteminin tercih edilmesi her zaman doğru adım olmayabilir. Bu çalışmanın ilk amacı, bu değerlendirmenin yapılmasında kullanılabilecek bir metodoloji sunmaktır.

Bir hukuki düzenlemenin yapılmasına karar verildiğinde ise yapılacak düzenlemeyi etkileyebilecek birçok farklı faktör söz konusu olmakla birlikte özellikle uluslararası alanda gelişme gösteren teknolojilerde bu alandaki diğer gelişmeler oldukça önemli bir etken haline gelmektedir. Bunlar ara-

* Galatasaray Üniversitesi Hukuk Fakültesi Bilişim ve Teknoloji Hukuku ABD Öğretim Üyesi, ogucluturk@gsu.edu.tr

sından da daha önce kişisel verilerin korunması alanında tüm dünyadaki gelişmeleri önemli ölçüde etkilemiş Genel Veri Koruma Tüzüğü (General Data Protection Regulation, ("**GVKT**")[1] gibi bir düzenlemeyi çıkarmış ve yıllardır uygulanmasını sağlamış Avrupa Birliği ("**AB**" veya "**Birlik**") gibi bir aktör tarafından çıkarılan düzenleme de ayrıca öne çıkmaktadır. İşte bu çalışmanın bir diğer amacı da yapay zekâyı hukuki düzenleme ile regüle etme yolunu seçmiş ve bu konuda yapılacak sonraki çalışmaları etkilemesi beklenen AB Yapay Zekâ Tüzüğü ("**YZT**")[2] hakkında Türkiye'de yapılacak sonraki çalışmalara ışık tutması açısından genel bir bilgilendirme sağlamaktır. Bu noktada AB yasa yapma sürecindeki detaylar sebebiyle YZT'nin niteliğine, tarihsel gelişimine, AB kurumlarıyla veya Avrupa Konseyi gibi yasama anlamında AB ile ilişkisi olmayan kurumlarla ilişkisine dair bazı karmaşalar yaşandığı[3] görülmektedir. Çalışmanın bu noktalara da ışık tutması ve bazı karmaşıklıkların giderilmesi amaçlanmaktadır.

Bu çalışma dört ana bölümden oluşmaktadır: İlk bölümde regülasyon kavramı, ikinci ve üçüncü bölümlerde teknoloji regülasyonuna metodolojik bir yaklaşım ile yapay zekânın bir hukuki düzenleme konusu olmasına dair açıklamalar, dördüncü bölümde ise YZT'nin incelenmesi yer almaktadır. Yukarıda yapılan açıklamalar doğrultusunda çalışma öncelikle regülasyon kavramı üzerine bazı kavramsal değerlendirmelerle başlayacak; daha sonra teknoloji regülasyonuna ilişkin metodolojik bir değerlendirmeye yer verilecek ve yapay zekânın bir hukuki düzenleme konusu yapılmasına dair açıklamalar yapılacak; nihayet son bölümde hâlihazırda yapay zekânın

---

1 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), (https://eur-lex.europa.eu/eli/reg/2016/679/oj, E.T.: 09.06.2024).

2 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (https://eur-lex.europa.eu/eli/reg/2024/1689/oj, E.T.: 01.12.2024).

3 Bkz. Görentaş, M.B/Çiftçi, H.**:** Avrupa Birliği Yapay Zekâ Yasası Çerçevesinde Yargılamada Yapay Zekâ Kullanımının Değerlendirilmesi, İzmir Barosu Dergisi, 2024, S. 1, s. 181 vd. Avrupa Konseyi, AB'den bağımsız ve Türkiye'nin de üye olduğu bir uluslararası örgüt olup yapay zekâ regülasyonu konusunda bu çalışmada da atıf yapılan ve yine AB'den kurumsal olarak bağımsız bir uluslararası sözleşme çalışması yürütmektedir. Avrupa Konseyi hakkında bilgi için bkz. https://www.coe.int/tr/web/about-us (E.T.: 11.06.2024).

hukuki düzenleme yoluyla regülasyonundaki en önemli metin olan YZT'nin getirdiği rejim hakkında bazı bilgilere yer verilecek ve çalışma YZT'ye ve genel olarak yapay zekânın regülasyonuna ilişkin bazı değerlendirmelerle sonuçlandırılacaktır.

I. TEKNOLOJİ REGÜLASYONU, HUKUK VE YAPAY ZEKÂ

A. REGÜLASYON KAVRAMI

Regülasyon kavramı Türk Dil Kurumu tarafından "ayarlama, düzenleme" olarak tanımlanmaktadır[4]. Bu tanımda her ne kadar hukuk sistemine doğrudan bir atıf olmasa da günlük hayatta ve şaşırtıcı olmayacak şekilde hukukçular arasında regülasyon kavramının sıklıkla hukuki düzenleme yapılmasını ifade edecek şekilde daha dar kapsamda kullanıldığı görülmektedir[5]. Bu çalışmada da bir türüne detaylı değinilecek olan Avrupa Birliği düzenlemelerinin en yaygın iki türünden birinin İngilizce karşılığının '*Regulation*' olması da[6] bu kullanımı özellikle AB'deki gelişmeler ekseninde çalışan çevrelerde daha yaygın hale getirmektedir.

Diğer yandan insan davranışları, piyasalar, kurumlar veya genel olarak sosyo-ekonomik faktörler ve etkileşimler sadece hukuk ile "düzenlenmez". Hukuk bu düzenleme ağında yer alan araçlardan sadece bir tanesi ve belki de doğrudan devletin yaptırımcı yüzüyle temasa geçireni olduğu için en çok öne çıkanıdır. Fakat aslında etkileşimlerimiz, davranışlarımız, içinde bulunduğumuz çevre ve yapılar, hukuktan çok daha geniş bir sürü faktör tarafından şekillendirilmektedir, diğer bir deyişle regüle edilmektedir. Bu doğrultuda "regülasyon" kavramı bu çalışmada her türlü araçla gerçekleştirilen sosyal, davranışsal ve sonuca yönelik kontrolü ifade etmek için kullanılacaktır[7]. Bu itibarla insanların hukuki bir düzenlemeyle yasaklandığı

---

4 TDK Güncel Türkçe Sözlük, (sozluk.gov.tr, E.T.: 09.06.2024).

5 Ayrıca bkz. Morgan, B./Yeung K.: An Introduction to Law and Regulation, 1. Baskı, Cambridge 2007, s. 4.

6 EUR-Lex (2024), "*Regulation*", (https://eur-lex.europa.eu/EN/legal-content/glossary/regulation.html#:~:text=Regulations%20are%20legal%20acts%20defined,Union%20(EU)%20Member%20States., E.T.: 09.06.2024).

7 Öğretide de regülasyon kavramının tanımına ilişkin bir uzlaşı olmamakla birlikte benzer tanımlar verilmektedir. Örneğin Koops regülasyonu "bilinçli olarak birinin ya da bir şeyin davranışını etkilemek" olarak tanımlamaktadır, bkz. KOOPS, B.J.: Ten dimensions of technology regulation: Finding your bearings in the research space of an emerging discipline, (ed. Goodwin M.E.A., Koops, B.J. ve Leenes, R.E.), "Dimensions of Technology

ve yaptırıma tabi olduğu için diğer insanlara zarar vermemeleri de, yola koyulan kapanlar izin vermediği için araçların belirli bir yolda sadece tek bir yönde hareket edebilmeleri de, bir internet sitesine A ülkesinden ulaşılabilirken teknik bir yasaklama ya da site operatörünün kendi tercihi olan bir erişim kontrolü sebebiyle B ülkesinden ulaşılamaması da, zorunlu olmadığı halde kültürel alışkanlıklar veya toplumsal beklentiler sebebiyle bayramlarda çocuklara hediye ya da harçlık verilmesi ya da aile büyüklerinin ellerinden öpülmesi de bir tür regülasyondur. Bu hukuku aşan regülasyon kavramıyla bağlantılı olarak, bu çalışmada "teknoloji regülasyonu"[8] kavramı ile de teknolojinin sadece hukuki kurallara tabi tutulmasının ötesinde gerek teknik araçların gerek sosyal unsurların veya başka herhangi bir yöntemin kullanılmasıyla şekillendirilmesi ve kontrol edilmesi ifade edilmektedir.

Regülasyon dış dünyada belirli bir değişiklik meydana getirmeyi, insan davranışlarını belirli bir yöne doğru veya belirli yönlerden uzaklaştıracak şekilde değiştirmeyi amaçlayan bir kontrol girişimidir. Bu girişim her zaman farklı büyüklükte ve tipte maliyetlerle gelecektir. Hukuki düzenlemeler yoluyla regülasyon kamu kaynaklarını kullanır ve uzun sürer. Teknik düzenlemeler iş yapış şekillerini etkileyerek operasyonel maliyetleri veya hizmet ya da ürün ücretleri üzerinde etki yaratır[9]. Sosyal normların ilk bakışta bir maliyeti olmayabilir ama bunlar hem çok uzun zamanda gerçekleşir hem de geri kalan dinamikleri etkisi altına alır. İsteğe bağlı olarak sosyal normlarda değişiklik, diğer bir ifadeyle sosyal mühendislik de aynı şekilde uzun vadeli ve maliyetli bir planlama gerektirmektedir. Bu maliyetler göz önünde bulundurulduğunda ideal olan regülasyonun bu maliyetlere katlanılmasını meşru kılacak bir amacının olmasıdır. Diğer bir deyişle

---

Regulation", Nijmegen 2010, s. 312. Black'e göre ise regülasyon "genişçe ifade edilmiş sonuçları üretme amacıyla başkalarının davranışlarını değiştirmeye yönelik sürekli ve odaklanmış bir çabayı içeren bir süreci" ifade eder, bkz. Nlack, J.: Critical Reflections on Regulation, Australian Journal of Legal Philosophy, 2002, C. 27, s. 25. Bu konudaki daha farklı görüş ve değerlendirmelerin derlemesi için ayrıca bkz. Bennett Moses, L.: How to Think about Law, Regulation and Technology: Problems with 'Technology' as a Regulatory Target, Law, Innovation and Technology, 2013, C. 5, S. 1, s. 4 vd.

8 Teknoloji regülasyonuna ilişkin daha detaylı kavramsal açıklamalar ve farklı görüşler için bkz. Bennett Moses, s. 3 vd.

9 Uyum faaliyetlerinin işletmeler üzerindeki maliyetleri ve bunun ölçümü hakkında detaylı bilgi için bkz. OECD: "*OECD Regulatory Compliance Cost Assessment Guidance*", (https://www.oecd-ilibrary.org/oecd-regulatory-compliance-cost-assessment-guidance_5jz78m5mpm0t.pdf, E.T.: 09.06.2024).

sadece yapmış olmak için bir regülasyon adımı atmak, örneğin bir amaç ve etki analizi yapmadan sırf yeni gözüktüğü için bir konuda hemen apar topar bir hukuki düzenleme yapmak kaynak israfı anlamına gelecek olup çoğu zaman sorun çözmekten çok sorun yaratacaktır.

Regülasyonun bir de hedefi olmalıdır. Çoğu zaman regülasyon ile ulaşılmak istenen şey insan davranışlarında bir değişikliktir. Ancak bunu gerçekleştirmek için her zaman davranışı değiştirilmesi istenen insanları hedeflemek gerekmez. Örneğin sigara yasaklarının amacı genel olarak toplumdaki tüm bireylerin sigara tüketimini azaltmak ve özellikle de kamuya açık alanlarda sigara dumanının sigara içmeyen kişileri zarar vermesini engellemek olarak düşünülebilir. Bu yasağın etkin şekilde uygulanmasını sağlamak için ise bireysel cezaların yanında sigara içilmesine müsaade eden işletmelere de idari para cezası uygulanmakta ve bu şekilde bireyleri gözetim yükümlülüğü her bir işletmeciye delege edilerek regülasyonun etkisi artırılırken operasyonel maliyetleri de azaltılmaktadır. Başka bir örnek olarak çevrim içi içerik izleme platformlarındaki telif hakkı ihlallerini önlemek için getirilen algoritmik denetim düşünülebilir. Bu platformlarda üçüncü kişilerin eser sahipliği hakları dahil haklarını ihlal eden içeriklerin bulunması durumunda 5651 sayılı Kanun'un[10] ve 5846 sayılı Fikir ve Sanat Eserleri Kanunu'nun[11] muhtelif düzenlemeleri sebebiyle içeriği kaldırma yükümlülüğü ve kaldırılması istenen içerik kaldırılmaz ise bu içerikten sorumlu olma gündeme gelebilecektir. Benzer düzenlemeler başta AB seviyesinde olmak üzere diğer hukuk sistemlerinde de görülmektedir. Bunun önüne geçmek için doğrudan yüklenen içerikleri hedefleyen ve bu içerikleri yükleme aşamasında algoritmik olarak denetleyen sistemler kullanılmakta, bu platformların gözetim yükü ve sorumlu olma ihtimali azaltılmaktadır.

Regülasyon hedefi seçilirken istenen amacın ne olduğu, en yüksek etkinliğin nasıl sağlanacağı, maliyetin ne olduğu gibi çeşitli faktörlerin değerlendirilmesi gerekir. Ancak özellikle davranışı yönlendirilmek istenen aktör

---

10 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun 23.05.2007 tarih ve 26530 sayılı Resmî Gazete'de yayımlanmıştır (https://mevzuat.gov.tr/mevzuat?MevzuatNo=5651&MevzuatTur=1&MevzuatTertip=5, E.T.: 09.06.2024).

11 5846 sayılı Fikir ve Sanat Eserleri Kanunu 13.12.1951 tarih ve 7981 sayılı Resmî Gazete'de yayımlanmıştır (https://mevzuat.gov.tr/mevzuat?MevzuatNo=5846&MevzuatTur=1&MevzuatTertip=3, E.T.: 09.06.2024).

sayısının belirsiz olduğu ya da teorik olarak belirlenebilir olsa bile bu kişi ya da sistemlerin teker teker kontrol edilmesinin pratik gerekçelerle çok zor olduğu durumlarda yukarıda gösterilen iki örnekte de olduğu gibi hedef olarak genelde bu kişi ya da sistemler üzerinde istenen yönde bir gözetim ya da kontrol icra edebilecek aracılar, platformlar, ya da varsa bunların tamamının bir şekilde ilişki içerisinde olduğu darboğazlar seçilir. Dahası böyle bir aktör ya da darboğaz yoksa öncelikle bunun yaratılması ya da yaratılmasının kolaylaştırılması yoluna gidilebilir. Örneğin internet üzerindeki davranışa ilişkin belirli kuralların herkeste etkili olabilecek şekilde icra edilebilmesi için seçilen aracı internet servis sağlayıcıları ya da 5651 sayılı Kanun'un ifadesiyle erişim sağlayıcılardır. Önce internete erişim sağlamak hizmeti vermek için belirli kriterler getirip sonrasında internet altyapısına erişmek için bu kriterleri sağlayan bir internet sağlayıcıyla sözleşme yapmayı zorunlu tutmak tüm internet kullanıcılarının doğrudan ya da dolaylı olarak az sayıda ve kontrol edilebilir bir grup aktörle temasa geçmek zorunda kalmasını ve olası regülatif adımlar için son derece etkili bir hedef oluşturulmasını sağlamaktadır.

Regülasyonun diğer önemli unsuru ise sonucu ve etkileridir. Regülasyon her zaman istenen sonucu vermeyebilir. Hukuki düzenlemeler özelinde bakıldığında bir düzenlemenin yapılması insanların o düzenlemeye uygun davranacağı, bir teknik sınırlamanın getirilmesi bu sınırlamanın aşılmayacağı veya bir konuda toplumda bir beklenti ya da baskı olması bu duruma herkesin uyum sağlayacağı anlamına gelmez[12]. Sonuçların istendiği gibi olması ya da olmaması bir kontrol girişiminin regülasyon olup olmamasına değil, söz konusu regülatif adımın başarılı ya da etkili olup olmamasına ilişkindir. Örneğin Covid-19 pandemisi döneminde hastalığın yayılmasını engellemek için sokağa çıkma kısıtlaması getirilmesi bir regülasyondur. Bu kısıtlamaya uyulmasını sağlamak için ihlalinin para cezasına bağlanması başka bir regülasyondur. Kural konulmasının tek başına yeterli olmadığı, yaptırımın da etkin bir regülasyon için gerekli olduğu bir ortamda bu para cezasının miktarı da regülasyonun etkinliği için önemli olur. Örneğin ceza miktarı çok düşükse ceza ödeme riskine rağmen ihlaller söz konusu olabilecekken çok yüksekse de özellikle ihlal durumunda ceza ödemeden kaçınma eğilimi sebebiyle etkinlik azalacaktır.

[12] Regülasyonun etkinliği ve beklendiğinden farklı sonuçlanan detaylı regülasyon örnekleriyle ilgili olarak bkz. Clarke, M.: Regulation The Social Control of Business between Law and Politics, New York 2000, s. 162 vd.

Çalışmanın devamında teknolojinin ve daha özelde yapay zekânın regülasyonundan söz edilirken de söz konusu regülasyonun yapılış şekli, amacı, bu amaç için katlanılması gereken maliyet ve ulaşılması istenen sonuç ile ulaşılan sonuç birlikte değerlendirilecektir. Bu hususlar hukuki düzenleme yoluyla bir regülasyon hedeflendiğinde de yapılacak hukuki düzenlemenin niteliğine göre değerlendirilmelidir. Bu değerlendirmenin yapılabilmesi için ise öncelikle hukukun teknoloji regülasyonundaki yeri ayrıca incelenmelidir.

B. HUKUKUN TEKNOLOJİ REGÜLASYONUNDAKİ YERİ

Daha önce de belirtildiği üzere bu çalışmada kullanıldığı şekliyle regülasyon kavramı hukuki düzenlemelerin ve araçların kullanımının ötesine geçmektedir. Bu kapsamda hukuki düzenlemeler, prensipler ve araçlar teknoloji regülasyonunda kullanılan düzenleyici -ya da regülatif- araçlardan sadece bir tanesidir. Önemli olan ise hukuki araçların her zaman en etkili araç olmayabileceğidir. Özellikle regüle edilecek hedef sayısının belirsiz ya da çok olduğu, darboğaz oluşturacak fiziksel kontrollerin de olmadığı durumlarda doğrudan bu kişileri hedef alan hukuki düzenlemeler etkinlik bakımından oldukça sıkıntılı olabilir. Daha önce bahsedildiği gibi hedef haline getirilebilecek darboğazların oluşturulması mümkün de olmayabilir. Bu gibi ihtimallerde istenen sonuca ulaşmak için salt hukuki düzenleme yapma yoluna gitmek büyük ölçüde kaynak israfı olmaktan öteye gidemeyecektir.

Dikkat edilmesi gereken bir husus hukuki düzenlemenin yapılabiliyor olmasıyla yapılmasının gerekli olup olmadığı arasındaki çizgidir. Hukukun kendi koyduğu sınırlar ve kurallar hiyerarşisi içerisinde hukuki düzenleme yapmak neredeyse her konuda mümkündür. Bir kanunun, örneğin konuyla alakalı olduğunu düşünürsek 5651 sayılı Kanun'un, içerisine "internet üzerindeki etkileşimlerinde herkes hukuka uygun, insan haklarına saygılı ve diğer insanlara zarar vermemeye dikkat edecek şekilde davranacaktır" şeklinde bir cümle eklemenin önünde kâğıt üzerinde hiçbir engel yoktur. Ama böyle bir düzenleme zaten genel nitelikte olan ve başta Anayasa olmak üzere diğer bazı temel kanunlarda tekrar edilen geniş nitelikli prensipleri tekrarlamaktan ve üstelik bunu yaparken de kaynak israf etmekten öteye gitmeyecek ve hatta belki bazı durumlarda "neden var olduğuna ilişkin" düşüncelere sebep olarak karmaşıklık yaratacaktır. Benzer şey yeni teknolojiler için de geçerlidir. Ancak yeni teknolojileri regüle etmek için

şekli hukuki düzenlemelerin yapılabilecek olması, yapılmasını gerektirmez. Hatta çoğu zaman ön çalışma yapılmadan ilk olmak ya da bir şey yapmak için yapılan prematüre hukuki düzenleme mevcut kurallarla uyumsuzluk ve istenmeyen sonuçlara sebep olma riski taşır.

Bazı istisnai hallerde pratik açıdan çok bir etkisi olmayacaksa bile tartışma zemini doğurması, diğer düzenlemelere yol göstermesi ve ülkenin hukuki politikalarını yansıtması amacıyla prensip niteliği taşıyan bazı genel nitelikli düzenlemeler pekâlâ yapılabilir. Yapay zekânın insan odaklı şekilde geliştirilmesine, güvenilir olmasına, hesap verilebilir olmasına ilişkin düzenlemeler buna örnek olarak gösterilebilir. Ancak bu yaklaşımın özellikle iç hukuk düzenlemelerinde somut adımlarla veya yöntemlerle desteklenmedikçe diğer benzerleri gibi "temenni" olmanın ötesine geçemeyeceği unutulmamalıdır. Bu tarz yaklaşımın görece daha anlamlı ve verimli olabileceği bir hukuki düzenleme tipi uluslararası antlaşmalardır. Uluslararası iş birliği gerektiren alanlarda devletlerin herhangi bir konuya yaklaşımları farklıysa bir uzlaşı sağlamak ve bu uzlaşıyı ilkesel bir seviyede dahi olsa bağlayıcı bir hukuki enstrümana dökmek o alandaki sonraki pratik uzlaşıya da zemin hazırlayacağından önemli bir adım olabilir. Yapay zekâ alanında Avrupa Konseyi bünyesinde hazırlanan uluslararası çerçeve antlaşma buna örnek olarak gösterilebilir. Antlaşma içerisinde genelde oldukça geniş anlama gelebilecek ifadeler kullanılmış olmakla birlikte -ki çok detaylı düzenlemeler üzerinde devletlerin uzlaşması iç hukuk kurallarındaki sürece göre çok daha çetrefilli olabilir- bu antlaşmanın hazırlanmış olması ve önümüzdeki günlerde yürürlüğe girmesi atılacak pratik adımları çevreleyecek bir genel uzlaşıya hazırlık yapılması açısından oldukça değerlidir. Bu istisnai hal haricinde ise temenni olmanın ötesine geçilemeyecek hukuki düzenlemelerin yapılması kaynak harcanmasına sebep olup pratikte bir sorun çözmeyip bir de üstüne yorum faaliyetlerinde karışıklığa sebep olabileceğinden regülasyon çalışmalarında tercih edilmemelidir.

Etkisiz hukuki düzenlemenin tek zararı kaynak israfı veya yorum karmaşası değildir. Hukuki düzenlemeler çoğunlukla izin verdikleri davranışlara meşruiyet zemini de hazırlar. Örneğin kurallarına uygun olarak gerçekleştirilen bir haczin paraya çevrilmesi işlemi en masum ifadeyle ilk bakışta "tatsız" bir işlem olmakla birlikte hukukun izin verdiği bir işlem olduğu için üstelik kamu gücünün de dahliyle gerçekleştirilebilir. Bunun gibi birçok bireysel açıdan tatsız görünen ya da memnuniyetsizlik yaratan husus hukuk yoluyla meşruiyet kazanır. Bu gibi durumlarda zorlayıcı etkisi sebe-

biyle hukuki düzenlemeler diğer regülasyon unsurlarına -buradaki örneğiyle mesela sosyal normlara- karşı öne çıkabilir. Bu da kural olarak olumsuz ya da istenmeyecek bir durum olarak değerlendirilmemelidir. Zira hukuk esasen bireysel memnuniyetsizlikleri gidermek için değil toplumsal ilişkileri daha geniş ölçekte yönetmek için kurallar getirir; en azından olması gereken budur. İşte yanlış yapılan hukuki düzenleme de bu etkinin bir uzantısı olarak aslında meşru olmayan bir şeyin meşruiyet kazanmasına sebep olabilir. Örneğin kişisel verilerin korunmasına ilişkin düzenlemelerde amaç kişisel verilerin korunması hakkına uygun şekilde veri işlenmesini sağlamak, ilgili kişiye belirli ölçüde kontrol, bazı haklar ve bunları kullanabileceği kadar bilgi vermek olabilir. Ancak kişisel verileri koruma düzenlemelerinin uygulaması esaslı bir incelemeden şekli bir kontrol listesine ya da sadece belirli metinlerin hazırlanmış olup olmadığının incelenmesine indirgenirse o zaman hem ilgili kişilerin kişisel verileri anlamlı şekilde korunmamış hem de bu uygulama hatalı şekilde bir düzenlemeye dayandırılmış olur. Bu gibi durumların ortaya çıkmasını engellemek için hukuki düzenlemelerin uygulanmasına ilişkin hususlara dikkat edilerek belirli düzenlemelerin yapılması gerekir. Kişisel verilerin korunmasına ilişkin örnekte 6698 sayılı Kişisel Verilerin Korunması Kanunu ("**KVKK**")[13] m. 4'te yer alan ilkeler ve Kurul'un uygulamaları KVKK ile uyumun basit bir kontrol listesine dönüşmesini engellemeye yönelik önemli enstrümanlardır.

Bütün bu açıklamalardan çıkan en temel sonuç ise şudur: Hukuk teknolojinin regülasyonunda önemli bir araç olabilir ancak her zaman en doğru ve etkili araç değildir. Teknolojiyi regüle etmek için hukuki düzenleme yapılabiliyor olması da tek başına o düzenlemenin faydalı ya da gerekli olduğu veya faydaları varsa bile uygulanacağı anlamına gelmez. Bu sebeple teknolojinin regülasyonuyla ilgili bir konuda doğrudan hukuki düzenleme yoluyla müdahale talebinde bulunmadan ve hatta bu konuda yaygın olarak görüldüğü üzere kamuya yönelik yeni regülasyon çağrılarında bulunmadan, tabir-i caizse hukuki müdahale çığırtkanlığı yapmadan, önce hukuki düzenlemelerin ya da araçların amaç, hedef, etkinlik bakımından uygun olup olmadığı ve söz konusu teknoloji ile getirilecek düzenlemelerin mevcut hukuki düzenlemelerle ilişkisi incelenmelidir.

---

[13] 6698 sayılı Kişisel Verilerin Korunması Kanunu 07.04.2016 tarih ve 29677 sayılı Resmî Gazete'de yayımlanmıştır (https://mevzuat.gov.tr/mevzuat?MevzuatNo=6698&MevzuatTur=1&MevzuatTertip=5, E.T.: 09.06.2024).

Çalışmanın devamında regülasyon, hukuk ve teknoloji arasındaki ilişkiyle ilgili olarak bu bölümde yapılan açıklamalara dayanılarak yapay zekânın hukuk yoluyla regülasyonunun gerekli olup olmadığının tespitine ve dikkat edilmesi gereken hususlara dair bir değerlendirme yapılacaktır. Daha sonra ise bir hukuki düzenleme konusu olarak yapay zekânın ne ifade ettiğine, nasıl tanımlanması gerektiğine ve sonuçlarına dair açıklamalarda bulunulacaktır.

II. YAPAY ZEKÂNIN HUKUK YOLUYLA REGÜLASYONUNUN GEREKLİLİĞİ ÜZERİNE BİR METODOLOJİ ÖNERİSİ VE DİKKAT EDİLMESİ GEREKEN HUSUSLAR

Çalışmanın bu bölümünde öncelikle sadece yapay zekâ ile kısıtlı olmayacak şekilde teknolojilerin regülasyonunun gerekli olup olmadığının ve daha özelde hukuki müdahalenin gerekli olup olmadığının incelenmesinde kullanılacak metodolojik bir yaklaşım önerisinde bulunulup daha sonra da bu metodolojiyi yapay zekâ özelinde uygulayarak yapay zekânın hukuki düzenleme yoluyla regüle edilmesinin gerekli olup olmadığı yönünde bir değerlendirmede bulunulacaktır.

A. TEKNOLOJİ REGÜLASYONUNDA GEREKLİLİK ANALİZİ

Bizce bir teknolojiye yönelik regülasyonun gerekli olup olmadığı değerlendirilirken sırasıyla incelenmesi gereken üç husus mevcuttur:

1) Öncelikle söz konusu teknolojinin regülasyonunu gerekli kılan amaç tespit edilmelidir. Bu amaç çoğunlukla bir sorunun çözülmesi, bir riskin yönetilmesi ya da ortadan kaldırılması veya bir iyileştirmenin sağlanması olacaktır. Somut bir amaç belirlenemiyorsa sırf bir şeyler yapmış olmak için regülasyona da ihtiyaç yoktur.

2) Somut bir amaç belirlendikten sonra bu amacın regülasyon adımını gerekli kılıp kılmadığı incelenmelidir. Bu da çoğunlukla amaçla bağlantılı sorunun önemi, büyüklüğü ve olası etkisinin ya da amaçlanan iyileştirmenin incelenmesini ve bunların bir regülasyonu gerekli kılıp kılmadığının değerlendirilmesini gerektirmektedir. Zira ortada bir sorunun olması her durumda müdahale edilmesini gerekli kılmayabilir. Bazı sorunlar tamamen konjonktürel olarak ortaya çıkıp yine zamanla kendiliğinden bir müdahale gerek olmaksızın kaybolabilir. Böyle durumlarda hemen güçlü müdahalelerde bulunmak sorunu çözmek yerine tam ak-

sine sorunu daha da artıracak ve sistematik hale getirecek etkiler yaratabilir. Yine bu aşamada mevcut düzenlemelerin işlevselliği de göz önünde bulundurulmalıdır. Yeni olaylardan, gelişmelerden -bu çalışma özelinde teknolojilerden- kaynaklı sorunlar mevcut araçların kullanımıyla, hukuk düzleminde de mevcut düzenlemelerin yorumlanmasıyla veya esnek uygulamalarla çözümlenebilir. Örneğin mevcut genel veya özel nitelikli düzenlemeler amaca ulaşmayı mümkün kılıyorsa yeni adım atmak hem kaynak israfı hem de mevcut düzenlemelerle karışıklık anlamına gelebilecektir.

3) Belirlenen amaca ulaşılması için bir regülasyon gerekli olduğu ve bunu sağlayabilecek mevcut bir düzenlemenin de olmadığı sonucuna ulaşılıyorsa o zaman da doğru müdahale aracının ne olduğu tespit edilmeli, hukuki müdahale yoluyla düzenlemenin uygun bir yöntem olup olmadığı incelenmelidir.

1. Amaç Tespiti

Doğru bir regülasyon adımı için öncelikle bir amaç tespit edilmesi gereklidir. Bu amaç da çoğu zaman ortada regülasyonu gerekli kılan bir sorunun ya da bir riskin olması, bunlar da yoksa ortada somut bir iyileştirme planının bulunması olacaktır. Yeni bir şeyi regüle etmek tek başına regülasyon için uygun bir amaç olamaz. Söz konusu yeniliğin getirdiği bir sorun, risk, ya da bir fayda varsa bunlara ilişkin bir amaç belirlenebilir. Regülasyonun nesnesinin, örneğin yapay zekânın, yeni bir şey olması, tek başına sorunlu ya da riskli hale getirmediği gibi regülasyonun doğrudan bir iyileştirme sağlayacağı da hiçbir ek inceleme yapmaksızın söylenemez.

Regülasyon amacı var olan bir sorunu çözmek olabilir. Burada dikkat edilmesi gereken önemli bir nokta bir hukuka aykırılığın ortadan kaldırılmasının regülasyon anlamında tek başına uygun bir amaç teşkil etmeyeceği ve mevcut hukuka uygunluğun da tek başına regülasyon tartışması anlamında sorunları ortadan kaldırmaya yetmeyeceğidir. Yani ortada yeni ortaya çıkmış olan bir sorun olabileceği gibi mevcut regülatif adımların çözmekte yetersiz kaldığı sorunlar veya regülatif adımlar sonucu ortaya sonradan çıkmış sorunlar olabilir. Yeni soruna örnek olarak yapay zekâ destekli yüz tanıma algoritmalarının ten rengine dayalı ayrımcılık yapması ve siyahi insanların yüzlerini tam olarak tanıyamaması ve hatta bazen insan olarak dahi tanıyamaması gösterilebilir. Mevcut regülatif adımlara, daha özelde hukuki düzenlemelerin varlığına rağmen çözülmemiş sorunla-

ra örnek olarak eser sahipliği haklarıyla korunan eserlerin izinsiz dağıtımı yani korsan içerikler ya da izinsiz gönderilen reklam, SMS veya e-postalar gösterilebilir. Mevcut hukuk kurallarına uyulmaması çoğu zaman gerçekten de bir soruna işaret edecektir. Korsan içerik ya da izinsiz kişisel veri işleme faaliyetlerinde durum böyledir. Bunlar hukuki düzenlemelerle yasaklanmış faaliyetler oldukları halde günlük hayatta sıklıkla karşılaşılan durumlardır. Bazense hukuki düzenlemenin uygulanmaması bir sorun değil tam tersine uygulanırsa oluşabilecek sorunların önüne geçen bir regülatif adım olabilir. Zira mevcut hukuk kurallarına görünüşte uygunluğun doğuracağı bazı sorunlar söz konusu olabilir. Örneğin 1925 tarihli 671 sayılı Şapka İktisası Hakkında Kanun[14] hala yürürlükte olan bir kanun olup bazı kişilerin şapka takmasını zorunlu kılmaktadır. Ancak bu düzenleme artık kadük kabul edilmekte ve ihlaline ilişkin hiçbir yaptırım uygulanmamaktadır

Regülasyonun bir diğer amacı risk yönetimi olabilir. Ancak regülasyonun gerektirdiği süre, efor, maliyet ve atılacak adımın olası etkileri göz önünde bulundurularak riskin planlanan adımın atılmasını gerekli kılıp kılmadığı her somut olay özelinde ayrıca değerlendirilmelidir. Örneğin yapay zekânın insanları işsiz bırakması "riski" hiçbir somut veriyle desteklenmeden genel bir kaygı olarak "yapay zekânın insanların işlerini elinden almalarını engellemek" gibi geniş nitelikli ve doğruluğu ve yanlışlığı dahi şu aşamada belli olmayan bir amaçla regülasyon adımları atılmasını gerektiren bir risk değildir. Zira meslek türlerinin gelişen teknolojiyle beraber değişiklik göstermesi, isimleri aynı kalsa da yapılan işlerin değişmesi ve bazı mesleklerin bu süreçte kaybolması yeni bir şey değildir. Değerlendirme her somut olay özelinde yapılacak olsa da çoğunlukla az sayıda kişiyi ilgilendiren ve uzak ya da uzun vadeli risklerin regülasyonu haklı kılmayacağı; bununla birlikte sistemik etki doğurabilecek riskler için adımlar atmanın daha doğru olacağı söylenebilir. Sistemik riskler etkilerine göre uzun vadeli ya da uzak da olabilir ama olası bir geri dönülemez ya da çok büyük zararların oluşacağı durumu engellemek için tedbir amaçlı olarak adımlar atılabilir. Örneğin metaverse olarak adlandırılan 360 derece sanal dünya tecrübesi sunan teknolojinin kullanımının uzun vadede insan sağlığı ve psikolojisi üzerindeki etkileri bilinmediği için bu teknolojinin kontrol edilemeyecek kadar yaygınlaşmasının önüne geçmek veya insanların en azından bazı hususlar belirginleşene kadar bu teknolojiyi olası geri dönü-

[14] 671 sayılı Şapka İktisası Hakkında Kanun 28.11.1925 tarih ve 230 sayılı Resmî Gazete'de yayımlanmıştır, (https://mevzuat.gov.tr/mevzuat?MevzuatNo=671&MevzuatTur=1&MevzuatTertip=3, E.T.: 09.06.2024).

lemeyecek zararlara maruz kalmayacak ölçüde kullanmalarını sağlamak için bazı adımlar atılabilir. Bu noktada metaverse teknolojisinin olası ve belki de uzak vadedeki etkilerine uygun bir risk derken yapay zekânın insanların işini elinden alması "risk"inin uygun gözükmemesi ilk bakışta bir çelişki olarak görünebileceğinden farkın ortaya konması da doğru olacaktır. Metaverse teknolojisinin anılan 360 derece sanal ortam sağlayan uygulaması somut bir uygulamayı ifade etmekte ve buna imkân sağlayan ekipmanları kullanan görünüşte sağlıklı bireylerde kısa süreli kullanımlarda bile baş dönmesi, istifra, uzuv etkileşimlerine yabancılaşma gibi etkiler görülmektedir. Yapay zekânın bazı meslekleri yok ederek insanları işsiz bırakması ise ilk bakışta oldukça geniş kapsamlı ve bilim kurgudan beslenen bir kaygıdır. Fakat pekâlâ yapay zekânın da bazı mesleklerin faaliyetleri üzerindeki etkisinin somut risk hatta sorun seviyesine ulaştığı söylenebilir. Örneğin mevcut eserlerin işlenmesi yoluyla insanların ürettiklerinden ayırt edilmesi çok mümkün olmayan yazılı içerikler üreten dil modellerinin yazarlık ya da senaryo yazarlığı üzerindeki etkisi somut bir sorun olarak ortaya çıkmakta ve uyuşmazlıklara da konu olmaktadır[15]. Veya OpenAI tarafından yakın zamanda duyurulan GPT-4o modelinin simültane tercüme kapasitesinin yakın zamanda tercümanlık mesleğini önemli bir sıkıntıya sokabileceği yönünde görüşler ileri sürülmektedir[16]. Bu konularda bir regülasyonun gerekli olup olmadığı somut olay özelinde yapılacak incelemelerde değerlendirilmelidir.

Regülasyon bazen de bir sorun çözmek ya da riski yönetmek yerine mevcut olan bir şeyi ya da süreci iyileştirme amacıyla da yapılabilir. Bu durumda çoğu zaman pratik olarak mümkün olan bir kolaylığa mevcut yasal düzenleme tarafından izin verilemiyor olmasının, aslında kılık değiştirmiş bir sorun olduğu söylenebilir. Bu sebeple de kâğıt üzerinde bir amacın sorun çözme mi yoksa iyileştirme mi olduğu zaman zaman çok belirsizleşebilir. Örneğin fiziksel olarak bankaya gitmek zorunda kalmadan uzaktan kimlik doğrulamasıyla banka hesabı açma işlemine izin verilmesi yerine göre çalışan sisteme getirilen bir iyileştirme, yerine göre ise insanlara zaman kazandıracak ve kolaylık sağlayacak bir uygulamanın mevcut olduğu halde kullanılamıyor olması sorununun çözülmesi olarak değerlendirilebilir.

---

15 Los Angeles Times (2023), "AI is causing panic for authors. Now the courts are involved", (https://www.latimes.com/entertainment-arts/business/story/2023-10-20/authors-ai-lawsuits-douglas-preston-george-rr-martin-michael-connelly, E.T.: 09.06.2024).

16 Bu konuda bilgi için bkz. Rest of World (2024), "OpenAI is making a risky bet on live translation", (https://restofworld.org/2024/exporter-openai-translation-gpt4o/, E.T.: 09.06.2024).

Burada önemli olan bu hususun nasıl isimlendirildiği değil, regülasyon adımını, ilk bakışta gerekli kılacak kadar önemli olup olmadığıdır.

Regülasyon ile ulaşılmak istenen amacın doğru şekilde belirlenmesi daha sonra müdahalenin gerekliliği, uygun aracın tespiti gibi aşamalarda da değerlendirmenin önemli bir parçası olacağından tüm regülasyon sürecinin yürütülmesi ve nihayetinde atılacak adımların başarısının değerlendirilebilmesi için de ayrıca önemlidir. Ancak bir amacın varlığı her durumda bir adım atılmasını gerekli kılmaz. Müdahalenin gerekli olup olmadığı amaçtan bağımsız ayrı bir inceleme konusudur.

2. Müdahalenin Gerekliliğini İncelemek

Regülasyonla ulaşılmak istenen bir amacın belirlenmesi ve hatta bu amacın önemli bir sorunu çözmek ya da ciddi bir riski bertaraf etmek olması bile tek başına bir regülasyon adımını gerekli kılmaya yetmez. Zira bazen bazı sorunlar, riskler ve gelişmeler tamamen geçici olarak anlık gelişmeleri takiben veya konjonktürel şekilde meydana gelir ve hiçbir müdahaleye gerek kalmaksızın da kendiliğinden ortadan kalkar. Örneğin Pokemon GO adlı artırılmış gerçeklik oyununun ilk çıktığı zamanlarda getirdiği popülarite sebebiyle oyunu oynayan kişilerin oyun içi bazı önemli nokta ve ödüllerle eşleştirilmiş gerçek dünyadaki mezarlıklara, ibadethanelere ve özel mülkiyete konu alanlara hücum etmesi ve buralarda toplumun bazı kesimleri için rahatsızlık oluşturması[17] sürekli-lik arz etmiş olsa özellikle manevi değerlerin korunması hassasiyeti sebebiyle belli adımların atılmasını gerektirebilecekken, bu olay özelinde oyunun yeni çıkmış olmasının getirdiği heyecan ve popülarite azaldıktan sonra kendiliğinden sona ermiştir. Böyle anlık etkilerde dikkatli hareket etmek ve dikkate yönlendirmek faydalı olmakla birlikte çok kritik bir risk mevcut aksini gerektirmiyorsa çoğu zaman daha somut regülasyon adımlarını atmadan önce gelişmeleri takip etmek ve izlemek daha doğru bir strateji olacaktır.

Özellikle uzun vadeli etkilerin öngörülmesinin mümkün olmadığı, çok yeni ve belirsizlik taşıyan durumlarda gelişmeleri takip edip izlemek ve panikle adım atmamak uzun vadede süreci iyi yönetmek ve yeni gelişmelerin

[17] Bkz. https://mashable.com/article/cincinnati-cemetery-pokemon-go (E.T.: 01.12.2024); https://www.haberturk.com/yasam/haber/1266338-diyanet-sen-camilerde-pokemon- go-oynanmasi-yasaklansin (E.T.: 01.12.2024).

olumlu taraflarından da faydalanmak için önemlidir. Anlık gelişmelerde meydana gelen zarara yönelik ilk ileri sürülen "çözüm" önerileri neredeyse her zaman statükoyu koruma ve bilinmeyeni uzaklaştırma eğiliminin bir sonucu olarak kısıtlayıcı nitelikte olacaktır. Kripto varlıkların ya da yakın zamandaki en çok ses getiren yapay zekâ uygulaması olan ChatGPT'nin yasaklanmasına ilişkin çağrılar bu duruma örnek olarak gösterilebilir[18]. Ancak unutulmamalıdır ki yasaklayıcı önlemler kısa vadede ilk zararlı etkileri azaltıcı etki yapsa da hem söz konusu araç ya da teknolojilerin kullanımı takip edilebilir bir izin ya da ruhsata tabi tutulmadığı sürece çok etkili olmayacak hem de hukuka uygun kanallarla söz konusu teknolojinin avantajlarından yararlanma imkanını azaltacaktır.

Müdahalenin gerekliliği incelenirken göz önünde bulundurulması gereken bir diğer husus da mevcut regülasyon araçlarının ve tabi ki bunun bir alt grubu olan mevcut hukuki düzenlemelerin etkisidir. Bazen bir hususu doğrudan hedef alan bir hukuki düzenleme olmasa da genel nitelikli düzenlemeler ve ilkeler yoluyla mevcut düzenlemelerin yeni sorunlara uygulanması mümkün olabilir. Ya da ilk bakışta yeni gelişmelerle uyuşmuyor gibi gözüken mevcut hukuki düzenlemelerin doğru bir hukuki analiz sonrasında aslında bir çelişki yaratmadığı anlaşılabilir. İlk duruma örnek olarak yapay zekâ sistemlerinin kullanılması sonucu oluşan zararlara uygulanacak hukuki mekanizmalar gösterilebilir. Doğrudan yapay zekâ sistemlerinden kaynaklanan zararları ve tazminini düzenleyen bir hukuki düzenleme olmasa da pek çok hukuk sisteminde hâlihazırda mevcut olan genel nitelikli sözleşmeye dayanan sorumluluk ve haksız fiil sorumluluğuna ilişkin düzenlemelerin yapay zekâya ilişkin bazı sorumluluk hallerinde de uygulanabileceği açıktır[19]. Aslında tam olarak bu genel nitelikli düzenlemeler sebebiyle hukuk sistemlerinin neredeyse tamamında bir şekilde yapay zekâ olarak adlandırılan sistemlere uygulanacak genel nitelikli hukuki düzenlemeler olacaktır. Yine bu sebeple neredeyse hiçbir hukuk sisteminde, yaygın kullanımın aksine, yapay zekâya uygulanacak hukuki düzenlemenin

---

[18] Örnek yasaklama çağrıları için bkz. https://dbknews.com/2023/01/30/chatgpt-is-detrimental-to-learning-and-should-be-banned-in-class/ (E.T.: 01.12.2024); https://www.cnbc.com/2023/12/06/jamie-dimon-lashes-out-on-crypto-if-i-was-the-government-id-close-it-down.html (E.T.: 01.12.2024).

[19] Üretken yapay zekâ özelinde Türk hukukunda sorumluluğa ilişkin olarak uygulanabilecek genel nitelikli hukuki düzenleme ve mekanizmalara dair açıklamalar için bkz. Yünlü, S.: *Üretici Yapay Zekâ Kaynaklı Norm ve Kişi Bazlı Hukuki Sorumluluk,* Adalet Dergisi, 2024, S. 72, s. 501-542.

olmadığını söylemek[20] doğru olmayacaktır. Var olmayan şey yapay zekâya uygulanacak hukuki ya da genel olarak bağlayıcı düzenleme değil, özellikle yapay zekâ olarak adlandırılan sistemleri hedef alan hukuki düzenlemelerdir. Bu düzenlemelere ilişkin çalışmaların görece yeni olduğu ve tam da bu çalışmanın yazıldığı dönem itibariyle bu alandaki hukuki düzenleme getirme çalışmalarının hız kazandığı söylenebilir. İkinci duruma örnek olarak ise gelişmiş yapay zekâ sistemlerinin yüksek hacimde veri ihtiyacı sebebiyle kişisel verilerin işlenmesinin ilk bakışta veri minimizasyonu ve amaçla sınırlılık gibi bazı ilkeler bakımından kişisel verilerin korunması kurallarıyla örtüşmüyor gibi görünmesi gösterilebilir. Bu noktada sadece yüksek hacimli veri ihtiyacına bakılarak doğrudan yapay zekâ ile kişisel verilerin korunması arasında bir çelişki olduğu sonucuna ulaşılmamalı, temel ilkeler dahil olmak üzere kişisel verilerin korunmasına ilişkin düzenlemelerin yapay zekâ sistemlerinin işleyişiyle uyumu detaylı şekilde incelenmelidir.

Bütün bu incelemeler sonucunda müdahalenin gerekli olduğuna karar verilmesi de doğrudan hukuki müdahale yapılmasını haklı kılmayabilir. Daha önce detaylı olarak açıklandığı üzere regülasyon başka bir sürü farklı araçlarla gerçekleştirilebilir. Hukuki müdahalenin doğru yöntem olup olmadığı ayrıca incelenmelidir.

3. Hukuki Müdahale

Regülasyonla ulaşılmak istenen amacın gerçekleştirilmesi için bir müdahalenin gerekli olduğuna karar verilirse bir sonraki aşama bu müdahalenin hangi araçla ve nasıl yapılacağının tespit edilmesidir. Bu noktada da hemen hukuki müdahale yoluna gitmek ya da düzenleme çağrısında bulunmak yerine öncelikle daha hızlı, etkili ve az maliyetli olabilecek diğer müdahale araçları da incelenmelidir.

Hangi araçla müdahalenin yapılacağı ancak somut olayın özellikleri dikkate alınarak belirlenebilir. Müdahale araçlarının etkisi toplumdan topluma, aynı toplum içerisinde yaş grupları arasında veya aynı yaş grubundaki

[20] Öğretide bazı yazarlar buradaki ilişkiyi "bağlayıcı düzenleme eksikliği" olarak ifade etmektedir. Bkz. Karacan, P.; Irgız, D.: *Yapay Zekâ Kullanımı için Hukuksal Çerçeve İhtiyacı,* LexPera Blog, 20.07.2023 (https://blog.lexpera.com.tr/yapay-zeka-kullanimi-icin-hukuksal-cerceve-ihtiyaci/, E.T.: 01.12.2024). Ancak yapay zekaya uygulanacak genel nitelikli düzenlemeler de bağlayıcı nitelikte olabileceğinden (örneğin KVKK gibi) bu ifade de yanıltıcı olabilecektir.

insanlar içerisinde daha spesifik özelliklere, örneğin cinsiyete ya da öğrenim seviyesine göre değişebilir. Müdahalenin hukuki araçlarla yapılmasının gerekli olup olmadığının tespitinde göz önünde bulundurulması gereken farklı hususlar mevcuttur.

İlk olarak değerlendirilmesi gereken husus hukuki düzenleme yapmanın gerektirdiği zaman ve süreç maliyetidir. Hukuki düzenlemelerin farklı türleri bulunmakla birlikte özellikle kanun seviyesinde yapılacak bir düzenlemenin yasama organlarından geçmesi gerekeceğinden müdahalenin hızlı şekilde yapılması gereken durumlarda hukuki müdahale en doğru yöntem olmayabilecektir. Veya hâlihazırda buna izin veren bir temel hukuki zemin mevcutsa ikincil düzenlemelerle müdahale yoluna gidilebilir. Ancak bu takdirde de ikincil düzenlemelerin düzenleme alanına ilişkin sınırlara dikkat edilmelidir. Örneğin temel hak ve özgürlüklere ilişkin sınırlamaların Anayasa m. 13 uyarınca sadece Anayasa'da belirtilen sebeplere bağlı olarak kanunla getirilebileceği unutulmamalıdır. Bu itibarla bir sorunu çözmek için temel hak ve özgürlükleri kısıtlayan çok daha hızlı ve efektif bir araç mevcut olsa bile artık Anayasa'nın açık hükmü gereğince kanun yapma prosedürünün işletilmesi ve kısıtlamanın hukuki müdahale yoluyla yapılması gerekecektir. Yapay zekânın regülasyonunda da toplumu, demokrasiyi veya ekonomik bütünlüğü korumak amacıyla temel hak ve özgürlüklerin kısıtlanması anlamına gelecek adımlar atılması söz konusu olursa, örneğin YZT'dekine benzer yasaklı uygulamaların düzenlenmesine karar verilirse bunun kanunla yapılması gerekecektir.

Dikkat edilmesi gereken bir diğer husus ise sadece hukuki düzenleme yapılabiliyor olmasının yapılacak düzenlemenin uygulanacağı anlamına gelmeyeceğidir. Özellikle yaygın kullanılan ve sınır aşan etkileri olan teknolojilere ilişkin kuralların getirilmesi ile getirilecek kuralların uygulanması arasında önemli farklılıklar ortaya çıkabilmektedir. Örneğin internet üzerinde çevrim içi erişilen korsan içeriklerin engellenmesine yönelik birçok hukuki düzenleme bulunmasına rağmen internetin işleyişi gereği bunun tamamen engellenmesi mümkün olmamaktadır. Yapay zekâ özelinde de yapay zekâ sistemlerinin yasaklanmasına veya bu sistemlerin işleyişinin hukuka, etik ilkelere, insan haklarına ve demokrasinin temel ilkelerine uygun şekilde gerçekleştirilmesi gerektiğine yönelik hukuki düzenlemeler yapılması mümkündür. Ancak bu yönde bir yasağın icrasının ya da etik ilkeler ve hukuka uygunluk gibi yoruma açık ifadelerin uygulamadaki yansımalarının nasıl olacağının takibi son derece zor olacaktır. Ulaşılmak iste-

nen amaç yasaklama ya da genel bir ilkenin hayata geçirilmesi ise o zaman bir hukuki düzenleme ile bu sonuca ulaşılıp ulaşılamayacağı değerlendirilmeli düzenleme yapılacaksa da bu hususlar göz önünde bulundurularak yapılmalıdır.

Bu noktada etik ilkelerin etkisine ve hukuk ile ilişkisine ayrıca değinilmesi de faydalı olacaktır. Yapay zekâ sistemlerinin geliştirilmesinde, kullanılmasında ve insanların hayatını etkilemesinde etik ilkelere uygunluk gerekliliği üzerinde belli bir uzlaşının sağlandığı bir amaçtır. Ancak "yapay zekânın etik olması gerekliliği" ile "hangi koşullarda bunun sağlanmış varsayılacağı" ya da "uygulamada etik yapay zekânın nasıl bir görünümünün olacağı" çok farklı sorulardır. Geldiğimiz noktada önemli olan "etik olma durumu"nun nasıl gerçek hayata geçirileceği olup "yapay zekâ etik olsun" demek mevcut tartışmaya katkı sağlamayan bir temenni olmaktan öteye gitmemektedir. Bu sebeple "yapay zekânın etik değerlere uygun olmaması" tek başına da hukuki müdahaleyi meşru kılmayacaktır. Yine bu sebeple çalışmanın genelinde yapay zekâ ve etik ilkeler arasındaki ilişkiye ayrıca değinilmeyecektir. Ancak bu durum etik ilkelerin önemsiz olduğuna dair bir duruş olarak anlaşılmamalıdır. Tam aksine etik ilkelerin teknoloji ile ilgili hukuki düzenlemelerde kanımızca da oldukça önemli bir yeri vardır. Ancak yine kanımızca etik ilkeler, olabildiğince temenninin ötesine geçecek ve operasyonel hale getirilebilen daha somut düzenlemeler şeklinde hukuki düzenlemelere eklemlendirilmelidir.

Teknolojinin hukuki düzenleme yoluyla regülasyonunda sadece hukuki düzenlemenin yapılması, özellikle de internet üzerinden çok kolay bir şekilde erişilebilen ve her bir kullanımın teker teker gözetlenmesinin pratik gerekçelerle imkânsız olduğu uygulamalar bakımından, neredeyse hiçbir zaman tek başına yeterli olmayacaktır. Çoğu zaman bunun diğer regülasyon araçlarıyla da desteklenmesi gerekecektir. Bu noktada yapay zekâ özelindeki incelemeye geçilmeden önce son olarak siber dünyanın regülasyonunda sıklıkla atıf yapılan, Lawrence Lessig tarafından ileri sürülen ve "bir kanun olarak kod" şeklinde Türkçe'ye tercüme edilebilecek "*code is law*" yaklaşımından söz etmek faydalı olacaktır.

"*Code is law*", yazılım altyapısına dayalı sistemlerdeki davranışların doğrudan yazılım altyapısındaki kodlara entegre edilecek kurallarla bu sistemdeki davranışların sanki kanunlar gibi yönlendirilebilmesini ifade eder[21].

[21] Lessig, s. 5.

Örneğin çevrim içi izleme platformlarının farklı ülkelerdeki lisans anlaşmalarının doğrudan uygulanabilmesi için hangi ülkelerden hangi içeriklerin erişilebileceğinin IP adresine dayalı yer tespiti ile doğrudan yazılım altyapısı üzerinden denetlenmesi bu yaklaşıma örnektir. Bu çalışmanın başlığının da esin kaynağı olan bu yaklaşım özellikle Türk hukuk literatüründeki çalışmalarda teknoloji regülasyonuna yönelik tek ve geçerli bir yaklaşımmış gibi yansıtılsa da aslında bu alandaki çok sayıda yaklaşımdan biri olup siber dünyanın kontrol edebileceğini ileri süren ve aslında güncel gelişmeler ışığında geçerliliği çokça tartışılan "siberpaternalizm" olarak adlandırılan bir yaklaşımın altında yer almaktadır[22]. Gerçekten de ilk bakıştaki albenisine ve teker teker tüm kullanıcıların kontrol edilmesinin pratik zorluğuna yönelik getirdiği kolaylıklara rağmen *code is law* yaklaşımı dinamik siber dünyanın ve teknolojinin regülasyonunda iki temel gerekçeyle kullanışlı olduğu kadar sorun yaratmaya da müsaittir.

İlk olarak yapay zekânın tarihsel gelişiminin de gösterdiği üzere tüm kural ve denetim mekanizmalarının koda dökülmesi mümkün değildir. Örneğin yapay zekânın etik olup olmadığının, yapay zekâda kullanılan verilerin etkilenecek toplulukları temsil kabiliyetini haiz olup olmadığının, yapay zekânın işlev ve çıktılarının temel hak ve özgürlüklere uygun olup olmadığının kod ile kontrol edilmesi mümkün değildir. İkincisi, kod aracılığıyla kontrole aşırı ve yaygın bağlılık denetimin çok katı olması, istenenin tam aksine sonuçlar ortaya çıkması sonucunu doğurabilecektir. Bu itibarla "*code is law*" yaklaşımı teknoloji regülasyonunun tüm sorunlarına derman olacak bir yaklaşım olmayıp tam aksine bazı sınırlarla beraber gelmektedir[23]. Bu sınırlar aslında çalışmanın ilerleyen kısımlarında da değinileceği üzere yapay zekâ da dahil teknoloji regülasyonunda teknik araçların diğer tür araçlarla beraber kullanılması gerektiğini gözler önüne sermektedir.

Çalışmanın bir sonraki bölümünde, bu bölümde ortaya konulan metodolojiye uygun şekilde yapay zekânın hukuki araçlar yoluyla regülasyonunun gerekli olup olmadığının incelenmesi durumunda karşımıza çıkan tablo değerlendirilecektir.

---

22 Bu konuda detaylı açıklamalar ve diğer yaklaşımlar için bkz. Murray, A.: Information Technology Law – The Law and Society, 5. Baskı, Oxford 2023, s. 64 vd.

23 Lessig'in teorilerine yönelik bazı eleştiriler için bkz. Post, D.G.: What Larry Doesn't Get: Code, Law, and Liberty in Cyberspace, Stanford Law Review, 2000, C. 52, s. 1439-1459.

B. YAPAY ZEKÂNIN HUKUKİ DÜZENLEME YOLUYLA REGÜLASYONUNUN GEREKLİLİĞİ

İlk olarak yapay zekâ olarak adlandırılan teknolojilerin çok geniş bir yelpazeye yayılmış olup gün geçtikçe de değişmeye devam ettiği açıktır. Şu an bir içerik platformunda izlenecek bir sonraki içeriği öneren sistem de ChatGPT gibi genel amaçlı metin bazlı içerik üreten sistemler de otonom araç yazılımları da onlarca yıldır kullanılmakta olan bazı sistemlerle birlikte yapay zekâ olarak adlandırılmaktadır. Dolayısıyla genel olarak yapay zekânın ortaya çıkardığı ve hukuki düzenleme ile çözülmesi gereken bir sorunun ya da ulaşılması gereken bir amacın varlığından söz etmek mümkün olmayacaktır. Bu incelemenin yapılabilmesi için sorun kaynağı olan ve düzenleme konusu yapılacak yapay zekânın daha dar kapsamda ortaya konulması gerekmektedir.

Daha özele inildiğinde makine öğrenmesi olarak adlandırılan tekniğe dayanan sistemlerin özellikle regülasyon açısından diğerlerinden ayrıldığı görülmektedir. Makine öğrenmesi de altında birçok farklı tekniği barındıran üst kavram olduğundan burada da bir ayrıma gidilmesi doğru olacaktır. Bu noktada en çok sorun ya da risk teşkil eden sistemlerin yüksek hacimli veri setlerini analiz edip bunlar üzerinden belirli çıkarımlar yapmak suretiyle tam olarak hangi aşamalardan geçtiği veya hangi kriterleri dikkate aldığı net olarak tespit edilemeyen ve bu itibarla da insanlar tarafından bakıldığında belirli bir teknik karmaşıklığın yanında öngörülemezlik de içeren sistemler olduğu görülmektedir. Bunun iki temel sebebi mevcuttur.

İlk sebep, bu sistemlerin insanların hayatını ve toplumu hiç olmadığı kadar geniş ölçekte ve önemli şekilde etkilemesidir. İşlevsellikleri ve getirdikleri verim artışı sebebiyle kullanıldıkları yere göre insanların bir işe girip giremeyecekleri, kredi alıp alamayacakları, kanser hastası olup olmadıkları, otonom araç sürücülerinin yolculukları boyunca güvende olup olmadıkları, kolluk tarafından kullanılan sistemler bakımından ilgili kişilerin özgürlüğünün kısıtlanıp kısıtlanmayacağı gibi birçok önemli karar doğrudan bu sistemler tarafından verilmekte veya nihai kararın insan tarafından verildiği hallerde bile kararın oluşmasında bu sistemler önemli bir rol oynamaktadır.

Regülasyon bakımından etkinlikten daha önemli olan ve hatta etkinlik sebebiyle de önemi daha da artan ikinci sebep ise daha önce de değinilen ve modern anlamda yapay zekâ olarak adlandırılan sistemlerin yıllardır kul-

lanmakta olduğumuz deterministik bilgisayar programlarından ve cihazlardan farklılaşan işleyişleridir[24]. Bilgisayar programlarının deterministik olması kural olarak programların açıkça kodlanmamış bir işlem yapmamalarını ve bu sebeple tüm olası çıktıların aslında gerçekleştirilecek işlemler izlenmek suretiyle takip edilebilmesini ya da öngörülebilmesini ifade eder. Bu durum bilgisayar programlarının hatasız olduğu anlamına gelmez ama deterministik sistemlerde aslında atılacak adımlar belli olduğundan eğer hataya sebep olan giriş adımları ya da girdiler bilinirse olası hatalar ya da eksikler öngörülebilir. Makine öğrenmesinin yapay zekâyı modern yapay zekâ haline getiren örneklerinde ise yine yazılımcılar tarafından sisteme bazı komutlar girilmektedir. Ama bu komutlar doğrudan nihai yapılması istenen işlemlere ilişkin değildir. O işi gerçekleştirecek olan ve- çoğunlukla model olarak karşımıza çıkan- yeni bir yazılım yapısının doğrudan bilgisayar tarafından oluşturulmasına ilişkindir. Bu adımların gerçekleştirilmesi sonucunda oluşturulan modelin bir girdiyi alıp hangi adımlardan geçerek çıktıya ulaştırdığı ise geleneksel kaynak kodları gibi insan üretimi olmadığından doğrudan insanlar tarafından anlaşılabilir değildir. Bu noktada özellikle vurgulamak gerekir ki ne kadar gelişmiş olursa olsun yapay zekâ olarak adlandırılan sistemlerin bir paranormal aktivite ya da sihir olmadığı ve en temelinde bazı istatistiksel hesaplamalar yoluyla modellerin oluşturulduğu unutulmamalıdır. Burada modelleri öngörülemez yapan şey o modelin oluşturulması için incelenen veri setlerinin büyüklüğü ve bu veri setlerinden bazı çıkarımlar yaparken çok kısa sürede ve çok sayıda gerçekleştirilen işlemlerin insanlar tarafından -en azından şimdilik- takip edilemez olmasıdır. Gerçekten de teknik yenilik seviyesi ne olursa olsun tüm işlemleri belirli bir seviye üzerinde öngörülebilir olan sistemlerin regülasyon bakımından yıllardır kullanmakta olduğumuz deterministik bilgisayar programlarından önemli ölçüde ayrışmayacağı genel olarak söylenebilirken teknolojiyi kontrol etmeye ve sonuçlarını yönetmeye dair genel yaklaşımlarımızın çıktıları öngörülemez sistemlerle baş etme noktasında daha yetersiz kalacağı açıktır.

Bu açıklamalar ışığında modern yapay zekâya ilişkin en temel sorunumuzun çıktıları öngörülemeyen kompleks sistemlerin insanların hayatlarını önemli ölçüde etkileyen kararlar vermesi ya da bu kararlar verilirken etkin şekilde kullanılması, ancak bu kararların hem hesap verilebilir ölçüde şeffaf olmayıp hem de hatalı olabilmesi olduğu söylenebilir. Tabi ki bununla

[24] Ayrıca bkz. Güçlütürk, *Verinin Kullanımı,* s. 47 vd.

bağlantılı olarak insanların kişisel verilerinin hiç olmadığı kadar fazla bağlantı noktasıyla bir arada işlenmesi, mahremiyet koruyucu düzenlemelerin yetersiz kalması, gelişmiş modellerin enerji ihtiyacı sebebiyle çevreye zarar verme ihtimalleri ve ekonomik etkiler gibi daha birçok yan husus da eklenebilir. Önemli olan ise bu sorunların bir müdahaleyi gerekli kılıp kılmadığıdır.

Bu konuda verilen kararın birçok farklı faktörden beslenen bir politika tercihi olduğu söylenebilir. Belirtilen sorunlar oldukça yeni geliştirilmiş modellerden kaynaklanmakta olup henüz gerçekten müdahaleyi meşru kılacak kadar uzun süreli olup olmayacaklarını kesin şekilde tespit etmek mümkün değildir. Bununla birlikte eğer bir adım atılmazsa objektif olarak geri dönülmesi zor bir durumun ya da çok önemli bir zararın meydana geleceğini söylemek de mümkün olmayabilir. Nihayet bir adım atılması gerektiğine karar verilirse bu adımın hukuki düzenleme yoluyla atılmasının gerekli olup olmadığı noktasında da tek bir doğru görüşün varlığından söz edilemez. Nitekim şu an yapay zekâ sistemleri dünyadaki farklı devletler ve düzenleyici otoriteler tarafından yakından takip edilmekte, bazı devletler doğrudan düzenleme yoluna giderken bazıları ise piyasa müdahaleleri yoluyla daha yumuşak adımlar atmakta veya sadece gelişmeleri izlemekle yetinmektedir.

Bu noktada sorunu bölge bazında da bir adım daha özelleştirerek incelemek doğru olacaktır. Cevaplanması gereken soru Türkiye'de yapay zekânın hukuki düzenleme yoluyla regülasyonunun gerekli olup olmadığıdır. Bu sorunun detaylı şekilde cevaplandırılması bu çalışmanın kapsamını aşmaktadır. Ancak en azından bu çalışmada bahsedilen hususlarla bağlantılı olarak Türkiye'de yapılacak hukuk yoluyla regülasyon çalışmalarında şu hususların dikkate alınmasının önemli olduğu söylenebilir.

- Türk hukukunda yapay zekâya da uygulanacak belirli genel nitelikte düzenlemeler mevcuttur. Bu itibarla Türk hukukunda yapay zekâya uygulanacak bir hukuki düzenleme olmadığını söylemek doğru olmayacaktır. Sözleşmelere, haksız fiile, fikir ve sanat eserlerine[25], kişisel verilerin korunmasına ilişkin genel nitelikli düzenlemeler buna örnek gösterilebilir.

[25] ChatGPT ile üretilen içeriklerin Türk fikir ve sanat eserleri hukuku kapsamında eser niteliğine ilişkin değerlendirme için bkz. GÜÇLÜTÜRK, O.G.: *ChatGPT ile Üretilen İçeriklerin Eser Niteliğinin 5846 sayılı Fikir ve Sanat Eserleri Kanunu Bakımından Değerlendirilmesi*, Galatasaray Üniversitesi Hukuk Fakültesi Dergisi, 2022, C. 2, s. 1899-1912.

- Ancak bu düzenlemelerin kapsamının teorik olarak yeterli genişlikte olması doğrudan bu alanda bir uygulamanın oluşacağı anlamına gelmemektedir. Özellikle bu düzenlemelerin uygulamasında etkili olacak başta hakimler ve savcılar olmak üzere ilgili profesyonellerin genel nitelikli düzenlemelerin yapay zekâya ve benzer diğer yeni nesil teknolojilere uygulanabilirliği noktasında bilgilendirilmesi önem taşımaktadır.

- Yapılacak bir düzenleme özellikle de politik ve ekonomik büyüklük olarak Türkiye'den önemli ölçüde farklılaşan AB, Amerika Birleşik Devletleri ("**ABD**") veya Çin'de çıkarılan düzenleme ya da çerçevelerin birebir çevrilmesi yoluyla yapılmamalıdır. Türkiye kendi yasama kültürü, kendi sosyo-kültürel gerçekleri ve ekonomik ihtiyaçları olan bir ulus devlettir. Yapılacak düzenlemelerin, bu karakteristik özellikler ile uluslararası gelişmelere uyum arasında kurulacak bir denge üzerinden oluşturulması doğru olacaktır. Bu noktada Türkiye'nin mevcut hukuk sistemine uyumluluk, uluslararası antlaşmalardan kaynaklı yükümlülükler ve Türkiye'nin AB ile arasındaki gümrük birliği ilişkisi ile aday üye ülke statüsü de göz önünde bulundurulduğunda AB hukuku kaynaklı düzenlemelerin diğerlerine nazaran Türkiye'de geliştirilecek hukuki çerçeve üzerinde de daha etkili olacağını söylemek yanlış olmayacaktır.

III. BİR HUKUKİ DÜZENLEME NESNESİ OLARAK YAPAY ZEKÂ

Neredeyse tüm çalışmalarda belirtildiği üzere yapay zekânın üzerinde uzlaşılmış bir tanımı bulunmamaktadır[26]. Bu çalışmanın amacı yapay zekâyı tanımlamak değildir. Kanımızca yapay zekânın ne olduğunu tanımlamak hukukçuların görevi de değildir. Yapay zekâ olarak adlandırılan teknolojilerin neyi kapsadığı zamana ve topluma göre değişebilecektir. Bundan elli sene önce yapay zekâ olarak adlandırılan sistemlerle şimdi yapay zekâ olarak adlandırılan sistemler arasında önemli farklar bulunmaktadır. Hatta, bir dönem yapay zekâ olarak adlandırılan teknolojiler aslında toplumda zamanla yaygınlaştıkça ve "normalleştikçe" bu kavram dışında kalabilmektedir[27].

---

26 Yapay zekânın tanımına ilişkin detaylı açıklamalarımız için bkz. Güçlütürk, Osman Gazi: Yapay Zekâ ve Verinin Kullanımı, İstanbul 2022 (Kısaltma: *Verinin Kullanımı)*, s. 36 vd.

27 A100 Standing Committee and Study Panel: "*One Hundred Year Study on Artificial Intelligence: Report of the 2015-2016 Study Panel*", (https://ai100.stanford.edu/2016-report, E.T.: 11.06.2024), s. 12.

Diğer yandan hukuki düzenlemelerin uygulanacağı sistemlerin hukuki belirlilik ilkesi kapsamında belirlenebilmesi için de bir "tanım" yapılması gerektiği açıktır. Örneğin KVKK kişisel verilerin işlenmesine uygulanacaktır. Bunun için kişisel verinin ne olduğu ve işlenmenin hangi faaliyetleri içerdiği belirlenebilmelidir. Yapay zekâyı hedef alacak bir hukuki düzenleme yapılacaksa da yapay zekânın ne olduğu veya bu kadar geniş yapay zekâ uygulamaları yelpazesi arasında kapsamda kalanların hangi yapay zekâ sistemleri olduğu belirlenebilmelidir. Peki bu kadar dinamik teknolojilerle ilgili olarak hukukçuların ve hukuki düzenlemelerin getirdiği tanımların niteliği ne olacak ve bu tanımlar nasıl yapılacaktır?

Öncelikle hukuki düzenlemelerle getirilen teknolojilere ilişkin tanımların çoğu zaman gerçek anlamda teknik bir tanım olmadığı, aslında düzenlemenin uygulanacağı nesneleri belirlemek için getirilen kriterler olduğu unutulmamalıdır. Örneğin Ödemelerde Kripto Varlıkların Kullanılmamasına Dair Yönetmelik[28] m. 3(1)'de yapılan kripto varlık tanımı bunun tipik bir örneğidir. Buna göre "*Yönetmeliğin uygulanmasında kripto varlık, dağıtık defter teknolojisi veya benzer bir teknoloji kullanılarak sanal olarak oluşturulup dijital ağlar üzerinden dağıtımı yapılan, ancak itibari para, kaydi para, elektronik para, ödeme aracı, menkul kıymet veya diğer sermaye piyasası aracı olarak nitelendirilmeyen gayri maddi varlıkları ifade eder*". Özellikle bu "tanım"ın son kısmına bakıldığında aslında teknik olarak kripto varlık olarak adlandırılabilecek, belki bir blokzincir üzerinde çıkarılmış olan ama örneğin elektronik para ya da sermaye piyasası niteliği taşıyan bir kripto varlık, anılan yönetmelik kapsamında "kripto varlık" olarak sınıflandırılamayacaktır. İşte bu aslında gerçek bir tanım değil hangi kripto varlıklara düzenlemenin uygulanacağını belirlemeye çalışan bir filtredir[29].

Yapay zekâya ilişkin tanımlar da bu kadar net olmasa da benzer bir ikilem taşımaktadır. Hukuki düzenlemeler bazen yeni teknolojik gelişmeler sebebiyle, bazen tamamen işlevsel farklılıklar sebebiyle ya da başka diğer bir sebeple teknik çevrelerde veya günlük hayatta yapay zekâ olarak adlandı-

---

[28] Ödemelerde Kripto Varlıkların Kullanılmamasına Dair Yönetmelik 16.04.2021 tarih ve 31456 sayılı Resmî Gazet'de yayımlanmıştır, (https://mevzuat.gov.tr/mevzuat?MevzuatNo=38569&MevzuatTur=7&MevzuatTertip=5, E.T.: 11.06.2024).

[29] Bu düzenlemede yer alan tanıma dair detaylı bir analiz için bkz. Güçlütürk, O.G./Cankat, R.: Güncel Gelişmeler Işığında Türk Hukukunda Kripto Varlıkların Hukuki Niteliği (ed. Aksoy Retornaz, E.E. ve Güçlütürk, O.G.), "Gelişen Teknolojiler ve Hukuk I: Blokzincir", Gözden Geçirilmiş ve Genişletilmiş 2.Bası, İstanbul 2021, s. 215-241.

rılan bazı sistemleri bilinçli olarak ya da belki farkında olmayarak kapsam dışı bırakabilecektir.

Peki, bir adım daha atarsak, bir hukuki düzenleme için yapılacak yapay zekâ "tanım"ı nasıl olmalıdır? Öncelikle bu tanım önceki bölümlerde açıklanan amaç, hedef, işlevsellik gibi kriterler dikkate alınarak dikkatli şekilde yapılmalıdır. Örneğin onlarca yıldır kullanılmakta olan ve dışarıdan bakıldığında gerçekleştirdiği işlem sebebiyle yapay zekâ olarak adlandırılabilecek oyun oynayabilen ya da kelime bazlı çeviri yapabilen deterministik sistemler modern anlamda yapay zekâ sistemleriyle ilgili çözmek istediğimiz sorunlara sebep olmadığından bunların yapılacak düzenlemedeki tanımın kapsamı dışında kalması doğru olacaktır.

Yapılacak tanımda önem arz eden bir diğer husus çok geniş ifadelerin kullanılmamasıdır. Özellikle teknoloji regülasyonunda düzenlemelerin çok hızlı bir şekilde güncelliğini kaybetmemesi ve olası yeni gelişmeleri de kapsamda tutabilmesi için bilinçli olarak belirli bir ölçüde geniş ifadeler kullanılabilir. Ancak kapsamı aşırı genişleten ifadelerden özellikle kaçınılmalıdır. Örneğin yapay zekâ tanımı yaparken sadece "insanlar tarafından gerçekleştirilen faaliyetleri gerçekleştirmek" gibi bir kriter kullanmak yine regülasyon gerektirmeyen ve hâlihazırda mevcut hukuki düzenlemelerle zaten belirli ölçülerde regüle edilmekte olan sistemleri de kapsayacak genişlikte[30] olduğundan sorun çözmekten çok sorun yaratacaktır.

Teknolojiyi hedef alan bir hukuki düzenlemede bir tanım yapılırken teknik işleyişe de uygun olan ifadelerin kullanılmasına dikkat edilmelidir. Örneğin yapay zekâ için bazı yerlerde kullanılan tanımlarda yer alan "insan zekâsını örnek alması"[31], "insanın bilişsel kabiliyetlerinin kopyalanması" veya "makinelerin düşünmesi"[32] gibi hususlar aslında dışarıdan bakıldığında insanlar tarafından yorum yoluyla oluşturulan ifadeler olup yapay zekâ olarak adlandırılan sistemlerin işleyişini doğru şekilde ifade edememektedir. Bu sistemler nihai olarak gerçekleştirilen işlemler bakımından her ne kadar bazı faaliyetleri insanlar gibi hatta onlardan daha iyi gerçekleştirseler de süreç bakımından ortada ne bir taklit ne de insanın gerçekleştirdiği gibi bilişsel bir faaliyet söz konusudur. Bu şekilde yapılacak bir tanım doğ-

30 Ayrıca bkz. Güçlütürk, *Verinin Kullanımı,* s. 43 vd.

31 Küçük, E.S.**:** *Yapay Zekâ Varlıkların Hukuki Statüsü Üzerine Disiplinler Arası Bir Muhakeme,* Bilişim Hukuku Dergisi, 2024, C. 6, S. 1, s. 2.

32 Erdoğan, G.**:** *Yapay Zekâ ve Hukukuna Genel Bir Bakış,* Adalet Dergisi, 2021, S. 66, s. 124.

ru bir şekilde kaleme alınmadığında kapsaması istenen sistemleri bile kapsayamayabilecektir[33].

Yine hukuki düzenlemelerde yer alacak yapay zekâ tanımının düzenlemenin amacına ve kapsamına göre değişebileceği açık olduğundan bütün düzenlemeler için isabetli olabilecek bir hukuki yapay zekâ tanımından söz etmek mümkün değildir. Bu çalışmada da yapay zekâ için genel bir tanım vermekten kaçınılacaktır. Fakat geniş kapsamlı düzenlemeler için uzun çalışmalar sonrası oluşturulmuş olan mevcut düzenleme çalışmalarındaki bazı tanımlar esas alınabilir. Bu düzenlemelerde de genel olarak yapay zekânın değil, yapay zekâ sisteminin tanımlandığı ve bazılarında modelle sistem arasında bir ayrım yapıldığı görülmektedir. Örneğin OECD tarafından Kasım 2023'te güncellenen ve YZT tanımını da etkileyen tanıma göre[34] yapay zekâ sistemi "*aldığı girdilerden çıkarımlar yaparak, açık veya örtük hedefler doğrultusunda, fiziksel veya sanal ortamları etkileyebilecek tahminler, içerikler, öneriler veya kararlar gibi çıktılar üreten makine tabanlı bir sistemdir*"[35]. Yapay Zekâ ve İnsan Hakları, Demokrasi ve Hukukun Üstünlü-

---

33 Türk hukukunda yapay zekânın genelde makinelerin insan ve insan zekâsı ile bağdaştırılan faaliyetleri yerine getirme kabiliyetiyle veya insan davranışlarını yerine getirmeyle bağlantılı olarak tanımlandığı yönünde bkz. Güçlütürk, *Verinin Kullanımı,* s. 41. Yine bu eserden alıntıyla şu örnekler verilebilir: "*Yapay zekâ bir makinenin insan aklının ürünü davranışları taklit etme yeteneği olarak tanımlanmaktadır*", bkz. Kangal, Z.T.: Yapay Zekâ ve Ceza Hukuku, 2021, s. 21; *"... "yapay zekâ" terimi, çoğu zaman bir makinenin yahut bilişim sisteminin "öğrenme", "yorumlama", ve "problem çözme" gibi insan zihniyetliyle doğrudan ilişkilendirilen bilişsel işlevleri taklit etmesi durumunda kullanılmaktadır*", bkz. Akkurt, S.S.: *Yapay Zekânın Otonom Davranışlarından Kaynaklanan Hukuki Sorumluluk*, Uyuşmazlık Mahkemesi Dergisi 2019, C. S. 13, 2019, s. 41; "*Yapay zekâ, insanlar tarafından yapıldığında belirli bir zekâ gerektiren işleri yapabilen makineler olarak tanımlanabilir*", bkz. Bak, B.: *Medeni Hukuk Açısından Yapay Zekânın Hukuki Statüsü ve Yapay Zekâ Kullanımından Doğan Hukuki Sorumluluk*, Türkiye Adalet Akademisi Dergisi 2018, C. S. 35, 2018, s. 212. Benzer yönde bkz. Bozkurt Yüksel, A.E./Bak, B.: Futurist Hukuk, 2018, s. 6; "*… yapay zekâ, insanın yaptıklarını taklit edebilen bilgisayarların geliştirilmesi konusunda kullanılan torba bir terim olarak da görülebilir*", bkz. Kapancı, K.B.**:** Özel Hukuk Perspektifinden Bir Değerlendirme: Yapay Zekâ ve Haksız Fiil Sorumluluğu, (ed. Aksoy Retornaz, E.E. ve Güçlütürk, O.G.), "Gelişen Teknolojiler ve Hukuk II: Yapay Zekâ", İstanbul 2021 s. 128.

34 Russell, S./Perset, K./Grobelnik, M.: OECD AI Wonk Blog (2023), "*Updates to the OECD's definition of an AI system explained*", (https://oecd.ai/en/wonk/ai-system-definition-update, E.T.: 11.06.2024).

35 Tanımın İngilizce orijinal hali şu şekildedir: "*An AI system is a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment.*"

ğüne Dair Çerçeve Sözleşme'de de (*Framework Convention on Artificial Intelligence and Human Rights, Democracy, and the Rule of Law*", ("**FCAI**"))[36] yapay zekâ sistemi neredeyse OECD tanımıyla tamamen aynı şekilde tanımlanmaktadır[37].

YZT m. 3(1)'de ise "*farklı ölçülerde özerklikle çalışacak şekilde tasarlanmış ve kullanıma alındıktan sonra da gelişip adapte olabilen ve açık veya örtülü hedefler doğrultusunda aldığı girdilerden, fiziksel veya sanal ortamları etkileyebilecek tahmin, içerik, öneri veya karar gibi çıktıları nasıl oluşturabileceği yönünde çıkarımlarda bulunan makine tabanlı bir sistem*" olarak tanımlanmıştır[38]. YZT etkileri daha sonraki bölümde açıklanacağı üzere yapay zekâ sistemlerini ve genel amaçlı yapay zekâ modellerini ayrı şekilde düzenlemektedir. Genel amaçlı yapay zekâ modelleri ise YZT m. 3(63)'te "*özerk bir gözetimle büyük miktarda veri kullanılarak geliştirilenler de dahil ama piyasaya sürülmeden önce araştırma, geliştirme veya prototip oluşturma faaliyetleri için kullanılanlar hariç olmak üzere, önemli genel yetenekler sergileyen ve piyasaya sürülme şekline bakılmaksızın geniş bir yelpazedeki farklı görevleri yetkin bir şekilde yerine getirebilen ve çeşitli alt sistemlere veya uygulamalara entegre edilebilen yapay zekâ modeli*" olarak tanımlanmıştır[39].

---

36 Council of Europe (2024), "Framework Convention on Artificial Intelligence and Human Rights, Democracy, and the Rule of Law", (https://rm.coe.int/1680afae3c, E.T.: 09.06.2024).

37 FCAI m. 2.

38 Tanımın İngilizce orijinal metni şu şekildedir: "'*AI system' means a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments*". Bu tanım AB Komisyonu'nun ilk önerisinden bu yana önemli değişiklikler geçirmiş ve özellikle de daha önceki tanımlar tanımın genişliği ve tekniklerin sayılmasının getireceği sorunlar sebebiyle eleştirilmiştir. EDWARDS, Lilian**:** Ada Lovelace Institute (2022), "*The EU AI Act: a summary of its significance and scope*", (https://www.adalovelaceinstitute.org/wp-content/uploads/2022/04/Expert-explainer-The-EU-AI-Act-11-April-2022.pdf, E.T.: 11.06.2024), s. 7; Ebers, M./Hoch, V.R.S../Rosenkranz, F./Ruschemeier, H./Steinrötter, B.**:** *The European Commission's Proposal for an Artificial Intelligence Act—A Critical Assessment by Members of the Robotics and AI Law Society (RAILS)***,** Multidisciplinary Scientific Journal, 2021, C. 4, S. 4, s. 590.

39 Tanımın İngilizce orijinal metni şu şekildedir: "'*general-purpose AI model' means an AI model, including where such an AI model is trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable of competently performing a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications,*

Bu tanımlardan görüldüğü üzere yapay zekâ için yapılan hukuki tanımlarda Avrupa odaklı gelişmelerde bir uzlaşı sağlanıyor gibi görünse de bir inceleme yapılırken somut olay özelinde yapılacak düzenlemenin niteliği, amacı, hedefi dikkate alınarak düzenlemeye özel isabetli bir tanım yapılmalıdır. Yapılacak tanımlar okunurken ve yorumlanırken de yine bu hususlar göz önünde bulundurulmalıdır.

Çalışmanın bir sonraki ve son bölümünde, yapay zekânın hukuk yoluyla regülasyonunda bu çalışmanın yazım tarihi itibariyle en önemli metin olan YZT'nin bu konudaki yaklaşımı ve getirdiği düzenlemeler mercek altına alınacaktır.

IV. YAPAY ZEKÂNIN HUKUK YOLUYLA REGÜLASYONUNDA BİR MİHENK TAŞI OLARAK AB YAPAY ZEKÂ TÜZÜĞÜ

Her yeni teknoloji gibi yapay zekânın regülasyonunda da farklı aşamalardan geçilmiştir ve geçilmektedir. Modern yapay zekâ sistemlerinin daha önce değinilen yeni nesil sorunları ortaya çıkardığının görülmesi üzerine öncelikle etik ve ilke odaklı kavramsal çalışmalar yapılmıştır. Bu çalışmaları, bu ilkeleri uygulamaya entegre etmeye çalışan çerçeve çalışmaları izlemiştir. Nihayetinde hem ulusal hem uluslararası alanda düzenlemelerin gerekli olup olmadığı tartışması başlamış ve düzenlemeler yapılmaya başlanmıştır.

Yapay zekâ regülasyonu konusunda dünyanın farklı bölgelerinde farklı yaklaşımlar görülmektedir. Uluslararası ölçekte belki de en önemli gelişme Türkiye'nin de üyesi bulunduğu Avrupa Konseyi tarafından çalışmalarına, 2019'da kurulan *Ad-Hoc Committee on Artificial Intelligence* (CAHAI) ile başlanılan ve daha sonra *Committee on Artificial Intelligence* (CAI) çatısı altında devam ederek yakın zamanda tamamlanan FCAI'dir. FCAI 17.05.2024 tarihinde Avrupa Konseyi tarafından da onaylanmıştır[40].

---

except AI models that are used for research, development or prototyping activities before they are placed on the market".

40 Council of Europe Newsroom (2024), "Council of Europe adopts first international treaty on artificial intelligence", (https://www.coe.int/en/web/portal/-/council-of-europe-adopts-first-international-treaty-on-artificial-intelligence, E.T.: 09.06.2024). FCAI bir uluslararası antlaşma olduğu için Avrupa Konseyi tarafından onaylanması doğrudan bağlayıcı hale gelmek olarak anlaşılmamalıdır. Bir uluslararası antlaşmanın bağlayıcı hale gelmesi için öncelikle antlaşmada öngörülen prosedüre göre yürürlüğe girmesi gerekmektedir. FCAI için bu 30. maddesinde öngörüldüğü üzere en az üçü Avrupa

Diğer yandan uluslararası arenada yapay zekâya ilişkin bağlayıcı olmayan başka birçok regülasyon girişimi de bulunmaktadır. Birleşmiş Milletler tarafından Ekim 2023'te Yapay Zekâya İlişkin Üst Seviye Danışma Kurulu (*High-level Advisory Body on Artificial Intelligence*) kurulmuştur[41]. Bir başka uluslararası örgüt olan OECD nezdinde yapay zekâ üzerine önemli çalışmalar yürütülmektedir. OECD yapay zekâya ilişkin ilkeleri derlediği "*OECD AI Principles*"ı[42] 2019'da ilk defa kabul etmiş[43] ve bunları Mayıs 2024'te güncellemiştir[44].

ABD'de federal ölçekte yapay zekâya özel bağlayıcı bir düzenleme mevcut olmamakla birlikte özellikle ABD Başkanı tarafından çıkarılan İcrai Kararlar (*Executive Order*) aracılığıyla özellikle de 30.10.2023 tarihli Yapay Zekânın Güvenli ve Güvenilir Gelişimi ve Kullanımına Dair İcrai Karar[45] ile idari otoriteleri bağlayan bazı kurallar getirilmiştir. Bununla birlikte ülke genelinde bağlayıcı olmayan, genel olarak güvenli yapay zekâ gelişimini desteklemek için NIST tarafından geliştirilen Yapay Zekâ Risk Yönetim Çerçevesi (*NIST AI Risk Management Framework*)[46] önemli bir çerçeve olarak karşımıza çıkmaktadır. Diğer yandan federe devletler seviyesinde oldukça fazla sayıda düzenleme ve düzenleme çalışması göze çarpmaktadır. Özellikle hâlihazırda uygulanmakta olan ve otomatik işe alım karar mekanizmalarının kullanımında bir önyargı denetimini zorunlu kılan 144

Konseyi üyesi olmak üzere beş imzacı devletin bağlı bulunma yönündeki iradelerini belirtmelerinden itibaren üç aylık bir sürenin geçmesine bağlanmıştır. Yürürlüğe girme sürecinden sonra da FCAI'nın her bir imzacı devleti bağlayıcı olması için imzacı devletlerin kendi iç hukuklarına göre onay sürecini yürütmesi gerekebilecektir.

41 United Nations (2024), "*High-Level Advisory Body on Artificial Inteligence*", (https://www.un.org/techenvoy/ai-advisory-body, E.T.: 09.06.2024).

42 OECD Policy Observatory (2024), "*OECD AI Principles Overview*", (https://oecd.ai/en/ai-principles, E.T.: 09.06.2024).

43 OECD (2019), "*Forty-two countries adopt new OECD Principles on Artificial Intelligence*", (https://www.oecd.org/science/forty-two-countries-adopt-new-oecd-principles-on-artificial-intelligence.htm, E.T.: 09.06.2024).

44 OECD Legal Instruments (2024), "*Recommendation of the Council on Artificial Intelligence*", (https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449, E.T.: 09.06.2024).

45 The White House (2023), "*Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*", (https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/, E.T.: 09.06.2024).

46 NIST (2023), "AI Risk Management Framework", (https://www.nist.gov/itl/ai-risk-management-framework, E.T.: 09.06.2024).

sayılı New York Kanunu[47] ile yakın zamanda Colorado'da imzalanan ve YZT'ye bazı açılardan benzeyen risk temelli bir yaklaşım benimseyen ancak YZT'nin ürün güvenliği odağından farklı olarak tüketicinin korunması odağı taşıyan SB24-205[48], yüksek riskli yapay zekâ sistemleri bakımından önemleri sebebiyle öne çıkmaktadır.

Yapay zekâya ilişkin ulusal ve uluslararası regülasyon girişimleri ile hukuki düzenlemelerin olgunlaşmaya başlaması regülasyon sorununun ya da belirsizliğinin çözülmesi demek değildir. Önemli olan getirilecek düzenlemelerin istenen amaçları ulaşmayı sağlayacak şekilde uygulamaya geçirilebilmesi ve icra edilmesidir. İşte bu noktada yapay zekâ için daha uygulanabilir bir hukuki düzenleme çerçevesi öngörmeyi amaçlayan ve bunu uluslararası bir etki doğuracak şekilde yapması beklenen YZT öne çıkmaktadır.

YZT AB düzeyinde yapay zekâya ilişkin ilk özel nitelikli düzenlemedir. Buradaki özel nitelik vurgusu önem taşımaktadır. Zira, daha önce bahsedildiği üzere, AB düzeyinde de hâlihazırda yapay zekâdan özel olarak bahsetmese de yapay zekâ sistem ve modellerine uygulanacak hukuki düzenlemeler, GVKT gibi, mevcuttur.

YZT 12.07.2024 tarihinde Avrupa Birliği Resmî Gazetesi'nde yayımlanmış, yürürlük maddesi uyarınca bunu izleyen yirminci günde, 01.08.2024'te yürürlüğe girmiştir. Ancak daha aşağıda detayları inceleneceği üzere YZT'nin yürürlüğe girmesi ile uygulanmaya başlaması arasında bir ayrım yapılmıştır ve YZT'nin genel olarak yürürlüğe girmesini takiben iki sene sonra 02.08.2026'da uygulanmaya başlayacağı düzenlenmiş; niteliği itibariyle de bazı özel düzenlemelerin uygulanma tarihleri ayrıca belirlenmiştir. İşbu metnin yazım tarihi itibariyle YZT yürürlükte olan ancak uygulaması başlamamış bir düzenleme niteliğindedir.

---

47 Bu konuda daha fazla bilgi için bkz. Hilliard, A.: HOLISTIC AI Blog (2023), "*What is New York City Local Law 144?*", (https://www.holisticai.com/blog/new-nyc-local-law-144, E.T.: 09.06.2024).

48 Bu konuda daha fazla bilgi için bkz. Hilliard, A./Anand N.: HOLISTIC AI Blog (2024), "*10 Things You Need to Know about Colorado's SB205 Consumer Protections for Artificial Intelligence*", (https://www.holisticai.com/blog/colorado-sb-205-artificial-intelligence-consumer-protections, E.T.: 09.06.2024).

A. NİTELİĞİ VE YASALAŞMA SÜRECİ

YZT Avrupa Birliği'nin İşleyişine İlişkin Sözleşme'nin ("**TFEU**") 294. maddesinde düzenlenen olağan yasama prosedüründen geçen bir AB Tüzüğü olarak hazırlanmaktadır. Tüzükler AB'nin iki temel hukuki aracından biri olup yasalaştıklarında ek bir düzenlemeye gerek olmaksızın doğrudan öngörülen alanda uygulanmaya başlarlar. Düzenlemenin kısa adında daha geleneksel bir yaklaşım olan ve AB'nin temel kişisel veri koruma düzenlemesi olan GVKT'de de geçen "*Regulation*" ifadesi yerine "*Act*" ifadesinin kullanılması ise AB yasa yapma kültüründe son dönemde etkisi görülen ve "*Actification*" olarak adlandırılan bir akımın sonucudur[49]. Ancak hukuken GVKT ile YZT -ilgili maddelerinde öngörülen sürelere uygun olarak yürürlüğe girdikten ve uygulanmaya başladıktan sonra- aynı etkiye sahip olacaktır.

AB'nin olağan yasama prosedürü uyarınca YZT için düzenleme teklifi AB Komisyonu tarafından Nisan 2021'de yapılmıştır[50]. Kural olarak olağan yasama prosedürü AB Komisyonu tarafından sunulan teklife ilişkin olarak sırasıyla AB Parlamentosu'ndan ve AB Konseyi'nden bir pozisyonun çıkması ve bu iki kurumun karşılıklı görüşmelerle olası değişiklik önerilerini de göz önünde bulundurarak anlaşması üzerine kuruludur. Ancak özellikle tartışmalı konularda resmi olarak pozisyonların görüşülmesinden sonra uzlaşının sağlanmaması ihtimalinde önerinin reddedilmiş sayılma ihtimali bulunduğundan "*Trilogue*"[51] adı verilen ve AB Parlamentosu ile AB Konseyi tarafından AB Komisyonu moderatörlüğünde gerçekleştirilen, resmi olmayan üçlü görüşmelerle AB Parlamentosu ve AB Konseyi arasında uzlaşma sağlanmaya çalışılmaktadır. Benzer şekilde doğrudan TFEU m. 294'te öngörülmeyen bazı ihtimallerde doğrudan önerinin reddedilmesi sonucuna gidilmemek için istisnai süreçler öngörülmüştür. YZT'nin yasa-

---

49 Bu konuda daha fazla bilgi için bkz. Papakonstantınou, V./De Hert, P.: *The Regulation of Digital Technologies in the EU: The Law-Making Phenomena of 'Act-ification', 'GDPR Mimesis' and 'EU Law Brutality',* SSRN 2022, (https://papers.ssrn.com/sol3/ papers.cfm?abstract_id=4123313, E.T.: 09.06.2024).

50 European Commission (2021), "*Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artıficial Intelligence (Artıficial Intelligence Act) and Amending Certain Union Legislative Acts" (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021PC0206, E.T.: 09.06.2024).*

51 EUR-Lex (2024), "*Trilogue*", (https://eur-lex.europa.eu/EN/legal-content/glossary/trilogue.html, E.T.: 09.06.2024).

laşma sürecinde ise bu istisnai süreçlerin birçoğuna başvurulduğu görülmektedir. Örneğin prensip olarak AB Komisyonu önerisini takiben AB Parlamentosu'nun pozisyonu beklendiği halde bunun uzun sürmesi üzerine çok nadir olmasa da normal sürecin istisnası olarak görülen bir prosedür işletilerek AB Konseyi tarafından AB Komisyonu önerisine ilişkin olan ve "*General Approach*" olarak adlandırılan görüşü 06.12.2022 tarihinde yayınlamıştır[52]. Bu görüş nihai niteliğinde bir metin olmayıp daha ziyade AB Parlamentosu'na bir metin üzerinde AB Konseyi ile uzlaşının nasıl sağlanabileceğine dair bir fikir verme işlevine sahiptir. AB Parlamentosu ise pozisyonunu 14.06.2023'te onaylamıştır[53]. Normalde bu aşamada daha önce belirtildiği üzere AB Parlamentosu'nun pozisyonuna dair AB Konseyi onayı ya da görüşü alınması beklenirken YZT yasama sürecinde uzlaşmanın uzun süreceği öngörülerek aynı gün doğrudan *Trilogue* üçlü görüşmeleri başlatılmış ve AB tarihinde en uzun üçlü görüşme toplantılarından biri olan 06.12.2023'te başlayıp 08.12.2023'te biten görüşmede AB Parlamentosu ile AB Konseyi arasında ortak bir metin üzerinde uzlaşma sağlanmıştır[54].

Aralık'ta metin üzerinde uzlaşma sağlanmasından sonra uzlaşma metni üzerinde detaylı noktalara ilişkin çalışmalar devam etmiş ve nihayet

---

52 Council of the European Union (2022), "*Artificial Intelligence Act: Council calls for promoting safe AI that respects fundamental rights*", (https://www.consilium.europa.eu/en/press/press-releases/2022/12/06/artificial-intelligence-act-council-calls-for-promoting-safe-ai-that-respects-fundamental-rights/, E.T.: 09.06.2024).

53 European Parliament (2023), "*Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts*", (https://www.europarl.europa.eu/doceo/document/ TA-9-2023-0236_EN.html, E.T.: 09.06.2024). Buradaki onayın YZT'nin bir yasa olarak onaylanması işle karıştırıldığı görülmektedir. Bkz. Diri, F.: *Yapay Zekâ Teknolojisi ve Beraberinde Getirdiklerinin Sağlık Hukuku Kapsamında Değerlendirilmesi,* Bilişim Hukuku Dergisi, 2024, C. 6, S. 1, s. 12; Dost, S.**:** *Yapay Zekâ ve Uluslararası Hukukun Geleceği,* Süleyman Demirel Üniversitesi Hukuk Fakültesi Dergisi, 2023, C. 13, S. 2, s. 1279. Ancak bu YZT'nin bir AB Tüzüğü olarak onayı değil diğer AB yasa koyucusu olan AB Konseyi ile yapılacak görüşmelerde AB Parlamentosu'nun duruşunu temsil edecek metnin onaylanmasıdır. AB Parlamentosu'nun tek başına bir metni onaylayarak AB Tüzüğü haline getirme yetkisi bulunmamaktadır.

54 European Parliament News (2023), "*Artificial Intelligence Act: deal on comprehensive rules for trustworthy AI*", (https://www.europarl.europa.eu/news/en/press-room/20231206IPR15699/artificial-intelligence-act-deal-on-comprehensive-rules-for-trustworthy-ai, E.T.: 09.06.2024).

02.02.2024 tarihinde bir taslak metin oluşturulmuştur[55]. Bu metin AB Parlamentosu'nda 13.03.2024 tarihinde onaylanmıştır[56]. Metindeki dil düzeltmeleri yapıldıktan sonra yine her zaman başvurulmayan *Corrigendum* prosedürü işletilerek metnin düzeltilmiş hali de itiraz olmadığı için onaylanmış sayılmıştır. Nihayet metin 21.05.2024'te AB Konseyi tarafından onaylanmıştır[57]. AB Konseyi tarafından onaylanan metin[58] ise 12.07.2024'te AB Resmî Gazetesi'nde yayımlanmıştır. YZT, 01.08.2024 itibariyle ise yürürlüktedir.

Diğer yandan YZT için yürürlüğe girme ve uygulama aynen GVKT'de olduğu gibi tam anlamıyla örtüşmeyecektir. YZT'nin getirdiği yükümlülüklere hazırlanmak için süre tanımak ve gerekli mekanizmaların kurulmasına izin vermek için genel olarak YZT düzenlemelerinin YZT'nin yürürlüğe girmesinden 24 ay sonra uygulanmaya başlayacağı düzenlenmiştir. Ancak bazı düzenlemeler için daha farklı tarihli uygulama zamanı öngörülmüştür. Örneğin ilk olarak uygulanacak düzenlemeler arasında yer alan yasaklanmış sistemlere ilişkin düzenlemeler YZT'nin yürürlüğe girmesinden itibaren altı ay içerisinde, 02.05.2025 itibariyle uygulanacaktır[59]. YZT'nin yasalaşma ve uygulanma takvimindeki önemli tarihler genel hatlarıyla şu şekildedir:

- **12.07.2024:** YZT'nin AB Resmî Gazetesi'nde yayımlanma tarihi.
- **01.08.2024:** YZT'nin yürürlüğe girme tarihi.

---

55 European Parliament (2024), "*Provisional Agreement Resulting From Interinstitutional Negotiations*", (https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/CJ40/AG/2024/02-13/1296003EN.pdf, E.T.: 09.06.2024).

56 European Parliament News (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, E.T.: 09.06.2024).

57 Council of the European Union (2024), "*Artificial intelligence (AI) act: Council gives final green light to the first worldwide rules on AI*", (https://www.consilium.europa.eu/en/press/press-releases/2024/05/21/artificial-intelligence-ai-act-council-gives-final-green-light-to-the-first-worldwide-rules-on-ai/, E.T.: 09.06.2024).

58 The European Parliament and the Council (2024), "*Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)* ", (https://data.consilium. europa.eu/doc/document/PE-24-2024-INIT/en/pdf, E.T.: 09.06.2024).

59 Uygulamaya dair tarihler için bkz. YZT m. 113.

- **02.02.2025:**
  - Genel düzenlemelere ilişkin I numaralı ve yasaklanmış uygulamalara ilişkin II numaralı bölümlerin uygulanmaya başlama tarihi.
- **02.05.2025:**
  - Genel amaçlı yapay zekâ modellerine ilişkin uygulama kurallarının (*codes of practice*) hazırlanmış olması için en son tarih.
- **02.08.2025:**
  - Onaylanmış kuruluşlara ilişkin III numaralı bölümün 4 numaralı kısmının; genel amaçlı yapay zekâ modellerine ilişkin V numaralı bölümün; yönetişim mekanizmalarına ilişkin VII numaralı bölümün; yaptırımlara ilişkin XII bölümün ve YZT'nin uygulanmasında etkili olan otoritelerin gizlilik yükümlülüğünü düzenleyen 78. maddenin uygulanmaya başlama tarihi.
  - Üye Devletlerin YZT uyarınca belirledikleri yetkili otoritelerin ve temas noktalarının elektronik ortamda kamuya açıklanması için son tarih.
  - Üye Devletlerin ulusal yetkili otoritelerin finansal ve insan gücü kaynaklarının durumuna dair ve her iki yılda bir tekrarlanacak olan ilk raporunun AB Komisyonuna bildirilmesi için son tarih.
  - Ciddi olaylara ilişkin yükümlülüklerle uyumun kolaylaştırılması için AB Komisyonu tarafından hazırlanacağı düzenlenen rehberin hazırlanması için son tarih.
- **02.02.2026:**
  - AB Komisyonu tarafından yüksek riskli yapay zekâ sınıflandırmasına ilişkin 6. maddenin uygulanmasına ilişkin ve yüksek riskli olan ve olmayan sistemlere dair detaylı örneklerin bulunduğu rehberin hazırlanması için son tarih.
  - AB Komisyonu tarafından piyasa sonrası gözetim planının şablonunu oluşturan ve planda yer alacak unsurları listeleyen ikincil düzenlemenin (*implementing act*) çıkarılması için son tarih.
- **02.08.2026:**
  - **Genel uygulanmaya başlama tarihi.**

- Üye Devletler bazında ulusal ölçekte en az bir düzenleme deneme alanının (*regulatory sandbox*) faaliyete geçirilmesi için son tarih.
- **Ayrıca,** yasaklanmış uygulamalara ilişkin düzenlemeler saklı kalmak kaydıyla YZT, bu tarihten önce piyasaya sürülen yüksek riskli yapay zekâ sistemlerinin operatörlerine ancak bu sistemlerin önemli değişikliğe uğraması durumunda uygulanacaktır. Diğer bir deyişle, YZT *kural olarak* bu tarihten önce piyasaya sürülen yüksek riskli yapay zekâ sistemlerine uygulanmayacaktır.

- **02.08.2027:**
  - Ek I'de sayılan AB düzenlemeleriyle bağlantılı olarak yüksek riskli sistem sınıflandırması yapan 6. maddenin birinci fıkrasının ve buna bağlı yükümlülüklerin uygulanmaya başlama tarihi.
  - 02.08.2025'ten önce piyasaya sunulmuş olan genel amaçlı yapay zekâ modellerinin sağlayıcılarının YZT'ye uyumu için son tarih.

- **02.08.2029:**
  - AB Komisyonu tarafından YZT ekinde yer alan yüksek riskli kullanım alanlarının değiştirilme ihtiyacı olup olmadığına ilişkin olarak yapılacak ve her dört yılda bir tekrarlanacak olan değerlendirmenin ilkinin AB Parlamentosu ve AB Konseyine raporlanması için son tarih.
  - AB Komisyonu tarafından yüksek riskli sistemler için getirilen yükümlülüklerin diğer sistemlere de uygulanmasını sağlamaya ilişkin isteğe bağlı kuralların (*voluntary codes of conduct*) etkisine ve verimliliğine ilişkin olarak yapılacak ve her üç yılda bir tekrarlanacak olan değerlendirmenin ilki için son tarih.
  - AB Komisyonu'nun, Yapay Zekâ Ofisinin işleyişini, görevlerini yerine getirebilmesi için yeterli yetki ve yetkinliklere sahip olup olmadığını ve bu YZT'nin düzgün bir şekilde uygulanması ve yürütülmesi için Yapay Zekâ Ofisinin yetkilerini güçlendirmenin ve kaynaklarını artırmanın uygun ve gerekli olup olmadığını değerlendirmesi için son tarih.
  - AB Komisyonu tarafından genel amaçlı yapay zekâ modellerinin enerji verimliliği gözetilerek geliştirilmesine yönelik standartlaştırma çalışmalarının gelişimine ve bağlayıcı önlemler veya eylemler dahil olmak üzere ek önlemler veya eylemler gerekip gerekmediğine

ilişkin olup AB Parlamentosu ile AB Konseyi' ne sunulacak olan ve her dört yılda bir tekrarlanacak olan raporun ilki için son tarih.

- **02.08.2029:** AB Komisyonu tarafından YZT'ye ilişkin olarak yapılacak ve her dört yılda bir tekrarlanacak olan değerlendirme ve gözden geçirmenin ilkinin AB Parlamentosu ve AB Konseyine raporlanması için son tarih.
- **02.08.2030:** Kamu otoriteleri tarafından kullanılmak üzere tasarlanan yüksek riskli yapay zekâ sistemlerinin sağlayıcıları ve yerleştiricilerinin, YZT'ye uyumu için son tarih.
- **31.12.2030:** Yasaklanmış sistemlere ilişkin yükümlülükler saklı kalmak kaydıyla, Ek X'te listelenen yasal düzenlemelerle kurulan büyük ölçekli bilişim teknolojileri sistemlerinin bir parçası olan ve 02.08.2027 tarihinden önce piyasaya sürülen veya hizmete sunulan yapay zekâ sistemlerinin YZT'ye uyumu için son tarih.
- **02.08.2031:** AB Komisyonu'nun, YZT'nin uygulanmasına ilişkin olarak yapacağı ve YZT'nin ilk yıllardaki uygulamasını dikkate alan değerlendirmeyi ve bu değerlendirmeye dair raporunu AB Parlamentosuna, AB Konseyine ve Avrupa Ekonomik ve Sosyal Komitesine sunması için son tarih.

Çalışmanın devamında YZT'nin kapsamı ve uygulanmasına dair bazı noktalarda açıklamalar yapılacak ve nihayet çalışma YZT'ye ilişkin bazı değerlendirmelerle sonuçlandırılacaktır.

B. YZT'NİN KAPSAMI

YZT'nin bir somut olayda uygulanması için üç olumlu bir olumsuz şartın bir arada bulunması gerekmektedir:

1. Bir yapay zekâ sistemi ya da genel amaçlı bir yapay zekâ modeli bulunmalıdır

YZT'nin uygulanması için ortada bir yapay zekâ sistemi veya bir genel amaçlı yapay zekâ modeli bulunmalıdır[60]. YZT, yüksek riskli yapay zekâ sistemlerini genel olarak tanımlarken ve tamamını belirli sınıflara ayırır-

[60] YZT kapsamındaki yapay zekâ sistemi ve genel amaçlı yapay zekâ modeli tanımları için bkz. yuk. Başlık III: *Bir Hukuki Düzenleme Nesnesi Olarak Yapay Zekâ*.

ken AI modelleri için farklı bir yaklaşım benimsemiş ve sadece genel amaçlı yapay zekâ modellerini tanımlamıştır. Genel amaçlı yapay zekâ modellerine dayalı yapay zekâ sistemleri ise YZT'de genel amaçlı yapay zekâ sistemleri olarak ifade edilmiştir.

YZT kapsam bakımından, daha sonra değinilecek istisnai düzenlemeleri saklı kalmak üzere, tüm yapay zekâ sistemlerine uygulanmakta ancak bunları kendi içerisinde belirli risk gruplarına ayırıp risk seviyesine göre yükümlülükler getirmektedir. Yapay zekâ modelleri bakımından ise genel amaçlı olmayan modellere ilişkin hiçbir düzenleme bulunmamakta sadece genel amaçlı modellere ilişkin özel düzenlemeler getirilmektedir.

YZT'nin bu yaklaşımı, bir düzenleme olma niteliği ile yakından ilgilidir. Yapay zekâ modellerinin piyasaya sürülmesi genel olarak YZT'nin odağına almaya çalıştığı bir husus değildir. YZT insan hakları referansları da bulunan ancak temel itibariyle piyasayı kontrol eden ve niteliği itibariyle ürün güvenliği düzenlemesi, doğası ağır basan bir düzenlemedir. Daha ileride değinileceği üzere düzenlemelerini de genelde sistemlerin piyasaya veya hizmete sunulması ile ilişkilendirmektedir. Genel amaçlı olmayan, özel işlemler gerçekleştirmek üzere geliştirilen yapay zekâ modelleri tek başına model olarak YZT'nin kontrol etmek istediği ölçekte etki doğuracak şekilde piyasaya sunulmamaktadır. Bir sisteme dönüştürüldüklerinde ise zaten yapay zekâ sistemi olarak YZT düzenlemelerine tabi olacaktır. Burada bir politika tercihi göze çarpmaktadır. YZT için regülasyon hedefi temelde yapay zekâ sistemleridir ve kural olarak yapay zekânın son kullanıcıya bir sistem olarak ulaşacağı öngörülmüş, regülatif darboğaz yapay zekâ sistemleri üzerinde yaratılmıştır.

Diğer yandan genel amaçlı yapay zekâ modelleri hem doğrudan model olarak piyasayı etkileyecek ticari modellere konu olmaları, hem de genel ve yüksek kapasiteli niteliklerinden kaynaklı birçok sistemin tabir-i caizse motorunu teşkil edecek olmaları sebebiyle doğrudan YZT'nin kapsamına alınmıştır. Belirtilmelidir ki YZT'nin sisteme ve modele ilişkin bu yaklaşım farkı bir sonraki başlıkta inceleneceği üzere başta operatörler olmak üzere birçok düzenleme noktasında karşımıza çıkmaktadır.

2. YZT kapsamında sayılan operatörlerden biri bulunmalıdır

YZT bir yapay zekâ sisteminin veya bir genel amaçlı yapay zekâ modelinin geliştirme ya da kullanım sürecine dahil olan herkesi hedef almamakta

sadece YZT'nin "operatör" olarak adlandırdığı ve belirli sayıda olan aktörlere özel yükümlülükler getirmektedir. YZT kapsamında altı farklı operatör bulunmaktadır. Bunlardan beş tanesi YZT m. 3'te açıkça tanımlanmıştır:

- Sağlayıcı (*provider*): "Sağlayıcı, bir yapay zekâ sistemini veya genel amaçlı bir yapay zekâ modelini geliştiren ya da geliştirilmiş bir yapay zekâ sistemini veya genel amaçlı bir yapay zekâ modelini kendi adı veya markası altında ücretli veya ücretsiz olarak piyasaya süren veya hizmete sunan gerçek veya tüzel kişi, kamu otoritesi, ajans veya diğer kurumları ifade eder"[61]. Sağlayıcının her durumda geliştirici olması gerekmez. Bu durum YZT'nin piyasa gözetimi rolüyle ve mevcut bir sistemi alıp kendi ismi ya da markası altında piyasaya süren kişiyi de sağlayıcı gibi yükümlülüklere tabi tutmasına ilişkin yaklaşımıyla da uyum içindedir.

- Yerleştirici (*deployer*)[62]: "Yerleştirici, kişisel olan ya da profesyonel olmayan kullanımlar hariç olmak üzere bir yapay zekâ sistemini kendi otoritesi altında kullanan gerçek veya tüzel kişi, kamu otoritesi, ajans veya diğer kurumları ifade eder"[63]. YZT'nin AB Komisyonu önerisinde aslında bu kavram yerine kullanıcı (*user*) kavramı yer almaktaydı. Kullanıcı, AB Parlamentosu'nun 14.06.2023 tarihli pozisyon metninde yerleştirici ile değiştirilmiş ve ortak metne de bu şekilde yansımıştır.

---

61 YZT m. 3(3). Tanımın İngilizce orijinal hali şu şekildedir: "*'Provider' means a natural or legal person, public authority, agency or other body that develops an AI system or a general-purpose AI model or that has an AI system or a general-purpose AI model developed and places it on the market or puts the AI system into service under its own name or trademark, whether for payment or free of charge*".

62 Yazılım anlamında kullanılan "*deployer*" kavramının yerleşik bir Türkçe karşılığı bulunmamaktadır. "*Deployer*" aslında bir anlamda kullanım gerçekleştirmektedir. Ancak "kullanıcı" olarak çevrilmesi son kullanıcılarla karışıklığa sebep olabileceği için çok isabetli olmayacaktır. Yazılımların veya sistemlerin "*deploy*" edilmesi aslında bir dağıtım anlamına da gelmektedir. Bu sebeple Türkçe karşılık olarak "dağıtıcı" kavramı da düşünebilir fakat bu da başka bir operatör olan "*distributor*" kavramıyla karışıklık yaratabilecek niteliktedir. *"Deploy"* kelimesi aynı zamanda başta savunma sanayi ekipmanı olmak üzere silah ve fiziksel teçhizatı konuşlandırmak anlamına da gelmektedir. Buradan hareketle olası bir diğer Türkçe ifade "*konuşlandırıcı/konuşlandıran*" olabilir. Ancak bu da fiziksel çağrışımı sebebiyle kanımızca tam olarak istenen anlamı karşılamamaktadır. Bunlara karşılık hem kullanımı ifade ettiği hem de son kullanıcıyla karışma riski taşımadığı için bu çalışmada "yerleştirici" kavramı tercih edilmiştir.

63 YZT m. 3(4). Tanımın İngilizce orijinal hali şu şekildedir: "*'deployer' means a natural or legal person, public authority, agency or other body using an AI system under its authority except where the AI system is used in the course of a personal non-professional activity*".

- Yetkili temsilci (*authorised representative*): "Yetkili temsilci, Birlik içerisinde yerleşik bulunan veya kurulmuş olan ve bir yapay zekâ sisteminin veya genel amaçlı bir yapay zekâ modelinin sağlayıcısından, bu Tüzük ile belirlenen yükümlülükleri ve prosedürleri kendi adına yerine getirmek ve yürütmek üzere yazılı bir yetki almış ve kabul etmiş olan gerçek veya tüzel kişiyi ifade eder"[64].

- İthalatçı (*importer*): "İthalatçı, Birlik içerisinde yerleşik bulunan veya kurulmuş olan ve üçüncü bir ülkede kurulmuş bir gerçek veya tüzel kişinin adını veya ticari markasını taşıyan bir yapay zekâ sistemini piyasaya süren gerçek veya tüzel kişiyi ifade eder"[65].

- Distribütör/dağıtıcı (*distributer*): "Distribütör, sağlayıcı veya ithalatçı dışında tedarik zincirinde yer alan ve Birlik pazarında bir yapay zekâ sistemini kullanıma sunan gerçek veya tüzel kişi anlamına gelir"[66].

YZT'de tanımlanmayan operatör ise ürün imalatçısıdır (*product manufacturer*). YZT kural olarak imalatçıya ilişkin doğrudan düzenleme yapmamakta, çoğunlukla atıf yaptığı AB ürün güvenliği ve sektörel düzenlemeler kapsamında kalan ürünlerin üreticileriyle sağlayıcı arasında bir ilişki kurmaktadır. Örneğin YZT m. 25(3)'te açıkça Ek I Bölüm A'da sayılan Birlik düzenlemeleri bakımından imalatçının belirli koşullarda yüksek riskli yapay zekâ sistem sağlayıcısı sayılacağı ve ilgili yükümlülüklere tabi olacağı düzenlenmiştir. Bu bölümde sayılan düzenlemelerin hepsinde ilgili ürünle bağlantılı olarak özelleştirilmiş bir imalatçı tanımı bulunmaktadır. Ancak genel olarak bu tanımların hepsi 13.12.2024 tarihiyle AB Genel Ürün Güvenliği Yönergesi'ni[67] yürürlükten kaldırarak uygulanmaya başlayan AB

---

64 YZT m. 3(5). Tanımın İngilizce orijinal hali şu şekildedir: "'*authorised representative' means a natural or legal person located or established in the Union who has received and accepted a written mandate from a provider of an AI system or a general-purpose AI model to, respectively, perform and carry out on its behalf the obligations and procedures established by this Regulation*".

65 YZT m. 3(6). Tanımın İngilizce orijinal hali şu şekildedir: "'*importer' means a natural or legal person located or established in the Union that places on the market an AI system that bears the name or trademark of a natural or legal person established in a third country*".

66 YZT m. 3(7). Tanımın İngilizce orijinal hali şu şekildedir: "'*distributor' means a natural or legal person in the supply chain, other than the provider or the importer, that makes an AI system available on the Union market*".

67 Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety, (https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32001L0095, E.T.: 09.6.2024).

Genel Ürün Güvenliği Tüzüğü'nde (**GPSR**)[68] yer alan tanımın varyasyonlarıdır. GPSR m. 3(8)'de ise imalatçı "bir ürünü imal eden veya bir ürünü tasarlayan ya da imal ettiren ve bu ürünü kendi adı veya ticari markası altında pazarlayan herhangi bir gerçek veya tüzel kişi"[69] olarak tanımlanmıştır.

YZT yapay zekâ sistemlerinin son kullanıcılarını da odağına yerleştirmemekte ve aktif yükümlülükler yüklememektedir. Ancak yapay zekâ sistemlerinden etkilenen kişilere ilişkin bazı düzenlemeler getirmiş ve önemli etki doğuran sistemlerdeki karar verme mekanizmasına ilişkin açıklama talep etme[70] gibi haklar tanımıştır.

3. İlgili operatörle bağlantılı olarak YZT'nin öngördüğü coğrafi uygulama şartlarından biri sağlanmalıdır.

YZT'nin uygulanması için üçüncü olumlu şart YZT'nin coğrafi uygulama kapsamına ilişkindir. Coğrafi uygulama kapsamı özellikle sağlayıcı ve yerleştirici için değişiklik göstermektedir. YZT m. 2 uyarınca YZT:

- Sağlayıcılardan:
    - Bir yapay zekâ sistemini ya da genel amaçlı yapay zekâ modelini Birlik içerisinde piyasaya veya hizmete sunanlara yerleşim yerlerinin Birlik içerisinde olup olmadığına bakılmaksızın tamamına[71];
    - Birlik içerisinde bulunmayan[72] ya da yerleşik olmayan ve sistemlerini Birlik içerisinde piyasaya ya da hizmete sunmayanlardan yapay zekâ sistemlerinin çıktıları Birlik içerisinde kullanılanlara[73];

---

68 Regulation (EU) 2023/988 of the European Parliament and of the Council of 10 May 2023 on general product safety, amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council and Directive (EU) 2020/1828 of the European Parliament and the Council, and repealing Directive 2001/95/EC of the European Parliament and of the Council and Council Directive 87/357/EEC, (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2023.135.01.0001.01.ENG&toc=OJ%3AL%3A2023%3A135%3ATOC, E.T.: 09.6.2024).

69 Tanımın İngilizce orijinal hali şu şekildedir: "'*manufacturer' means any natural or legal person who manufactures a product or has a product designed or manufactured, and markets that product under that person's name or trademark*".

70 YZT m. 86.

71 YZT m. 2(1)(a).

72 Buradaki bulunma (*located*) ifadesinden ne anlaşılması gerektiği tartışma konusudur. Bkz. Ebers/Hoch/Rosenkranz/Ruschemeier/Steinrötter, s. 591.

- Yerleştiricilerden:
    - Birlik içerisinde bulunan veya yerleşik olanların tamamına[74];
    - Birlik içerisinde bulunmayan ya da yerleşik olmayanlardan yapay zekâ sistemlerinin çıktıları Birlik içerisinde kullanılanlara uygulanır[75].

Sağlayıcı ve yerleştiriciye ek olarak etkilenen kişilerin, kendilerine YZT kapsamında tanınan imkânlardan yararlanabilmeleri için de Birlik içerisinde bulunma koşulu getirilmiştir[76].

4. YZT'nin istisnalarından biri uygulanmıyor olmalıdır

YZT'nin uygulanmasına ilişkin olumsuz şart ise YZT kapsamındaki istisnalardan birinin bulunmamasıdır. YZT m. 2'de YZT'nin uygulanmasına ilişkin bazı istisnalara yer verilmiştir. Bu istisnaların farklı gerekçeleri bulunmaktadır. Örneğin hâlihazırda yeknesak Birlik kurallarına tabi olan ürünler için getirilen istisna[77] aslında ilgili düzenlemelerdeki gereksinimlerin tekrarlanmamasını amaçlamaktadır. Özellikle ulusal güvenlik ve savunma sanayisine ilişkin istisnalar[78] ise temelde YZT'nin bir Birlik düzenlemesi olmasının ve Birlik seviyesinde bu konulara ilişkin düzenleme yapılamamasının sonucudur.

Bunlar haricinde özellikle uygulamada tartışma konusu olabilecek salt bilimsel araştırma ve geliştirme amacıyla piyasaya sunulan ve hem yapay zekâ sistemlerine hem de genel amaçlı yapay zekâ modellerine uygulanacak bir istisna söz konusudur[79]. Özellikle gelişmiş sistem ve modellerin ticarileştirme potansiyeli düşünüldüğünde hangi sistem ya da modellerin salt bilimsel araştırma ve geliştirme amacıyla geliştirilmiş kabul edileceği şu aşamada belirsiz olup zamanla uygulamada netleşecektir. Dibacede bu istisna YZT'nin yenilikleri destekleme ve AR-GE faaliyetlerine engel olma-

73 YZT m. 2(1)(c).
74 YZT m. 2(1)(b).
75 YZT m. 2(1)(c).
76 YZT m. 2(1)(g).
77 YZT m. 2(2).
78 YZT m. 2(3).
79 YZT m. 2(5).

ma amacıyla ilişkilendirilmiştir[80]. Bu amaçla bağlantılı olan bir diğer istisna da YZT'nin piyasaya ya da hizmete sunulmadan önce model ya da sistemlerin geliştirilmesi, test edilmesi ve araştırılması için gerçekleştirilen faaliyetlere ilişkindir[81]. Ancak gerçek dünyada test edilmeye ilişkin hususlar bu istisnanın kapsamı dışındadır.

YZT, aynı zamanda gerçek kişiler tarafından tamamen kişisel olan ve profesyonel olmayan amaçlar için yapılan kullanımları da yerleştiricilerin yükümlülüklerine ilişkin düzenlemeler bakımından kapsam dışında tutmaktadır[82]. Yukarıda belirtildiği üzere bu tür kullanımlar tanım gereği kullanan kişinin yerleştirici olarak nitelendirilmesini engelleyeceği için bu aslında ayrıca düzenlenmesine gerek olmayan bir istisnadır. Ancak hem kapsam maddesinde hem de yerleştiricinin tanımında açıkça bu hususun vurgulanması YZT'nin bireysel kullanımları kapsamayı amaçlamadığı yönündeki net duruşunun bir göstergesi olarak okunabilir.

Uygulamada önem arz edebilecek bir diğer ve bu başlık altında değineceğimiz son istisna ise ücretsiz ve açık kaynak lisanslarıyla erişime sunulmuş olan sistemlere ilişkindir. YZT, bu şekilde sunulan sistemlere yüksek riskli veya şeffaflık yükümlülüğüne tabi bir yapay zekâ sistemi olarak piyasaya sunulmadıkları sürece uygulanmayacaktır[83]. YZT m. 2'de yer alan bu istisna sadece yapay zekâ sistemlerini kapsayacak şekilde yazılmıştır. Ancak benzer bir düzenleme genel amaçlı yapay zekâ modelleri için de YZT'de ayrıca düzenlenmiştir. Genel amaçlı yapay zekâ model sağlayıcıları için öngörülen yükümlülüklerin bazılarının açıkça modele erişim, kullanım, değiştirme ve dağıtım izni veren ücretsiz ve açık kaynak bir lisans altında yayımlanan ve parametreleri, ağırlıkları, model mimarisi bilgileri ve model kullanımı ile ilgili bilgileri kamuya açık olan yapay zekâ modellerinin sağlayıcıları için uygulanmayacağı düzenlenmiştir[84]. Sistemlere ilişkin istisna-

80 Dibace, para. 25.

81 YZT m. 2(8).

82 YZT m. 2(10).

83 YZT m. 2(12). Bu istisnanın uygulanıp uygulanmadığının tespit edilebilmesi için öncelikle sanki YZT uygulanıyormuş gibi sistem bakımından risk sınıflandırmasına ve YZT m. 50'de yer alan işleve dayalı şeffaflık yükümlülüklerine dair inceleme yapılması gerekecek ve bunların her ikisi bakımından da kapsam dışı kalınıyorsa istisnanın uygulanacağı sonucuna ulaşılması gerekecektir.

84 YZT m. 53(2). Bu istisnanın kötüye kullanım risklerine kapı araladığı yönünde bkz. Arda, S.:*Taxonomy to Regulation: A (Geo)Political Taxonomy for AI Risks and Regulatory*

ya benzer olarak bu istisnanın da istisnası öngörülmüş ve sistemik risk taşıyan genel amaçlı yapay zekâ modeller kapsam dışı bırakılmıştır[85]. Benzer bir istisna genel amaçlı yapay zekâ modellerinin, yetkili temsilcilerine ilişkin yükümlükler için de ayrıca düzenlenmiştir[86].

Görüldüğü üzere YZT'nin istisnaları çoğunlukla açık uçlu olup somut olay bazında değerlendirme ve yorum yapılmasını gerektirmektedir. Dahası bu değerlendirmelerin bir kısmı doğrudan YZT'nin esasına ilişkin inceleme yapılmasını da gerektirebilecektir. Örneğin ücretsiz ve açık kaynak lisansına dayalı istisnanın uygulanması için yapay zekâ sisteminin ve genel amaçlı yapay zekâ modelinin analizinin yapılması; yapay zekâ sisteminin yüksek riskli veya şeffaflık yükümlülüğüne tabi olup olmadığının, genel amaçlı yapay zekâ modelinin ise sistemik risk taşıyıp taşımadığının tespit edilmesi gerekecektir.

C. YZT'NİN UYGULANMASI

1. YZT'nin Yapay Zekâ Sistemi ve Yapay Zekâ Modellerine Yaklaşımı

YZT ana regülatif hedef olarak geniş anlamda yapay zekâyı değil, yapay zekâ sistemlerini odağına almıştır. Düzenlemeler yapay zekâ sistemlerine, onların risk seviyelerine ve bu sistemlerin yaşam döngülerine dahil olacak kişilere göre belirlenmektedir. Kural olarak YZT yapay zekâ sistemlerinin yaşam döngüsünün tamamını regüle etmeyi amaçlamaktadır. Yapay zekâ sistemlerinin geliştirilmesi sürecine ilişkin bazı teknik gereksinimler öngörmekte, kullanılmalarına ilişkin ilgili operatörlere bazı yükümlülükler getirmekte, piyasaya veya hizmete sunulduğu süre içerisinde de sürekli gözetim mekanizması öngörmektedir.

Daha önce de belirtildiği üzere YZT yapay zekâ sistemleri ile yapay zekâ modelleri arasında da bir ayrım yapmaktadır. YZT'nin varsayımı, modellerin YZT tarafından konulan kurallara, bir sisteme dönüştürüldüğü zaman tabi olacağıdır. Regülatif bir tercih olarak YZT bir sisteme dönüşmeyen yapay zekâ modellerini kural olarak regüle etmemektedir. Bununla birlikte bazı modellerin kapasitesi ve kullanıcılara etkisi gibi sebeplerle sisteme dönüşmeden de regüle edilmesi öngörülmüştür. Bunlar da genel amaçlı

Measures in the EU AI Act, arXiV, 2024, (https://arxiv.org/abs/2404.11476, E.T.: 11.06.2024), s. 13-15.

85 YZT m. 53(2).

86 YZT m. 54(6).

yapay zekâ modelleridir. YZT sistematiğinde bir model sağlayıcısı veya bir yerleştirici tarafından bir yapay zekâ sistemine dönüştürüldüğünde otomatik olarak yapay zekâ sistemlerine tabi olacaktır. Bu mantığın doğal bir sonucu olarak genel amaçlı yapay zekâ modellerine ilişkin yükümlülükler kural olarak sağlayıcılar ve sağlayıcıların yetkili temsilcileri için öngörülmüştür.

Bu noktada sağlayıcılar yapay zekâ sistemleri ile genel amaçlı yapay zekâ modellerine ilişkin risk sınıflandırmasının ve yükümlülüklerin paralel şekilde işlediği vurgulanmalıdır. Örneğin bir geniş dil modelini geliştiren ve bunu bir internet arayüzüyle işe alım süreçlerinde kullanılmak üzere bir görüşme botu olarak hizmete sunan ama aynı zamanda modeli başkaları tarafından kullanılabilecek şekilde ayrıca da erişime sunan bir sağlayıcı hem arayüz üzerinden doğrudan hizmete sunulan yapay zekâ sisteminin sağlayıcısı olarak, hem görüşme botları doğrudan kullanıcıyla etkileşime geçtiği için özel şeffaflık yükümlülüğüne tabi yapay zekâ sisteminin sağlayıcı olarak, hem de geniş dil modelleri genel amaçlı yapay zekâ modellerini tipik örneği olduğundan bir genel amaçlı yapay zekâ modeli sağlayıcısı olarak belirli yükümlülüklere tabi olacaktır. Bu başlığın devamında yapay zekâ sistemleri ve genel amaçlı yapay zekâ modelleri için ayrı ayrı uygulamaya ilişkin temel hususlara değinilecektir. Ancak bu ayrım sadece tespiti kolaylaştırmak için yapılmakta olup, bunların bir arada uygulanabileceği unutulmamalıdır.

2. Yapay Zekâ Sistemleri Bakımından

a. Risk Temelli Yaklaşım

YZT'nin kapsama ilişkin analizi sonrasında uygulanacağı sonucuna ulaşılmışsa atılması gereken bir sonraki adım risk sınıflandırmasının yapılmasıdır. YZT risk temelli yaklaşımı (*risk-based approach*) benimsemektedir. Risk temelli yaklaşım genel olarak kural odaklı yaklaşımın (*rule-based approach*) karşısında konumlandırılan ve bir düzenlemenin uygulanmasını bir riskin varlığına bağlayan bir yaklaşımı ifade eder. Ancak belirtilmelidir ki YZT kapsamındaki risk temelli yaklaşım riskin tam anlamıyla aktörler ya da otoriteler tarafından olay bazında değerlendirildiği bir yaklaşım değildir. Daha ziyade YZT nelerin riskli olduğunu veya riskli kabul edildiğini önceden kendisi belirlemekte ve sadece çok küçük bir çerçevede operatörlere bu sınıflandırmanın dışında kaldığını ileri sürme fırsatı tanımaktadır.

YZT yapay zekâ sistemleri ve daha ileride ayrıca değinileceği üzere genel amaçlı yapay zekâ modelleri için farklı risk sınıflandırması benimsemektedir. YZT'nin getirdiği yükümlülükler ve yaptırımlar da doğrudan bu sınıflandırmayla ilişkilendirildiğinden YZT'nin doğru şekilde uygulanabilmesi için risk sınıflandırmasının özenli şekilde yapılması gerekmektedir.

YZT uyarınca yapay zekâ sistemleri üç ana gruptan birine dahil olabilir:

1) *Yasaklı uygulamalar gerçekleştiren yapay zekâ sistemleri:*

Bunlar YZT m. 5'te sayılan ve yasaklanmış uygulamalar olarak adlandırılan faaliyetleri gerçekleştiren yapay zekâ sistemleridir. Madde metninde açıkça kabul edilemez risklerden bahsetmese de Dibace'de belirtilen ve bu sistemlerin yasaklanmasına ilişkin gerekçeye dayanılarak bu sistemlere kabul edilemez risk (*unacceptable risk*) taşıyan yapay zekâ sistemleri denmektedir.

Mevcut metin itibariyle YZT m. 5'te yer alan yasaklanmış uygulamalar arasında bir kişinin veya grubun bilinçli bir karar verme yetilerini önemli ölçüde bozarak davranışlarını önemli ölçüde çarpıtmak amacıyla veya bu etkiye sahip olacak şekilde, aksi takdirde almayacakları bir kararı almalarına neden olarak, kendilerinin, başka bir kişinin veya bir grup kişinin önemli ölçüde zarar görmesine neden olan ya da makul bir şekilde zarar görme olasılığı bulunan bir karar almalarına yol açacak, bilinç düzeyinin ötesinde subliminal teknikler veya kasten manipülatif veya aldatıcı teknikler kullanılması; verilerin aslen üretildiği veya toplandığı durumla ilgisiz sosyal bağlamlarda gerçek kişi veya kişi gruplarına zarar verici veya olumsuz muamele yapılmasına veya gerçek kişi ve gruplarına sosyal davranışlarına veya bu davranışın niteliğine kıyasla haksız veya orantısız zarar verici veya olumsuz muamele yapılmasına yol açabilecek şekilde ve çıkarılan veya öngörülen kişisel veya kişilik özelliklerine dayalı olarak belirli bir süre boyunca değerlendirilmesi veya sınıflandırılması yoluyla bir sosyal derecelendirme yapılması, kolluk amacıyla kamuya açık alanlarda gerçek zamanlı biyometrik tanıma gerçekleştirilmesi ve işyerlerinde ya da eğitim-öğretim kurumlarında duygu tanıma gibi faaliyetler yer almaktadır.

YZT m. 5'te yer alan haller şekli olarak sınırlı sayıdadır. Ancak madde metninde yer alan ifadelere bakıldığında somut olay incelemesi gerektiren oldukça yoruma açık ifadelere yer verildiği görülmektedir. Bir yapay zekâ sisteminin YZT m. 5 uyarınca yasaklanmış bir faaliyet gerçekleştirip gerçekleştirmediği her somut olay özelinde ayrıca değerlendirilmelidir.

2) *Yüksek riskli yapay zekâ sistemleri:*

Yüksek riskli yapay zekâ sistemleri YZT'nin odağında yer alan sistemlerdir. Teknik gereksinimler ve yükümlülükler en temelde yüksek riskli yapay zekâ sistemleri için öngörülmüştür. Bir yüksek riskli yapay zekâ sisteminin yüksek riskli yapay zekâ sistemi olarak sınıflandırılması iki ihtimalde söz konusu olabilir:

a. İlk olarak YZT Ek-1'de listelenen AB düzenlemeleri kapsamında ürün veya bir ürünün güvenlik bileşeni olan ve bu listede tabi olduğu ilgili düzenleme uyarınca piyasaya ya da hizmete sunulması için üçüncü parti bir uyum değerlendirmesinden geçmesi gereken yüksek riskli yapay zekâ sistemleri yüksek riskli yapay zekâ sistemleridir[87].

b. İkinci ihtimal olarak ise YZT Ek-3'te yer alan alanlarda kullanılan yüksek riskli yapay zekâ sistemleri yüksek riskli yapay zekâ sistemleri olarak belirlenmiştir[88].

Ek-3'ün mevcut halinde alt kullanım senaryolarına ayrılan sekiz sektör yer almaktadır. Ancak yasaklanmış uygulamaların aksine AB Komisyonu'na belirli koşullarda bu kullanım senaryolarını değiştirme veya yenilerini ekleme yetkisi verilmiştir[89]. Mevcut metin itibariyle Ek-3'te yer alan yüksek riskli yapay zekâ kullanım alanları ve senaryoları şunlardır:

[87] YZT m. 6(1). Ek-1'de listelenen AB düzenlemeleri iki bölüme ayrılmaktadır. Bunlar arasındaki ayrımın temel kaynağı *New Legislative Framework* olarak adlandırılan yeni yaklaşıma tabi olup olmadıklarıdır. Yeni yaklaşım hakkında bilgi için ayrıca bkz. European Commission, "*New legislative framework*", (https://single-market-economy.ec.europa.eu/single-market/goods/new-legislative-framework_en, E.T.: 11.06.2024).

[88] YZT m. 6(2).

[89] YZT m. 7.

Tablo 1

YZT Ek-3'te yer alan yüksek riskli yapay zekâ kullanım alanları ve senaryoları

Kullanım Alanı	Kullanım Senaryoları
Biyometrik sistemler	1) Sadece bir kişinin söylediği kişi olup olmadığını doğrulamak için kullanılan sistemler haricinde uzaktan biyometrik tanıma sistemleri; 2) Hassas veya korunan nitelikler ya da bu niteliklerin çıkarımına dayalı özelliklere göre biyometrik kategorilendirme için kullanılmak üzere tasarlanmış yapay zekâ sistemleri; 3) Duygu tanıma ve tespiti için kullanılması amaçlanan yapay zekâ sistemleri.
Kritik altyapı	Kritik dijital altyapının, karayolu trafiğinin yönetimi ve işletilmesinde veya su, gaz, ısıtma ya da elektrik tedarikinde güvenlik bileşenleri olarak kullanılmak üzere tasarlanmış yapay zekâ sistemleri.
Öğrenim ve mesleki eğitim	1) Her seviyedeki öğrenim ve mesleki eğitim kurumlarına erişimi veya kabulü belirlemek ya da gerçek kişileri bu kurumlara yerleştirmek amacıyla kullanılmak üzere tasarlanmış yapay zekâ sistemleri; 2) Öğrenme sürecini yönlendirmek amacıyla kullanılan sonuçlar da dahil olmak üzere, öğrenme çıktılarını değerlendirmek amacıyla kullanılmak üzere tasarlanmış yapay zekâ sistemleri; 3) Bir bireyin alacağı veya erişebileceği uygun eğitim-öğrenim seviyesini değerlendirmek amacıyla her seviyedeki öğrenim ve mesleki eğitim kurumları bağlamında veya bu kurumlar içinde kullanılmak üzere tasarlanmış yapay zekâ sistemleri; 4) Her seviyedeki öğrenim ve mesleki eğitim kurumlarında, sınavlar sırasında öğrencilerin yasaklanmış davranışlarını izlemek ve tespit etmek amacıyla kullanılmak üzere tasarlanmış yapay zekâ sistemleri.
İstihdam, işçi yönetimi ve serbest mesleğe erişim	1) Gerçek kişilerin işe alınması veya seçilmesi amacıyla, özellikle hedeflenmiş iş ilanları yerleştirmek, iş başvurularını analiz etmek ve filtrelemek ve adayları değerlendirmek için kullanılmak üzere tasarlanmış yapay zekâ sistemleri; 2) İş ile ilgili ilişkilerin şartlarını etkileyen kararlar almak, iş ile ilgili sözleşme ilişkilerinin terfi veya sonlandırılması, bireysel davranış veya kişisel özelliklere dayalı görevlerin tahsisi ya da bu ilişkilerdeki kişilerin performans ve davranışlarını izlemek ve değerlendirmek amacıyla kullanılmak üzere tasarlanmış yapay zekâ sistemleri.
Zaruri özel hizmetler ile kamu hizmetlerine ve yardımlara	1) Kamu otoriteleri tarafından veya kamu otoriteleri adına, gerçek kişilerin sağlık hizmetleri de dahil olmak üzere temel kamu yardımları ve hizmetleri için uygunluğunu değerlendirmek, bu yardımları ve hizmetleri vermek, azaltmak, geri almak veya geri talep etmek amacıyla kullanılmak üzere tasarlanmış yapay zekâ sistemleri;

erişim ve bunlardan yararlanma	2) Mali dolandırıcılığı tespit etmek amacıyla kullanılan yapay zekâ sistemleri hariç olmak üzere gerçek kişilerin kredibilitesini değerlendirmek veya kredi notunu belirlemek amacıyla kullanılmak üzere tasarlanmış yapay zekâ sistemleri; 3) Gerçek kişilere yönelik olarak hayat ve sağlık sigortasında risk değerlendirmesi ve fiyatlandırma amacıyla kullanılmak üzere tasarlanmış yapay zekâ sistemleri; 4) Gerçek kişiler tarafından yapılan acil çağrıları değerlendirmek ve sınıflandırmak veya polis, itfaiyeciler ve tıbbi yardım dahil olmak üzere acil ilk müdahale hizmetlerinin sevk edilmesi ya da öncelik sıralamasının belirlenmesi ve acil sağlık hizmetleri hasta triyaj sistemleri için kullanılmak üzere tasarlanmış yapay zekâ sistemleri.
Kolluk faaliyetleri	1) Kolluk otoriteleri tarafından veya adına, ya da Birlik kurumları, organları, ofisleri veya ajansları tarafından kolluk otoritelerini desteklemek veya onların adına, bir gerçek kişinin suç mağduru olma riskini değerlendirmek amacıyla kullanılmak üzere tasarlanmış yapay zekâ sistemleri; 2) Kolluk otoriteleri tarafından veya adına ya da Birlik kurumları, organları, ofisleri veya ajansları tarafından kolluk otoritelerini desteklemek amacıyla poligraf veya benzeri araçlar olarak kullanılmak üzere tasarlanmış yapay zekâ sistemleri; 3) Kolluk otoriteleri tarafından veya adına ya da Birlik kurumları, organları, ofisleri veya ajansları tarafından kolluk otoritelerini desteklemek amacıyla suçların soruşturulması veya kovuşturulması sırasında delillerin güvenilirliğini değerlendirmek amacıyla kullanılmak üzere tasarlanmış yapay zekâ sistemleri; 4) Kolluk otoriteleri tarafından veya adına ya da Birlik kurumları, organları, ofisleri veya ajansları tarafından kolluk otoritelerini desteklemek amacıyla gerçek kişilerin veya grupların kişilik özelliklerini ve geçmiş suç davranışlarını değerlendirmek veya bir kişinin suç işleme veya tekrar suç işleme riskini değerlendirmek amacıyla kullanılmak üzere tasarlanmış yapay zekâ sistemleri; 5) Kolluk otoriteleri tarafından veya adına ya da Birlik kurumları, organları, ofisleri veya ajansları tarafından kanun uygulama otoritelerini desteklemek amacıyla, suçların tespiti, soruşturulması veya kovuşturulması sırasında gerçek kişilerin profil oluşturması amacıyla kullanılmak üzere tasarlanmış yapay zekâ sistemleri.
Göç, sığınma ve sınır kontrolü yönetimi	1) Yetkili kamu otoriteleri tarafından veya adına ya da Birlik kurumları, organları, ofisleri veya ajansları tarafından poligraf veya benzeri araçlar olarak kullanılmak üzere tasarlanmış yapay zekâ sistemleri; 2) Bir Üye Devletin topraklarına girmeyi amaçlayan veya girmiş olan bir gerçek kişinin oluşturduğu güvenlik riski, düzensiz göç riski veya sağlık riski gibi bir riski değerlendirmek amacıyla yetkili kamu otoriteleri tarafından veya adına ya da Birlik kurumları, organları, ofisleri veya ajansları tarafından kullanılmak üzere tasarlanmış yapay zekâ sistemleri;

	3) Yetkili kamu otoritelerine sığınma, vize veya oturma izni başvurularının incelenmesi ve başvuran gerçek kişilerin uygunluğuna ilişkin şikayetlerin değerlendirilmesi konusunda, delillerin güvenilirliğinin değerlendirilmesi dahil olmak üzere yardımcı olmak amacıyla yetkili kamu otoriteleri tarafından veya adına ya da Birlik kurumları, organları, ofisleri veya ajansları tarafından kullanılmak üzere tasarlanmış yapay zekâ sistemleri; 4) Seyahat belgelerinin doğrulanması hariç olmak üzere, göç, sığınma veya sınır kontrolü yönetimi bağlamında gerçek kişileri tespit etmek, tanımak veya kimliğini belirlemek amacıyla yetkili kamu otoriteleri tarafından veya adına ya da Birlik kurumları, organları, ofisleri veya ajansları tarafından kullanılmak üzere tasarlanmış yapay zekâ sistemleri.
Yargı süreçlerinin yönetimi ve demokratik süreçler	1) Yargı mercileri tarafından veya adına, bir yargı merciine, vakıaları ve hukuku araştırmada ve yorumlamada, hukuku belirli bir olaya uygulamada veya alternatif uyuşmazlık çözümünde benzer bir şekilde kullanılmak üzere tasarlanmış yapay zekâ sistemleri; 2) Gerçek kişilerin doğrudan maruz kalmadığı, siyasi kampanyaların idari veya lojistik açıdan organize edilmesi, optimize edilmesi veya yapılandırılması için kullanılan araçlar dahil olmamakla birlikte bir seçim veya referandum sonucunu veya gerçek kişilerin seçimlerde veya referandumlarda oy kullanma davranışını etkilemek amacıyla kullanılmak üzere tasarlanmış yapay zekâ sistemleri.

Ek-3'te yer alan sektörlerde ve sektörlere ilişkin kullanım senaryolarında kullanılan yüksek riskli yapay zekâ sistemleri kural olarak yüksek riskli yapay zekâ sistemi olarak sınıflandırılacaktır. Ancak YZT'de ayrıca Ek-3'te yer alan sistemlerden kişilerin sağlık, güvenlik ve temel haklarına yönelik önemli bir risk teşkil etmeyenlerin yüksek riskli yapay zekâ sistemi olarak sınıflandırılmayacağı düzenlenmiştir[90]. Sistemlerinin Ek-3 kapsamında kaldığı halde yüksek riskli yapay zekâ sistemi olmadığını düşünen sağlayıcıların ya da sağlayıcılar AB dışında ise yetkili temsilcilerinin ilgili sistemin piyasaya veya hizmete sunulmasından önce bu değerlendirmeyi belgelemesi ve YZT uyarınca oluşturulacak olan sicile sistemi kaydettirmesi gerekmektedir[91].

Ek-3'te yer alan sistemlerin hangi durumlarda sağlığa, güvenliğe ve temel haklara önemli risk teşkil edip etmediği kanımızca somut olay özelinde yapılacak bir değerlendirme ile belirlenmelidir. Zira YZT'de bu durumun sağlandı-

[90] YZT m. 6(3).

[91] YZT m. 6(4).

ğı varsayılan dört hal ilk bakışta sınırlı olmayacak bir ifade ile sayılmıştır. Diğer yandan YZT'nin yasalaşma sürecinde bu listenin aslında sınırlı sayıda olmak üzere oluşturulduğu da belirtilmiştir. Bu listeye göre şu hallerde ilgili yüksek riskli yapay zekâ sisteminin gerçek kişilerin sağlığına, güvenliğine ve temel haklarına önemli risk teşkil etmediği kabul edilecektir[92]:

- Yapay zekâ sisteminin basit prosedürel işlemleri gerçekleştirmek için kullanıldığı haller;
- Yapay zekâ sisteminin daha önce insan tarafından gerçekleştirilmiş bir işlemin sonucunu iyileştirmek için kullanıldığı haller;
- Yapay zekâ sisteminin karar alma kalıplarını veya önceki karar alma kalıplarından sapmaları tespit etmek amacıyla tasarlanmış olduğu, uygun bir insan incelemesi olmaksızın önceki insan değerlendirmesini değiştirme veya etkileme amacı taşımadığı haller;
- Yapay zekâ sisteminin, Ek-3'te listelenen kullanım senaryolarıyla ilgili bir değerlendirme öncesinde hazırlık işlemleri yapmak için kullanıldığı haller.

Diğer yandan istisnanın da istisnası olarak Ek-3'te yer alan bir sistem profilleme gerçekleştiriyorsa her durumda yüksek riskli kabul edilecektir.

3) *Diğer yapay zekâ sistemleri:*

YZT uyarınca yasaklanmış ya da yüksek riskli olmayan tüm sistemler bu risk sınıfına dahildir. Bu sistemler düşük, minimum, ya da sıfır riskli sistemler olarak da adlandırılmaktadır. YZT bunlara ilişkin bağlayıcı kurallar getirmemektedir.

Bu üç risk sınıflandırması (*yasaklanmış uygulamalar-yüksek riskli yapay zekâ sistemleri-diğer sistemler*) inhisari olup bir yüksek riskli yapay zekâ sisteminin bunlardan sadece bir tanesine dahil olması mümkündür. Ancak bu risk sınıflandırmasına ek olarak YZT bazı yüksek riskli yapay zekâ sistemlerini sadece işlevleri itibariyle ek şeffaflık yükümlülükleriyle özdeşleş-

[92] YZT'nin AB Komisyonu öneri versiyonunda da bu listede yer alan kullanımlar doğrudan yüksek riskli sayılmıştı. Ancak AB Parlamentosu'nun pozisyonunda bu kullanımların yüksek riskli olarak sınıflandırılması için ayrıca gerçek kişilerin sağlığına, güvenliğine ve temel haklarına yönelik önemli bir zarar riski taşımaları aranmıştı. Mevcut nihai metinde ise bu sistemlerin kural olarak yüksek riskli kabul edilmesi yaklaşımına geri dönülmüş ancak zarar riski taşımaması ihtimali sağlayıcının başvurabileceği ayrı bir mekanizma olarak öngörülmüştür.

tirmiştir. Bu hususu düzenleyen YZT m. 50'ye göre örneğin doğrudan gerçek kişilerle etkileşime geçen sistemlerde kişilerin bir yapay zekâ ile etkileşimde oldukları noktasında bilgilendirilmesi ya da içerik üreten sistemlerle ilgili olarak üretilen içeriklerde içeriğin yapay zekâ tarafından üretildiğinin belirtilmesi bir yükümlülük olarak öngörülmüştür. Bu yükümlülüklerle bağdaştırılan sistemler hatalı şekilde risk sınıflandırmasının bir parçasıymış gibi gösterilebilmekte ve aslında YZT'nin terminolojisinde olmamasına rağmen sınırlı riskli sistemler olarak adlandırılabilmektedir[93]. Ancak bu yükümlülükler risk sınıflandırmasıyla değil sistemin işleviyle ilgili olup yasaklanmamış tüm sistemler -hem yüksek riskli yapay zekâ sistemleri hem de diğer sistemler- için uygulanabilecektir.

Bir yapay zekâ sisteminin hangi risk sınıfında kaldığının tespiti o sistemle bağlantılı olarak YZT kapsamındaki geri kalan tüm yükümlülükleri, alınması gereken önlemleri ve olası yaptırımları etkilediğinden bu tespitin her somut olay özelinde özenle yapılması gerekmektedir. Bu noktada yanıltıcı sonuca ulaştıracak genel nitelikli çıkarımlardan da özellikle sakınılmalı ve YZT'nin sınıflandırma için getirdiği kurallara ve bu kurallar içerisindeki detaylara dikkat edilmelidir. Örneğin öğretide bir yazar tarafından ifade edildiğinin[94] aksine YZT genel olarak insan sağlığı ile ilgili durumlarda yapay zekâ sistemlerini yüksek riskli olarak değerlendirmemektedir. Sağlık sektöründe yapay zekâ sistemlerinin kullanımının bir görünümünü teşkil eden yapay zekâ destekli medikal cihazlar veya bu cihazlardaki sistemler sağlık alanında kullanıldıkları için değil medikal cihazlara ilişkin AB sektörel düzenlemeleri Ek-1'de yer alan ve harici uyum değerlendirmesi gerektiren düzenlemelerden olduğu için doğrudan yüksek riskli yapay zekâ sistemi olarak değerlendirilebilecektir. Sağlık hizmetlerine erişimde kullanılan sistemlerle acil müdahalede kullanılan sistemler ise

---

93 Bu durumun sebebi AB Komisyonu tarafından YZT'nin anlaşılmasını kolaylaştırmak için hazırlanan materyallerde bir piramit yapısının kullanılmasıdır. Örneğin bu çalışmanın yazım tarihi itibariyle de AB Komisyonu'nun YZT'ye ilişkin bilgilendirme sayfasında benzer bir piramit bulunmakta ve dört risk sınıfı göstermektedir. (European Commission: "*AI Act*", (https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai, E.T.:11.06.2024). Ancak bu sistemler metnin hiçbir versiyonunda açıkça sınırlı risk grubu olarak tanımlanmamış, tam tersine içeriğinde bazı değişiklikler olmakla birlikte baştan beri "şeffaflık yükümlülüğüne tabi bazı sistemler" olarak düzenlenmiştir. Bu itibarla doğrudan YZT'nin sınırlı riskli yapay zekâ sistemlerini bir risk grubu olarak gördüğüne dair ifadeler aslında isabetli değildir. Bu yönde örnek bir değerlendirme için bkz. Kağıtcıoğlu, M.: *Yapay Zekâ ve İdare Hukuku (Bugünden Geleceğe Yönelik Bir Değerlendirme),* Hacettepe Hukuk Fakültesi Dergisi, 2021, C. 11, S. 1, s. 144.

94 Diri, s. 12.

duruma göre Ek-3'te yer alan kullanım alanları sebebiyle yüksek riskli olabilecektir. Ancak gerçek kişilerin sağlığına dair önemli bir zarar riski barındırmıyor olmak bu aşamada da bir sistemin Ek-3'te yer alan kullanım senaryolarında yer almasına rağmen yüksek riskli olarak değerlendirilmemesi için yapılacak inceleme bakımından önem taşıyacaktır. Yine öğretide bir yazar tarafından ifade edilenin[95] aksine hukuk alanında kullanılan sistemlerin genellikle yüksek riskli yapay zekâ sistemi olarak sınıflandırılacağını söylemek mümkün değildir. Ek-3'te bu hususla ilgili yer alan kullanım senaryoları hukukta genel bir kullanımı değil en azından şu an için yargı mercileri tarafından yapılacak olan veya seçim sonuçlarını etkileyecek kullanımları kapsamaktadır.

b. Yükümlülüklerin Tespiti

Risk sınıflandırmasının pratik sonucu YZT kapsamında uygulanması gereken yükümlülükleri etkilemesidir. Eğer bir yüksek riskli yapay zekâ sistemi yasaklıysa Birlik içerisinde kullanılmaması gerektiğinden ek başka bir yükümlülük söz konusu olmayacaktır. Ne yasak ne de yüksek riskli olan diğer sistemler için ise YZT zorunlu bir rejim öngörmemektedir. Yüksek riskli yapay zekâ sistemleri için yükümlülükler ise yüksek riskli yapay zekâ sistemleri için ve işlevlerine bağlı olarak bazı sistemler için öngörülmüştür.

Yüksek riskli yapay zekâ sistemlerine ilişkin olarak operatörlerin en ağır grubu sağlayıcıya ait olmak üzere farklı yükümlülükleri mevcuttur. Yüksek riskli yapay zekâ sistemlerinin sağlayıcılarının yükümlülükleri genel olarak YZT m. 16'da düzenlenmiş olup bu yükümlülüklere ilişkin bazı detaylar ise YZT m. 17-20 arasında düzenlenmiştir. YZT m. 16 uyarınca sağlayıcıların yükümlülüklerinden bir tanesi de yüksek riskli yapay zekâ sistemlerinin YZT m. 8-15 arasında düzenlenen teknik gerekliliklere uygun olmasını temin etmektir. Bu noktada YZT yükümlülük (*obligation*) ve gereklilik (*requirement*) arasında bir ayrım yapmaktadır. Gereklilikler yüksek riskli yapay zekâ sisteminin geliştirilme sürecine ilişkin teknik detaylar olup sistemin bunlara uygunluğunu sağlamak sağlayıcının yükümlülüğüdür. Bunlara ek olarak sağlayıcıların yüksek riskli yapay zekâ sistemlerinin piyasaya ya da hizmete sunulmasından kullanım ömrünün sonuna kadar geçen sürede izlenmesini sağlayacak bir sistem kurması ve bir izleme planı hazırlaması da gerekmektedir[96]. Bu açıklamalar ışığında yüksek riskli yapay zekâ sistemlerinin sağlayıcılarına ilişkin yükümlülükler aşağıdaki şemayla özetlenebilir.

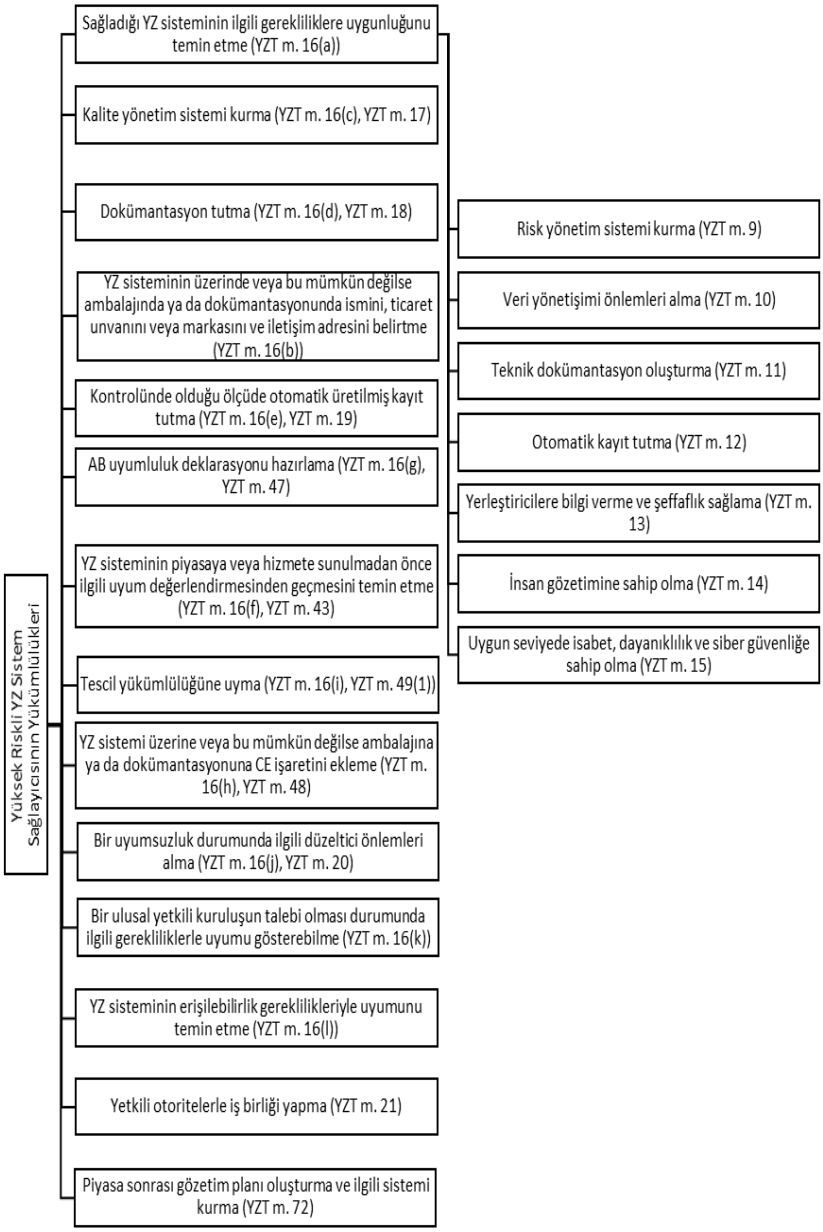
---

95 Görentaş/Çiftçi, s. 179.

96 YZT m. 72.

Şekil 2

YZT m. 16 kapsamında yüksek riskli yapay zekâ sistemi sağlayıcılarının yükümlülükleri



Sağlayıcılardan sonra en ağır yükümlülüklere sahip olan yerleştiricilerin yüksek riskli yapay zekâ sistemlerine ilişkin yükümlülükler YZT m. 26'da tek bir maddede sayılmıştır. Ayrıca özellikle yüksek riskli yapay zekâ sistemlerinin temel hak ve özgürlüklere etkisinin analizinde önemli bir rol oynayacak Temel Haklar Etki Değerlendirmesi (*Fundamental Rights Impact Assessment*) yapma yükümlülüğü de yine sadece belirli yerleştiriciler için öngörülmüştür[97].

Risk sınıflandırmasına dayalı yükümlülükler ötesinde sağlayıcılar ve yerleştiriciler için daha önce belirtildiği üzere yüksek riskli yapay zekâ sistemlerinin işlevleriyle bağlantılı olarak bazı şeffaflık yükümlülükleri de öngörülmüştür[98].

YZT m. 22-23-24 de sırasıyla yüksek riskli yapay zekâ sistemler için yetkili temsilcilerin, ithalatçıların, distribütörlerin ve yerleştiricilerin yükümlülüklerini düzenlemektedir. Bu operatörlerin yükümlülükleri sağlayıcılardan ve yerleştiricilerden farklı olarak genellikle bilgilendirme, koordinasyon ve doğrulama odaklıdır.

c. Uyum Değerlendirmesi ve Yaptırımlar

YZT'nin getirdiği yükümlülüklere uyumun denetimi için öngörülen en temel mekanizma uyum değerlendirmesidir (*conformity assessment*). Uyum değerlendirmesi AB ürün güvenliği mevzuatında YZT haricinde de mevcut olan ve kendine özel düzenlemesi de bulunan, bir düzenlemenin öngördüğü gerekliliklere uyumun incelendiği süreci ifade etmektedir. YZT kapsamında da uyum değerlendirmesi özellikle Kısım III Bölüm 2'de yer alan gerekliliklere uyumluluğun sağlanıp sağlanmadığının değerlendirilmesi olarak tanımlanmaktadır[99].

Uyum değerlendirmesinin yapılması yüksek riskli yapay zekâ sistemleri için bir zorunluluktur ve bunu yapmak YZT m. 16(f) uyarınca sağlayıcının yükümlülükleri arasındadır. Uyum değerlendirmesinin nasıl yapılacağı YZT m. 43'te düzenlenmiştir. YZT kapsamında biri sağlayıcının kendisi

97 YZT m. 27.

98 YZT m. 50

99 YZT m. 3(20).

tarafından dahili olarak yapılabilecek[100] diğeri ise harici bir onaylanmış kuruluşun (*notified body*) dahil olduğu[101] iki farklı tür uyum değerlendirmesi mümkündür. Bu iki uyum değerlendirmesi arasındaki temel fark ise onaylanmış kuruluşun dahil olduğu harici değerlendirme sonrasında bu değerlendirmeyi yapan kuruluşun bir sertifika düzenleyebiliyor olmasıdır[102].

Ek-3'te yer alan kullanım senaryolarından biyometri haricindekilerde sağlayıcılar için harici uyum değerlendirmesine gitmek zorunluluk değildir[103]. Biyometri alanındaki yüksek riskli yapay zekâ sistemlerinde ise uyum değerlendirmesinde bir kriter teşkil edecek olan yeknesak standartların veya ortak teknik özelliklerin her ikisinin de yayımlanmamış olması veya birinin yayımlanmış ancak sağlayıcı tarafından uyum sağlanmamış olması durumlarında harici uyum değerlendirmesinin yapılması zorunludur[104].

Bu noktada belirtilmesi gereken önemli bir husus bütün detaylı düzenleme görünümüne rağmen YZT'nin ifadelerinin aslında pratik açıdan çok net olmadığı ve uygulamadaki yeknesaklığın standartlar aracılığıyla sağlanmasının beklendiğidir. Yine belirtilmelidir ki sadece AB standardizasyon kuruluşları tarafından çıkarılan standartlar yeknesak standart statüsüne sahip olabilir. Ne kadar kapsamlı ya da yaygın olursa olsun, diğer standartlara, örneğin ISO 42005 ya da ISO 42006'ya uygunluk yeknesak standartlara uygunluğun getirdiği imkanlardan faydalanmak için yeterli olmayacaktır. Yeknesak standartların çıkarılması için AB Komisyonu tarafından üç AB standardizasyon kuruluşundan iki tanesi olan CEN ve CENELEC'e talepte bulunulmuş ve 30.04.2025'e kadar bu standartların hazır olması istenmiştir[105]. Standartlar tüm gereklilik ya da yükümlülükler için tek bir paket halinde değil, parça parça ve özellikle de YZT m. 9-15 arasında düzenlenen teknik gerekliliklerle bağlantılı olmak üzere farklı hususlarda ayrıca çıkarılacaktır.

---

100 Bu uyum değerlendirmesinin içeriğine ilişkin bilgiler YZT Ek-6'da yer almaktadır.

101 Bu uyum değerlendirmesinin içeriğine ilişkin bilgiler YZT Ek-7'de yer almaktadır.

102 Bu sertifikaya ilişkin detaylar YZT m. 44'te düzenlenmektedir.

103 YZT m. 43(2).

104 YZT m. 43(1).

105 European Commission (2023), "*Commission implementing decision on a standardisation request to the European Committee for Standardisation and the European Committee for Electrotechnical Standardisation in support of Union policy on artificial intelligence*", (https://ec.europa.eu/transparency/documents-register/detail?ref=C(2023)3215&lang=en, E.T.: 11.06.2024).

YZT tarafından yüksek riskli yapay zekâ sistemleri için öngörülen yükümlülüklere uygun davranmamanın yaptırımı ise idari para cezasıdır. Burada katmanlı bir yapı öngörülmüştür. Buna göre:

- YZT m. 5'te yer alan yasaklı sistemlere ilişkin düzenlemeleri ihlal etmenin yaptırımı 35.000.000 EUR'ya ya da bir teşebbüs söz konusu ise, bir önceki yıllık global mali bilanço toplamının %7'sinden yüksek olana kadar[106];
- YZT m. 16, 22, 23, 24, 26, 31, 33(1,3,4), 34 ve 50'de yer alan operatörlerin ve onaylamış kuruluşların yükümlülüklerine ilişkin düzenlemeleri ihlal etmenin yaptırımı 15.000.000 EUR'ya ya da bir teşebbüs söz konusu ise, bir önceki yıllık global mali bilanço toplamının %3'ünden yüksek olana kadar[107];
- Taleplerine cevap olarak onaylanmış kuruluşlara ya da ulusal yetkili otoritelere yanlış, yanıltıcı ya da eksik bilgi vermenin yaptırımı ise 7.500.000 EUR'ya ya da bir teşebbüs söz konusu ise, bir önceki yıllık global mali bilanço toplamının %1'inden yüksek olana kadar para cezasıdır[108].

KOBİ'ler için uygulanacak olan cezalarda bu tutar ya da yüzdelerden yüksek değil düşük olanlar dikkate alınır[109].

3. Genel Amaçlı Yapay Zekâ Modelleri Bakımından

Genel amaçlı yapay zekâ modelleri bakımından YZT'nin uygulanma aşamaları YZT'nin daha önce açıklanan model-sistem yaklaşımı sebebiyle yüksek riskli yapay zekâ sistemlerinden farklılaşmaktadır. Burada da bir risk sınıflandırması mevcuttur. Yerine getirilmesi gereken bazı yükümlülükler söz konusudur ancak yüksek riskli yapay zekâ sistemlerinde olduğu gibi bir teknik gereksinim seti ya da standart rejimi getirilmemiştir. Yükümlülüklerin ihlali halinde bazı yaptırımların uygulanması söz konusu olabilecektir. Ama genel amaçlı yapay zekâ modellerinin getirilen yükümlülüklere uyumunda bir uyum değerlendirmesi mekanizması öngörülmemiştir.

---

106 YZT m. 99(3).

107 YZT m. 99(4).

108 YZT m. 99(5).

109 YZT m. 99(6).

a. Genel Amaçlı Yapay Zekâ Modelleri ile İlgili Yükümlülükler

Öncelikle yüksek riskli yapay zekâ sistemlerindeki sınıflandırmanın aksine daha önce de belirtildiği gibi YZT genel olarak yapay zekâ modellerini düzenlemezken diğer yandan genel amaçlı yapay zekâ modellerinin tamamı için bir risk analizi yapılmadan doğrudan uygulanacak bazı yükümlülükler getirilmiştir. Bu yükümlülüklerin muhatabı kural olarak genel amaçlı yapay zekâ model sağlayıcısı ve eğer bu kişi AB dışındaysa da aynı zamanda yazılı bir yetkilendirmeyle atanacak olan[110] AB içerisinden yetkili temsilcisidir.

Genel amaçlı yapay zekâ model sağlayıcılarının dört temel yükümlülüğü bulunmaktadır:

- İlk yükümlülük teknik dokümantasyona ilişkindir. Yüksek riskli yapay zekâ sistemlerdekine benzer şekilde genel amaçlı yapay zekâ modeller için de bir teknik dokümantasyon oluşturulması gerekmektedir. Bu dokümantasyonun, eğitim ve test süreçleri ile değerlendirme sonuçlarını içerecek şekilde hazırlanması ve güncel tutulması, en azından Ek-11'de belirtilen bilgileri içermesi ve gerektiğinde AB Yapay Zekâ Ofisi ile ulusal yetkili makamlara sunmak üzere saklanması gerekmektedir[111].

- İkinci yükümlülük ise genel amaçlı yapay zekâ modeli kullanarak sistem oluşturmak ya da modeli kendi sistemlerine entegre etmek isteyen kişilere yönelik bir bilgilendirme dokümantasyonunun oluşturulmasıdır. Bu dokümantasyonun ise yine en az Ek-12'de yer alan bilgileri içerecek ve modeli entegre edecek sağlayıcılara modelin yetkinlikleri ile sınırları hakkında bilgi verip onlara yüksek riskli yapay zekâ sistemlerine ilişkin yükümlülüklerine uyum sağlamalarına imkân tanıyacak şekilde hazırlanması gerekmektedir[112].

- Üçüncü yükümlülük AB telif hakkı ile bağlantılı haklara ilişkin düzenlemelerle uyuma ve özellikle de veri madenciliğine ilişkin hakların takibine dair bir politikanın oluşturulmasıdır[113].

- Dördüncü ve son yükümlülük ise AB Yapay Zekâ Ofisi tarafından yayınlanacak şablona uygun olarak genel amaçlı yapay zekâ modelinin geliş-

110 YZT m. 54(1).

111 YZT m. 53(1)(a).

112 YZT m. 53(1)(b).

113 YZT m. 53(1)(c).

tirilmesi için kullanılan içeriklerin yeterince detaylandırılmış bir özetinin hazırlanması ve kamuya açık şekilde paylaşılmasıdır[114].

b. Sistemik Risk Taşıyan Genel Amaçlı Yapay Zekâ Modelleri ve İlgili Yükümlülükler

YZT genel amaçlı yapay zekâ modelleri için de daha dar kapsamlı bir risk temelli yaklaşım benimsemektedir. Özellikle etki ve kapasiteleri sebebiyle bazı modeller daha katı kurallara ve ek önlemlere tabi tutulmaktadır. Bunlar sistemik risk taşıyan genel amaçlı yapay zekâ modelleri olarak adlandırılmaktadır. Bir genel amaçlı yapay zekâ modelinin sistemik risk taşıyan genel amaçlı yapay zekâ olarak sınıflandırılması için uygun teknik araçlar, metodolojiler, göstergeler ve metriklere göre yüksek etki doğuracak yetkinliğe sahip olması ya da AB Komisyonu tarafından Ek-13'te yer alan kriterler de dikkate alınarak yüksek etki doğurabilecek denklikte etki ya da yetkinliğe sahip olduğu yönünde bir karar verilmesi gerekmektedir[115]. Ayrıca objektif bir eşik olarak geliştirilme sürecinde kullanılan toplam işlemci gücü 10^{25} FLOP'tan fazla olan genel amaçlı yapay zekâ modellerinin yüksek etki doğurabilecek yetkinliğe sahip olduğu yönünde bir varsayım getirilmiş[116]; ancak AB Komisyonu'na genel amaçlı yapay zekâ modellerinin sistemik risk taşıyıp taşımadığının tespitine dair bu kriterleri değiştirme yetkisi verilmiştir[117]. Mevcut haliyle bu GPT-4, Gemini gibi eşik az sayıda çok gelişmiş modeli kapsamaktadır[118].

Yüksek riskli yapay zekâ sistemlerindekine benzer şekilde burada da bir sistemik risk taşıyan genel amaçlı yapay zekâ modeli sağlayıcısına bu koşulların sağlandığı ile modelin karakteristik özellikleri sebebiyle sistemik bir risk teşkil etmediğini ileri sürme imkânı da tanınmıştır[119]. Yine yüksek riskli yapay zekâ sistemleri için getirilen sicilin kısmen benzeri bir işlev görecek şekilde AB Komisyonu'nun sistemik risk taşıyan genel amaçlı yapay zekâ modellerinin bir listesini tutacağı da düzenleme altına alınmıştır[120].

---

114 YZT m. 53(1)(d).

115 YZT m. 51(1).

116 YZT m. 51(2).

117 YZT m. 51(3).

118 European Commission (2023), "*Artificial Intelligence – Questions and Answers*", (https://ec.europa.eu/commission/presscorner/detail/en/qanda_21_1683, E.T.: 11.06.2024).

119 YZT m. 52(2).

120 YZT m. 52(6).

Yapay zekâ sistemlerinden farklı olarak genel amaçlı yapay zekâ modelleri ile sistemik risk taşıyan genel amaçlı yapay zekâ modellerine ilişkin yükümlülükler arasında da kümülatif bir ilerleme söz konusudur. Genel amaçlı yapay zekâ-SR modellerinin sağlayıcıları daha önce değinilen genel amaçlı yapay zekâ modellerinin sağlayıcılarına getirilen yükümlülüklere ek olarak dört yükümlülük daha getirilmiştir:

- Bu yükümlülüklerin ilki tekniğin bilinen durumunu yansıtan güncel prosedür ve araçlar kullanılarak ve modelin taşıdığı sistemik riskleri tespit etmek ve yönetmek amacıyla modelin test edilmesini de kapsayacak şekilde bir model analizi gerçekleştirmektir.
- İkinci yükümlülük modelin piyasaya sunulmasının ve kullanılmasının sebep olacağı sistemik risklerin AB genelinde değerlendirilmesi ve bu risklerin yönetilmesidir.
- Üçüncüsü, bir önemli olay meydana geldiği takdirde bunların ve bunlara yönelik alınacak düzeltici önlemlerin kaydının tutulması, dokümantasyonunun yapılması ve gecikme olmaksızın AB Yapay Zekâ Ofisi ile ilgili ulusal yetkili kuruluşlara bildirilmesidir.
- Son yükümlülük ise model ve modelin fiziksel altyapısı için yeterli siber güvenlik korumasının temin edilmesidir.

c. Genel Amaçlı Yapay Zekâ Modelleri ile İlgili Yükümlülüklere Uyum ve Yaptırımlar

Genel amaçlı yapay zekâ modelleri ile ilgili yükümlülükler için yüksek riskli yapay zekâ sistemlerindekine benzer bir uyum değerlendirmesi süreci öngörülmemiştir. Genel amaçlı yapay zekâ modelleri için getirilen yükümlülüklere uyumluluğun ise yine YZT uyarınca çıkarılacak olan uygulama rehberlerine (*codes of practice*) veya bu konuda bir AB yeknesak standardı çıkarılmış ise buna uyumluluk suretiyle gösterilebileceği düzenlenmiştir. Bir yeknesak standarda uygunluk, o standardın ilgili olduğu yükümlülüğün yerine getirildiği yönünde bir varsayım yaratmaktadır. Ancak bu standartlara uygunluk bir yükümlülük olarak öngörülmemiştir. Uygulama rehberlerine ya da mevcut yeknesak standartlara uygunluk sağlamayan sağlayıcıların da AB Komisyonu tarafından yapılacak değerlendirme için alternatif uyum tedbirlerini sağlayabileceği düzenlenmiştir[121].

[121] Bütün bu hususlar genel amaçlı yapay zekâ modelleri için YZT m. 53(4)'te, sistemik risk taşıyan genel amaçlı yapay zekâ modelleri için ise YZT m. 55(4)'te düzenlenmiştir.

Genel amaçlı yapay zekâ modellerine ilişkin yükümlülüklere uymamanın yaptırımında da yüksek riskli yapay zekâ sistemlerinden farklılaşma söz konusudur. Burada da yine yaptırım idari para cezası olarak düzenlenmiştir. AB Komisyonu, genel amaçlı yapay zekâ modeli sağlayıcılarının ilgili yükümlülüklere uymadığını tespit ettiği takdirde 15.000.000 EUR veya bir önceki yıl global mali bilanço toplamının %3'ünden yüksek olanını aşmamak koşuluyla idari para cezası uygulayabilecektir[122].

D. BİR REGÜLASYON ARACI OLARAK YZT'YE DAİR DEĞERLENDİRMELER

YZT getirdiği rejim ve olası etkileri sebebiyle şu anda dünyadaki en önemli hukuki yapay zekâ regülasyon aracı olarak düşünülebilir. Ancak YZT ile ilgili değerlendirme yapılırken unutulmaması gereken şey YZT'nin yapay zekâ regülasyonunu tamamen kapsayan bir araç olmadığıdır. YZT en temelde bir ürün güvenliği düzenlemesidir. Regülasyon konusu olarak yapay zekâ sistemlerini ve genel amaçlı yapay zekâ modellerini, regülasyon hedefi olarak ise bunların yaşam döngüsünde yer alan bazı aktörleri seçmiştir. Bu doğrultuda bir yapay zekâ sisteminin ya da genel amaçlı bir yapay zekâ modelinin geliştirilme sürecine, piyasaya ya da hizmete sunulmasına, sonrasındaki kullanımına dair bazı düzenlemeler ve gereklilikler getirmektedir. Ama temel odağı önleyici nitelikte olmaktır. Bir ihlal durumunda da zararın tazminine ilişkin rejim öngörmemekte, sadece idari para cezası uygulamaktadır.

YZT'nin bir ürün güvenliği düzenlemesi olarak kurgulanması ve sorumluluğa ilişkin bir rejim öngörmemesi de ayrıca eleştirilere konu olmuştur[123]. Benzer unsurlar barındırıyor gibi görünen oldukça yeni tarihli Colorado SB24-205 düzenlemesi yapay zekâyı tüketicinin korunması açısından düzenlemektedir. Bunun en temelde bir politika tercihi olduğu unutulmamalıdır[124]. YZT ile düzenlenmek istenen şey YZ sistemlerinin ve genel amaçlı

---

122 YZT m. 101.

123 Smuha, N.; Ahmed-Rengers, E.; Harkens, A.; Lı, W.; Maclaren, J.; Piselli, R./Yeung, K.: "*How the EU Can Achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act*", 2021, (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3899991, E.T.: 11.06.2024), s. 9 vd.

124 YZT m. 5'te yer alan yasaklanmış uygulamaların AB'deki haksız ticari uygulamalarla bağlantılı olduğu yönünde bir görüş için bkz. Goanta, C.: Regulatory Siblings: The Unfair Commercial Practices Directive Roots of the AI Act (ed. Graef, I ve Van Der Sloot, B.), "The Legal Consistency of Technology Regulation in Europe", 2024, s. 72 vd.

yapay zekâ modellerinin AB içerisinde yeknesak kurallara tabi şekilde geliştirilmesi ve piyasaya ya da hizmete sunulması olduğundan doğrudan tüketicinin refahını konu alan ve her bir kullanımın değerlendirilmesini gerektirecek, piyasa dinamiklerini ikincil öncelikte bırakan bir çerçevedense ürün güvenliği düzenlemesi olarak gelmesi hukuk tekniği açısından daha uygundur.

Dahası YZT kapsamında kalan yapay zekâ sistemleri ve genel amaçlı yapay zekâ modellerinin yaşam döngüsünde meydana gelebilecek ve ilgili olabilecek bazı hususları da açıkça ilgili diğer düzenlemelere bırakmaktadır. Bunların başında kişisel verilerin korunmasıyla ilgili olarak GVKT'ye yapılan atıflarla AB telif hakkı ve bağlantılı haklar düzenlemelerine yapılan atıflar gelmektedir. Bir yapay zekâ sistemi ya da genel amaçlı bir yapay zekâ modeli kişisel veri işliyorsa veya telif hakkıyla korunan bir eseri işliyorsa -ki gelişmiş sistem ve modeller için neredeyse her zaman bunlardan en az bir tanesinin işlenmesi söz konusudur- o zaman bu düzenlemelere bakılacaktır. Yine tüketicilerin korunmasına ilişkin düzenlemeler tüketiciyle temas ettikleri ölçüde yapay zekâ sistemleri ve ilgili operatörler bakımından da uygulanmaya devam edecektir. Özellikle GVKT kapsamında alınacak önlemlerle YZT kapsamında alınacak verilere ilişkin önlemlerin ne ölçüde örtüştüğü önemli bir pratik soru olarak karşımıza çıkmaktadır. Kural olarak bu iki düzenlemenin veriye ilişkin noktalarda bile hem veri türü hem de genel düzenleme amacı bakımından farklı hususları düzenlediği ve bu itibarla GVKT'ye uyumun tek başına YZT m. 10 başta olmak üzere YZT'nin veri yönetimine ilişkin yükümlülüklere uyum anlamına gelmeyeceği ve hatta yapay zekâ ile kişisel veri işleme faaliyetinin dahil edildiği durumlarda mevcut kişisel veri mevzuatına uyum durumunun bundan ek önlemlerin atılmasını gerektirecek ölçüde etkilenebileceği unutulmamalıdır.

YZT'nin ilk bakışta detaylı görünen teknik gerekliliklere, yükümlülüklere ve gözetime ilişkin düzenlemelerine rağmen nasıl uygulanacağına dair de önemli belirsizlikler mevcuttur. YZT'nin en çok tartışma konusu yapılan yüksek riskli yapay zekâ sistemleri için getirdiği gerekliliklerin sahada nasıl uygulanacağının belirlenmesi büyük oranda bu alanda çıkarılacak standartlara bırakılmıştır. Standartlar da kanun koyucular değil bu alanda uzmanlaşmış kişilerin çalıştığı standardizasyon kuruluşları tarafından hazırlanmaktadır. Diğer bir ifadeyle aslında en önemli risk grubunun en katı yükümlülüklerinin belirlenmesi, genel bir çerçeve çizildikten sonra

büyük ölçüde hukuki olmayan regülasyon araçlarına bırakılmıştır. Tabi ki tüm gereklilikler için bir teknik standart çıkarılması zorunlu değildir ancak çoğu için durum bu olacaktır. Dahası YZT, uyum değerlendirmesi için de bu standartlara dayanmakta ve ilgili oldukları ölçüde çıkarılan standartlara uygunluğun kendi getirdiği gerekliliklere uyum yönünde bir varsayım olarak değerlendirmektedir. Standartlar ile hukuki uyum arasındaki bu ilişki aslında teknolojiye doğrudan mutfağında, kodunda ama bunu aynı zamanda hukuk sisteminin verdiği otoriteyi de kullanarak regüle etme denemesinin güzel bir görünümüdür.

YZT'nin getirdiği yükümlülükler içerisinde önemli bir kısmı dokümantasyona ve bilgi vermeye ilişkindir. Bu bilgi ve belgelerin toplanmasının istenmesi ürün güvenliği düzenlemelerinin yabancı olduğu bir yaklaşım değildir. Ancak yapay zekâ özelinde sistemlerin yaygınlığı, karmaşıklığı ve kullanıcı sayıları düşünüldüğünde bir tercihten çok fiili bir gereklilik olarak ortaya çıkmaktadır. YZT'nin genel olarak yaklaşımı teknik standartlara uyumun gerekmesi, olabildiğince fazla bilgi ve belgenin dokümantasyonunun yapılmasıdır. Bir denetim, değerlendirme gerektiğinde ya da bir sorun çıktığında bu dokümantasyon temel alınacaktır, ki uyum değerlendirmesinin temelde kalite yönetim sistemi ve teknik dokümantasyon üzerinden yapılacağının öngörülmesi de bunun bir göstergesidir.

Diğer yandan bu bilgilendirme rejiminin işe yaraması için bilgilendirmenin yapıldığı hedef kitlenin bu bilgilendirmeyi anlamlı şekilde değerlendirebilecek bilgi birikimine sahip olması gerekmektedir. YZT m. 4 yapay zekâ okur yazarlığına ilişkin bir düzenlemeyle bu konuda önlemlerin alınması gerektiğini düzenlemektedir. Ancak bu tip düzenlemeler hukuki çerçeveye oturtmanın yeterli olmadığı düzenlemelerin tipik örneği olup bunun bir temenni olarak kalmaması için aktif adımların atılması gerekecektir. Dahası küçük bir detay olarak gözükmekle birlikte bu, okur-yazarlık seviyesinin düşük kaldığı durumlarda operatörler tarafından verilen bilgiler de düzenleyici otoriteler tarafından yapılan denetimler ve tedarik zincirinin dışındaki aktarımlar dışında doğrudan son kullanıcı ya da etkilenen kişiler tarafından tam olarak değerlendirilemeyeceğinden aslında YZT'nin bütün mimarisinin etkinliği azalacaktır.

YZT ile ilgili en çok bahsedilen bir diğer konuda Brüksel etkisinin de sebebiyle GVKT'nin kişisel verilerin korunması alanında olduğu gibi yapay zekâ alanında bir altın standart teşkil edip etmeyeceğidir. Bu noktada GVKT ile arada bir analoji kurulurken dikkatli olunmasında fayda vardır. GVKT'nin konusu neredeyse her teşebbüsün gerçekleştirdiği, gerçekleştirmek zo-

runda olduğu bir faaliyet olup kapsam itibariyle de AB içinde veya AB ile öngörülen şekillerde temas edecek şekilde tüm kişisel veri işleme faaliyetleri kapsama alınarak devasa bir uygulama ölçeği yaratılmıştır. YZT de coğrafi uygulama alanı bakımından benzer düzenlemeler içermektedir. Ancak YZT'nin konusu bir teknolojik uygulama olup bunun nicel anlamda çok daha az muhatabı olmakla birlikte sosyo-ekonomik anlamda çok daha geniş ölçekli etkileri olabilecektir. Bununla bağlantılı olarak uyum maliyetlerinin etkisi de değişecektir. GVKT'ye uygun veri aktarımı ilk çıktığı dönemde veri sorumlularını korkutmuş olsa da bugün geldiğimiz nokta itibariyle GVKT uyumu çoğu KOBİ için dahi erişilebilir bir hizmet halini almıştır. Ancak bir yapay zekâ sisteminin ya da genel amaçlı bir yapay zekâ modelinin gelişme sürecini önemli ölçüde etkileyecek teknik standartlar ve yükümlülükler maliyet sebebiyle doğrudan AB dışına taşınabilir. Konu ve ölçek farkı burada farklı bir eğilim görmemize sebep olabilir.

Henüz sayıları çok fazla olmasa da YZT'nin getirdiği yükümlülükler sebebiyle AB dışında yeniden konumlanmayı düşünen yapay zekâ geliştiriciler olduğu görülmektedir. Şu aşamada bunlar sadece planlamadan ibaret kalabilir. Ancak burada değinilmesinde fayda olabilecek bir diğer husus bazı yapay zekâ sistemlerinin ya da genel amaçlı yapay zekâ modellerinin YZT sebebiyle AB dışarısına çıkmasının bir regülasyon aracı olarak YZT'nin etkinliği bakımından ne anlama geldiğidir. YZT'nin AB içerisinde yapay zekâ ekosisteminin gelişmesini olumsuz etkilemek üzere getirilmediği açıktır. Ancak YZT'nin yasaklanan faaliyetlere girişen sistemler başta olmak üzere bazı yapay zekâ sistemlerini AB içerisinde istemediği de açıktır. Bu etkinin ne anlama geleceği ve uzun vadeli sonuçları detaylı bir analiz gerektirecektir. Ancak bazı sistem ve modellerin önünün kapatılıyor olmasının tek başına YZT'yi etkili olmayan veya teknolojiyi sekteye uğratan bir düzenleme haline getirmeyeceği, hatta etkiler doğru yönde ise bunun tam olarak amaçlanan şeylerden birinin gerçekleştirilmesi ve etkinlik göstergesi olabileceği unutulmamalıdır.

SONUÇ

Bu çalışmanın sui generis yapısı içerisinde öncelikle teknoloji regülasyonuna dair bazı genel açıklamalar yapılmış, sonra bir metodoloji önerilmiş, bunu takiben yapay zekânın bir hukuki düzenleme nesnesi olarak seçilmesine dair bazı değerlendirmeler yapıldıktan sonra da hâlihazırda bu alandaki en önemli hukuki düzenleme örneği olan YZT'ye ilişkin açıklamalara yer verilmiştir. Teknoloji regülasyonuna ilişkin açıklamalarla YZT arasındaki boşluk bir kopukluk değil bilinçli bırakılmış bir aralıktır. Kanımızca

bu boşluk Türkiye'nin şu an yapay zekâ regülasyonu konusunda bulunduğu yerden bakabileceği bir boşluktur. Türkiye'de yapay zekâ regülasyonu için atılacak adımlarda hem sistemli bir metodolojik çalışma yapılmalı, hem de hukuki ve ekonomik gerekçelerle YZT'nin getirdiği düzenlemeler ve YZT'nin olası etkileri göz önünde bulundurulmalıdır.

Yapay zekâ regülasyonu her ne kadar hukukçular tarafından bazı tarihi ve pratik gerekçelerle daha çok sahiplenilse de çok katmanlı ve çok disiplinli müdahale gerektiren bir alandır. Hukuki düzenleme ise hem devletin zorlayıcı gücünü ve yaptırım kanalını devreye soktuğu için hem de merkezi denetim ve sertifikasyon mekanizmaları oluşturduğu için bunun en göz önünde olan araçlarından biridir, ama her zaman en doğru araç olmayabilir. Bir hukuki müdahale yapılmadan önce, özellikle gerektirdiği zaman ve kaynak da düşünüldüğünde, bunun ne için yapıldığı, kimi ya da neyi hedef aldığı ve nasıl sonuçları olacağı dikkatlice değerlendirilmeli ve mevcut diğer regülasyon araçlarının uygunluğuyla birlikte incelendikten sonra bir hukuki müdahalenin gerekli olup olmadığına karar verilmelidir. Yeni bir teknoloji çıktığında sırf bu görünüşteki yenilik sebebiyle hemen hukuki düzenleme çağrısında bulunmak tehlikeli ve faydasından çok zararı olabilecek bir adımdır.

Bu aşamalar uzun bir süredir kat etmekte olan ve nihayetinde özellikle AB içi dinamikler sebebiyle böyle bir düzenlemenin gerekliği olduğuna karar vermiş olan AB de Nisan 2021'den beri bu düzenlemenin detayları üzerine çalışmaktadır ve nihayet Mayıs 2024'te metin nihai halini almış, 12.07.2024'te de AB Resmî Gazetesi'nde yayımlanmıştır. Ancak hukuki düzenlemeyi yapmak doğrudan etkin bir regülasyon yaratmak değil sadece bir adım atmak, bir araç oluşturmaktır. YZT için de durum çok farklı değildir. YZT niteliği itibariyle ürün güvenliği alanında görece kapsayıcı ve güzel bir sistem getirmektedir. Ama şimdi önemli olan bunun uygulanmasıdır ve YZT'nin aktif şekilde uygulanabilmesi için gereken hazırlıkların yapılması, mekanizmaların oluşturulması yıllar alabilecektir. YZT'nin maddelerinin neredeyse tamamının uygulanmaya başlaması yürürlüğe girme tarihinden itibaren 24 ay sonra gerçekleşecektir, ki bu arada da tam olarak bu sistem ve mekanizmaların oluşturulması ve hazırlıkların yapılması için çalışılacaktır. Bir regülasyon aracı olarak YZT'nin etkinliğinin değerlendirilmesi için henüz erkendir. Ancak Türkiye bakımından AB'nin hem hukuki hem de ekonomik önemi YZT'nin sınır aşan uygulamasıyla birlikte göz önünde bulundurulduğunda YZT'nin Türkiye üzerindeki etkileri üzerine çalışmaya başlamak için doğru zamanın şimdi olduğu da şüphesizdir.

KAYNAKÇA

A100 Standing Committee and Study Panel: "*One Hundred Year Study on Artificial Intelligence: Report of the 2015-2016 Study Panel*", (https://ai100.stanford.edu/2016-report, E.T.: 11.06.2024).

AKKURT, Sinan Sami: *Yapay Zekânın Otonom Davranışlarından Kaynaklanan Hukuki Sorumluluk*, Uyuşmazlık Mahkemesi Dergisi 2019, C. S. 13, 2019, s. 39-59.

ARDA, Sinan: *Taxonomy to Regulation: A (Geo)Political Taxonomy for AI Risks and Regulatory Measures in the EU AI Act,* arXiV, 2024, (https://arxiv.org/abs/2404.11476, E.T.: 11.06.2024).

BAK, Başak: *Medeni Hukuk Açısından Yapay Zekânın Hukuki Statüsü ve Yapay Zekâ Kullanımından Doğan Hukuki Sorumluluk*, Türkiye Adalet Akademisi Dergisi 2018, C. S. 35, 2018, s. 211-232.

BENNETT MOSES, Lyria: *How to Think about Law, Regulation and Technology: Problems with 'Technology' as a Regulatory Target,* Law, Innovation and Technology, 2013, C. 5, S. 1, s. 1-20.

BLACK, Julia: *Critical Reflections on Regulation,* Australian Journal of Legal Philosophy, 2002, C. 27, s. 1-35.

BOZKURT YÜKSEL, Armağan Ebru ve BAK, Başak: Futurist Hukuk, 2018.

CLARKE, Michael: Regulation The Social Control of Business between Law and Politics, New York 2000.

Council of Europe (2024), "*Framework Convention on Artificial Intelligence and Human Rights, Democracy, and the Rule of Law*", (https://rm.coe.int/1680afae3c, E.T.: 09.06.2024).

Council of Europe Newsroom (2024), "*Council of Europe adopts first international treaty on artificial intelligence*", (https://www.coe.int/en/web/portal/-/council-of-europe-adopts-first-international-treaty-on-artificial-intelligence, E.T.: 09.06.2024).

Council of the European Union (2024), "*Artificial intelligence (AI) act: Council gives final green light to the first worldwide rules on AI*", (https://www.consilium.europa.eu/en/press/press-releases/2024/05/21/artificial-intelligence-ai-act-council-gives-final-green-light-to-the-first-worldwide-rules-on-ai/, E.T.: 09.06.2024).

Council of the European Union (2022), "*Artificial Intelligence Act: Council calls for promoting safe AI that respects fundamental rights*", (https://www.consilium.europa.eu/en/press/press-releases/2022/12/06/artificial-intelligence-act-council-calls-for-promoting-safe-ai-that-respects-fundamental-rights/, E.T.: 09.06.2024).

Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety, (https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32001L0095, E.T.: 09.6.2024).

DİRİ, Feyza: *Yapay Zekâ Teknolojisi ve Beraberinde Getirdiklerinin Sağlık Hukuku Kapsamında Değerlendirilmesi,* Bilişim Hukuku Dergisi, 2024, C. 6, S. 1, s. 1-29.

DOST, Süleyman: *Yapay Zekâ ve Uluslararası Hukukun Geleceği,* Süleyman Demirel Üniversitesi Hukuk Fakültesi Dergisi, 2023, C. 13, S. 2, s. 1271-1318.

EBERS, Martin; HOCH, Veronica R.S..; ROSENKRANZ, Frank; RUSCHEMEIER, Hannah ve STEINRÖTTER, Björn: *The European Commission's Proposal for an Artificial Intelligence Act—A Critical Assessment by Members of the Robotics and AI Law Society (RAILS)***,** Multidisciplinary Scientific Journal, 2021, C. 4, S. 4, s. 589-603.

EDWARDS, Lilian: Ada Lovelace Institute (2022), "*The EU AI Act: a summary of its significance and scope*", (https://www.adalovelaceinstitute.org/wp-content/uploads/2022/04/Expert-explainer-The-EU-AI-Act-11-April-2022.pdf, E.T.: 11.06.2024).

ERDOĞAN, Gökhan: *Yapay Zekâ ve Hukukuna Genel Bir Bakış,* Adalet Dergisi, 2021, S. 66, s. 117-192.

EUR-Lex (2024), "*Regulation*", (https://eur-lex.europa.eu/EN/legal-content/glossary/regulation.html#:~:text=Regulations%20are%20legal%20acts%20defined,Union%20(EU)%20Member%20States., E.T.: 09.06.2024).

EUR-Lex (2024), "*Trilogue*", (https://eur-lex.europa.eu/EN/legal-content/glossary/trilogue.html, E.T.: 09.06.2024).

European Commission: "*AI Act*", (https://digital-strategy.ec.europa.eu/en/ policies/regulatory-framework-ai, E.T.:11.06.2024).

European Commission (2023), "*Commission implementing decision on a standardisation request to the European Committee for Standardisation and the European Committee for Electrotechnical Standardisation in support of Union policy on artificial intelligence*", (https://ec.europa.eu/transparency/documents-register/detail?ref=C(2023)3215&lang=en, E.T.: 11.06.2024).

European Commission (2023), "*Artificial Intelligence – Questions and Answers*", (https://ec.europa.eu/commission/presscorner/detail/en/qanda_21_1683, E.T.: 11.06.2024).

European Commission (2021), "*Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts*" (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021PC0206, E.T.: 09.06.2024).

European Parliament (2024), "*Provisional Agreement Resulting From Interinstitutional Negotiations*", (https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/CJ40/AG/2024/02-13/1296003EN.pdf, E.T.: 09.06.2024).

European Parliament (2023), "*Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts*", (https://www.europarl. europa.eu/doceo/document/TA-9-2023-0236_EN.html, E.T.: 09.06.2024).

European Parliament News (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, E.T.: 09.06.2024).

European Parliament News (2023), "*Artificial Intelligence Act: deal on comprehensive rules for trustworthy AI*", (https://www.europarl.europa.eu/news/en/press-room/20231206IPR15699/artificial-intelligence-act-deal-on-comprehensive-rules-for-trustworthy-ai, E.T.: 09.06.2024).

GOANTA, Catalina: Regulatory Siblings: The Unfair Commercial Practices Directive Roots of the AI Act (ed. Graef, I ve Van Der Sloot, B.), "The Legal Consistency of Technology Regulation in Europe", 2024, s. 71-88.

GÖRENTAŞ, Muhammed Burak ve ÇİFTÇİ, Hamza: Avrupa Birliği Yapay Zekâ Yasası Çerçevesinde Yargılamada Yapay Zekâ Kullanımının Değerlendirilmesi, İzmir Barosu Dergisi, 2024, S. 1, s. 177-203.

GÜÇLÜTÜRK, Osman Gazi: *ChatGPT ile Üretilen İçeriklerin Eser Niteliğinin 5846 sayılı Fikir ve Sanat Eserleri Kanunu Bakımından Değerlendirilmesi,* Galatasaray Üniversitesi Hukuk Fakültesi Dergisi, 2022, C. 2, s. 1899-1912.

GÜÇLÜTÜRK, Osman Gazi: Yapay Zekâve Verinin Kullanımı, İstanbul 2022 (Kısaltma: *Verinin Kullanımı*).

GÜÇLÜTÜRK, Osman Gazi ve CANKAT, Rifat: Güncel Gelişmeler Işığında Türk Hukukunda Kripto Varlıkların Hukuki Niteliği (ed. Aksoy Retornaz, E.E. ve Güçlütürk, O.G.), "Gelişen Teknolojiler ve Hukuk I: Blokzincir", Gözden Geçirilmiş ve Genişletilmiş 2.Bası, İstanbul 2021, s. 215-241.

HILLIARD, Airlie/ANAND Nikitha: HOLISTIC AI Blog (2024), "*10 Things You Need to Know about Colorado's SB205 Consumer Protections for Artificial Intelligence*", (https://www.holisticai.com/blog/colorado-sb-205-artificial-intelligence-consumer-protections, E.T.: 09.06.2024).

HILLIARD, Airlie: HOLISTIC AI Blog (2023), "What is New York City Local Law 144?", (https://www.holisticai.com/blog/new-nyc-local-law-144, E.T.: 09.06.2024).

KAĞITCIOĞLU, Mutlu: *Yapay Zekâ ve İdare Hukuku (Bugünden Geleceğe Yönelik Bir Değerlendirme),* Hacettepe Hukuk Fakültesi Dergisi, 2021, C. 11, S. 1, s. 118-168.

KANGAL Zeynel T.: Yapay Zekâ ve Ceza Hukuku, 2021.

KAPANCI, Kadir Berk: Özel Hukuk Perspektifinden Bir Değerlendirme: Yapay Zekâ ve Haksız Fiil Sorumluluğu, (ed. Aksoy Retornaz, E.E. ve Güçlütürk, O.G.), "Gelişen Teknolojiler ve Hukuk II: Yapay Zekâ", İstanbul 2021, s. 127-193.

KARACAN Pınar.; IRGIZ, Doğa.: Yapay Zekâ Kullanımı için Hukuksal Çerçeve İhtiyacı, LexPera Blog, 20.07.2023 (https://blog.lexpera.com.tr/yapay-zeka-kullanimi-icin-hukuksal-cerceve-ihtiyaci/, E.T.: 01.12.2024).

KOOPS, Bert-Jaap: Ten dimensions of technology regulation: Finding your bearings in the research space of an emerging discipline, (ed. Goodwin M.E.A., Koops, B.J. ve Leenes, R.E.), "Dimensions of Technology Regulation", Nijmegen 2010, s. 309-324.

KÜÇÜK, Emin Seyyid: *Yapay Zekâ Varlıkların Hukuki Statüsü Üzerine Disiplinler Arası Bir Muhakeme,* Bilişim Hukuku Dergisi, 2024, C. 6, S. 1, s. 1-7.

Los Angeles Times (2023), "AI is causing panic for authors. Now the courts are involved", (https://www.latimes.com/entertainment-arts/business/story/2023-10-20/authors-ai-lawsuits-douglas-preston-george-rr-martin-michael-connelly, E.T.: 09.06.2024).

MORGAN, Bronwen ve YEUNG Karen: An Introduction to Law and Regulation, 1. Baskı, Cambridge 2007.

MURRAY, Andrew: Information Technology Law – The Law and Society, 5. Baskı, Oxford 2023.

NIST (2023), "*AI Risk Management Framework*", (https://www.nist.gov/itl/ai-risk-management-framework, E.T.: 09.06.2024).

OECD: "*OECD Regulatory Compliance Cost Assessment Guidance*", (https://www.oecd-ilibrary.org/oecd-regulatory-compliance-cost-assessment-guidance_5jz78m5mpm0t.pdf, E.T.: 09.06.2024).

OECD (2019), "*Forty-two countries adopt new OECD Principles on Artificial Intelligence*", (https://www.oecd.org/science/forty-two-countries-adopt-new-oecd-principles-on-artificial-intelligence.htm, E.T.: 09.06.2024).

OECD Legal Instruments (2024), "*Recommendation of the Council on Artificial Intelligence*", (https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449, E.T.: 09.06.2024).

OECD Policy Observatory (2024), "*OECD AI Principles Overview*", (https://oecd.ai/en/ai-principles, E.T.: 09.06.2024).

PAPAKONSTANTINOU, Vagelis ve DE HERT, Paul: *The Regulation of Digital Technologies in the EU: The Law-Making Phenomena of 'Act-ification', 'GDPR Mimesis' and 'EU Law Brutality'*, SSRN 2022, (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4123313, E.T.: 09.06.2024).

POST, David G.: What Larry Doesn't Get: Code, Law, and Liberty in Cyberspace, Stanford Law Review, 2000, C. 52, s. 1439-1459.

Regulation (EU) 2023/988 of the European Parliament and of the Council of 10 May 2023 on general product safety, amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council and Directive (EU) 2020/1828 of the European Parliament and the Council, and repealing Directive 2001/95/EC of the European Parliament and of the Council and Council Directive 87/357/EEC, (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2023.135.01.0001.01.ENG&toc=OJ%3AL%3A2023%3A135%3ATOC, E.T.: 09.6.2024).

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), (https://eur-lex.europa.eu/eli/reg/2016/679/oj, E.T.: 09.06.2024).

Rest of World (2024), "OpenAI is making a risky bet on live translation", (https://restofworld.org/2024/exporter-openai-translation-gpt4o/, E.T.: 09.06.2024).

RUSSELL, Stuart; PERSET, Karine ve GROBELNIK, Marko: OECD AI Wonk Blog (2023), "*Updates to the OECD's definition of an AI system explained*", (https://oecd.ai/en/wonk/ai-system-definition-update, E.T.: 11.06.2024).

SMUHA, Nathalie; AHMED-RENGERS, Emma; HARKENS, Adam; LI, Wenlong; MACLAREN, James; PISELLI, Riccardo ve YEUNG, Karen: "*How the EU Can Achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act*", 2021, (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3899991, E.T.: 11.06.2024).

TDK (2024), "*TDK Güncel Türkçe Sözlük*", (sozluk.gov.tr, E.T.: 09.06.2024).

The European Parliament and the Council (2024), "*Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)* ", (https://data.consilium.europa.eu/doc/document/PE-24-2024-INIT/en/pdf, E.T.: 09.06.2024).

The White House (2023), "*Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*", (https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/, E.T.: 09.06.2024).

United Nations (2024), "*High-Level Advisory Body on Artificial Inteligence*", (https://www.un.org/techenvoy/ai-advisory-body, E.T.: 09.06.2024).

YÜNLÜ, Semih: *Üretici Yapay Zekâ Kaynaklı Norm ve Kişi Bazlı Hukuki Sorumluluk,* Adalet Dergisi, 2024, S. 72, s. 501-542.

YAPAY ZEKÂNIN YOL AÇTIĞI ZARARLARDAN HUKUKİ SORUMLULUK

Doç. Dr. Hüseyin Can AKSOY*

GİRİŞ

Yapay zekâ teknolojisinin hızla gelişmesi ve kullanım alanlarının çoğalması, kısa süre öncesine kadar var olmayan yeni hukuki sorunları da beraberinde getirmiştir. Kendi kendine öğrenebilen ve kararlar alabilen bu teknolojik sistemlerin kullanımının artmasıyla birlikte, özellikle bunların yol açacağı zararların kim ya da kimler tarafından tazmin edilmesi gerekeceği meselesi tartışılmaya başlanmıştır. Örneğin, bir otonom aracın kazaya sebep olması ve bir kişiyi yaralaması durumunda, zarar gören kişi zararının tazmini için kime ya da kimlere başvurabilecektir? Bir yapay zekâ tabanlı tıbbi tanı sisteminin bir hastaya yanlış teşhis koyması ve bu nedenle yanlış tedavi uygulanması durumunda hukuki sorumluluk kime ait olmalıdır? Mali danışmanlık hizmeti sunan bir yapay zekâ uygulamasının yanlış yatırım tavsiyesi vermesi durumunda, yatırımcıların zararlarını kim tazmin edecektir? Benzer şekilde, yapay zekâ destekli bir işe alım değerlendirmesinde, yapay zekâ sisteminin ırksal veya cinsiyet temelli ayrımcılık yapması ihtimalinde ortaya çıkacak zararların tazmini yapay zekâ sistemini geliştiren yazılımcıdan istenilebilecek midir?

Her ne kadar hukukçuların ilk refleksi yapay zekânın yol açtığı zararlara ilişkin sorumluluğu mevcut hukuki kurum ve ilkeler çerçevesinde belirlemeye çalışmak olmuş ise de[1] yapay zekânın yol açtığı zararlardan kimlerin hangi esaslar çerçevesinde sorumlu olacağı meselesini, geleneksel hukuk sistemlerinin mevcut kurum ve ilkeleri ile çözümleme gayretinin başarılı

* Bilkent Üniversitesi Hukuk Fakültesi Öğretim Üyesi. hcaksoy@bilkent.edu.tr

1 Bu konuda yapılan bazı çalışmalar için bkz. Sarı, O.: *Yapay Zekânın Sebep Olduğu Zararlardan Doğan Sorumluluk*, TBBD 2020, S.147, s.251-312; Čerka, P. / Grigienė, J. / Sirbikytė, G.: *Liability For Damages Caused By Artificial Intelligence*, Computer Law & Security Review 2015, C. 31, s. 376-389.

olduğu söylenemez. Bu nedenle, Avrupa Birliği'nde yapay zekânın yol açtığı zararların tazminine ilişkin özel düzenlemeler yapılması ve sorumluluğun esaslarının belirlenmesine karar verilmiştir.

Ülkemizde yapay zekânın yol açtığı zararlara ilişkin hukuki sorumluluğu ele alan özel bir yasal düzenleme mevcut değildir. Ancak yapay zekâ teknolojisinin gelişimiyle birlikte, hukuki sorumluluk ekseninde çok çeşitli sorunlar ortaya çıktığından, ülkemizde de yakın gelecekte bu alanda bir yasal düzenleme yapılmasını beklemek mümkündür. Bu bağlamda, kanun yapma sürecinde ülkemizin Avrupa Birliği düzenlemelerini yakından takip ettiği dikkate alındığında, ülkemizde yapılacak bir düzenlemenin konuya ilişkin Avrupa Birliği düzenlemelerini esas alması muhtemeldir. Bu nedenle, Avrupa Birliği'nde yapay zekâdan sorumluluğa ilişkin yapılan düzenlemeler de çalışmada ana hatlarıyla irdelenecektir.

I. YAPAY ZEKÂ SORUMLULUĞU VE HUKUKİ ÇERÇEVE

Kendi kendine öğrenebilen ve kararlar alabilen yapay zekâ sistemleri, günümüzde tıbbi teşhis ve tedaviden kredi başvurularının değerlendirilmesine, önleyici kolluk faaliyetlerinden sigorta primlerinin hesaplanmasına kadar çok çeşitli alanda ve giderek yaygınlaşan şekilde kullanılmaktadır. [2] Ancak bu sistemlerin hatalı kararları veya hukuka aykırı uygulamaları ile kişilere maddi ve manevi zararlar vermeleri durumunda, ortaya çıkan zararların tazmininden kimin ya da kimlerin hangi esaslar çerçevesinde sorumlu olacağı sorusu önemli bir hukuki tartışma konusudur. Aşağıda, öncelikle yapay zekânın temel özellikleri ve doğurduğu başlıca riskler ele alınacaktır.

A. YAPAY ZEKÂNIN TEMEL ÖZELLİKLERİ VE DOĞURDUĞU BAŞLICA RİSKLER

Hukuki sorumluluk ekseninde yapay zekâ teknolojisini ele alan hukukçuların bu konudaki ilk yaklaşımı, sorumluluğun esasını mevcut hukuki kurum ve kurallar içinde çözümlemeye çalışmak olmuş ise de bu gayretin başarılı olduğu söylenemez. Yapay zekânın yol açtığı zararlara ilişkin sorumluluğun, geleneksel hukuk sistemlerinin mevcut kurum ve ilkeleri ile çözümlenememiş olmasının en temel sebebi, aşağıda detaylıca ortaya konulacağı

[2] Aksoy, H.C.: *Kişisel Verilerin Korunması Yönüyle Algoritmik Karar Verme*, Kişisel Verileri Koruma Dergisi 2022, C. 4, S. 2, s. 73.

üzere, bu teknolojinin özellikleri ve doğurduğu risklerin şimdiye kadar aşina olduğumuz hiçbir sorumluluk kaynağı ile tam olarak benzeşmiyor olmasıdır. Bu nedenle, yapay zekâ sistemlerinin bir kimseye verdiği zararların kim tarafından, ne ölçüde ve hangi ilkeler çerçevesinde tazmin edilmesi gerektiğinin belirlenebilmesi için öncelikle bu teknolojinin başlıca özelliklerinin ve risklerinin irdelenmesi gerekir.

İlk olarak, yapay zekâ sistemlerinin otonom nitelikleri gereği kendi başlarına hareket etmeleri söz konusu olabilmektedir. Bunun anlamı, sistemin davranışlarının insanlar tarafından önceden tanımlanmamasıdır.[3] Yapay zekâ sistemleri onları üretenlerden ve kullananlardan bağımsız olarak hareket etme kabiliyetine sahip olmaları, bir yandan sistemin nasıl harekete edeceğini öngörmeyi güçleştirirken öte yandan bunların sebep oldukları zararları üreticilerine veya kullanıcılarına atfetmeyi de zorlaştırır. [4]

İkinci olarak, gelişmiş yapay zekâ sistemleri çok sayıda paydaşın katılımını ve farklı yapay zekâ bileşenlerinin birbirine entegre edilmesini gerektirir. Bu durum, yapay zekâ sisteminin arzu edildiği gibi çalışmamasının, sistemde kullanılan parçalardan hangisini üreten veya satan tarafa yüklenebileceğinin tespitini güçleştirir.[5]

Üçüncü olarak, yapay zekâ sistemleri opak olabilir. Bunun anlamı, kendi kendine karar alan sistemlerin bu kararları hangi sebeplerle aldığını anlama olasılığının sınırlı olmasıdır. [6] "Kara kutu etkisi" olarak da anılan bu durum nedeniyle, meydana gelme gelen "zarar" ile "yapay zekâ sisteminin ürettiği veya üretmeyi ihmal ettiği çıktı" arasındaki nedensellik bağının ortaya konması güçleşir.[7] Benzer şekilde bu durum, yapay zekânın zarar verici davranışına sebep olan, örneğini sistemi izleme ödevini ihmal eden gerçek kişinin davranışı ile zarar arasındaki nedensellik bağını tespit etmeyi de zorlaştırır. [8]

---

3 Borges, G.: *Liability for AI Systems Under Current and Future Law*, Computer Law Review International 2023, Vol. 24, No. 1, s. 2.

4 Buiten, M./ de Streel, A. / Peitz, M.: *The Law and Economics of AI Liability*, Computer Law & Security Review 2023, Vol. 48, s. 6.

5 Buiten/ de Streel / Peitz, s. 5.

6 Borges, s. 3.

7 Buiten/ de Streel / Peitz, s. 6.

8 Borges, s. 4.

Yapay zekâ sistemlerinin yukarıda sayılan bu özellikleri, yapay zekânın yol açtığı zararlara ilişkin sorumluluğun, geleneksel hukuk sistemlerinin mevcut kurum ve ilkeleri ile çözümlenememesine yol açtığı gibi hukuki sorumluluğa ilişkin olarak çözümlenmesi gereken kimi temel sorunları da beraberinde getirmiştir. Aşağıda, yapay zekâ sistemlerinin yol açtığı zararlardan hukuki sorumluluğa ilişkin temel sorunlar açıklanacaktır.

B. YAPAY ZEKÂNIN YOL AÇTIĞI ZARARLARDAN HUKUKİ SORUMLULUĞA İLİŞKİN TEMEL SORUNLAR

Yapay zekâ sistemlerinin yol açtığı zararlardan sorumluluğa ilişkin birçok mesele bulunmakla birlikte, iki husus ön plana çıkmaktadır. Bunlardan ilki, yapay zekâ sistemlerinin yol açtığı zararların tazmininden kimin veya kimlerin sorumlu olacağıdır. Gerçekten de yapay zekâdan kaynaklı bir zararın ortaya çıkması, bu sistemi geliştiren yazılımcının kusurundan veya bu sisteme veri sağlayan kişilerin hatalarından kaynaklanması mümkündür. Bu halde, yapay zekâyı geliştiren yazılımcının hatta bunu nihai kullanıcıya satan satıcının doğacak zararları tazmin etmesi gerekip gerekmeyeceği meselesi gündeme gelecektir. Keza, bir yapay zekâ sistemi kimsenin kusuru olmaksızın da bir başkasına zarar verebilir. Bu durumda yapay zekâ sistemini satın alan ve/veya kullanan kişinin bu sistemin yol açacağı zararları tazmin etmesi gerekeceği düşünülebilir. Özellikle tüm yapay zekâ sistemlerinin aynı şekilde öğrenmediği, bazılarının öğrenme sürecine bunları kullanan kişinin daha aktif katılımı olduğu dikkate alındığında, bu gibi hallerde kullanıcının sorumluluğunun belki de daha yüksek düzeyde olması gerektiği söylenilebilir. Hatta bu sistemi denetleyen kişilerin veya mevcut ise sigorta şirketlerinin sorumluluğu dahi gündeme gelebilir.

Yapay zekânın yol açtığı zararlardan sorumluluğa ilişkin ön plana çıkan meselelerden ikincisi ise sorumluluğun esasına ilişkindir. Hukuki yapay zekâ teknolojisini sorumluluk ekseninde ele alan hukukçular, ilk olarak yapay zekânın yol açacağı zararlardan doğan sorumluluğun hukukumuzdaki kusursuz sorumluluk halleri çerçevesinde ele alınıp alınamayacağı değerlendirilmiştir. Bu çerçevede, bu zararların tazmini bakımından adam çalıştıranın sorumluluğu, hayvan bulunduranın sorumluluğu, kölelerden doğan sorumluluk, tehlike sorumluluğu ve üreticinin sorumluluğu kurumlarına dayanılmasının mümkün olup olmadığı irdelenmiştir.[9] Ancak yıllar

[9] Bkz. Bak, B.: *Medeni Hukuk Açısından Yapay Zekânın Hukuki Statüsü ve Yapay Zekâ Kullanımından Doğan Hukuki Sorumluluk*, TAAD 2018, S. 35, s. 217 vd; Ercan, C.: *Robotların*

içerisinde yapılan tartışmaların da ortaya koyduğu üzere yapay zekâ teknolojisi tamamen kendine özgü ve yeni bir hukuki paradigma gerektirmektedir. Bu bağlamda, yapay zekâ tarafından ortaya çıkan zararların tazmini konusunda, geleneksel sorumluluk ilkelerinin yeniden düşünülmesi gerektiği gibi bu alanda yeni ve özel bir yasal düzenleme yapılması ihtiyacı söz konusudur. İşte bu nedenle 13 Mart 2024 tarihinde yapay zekâ konusunda dünyadaki ilk kapsamlı düzenleme olan Yapay Zekâ Yasası'nı kabul eden Avrupa Birliği'nde, bu yasayı tamamlar nitelikte olarak yapay zekânın yol açacağı zararlara ilişkin özel düzenleme yapılması yöntemi benimsenmiştir. Hatta, günümüzde pek taraftar bulamasa da Avrupa Parlamentosu Hukuki İşler Komisyonu tarafından 27 Ocak 2017 tarihinde yayınlanan robotik raporunda[10] uzun vadede yapay zekâ sistemlerine e-kişilik adı altında özel bir tür hukuki statü tanınması dahi önerilmiştir. [11] Aşağıda Avrupa Birliği'nin meseleye ilişkin düzenlemeleri olan Yapay Zekâ Yasası (AI Act)[12], Yapay Zekâ Sorumluluk Direktifi Taslağı ve (güncellenmiş haliyle) Ürün Sorumluluğu Direktifi Taslağı açıklanacaktır. [13]

Fiillerinden Doğan Hukuki Sorumluluk- Sözleşme Dışı Sorumluluk Hallerinde Çözüm Önerileri, TAAD 2019, S.40, s. 37 vd.

10 Bkz. European Parliament : "*Report A8-005/2017 with recommendations to the Commission on Civil Law Rules on Robotics*", (https://www.europarl.europa.eu/doceo/document/A-8-2017-0005_EN.html, E.T.: 11 Mayıs 2024).

11 Bu konuda bkz. Doğan, E.: *Dijital Çağda Yeni Bir Hukuki Kişilik Arayışı: Yapay Zekâ*, TBBD 2022, S. 158, s.213-254; Bak, s. 219 vd.

12 Aralık 2023'te Avrupa Parlamentosu ve Konsey tarafından üzerinde anlaşmaya varılan Yapay Zekâ Yasası, Avrupa Parlamentosu tarafından 13 Mart 2024 tarihinde resmen kabul edilmiştir. Yasa, Konsey'in de resmen kabul etmesi durumunda AB Resmî Gazetesi'nde yayımlanacak ve yayımından sonraki 36 ay içerisinde kademeli olarak uygulanmaya başlayacaktır.

13 Her iki metne ilişkin öneri de 28 Eylül 2022 tarihinde Avrupa Komisyonu tarafından yayınlanmıştır. Avrupa Parlamentosu ve Konsey, 14 Aralık 2023 tarihinde yeni ve güncellenmiş Ürün Sorumluluğu Direktifi üzerinde anlaşmaya varmıştır. Bu metin Avrupa Parlamentosu tarafından 12 Mart 2024 tarihinde resmi olarak kabul edilmiş olup Konsey'in de resmen kabul etmesi durumunda AB Resmî Gazetesi'nde yayımlanacak ve yayımından sonraki 24 ay içerisinde üye devletlerce iç hukuklarına aktarılarak uygulanmaya başlayacaktır. Buna karşılık, bu çalışmanın kaleme alındığı Mayıs 2024 tarihi itibarıyla Yapay Zekâ Sorumluluk Direktifi'ne ilişkin müzakere ve kabul süreci henüz devam etmektedir.

C. AVRUPA BİRLİĞİ'NDEKİ YAPAY ZEKÂ DÜZENLEMELERİ BAĞLAMINDA YAPAY ZEKÂNIN YOL AÇTIĞI ZARARLARDAN HUKUKİ SORUMLULUK

Avrupa Birliği'nde, yapay zekâ teknolojisinin kullanımını çeşitli yönleriyle ele alan üç farklı düzenleme mevcuttur: Yapay Zekâ Yasası, Yapay Zekâ Sorumluluk Direktifi Taslağı ve (güncellenmiş haliyle) Ürün Sorumluluğu Direktifi Taslağı. Aşağıda açıklanacağı üzere, bu düzenlemelerin üçü de yapay zekâ teknolojisinin farklı boyutlarını düzenlediğinden birbirlerini tamamlar niteliktedirler.

1. Yapay Zekâ Yasası

Yapay zekâ kullanımı, kişilerin yaşama hakkı ve fiziksel bütünlüğü ile ayrımcılığa maruz kalmama ve eşit muamele gibi bir dizi temel hakkını olumsuz yönde etkileyebilir. 13 Mart 2024 tarihinde kabul edilen Yapay Zekâ Yasası, esas itibarıyla yapay zekâ sistemlerinin güvenliği ve etik kullanımını düzenlemektedir. AB içinde yapay zekâ kullanımından kaynaklanan zararları önlemek için tasarlanmış olan bu yasa, yapay zekâ sağlayıcıları[14] veya kullanıcıları için geçerli olan düzenleyici çerçeveyi çizerek, kişilerin temel hak ve özgürlüklerine yönelik riskleri azaltmayı ve doğacak zararları önlemeyi hedeflemektedir.

Yapay Zekâ Yasası, yapay zekâ sistemlerinin ürettiği veya üretmeyi ihmal ettiği bir çıktı nedeniyle zarara uğrayan kişilere herhangi bir hukuki çözüm sunmaz. Bu konuları düzenlemek ve Yapay Zekâ Yasası'nı tamamlamak amacıyla Avrupa Komisyonu 28 Eylül 2022 tarihinde Yapay Zekâ Sorumluluk Direktifi ve güncellenmiş Ürün Sorumluluğu Direktifi taslaklarını yayınlamıştır. Kabul edilerek yürürlüğe girmeleri halinde, bu iki Direktif yapay zekâ sistemlerinin kullanımından doğan zararların tazminine ilişkin esasları belirleyecektir. Bu konudaki hukuki açıklık, bir yandan son kullanıcıların bu teknolojilere olan güvenini arttırırken diğer yandan yapay zekâ sistemlerini tasarlayan, pazarlayan ve kullanan teşebbüslerin, bu sis-

[14] "Sağlayıcı" kavramı Yapay Zekâ Yasası m. 3(3)'te tanımlanmıştır. Buna göre, sağlayıcı ücretli veya ücretsiz olarak bir yapay zekâ sistemi veya genel amaçlı bir yapay zekâ modeli geliştiren veya bir yapay zekâ sistemi veya genel amaçlı bir yapay zekâ modeline sahip olup bunu piyasaya süren ya da yapay zekâ sistemini kendi adı veya ticari markası altında hizmete sunan gerçek veya tüzel kişi, kamu kurumu, ajans veya başka bir kuruluş anlamına gelir.

temlerden kaynaklı zararlara ilişkin hukuki riskleri ve sorumluluklarının çerçevesini açık şekilde bilebilmelerini sağlayacaktır. [15]

2. Yapay Zekâ Sorumluluk Direktifi Taslağı

Yapay Zekâ Yasası, yapay zekâ sistemlerinin yol açtığı zararların tazmini meselesini düzenlemediğinden, bu konuda henüz taslak niteliğinde olan Yapay Zekâ Sorumluluk Direktifi[16] kaleme alınmıştır. Bu Direktif Yapay Zekâ Yasası'nın bir parçası olarak kabul edilmekte olup bir yapay zekâ sisteminin sebep olduğu zararlar ile bir yapay zekâ sisteminin belirli bir çıktıyı üretmemesi nedeniyle ortaya çıkan zararların tazminini konu edinmektedir.

Yapay Zekâ Sorumluluk Direktifi, zararın meydana geldiği durumlarda tazminata erişimin önündeki engelleri kaldırmaya yönelik *kusura dayalı sözleşme dışı sorumluluk* mekanizmasını konu alır. Ancak Direktif bütünsel bir sorumluluk rejimi ortaya koymayıp Direktif'te yer alan düzenlemeler iki temel usulî meseleye ilişkindir: (i) zarar görenlerin delillere erişme hakkı ve (ii) nedensellik bağı karinesi.

a. Zarar Görenin Delillere Erişme Hakkı

Yapay Zekâ Sorumluluk Direktifi'nin düzenlediği ilk usulî mesele, zarar gören potansiyel bir davacının uğradığı zararı ispatlaması bakımından ihtiyaç duyduğu; fakat karşı tarafın hakimiyetinde bulunan delillere erişme kabiliyeti ile ilgilidir. Direktif'e göre, ulusal mahkemeler, *yüksek riskli* yapay zekâ sistemi nedeniyle zarara uğrayanların talebi halinde, sistem sağlayıcıları veya kullanıcılarının, zarara uğrayanların iddialarını ispatlamaları bakımından gerekli belgeleri açıklamalarını emredebilir.[17]

Zarara neden olduğundan şüphelenilen yüksek riskli yapay zekâ sistemlerine ilişkin delillere erişim hakkının tanınması, zarar gören kişinin hem

---

15 Launders, J. (2024), *Beyond the AI Act: The AI Liability Directive & the Product Liability Directive*, (https://www.techlaw.ie/2024/03/articles/artificial-intelligence/beyond-the-ai-act-how-the-ai-liability-directive-and-the-product-liability-directive-will-also-shape-the-regulation-of-ai-in-the-eu/, E.T.: 11 Mayıs 2024).

16 Bkz. Eur-Lex: "*Proposal for a Directive of the European Parliament and of the Council on Adapting Non-Contractual Civil Liability Rules To Artificial Intelligence (AI Liability Directive)*", (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0496, E.T.: 11 Mayıs 2024).

17 Yapay Zekâ Sorumluluk Direktifi Taslağı m. 3 (1).

tazminat talep edip etmeme kararını vermesi hem de zararını kanıtlayarak bu zararın tazminini sağlayabilmesi bakımından önemli bir araçtır. Bununla birlikte, mahkemenin emri üzerine delilleri sunma yükümlülüğünün yerine getirilmesi, potansiyel davacıların iddialarını kanıtlayabilmeleri bakımından önemli olduğu kadar bu yükümlülüğü yerine getirmeyenler bakımından da önemli sonuçlar doğurur. Zira mahkeme kararına rağmen bu yükümlülüğün yerine getirilmemesi, ilgili sağlayıcı veya kullanıcının özen yükümlülüklerini ihlal ettiklerine dair-aksi ispatlanabilir- karine oluşturur.[18]

Bir ulusal mahkemenin zarar görenin erişim talebini kabul etmesi için belirli koşulların sağlanması gereklidir. Bu türden bir açıklama kararı verilebilmesi, yalnızca (i) davacının tazminat talebinin makullüğünü desteklemek için gerekli olgu ve kanıtları sunması, (ii) mahkemeye başvurmadan önce söz konusu delillere erişim bakımından sağlayıcı veya kullanıcıya başvurmuş olması; fakat (iii) bu taleplerinin kabul edilmemiş olması şartlarının yığışmalı olarak sağlanması halinde mümkündür. [19] Ayrıca, bu süreçte tüm tarafların meşru menfaatleri dikkate alınmalı ve yalnızca olası bir iddiayı veya tazminat talebini desteklemek için gerekli ve orantılı olan delillerin açıklanmasına hükmedilmelidir. Bununla birlikte, paylaşılmasına hükmedilen delillerin ticari sır veya gizli bilgi niteliğinde olması halinde, ulusal mahkemeler, taraflardan birinin gerekçeli talebi üzerine veya kendi inisiyatifleriyle, dava sürecinde kullanılan delillerin gizliliğin korunması için gerekli özel tedbirleri alma yetkisine sahiptir. [20]

b. Nedensellik Bağı Karinesi

Yapay Zekâ Sorumluluk Direktifi'nin düzenlediği ikinci usulî mesele bir yapay zekâ sisteminin yol açtığı zararın (ortaya koyduğu veya ortaya koymayı ihmal ettiği çıktının), bunları sağlayan veya kullanan kişilerin üzerlerine düşen özen yükümlülüğünü yerine getirmemiş olmalarından kaynaklandığına dair aksi ispatlanabilir[21] bir karinenin getirilmiş olmasıdır. [22]

---

18 Yapay Zekâ Sorumluluk Direktifi Taslağı m. 3 (5).

19 Yapay Zekâ Sorumluluk Direktifi Taslağı m. 3 (1).

20 Yapay Zekâ Sorumluluk Direktifi Taslağı m. 3 (4).

21 Yapay Zekâ Sorumluluk Direktifi Taslağı m. 4 (7).

22 Yapay Zekâ Sorumluluk Direktifi Taslağı m. 4 (1).

Klasik hukuk düzenlerinde sorumluluk hukuku, davacı tarafın, kendi uğradığı zarar ile davalı tarafın davranışı arasındaki nedensellik bağını kanıtlamasını gerektirmektedir. Ancak, yapay zekâ sistemlerinin opaklığı, yapay zekâ sistemini kullananların söz konusu sebep sonuç ilişkisini kanıtlamasını son derece güçleştirmekte, hatta kimi hallerde imkânsız hale getirmektedir. İşte bu nedenle Direktif, yüksek riskli olsun olmasın, "davalının kusuru" ile "yapay zekâ sistemi tarafından üretilen zararlı çıktı veya ilgili bir çıktının üretilememesi" arasında nedensellik bağının varlığına ilişkin bir karine getirmektedir.

Direktif'e göre yüksek riskli yapay zekâ sistemleri söz konusu ise, davalı, davacının nedensellik bağını ortaya koymak bakımından yeterli kanıt ve uzmanlığa makul ölçüde erişebilir olduğunu kanıtlayabilirse, nedensellik karinesine dayanılamayacaktır. [23] Karinenin yüksek riskli olmayan yapay zekâ sistemleri bakımından söz konusu olması için ise ulusal mahkeme, davacının nedensellik bağını kanıtlamasının aşırı derecede zor olduğunu kabul etmelidir. [24] Ayrıca, yapay zekâ sistemini kişisel ve mesleki olmayan bir faaliyet için kullanan bir davalıya karşı tazminat talebinde bulunulması durumunda, nedensellik karinesinin geçerli olması (i) davalının yapay zekâ sisteminin çalışma koşullarına önemli ölçüde müdahale etmesi veya(ii) sistemin çalışma koşullarını belirleme zorunluluğu ve kabiliyeti bulunmasına rağmen bunu yapmadığı durumlarda geçerli olacaktır.[25]

Yüksek riskli olsun veya olmasın, bir yapay zekâ sisteminin yol açtığı zararlar bakımından nedensellik bağı karinesinin söz konusu olabilmesi için Direktif'in aradığı bazı koşullar bulunmaktadır: [26]

(i) Bunlardan ilki, davacının, davalının neden olunan zararın doğmasını engellemeyi amaçlayan bir özen yükümlülüğünü yerine getirmediğini kanıtlamış olmasıdır. Direktif, özen yükümlülüğünün yerine getirilmediğinin nasıl kanıtlanacağını yüksek riskli yapay zekâ sistemlerinin *sağlayıcıları* ile *kullanıcılarına* yöneltilecek talepler bakımından ayrı ayrı düzenlemiştir. [27]

---

23 Yapay Zekâ Sorumluluk Direktifi Taslağı m. 4 (4).

24 Yapay Zekâ Sorumluluk Direktifi Taslağı m. 4 (5).

25 Yapay Zekâ Sorumluluk Direktifi Taslağı m. 4 (6).

26 Yapay Zekâ Sorumluluk Direktifi Taslağı m. 4 (1).

27 Buna göre, yüksek riskli bir yapay zekâ sisteminin *sağlayıcısına* yöneltilen talepler bakımından bu koşulun sağlanması *yalnızca* davacı tarafından sağlayıcının Yapay Zekâ Yasasında

(ii) İkinci koşul, ilgili özen yükümlülüğünün yerine getirilmemesinin yapay zekâ sistemi tarafından üretilen çıktıyı veya yapay zekâ sisteminin bir çıktı üretememesini etkilemiş olmasının somut olayın koşullarında makul bir olasılık olmasıdır.

(iii) Üçüncü olarak ise, davacı, yapay zekâ sistemi tarafından üretilen çıktının zarara yol açtığını kanıtlamış olmalıdır.

Bu üç koşulun varlığı halinde, zararın ihlal edilen özen yükümlülüğünden kaynaklandığı yönünde aksi ispatlanabilen bir karine söz konusu olacaktır. Ancak bu karinenin, zarar gören üzerinde bulunan, kendi zararını ve davalının kusurunu ispatlama yükünü ortadan kaldırmadığının altı çizilmelidir.

3. Ürün Sorumluluğu Direktifi

Yapay Zekâ Yasası'nı tamamlayan bir diğer düzenleme Ürün Sorumluluğu Direktifi'dir. Bu Direktif ürünlerin güvenliğiyle ilgili olarak ortaya çıkan zararlar nedeniyle imalatçıların sorumluluğunu düzenlemektedir. Aslında Ürün Sorumluluğu Direktifi 1985 yılında kabul edilmiş olup bu tarihten beri yürürlükte olan bir düzenlemedir. Ancak yapılması planlanan değişiklik[28] neticesinde, yapay zekâ sistemlerinin güvenliği ile yapay zekâ sistemlerinden kaynaklanabilecek zararlar da Direktif kapsamına girecektir.

Kusura dayalı bir sorumluluk rejimini esas alan Yapay Zekâ Sorumluluk Direktifi'nin aksine, Ürün Sorumluluğu Direktifi, tüketicilerin, piyasaya sürülen ürünler nedeniyle uğradıkları zararların tazminine ilişkin bir kusursuz sorumluluk rejimi yaratır. Değişiklik önerisinin kabul edilmesi halinde Direktif'in kapsamına, yapay zekâ sistem sağlayıcıları ile bir yapay zekâ sistemini başka bir ürüne entegre eden imalatçıların sorumluluğu da dahil olacaktır. Bununla birlikte, burada yer alan kusursuz sorumluluk

öngörülen belirli yükümlülüklerinin yerine getirilmediğinin ispatı haline mümkündür. Yapay Zekâ Sorumluluk Direktifi Taslağı m. 4 (2). Yüksek riskli bir yapay zekâ sisteminin *kullanıcısına* yöneltilen talepler bakımından ise bu koşulun sağlanması için davacı, (i) kullanıcının yapay zekâ sistemini, beraberindeki kullanım talimatlarına uygun olarak kullanma veya izleme ya da uygun olduğu durumlarda kullanımını askıya alma yahut kesintiye uğratma yükümlülüklerine uymadığını; ya da (ii) yapay zekâ sistemini, kendi kontrolü altında olan ve sistemin kullanım amacı ile ilgili olmayan girdi verilerine maruz bıraktığını kanıtlamalıdır. Bkz. Yapay Zekâ Sorumluluk Direktifi Taslağı m. 4 (3).

28 Bkz. Eur-Lex: "*Proposal for a Directive of the European Parliament and of the on Liability for Defective Products*", (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0495, E.T.: 11 Mayıs 2024).

rejiminin, talepte bulunan kişinin, zararını, ürünün ayıplı olduğunu ve ayıp ile zarar arasındaki nedensellik bağını ispatlama yükünü ortadan kaldırmadığının altı çizilmelidir. [29]

Yapılması planlanan değişiklik neticesinde, (i) ürün tanımı yapay zekâ sistemlerini kavrar şekilde genişletilecek, (ii) tazmin edilebilir zarar türleri çoğalacak, (iii) ayıp değerlendirmesinde dikkate alınacak unsurlar yapay zekâ sistemleri ile uyumlu hale getirilecek, (iv) zarar görene delillere erişme hakkı tanınacak ve (iv) ispat yükü zarar gören lehine hafifletilecektir.

a. Ürün Tanımının Yapay Zekâ Sistemlerini Kapsar Şekilde Genişletilmesi

Ürün Sorumluluğu Direktifi'nde yapılması planlanan ilk değişiklik, yazılımların da "ürün" kavramı kapsamına girdiğinin açıkça kabul edilmesidir. [30] Direktif'in yürürlüğe girmesinin ardından sadece donanım üreticileri değil, aynı zamanda yazılım sağlayıcıları ve (otonom bir araçtaki navigasyon hizmeti gibi) bir ürünün nasıl çalıştığını etkileyen dijital hizmet sağlayıcıları da Direktif kapsamında sorumlu tutulabilecektir.[31] O halde, yapay zekâ sistem sağlayıcıları da piyasaya sürdükleri kusurlu yapay zekâ sistemleri ve yapay zekâ destekli ürünlerin verdikleri zararlardan Direktif dahilinde sorumlu olacaklardır.

Direktif, ticari bir faaliyet dışında geliştirilen veya sunulan ücretsiz ve açık kaynaklı yazılımların yol açtığı zararlara uygulanmayacaktır. [32] Ancak ücretsiz ve açık kaynaklı bir yazılımı ürünlerine entegre eden üreticilerin de Direktif çerçevesinde sorumlu olacakları kabul edilmelidir.

b. Tazmin Edilebilir Zarar Türlerinin Çoğaltılması

Yapılması planlanan değişiklik ile Direktif kapsamında tazmin edilebilecek zarar türlerine bir yenisi eklenmektedir. Her ne kadar Direktif yalnızca maddi zararların tazminine imkân tanımakta (ve manevi zararların tazminini üye devletlerin ulusal düzenlemelerine bırakmakta) ise de zarar kavramının "verilerin kaybı ve bozulmasını" da kapsar şekilde genişletilmesi

---

29 Ürün Sorumluluğu Direktifi Taslağı m. 9 (1).

30 Ürün Sorumluluğu Direktifi Taslağı m. 4 (1).

31 Ürün Sorumluluğu Direktifi Taslağı, Bilgi Notu, s. 5.

32 Ürün Sorumluluğu Direktifi Taslağı, Recital, 13.

planlanmaktadır.[33] Bu bağlamda, zarar gören tarafın kaybolan veya bozulan verileri münhasıran mesleki amaçlarla kullanmaması şartıyla Direktif çerçevesinde tazmin edilebilir bir maddi zarar doğacaktır.

c. Ayıp Değerlendirmesinde Dikkate Alınacak Unsurların Yapay Zekâ Sistemleri ile Uyumlu Hale Getirilmesi

Bir ürünün ayıplı olup olmadığının tespitine ilişkin değerlendirme yaparken dikkate alınacak unsurların dijital çağda ürünlerin değişen doğasına uyum sağlamak ve ABAD içtihadını yansıtmak amacıyla güncellenmesi planlanmaktadır. Bu bağlamda tasarıda, ürünlerin birbirine bağlılığı veya kendi kendine öğrenme fonksiyonları gibi unsurların, bir ürünün ayıplı olup olmadığı değerlendirirken mahkemeler tarafından dikkate alınması gerektiği kabul edilmiştir. Benzer şekilde, ürünlerin siber güvenlik açıkları nedeniyle de ayıplı kabul edilebileceği benimsenmiştir.[34]

Ayıp kavramı çerçevesinde altı çizilmesi gereken bir husus da üründeki ayıbın yapay zekâ sistemi piyasaya sürüldükten sonra ortaya çıktığı hallere ilişkindir. Nitekim, yapay zekâ sistemi piyasaya sürüldükten sonra dahi sağlayıcıların, ayıplı yazılım güncellemeleri sunmaları veya bir güvenlik güncellemesini sunmayı ihmal etmeleri söz konusu olabilir.[35] Bu gibi hallerde ürün piyasaya sürüldükten sonra dahi yapay zekâ sistemi üzerinde kontrolleri devam eden kişilerin sorumluluğu da devam edecektir.[36]

d. Zarar Görenin Delillere Erişme Hakkı

Tıpkı Yapay Zekâ Sorumluluk Direktifi gibi güncellenen Ürün Sorumluluğu Direktifi de ulusal mahkemelerin, ayıplı bir ürünün neden olduğu zararın tazminini talep eden ve tazminat talebinin inandırıcılığını desteklemek için yeterli olgu ve delilleri sunan bir kişinin talebi üzerine, davalının elinde bulunan ilgili delilleri açıklamasını emretme yetkisine sahip olduğunu kabul etmiştir. Yapay Zekâ Sorumluluk Direktifi'nde yer alan düzenlemeye benzer şekilde, bu süreçte tüm tarafların meşru menfaatlerinin göz önünde bulundurulması, açıklanması emredilecek delillerin "gerekli ve orantılı"

33 Ürün Sorumluluğu Direktifi Taslağı m. 4 (6) (c).

34 Ürün Sorumluluğu Direktifi Taslağı m. 6.

35 Bkz. Launders.

36 Ürün Sorumluluğu Direktifi Taslağı m. 6.

olanlarla sınırlı tutulması ve bu delillerin gizliliğinin korunması için gerekli tedbirlerin alınması gerektiği kabul edilmiştir. [37]

e. İspat Yükünün Zarar Gören Lehine Hafifletilmesi

Direktif belirli durumlarda, zarar gören bakımından ispat yükünü hafifleten hükümler içermekte ve tamamının aksi kanıtlanabilir türden karineler getirmiştir. [38] Direktif'in getirdiği karinelerden ilki, ürünün ayıplı olduğuna ilişkin karinedir. Bu bağlamda, (i) davacının mahkemece emredilen delilleri paylaşma yükümlülüğüne uymaması, (ii) ürünün, ortaya çıkan zarara karşı korumayı hedefleyen bir zorunlu güvenlik kuralına uymadığının davacı tarafından ispatlanması veya (iii) zararın olağan bir kullanım sırasında meydana gelen bariz bir ürün arızasından kaynaklandığının davacı tarafından ispatlanması halinde ürünün ayıplı olduğu varsayılacaktır. [39]

Direktif'te yer alan ikinci karine, yapay zekâ sisteminde yer alan ayıp ile zarar arasında nedensellik bağı bulunduğuna ilişkindir. Buna göre, ürünün ayıplı olduğu ve meydana gelen zararın söz konusu ayıp ile tipik şekilde uyumlu olduğu tespit edildiğinde, ayıp ile zarar arasında nedensellik bağı karineten kurulmuş olacaktır. [40]

Direktif'te yer alan üçüncü karine, (örneğin, kara kutu etkisi gibi) teknik veya bilimsel karmaşıklık nedeniyle, davacının üründeki ayıbı veya ayıp ile zarar arasındaki nedensellik bağını ya da her ikisini birden kanıtlamakta aşırı güçlükle karşılaştığı hallerde söz konusu olacak ve ürünün ayıplı olduğu ve/veya ayıp ile zarar arasında uygun nedensellik bağının bulunduğu varsayılacaktır. Ancak bunun için davacının, yeterli ölçüde alakalı deliller ile (i) ürünün zarara katkıda bulunduğunu ve (ii) ürünün ayıplı olmasının muhtemel olduğunu veya ürünün ayıplı olmasının zararın muhtemel bir nedeni olduğunu veya ya da bunların her ikisini ispatlaması gereklidir.

II. KİŞİSEL VERİLERİN KORUNMASI BAĞLAMINDA YAPAY ZEKÂNIN SORUMLULUĞU

Yapay zekânın yol açtığı zararlardan hukuki sorumluluk meselesinin doğrudan doğruya kişisel verilerin korunması ile ilişkili bir boyutu mevcuttur. Bu bağlamda, yapay zekâ teknolojisini besleyen kişisel veri niteliğindeki

37 Ürün Sorumluluğu Direktifi Taslağı m. 8.
38 Ürün Sorumluluğu Direktifi Taslağı m. 9 (5).
39 Ürün Sorumluluğu Direktifi Taslağı m. 9 (2).
40 Ürün Sorumluluğu Direktifi Taslağı m. 9 (3).

verilerin, veri koruma mevzuatına aykırı olarak işlenmesi mümkün olabilir. Keza, gerçek kişilerin kişisel verilerini dikkate alarak karar alan bir algoritmanın ön yargılı davranması veya ayrımcılık yapması da söz konusu olabilir. Her iki halde de zarar gören kişilerin zararlarının tazmini meselesi gündeme gelecektir. Aşağıda ilk olarak yapay zekâ sistemlerinin çalışmasında kişisel verilerin işlevi açıklanacak, ardından yapay zekâ sistemlerinin kişisel veri ihlallerinden doğan sorumluluk ele alınacaktır.

A. YAPAY ZEKÂ SİSTEMLERİNİN ÇALIŞMASINDA KİŞİSEL VERİLERİN İŞLEVİ

Yapay zekâ sistemlerinin işlevselliği büyük ölçüde veriye dayandırır. Zira, bu sistemler veri üzerinde eğitilir ve çalışır. Gerçekten de yapay zekâ sistemleri ve algoritmalar, gelişim aşamasında bir öğrenme sürecinden geçerler. Büyük miktarda veri kullanılarak eğitilen bu algoritmalar, beslendikleri veri setlerini analiz ederek sebep-sonuç ilişkileri çıkarırlar. Keza yapay zekâ algoritmaları karar alırken de bu veri setine ve bu veri setinden elde ettikleri çıkarımlara dayalı olarak hareket ederler.

Yapay zekâ sistemlerini besleyen verilerin tamamı kişisel veri niteliğinde değildir. Örneğin, bir yapay zekâ sistemine sunulan veriler belirli bir coğrafyada geçmiş yıllarda gerçekleşen hava sıcaklılarından veya o bölgeye yağan yağmur miktarından ibaret olabilir. Ancak bunun tam aksi de mümkündür. Örneğin, bir e-ticaret platformu, kullanıcıların geçmişte yaptıkları alışverişlere dayanarak gelecekteki satın alma davranışlarını tahmin eden bir yapay zekâ uygulaması kullanabilir. İşte bu gibi hallerde yapay zekâ sistemlerinin kişisel verileri ihlal etmesi riski gündeme gelir. Aşağıda yapay zekâ sistemlerinin kişisel veri ihlallerinden doğan zararların tazmini meselesi ele alınacaktır.

B. YAPAY ZEKÂ SİSTEMLERİNİN KİŞİSEL VERİ İHLALLERİNDEN DOĞAN HUKUKİ SORUMLULUK

Yapay zekâ sistemlerinin performansı, kullanılan verinin çeşitliliği, doğruluğu ve kalitesine bağlıdır. Nitekim yalnızca doğru, temsil edici ve geniş bir veri seti, güvenilir ve etkili sonuçlar üretme olasılığını artırır. Ancak yapay zekânın sisteminin beslendiği verilerin bir kısmı kişisel veri niteliğinde olup kimliği belirli veya belirlenebilir gerçek kişilere ilişkin olduğundan, bu verilerin yapay zekâ sistemlerince işlenmesi faaliyeti de kişisel verilerin korunmasına ilişkin mevzuat ile uyumlu olmalıdır. Örneğin, yapay zekâ

sisteminin beslendiği ve kişisel veri içeren veri seti hukuka aykırı olarak ele geçirilmiş olabilir. Keza, yapay zekâ sisteminin maruz kalacağı bir saldırı nedeniyle söz konusu kişisel veriler sızabilir ve yetkisiz üçüncü kişilerin eline geçebilir. İşte bu gibi hallerde, yapay zekâ uygulamaları ilgili kişilerin kişilik hakkını ihlal edebilir, maddi ve manevi zararlara yol açabilir.

Yapay zekâ sistemlerinin, eğitim setlerindeki ön yargılar veya eksiklikleri de gerçek kişilerin maddi manevi zarara uğramalarına yol açabilir. Nitekim, eğitim setlerindeki ön yargılar veya eksikliklerden nedeniyle yapay zekâ sistemleri belirli gruplara veya bireylere ön yargılı davranabilir veya haksız bir şekilde ayrımcılık yapabilir.[41] Gerçekten de yapay zekânın temelinde istatistik bilimi yattığından, algoritmalar beslendikleri veri setlerini analiz ederek sonuç çıkartmayı öğrenirler.[42] Eğer algoritmaların eğitildiği veri setleri ön yargılar içermekteyse, geçmiş veriler üzerine eğitilen algoritmalar statükoyu devam ettirdiklerinden, bu ön yargı algoritmaların gelecekte vereceği kararlara da yansır. Böylelikle, yapay zekâ sistemleri geçmişten gelen adaletsizlik ve/veya ayrımcılık kalıplarını tekrarlama riski taşırlar.[43] Örneğin, bir işe alım sürecinde kullanılan bir yapay zekâ algoritmasının, geçmiş işe alım kararlarına dayanan verilerle eğitilmesi cinsiyet, etnik köken veya yaş gibi ön yargılara neden olabilir. Bu çerçevede, geçmişteki uygulamaları yansıtan eğitim verilerinde erkek adayların daha fazla tercih edilmiş olması söz konusu ise bu tür bir algoritma kadın adaylara karşı ayrımcılık uygulayabilir. Nitekim, 2015 yılında Amazon, çalışanları işe almak için kullandığı algoritmanın, seçim yaparken son on yılda gönderilen özgeçmişleri esas aldığını, bu dönemde iş başvurusu yapanların çoğunluğu ise erkek olduğundan kadınlara karşı ön yargılı davrandığını kabul etmiştir. [44] Keza, Amerika Birleşik Devletleri'nde, faillerin

---

41 Algoritmik karar verme hk. detaylı bilgi için bkz. Aksoy, s. 69 vd.

42 Bader, V./Kaiser, S.: "*Algorithmic Decision-Making? The User Interface and Its Role For Human Involvement In Decisions Supported By Artificial Intelligence*" Organization 2019, Vol. 26, I. 5, s. 655-672.

43 Edwards L./Veale, M.: *"Enslaving the Algorithm: From a 'Right to an Explanation 'to a 'Right to Better Decisions'?"*, IEEE Security & Privacy 2018, Vol.16, I.3, s. 46-54; Xenidis, R./Senden, L: "*EU non-Discrimination Law in the Era of Artificial Intelligence: Mapping the Challenges Discrimination*", *General Principles of EU Law and the EU Digital Order*, Kluwer Law International 2020, (https://cadmus.eui.eu/bitstream/handle/1814/65845/ Preprint%20version%20Chapter%20Xenidis_Senden.pdf?sequence=2&isAllowed=y, E.T.: 11 Mayıs 2024).

44 Bkz. Heilweil, R.: "*Why Algorithms Can Be Racist and Sexist*", Vox 2020, (https://www.vox.com/recode/2020/2/18/21121286/algorithms-bias-discrimination-facial-recognition-transparency, E.T.: 11 Mayıs 2024).

yeniden suç işleme riskini hesaplamak amacıyla kullanılan ve aslında ırkı kıstas olarak almayan bir yazılım olan COMPAS'ın (Correctional Offender Management Profiling for Alternative Sanctions) da siyahilere karşı ayrımcılık yaptığı tespit edilmiştir. [45]

Kişisel verilerin yapay zekâ sistemleri aracılığıyla işlenmesi halinde, 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun[46] ("KVKK") öngördüğü kurallar ile kişisel verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi halinde, kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme hakkını düzenleyen 11(1)(g) maddesi uygulanacaktır. Keza yapay zekâ sistemlerinin kişisel veri ihlalinde bulunması halinde KVKK'nın öngördüğü yaptırımların uygulanması da gündeme gelecektir. Bununla birlikte, KVKK m. 14 (3)' göre *"Kişilik hakları ihlal edilenlerin, genel hükümlere göre tazminat hakkı saklıdır."* hükmünü haizdir. Bu bağlamda, ülkemizde yapay zekâ sorumluluğuna ilişkin özel bir düzenleme yapılması halinde bu düzenleme yapay zekâ sistemlerinin yol açtığı zararların tazminine de uygulanacaktır.

SONUÇ VE ÖNERİLER

Yapay zekâ teknolojisinin hızla gelişmesi ve kullanım alanlarının çoğalması, kısa süre öncesine kadar var olmayan yeni hukuki sorunları da beraberinde getirmiştir. Bu teknolojinin sorumluluk hukuku açısından ortaya çıkardığı sorulara yanıt arayan hukukçuların ilk refleksi yapay zekânın yol açtığı zararlara ilişkin sorumluluğu mevcut hukuki kurum ve ilkeler çerçevesinde belirlemeye çalışmak olmuştur. Ancak bu teknolojinin özellikleri ve doğurduğu riskler şimdiye kadar aşina olduğumuz hiçbir sorumluluk kaynağı ile tam olarak benzeşmemektedir. Nitekim, gelişmiş yapay zekâ sistemleri çok sayıda paydaşın katılımını ve farklı yapay zekâ bileşenlerinin birbirine entegre edilmesini gerektiren, opak ve otonom sistemlerdir. Yapay zekânın bu özellikleri, meydana gelen zarara yapay zekâ sisteminin yol açtığına dair nedensellik bağını kurmayı güçleştirdiği gibi zarardan kimin sorumlu olacağına tespit etmeyi de bir o kadar zorlaştırır.

---

[45] COMPAS tarafından yüksek riskli görüldüğü halde tekrar suç işlemeyen siyahi sanık oranı %44,9 iken beyaz sanık oranı %23,5, algoritma tarafından düşük riskli görüldüğü halde tekrar suç işleyen siyahi sanık oranı %28, beyaz sanık oranı ise %47,7' dir. Bkz. Angwin, J./ Larson, J./ Mattu, S./ Kirchner, L.: "*Machine Bias*", Propublica 2016, (https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing, E.T.: 11 Mayıs 2024).

[46] 7.4.2016 tarihli ve 29677 sayılı Resmî Gazete'de yayımlanmıştır.

Mevcut hukuki kurum ve kuralların yapay zekânın yol açtığı zararların tazminini düzenlemek bakımından yetersiz kaldığını tespit eden Avrupa Birliği'nde meseleyi özel olarak düzenleyen iki Direktif taslağı yayınlanmıştır. Bu Direktiflerden Yapay Zekâ Sorumluluk Direktifi, yapay zekânın yol açtığı sözleşme dışı sorumluluk bakımından kusur esasını benimsemekle birlikte bütünsel bir sorumluluk rejimi ortaya koymamaktadır. Direktifte yer alan düzenlemeler zarar görenin iddiasını ispatlamasını kolaylaştıracak iki temel usulî meseleye ilişkindir. Değiştirilmiş hali ile Ürün Sorumluluğu Direktifi ise tüketicilerin kusurlu yapay zekâ sistemleri nedeniyle uğradıkları zararların tazminine ilişkin bir kusursuz sorumluluk rejimi yaratmaktadır. Ürün, ayıp ve zarar kavramlarını, yapay zekâ sistemlerini de dikkate alarak kapsam yönünden yeniden ele alan Direktif, zarar gören lehine ispat yükünü hafifleten düzenlemeler getirmektedir. Ülkemizin Avrupa Birliği düzenlemelerini yakından takip ettiği dikkate alındığında, bu düzenlemelerin benzerlerinin hukukumuzda yapılması olasıdır.

Yapay zekâ sistemlerinin yol açtığı zararlardan hukuki sorumluluk meselesi bir boyutu ile kişisel verilerin korunması ile doğrudan doğruya ilişkilidir. Nitekim yapay zekâ sistemlerini besleyen kişisel veri niteliğindeki verilerin, veri koruma mevzuatına aykırı olarak işlenmesi mümkün olabilir. Ayrıca, gerçek kişilere ilişkin karar alan süreçlerinde faydalanılan algoritmaların ön yargılı davranarak veya ayrımcılık yaparak bu kişilere zarar vermesi söz konusu olabilir. Her iki halde de zarar gören kişilerin zararlarının tazmini meselesi gündeme gelecektir.

Kişisel verilerin yapay zekâ sistemleri aracılığıyla işlenmesi halinde, KVKK'nın kişisel verilerin işlenmesine ilişkin kuralları ve hukuka aykırı veri işleme halleri bakımından öngördüğü yaptırımların uygulanması gündeme gelecektir. Bununla birlikte, kişilik hakları ihlal edilenlerin genel hükümlere göre tazminat hakkı saklı olduğundan, ülkemizde yapay zekâ sorumluluğuna ilişkin özel bir düzenleme yapılması halinde bu düzenleme yapay zekâ sistemlerinin kişisel veri ihlalleri suretiyle yol açtığı zararların tazminine de uygulanacaktır.

KAYNAKÇA

AKSOY, Hüseyin Can: *Kişisel Verilerin Korunması Yönüyle Algoritmik Karar Verme*, Kişisel Verileri Koruma Dergisi 2022, C. 4, S. 2, s. 69-87.

ANGWIN, Julia/ LARSON, Jeff/ MATTU, Surya/ KIRCHNER, Lauren: Machine Bias, Propublica 2016, (https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing, E.T.: 11 Mayıs 2024).

BADER, Verena/ KAISER, Stephan: *Algorithmic Decision-Making? The User Interface and Its Role For Human Involvement In Decisions Supported By Artificial Intelligence* Organization 2019, Vol. 26, I. 5, s. 655-672.

BAK, Başak: *Medeni Hukuk Açısından Yapay Zekânın Hukuki Statüsü ve Yapay Zekâ Kullanımından Doğan Hukuki Sorumluluk*, TAAD 2018, S. 35, s. 211-232.

BORGES, Georg: *Liability for AI Systems Under Current and Future Law*, Computer Law Review International 2023, Vol. 24, No. 1, s. 1-8.

BUITEN, Miriam/ DE STREEL Alexandre / PEITZ, Martin: *The Law and Economics of AI Liability*, Computer Law & Security Review 2023, Vol. 48, s. 6. s. 1-20.

ČERKA, Paulius/ GRIGIENÈ, Jurgita/ SIRBIKYTÈ, Gintare: *Liability For Damages Caused By Artificial Intelligence*, Computer Law & Security Review 2015, C. 31, s. 376-389.

DOĞAN, Erdem: *Dijital Çağda Yeni Bir Hukuki Kişilik Arayışı: Yapay Zekâ*, TBBD 2022, S. 158, s. 213-254.

EDWARDS, Lilian/ VEALE, Michael: *Enslaving the Algorithm: From a 'Right to an Explanation 'to a 'Right to Better Decisions'?*, IEEE Security & Privacy 2018, Vol.16, I.3, s. 46-54.

ERCAN, Cannur: *Robotların Fiillerinden Doğan Hukuki Sorumluluk - Sözleşme Dışı Sorumluluk Hallerinde Çözüm Önerileri*, TAAD 2019, S.40, s. 19-51.

Eur-Lex: Proposal for a Directive of the European Parliament and of the Council on Adapting Non-Contractual Civil Liability Rules To Artificial Intelligence (AI Liability Directive) (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0496, E.T.: 11 Mayıs 2024).

Eur-Lex: Proposal for a Directive of the European Parliament and of the on Liability for Defective Products, (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0495, E.T.: 11 Mayıs 2024).

European Parliament: Report A8-005/2017 with recommendations to the Commission on Civil Law Rules on Robotics, (https://www.europarl.europa.eu/doceo/document/A-8-2017-0005_EN.html, E.T.: 11 Mayıs 2024).

HEILWEIL, Rebecca: Why Algorithms Can Be Racist and Sexist, Vox 2020, (https://www.vox.com/recode/2020/2/18/21121286/algorithms-bias-discrimination-facial-recognitiontransparency, E.T.: 11 Mayıs 2024).

Launders, J. (2024), *Beyond the AI Act: The AI Liability Directive & the Product Liability Directive*, (https://www.techlaw.ie/2024/03/articles/artificial-intelligence/beyond-the-ai-act-how-the-ai-liability-directive-and-the-product-liability-directive-will-also-shape-the-regulation-of-ai-in-the-eu/, E.T.: 11 Mayıs 2024).

SARI, Onur: *Yapay Zekânın Sebep Olduğu Zararlardan Doğan Sorumluluk*, TBBD 2020, S.147, s.251-312.

XENIDIS, Raphaële/ SENDEN, Linda: EU non-Discrimination Law in the Era of Artificial Intelligence: Mapping the Challenges Discrimination, General Principles of EU Law and the EU Digital Order, Kluwer Law International 2020, (https://cadmus.eui.eu/bitstream/handle/1814/65845/Preprint%20version%20Chapter%20Xenidis_Senden.pdf?sequence=2&isAllowed=y, E.T.: 11 Mayıs 2024).

VERİ KORUMA HUKUKUNUN TEMEL PRENSİPLERİ VE YAPAY ZEKÂ UYGULAMALARI AÇISINDAN DEĞERLENDİRİLMESİ

Dr. Öğr. Üyesi Çiçek ERSOY*

GİRİŞ

6698 sayılı Kişisel Verilerin Korunması Kanunu'nun (6698 Sayılı Kanun) 4. maddesinde, GVKT (AB Genel Veri Koruma Tüzüğü)'nin 5. maddesi ile paralel olarak sayılmış olan temel ilkeler, tüm veri işleme faaliyetlerinde öncelikli olarak uygulanacak kurallardır. Kanun'un sistematiğinde ikinci bölümde 'kişisel verilerin işlenmesi' başlığı altında ilk olarak genel ilkelere yer verilmiştir. Bu ilkeler sistematik olarak daha sonra gelen 5. ve 6. maddelerin tamamlayıcısı işlevi görür ve bütünsel olarak değerlendirilir. Genel ilkeler veri sorumluları ve veri işleyenler tarafından yürütülen her tür veri işleme faaliyetinin kalbidir[1].

Yapay zekâ uygulamalarına ilişkin özel olarak zikredilmiş temel prensipler 6698 Sayılı Kanun'da yer almamakta, GVKT'de ise profilleme ve algoritmik karar vermeye dayalı veri işleme özel bir rejime tabii tutularak (GVKT m.22[2]) yapay zekâ uygulamalarına ilişkin dolaylı bir hüküm getirilmektedir[3]. Kişisel Verileri Koruma Kurumu (Kurum) tarafından 15.09.2021'de

* İstanbul Teknik Üniversitesi, İşletme Fakültesi, İşletme Mühendisliği Bölümü, Hukuk Çalışma Grubu Öğretim Üyesi

1 Bilgiç, s. 256.

2 GVKT'nin 22/I. maddesi uyarınca ilgili kişiler, profilleme de dahil olmak üzere, salt otomatik yollarla kişisel verilerinin işlenmesine dayanan ve kendileri hakkında hukuki sonuçlar doğuran ya da kendilerini önemli derecede etkileyen kararlara konu olmama hakkına sahiptir. Düzenlemeye göre, bir kararın ilgili kişi üzerinde hukuki sonuçlar doğurup doğurmadığı ya da onu ciddi derecede etkileyip etkilemediği her somut olayın özelliğine göre ayrı değerlendirilmelidir. Birinci fıkrada getirilen yasağın istisnaları, aynı maddenin 2. fıkrasında sınırlı olarak sayılmıştır.

3 Profilleme ve algoritmik karar verme nedeniyle kişisel verilerin işlenmesi ve Türk hukukuna uyarlanması konusunda bkz. Büyüksağış, Egemen, Yapay Zekâ Karşısında Kişi-

Yapay Zekâ Alanında Kişisel Verilerin Korunmasına Dair Tavsiyeler ("Tavsiyeler")[4] yayınlanmıştır. Bu tavsiye metni Kanun'un yapay zekâ sistemleri açısından nasıl uygulanacağına ilişkin çerçeve niteliğinde bazı öneriler sunmaktadır.

Öncelikle hatırlatmak gerekir ki, yapay zekâ sistemleri kişisel olan veya olmayan her tür veri kullanılarak oluşturulabilir ve geliştirilebilir. Aşağıdaki açıklamalar, işlenen verinin kişisel veri olması[5] ve bu nedenle de veri işleme faaliyetinin 6698 Sayılı Kanun kapsamında olması ön şartı gerçekleşerek yürütülen yapay zekâ geliştirme ve uygulamaları için geçerlidir.

Yapay zekâ uygulamalarıyla kişisel verilerin işlenmesinin yaygınlaşması ve buna bağlı olarak veri işleme faaliyetlerinin çeşitlenmesi ile birlikte, geleneksel veri koruma hukuku yaklaşımı yetersiz kalmaya başlamıştır. Zira yapay zekâ uygulamalarının en önemli özelliği, veri koruma ve mahremiyet hukuku açısından, diğer veri işleme faaliyetlerine kıyasen daha ciddi riskler doğurabilecek nitelikte olmasıdır. Bu riskler özellikle ilgili kişilerin temel hak ve özgürlüklerine müdahale ve veri sorumluları açısından uyum yükümlülüklerinin artması olarak karşımıza çıkmaktadır[6]. Bu risklerin bertaraf edilmesi için ise, genel ilkelerin yapay zekâ uygulamalarının özel niteliği göz önüne alınarak yeniden yorumlanması zorunluluğu ortaya çıkmıştır. Aşağıda her ilke açısından yapay zekâ uygulamaları özelinde açıklamalar yapılacaktır.

6698 Sayılı Kanun m. 4 ve GVKT m. 5'te doğrudan yer almamakla beraber, GVKT'de düzenlenmiş olan tasarımdan itibaren veri koruma ilkesi *(data protection by design-GVKT m. 25)* ve varsayılan ayarların veri korumaya uygunluğu ilkesi *(data protection by default-GVKT m. 25)* yapay zekâ sistemleri açısından da büyük önem arz etmektedir. Zira Kişisel Verileri Koruma Kurulunun (Kurul) da yayınladığı Tavsiyeler metninde, kişisel veri işleme esaslı yapay zekâ çalışmalarında ilk aşamadan itibaren kişisel verilerin korunması mevzuatına uyum sağlanması gereğine vurgu yapılarak,

sel Verilerin Korunması ve Revizyon İhtiyacı, 2021, Yeditepe Üniversitesi Hukuk Fakültesi Dergisi, 18(2), 529-541.

4 https://www.kvkk.gov.tr/Icerik/7048/Yapay-Zeka-Alaninda-Kisisel-Verilerin-Korunmasina-Dair-Tavsiyeler

5 Kişisel veri kavramı için bkz. Ersoy, s. 103 vd.

6 https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/what-are-the-accountability-and-governance-implications-of-ai/

tüm sistemlerin tasarımdan itibaren veri koruma ilkesine göre geliştirilmesi ve yönetilmesini önerilmektedir. Kurul'a göre bu kapsamda her projeye özel bir veri koruma uyum programı oluşturulmalı ve uygulanmalıdır. Ayrıca kişisel veri işleme temelli yapay zekâ çalışmalarında, kişisel verilerin korunması açısından yüksek risk öngörülüyorsa, mahremiyet (veri koruma) etki değerlendirmesinin *(data protection impact assessment-GVKT m. 35)* uygulanması ve veri işleme faaliyetinin hukuka uygunluğuna bu çerçevede karar verilmesi gereği ifade edilmiştir.

I. HUKUKA UYGUN İŞLEME VE ŞEFFAFLIK

Hukuka uygun işleme ve şeffaflık *(lawfulness, fairness and transparency)* ilkesi, 6698 Sayılı Kanun m.4/I'de *'Kişisel veriler, ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebilir.'* cümlesiyle ve arkasından gelen 'hukuka ve dürüstlük kurallarına uygun olma' (6698 Sayılı Kanun m. 4/II-a bendi) ifadesiyle somutlaşmıştır. Türk hukukundaki hükmün mehaz GVKT m.5/I-a[7]'da yer alan karşılığı ise kişisel verilerin hukuka uygun, adil ve şeffaf işlenmesi ilkesi karşımıza çıkmaktadır. Söz konusu düzenlemeler, dayanağını Anayasa m. 20/III'teki 'Kişisel veriler ancak kanunda öngörülen hallerde veya kişinin açık rızası ile işlenebilir' hükmünden almaktadır. Bu düzenlemelerde ifade edilen 'hukuka uygunluk' açıkça tanımlanmamakla beraber, öncelikle 6698 Sayılı Kanun m.5 ve 6'daki (GVKT m. 6 vd.) hukuka uygun işleme şartlarının kastedildiği kabul edilmelidir[8].

Adil işleme, kişisel verilerin ilgili kişinin bilgisi dışında haksız veya hukuka aykırı yollarla elde edilmediğini ve ilgili kişinin veri işleme faaliyetine ilişkin aldatılmadığını ve yanıltılmadığını ifade eder[9]. Veri işlemenin ilgili kişilere olası olumsuz etkilerinin objektif olarak değerlendirilmesi ve bu olumsuz etkiyi dengeleyecek başka bir yarar olup olmadığının tespiti de adil işleme ilkesi kapsamında yapılmalıdır[10]. Adil işleme ilkesi uyarınca veri sorumlusu, veri işlemedeki hedeflerine ulaşmaya çalışırken, ilgili kişi-

---

7 *processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency')*

8 Yücedağ, Genel İlkeler, s. 48.

9 Bilgiç, s. 258.

10 https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/the-principles/lawfulness-fairness-and-transparency/

lerin menfaatlerini ve makul beklentilerini dikkate alarak, ilgili kişinin öngöremeyeceği olumsuz sonuçların ortaya çıkmasını önlemelidir[11]. Adil işleme, işleme faaliyetinin ilgili kişi açısından zarar doğurucu, ayrımcılık yaratıcı, öngörülemez veya yanıltıcı işleme faaliyetlerine yasak getiren oldukça geniş ve soyut bir ilkedir. Adil işleme ilkesinin alt unsurları şu şekilde özetlenebilir[12]:

- Verisi işlenen ilgili kişiye mümkün olan en yüksek düzeyde verilerine ilişkin karar verme yetkisi verilmeli ve veri üzerindeki esas kontrolün ilgili kişide olduğu her zaman göz önüne alınmalıdır.
- İlgili kişilerin, veri işleyen ile iletişim kurabilme ve işlemeye ilişkin bazı haklarını kullanabilme ve öne sürebilme yetkisi olmalıdır.
- Veri işleme, ilgili kişi açısından öngörülebilir ve onun beklentilerine uygun olmalıdır.

İlgili kişilerin aleyhine ayrımcılık sonucu doğuran veri işleme faaliyetlerinden kaçınılmalıdır.

- İlgili kişilerin talep ve ihtiyaçları veya güvenlik açıkları istismar edilmemelidir. Veri işleme faaliyeti ile bağlantılandırılarak, ilgili kişiler belirli tavizleri vermeye zorlanmamalıdır.
- Veri işleme faaliyetlerinde, olabildiğince veri sorumlusu ve ilgili kişi arasındaki denge mekanizması gözetilmeli ve menfaatler arasında dengesizlik yaratacak uygulamalardan kaçınılmalıdır.
- Veri işleme faaliyetleri, ilgili kişinin temel hak ve özgürlükleri ihlal edilmeksizin yürütülmeli, tüm uygun güvence ve önlemler alınmalıdır.

Adil işleme ilkesi yukarıda anlatıldığı üzere, aslında tüm diğer ilkelerin üzerinde ve onları kapsayıcı bir çerçeve oluşturur ve somut hale getirilmeye muhtaç bir prensiptir. Yapay zekâ uygulamaları açısından pek çok noktada bu ilkenin uygulanmasında zorluklar olduğu aşikârdır. Bu nedenle önümüzdeki yıllarda bu temel prensiplerin esnetilerek uygulanması literatürde tartışılabilecektir.

---

[11] KVKK, Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler, s. 2. https://www.kvkk.gov.tr/Icerik/4189/Kisisel-Verilerin-Islenmesine-Iliskin-Temel-Ilkeler.

[12] European Data Protection Board, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, s. 16.

Şeffaflık prensibine göre, kişisel veri işleme faaliyeti, ilgili kişiye açık ve sade bir iletişimle kolay erişebileceği ve anlayacağı şekilde açıklanmalıdır[13]. Böylece veri işleme faaliyetinin niteliği, içeriği ve olası sonuçları kişi açısından öngörülebilir ve anlaşılabilir hale getirilir. Şeffaflık, kişisel verilerin toplanması, kullanılması ve aktarılması da dahil olmak üzere tüm süreçler açısından sağlanmalıdır[14].

Yapay zekâ uygulamaları açısından şeffaflık yükümlülüğünün yerine getirilmesinde bazı zorluklar söz konusu olabilmektedir. Zira şeffaflık yükümlülüğünü yerine getirmesi gereken veri sorumlusu, bu görevini ancak işlenecek verilerle ilgili kendisi de net ve yeterli bilgi sahibi olması şartıyla yapabilir. Ayrıca veri sorumlusunun ilgili kişinin 6698 Sayılı Kanun m. 11'de yer alan verilerinin silinmesine veya verilere ilişkin bilgi edinilmesine ilişkin haklarını kullanması halinde, kişisel veriler üzerinde bu talepleri yerine getirebilecek hakimiyeti olmalıdır. Kompleks ve çok sayıda veri toplanması ve kullanılmasını gerektiren yapay zekâ uygulamalarında, çıktı üretmek için girdiler üzerindeki yapılacak işlemler her zaman insanlar tarafından anlaşılabilir veya okunabilir olmamaktadır. Bu nedenle veri sorumlusu tarafında, öğrenme sonucu üretilecek çıktılara ilişkin de bir öngörülebilirlik söz konusu olmayabilir. Kara kutu problemi *(black box problem)* olarak da adlandırılan bu durum, şeffaflık prensibinin yerine getirilmesinde sorunlar yaratabilmektedir. Yapay zekâ modeli ne kadar otonom ve karmaşık hale gelirse, kara kutu problemi ve dolayısıyla şeffaflık prensibinin yerine getirilmesi de o kadar zorlaşır (ör. nöronal ağlara ilişkin derin öğrenme) [15].

İlgili kişiye açıklanması gereken veri işleme faaliyetiyle ilgili bilgiler, aydınlatma metinleri yoluyla sunulur ve bu metinlerin net, açık, kolay anlaşılır şekilde kaleme alınmış olması gerekir[16]. Yapay zekâ uygulamalarında ise otonom algoritmik veri işleme gibi karmaşık teknik yapıların ilgili kişiye basit şekilde açıklanması oldukça zordur[17].

---

13 GVKT Resital 39.

14 Bilgiç, s. 256.

15 Willecke, Hoeren/Sieber/Holznagel, Handbuch Multimedia-Recht, 2024, Bölüm 29.3, KI im Datenschutzrecht, Kn. 30.

16 KVKK, Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi.

17 Willecke, Hoeren/Sieber/Holznagel, Handbuch Multimedia-Recht, 2024, Bölüm 29.3, KI im Datenschutzrecht, Kn. 30 vd.

Kişisel veriler ilgili kişiden toplanırken veri işleme amacı da açıklanmalıdır. Ancak kendi kendine öğrenen yapay zekâ modellerinde *(self learning AI)*, sürekli olarak yeni veriler işlendiği ve bu verilerden elde edilen sonuçlar daha karmaşık karar verme mekanizmalarına eklemlendiği için, birbirini tamamlayan her işlem için yeniden veri işleme amacı belirlenmesi ve işleme faaliyetinin yeniden şeffaflaştırılması oldukça zordur. Bunun dışında kişisel verinin doğrudan ilgili kişiden değil, üçüncü kişiden temin edilmesi halinde de şeffaflık yükümlülüğü açısından sorunlar ortaya çıkabilecektir.

Şeffaflık yükümlülüğünün uygulanmasına ilişkin bir diğer soru işareti, yapay zekâ uygulamasının nasıl çalıştığına ilişkin ilgili kişinin ne kapsamda aydınlatılacağı meselesidir[18]. Yapay zekâ algoritmaları ticari sır nitelikleri nedeniyle hukuki korumayı haiz olduklarından, ilgili kişinin aydınlatılması yükümlülüğü kapsamında algoritmaya ilişkin ayrıntılı bilgi verilmesi mümkün olmayacaktır. Bu noktada da geleneksel yaklaşımdan uzaklaşılarak yapay zekâ uygulamaları özelinde yorum yapılması ve aydınlatma kapsamının gerektiğinde daraltılması literatürde tartışma konusu olabilecektir. İlgili kişinin aydınlatılması ve şeffaflık yükümlüğü ve veri sorumlusunun ticari sırlarının korunması arasında bir denge oluşturulmalıdır.

Yapay zekâ uygulamalarına ilişkin geliştiriciler, üreticiler ve servis sağlayıcıları gibi farklı paydaşlar arasındaki veri aktarımları söz konusu olduğunda, aydınlatma ve şeffaflık yükümlülüklerinin de veri işlemenin niteliğine göre yerine getirilmesi gerekmektedir. Bu aktarımlar söz konusu olduğunda aktarımın hukuki dayanağı ve hangi veri işleme şartı kapsamında aktarımın yapılacağının belirlenmesi, karmaşık yapay zekâ modülleri açısından zor olabilmektedir. Yukarıdaki pek çok konuda ifade edildiği gibi burada da, özellikle ikincil işlemenin *(further processing)* geleneksel veri koruma hukuku kurallarına göre daha esnek yorumlanması literatürde tartışma konusu olabilecektir.

II. AMACA UYGUN İŞLEME

Amaca uygun işleme *(purpose limitation)* prensibi, 6698 Sayılı Kanun'un 4/II-c bendinde 'Belirli, açık ve meşru amaçlar için işlenme' olarak ifade edilmiştir. Hemen sonra gelen bentte ise yine amaca uygun işleme prensi-

[18] Willecke, Hoeren/Sieber/Holznagel, Handbuch Multimedia-Recht, 2024, Bölüm 29.3, KI im Datenschutzrecht, Kn. 30 vd.

bini tamamlayıcı olarak ölçülülük prensibi yer almıştır. Mehaz AB hukukunda ise, GVKT m. 5/I-b) bendine göre kişisel veriler belirli, meşru ve açık amaçlara uygun şekilde toplanır. Kişisel verilerin belirli, açık, meşru amaçlarla işlenmesi ilkesi şu üç temel unsuru içermektedir[19]:

"1) Kişisel veri işleme faaliyetlerinin ilgili kişi tarafından açık bir şekilde anlaşılabilir olması,

2) Kişisel veri işleme faaliyetlerinin hangi hukuki işleme şartına dayalı olarak gerçekleştirildiğinin tespit edilmesi,

3) Kişisel veri işleme faaliyetinin ve bu faaliyetin gerçekleştirilme amacının belirliliğini sağlayacak detayda ortaya konulması"

Bu ilke, veri sorumlusuna öncelikle veri işleme amacını açık ve kesin olarak belirleme ve bu amacın meşru olup olmadığını değerlendirme yükümlülüğü getirir. Veri sorumlusunun baştan belirlenen ve hukuka uygunluğu buna göre tasarlanan amaç dışında farklı amaçlarla veri işlemesi hukuka aykırıdır. Bu ilke kapsamında amacın meşruiyetinden kasıt, veri sorumlusunun işlediği verilerin, yapmış olduğu iş veya sunmuş olduğu hizmetle bağlantılı ve bunlar için gerekli olmasıdır[20].

AB hukukuna göre, amaca uygun işleme ilkesi iki kümülatif unsurdan oluşur[21]. Buna göre, kişisel veriler:

1) Belirli, açık ve meşru amaçlar (amaç belirleme) için toplanacak ve

2) Bu amaçlarla bağdaşmayan bir şekilde daha fazla işlenemez (amaca uygun kullanım veya uygun amaç testi).

Buna göre amaca uygun işleme ilkesinin ilk koşulu, şu unsurun veri işlemenin amacı açısından bir arada bulunmasıdır[22]:

1) Veri işleme amacı belirli *(spesific)* olmalıdır. Buna göre, amaçlar, kişisel verilerin toplanmasından önce kesin ve tam olarak tanımlanmış olmalıdır.

---

19 KVKK, Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler, s. 8. https://www.kvkk.gov.tr/Icerik/4189/Kisisel-Verilerin-Islenmesine-Iliskin-Temel-Ilkeler.

20 KVKK, Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler, s. 2. https://www.kvkk.gov.tr/Icerik/4189/Kisisel-Verilerin-Islenmesine-Iliskin-Temel-Ilkeler.

21 Article 29 Data Protection Working Party (Çalışma Grubu), No. 203 (2013). Opinion 03/2013 on purpose limitation, s. 15 vd.

22 Article 29 Data Protection Working Party (Çalışma Grubu), No. 203 (2013). Opinion 03/2013 on purpose limitation, s. 15 vd.

2) Veri işleme amacı açık *(explicit)* olmalıdır. Buna göre amaçlar, açıkça ortaya konmuş, açıklanmış veya net bir şekilde ifade edilmiş olmalıdır.

3) Veri işleme amacı meşru *(legitimate)* olmalıdır. Buradaki meşruiyet, sadece kişisel veri koruma hukuku açısından değil, hukukun diğer alanları açısından da gözetilmeli ve geniş yorumlanmalıdır.

Amaca uygun kulanım veya uygun amaç unsuru, verinin ilk işleme (toplama) amacı ve sonradan gerçekleşen işleme faaliyetindeki amacın örtüşüyor olması anlamına gelir. Örneğin, bir hekim tarafından hastalığı teşhis ve tedavi amacıyla alınan sağlık verisi, sonradan hastaya sigorta yaptırılması için kullanılamaz. Bir mobil spor uygulamasında ilk toplama amacı kullanıcıya kişiselleştirilmiş spor programı hizmeti sunmak iken, aynı veriler uygulamadaki teknik sorunları giderme amacıyla kullanılabilir. Zira bu durumda ilk amaç ve ikinci amaç birbirine uygundur[23].

Büyük veriye dayalı yapay zekâ uygulamalarında amaca uygun işleme prensibi, geleneksel veri işleme faaliyetlerine kıyasen çok daha zor uygulanır[24]. Zira büyük veride veri işleme sürecinde en başta yola çıkılan amaçtan farklı amaçlar türetilerek genişletilir. Amaca uygunluk prensibine göre, sonradan ortaya çıkacak her yeni işleme amacı için yeni bir hukuki dayanak oluşturulmalıdır. Örneğin, ilgili kişinin rızasına ihtiyaç duyulan bir veri işleme faaliyetinde, başta alınan rızanın kapsamını aşan yeni amaçlar için yeniden rıza alınması gerekmektedir. Amaca uygunluk prensibinin yapay zekâ açısından uygulanmasındaki zorluklardan biri, test verilerinin yeniden işlenmesidir. Projenin başında veri toplama aşamasında belirlenen toplanma amacı, sonraki test ve geliştirme aşamalarında ilk amacı aşacak şekilde yeniden tanımlanabilmektedir. Özellikle test verileri açısından oluşan bu durumun, amaç değişikliği anlamına geliyorsa, bu veriler için o amaca uygun rıza alınması zorunluluğu doğmaktadır. Amaç değişiklikleri veya amacın genişletilmesi, yapay zekâ uygulamalarında veri işleme konusundaki en önemli tartışma konusudur. Yapay zekâ uygulamalarında veri işlemeye başlanmadan önce, veri işleme amaçlarının (ilk amacın ve ona bağlantılı olarak ortaya çıkabilecek sonraki işleme amaçlarının) açıkça belirlenmesi gerekmektedir. Burada ayrıca, olası hukuka aykırı işlemelerde alınacak tedbirlerin de belirlenmesi tavsiye edilmektedir. Makine öğrenmesi algoritmalarında da verilerin işlenme amacının, ilk toplanma

[23] Yücedağ, Akademik Bakış, s. 145.

[24] Willecke, Hoeren/Sieber/Holznagel, Handbuch Multimedia-Recht, Teil 29.3 KI im Datenschutzrecht, Kn. 37.

amacının farklılaşması sık rastlanan bir durumdur. Zira sistem ancak bu şekilde kendini geliştirebilmektedir. Veri işleme amaçlarının bu otomatik genişlemesi, aslında sistemin işleyişinin ön koşuludur. Geliştiriciler ve kullanıcılar açısından da makine öğrenmesi sistemlerinde verinin toplanma amacı ve sonradan evrildiği amacın tahmin edilmesi zor olabilmektedir. İlk amaç ve sonraki amacın birbirine uygun olmadığı değerlendirmesinin yapılması halinde yapay zekâ geliştiricileri açısından ciddi bir engel ortaya çıkacaktır. Amaca uygunluk prensibinin yapay zekâ sistemleri açısından yeniden yorumlanması ve bu ilkeye bazı istisnalar getirilmesi, yapay zeka uygulamalarının teşvik edilmesi açısından literatürde tartışma konusu olabilecektir.

Amaca uygunluk ilkesinin yapay zekâ sistemleri açısından uygulanmasında bir diğer problem ise, yukarı da da bahsedildiği üzere, test verileri ile ilgili karşımıza çıkabilmektedir. Verinin ilk toplanması aşamasındaki amacın sonradan değiştirilmesi, test verilerinin işlenmesinde sıklıkla söz konusu olmaktadır. Toplanan kişisel verilerin anonimleştirilerek test verisi olarak kullanılması da bir veri işleme faaliyeti kabul edildiğinden, bu durumun da en baştan belirlenmesi ve işlemenin hukuki dayanağının buna göre projenin en başında oluşturulması gerekmektedir[25]. Bu bağlamda anonimleştirme, tüm yapay zekâ projelerinde projenin en başından düşünülerek tasarlanması gereken bir tedbir olarak karşımıza çıkmaktadır.

III. ÖLÇÜLÜLÜK

6698 Sayılı Kanun'un m. 4/II-ç bendinde 'işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma' şeklinde ifade edilmiş olan bu prensip, hukukun farklı alanlarında geçerlilik bulan[26] ölçülülük prensibinin veri koruma hukukundaki görünümüdür. Ölçülülük prensibi, kişisel verilerin işlendikleri amaçlarla ilişkili olarak yeterli, ilgili/bağlantılı ve gerekli olanla sınırlı olmasını ifade eder ve yukarıda açıklanan uygun işleme ilkesi ile doğrudan bağlantılıdır ve uygun işleme ilkesi ile beraber değerlendirilmelidir[27].

---

25 Willecke, Hoeren/Sieber/Holznagel, Handbuch Multimedia-Recht, Teil 29.3 KI im Datenschutzrecht, Kn. 38.

26 Ölçülülük ilkesine genel bir bakış için bkz. Oğurlu, Yücel, AİHM Kararları ve Türk İdare Hukukunda Temel Hak ve Özgürlüklerin Sınırılandırılmasında Bir Yargısal Denetim Ölçütü Olarak Ölçülülük İlkesi, Dokuz Eylül Üniversitesi Hukuk Fakültesi Turhan Tufan Yüce Armağanı, 2001, s. 285-522.

27 Yücedağ, Akademik Bakış, s. 147.

IV. VERİ MİNİMİZASYONU VE GEREKLİ SÜRE KADAR SAKLANMA

Veri minimizasyonu ve gerekli süre kadar saklanma *(data minimisation and store limitation)* ilkesi, ulaşılmak istenen amaçla sınırlı olmak üzere toplanması ve kullanılması anlamına gelir. GVKT m. 5/I-e hükmüne göre, kişisel veriler, kişisel verilerin işlenme amaçlarının gerekli olduğu süreyi aşmadan muhafaza edilir[28]. 6698 Sayılı Kanun'un m. 4/II-d) bendine göre ise, kişisel veriler ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmek zorundadır. Verilerin belirli süre saklanabilmesi ilkesi aslında veri işlemeye zamansal bir sınırlama getirmektedir. Bu zamansal sınırlama aynı zamanda ölçülülük ilkesinin bir görünümü olarak karşımıza çıkmaktadır[29].

Kişisel verilerin "amaçla sınırlılık ilkesi" nin bir gereği olarak işlendikleri amaç için gerekli olan süreye uygun olarak muhafaza edilmesi gerekir[30]. Veri işleme faaliyeti, veri işlemenin amacının geçerli olduğu süre ile sınırlı olmak zorundadır. Bir başka deyişle, bu amaca ulaşmak için belirlenmiş olan süre aşıldıktan sonra veri işleme artık ölçüsüz kabul edilecektir.

Kişisel verilerin muhafaza edileceği süre, özel bir mevzuatta (bankacılık, milli eğitim bakanlığı, iş mevzuatı gibi) özel olarak belirlenmişse bu asgari süreye uygun olarak muhafaza edilmeleri gereklidir. Böyle bir özel düzenleme bulunmuyorsa, veri sorumlusu, subjektif bir bakış açısıyla, ancak kendi içinde tutarlı olmak kaydıyla bazı süreler belirleyebilir. Bu süreler belirlenirken her veri işleme faaliyetinin parametreleri dikkate alınabilir. Ne AB hukukunda ne de Türk veri koruma hukukunda, kanun koyucu katı süreler belirlemiştir. Önemli olan, veri sorumlusunun silme ve saklamaya ilişkin kendi risk değerlendirmesini yaparak, işleyen bir sistem oluşturmasıdır.

Yapay zekâ uygulamalarında çok yoğun ve büyük veri kullanımı göz önüne alındığında gerektiği kadar süre saklanma ilkesinin nasıl uygulanacağı soru işaretleri oluşturmaktadır. Bu büyüklükte verilerin saklanma alanlarının ve alınması gereken bilgi güvenliği önlemlerinin büyüklüğü ve maliyeti de şirketler için ayrı bir dezavantaj oluşturmaktadır. Makine öğren-

---

28 *adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')*

29 Yücedağ, Akademik Bakış, s. 150.

30 KVKK, Temel İlkeler, s. 3.

mesi gibi sürekli ve düzenli olarak gözetim gerektiren yapay zekâ modellerinde verilerin saklanma politikaları oluşturulurken, hukuki gerekliliklerin yanında teknik ve ticari koşullar da göz önünde bulundurulmalıdır.

V. DOĞRULUK VE GEREKTİĞİNDE GÜNCEL OLMA

6698 Sayılı Kanun m.4/II-b) ve GVKT m. 5/I-d hükümlerine göre, kişisel veriler, doğru ve gerektiğinde güncel olmalıdır. Kişisel verilerin doğruluğunun ve güncelliğinin önemini vurgulayan bu ilke *(accuracy and being up to date)* 6698 Sayılı Kanun m. 11/I-d) maddesindeki ilgili kişinin verilerin düzeltilmesini talep etme hakkını tamamlayıcı bir düzenleme olarak görülmelidir[31]. Bu temel ilkeye göre, kanun koyucu veri sorumlusuna, doğru olmayan veya yanıltıcı olan kişisel verileri gecikmeye mahal vermeksizin silmek veya düzeltmek yükümlülüğünü getirmektedir[32]. Bunun için öncelikle veri sorumlusunun verinin doğruluk ve güncelliğini tespit edebilecek bir sistemi olması gerekmektedir. Bu sistemin karmaşık bir uygulama olması şart değildir, güncelleme işlevini yerine getirebilecek ve ilgili kişiye verisinin düzeltilmesini talep hakkını kolaylıkla sağlayan bir mekanizma olması yeterlidir.

Bir yapay zekâ sisteminin istatistiksel doğruluğu ve 6698 Sayılı Kanun anlamındaki doğruluk prensibi birbirinden farklı kavram ve konulardır. Yapay zekâ modelinde veri işleme faaliyeti çerçevesinde verilerin doğru ve güncel olma ilkesine uyulması için, yapay zekâ sisteminin %100 istatistiksel doğruluğu şartı aranmaz[33].

VI. BÜTÜNLÜK, GİZLİLİK VE GÜVENLİK

Bilgi güvenliğinde birbirini tamamlayan üç temel ilke olan gizlilik-bütünlük ve güvenlik *(integrity, confidentiality and security)* ilkeleri, bilginin kişisel veri olması halinde de aynı şekilde önem arz etmektedir. Gizlilik ilkesi, "verilerin yetkisiz erişime karşı korunması ve sadece yetkili kişilere erişilebilir olmasının temini"; bütünlük ilkesi, "bilgilerin eksiksiz, tam, tutarlı ve doğru olması ve bilgi işleme yöntemleri ile veri içeriğinin değişme-

31 KVKK, Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler, s. 2. https://www.kvkk.gov.tr/Icerik/4189/Kisisel-Verilerin-Islenmesine-Iliskin-Temel-Ilkeler.

32 Yücedağ, s. 51.

33 https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/what-do-we-need-to-know-about-accuracy-and-statistical-accuracy/

diğinin temini ve erişilebilirlik ilkesi ise "bilgilere yetkililerce ihtiyaç duyulduğunda erişilebilir olması anlamına gelir[34].

6698 sayılı Kanun'da açıkça yer almamakla beraber, GVKT m. 5/I-d ve f maddelerinde düzenlenmiş olan bütünlük, gizlilik ve güvenlik ilkesi, yapay zekâ sistemlerinin teknik karmaşıklığı ve uygulamaların kişilerin temel hak ve özgürlükleri üzerindeki olası olumsuz etkileri nedeniyle büyük önem arz etmektedir. Bütünlük ilkesinin göz önüne alınması özellikle yapay zekâ uygulamalarının yaratabileceği ön yargı *(bias)* ve bunun yaratacağı adaletsiz sonuçların ve ayrımcılığın önlenmesi açısından önemlidir[35]. Test verilerinin bütünlük ilkesi çerçevesinde düzenli ve sistemli olarak denetlenmesi, yapay zekâ sistemleri ile ulaşılan sonuçların manipülasyonunu önlemeye hizmet eder. Bunun dışında, yüksek gizlilik ve güvenlik standartlarının sağlanması, özellikle de özel nitelikli kişisel verilerin veya çocuklara ait verilerin işlenmesi söz konusu ise büyük önem arz etmektedir. Projenin niteliği ile örtüştüğü sürece, verilerin anonimleştirilerek veya maskelenerek işlenmesi, gizlilik ve güvenlik ilkelerinin uygulanmasının somut bir görünümü olarak karşımıza çıkmaktadır. Son olarak, verilerin kamuya açık kaynaklardan elde edilmiş olması halinde de bu ilkeler özenle uygulanmalıdır.

VII. HESAP VERİLEBİLİRLİK

6698 Sayılı Kanun'da açıkça yer almayan ancak GVKT m. 5/II'de düzenlenmiş olan hesap verilebilirlik *(accountability)* ilkesi, veri sorumlusunun (ve belli durumlarda veri işleyenin) veri koruma mevzuatına uyum yükümlülüğünü doğrudan üstlenmesi ve bunu ispat edebilmesidir[36]. GVKT m. 5/II bu ilkeyi *'veri sorumlusunun f. 1'de belirtilen yükümlülüklere uymakla sorumlu olduğunu ve gerektiği takdirde bu uyumu ispat etmesi'* olarak tanımlamaktadır. Hesap verilebilirlikten kasıt, veri sorumlusunun bu ispat yükü çerçevesinde dokümantasyon (belgelendirme) yapmasıdır. Bu belgelendirme yükümlülüğünün çerçevesi Türk hukukunda mevzuat tarafından kesin çizgilerle belirlenmemiştir. Veri sorumlusunun kendi risk analizi

---

34 Gürol CANBEK, Şeref SAĞIROĞLU, Politeknik Dergisi, Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme, Cilt: 9, Sayı: 3, s. 165-174, 2006, S. 165-174, s. 170.

35 Hoeren/Sieber/Holznagel, Handbuch, Kn. 41.

36 Kaya, M. B. (2021). Kişisel Verilerin Korunmasında Yeni Paradigma: Hesap Verebilirlik İlkesi. İstanbul Hukuk Mecmuası, 78(4), 1859-1897. https://doi.org/10.26650/ mecmua.2020.78.4.0005.

çerçevesinde belgelendirme yapacağı ve terzi işi *(tailor-made)* bir risk yönetimi yaklaşımını benimseyeceği söylenebilir. GVKT çerçevesinde ise veri sorumlusunun veri işlemeye ilişkin süreçleri kayıt altına alarak gerekli olması halinde otoritelere bildirmesi, veri ihlal bildiriminde bulunması, veri koruma etki değerlendirmesi *(data protection impact assessment)* yapması gibi somut yükümlülükler, hesap verilebilirlik ilkesinin görünümleridir[37].

Yapay zekâ uygulamaları açısından hesap verilebilirlik ilkesinin en önemli görünümü, veri koruma etki değerlendirmesi *(data protection impact assessment)* olarak karşımıza çıkmaktadır. Veri koruma etki değerlendirmesi, bir kişisel veri işleme faaliyetinin veri koruma bakımından risklerini belirlemeye ve bu riskleri minimize etmeye hizmet eden bir metottur. Özellikle çok riskli veri işleme faaliyetleri açısından gündeme gelen bu yöntem, 6698 Sayılı Kanun'da açıkça düzenlenmemiş olmakla beraber, yapay zekâ uygulamaları açısından AB hukukunda kabul gören uygulamalardan biridir.

[37] Ekmekçi/Yücedağ/Akkanat-Öztürk/Aşıkoğlu, s. 139.

KAYNAKÇA

BÜYÜKSAĞIŞ, Erdem, Yapay Zeka Karşısında Kişisel Verilerin Korunması ve Revizyon İhtiyacı, Galatasaray Üniversitesi Hukuk Fakültesi Dergisi, 2021, C. XVII, Sayı 2, s. 529-542.

CANBEK, Gürol, SAĞIROĞLU, Şeref, Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme, Politeknik Dergisi, Cilt: 9, Sayı: 3, s. 165-174, 2006, S. 165-174.

EKMEKÇİ, Ömer, YÜCEDAĞ, Nafiye, AKKANAT-ÖZTÜRK, Elif Beyza, AŞIKOĞLU, Şehriban İpek, Kişisel Verilerin Korunması, 1. Baskı, İstanbul 2024.

ERSOY, Çiçek, Temel Kavramlar, (ed. Aksoy P.Ç., Aksoy, H.C.), Kişisel Verilerin Korunmasına Akademik Bakış, 1. Baskı, Ankara, 2023, s. 103-133.

EUROPEAN DATA PROTECTION BOARD (EDPB), Article 29 Data Protection Working Party (Çalışma Grubu), No. 203 (2013). Opinion 03/2013 on purpose limitation.

EUROPEAN DATA PROTECTION BOARD (EDPB), Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en.

HOEREN Thomas/SIEBER Ulrich/HOLZNAGEL Bernd, Handbuch Multimedia-Recht, 2024, KI im Datenschutzrecht.

INFORMATIONS COMMISSONERS OFFICE (ICO), What are the Accountability and Governance Implications of AI? https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/what-are-the-accountability-and-governance-implications-of-ai/.

KAYA, Mehmet Bedii, Kişisel Verilerin Korunmasında Yeni Paradigma: Hesap Verebilirlik İlkesi. İstanbul Hukuk Mecmuası, (2021), 78(4), s. 1859-1897.

KİŞİSEL VERİLERİ KORUMA KURUMU, Yapay Zekâ Alanında Kişisel Verilerin Korunmasına Dair Tavsiyeler, https://www.kvkk.gov.tr/Icerik/7048/Yapay-Zeka-Alaninda-Kisisel-Verilerin-Korunmasina-Dair-Tavsiyeler.

KİŞİSEL VERİLERİ KORUMA KURUMU, Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi

OĞURLU, Yücel, AİHM Kararları ve Türk İdare Hukukunda Temel Hak ve Özgürlüklerin Sınırılandırılmasında Bir Yargısal Denetim Ölçütü Olarak Ölçülülük İlkesi, Dokuz Eylül Üniversitesi Hukuk Fakültesi Turhan Tufan Yüce Armağanı, İzmir, 2001, s. 285-522.

TURGUT BİLGİÇ, Ezgi, Genel Veri Koruma İlkelerinin Yapay Zeka Karşısında Uygulanabilirliği Sorunu, TAAD Yıl 15, Sayı 57, Ocak 2024, Sayı 57, s. 247-282.

YÜCEDAĞ, Nafiye, Kişisel Verilerin Korunması Kanunu Kapsamında Genel İlkeler, ed. Aksoy P.Ç., Aksoy, H.C.), Kişisel Verilerin Korunmasına Akademik Bakış, 1. Baskı, Ankara, 2023, s. 135- 153

YÜCEDAĞ, Nafiye, Kişisel Verilerin Korunması Kanunu Kapsamında Genel İlkeler, Kişisel Verileri Koruma Dergisi, 2019, Sayı 1, s. 47-63.

YAPAY ZEKÂ ALGORİTMALARIYLA PROFİLLEME VE KİŞİSEL VERİLERİN KORUNMASI

Prof. Dr. E. Eylem AKSOY RETORNAZ*

GİRİŞ

Bireylerin nesnel veya öznel özelliklerine dayanılarak sınıflandırmalar yapılması, bu özelliklere dayanılarak bazı çıkarımlarda bulunulması, başka bir ifadeyle profilleme, yeni bir kavram değildir[1]. Kişisel veriler kullanmak suretiyle yapılan profilleme ise gerçek kişinin belirli kişisel yönlerinin analizler veya tahminler yoluyla değerlendirmesine yönelik bir işlemdir. Profilleme yapıldığında kişi, gelecekteki davranışlarının önceden tahmin edilebilmesi için belli davranış kategorileri içinde sınıflandırılır.

Yapay zekâ sistemlerinin kullanımı, profillemenin kapsamı ve koşullarında köklü bir değişikliğe neden olmuştur. Bu teknolojilerle birlikte, kişisel verilerin çok daha etkin bir şekilde kullanılması mümkün hale gelmiştir. Büyük veri, nesnelerin interneti veya dijital teknolojiler aracılığıyla elde edilen kişisel veriler, bu verileri elinde bulunduranların bir araya getirmesi suretiyle ayrıntılı şekilde profilleme yapmalarını mümkün kılmaktadır[2]. Büyük miktardaki veriyi analiz etmek için güçlü algoritmalar kullanılmaktadır. Geçmişte bankacılık sektöründe kredi verirken veya sigorta sektöründe prim belirlerken kullanılan uzman sistemlerin yerini insan beyninin işleyebileceğinden çok daha fazla veri üzerinde çalışabilen, "makine öğrenmesi", "derin öğrenme" olarak adlandırılan sistemler almıştır. Bu sistemler,

* Galatasaray Üniversitesi Hukuk Fakültesi Bilişim ve Teknoloji Hukuku Anabilim Dalı

1 Poullet, Y. : *Cinq ans après: le RGPD et les défis du profilage à l'heure de l'intelligence artificielle*, Revue des affaires européennes, S.1, 2021 s. 88.

2 KVKK, Facebook'ta yaşanan veri ihlaline ilişkin 18/09/2019 tarih ve 2019/269 sayılı kararında *"ihlalden etkilenen kişilere ait çok sayıda kişisel verilerin elde edildiği dikkate alındığında, bu verilere yetkisiz bir şekilde erişenler tarafından ilgili kişiler hakkında profilleme yapılabileceği ve bu faaliyetlerin bu kişilerin aleyhine bir sonuç oluşturabileceği"*ne dikkat çekmiştir.

verilerle karşılaştıkça yavaş yavaş beslenen algoritmalar aracılığıyla, giderek daha güçlü hale gelen sinir ağları arasındaki etkileşimler yoluyla, sayıları artan veriler arasındaki bağıntı (korelasyon) kurmaktadır[3].

Bu otomatik veri işlemeyle birlikte manipülasyonla bağlantılı riskler de artmaktadır. Yapay zekâ algoritmaları ile kullanıcıya sunulan içeriklerin kişiselleştirmesi, önceki deneyimlere göre uyarlama yeteneği ve veri analizi araçları, bu manipülasyonu çoğunu kullanıcı için görünmez kılmaktadır[4]. Birey, internette gezinirken, akıllı telefonunu veya akıllı ev sistemlerini kullanılırken profillemeye maruz kalabileceğinden veya kişisel verilerinin korunmasına yönelik diğer tehlikelerden şüphe etmekten uzaktır. Örneğin bir dijital platformun, video öneri algoritmasının ana hedeflerinden biri, kullanıcının mümkün olduğu kadar uzun süre platforma bağlanmasını sağlayarak kullanıcıya reklam göstermek ve platformun reklam gelirini artırmaktır. Bu hedefe ulaşmak için algoritma, önerdiği videoların yoğunluğunu kademeli olarak değiştirmekte böylece kullanıcıya, fikrini doğrulayan videolar veya sansasyonel içerikler sunmaktadır[5]. New York Times gazetesinde yayımlanan bir habere göre bu dijital platformda izlenme süresinin %70'i öneri algoritması tarafından seçilmektedir[6].

Profilleme esasen kişinin kendi geleceğini ilişkin seçimle bağdaşmayan, insan davranışının karmaşıklığını göz ardı eden bir bir determinizm biçimidir[7]. Kişinin aynı durumdaki başka bir kişiyle aynı şekilde davranacağı yönündeki tahmin ve ön yargı ve ayrımcılığa neden olabilir. Çıkarım yapmak için birbirleriyle karşılaştırılan izler ve devasa veriler çağında, toplumsal yapı da değişmektedir. Bireylerin tercihlerini anında değerlendirmeyi ve bu tercihleri üretken kılmak için disipline etmeyi amaçlayan toplumsal yapı, bireyin davranışlarının kontrolü ve normatif gözetimine dayalı bir yapıdan, bir tahmin toplumuna, "profilleme toplumuna"[8] evrilmektedir.

---

3 Poullet, s. 88.

4 Vergnolle, S.: "L'effectivité de la protection des personnes par le droit des données à caractère personnel", Yayımlanmamış Doktora Tezi, Université Panthéon-Assas, 2020, s. 286.

5 Söz konusu video izleme platformunun algoritma analizi için bkz. Covington, P./ Adams, J/ Sargin, E.: *Deep neural networks for YouTube recommandations* », RecSys, 2016.

6 Fisher, M./ Taub, A*: "How YouTube Radicalized Brazil,* The New York Times", 11/08/2019, (https://www.nytimes.com/2019/08/11/world/americas/youtube-brazil.html, E. T. 20:05.2024)

7 Vergnolle, 285.

8 Profillemenin toplumsal yapıya etkisi hakkında bir inceleme için bkz. Huneman, P.: Les Sociétés de profilage, Paris, 2023.

Profillemeye yönelik yapay zekâ teknolojilerinin kullanımının temel hak ve özgürlükler üzerindeki etkisi ve toplumsal yapıda yaşanan dönüşümler, profilleme karşısında kişisel verilerin korunmasının gerekliliğini ortaya koymaktadır[9]. Yapay zekâ algoritmalarıyla profilleme ve kişisel verilerin korunmasına ilişkin bu çalışmanın ilk bölümünde, profilleme kavramının tanımı ve türlerine yer verilmiştir. Kişisel verilerin korunmasına ilişkin uluslararası ve ulusal metinlerde profillemeye ilişkin düzenlemeler ikinci bölümde incelenmiştir. Çalışmanın üçüncü bölümü ise kişisel verilerin korunması kapsamında yapay zekâ teknolojileri ile profillemenin değerlendirilmesine ayrılmıştır.

I. PROFİLLEME KAVRAMINA GENEL BİR BAKIŞ

A. TANIM

Profilleme, farklı veri tabanlarındaki veriler arasındaki bağıntıların ortaya çıkarılmasına olanak veren bir süreçtir. Profilleme, bir kişiyi, belli bir olasılıkla, belirli bir kategoride sınıflandırmayı, ona uygun kararlar almayı ve gelecekteki seçimlerini, mesleki performansını, ekonomik durumunu, konumunu, kişisel tercihlerini, güvenilirliğini, geleceğini veya davranışlarını tahmin etmeyi mümkün kılan bir yöntemdir[10].

Bir kişinin veya bir grup insanın yaşam tarzının, alışkanlıklarının, kaldıkları ve seyahat ettikleri yerlerin, faaliyetlerinin, kişisel verilerine dayanarak öğrenilmesine olanak sağlayan, ayrıca potansiyel suçluları ve suç mahalini tespit amacıyla özellikle önleyici kolluk faaliyetleri sırasında da kullanılan profilleme, güçlü bir araç olması nedeniyle kişisel verilerin korunmasında temel konulardan biridir[11].

Profilleme, günümüzde gelişen teknolojilerle birlikte, anlaşılması zor ve sürekli değişen çok sayıda tekniği bir araya getiren bir kavram haline

---

9 Poullet, Y./ Frénay, B.: Rapport et propositions de recommandations sur le "Profilage et la Convention 108+ du Conseil de l'Europe", Strasbourg, 2019.

10 Hildebrandt, M.:, Defining Profiling: a New Type of Knowledge ?, (ed. Hildebrandt M./Gutwirth S.) "Profiling the European Citizen, Cross-Disciplinary Perspectives", Dordrecht, 2008, s. 19.

11 Küzeci, E: Sayısal Fil, İstanbul, 2021, s. 214; Öğretmen Kotil Z.: "Yapay Zekâ Teknolojilerinin Kişisel Verilerin Korunmasına Etkileri, Mevcut Problemler ve Çözüm Önerileri", Bahçeşehir Üniversitesi Lisansüstü Eğitim Enstitüsü, Kamu Hukuku Anabilim Dalı, Yüksek Lisans Tezi, İstanbul, 2022, s. 28.

gelmiştir. Otomatik ve günlük olarak depolanan çok sayıda veri, karmaşık ve çoğu zaman şeffaf olmayan teknik yöntemler profillemenin özellikleri arasında yer almaktadır[12].

Profilleme süreci birkaç aşamadan oluşur. İlk aşamada, bireylerin davranışlarına ilişkin kişisel veriler geniş ölçekli toplanmakta, bu veriler ile belirli davranışlar arasında bağıntı kurmak amacıyla analiz edilmekte ve bu analizin sonucunda bir profil oluşturulmaktadır. Ardından bu oluşturulan profil bir bireye uygulanmaktadır.

İkinci aşamada amaç, istatistiklere dayanarak gözlemlenebilir değişkenler arasındaki bağıntı kurmaktır (veri madenciliği). Toplanan veriler, farklı amaçlar ve farklı kullanımlar için birçok şekilde kullanılabilecek profillerin oluşturulması amacıyla hesaplama, karşılaştırma ve istatistiksel bağıntı yazılımı tarafından işlenir. Algoritmalar sayesinde veriler sıralanabilir veya filtrelenebilir, istatistiksel hesaplamalar yapılabilir veya verileri yakınlıklara göre gruplandırılabilir. Karşılaştırma ölçütünü belirleyen, algoritmaların uygunluğu ve özgünlüğüdür.

"Çıkarım" olarak da adlandırılan üçüncü aşamada ise kimliği belirli veya belirlenebilir bu kişiden toplanan kişisel verilere dayanarak ilgili kişinin ait olduğu kategoriye ait yeni veriler atamak amacıyla grup profili uygulanır[13].

Gelişen teknolojilerle birlikte yukarıdaki üç aşamadan yola çıkarak profilleme "*belirli bir olasılıkla sınıflandırmaya izin veren veya izin vermesi beklenen, veri ambarları üzerinde veri madenciliği süreçlerini kullanan ve dolayısıyla belirli bir hata oranıyla, belirli bir kategorideki bir bireyin hakkında münferit karar alınması için kullanılan bilişim sistemli bir yöntem*" [14] olarak tanımlanmaktadır.

B. PROFİLLEME TÜRLERİ

Yukarıda da ifade edildiği üzere profilleme yapılırken kişisel veri kümeleri arasında bir bağıntı kurulmaktadır. Bu bağıntı sonucunda bir kategori

---

12 Grosjean, A.: Le profilage: un défi pour la protection des données à caractère personnel, (ed. Grosjean, A.), "Enjeux européens et mondiaux de la protection des données personnelles", Bruxelles, 2015, s. 291.

13 Grosjean, s. 292.

14 Dinant, J./ Lazaro, M. Ch./Poullet, Y./ Lefever, N./Rouvroy, A., L'application de la Convention 108 au mécanisme de profilage: éléments de réflexion destinés au travail futur du Comité consultatif (T-PD), s. 9.

oluşturulmakta ya da özellikler bir bireye ya da gruba atfedilmektedir[15]. Profilleme sınıflandırılan kişi veya gruplar, verilerin toplanma ve kullanılma biçimine veya temel hak ve özgürlükler bakımından yarattığı risklere göre farklı türlere ayrılmaktadır.

Profilleme sınıflandırılan kişiler bakımından bireysel profilleme ve grup profillemesi olarak ikiye ayrılmaktadır[16]. Bireysel profilleme ise doğrudan ve dolaylı bireysel profilleme olarak iki alt kategoriye ayrılmaktadır.

Profillemenin temel hak ve özgürlükler üzerinde yarattığı riskler bakımından ise profilleme-yüksek riskli profilleme şeklinde bir tasnif yapılmaktadır.

1. Bireysel Profilleme-Grup Profillemesi

Bireysel profilleme, tek bir bireyin davranışlarını, özelliklerini ve eğilimlerini anlamak ve tahmin etmek için yapılan bir veri toplama ve analiz etme sürecidir. Bu süreçte, bireyin demografik bilgileri, alışveriş alışkanlıkları, dijital ayak izleri, sosyal medya aktiviteleri ve diğer kişisel verileri kullanılır. Bireysel profilleme, grup içindeki bireylerin tanımlanmasında veya bir bireyin alışkanlıklarını, tercihlerini, riskini veya diğer sosyal ve ekonomik özelliklerini tanımlamak amacıyla kullanılabilir[17].

Grup profillemesi ise belirli bir grup insanın ortak özelliklerini, davranışlarını ve eğilimlerini anlamak ve tahmin etmek için yapılan profilleme türüdür. Bu gruplar demografik, coğrafi, davranışsal veya başka kategorilere göre ayrılabilir. Grup profilleri hâlihazırda bilinen bilgilere ilişkin olabileceği gibi yeni durumlara da ilişkin olabilir. Grup profillerinin nedensel bir ilişkiyi tanımlaması gerekmez[18].

Bireysel profilleme detaylı ve kişiye özelken grup profillemesi genelleştirilmiş ve geniş bir kitleyi kapsar. Bireysel profilleme kişisel verilerin işlenmesini gerektirirken, grup profillemesi grupların ortak verilerini kullanır. Bireysel profilleme genellikle kişiselleştirme için kullanılırken, grup profillemesi stratejik planlama ve segmentasyon için kullanılır.

---

15 Nišević, Maja: Profiling through Big Data Analytics, Antwerp, 2023, s. 33.

16 Erdoğan, I.: Yapay Zekâ ve Profilleme Teknolojilerinin Ceza Muhakemesinde Kişisel Veri İşlenmesine Etkisi, Ankara, 2022, s. 78.

17 Nišević, s. 33.

18 Custers, B.: Data Mining and Profiling in Big Data, (ed. Arrigo B.A.) "The SAGE Encyclopedia of Surveillance, Security, and Privacy", 2018, s. 279.

2. Doğrudan Profilleme-Dolaylı Profilleme

Doğrudan ve dolaylı profilleme, verilerin toplanma ve kullanılma biçimine göre yapılan bir ayrımdır.

Doğrudan profilleme, verilerin doğrudan ilgili kişiden toplandığı ve analiz edildiği bir profilleme yöntemidir. Bu yöntem, kişinin doğrudan verdiği bilgiler ve etkileşimlerinden elde edilen verilerle gerçekleştirilir[19]. Bu profilleme yönteminde kullanılan veriler, e-ticaret sitelerinde kullanıcıların alışveriş geçmişi ve site içi davranışları, sosyal medya platformlarında kullanıcıların paylaştığı bilgiler ve etkileşimler, bankaların müşterilerinden aldıkları finansal ve kişisel bilgiler olabilir.

Dolaylı profilleme, verilerin üçüncü taraf kaynaklardan alındığı veya kullanıcı davranışlarının dolaylı gözlemle toplandığı bir profilleme yöntemidir. Dolaylı profillemede, kullanıcı davranışlarının gözlemlenmesi sonucu elde edilen ve üçüncü taraftan sağlanan verilerinden yararlanılır. Dolaylı profillemenin bir örneği, bir başkasının aynı e-ticaret platformunda yaptığı satın alma işlemine dayanarak bir ürünü birine tavsiye etmektir. Toplanan verilere dayalı olarak sınıflandırmaya ve genellemeye dayanması nedeniyle dolaylı profilleme, doğrudan profillemeye göre daha belirsizdir[20].

3. Profilleme-Yüksek Riskli Profilleme

Profillemenin temel hak ve özgürlükler üzerindeki yarattığı riskler bakımından yapılan sınıflandırmada, yüksek riskli profilleme ayrı bir kategori profilleme olarak kabul edilerek, bu profilleme türü bakımından farklı düzenlemeler yapılmaktadır.

Yüksek profillemenin tanımına karşılaştırmalı hukukta, İsviçre Federal Kişisel Verilerin Korunması Kanunu'nda (LPD)[21] 2023 yılında yapılan değişiklikle yer verildiği görülmektedir.

LPD m. 5'te GVKT'deki profilleme tanımına benzer genel bir profilleme tanımının yanı sıra yüksek riskli profilleme tanımına yer verilmiştir. Söz konusu tanıma göre "*yüksek riskli profilleme gerçek bir kişinin, kişiliğinin temel özelliklerini değerlendirmeyi mümkün kılan veri eşleştirmesine yol*

19 Nišević, s. 33; Erdoğan, s. 79.

20 Nišević, s. 35.

21 Loi fédérale sur la protection des données https://www.fedlex.admin.ch/eli/cc/2022/491/fr

açtığı için, ilgili kişinin kişiliği veya temel hakları açısından yüksek risk içeren herhangi bir profil oluşturma faaliyeti" [22] olarak tanımlanmıştır.

LDP'de yer alan bu düzenleme ile kişilik profiliyle sonuçlanan herhangi bir profillemenin kanun anlamında yüksek riskli profilleme olarak mı değerlendirilmesi gerektiği, yoksa profilleme sonucunda kişilik profiline ulaşılıp ulaşılmadığının ayrıca analiz edilmesinin mi gerektiği öğretide tartışılmıştır. Yüksek riskli profilleme kavramının, somut riskten bağımsız olarak bir kişilik profilinin oluşturulmasına yol açan herhangi bir profilleme olarak yorumlanmasının gerektiği ifade edilmiştir[23].

LDP'de profilleme veya yüksek riskli profilleme için rıza her zaman gerekli değildir. Profilleme için rızanın arandığı hallerde yüksek riskli profilleme bakımından da ilgili kişinin açık rızası gereklidir[24].

LDP'de kanunlarda öngörülen hallerde bir federal organın yüksek risk profili çıkarabilmesi için yasal dayanağın bulunması aranmaktadır[25].

İlgili kişinin borç ödeme kabiliyetinin değerlendirilmesi amacıyla yüksek riskli profillemeye izin verilmez, başka bir ifadeyle veri sorumlusu bu kapsamda yüksek risk profillemenin gerçekleştirilmesinde üstün bir menfaat iddiasında bulunamaz[26].

Profilleme-yüksek riskli profilleme ayrımına Avrupa Konseyi Profil Oluşturma Bağlamında Kişisel Verilerin İşlenmesiyle İlgili Olarak Bireylerin Korunması Tavsiye Kararında da (CM/Rec(2021)8) [27] yer verilmiştir. LPD'den farklı olarak Tavsiye Kararında yüksek riskli profillemenin tanımı yapılmamış, hangi hallerde profillemenin yüksek riskli profilleme olarak değerlendirileceği belirtilmekle yetinilmiştir.

Tavsiye Kararına göre hukuki sonuçlar doğuran veya ilgili kişi veya profil oluşturma işlemiyle belirlenen kişi grubu için önemli etkiye sahip olan profilleme; hedef kitleye, işlemenin bağlamına veya amacına bağlı olarak,

---

22 LPD m. 5/g.

23 Jacot-Guillarmod, E.: Le profilage à risque élevé de la nLPD : réflexions autour d'un monstre de Frankenstein, 24 août 2021, (*www.swissprivacy.law/86, E. T.: 22/05/2024*).

24 LPD m. 6/7-b).

25 LPD m. 34/2-b.

26 ibid.

27 Tavsiye kararının metni için bkz. https://rm.coe.int/profilleme-uygulamalar-kapsamnda-kisisel-verilerin-otomatik-isleme/1680a4396d (Erişim Tarihi: 22/05/2024).

özellikle bilgi gücündeki dengesizlik durumunda, ilgili kişileri, özellikle de reşit olmayan veya savunmasız insanları, etkileme riski taşıyan profilleme; 108+ sayılı Sözleşme'nin 6. maddesi anlamında hassas nitelikli veri kategorilerini içeren veya bunları tespit etme veya tahmin etme amacını taşıyan profilleme; çok sayıda insanı etkileyen, özellikle çevrim içi aracılık hizmetleri tarafından kendilerinin veya üçüncü tarafların yararına gerçekleştirilen profilleme halinde yüksek riskli profilleme söz konusudur[28].

II. KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN ULUSAL VE ULUSLARARASI METİNLERDE PROFİLLEME

A. AVRUPA KONSEYİ METİNLERİNDE PROFİLLEME

1. Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi (108 sayılı Sözleşme)

Kişisel verilerin korunması alanında ilk bağlayıcı uluslararası sözleşmesi olan Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunmasına İlişkin 108 Sayılı Sözleşme, Avrupa Konseyi üyesi Devletler tarafından 1980'li yılların başında otomatik işleme yoluyla kişisel verilerin işlenmesindeki artış göz önüne alınarak Konsey üyesi ülkelerin vatandaşlarının özel hayatına saygı hakkının kapsamını genişletmek amacıyla kabul edilmiştir[29]. Türkiye'nin de taraf olduğu[30] 1981 tarihli Sözleşme her ne kadar kişisel verilerin korunması bakımından öncü bir rol oynamış olsa da, profillemeye ilişkin bir tanım içermemektedir.

Teknolojik gelişmelerle birlikte kişisel verilerin işlenmesinin yaygınlaşması ve verilerin işlenmesinin kolaylaşması, 108 sayılı Sözleşmenin yenilenmesi ve uyarlanması gereğini doğurmuştur. Avrupa Konseyi Bakanlar Komitesi tarafından 18 Mayıs 2018 tarihinde 108 sayılı Sözleşmeyi yenileyen bir Protokol kabul edilmiş ve anılan sözleşme 108+ Sözleşmesi adını almıştır.

108+ sayılı Sözleşme, güncel teknolojik gelişmelere uygun olarak kişisel verilerin korunmasını amaçlamaktadır. 108+ sayılı Sözleşmede de profilleme tanımı yapılmamıştır. 108+ sayılı Sözleşmenin ilgili kişinin haklarına ilişkin m. 9/c'de ilgili kişilere veri işleme sonucu elde edilen neticelerin

---

28 CM/Rec(2021)8 m. 1-1/j.

29 Christ, M. : Le profilage dans le cadre d'une procédure d'embauche entre particuliers, Zurich, 2023, s. 40.

30 R. G. Tarih 17/03/2016, Sayı 29656.

ilgili kişiye uygulandığı hallerde veri işleme faaliyetinin altında yatan gerekçe hakkında bilgi edinme hakkı tanınmıştır[31]. 108+ sayılı Sözleşme'nin açıklayıcı raporunda m. 9/c düzenlemesi ile ilgili kişilere, profil oluşturma da dahil olmak üzere, otomatik yollarla alınan kararlar için algoritmaların kullanılmasını içeren işlemelerde, bu işlemelerin altında yatan sebepleri ve işlemelerin olası amaçlarını bilme hakkı tanındığı ifade edilmektedir[32]. Profilleme uygulamalarının kişisel veriler üzerinde yarattığı riskler karşısında 108+ sayılı Sözleşmede profilleme hakkında bilgilenme hakkının tanındığı görülmektedir[33].

Bu hakkın varlığına rağmen, 108+ sayılı Sözleşme, taraf Devletlerin iç hukuklarında profillemenin tanımlanması veya bu veri işlemenin özel olarak düzenlenmesi yükümlülüğü getirmemektedir. Başka bir ifadeyle, taraf devletlerin iç hukuklarında, profillemeye ilişkin olarak Sözleşmenin 5, 7 ve 8. maddelerinde öngörülen genel ilkelerin ve 9. maddede güvence altına alınan ilgili kişi haklarının ötesine geçen bir yasal çerçevenin oluşturulmasına ilişkin bir yükümlülük bulunmamaktadır[34].

2. Profil Oluşturma Bağlamında Kişisel Verilerin İşlenmesiyle İlgili Olarak Bireylerin Korunması Tavsiye Kararı - CM/Rec(2021)8

Avrupa Konseyi Bakanlar Komitesi profillemeye ilişkin bir düzenlenme yapılmasının gerekli olduğu düşüncesiyle, 2010 yılında. CM/Rec(2010)13 sayılı Profil Oluşturma Bağlamında Kişisel Verilerin İşlenmesiyle İlgili Olarak Bireylerin Korunması Tavsiye Kararını kabul etmiştir. Teknolojik gelişmelere bağlı olarak profilleme yöntemlerinin ve etkisinin değişmesi nedeniyle 2010 tarihli Tavsiye kararı gözden geçirilerek profillemeyle kişisel verilerin işlenmesine ilişkin olarak CM/Rec(2021) 8 sayılı Tavsiye kararı yayımlanmıştır[35].

---

31 Walter, J.-P: *La Convention 108, un complément nécessaire à l'article 8 de la CEDH à l'heure du numérique*, Civitas Europa 2022, C. 49, S. 2, 2022, s. 25.

32 Açıklayıcı Raporun Türkçe metni için bkz. (*https://itlaw.bilgi.edu.tr /media/2020/3/30 /Convention108 Plus_A%C3%A7%C4%B1klay%C4%B1c%C4%B1_Raporu_HUHXpvC.pdf*, E. T.: 22/05/2024).

33 Christ, s. 42.

34 Christ, s. 209.

35 https://edoc.coe.int/en/international-law/10666-protection-des-personnes-a-l-egard-du-traitement-des-donnees-a-caractere-personnel-dans-le-cadre-du-profilage-recommandation-cmrec20218.html (E. T.:22/05/2024).

Profillemenin tanımı CM (2021) 8 sayılı Tavsiye Kararı m.1/c'de yer almaktadır. Söz konusu tanıma göre profilleme; "*kişisel verilerin, özellikle makine öğrenmesi sistemleri aracılığıyla, bu verilerin, bir gerçek kişiyle ilgili belirli kişisel yönleri değerlendirmek, özellikle bu kişinin iş performansı, ekonomik durumu, sağlığı, kişisel tercihleri, ilgi alanları, güvenilirliği, davranışı, konumu veya hareketleriyle ilgili unsurları analiz etmek veya tahmin etmek için kullanılmasından oluşur*".

Tavsiye kararı, tüm profilleme işlemleri sırasında hem kamu hem de özel sektörde temel hak ve özgürlüklere, özellikle de insan onuruna ve özel hayatın gizliliğine, ifade özgürlüğüne, ayrımcılık yapmama ilkesine ve sosyal adalet, kültürel çeşitlilik ve demokrasinin gereklerine saygı gösterilmesini öngörmektedir.

CM (2021) 8 sayılı Tavsiye Kararının 5. maddesinin 5. fıkrasında, bir kişinin yalnızca profilleme esas alınarak kendisi hakkında hukuki sonuç doğuran veya kendisini önemli derecede etkileyen bir karara tabi olması durumunda, ilgili kişinin bu karara itiraz edebilmesi gerektiği ifade edilmektedir.

CM (2021) 8 sayılı Tavsiye Kararı, işlemenin meşru ve özel amaçlar için gerekli olması ve iç hukukun uygun önlemleri öngörmesi koşuluyla profilleme bağlamında hassas verilerin toplanmasını ve işlenmesini yasaklamayı önermektedir. Tavsiye Kararı ayrıca hassas veriler söz konusu olduğunda profillemenin açık rıza koşuluna bağlı olarak yapılabileceğini öngörmektedir36.

CM (2021) 8 sayılı Tavsiye Kararına göre veri ve algoritma kalitesinin sağlanması, verinin yanlış olma olasılığını azaltmak ve profilleme sürecindeki hata ve ön yargı risklerini en aza indirmek için, veri sorumluları ve uygun durumlarda veri işleyenler tarafından gerekli önlemler alınması gereklidir. Veri sorumluları ve uygun durumlarda veri işleyenler, profilleme amacıyla kullanılan verilerin ve istatistiksel çıkarımların kalitesini periyodik olarak ve makul süreler içinde yeniden değerlendirmeli ve profilleme faaliyetinin ilgili kişinin hakları üzerindeki etkisini gözden geçirmelidir. Veri sorumluları veya veri işleyenler, üçüncü kişilerden veri veya algoritma temin ettiklerinde, bu verilerin ve algoritmaların kalitesini ve işleme amacına uygunluğunu kontrol etmek için gerekli belgeleri de ilgili üçüncü kişilerden almalıdır[37].

---

[36] CM/Rec(2021)8, m.3/1.

[37] Lens, M.: "GDPR & Convention 108: Adequate Protection in A Big Data Era?,– LLM Law and Technology", Tilburg University, Tilburg, 2018, s. 19.

Tavsiye Kararı uyarınca profil oluşturmada kullanılan kişisel veriler yeterli, ilgili olmalı ve toplanma ve işlenme amaçlarına göre aşırı olmamalıdır. Makine öğrenimi sistemlerinde hangi verinin anlamlı bağıntıya izin vereceğini önceden bilmek zordur. Ancak profil oluşturma işleminin, ilgili kişinin profil oluşturma amaçları açısından dikkate alınmasını makul olarak bekleyebileceği (meşru beklentiler) veri kategorileriyle sınırlandırılması önemlidir[38].

Tavsiye Kararında rızalarını özgürce ifade edemeyen kişilerin, özellikle de engelli bireylerin ve çocukların profillerinin çıkarılmasının ilkesel olarak yasaklanması için katı önlemler önerilmektedir[39]. Profillemenin hassas kategorilere yönelik manipülasyon ve negatif ayrımcılık yaratma riskleri göz önüne alındığında, böyle bir yasağın isabetli olduğunu ifade etmek gerekir[40]. Profilleme rızaya dayalı olduğunda, bilgilendirmenin CM (2021) 8 sayılı Tavsiye Kararında belirtilen şekilde yapıldığını kanıtlamak veri sorumlusunun yükümlükleri arasındadır.

3. Avrupa Konseyi Yapay Zekâ, İnsan Hakları, Demokrasi ve Hukukun Üstünlüğü Çerçeve Sözleşmesi

Avrupa Konseyi Yapay Zekâ, İnsan Hakları, Demokrasi ve Hukukun Üstünlüğü Çerçeve Sözleşmesi[41], Avrupa Konseyi Bakanlar Komitesi'nin 17 Mayıs 2024 tarihinde Strazburg'da düzenlenen 133. toplantısında kabul edilmiştir. Sözleşme 5 Eylül 2024'te Vilnius'ta imzaya açılmıştır.

Avrupa Konseyi Yapay Zekâ Sözleşmesi'nde doğrudan profillemeye ilişkin bir düzenleme bulunmamakla birlikte, 7. maddede, yapay zekâ sistemlerinin yaşam döngüsü içindeki faaliyetlerle ilgili olarak insan onuruna ve bireysel otonomiye saygı gösterilmesi gerekliliği, 11. maddede ise mahremiyet ve kişisel verilerin korunması düzenlenmiştir. Sözleşmenin açıklayıcı raporunda, kişisel özerkliğin insan onurunun önemli bir yönü olduğunun altı çizilmiştir[42]. Kişisel özerklik bireylerin baskıya maruz kalmadan

38 CM/Rec(2021)8, m.3/2.

39 CM/Rec(2021)8, m. 3/5.

40 Christ, s. 216.

41 Sözleşme metni için bkz. https://www.coe.int/fr/web/artificial-intelligence/la-convention-cadre-sur-l-intelligence-artificielle (E.T. 23/05/2024).

42 Rapport explicatif de la Convention-cadre du Conseil de l'Europe sur l'intelligence artificielle et les droits de l'homme, la démocratie et l'État de droit, https://rm.coe.int/1680afae68 (E.T.26/11/2024).

seçim yapma, karar verme ve hayatlarını özgürce yaşama kapasitelerini ifade eder. Yapay zekâ bağlamında kişisel özerklik, bireylerin yapay zekâ teknolojilerinin yaşamlarındaki kullanımı ve etkisi üzerinde denetime sahip olmasını gerektirmektedir. İnsan merkezli düzenleme ile Sözleşme, bireylerin yapay zekâ deneyimlerini şekillendirmelerine izin vermenin önemini kabul ederek bu teknolojilerin onların özerkliğini zayıflatmak yerine geliştirmesini sağlaması gerektiğini vurgulamaktadır. Sözleşmenin 7. ve 11. maddeleri birlikte değerlendirildiğinde kişisel özerklik hakkı, kişisel verilerin korunması hakkı çerçevesinde yapay zekâ sistemleri aracılığıyla profillemeye ilişkin olarak bireyin kişisel verileri üzerinde denetim yetkisine sahip olması gerekliliği ve verilerinin nasıl kullanılacağını seçme hakkına ilişkin düzenlemeler olarak kabul edilebilir.

B. AVRUPA BİRLİĞİ MEVZUATI

1. Genel Veri Koruma Tüzüğü (GVKT)

a. Profilleme Tanımı

Profilleme, GVKT'nin 4. maddesinin 4. fıkrasında "*kişisel verilerin, bir gerçek kişiyle ilgili bazı kişisel özellikleri değerlendirmek, özellikle söz konusu gerçek kişinin işteki performansı, ekonomik durumu, sağlığı, kişisel tercihleri, ilgi alanları, güvenilirliği, davranışları, konumu veya hareketlerine ilişkin hususları analiz etmek veya tahmin etmek amacıyla kişisel verilerin kullanılmasını içeren her türlü otomatik işlenme biçimi*" olarak tanımlanmıştır.

GVKT'nin 4. maddesindeki profilleme tanımı, kısmen otomatik yollarla yapılan bir veri işleme sürecini de kapsamaktadır[43]. GVKT'de yer alan profilleme tanımında "değerlendirme" ifadesinin kullanılmasının, profillemenin bir kişiye ilişkin belirli bir takdir veya yargılama biçimini içermesi gerektiği anlamına geldiği ifade edilmektedir[44].

---

[43] Aşıkoğlu, Ş. İ.: Avrupa Birliği ve Türk Hukukunda Kişisel Verilerin Korunması ve Büyük Veri, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Yüksek Lisans Tezi, İstanbul 2018, s. 143; Kavak Güven, N.: Avrupa Birliği Genel Veri Koruma Tüzüğü Doğrultusunda Profilleme Ve Otomatik Karar Alma, TOBB Ekonomi ve Teknoloji Üniversitesi Sosyal Bilimler Enstitüsü Yüksek Lisans Tezi, Ankara, 2022, s. 30.

[44] Mettalinos, N: *Lignes directrices du G29 sur le profilage – Tentative de clarification sur le régime spécial applicable au profilage et à la prise de décision automatisée*, Communication commerce électronique, LexisNexis, février 2018, n° 2, comm. 14, s. 2.; Guissart/Henrotte, s. 11.

Bu geniş tanımdan yola çıkarak 29 WP, Münhasıran Otomatik Karar Alma ve Profilleme Rehberi'nde profillemenin üç unsurdan oluştuğunu belirtmiştir[45].

Bu unsurlardan ilki; otomatik veri işleme süreci, ikincisi; işlem sürecinin kişisel veriler üzerinden yürütülmesi ve nihayet üçüncüsü ise kişisel veriler üzerinde yürütülen otomatik işlem sürecinin bir gerçek kişinin kişisel özelliklerini değerlendirme amacıyla yapılmasıdır.

WP 29'a göre profilleme oluşturma üç aşamaya ayrılabilir: Kişisel verilerin toplanması ve gruplandırılması ilk aşamasıdır. İkinci aşamada, toplanan kişisel veriler, (genellikle algoritmalar veya matematiksel yöntemler kullanılarak) toplanan bilgiler arasındaki bağıntı ve karşılıklı ilişkileri belirlemek amacıyla (otomatik) analize tabi tutulur. Üçüncü aşamada, ise belirlenen bağıntılar, kişisel yönlerini değerlendirme veya gelecekteki davranışlarını tahmin etme nihai amacı ile ilgili bireye uygulanır[46].

b. Profilleme Türleri

WP29, GVKT'de üç kategori profillemenin yer aldığı görüşündedir[47]. Bu kategorilerden ilki madde 4/4'te tanımlanan genel nitelikli profillemedir. Örneğin kullanıcının günlük fiziksel aktivitesini analiz eden akıllı bir saat gibi, ilgili kişinin belirli yönlerini değerlendirmek için verilerin toplandığı profilleme, ilk kategoriye örnek olarak verilebilir.

Genel nitelikli profilleme, GVKT'nin temel ilkelerine başka bir ifadeyle hukuka uygunluk, adalet ve şeffaflık ilkelerine uygun olmalıdır. İşlemenin hukuka uygun, adil ve şeffaf olması, işleme amaçlarının belirlenmiş, açık ve meşru olması, veri minimizasyonu şartına uyulması, verilerin doğru olması ve bunların gizliliğinin ve bütünlüğünün garanti edilmesi gerekmektedir[48].

İkinci kategori profilleme ise gerçek kişilerle ilgili hukuki sonuçlar doğuran veya benzeri biçimde, gerçek kişileri önemli ölçüde etkileyen kararların dayandığı profillemedir. (GVKT m. 35). Bu profilleme kategorisinde

---

45 Article 29 Data Protection Working Party: *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251rev.01)* (https://ec. europa.eu /newsroom /article29/items/612053/en E.T.: 25/05/2024).

46 Article 29 Data Protection Working Party: *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251rev.01).*

47 İbid.

48 Douville, T.: Droit des données à caractère personnel, Paris, 2023, s. 425.

insan müdahalesiyle söz konusu kişiyle ilgili karar verme sürecinin bir parçası olarak profillemeye başvurulmaktadır. Bir bankacının otomatik olarak toplanan bilgilere dayanarak ilgili kişinin kredi almak için gerekli koşulları karşılayıp karşılamadığına karar vermesi örneğinde olduğu gibi.

Son kategori ise insan müdahalesi olmaksızın otomatik işlemeye dayalı kararlar, başka bir ifadeyle otomatik karar almadır (GVKT m. 22). Kredinin verilmesine ilişkin karar gerçek bir kişi tarafından değil, ancak bir algoritma tarafından oluşturulması ve insan müdahalesi olmadan otomatik olarak ilgili kişiye iletilmesi bu kategoriye örnek verilebilir.

İlk iki profilleme kategorisi, GVKT uyarınca tüm kişisel veri işleme işlemleri için geçerli olan ve özellikle bilgi edinme, şeffaflık ve erişim hakkı yükümlülükleri getiren "genel" rejime tabiyken, üçüncü kategori profilleme, profillemeye dayalı otomatik münferit karar alma, GVKT'nin 22.maddesindeki özel düzenlemeye tabidir.

Her ne kadar GVKT m. 13 ve 14'te açık bir şekilde düzenlenmese de genel nitelikli profilleme ve gerçek kişilerle ilgili hukuki sonuçlar doğuran veya benzeri biçimde, gerçek kişileri önemli ölçüde etkileyen kararların dayandığı profilleme faaliyetleri ve bu profillemenin varlığının sonuçları hakkında ilgili kişiye bilgi verilmelidir[49].

Hakkında profilleme yapılan ilgili kişinin profillemeye itiraz hakkı bulunmaktadır. İtiraz hakkı GVKT m. 21'de yer almaktadır. GVKT m. 21/1'e göre ilgili kişinin itiraz hakkı iki durumda söz konusudur. İlk olarak GVKT m. 6/1(e) uyarınca kamu yararına gerçekleştirilen bir görevin yerine getirilmesi veya veri sorumlusuna verilen resmi bir yetkinin kullanılması için kişisel verilerin işlenerek profilleme yapılmasına itiraz edebilir. GVKT m. 6/1(f)'ye göre ilgili kişinin çocuk olduğu durumlarda da profillemeye itiraz hakkı tanınmıştır. Son olarak GVKT m. 21/2'de kişisel verilerin doğrudan pazarlama amaçları doğrultusunda işlenmesi durumunda, ilgili kişinin doğrudan söz konusu pazarlamayla ilgili olduğu ölçüde profilleme de dâhil olmak üzere, kendisiyle ilgili kişisel verilerin söz konusu doğrudan pazarlama amacıyla işlenmesine her zaman itiraz etme hakkı bulunduğu düzenlemesi yer almaktadır.

İtiraz hakkının bir uzantısı olarak, ilgili kişi GVKT m. 17/1 uyarınca unutulma hakkını da kullanabilir.

---

[49] GVKT Rec. 60.

Yukarıda açıklanan haklar dışında, GVKT'de ilgili kişilere ilk iki kategori profillemeye mahsus başka haklar tanınmamıştır. Bu durum ise mevcut hakların etkililiği konusunda şüpheler doğurduğu gerekçesiyle eleştirilmektedir[50].

c. Profillemeye Dayalı Otomatik Münferit Karar Alma

GVKT'nin 4. maddesindeki profilleme tanımı, bir birey açısından hukuki sonuçlar veya önemli sonuçlar doğuran (muhtemelen tamamen otomatikleştirilmiş) bir karar kavramını içermememektedir[51].

Profilleme ile otomatik münferit karar birbiriyle bağlantılı ancak farklı iki kavramdır[52]. Otomatik münferit karar alma profillemeye dayanarak yapılabileceği gibi herhangi bir profilleme olmadan da yapılabilir[53].

Teknolojik açıdan bakıldığında, otomatik karar verme süreci (profil oluşturma) ile sonuca dayalı otomatik karar verme (profil uygulaması) arasında bir fark söz konusudur. Otomatik münferit karar kavramından, ilgili kişi üzerinde hukuki sonuçlar doğuran veya onları benzer şekilde önemli ölçüde etkileyen, yalnızca otomatik işlemeye dayanan bir karar anlaşılmaktadır.

GVKT'de yer alan profilleme tanımı yalnızca kişisel tercihleri tahmin etmeye yönelik veri analizini içerdiğinden, profilleme ile profil uygulaması arasında bir ayrım yapılmamaktadır[54].

Otomatik münferit kararlar, ilgili kişi üzerinde gerçekleştirilen profillemeden elde edilen sonuçlara ve bağıntılara dayanarak alınabilir. Otomatik münferit karar alma sürecinde profillemenin aksine insan müdahalesi söz konusu değildir. Otomatik münferit kararlar hukuki sonuç doğuran başka bir ifadeyle ilgili kişinin kanuni ya da sözleşmeden doğan haklarını etkilerler ya da ilgili kişinin davranışları ya da seçimleri üzerinde önemli bir etkiye sahiptirler.

---

50 Douville, s. 426.

51 Guissart, E./Henrotte, J.-F.: *Profilage: la segmentation jusque dans le régime du RGPD*, PIN CODE 2020, S. 5, s. 10.

52 Aksoy, H. C.: *Kişisel Verilerin Korunması Yönüyle Algoritmik Karar Verme*, Kişisel Verileri Koruma Dergisi. 4(2) 2022, s.73.

53 Douville, s. 425.

54 Nišević, Maja: Profiling through Big Data Analytics, Antwerp, 2023, s. 59.

Profilleme ile otomatik münferit karar arasındaki ayrım farklı hukuki rejimlere tabi olmaları nedeniyle önemlidir.

Profilleme durumunda, hangi kararların tamamen otomatikleştirilmiş olup olmadığına göre bir veri koruma etki değerlendirilmesi gereklidir[55]. Profilleme yapıldığında ilgili kişilerin hak ve özgürlüklerine yönelik riskler, örneğin ayrımcılık riski veya özel hayata saygı hakkının ihlali riski yüksektir. Karar vermeye yönelik olmayan profil oluşturma faaliyetlerinde de, genel ölçütler karşılandığı sürece bir etki değerlendirmesi yapılabilir[56].

GVKT m. 22'de, ilgili kişinin kendisiyle ilgili hukuki sonuçlar doğuran veya benzer biçimde kendisini kayda değer şekilde etkileyen, profilleme de dâhil olmak üzere yalnızca otomatik işlemeye dayalı bir karara tabi olmama hakkı bulunduğu düzenlenmiştir.

Bir kişinin haklarını etkileyen herhangi bir kararın, örneğin seçimde oy kullanma, yasal işlem başlatma veya başkalarıyla ilişki kurma hakkı gibi hukuki sonuçlar doğurduğu düşünülebilir[57].

GVKT m. 22 verileri üzerinde denetime sahip olan ilgili kişinin korunmasını güçlendirmek amacıyla konulmuş genel bir yasak olarak değerlendirilmektedir[58]. Söz konusu düzenleme ile bireysel özerklik ve bilgilerin geleceğini belirleme hakkı kavramları ile doğrudan bağlantılı olarak ilgili kişiye insan müdahalesi olmadan otomatik münferit karar almanın konusu

55 GVKT m. 35/3,a.

56 GVKT m. 35/1.

57 Kişiyi benzer şekilde önemli ölçüde etkileyen etkilerle ilgili olarak GVKT Rec. 71. Başlangıç Paragrafı'nda, otomatik karar vermenin kredi vermenin reddedilmesiyle sonuçlandığı tüm durumlar ve hatta insan müdahalesi olmadan tüm işe alım uygulamaları örnek olarak verilmektedir.

58 Kredi başvurusunun bir profesyonel tarafından incelenmesi amacıyla bir kişiye otomatik olarak puan verilmesi alanında faaliyet gösteren bir şirketle ilgili bir davada, ABAD bu hususu otomatik karar alma olarak değerlendirmiştir. Mahkeme'ye göre 22. maddenin dar yorumlanması suretiyle olasılık değerinin belirlenmesinin yalnızca bir hazırlık eylemi olarak değerlendirilmesi ve yalnızca üçüncü kişinin eyleminin karar olarak nitelendirilmesi halinde maddenin dolanılması riski doğacaktır. Bu nedenle somut olayda 22. madde anlamında bir kararın söz konusu olduğunun altı çizilmiştir. Bu kararda Mahkeme, otomatik tahminlerin, şirketlerin kararlarına kesin bir şekilde rehberlik ettiğini ve bunun da süreci otomatik hale getirdiğini belirtmiştir (CJEU, 7 Aralık 2023, C-634/21, SCHUFA Holding).

olmama hakkı tanınmıştır[59]. Yapay zekâ algoritmalarında makine öğrenmesiyle veri işleme profillemeyi otomatikleştirme kapasitesine sahip olduğundan GVKT m. 22 büyük önem taşımaktadır[60].

GVKT'nin 22. maddesinin yalnızca profillemeye dayanan karar alma hallerinde değil hukuki sonuçlar veya benzer etkiler yaratan tüm otomatik münferit karar alma hallerine uygulandığının altı çizilmelidir. Profillemeye dayanan otomatik münferit karar alma söz konusu olduğunda 22. madde uygulanma alanı bulacaktır.

Otomatik münhasır karar alma yasağının üç istisnası söz konusudur[61]. İlk istisna ilgili kişi ile veri sorumlusu arasında bir sözleşmenin kurulması veya ifası için bir kararın gerekliliğidir. Örneğin işe alımda adayların seçimi veya ihtiyaç kredisi talebinde bulunulma örnek olarak verilebilir.

İkinci istisna, veri sorumlusunun tabi olduğu ve ilgili kişinin hak ve özgürlükleri ile meşru menfaatlerinin güvence altına alınması amacıyla uygun tedbirlerin de belirtildiği AB veya Üye Devlet hukuku tarafından verilen yetkiye dayanmasıdır.

Üçüncü istisna ise ilgili kişinin açık rızasının bulunmasıdır.

Profilleme ve otomatik karar vermenin bireylerin hak ve özgürlükleri üzerindeki etkisi nedeniyle veri sorumlusunun belirli yükümlülükleri bulunmaktadır.

Bir veri sorumlusu, GVKT m 22'de öngörülene benzer şekilde otomatik münferit karar alması halinde ilgili kişiyi böyle bir kararın varlığı konusunda bilgilendirmelidir. Bu bilgilendirme profilleme ve otomatik karar alma sürecinin nasıl işlediği hususunda olabildiğince açık ve anlaşılır bir şekilde yapılmalıdır[62]. Profillemeye dayanan bir veri işleme ile karar alındığı

---

59 Küzeci, E: Kişisel Verilerin Korunması, 4. Baskı, İstanbul, 2020, s. 230, Yalçınkaya Özdamar, İ.: Büyük Veri Çağında Kişisel Verilerin Korunması: Avrupa Birliği Genel Veri Koruma Tüzüğü'nde Profilleme Ve Otomatik Karar Alma Düzenlemeleri, İstanbul Bilgi Üniversitesi Lisansüstü Programlar Enstitüsü, Yayımlanmamış Yüksek Lisans Tezi, İstanbul, 2022, s. 50.

60 Charlet, F.: Réseaux sociaux et protection des données - Analyse des pratiques de Facebook en regard des exigences des droits européen et suisse de la protection des données, "L'ère numérique et la protection de la sphère privée", Zurich, 2018, s. 109.

61 GVKT m. 22/2.

62 Article 29 Data Protection Working Party: *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251rev.01).*

durumlarda, karar alma sürecinde insan müdahalesi olup olmadığına bakılmaksızın, ilgili kişinin, kişisel verilerinin profilinin çıkarılması ve bu profile dayanılarak kendisi hakkında bir karar alınması amacıyla işlendiği hususunda da bilgilendirilmesi gerekir. İlgili kişi profilleme hakkında bilgilendirildikten sonra, profillemeye dayalı bir karar verilmiş olup olmamasından bağımsız olarak profillemeye itirazda bulunma hakkına da sahiptir[63].

2. AB Polis ve Yargı Direktifi (2016/80 sayılı Direktif)

AB Polis ve Yargı Direktifinde de profillemeye ilişkin düzenlemeler bulunmaktadır. GVKT m. 2/f.2 (d) bendinde GVKT hükümlerinin kamu güvenliğine yönelik tehditlere karşı güvence sağlanması ve bu tehditlerin önlenmesi de dâhil olmak üzere suçların önlenmesi, soruşturulması, tespiti veya kovuşturulması ya da cezaların infaz edilmesiyle ilgili olarak yetkili makamlar tarafından kişisel verilerin işlenmesi sürecine uygulanmayacağı düzenlenmiştir. Bu alanda kişisel verilerin işlenmesi ise 2016/680 sayılı Direktif ile düzenlenmektedir.

Profillemeye ilişkin düzenlemeler bakımından Direktif ile GVKT arasında paralellik bulunmaktadır. Profilleme, Direktif m. 3/4'te GVKT ile aynı biçimde tanımlanmıştır. Profilleme de dâhil olmak üzere yalnızca otomatik yollarla karar alma ise Direktif'in 11. maddesinde düzenlenmiştir. Bu madde kapsamına giren bir uygulamanın söz konusu olması için, kişisel verilerin işlenmesi, insani müdahale söz konusu olmadan, salt otomatik şekilde karar alınması, bu kararın kişinin hukuki statüsü ve haklarını olumsuz yönde etkilemesi veya ciddi sonuçlar doğurması aranmaktadır. Profillemeye dayanan otomatik bir karara tabi olmama bir hak olarak olarak düzenlenmemiştir. Bu düzenleme münhasıran otomatik karar alma yasağına ilişkindir. Nitekim maddede, kişi üzerinde olumsuz hukuki sonuç doğuran veya kişiyi ciddi şekilde etkileyen salt otomatik veri işlemeye dayalı karar almanın ilgili üye devlet ve AB mevzuatı uyarınca açıkça aksi öngörülmediği müddetçe yasak olduğu belirtilmektedir. Bu şartlar GVKT kapsamında düzenlenen m. 22 ile benzerlik göstermektedir[64].

GVKT m. 22 düzenlemesi ile benzer şekilde Direktif m. 11 kapsamındaki profilleme düzenlemeleri açısından bir sorun, ilgili maddelere başvurmanın, ancak kişinin bireysel olarak süreçten etkilenmesi ve hakkında profil-

63 İbid.

64 Erdoğan, s. 125.

lemeye dayanılarak ciddi etki doğuran hukuki veya benzer nitelikte kararların alınması halinde mümkün olmasıdır.

Ancak, kimi profilleme türleri bizzat belirli kişileri değil, örneğin risk taşıyan mahalleleri tespit etmekte kullanılmakta, bu durumda, GDPR m. 22 veya 2016/680'de aranan ilgili kişiyi ciddi şekilde etkileyen bir kararın varlığı unsurunun karşılanıp karşılanmadığı tartışmalı hale gelmektedir[65].

Bu durumda, ilgili kişilerin bölgeye çok sayıda kolluk görevlisi seferber edilmesinin, profilleme teknolojilerinin vardığı sonuca dayanılarak alınan bir karar olduğundan haberdar olmaları güçtür. Sürece ilişkin bilgi edinmenin güçlüğünün yanı sıra, bu durumun kişiler üzerinde doğan doğrudan ve dolaylı sonuçlarını kanıtlamak daha güçtür.

GVKT ve Direktif kapsamındaki düzenlemeler, belirli bir kişinin haklarına yönelik tehlikenin doğduğu aşamada uygulanmakta, kişilerin üzerinde ciddi bir etki veya hukuki statülerinde değişiklik oluşmasını beklemektedir. Bu nedenle, söz konusu hakların, grup ve bölge profillemelerine karşı bir koruma oluşturmadığı dikkate alınmalı, doğrudan ihlal beklenmeksizin bu teknolojilerin kullanımına ilişkin sınırlamalar öngören daha geniş kapsamlı düzenlemeler yapılmalıdır[66].

3. AB Yapay Zekâ Tüzüğü

Yapay zekânın benimsenmesini teşvik etmek ve bireylerin yapay zekâyı sorumlu, etik ve güvenilir bir şekilde kullanmasını sağlamak arasında bir denge kurmayı amaçlayan Avrupa Birliği 13 Mart 2024 tarihinde Avrupa Birliği Yapay Zekâ Tüzüğü'nü kabul etmiştir. 12 Temmuz 2024 tarihinde AB Resmî Gazetesi'nde yayınlanan Avrupa Birliği Yapay Zekâ Tüzüğü 1 Ağustos 2024 tarihinde yürürlüğe girmiştir.

AB Yapay Zekâ Tüzüğü m. 3/52'de profillemenin tanımına, GVKT m.4/4'e, AB Polis ve Yargı Direktifi'ne ve 2018/1725 sayılı Tüzükte yer alan düzenlememelere atıfla yer verilmiştir.

Yapay Zekâ Tüzüğü, risk temelli bir yaklaşımla yapay zekâ sistemlerini risk seviyelerine göre sınıflandırmaktadır. Yapay zekâ sistemleri, profilleme yaptığında başka bir ifadeyle bir kişinin mesleki performansı, ekonomik

65 İbid.

66 Erdoğan, s. 132.

durumu, sağlığı, tercihleri, ilgi alanları, güvenilirliği, davranışı, konumu veya hareketleri gibi hayatının çeşitli yönlerini değerlendirmek için kişisel verilerin otomatik olarak işlenmesi durumunda kabul edilemez risk veya yüksek risk kategorisinde sınıflandırılabilir.

Sosyal derecelendirme, başka bir ifadeyle bireylerin veya grupların sosyal davranışlarına veya kişisel özelliklerine göre değerlendirilmesi veya sınıflandırılmasına yönelik yapay zekâ uygulamaları kabul edilemeyecek derecede risk barındırdığı gerekçesiyle yasaklanmıştır.

AB Yapay Zekâ Tüzüğü 5/1-c ile yalnızca genel sosyal derecelendirme başka bir ifadeyle bir bireyin davranışlarının genel olarak değerlendirmesi yasaklanmaktadır[67]. Bununla birlikte, Tüzük (EK III) ve m.5/b'e göre, kredi puanlaması, ödeme gücü değerlendirmesi veya risk değerlendirmeleri ve hayat veya sağlık sigortası fiyatlandırması gibi daha kısıtlı puanlama yapan yapay zekâ sistemleri yüksek riskli olarak sınıflandırılacaktır. Dolandırıcılığı tespit etme veya araç sigortasında fiyat belirleme amacıyla puanlama yapan sistemler ise Tüzüğün kapsamı dışındadır[68].

Bir kişinin suç işleme olasılığının yalnızca profilleme suretiyle kişilik özelliklerine dayalı olarak değerlendirilmesine yönelik yapay zekâ uygulamaları da kabul edilemez risk kategorisinde sınıflandırılmış ve yasaklanmıştır (m. 5/1/d)[69]. Ancak, yapay zekâ sistemlerinin doğrudan suç faaliyetiyle ilgili nesnel ve doğrulanabilir gerçeklere dayanan insani değerlendirmeleri desteklemek için kullanıldığı durumlar yasağın kapsamı dışındadır. Bu istisna ile bir yandan yapay zekâ uygulamalarının suç soruşturması ve suçu önleme bağlamındaki önemine vurgu yapılırken öte yandan değerlendirmenin salt profillemeye değil gerçek verilere dayanması aranmakta-

---

67 Geslevich Packin, N.: *Disability Discrimination Using Artificial Intelligence Systems and Social Scoring: Can We Disable Digital Bias?*, Journal of International Comparative Law 2021, s. 496; Sousa e Silva, N.:, *The Artificial Intelligence Act: Critical Overview* (July 30, 2024), SSRN: https://ssrn.com/abstract=4937150, (E.T: 30/11/2024).

68 Sousa e Silva, s. 22.

69 AB Yapay Zekâ Tüzüğü Gerekçe 42'e göre bir gerçek kişi yalnızca yapay zekâ uygulamaları yapılan profillemeye dayalı olarak tahmin edilen davranışa göre yargılanamaz. Bununla birlikte bu yasak, risk analizinin kişilerin profillenmesine ya da bireylerin kişilik özelliklerine ve özelliklerine dayanmadığı, şüpheli işlemlere dayalı olarak şirketlerin mali dolandırıcılık riskini değerlendirmek için risk analizini kullanan yapay zekâ sistemleri veya örneğin bilinen kaçakçılık rotalarına dayanarak, narkotik veya yasa dışı malların gümrük yetkilileri tarafından bulunma olasılığını tahmin etmeye yönelik risk analizi araçlarını kapsamamaktadır.

dır[70]. Suç önleme veya suç soruşturması amacıyla kullanılan yapay zekâ uygulamaları salt profillemeye dayanmadığında, yüksek risk sınıflandırmasına girecektir (Tüzük, Ek III, 6) [71].

AB Yapay Zekâ Tüzüğü, kullanımına izin verilen yüksek riskli olarak kabul edilen yapay zekâ sistemleri bakımından kurallar, sağlayıcılar, dağıtıcılar veya kendi sistemlerine entegre eden kuruluşlar için ise yükümlülükler belirlemiştir[72].

C. 6698 SAYILI KİŞİSEL VERİLERİN KORUNMASI KANUNU VE PROFİLLEME

6698 sayılı Kanun'da, GVKT'nin 4. maddesinde olduğu gibi profilleme tanımı yer almamaktadır. Bununla birlikte, 6698 sayılı Kanun'un ilgili kişinin haklarının düzenlendiği 11/g maddesinde, ilgili kişinin "*işlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme*" hakkı düzenlenmiştir. Söz konusu düzenleme profilleme ve otomatik karar alma faaliyetlerine atıf yapılan tek düzenlemedir.

6698 sayılı Kanun'daki düzenlemede GVKT'den farklı olarak münhasıran otomatik sistemlerle işlenen verilere itiraz hakkı, münhasıran otomatik sistemler vasıtasıyla işlenen verilerin kişiler aleyhinde olumsuz bir sonuç doğurması şartına bağlanmıştır[73]. 6698 sayılı Kanun'da GVKT'den farklı olarak otomatik karara tabi olmama hakkına bir istisna tanınmamıştır.

Otomatik işlemeye dayalı bir karara tabi olmaya itiraz hakkı bireyin kendi verileri üzerindeki denetimini güçlendirme bakımından önemli bir araçtır[74]. Bu nedenle 6698 sayılı Kanunda profilleme ve yüksek riskli profilleme tanımları yapılarak, hangi hallerde profilleme veya otomatik karar almanın söz konusu olabileceği haller istisnalarla birlikte açık bir biçimde düzenlenmelidir.

---

70 Sousa e Silva, s. 26.

71 Sousa e Silva, s. 27.

72 Bu hususta ayrıntılı bilgi için bkz. Voigt, P./ Hullen, N: The EU AI Act Answers to Frequently Asked Questions, Berlin, Springer, 2024.

73 Güçlütürk, O.: Yapay Zekâ ve Verinin Kullanımı, İstanbul, 2022, s. 301-302; Öğretmen Kotil, s. 116.

74 Öğretmen Kotil, s. 116.

III. KİŞİSEL VERİLERİN KORUNMASI KAPSAMINDA YAPAY ZEKÂ SİSTEMLERİ VE PROFİLLEME

A. KİŞİSEL VERİ TANIMI VE YAPAY ZEKÂ SİSTEMLERİ ARACILIĞIYLA PROFİLLEME

Yapay zekâ sistemlerinin işleyişi, çok sayıda verinin işlenmesine dayanmaktadır. Bu veriler kişisel veri olduğu andan itibaren kişisel verilerin korunmasına ilişkin hukuki düzenlemeler uygulama alanı bulacaktır.

Yapay zekâ sistemleri aracılığıyla gerçekleştirilen profillemede, anonim veriler de kullanılmaktadır. Bununla birlikte, yapay zekânın yüksek bağlantı tespit gücü sayesinde "*özel olarak anonimleştirme tekniklerine tabi tutulmuş veri setlerinin bire bir gerçek kişiyle ilişkilendirilmesi (reidentification*)"[75] de söz konusu olabilir. Örneğin, bir mahallede hangi adayın konut yardımından faydalanacağı saptamak için profillemenin bir parçası olarak belirli bir mahalledeki insanların ortalama geliri, sakinlerin eğitim düzeyi veya eğitim borçlanma durumu gibi verilere başvurulmaktadır[76]. Bu anonim veriler profilleme sonucu elde edilen veriler ile karşılaştırılarak ilgili kişinin kimliği veya diğer kişisel verileri tespit edilebilmektedir[77]. 29 WP profilleme ile ilgili açıklamalarında dijital sistemler tarafından mevcut verilerden yola çıkılarak ulaşılan yeni verileri kişisel veri olarak değerlendirmektedir[78].

Kişisel verilere ilişkin düzenlemelerde profilleme için kullanılabilen anonim verilerin kapsam dışı bırakılması şeffaflık açısından bir risk teşkil etmektedir[79]. Nitekim CM/Rec(2021)8 Tavsiye Kararında, özellikle makine öğrenimi sistemlerinin kullanımına dayanan otomatik işlemeyle, hangi verinin ilgili kişiyle ilgili bağıntılara veya tahminlere izin vereceğini önceden bilmenin zor olduğu, bu gibi durumlarda, kişisel verilerin adil bir şekilde işlenebilmesi için, kişisel olmayan veriler de dahil olmak üzere, ilgili bir kişi hakkında bağıntı veya tahminlerde bulunulabilecek tüm verilerin

---

75 Aksoy Retornaz, E.E./Güçlütürk, O: Yapay Zekâda Kişisel Verilerin Korunması Kanununun Uygulanmasındaki Sorunlara İlişkin Değerlendirmeler, (ed. Çağlayan Aksoy P. ve Aksoy H. C), "Kişisel Verilerin Korunmasına Akademik Bakış", Ankara, 2023, s. 417.

76 Poullet, s. 93.

77 Hildebrandt, M.: Profiling: From data to knowledge, Datenschutz und Datensicherheit – DuD, C. 30, S. 9, 2006, s. 551; Öğretmen Kotil, s. 77.

78 Article 29 Data Protection Working Party, s. 8.

79 Poullet, s. 93.

uygunluk ve kalitesinin sağlanması gerektiği ifade edilmektedir[80]. Böylece Avrupa Konseyi veri koruma düzenlemelerinin uygulama kapsamının genişletilmesi ihtiyacını kabul etmektedir. Bu doğrultuda özellikle yapay zekâ uygulamalarıyla profilleme bakımından, bire bir gerçek kişiyle ilişkilendirilmeye neden olabilecek anonim veriler de kişisel veri kapsamında değerlendirilmelidir[81].

B. KİŞİSEL VERİLERİN İŞLENMESİNE İLİŞKİN TEMEL İLKELER VE YAPAY ZEKÂ SİSTEMLERİ ARACILIĞIYLA PROFİLLEME

1. Aydınlatma Yükümlülüğü

6698 sayılı Kanun m. 10'da, veri sorumlusunun veya yetkilendirdiği kişinin ilgili kişilere belirli konularda bilgi vermekle yükümlü olduğu düzenleme altına alınmıştır. Aydınlatma yükümlülüğünün amacı ilgili kişiye kişisel verilerinin işlenmesine dair bilgi vermektir. Verilen bilginin ilgili kişiyi aydınlattığından söz edebilmek için ilgili kişinin anlayabileceği bir dil ve yöntem ile sunulması gerekmektedir.

Yapay zekâ sistemleriyle kişisel verilerin işlenmesi söz konusu olduğunda çok sayıda veri farklı kaynaklardan toplanabilir. Aydınlatma yükümlülüğünün yerine getirilmesi bakımından verilerin ilgili kişiden toplanıp toplanmadığının belirlenmesi önemli olacaktır[82].

Yapay zekâ sistemleriyle veri işleme ve profilleme bakımından, aydınlatma, profilleme mekanizmasının işleyişini, kişi üzerindeki etkisini, profillemenin kaynaklarını, bu profillemeden kaynaklanan sonuçlara itiraz yollarının açıklandığı, ilgili kişi tarafından kolayca anlaşılabilecek, şeffaf, hesap verilebilir ve basit bir dille yapılmalıdır[83]. Bu husus OECD Yapay Zekâ İlkeleri'nde yansımasını bulmuştur. Şeffaflık ve hesap verilebilirliğe ilişkin m.1/3'te yapay zekâ sistemleri kullanılarak profilleme yapıldığında aydınlatmanın bir yapay zekâ sisteminden etkilenenlerinin çıktıları anlamasını sağlamak üzere, mümkün ve faydalı olduğu durumlarda, tahmine, içeriğe, tavsiyeye veya karara yol açan veri/girdi kaynakları, faktörler, süreçler ve/veya mantık hakkında sade ve anlaşılması kolay bilgilerle yapılması

80 Recommandation CM/Rec(2021)8, s. 9.

81 Poullet, s. 94.

82 İbid.

83 Poullet, s.; Aşıkoğlu,s. 49-50; Öğretmen Kotil, s. 95.

gerekliliğinin altı çizilmiştir. Bu bilgilerin yanı sıra yapay zekâ sisteminden olumsuz etkilenenlerin sistemin çıktılarına itiraz etmelerini sağlayacak bilgiler de sunulmalıdır[84].

CM/Rec(2021)8 Tavsiye Kararında yüksek riskli profilleme durumunda, veri sorumlusunun, ilgili kişiyi bu tür işlemlerin ilgili kişi açısından sonuçları da dahil olmak üzere, veri işlemenin temelini oluşturan algoritmik işlemler hakkında bilgilendireceği, bilginin ise ilgili kişinin kararların veya karar taslaklarının gerekçelerini anlamasına olanak tanıyacak şekilde olması gerektiği vurgulanmıştır.

2. Amaçla Sınırlı İşleme İlkesi ve Veri Minimizasyonu

Yapay zekâ ile kişisel verilerin işlenmesinde, kişisel verilerin işlenmesine ilişkin temel ilkelerin tümüne uygun davranılması gerekmektedir[85]. Bu ilkelerden biri de kişisel verilerin belirli açık ve meşru amaçlar için işlenmesidir. Çok sayıda veri seti kullanan yapay zekâ algoritmaları mevcut verilerden daha önce tespit edilemeyen çıkarımlarda bulunabilmekte, kişisel verilerin toplanma amaçlarından çok daha farklı ve çeşitli amaçlar için işlenmesini mümkün kılmaktadır[86]. Kişisel verilerin toplanma amacından farklı amaçlar için işlenmesinin yanı sıra büyük veri ve algoritmalarının sağladığı kolaylıkla veri sorumlusu profilleme bakımından yeni amaçlar belirleyebilir. Örneğin müşteri profili oluşturma, başlangıçta yalnızca müşteri seçimi amacını taşıyabilir; sistemin iyileştirilmesi, potansiyel müşteriler hakkında daha iyi bilgi edinilmesine ve bu sayede seçilebilir hale getirilmesine ve onlara herhangi bir ürüne yönelik olarak potansiyel talep endekslerine göre farklılaştırılmış fiyatlar sunulmasına yol açabilir[87].

Kişisel veriler bir yapay zekâ sistemine girdi olarak verildiğinde yapay zekâ sistemi tarafından üretilen çıktı, bir kişisel veri olabileceği gibi yukarıdaki örnekte de açıklandığı üzere profillemeye neden olan bir çıktı, ilgili kişinin hayatına dair önemli etkiler doğuran bir çıktı da olabilir. Amaçlar arasındaki ilişki ilgili kişi üzerindeki etki ve veri sorumlusu tarafından

---

84 OECD: "*Recommendation of the Council on Artificial Intelligence*", OECD/LEGAL/0449

85 Kişişel Verileri Koruma Kurumu: "*Yapay Zekâ Alanında Kişisel Verilerin Korunmasına Dair Tavsiyeler*", (https://www.kvkk.gov.tr/Icerik/7048/Yapay-Zeka-Alaninda-Kisisel-Verilerin-Korunmasina-Dair-Tavsiyeler, E.T.10.05.2024), s. 10-11.

86 Aksoy Retornaz,/Güçlütürk, s. 424.

87 Poullet, s. 95.

alınan önlemler değerlendirildikten sonra ilgili kişiyi doğrudan etkileyebilecek yeni bir amaç için kişisel verilerin işlenmesinin baştaki amaçla uyumlu olup olmadığı söylenebilecektir[88].

Veri minimizasyonu ilkesi doğrultusunda kişisel verilerin işlenmesinde amacın gerçekleşmesini gerektirenden fazla verinin işlenmemesi gerekir. Yapay zekâ sistemlerinde makine öğrenimi sistemlerinde çoğu zaman öngörülemeyen veri karşılaştırmalarına dayanarak oluşturulan istatistiksel bağıntılar çok büyük veri setleri sayesinde çalışmaktadır. CM/Rec(2021)8 Tavsiye Kararında, makine öğrenmesi sistemlerinde hangi verinin anlamlı bağıntılara izin vereceğini önceden bilmenin zor olduğu belirtilerek profillemenin ilgili kişinin profil oluşturma amaçları açısından dikkate alınmasını makul olarak bekleyebileceği (meşru beklentiler) veri kategorileriyle sınırlandırılmasının önemi vurgulanmaktadır[89]. Ancak Avrupa Konseyi'nin önerdiği meşru beklentilerin yapay zekâ sistemleriyle profillemede veri minimizasyonunun bakımından yeterli olmadığı, gerekli olan hallerde kullanılan verilere belirli sınırlamalar getiren yasal müdahaleler ile sektörel bazda düzenleme yapılması gerektiği ifade edilmektedir[90].

C. İLGİLİ KİŞİNİN RIZASI

Açık rıza, kişisel veri işleme şartlarından birisidir. CM (2021) 8 sayılı Tavsiye Kararına göre hassas veriler ve yüksek riskli profilleme söz konusu olduğunda profilleme ancak açık rıza koşuluna bağlı olarak yapılabilir.

Açık rıza yoluyla ilgili kişinin yapay zekâ sistemleri aracılığıyla profillenmeme hakkından feragat edilebileceği akla gelebilir. Yapay zekâ teknolojileri tarafından desteklenen sistemleri kurmanın karmaşıklığı, kullanılan kaynakların çeşitliliği, veri sorumlusunun kararlarına temel olacak bağıntı-

88 Aksoy Retornaz/Güçlütürk, s. 426.

89 CM/Rec(2021)8, s. 5.

90 Poullet makine öğrenmesi sistemleriyle yapılan profillemede veri minimizasyonu ilkesine uygunluğun sağlanabilmesi için özellikle banka, sigorta ve kredi kurumlarının ve işe alımda kullanılan yapay zekâ sistemlerinin şu sorulara yanıt vermesinin aranmasını önermektedir: "*Bir sigorta şirketi, bireyselleştirilmiş hizmet sunumu kapsamında sigortalı kişilere ilişkin verileri ne ölçüde kullanabilir?; "Bir banka veya kredi kuruluşu, kredi sağlayıcı olarak sorumluluğu adına ve 'müşterini tanı' ilkesinin gereklerini yerine getirerek müşterilerinin profilini ne ölçüde çıkarabilir?"; "Bir işveren, çalışan veya aday çalışanlarıyla ilgili olarak seçim, kariyer yönetimi vb. bağlamda duyuşsal bilgi işlem sistemlerini ne ölçüde kullanabilir?"* bkz. Poullet s. 96.

ların tahmin edilememesi ve ücretsiz hizmetlere erişimin bir tıklamayla ulaşılabilir olması nedeniyle yapay zekâ sistemleri aracılığıyla gerçekleştirilen veri işleme faaliyetlerinde rıza yükümlülüğü dikkate alınmadan işlem yapılmasının sıklıkla karşılaşılan bir durum olduğunu da ifade etmek yanlış olmayacaktır[91]. Ayrıca yapay zekâ tabanlı profil oluşturma ve gizli dürtme *(nudging)* uygulamaları, hem seçme özgürlüğü hem de ilgili kişilerin verilerinin kontrolünü elinde tutması bakımından soru işaretlerini beraberinde getirmektedir[92]. Yapay zekâ algoritmalarının karmaşıklığı ve kapalılığı göz önüne alındığında, alınan rızanın gerçekten bilgilendirilmiş olması pek olası değildir. Bu nedenle, veri işlemeye yönelik açık rızanın yapay zekâ sistemleriyle profillemenin konusu olmama hakkını yeterince korumadığı da söylenebilir.

Bu hususta CM/Rec(2021)8 Tavsiye Kararı yol gösterici olabilir. Tavsiye Kararı'nda mümkün olduğu durumlarda, ilgili kişiye profillemenin yoğunluğuna ilişkin bir seçim yapma hakkını garanti etmek için hizmet sağlayıcılar ve platformlar, sunulan hizmete bağlı olarak mümkün olduğu ölçüde farklı, az çok kişiselleştirilmiş, hatta kişiselleştirilmemiş hizmetler sunmalıdır. Profilleme onayı, bir hizmetin sağlanmasının koşulu olarak aranmamalıdır[93]. Yapay zekâ sistemlerine dayalı belirli işleme durumlarında, ilgili kişinin özellikle de reklam amaçlı profilleme söz konusu olduğunda, istediği profil oluşturma amacını tanımlayabilmesi ve dolayısıyla veri işleme alanını ve kullanılacak verileri daraltabilmesi önem taşımaktadır[94].

CM/Rec(2021)8 Tavsiye Kararında belirtildiği üzere rızalarını özgürce ifade edemeyen kişilerin, özellikle de engelli bireylerin ve çocukların profillerinin çıkarılmasının yasaklanması gerektiği görüşündeyiz.

---

91 Gültekin Varkonyi, G.: Yapay Zekâ ve Kişisel Veriler: Teknoloji ve Hukuk Arasında Başka Bir Boyut, (https://www.cybermagonline.com/yapay-zek-ve-kisisel-veriler-teknoloji-ve-hukuk-arasinda-baska-bir-boyut, E. T. 10/06/2024); Öğretmen Kotil, s. 121.

92 Conseil de l'Europe: Intelligence Artificielle et Protection des Données, Strasbourg, 2019, s. 24.

93 CM/Rec(2021)8, s. 5.

94 Poullet, Y.: L'IA un défi pour nos législations et notre vie privée, (ed. Epiney, A. ve Rovelli S.), "Künstliche Intelligenz und Datenschutz / L'intelligence artificielle et protection des données", Zurich, 2021, s. 32.

D. İLGİLİ KİŞİNİN HAKLARI BAKIMINDAN YAPAY ZEKÂ SİSTEMLERİYLE PROFİLLEME

6698 sayılı Kanun m. 11/1'de "*işlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme*" hakkı düzenlenmiştir. Söz konusu hak, münhasıran otomatik sistemlerle kişisel verilerin işlenmesine yönelik genel bir itiraz hakkı niteliği taşımamaktadır[95].

İlgili kişinin itiraz hakkı özellikle yapay zekâ ile profilleme ile ilgili yapıldığı durumlarda önem arz etmektedir. Yapay zekâ sistemleriyle profilleme, bireylerin gelecekteki davranışları ve eğilimleri hakkında oldukça doğru tahminler yapması nedeniyle diğer veri işleme türlerinden farklılık gösterir. Yapay zekâ sistemleriyle profilleme, davranış ve eğilimlere ilişkin son derece doğru tahminlerin yapılmasına neden olabilir. Bu durum ise bireyler üzerindeki toplumsal denetim ve damgalanma riskini artırabilir[96]. 6698 sayılı Kanun m. 11/1'e göre itiraz hakkının kullanılması için hem işlemenin münhasıran otomatik sistemlerle yapılması hem de bu işleme sonucunda ilgili kişinin aleyhine bir sonucun ortaya çıkmış olması gerekmektedir. İtiraz hakkının, söz konusu profillemenin altında yatan gerekçenin ilgili kişi tarafından anlaşılır olması durumunda bir anlam taşıdığını belirtmek gerekir. Ancak profillemede yatan mantığın karmaşıklığı göz önüne alındığında, kişinin itiraz hakkının genel olarak tanınmasının bile ilgililerin kişisel verilerinin korunmasını sağlayacağını ifade etmek mümkün değildir.

Yapay zekâda modelleme çok yönlüdür. Aynı girdi verilerine dayanarak farklı tahminler yapan yapay zekâ modelleri geliştirmek mümkündür. Herhangi bir zamanda alenileştirilen herhangi bir veri, tahmine dayalı profilleme yapan bir yapay zekâ modeli için ilgili bir girdi haline gelebilir. Alenileştirilen veriler, kredi itibarı, suç davranışı ve uyuşturucu kullanımı riski, siyasi eğilimler ve ebeveyn yeterlilikleri dahil olmak üzere diğer kişisel eğilimleri tahmin etmek için kullanılabilir.

Öğretide GVKT m. 21/2'de tanımlanan kişisel verilerin doğrudan pazarlama amaçları doğrultusunda işlenmesi durumunda, ilgili kişinin doğrudan

---

95 Aksoy Retornaz/Güçlütürk, s. 434.

96 Ploug, Thomas: *The Right Not to Be Subjected to AI Profiling Based on Publicly Available Data—Privacy and the Exceptionalism of AI Profiling*, Philosophy & Technology, S. 36, 2023, s. 14.

söz konusu pazarlamayla ilgili olduğu ölçüde profilleme de dâhil olmak üzere, kendisiyle ilgili kişisel verilerin söz konusu doğrudan pazarlama amacıyla işlenmesine her zaman itiraz etme hakkının ötesinde, özellikle verilerin veya profillerin üçüncü taraflara aktarılması veya paylaşılması hususunda araştırma amaçlı işlemeyle sınırlı olarak gerekçesiz bir itiraz hakkının tanınmasının faydalı olacağının altı çizilmektedir[97].

Özellikle alenileştirilmiş verilere dayalı olarak profili çıkarılan kişinin açık rızası olmadan yapay zekâ sistemleriyle profillenmemenin bağımsız bir hak olarak düzenlenmesi gerektiği de ifade edilmektedir[98].

E. VERİ KORUMA ETKİ DEĞERLENDİRİLMESİ

Veri koruma etki analizi, GVKT m. 35'te, her veri işleme faaliyeti için değil, yalnızca gerçek kişilerin hak ve özgürlükleri açısından yüksek risk teşkil eden işleme faaliyetleri için bir yükümlülük olarak düzenlenmiştir[99]. GVKT m. 35, işleme faaliyetinin yüksek riski teşkil edecek şekilde nitelendirilmesine yol açan ölçütleri listelemekte ve uygun olduğu durumlarda, bu risk düzeyine karşılık gelen uygulamaları oluşturma ve listeleme işini denetim otoritesine bırakmaktadır[100].

GVKT m. 35'e göre yüksek riskli faaliyetler, gerçek kişiler üzerinde, profil çıkarma dahil otomatik bireysel kararlar alma amacıyla sistematik ve kapsamlı olarak işleme yapılması ve söz konusu kararların gerçek kişileri ilgilendiren hukuki sonuçlar doğurması veya kayda değer şekilde etkilemesi işlemenin gerçek kişilerin hak ve özgürlükleri açısından yüksek risk doğurmasının muhtemel olduğu faaliyetler olarak nitelendirilmiştir.

AB Yapay Zekâ Tüzüğü'nde yapay zekâ sistemleri, profilleme yaptığında, başka bir ifadeyle bir kişinin mesleki performansı, ekonomik durumu, sağlığı, tercihleri, ilgi alanları, güvenilirliği, davranışı, konumu veya hareketleri gibi hayatının çeşitli yönlerini değerlendirmek için kişisel verilerin oto-

97 Poullet, s. 98.

98 Ploug, s. 14.

99 Article 29 Data Protection Working Party: *Guidelines on Data Protection Impact Assessment (DPIA)* https://ec.europa.eu/newsroom/article29/items/611236/en, E. T.: 30/05/2024).

100 GVKT veri etki analizi değerlendirilmesi hakkında bir inceleme için bkz. Bayram, Ö. B.: *Bir Uyum Aracı Olarak Veri Koruma Etki Analizinin Türk Hukuku Bakımından Değerlendirilmesi*, Kişisel Verileri Koruma Dergisi, 2022, C. 4, S.1, s. 38-53.

matik olarak işlenmesi durumunda yüksek riskli olarak kabul edilmektedir.

GVKT'de veri etki değerlendirmesi uygun olduğu durumlarda veri koruma makamına danışma yükümlülüğü içeren bir iç kontrol ile sınırlıdır. AB Yapay Zekâ Tüzüğü yüksek riskli yapay zekâ sistemleri bakımından bir dizi sıkı teknik gereklilik ve yasal yükümlülükler öngörmektedir.

Yapay zekâ sistemleri ile profillemede kişisel verilerin korunması açısından yüksek risk söz konusu olduğunda mahremiyet etki değerlendirmesi uygulanmalı ve veri işleme faaliyetinin hukuka uygunluğuna bu çerçevede karar verilmelidir[101].

SONUÇ

Yapay zekâ ile profilleme yapıldığında kişisel verilerin korunmasına ilişkin tüm ilkeler uygulama alanı bulacaktır ancak bu düzenleme ve ilkelerin uygulanmasında bazı belirsizlikler söz konusudur. Bu doğrultuda kişisel veri tanımı ve kapsamının yeniden değerlendirilmesi, aydınlatma yükümlüğünün uygun bir biçimde yerine getirilmesi, kişinin açık rızası olmadan yapay zekâ sistemleriyle profillenmemenin bağımsız bir hak olarak düzenlenmesi veri etki değerlendirilmesi yapılmasına ilişkin düzenlemelerin yapılması, yapay zekâ sistemleriyle profillemede kişisel verilerin etkin bir biçimde korunması bakımından önem arz etmektedir.

Yapay zekâ ile profilleme uygulamaları, tek başına veri korumanın çok ötesinde etik sorunları gündeme getirmektedir. Yapay zekâ ile profillemede tüm temel hak ve özgürlüklere, özellikle mahremiyet ve insan onuruna, aynı zamanda ifade özgürlüğüne ve ayrımcılık yapmama ilkesine, ayrıca sosyal adalet, kültürel çeşitlilik ve demokrasinin gereklerine saygı güvence altına alınmalıdır[102].

---

[101] Kişişel Verileri Koruma Kurumu: "*Yapay Zekâ Alanında Kişisel Verilerin Korunmasına Dair Tavsiyeler*"

[102] Poullet, Y.: L'IA un defi, s. 42.

KAYNAKÇA

AKSOY RETORNAZ, E. Eylem ve GÜÇLÜTÜRK, Osman: Yapay Zekâda Kişisel Verilerin Korunması Kanununun Uygulanmasındaki Sorunlara İlişkin Değerlendirmeler, (ed. Çağlayan Aksoy P. ve Aksoy H. C), "Kişisel Verilerin Korunmasına Akademik Bakış", Ankara, 2023, s. 413-438.

AKSOY, Hüseyin Can: *Kişisel Verilerin Korunması Yönüyle Algoritmik Karar Verme*, Kişisel Verileri Koruma Dergisi. 4(2) 2022, s. 69-87.

Article 29 Data Protection Working Party: *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251rev.01)* (https://ec. europa.eu /newsroom /article29/items/612053/en E.T.: 25/05/2024).

Article 29 Data Protection Working Party: *Guidelines on Data Protection Impact Assessment (DPIA)* https://ec.europa.eu/newsroom/article29/items/611236/en, E. T.: 30/05/2024)

AŞIKOĞLU, Şehriban İpek: Avrupa Birliği ve Türk Hukukunda Kişisel Verilerin Korunması ve Büyük Veri, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, Yayımlanmamış Yüksek Lisans Tezi, İstanbul, 2018.

BAYRAM, Öykü Beste: *Bir Uyum Aracı Olarak Veri Koruma Etki Analizinin Türk Hukuku Bakımından Değerlendirilmesi*, Kişisel Verileri Koruma Dergisi, 2022, C. 4, S.1, s. 38-53.

CHARLET, François: Réseaux sociaux et protection des données - Analyse des pratiques de Facebook en regard des exigences des droits européen et suisse de la protection des données, "L'ère numérique et la protection de la sphère privée", Zurich, 2018, s. 77-115.

CHRIST, Myriam : Le profilage dans le cadre d'une procédure d'embauche entre particuliers; Zurich, 2023.

Conseil de L'Europe: Convention 108, T.PD(2019)07BISrev2, Profilage et la Convention 108+: pistes pour une actualisation 2010(13) sur le profilage, 18 juin 2020.

Conseil de L'Europe: Intelligence Artificielle et Protection des Données, Strasbourg, 2019

COVINGTON, Paul ve ADAMS, Jay ve SARGIN, Emre: *Deep neural networks for YouTube recommandations*, RecSys, 2016.

CUSTERS, Bart: Data Mining and Profiling in Big Data, (ed. Arrigo B.A.) "The SAGE Encyclopedia of Surveillance, Security, and Privacy", 2018, s. 277-279.

ÇEKİN, Mesut Serdar ve BERKTAŞ, Ahmet Esad ve AKINCI, Furkan: Veri Hukuku, İstanbul, 2023.

DELTORN, Jean-Marc: Le droit des données personnelles face à l'opacité des algorithmes prédictifs : les limites du principe de transparence, (Netter, E., Ndior, V, Puyraimond, J.-F., Vergnolle, S. (Ed)). *Regards sur le nouveau droit des données personnelles*. Centre de droit privé et de sciences criminelles d'Amiens., 2019, Morgane Daury, 979-10-97323-05-9. ffhal-02357967f, s. 153-206.

DİNANT, Jean-Marc ve LAZARO, Christophe ve POULLET, Yves ve LEFEVER, Nathalie ve ROUVROY, Antoinette: L'application de la Convention 108 au mécanisme de profilage : éléments de réflexion destinés au travail futur du Comité consultatif (T-PD), (http://www.coe.int /t/dghl/standardsetting /dataprotection /Reports/CRID_Profilage_ 2008_fr .pdf. E.T. 31.05.2024), s. 9.

DOUVILLE, Thibault: Droit des données à caractère personnel, Paris, 2023.

EMY, J.: Le droit de ne pas être soumis au profilage par l'IA basé sur des données publiquement disponibles sans consentement éclairé explicite, (https://intelligence-artificielle.developpez.com/actu/358874/Recherche-Le-droit-de-ne-pas-etre-soumis-au-profilage-par-l-IA-base-sur-des-donnees-publiquement-disponibles-sans-consentement-eclaire-explicite-car-le-reglement-RGPD-de-l-UE-ne-garantit-pas-ce-droit/, E.T. 10/06/2024)

ERDOĞAN, Irmak: Otomatik Karar Çağında Hukuk: Avrupa Birliği Ve Türkiye'de Karşılaştırmalı Profilleme Düzenlemeleri (ed. Aksoy Retornaz, E.E. ve Güçlütürk, O.G.), "Gelişen Teknolojiler ve Hukuk II: Yapay Zekâ", 1. Baskı, İstanbul 2021, s. 373-389.

ERDOĞAN, Irmak: Yapay Zekâ ve Profilleme Teknolojilerinin Ceza Muhakemesinde Kişisel Veri İşlenmesine Etkisi, Ankara, 2022.

FISHER, Max ve TAUB, Amanda: *How YouTube Radicalized Brazil*, The New York Times, 11/08/2019, (*https://www.nytimes.com/2019/08/11/world/americas/youtube-brazil.html*, E. T. 20:05.2024)

GESLEVICH PACKIN, Nizan: *Disability Discrimination Using Artificial Intelligence Systems and Social Scoring: Can We Disable Digital Bias?*, Journal of International Comparative Law 2021, s. 487-512.

GROSJEAN, Alain: Le profilage: un défi pour la protection des données à caractère personnel, (ed. Grosjean, A.), "Enjeux européens et mondiaux de la protection des données personnelles", Bruxelles, 2015, s. 277-314.

Groupe de Travail « Article 29 »: *WP251, Lignes directrices relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE)2016/679*.

GUISSART, Elisabeth ve HENROTTE, Jean-François: *Profilage: la segmentation jusque dans le régime du RGPD*, PIN CODE 2020, S. 5, s. 10-18.

GÜÇLÜTÜRK, Osman: Yapay Zekâ ve Verinin Kullanımı, İstanbul, 2022.

GÜLTEKİN VARKONYİ, Gizem: Yapay Zekâ ve Kişisel Veriler: Teknoloji ve Hukuk Arasında Başka Bir Boyut, (https://www.cybermagonline.com/yapay-zek-ve-kisisel-veriler-teknoloji-ve-hukuk-arasinda-baska-bir-boyut, E. T. 10/06/2024)

HILDEBRANDT, Mireille: Defining Profiling: a New Type of Knowledge?, (ed. Hildebrandt M./Gutwirth S.) "Profiling the European Citizen, Cross-Disciplinary Perspectives", Dordrecht, 2008, s. 17-30.

HILDEBRANDT, Mireille: *Profiling: From data to knowledge*, Datenschutz und Datensicherheit – DuD, C. 30, S. 9, 2006, s. 548-552.

HOUD, Manel: "La protection des données personnelles et de la personne concernée par le consentement au traitement de données", Master de Droit du Numérique, Université Panthéon-Asas, Paris, 2022.

HUNEMAN, Philippe: Les Sociétés de profilage, Paris, 2023.

HUTTNER, Liane: La décision de l'algorithme, Etude de droit privé sur les relations entre l'humain et la machine, Paris, 2024.

JACOT-GUILLARMOD, Emilie: Le profilage à risque élevé de la nLPD : réflexions autour d'un monstre de Frankenstein, 24 août 2021, www.swissprivacy.law/86.

KAVAK GÜVEN, Neslihan: Avrupa Birliği Genel Veri Koruma Tüzüğü Doğrultusunda Profilleme Ve Otomatik Karar Alma, TOBB Ekonomi ve Teknoloji Üniversitesi Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi, Ankara, 2022.

Kişisel Verileri Koruma Kurumu: *Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler Rehberi*, 2018.

Kişişel Verileri Koruma Kurumu: "*Yapay Zekâ Alanında Kişisel Verilerin Korunmasına Dair Tavsiyeler*", (https://www.kvkk.gov.tr/Icerik/7048/Yapay-Zeka-Alaninda-Kisisel-Verilerin-Korunmasina-Dair-Tavsiyeler, E.T.10.05.2024).

KÜZECİ, Elif: Kişisel Verilerin Korunması, 4. Baskı, İstanbul, 2020.

KÜZECİ, Elif: Sayısal Fil, İstanbul, 2021.

LENS, Margot: "GDPR & Convention 108: Adequate Protection in A Big Data Era?,– LLM Law and Technology", Tilburg University, Tilburg, 2018.

METTALINOS, Nathalie: *Lignes directrices du G29 sur le profilage – Tentative de clarification sur le régime spécial applicable au profilage et à la prise de décision automatisée*, Communication commerce électronique, LexisNexis, février 2018, n° 2, comm. 14, s. 2

NİŠEVİĆ, Maja: Profiling Through Big Data Analytics, Antwerp, 2023.

ÖĞRETMEN KOTİL, Zeynep: Yapay Zekâ Teknolojilerinin Kişisel Verilerin Korunmasına Etkileri, Mevcut Problemler Ve Çözüm Önerileri, Bahçeşehir Üniversitesi Lisansüstü Eğitim Enstitüsü, Kamu Hukuku Anabilim Dalı, Yayımlanmış Yüksek Lisans Tezi, İstanbul, 2022.

POULLET, Yves : *Cinq ans après: le RGPD et les défis du profilage à l'heure de l'intelligence artificielle*, Revue des affaires européennes, S.1, 2021 s. 87-101.

POULLET, Yves ve FRÉNAY Benoit: Rapport et propositions de recommandations sur le Profilage et la Convention 108+ du Conseil de l'Europe, Strasbourg, 2019.

POULLET, Yves: L'IA un défi pour nos législations et notre vie privée, (ed. Epiney, A. ve Rovelli S.), "Künstliche Intelligenz und Datenschutz / L'intelligence artificielle et protection des données", Zurich, 2021, s. 20-42.

SOUSA E SILVA, Nuno: *The Artificial Intelligence Act: Critical Overview (July 30, 2024),* (SSRN: https://ssrn.com/abstract=4937150, E.T. 30/11/2024)

VERGNOLLE, Suzanne: "L'effectivité de la protection des personnes par le droit des données à caractère personnel", Yayımlanmamış Doktora Tezi, Université Panthéon-Assas, 2020.

VOIGT, Paul ve HULLEN, Nils: The EU AI Act Answers to Frequently Asked Questions, Berlin, Springer, 2024.

WALTER, Jean-Philippe: *La Convention 108, un complément nécessaire à l'article 8 de la CEDH à l'heure du numérique*, Civitas Europa 2022, C. 49, S. 2, s. 251-261.

YALÇINKAYA ÖZDAMAR, İrem: Büyük Veri Çağında Kişisel Verilerin Korunması: Avrupa Birliği Genel Veri Koruma Tüzüğü'nde Profilleme Ve Otomatik Karar Alma Düzenlemeleri, İstanbul Bilgi Üniversitesi Lisansüstü Programlar Enstitüsü, Yayımlanmamış Yüksek Lisans Tezi, İstanbul, 2022.

YAPAY ZEKÂ VE TEMEL VERİ KORUMA YÖNTEMLERİ

Prof. Dr. Yücel SAYGIN[*]

Doç. Dr. Ali İNAN[**]

Dr. Öğr. Üyesi Mehmet Emre GÜRSOY[***]

GİRİŞ

Yapay zekâ 1950'lerden itibaren önce fikir olarak ortaya atılmış ve bunu takip eden yıllarda üzerinde çalışılmaya başlanmış bir alan olarak hem bilim dünyasının hem de toplumun ilgi odağı olmuştur. Fikir olarak ortaya çıkmasından sonra inişli çıkışlı bir seyir izleyen yapay zekâ alanı son yıllarda geliştirilen ve toplumun kullanımına açılan sistemlerle büyük bir patlama yaşamıştır. Yapay zekâ sistemlerinin doğal dil arayüzleri ile kullanımı ve karmaşık metin bazlı sorulara verdikleri cevaplar ile birçok probleme getirdikleri çözümler kullanıcı sayısını hızla artırmıştır. Örneğin ChatGPT kullanıma açıldıktan iki ay sonra yüz milyon kullanıcıya ulaşmıştır[1]. 1950'lerde bir fikir olarak başlayan, sonrasında bu derece gelişmiş sistemlerin ortaya çıkmasını sağlayan iki şey vardır. Bunlardan birincisi donanım alanında ölçeklenebilir çözümlerdir. Nitekim Sinir Ağları ve bunların üzerinde öğrenme algoritmaları 1970'lerde geliştirilmiş ancak bunların yaygın etkileri ancak 2010'lu yıllarda görülmeye başlanmıştır. Öte yandan, ölçeklenebilir donanımdan daha da önemli olan şey büyük miktarda verinin toplanarak işlenmesidir.

[*] Sabancı Üniversitesi, Mühendislik ve Doğa Bilimleri Fakültesi, Bilgisayar Mühendisliği Bölümü

[**] Adana Alparslan Türkeş Bilim ve Teknoloji Üniversitesi, Bilgisayar ve Bilişim Fakültesi, Bilgisayar Mühendisliği Bölümü

[***] Koç Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü

[1] https://www.reuters.com/technology/chatgpt-sets-record-fastest-growing-user-base-analyst-note-2023-02-01/

Verinin yapay zekâ için önemini "ilk elden" öğrenmek için ChatGPT'ye şu soruyu İngilizce olarak sorduk: "Veri ile yapay zekâ arasındaki ilişki nedir?". ChatGPT'nin verdiği uzun cevabın ilk cümlesi şu olmuştur: "Veri ve yapay zekâ arasındaki ilişki temel ve simbiyotiktir". Yani veri ile yapay zekâyı karşılıklı fayda anlamında birbirinden ayırmamız mümkün değildir. Bu cümleyi takip eden cevap metninde ChatGPT yedi ana noktada cevabını detaylandırmıştır. Bu noktalardan birincisi "Veri yapay zekânın yakıtıdır" ifadesidir[2]. Bu ifadenin benzeri daha önce "Veri çağımızın petrolüdür" şeklinde Büyük Veri kavramını anlatırken sıklıkla kullanılmaktayken ChatGPT bunu yapay zekâya uyarlamış görünmekte. Nitekim makine öğrenmesi modellerinin temel girdisi veri olup gerek modellerin eğitilmesi gerekse modellerin doğrulama ve test aşamaları için önemli miktarda veri gerekmektedir. ChatGPT'nin verdiği cevapta ikinci nokta verinin yapısı ve bu yapının düzenli ya da düzensiz olması üzerinedir. Üçüncü nokta büyük veri kavramının kısa bir özeti niteliğinde olup bu iki alanın birbiri ile ne kadar iç içe geçtiğini göstermektedir. Bu kitap bölümünde de değineceğimiz konularla ilgili olan dördüncü noktada ChatGPT, verinin kalitesinin yapay zekâ modellerinin iyi performans göstermesi için önemini anlatmıştır. Nitekim mahremiyeti koruyan yöntemlerin uygulanması verinin kalitesini bozabileceği için mahremiyet ve faydanın dengelenmesi önemlidir. Bu kitap bölümünde mahremiyet ve fayda ilişkisi bağlamında veri kalitesi konusuna değineceğiz. Beşinci noktada ChatGPT yapay zekâ modellerinin yeni veri oluşturulması için kullanılmasıdır ki bu da simbiyotik ilişkinin açıklaması niteliğindedir. ChatGPT, nihayet altıncı noktada kitap bölümümüzün ana konusu olan yapay zekâ uygulamaları için toplanan verinin mahremiyet ve etik açısından endişe oluşturduğunu belirtip buna uygun veri yönetişimi, anonimleştirme ve GVKT gibi regülasyonlara uymanın bu endişeleri gidermek için vazgeçilmez olduğunu anlatmıştır.

Yapay zekâ için verinin önemini daha iyi kavrayabilmek için biraz daha detaylara girmek gerekir. Yapay zekâ altında birçok alt alan mevcuttur; bunlardan belki de en eskisi kural bazlı çıkarımlardır. Kural ile neden bahsettiğimiz bir örnek ile daha rahat anlaşılabilir. Çoğumuz online alışveriş yapmaktayız. 1994'te online kitap satmak için kurulan Amazon.com ilk aşamada başarısını müşterilerine uygun kitap tavsiyeleri vermeye borçludur. Mesela bir kitaba baktığımızda bu kitabı alanlar şu kitabı da aldılar gibi bir tavsiye basit kurallara dayanılarak oluşturulur. Bu kurallar ise

[2] The Economist: "Data is giving rise to a new economy" 6 Mayıs 2017

daha önceden alışveriş yapanların birlikte aldığı veya beğendiği ürünler üzerinden çıkarılır. Dolayısıyla daha önceki müşterilerin alışveriş verisi kullanılarak kurallara dayalı bir model oluşturulur. Müşteri verisi olmadan bu kuralları bulmamız mümkün değildir ve günümüzde etkileştiğimiz yapay zekâ modelleri kadar "akıllı" sayılamayacak bu kural bazlı tavsiye modeli dev bir firmanın doğmasına zemin hazırlamıştır. Kural bazlı bu basit görünen yapay zekâ modelinin yakıtı müşteri alışveriş verisidir.

Yine kural bazlı sistemleri temel alarak mahremiyeti koruyan yöntemlerin nerede ve nasıl gerekli olduğunu anlamaya çalışalım. Kuralları elde etmek için çok sayıda kullanıcının alışveriş bilgisine gerek vardır. Eğer bu verinin saklanması ve işlenmesi için yeterli altyapı ve bilgi birikimi varsa bu veri toplandığı firmada işlenebilir. Eğer firmanın böyle bir imkânı yoksa o zaman veri işleme ve veri madenciliği konusunda uzman bir firmanın bunu yapması gerekir. Nitekim günümüzde büyük firmalar bile bu tip veri işleme ve analitik servisleri bulut ortamında almayı tercih etmektedir. Ancak veri içinde kişisel bilgiler ve hassas veri mevcut ise o zaman bu verinin direkt olarak üçüncü kişilerle paylaşılması veri koruması açısından sorun teşkil eder. Bu veriyi kimlik bilgileri gibi tanımlayıcılardan arındırdığımızda sorunu çözmüş gibi görünsek de veri koruması ile ilgili problemler devam edebilir. Bunun sebebi paylaştığımız verinin gerçek kişileri başka veri tabanları ile eşleştirerek tespit edilmesine yol açabilecek yarı tanımlayıcılar içermesidir. Örneğin tavsiye sistemleri kararlarını alırken kişilerin yaşı, cinsiyeti, yaşadığı bölge ve eğitim durumu gibi bilgileri kullanarak daha doğru tavsiyeler oluşturabilir. Halbuki yaş, cinsiyet, adres bilgileri en tipik yarı tanımlayıcılardır. Bu veri içinde T.C. kimlik no, isim ve soy isim gibi direkt tanımlayıcılar olmasa bile insanların yaş, cinsiyet, adres kombinasyonu kullanılarak umuma açık kişisel bilgilerinin olduğu veri tabanları ile birebir eşleşebileceği araştırmacılar tarafından gösterilmiştir. Bu eşleşmeyi sınırlandırmak için de anonimleştirme standartları ve yöntemleri geliştirilmiştir. Bu kitap bölümünün ikinci kısmında anonimleştirme standartları silsilesi ve ilgili standartlara ulaşabilmek için veri üzerinde ne gibi işlemler yapılması gerektiği detaylandırılmıştır. Anonimleştirme çalışmalarında temel hedef veri kalitesini mümkün olduğunca korurken anonimleştirme için gerekli işlemlerin yapılmasıdır. Örneğin tablolar halinde organize olmuş veride k-anonimlik standardına ulaşmak için yarı tanımlayıcıları aynı olan satırların sayısının en az k tane olmasını sağlamaktır. Mesela verinin 5-anonim olmasını istiyorsak ve verimiz için yarı tanımlayıcılar cinsiyet ve yaş ise, o zaman cinsiyet ve yaş değerleri aynı olan satırları

grupladığımızda her grupta en az 5 satır olmasını sağlamak gerekir. Bunun için yarı tanımlayıcılar üzerinde genelleştirme işlemi yapılır, bunu yaparken de veriyi en az genelleştirme ile 5-anonim hale getirmeye çalışmamız gerekir ki veri sonucunda geliştireceğimiz uygulamalar yeterince doğru sonuçlar elde edebilsin.

Veri anonimleştirme 2000'li yılların başından itibaren üzerinde uzun süre çalışılmış, ancak güçlü saldırgan ve arka plan bilgisi her zaman halihazırda geliştirilmiş anonimleştirme standartlarının ve yöntemlerinin güçlendirilmesi ihtiyacını doğurmuştur. Bu kitap bölümünde hâlihazırda literatürde bulunan anonimleştirme standartları anlatılmıştır ancak anonimleştirme ile ilgili araştırma çalışmaları sonrasında ulaşılan temel sonuç, veri ya da veri üzerinde çalışan herhangi bir algoritmanın sonucunun her zaman bir mahremiyet sorunu doğuracağı olmuştur. Dolayısıyla anonimleştirme standartları ve bunları sağlayan algoritmalar bir yere kadar mahremiyet sağlamaktadır ve her zaman bir mahremiyet riski bulunur. Bu sonuca istinaden veriden bağımsız ama veri üzerinde çalışan algoritmalara bağlı bir standart olan diferansiyel mahremiyet ortaya atılmıştır. Diferansiyel mahremiyet standardını ortaya atan araştırmacılar, veri tabanı sistemleri alanından gelip anonimleştirme konusunda çalışan araştırmacılardan farklı olarak kriptografi camiasından gelmektedir; dolayısıyla anlamsal mahremiyet garantisi sağlamayı amaçlamışlardır. Temel olarak diferansiyel mahremiyetin önerdiği çözüm, veriyi kesinlikle paylaşmamak ve hatta veri üzerinde çalışan algoritmaların sonuçlarını da belli bir çerçevede gürültü ekleyerek sonuçların tek bir kişinin verisinden bağımsız olmasını sağladıktan sonra paylaşmaktır. Yine burada algoritmaların sonuçlarının kalitesi ile mahremiyet arasında bir denge güdülmesi gerekmektedir. Diferansiyel mahremiyet veri tabanından bağımsız, ama ilgili algoritmaya bağlı olduğu için çok farklı alanlarda araştırmacılar hali hazırda kullandıkları teknikleri diferansiyel mahremiyet standardına uyarlayarak bu alanın farklı camialarda yaygınlaşmasını sağlamışlardır.

Yukarıdaki paragraflarda verinin tek elde toplandığını ve bu varsayım çerçevesinde mahremiyet ile ilgili neler yapılabileceğini kısaca özetledik. Öte yandan birçok senaryoda verinin üretildiği yerde saklanması mahremiyet ile ilgili sebeplerden dolayı tercih edilmektedir. Büyük miktarda veriye ihtiyaç duyan derin öğrenme algoritmaları ise ihtiyaç duydukları istatistikleri lokal veriden alarak global parametrelerini bu istatistiklere göre ayarlayabilirler. Bunun için verinin kendisine değil sadece veriden elde edile-

cek istatistiklere ihtiyaç vardır ve verinin merkezi bir sunucuda tutulmasına gerek yoktur. Lokal veriden alınan istatistikler verinin tümü sunucudaymış gibi kuralların bulunması, ya da verinin merkezi sistemde bulunduğu haldekine yakın doğrulukta modellerinin eğitilmesi için kullanılabilir. Bu şekilde model oluşturmaya federe öğrenme diyoruz. Federe öğrenme nispeten yeni bir terim olsa da temelinde verinin dağıtık ortamda bulunduğu durumda makine öğrenmesi ve veri madenciliği vardır. Yine kural bazlı tavsiye modellerine dönersek, mesela aynı şeyleri satan marketler müşteri verisini kendi veri tabanlarında tutabilir ama müşterilerin sıklıkla birlikte aldıkları ürünleri global olarak tüm veri tek bir veri tabanında tutuluyor gibi bulmak isteyebilir. Ancak buna gerek olmadan her market kendi veri tabanında sıklıkla alınan ürünlerin, ya da ürün kümelerinin istatistiklerini toplayıp veriyi paylaşmadan sadece kuralları ve istatistikleri bir koordinatör market ile paylaşır. Koordinatör de tüm istatistikleri topladıktan sonra global istatistikleri ve global olarak sık alınan ürün gruplarını diğer marketlerle paylaşabilir. Koordinatör dahil tüm marketlerin protokolü izlediği farz edilen bu tip yöntemler ile verinin paylaşılmasına gerek olmadan sadece istatistikler paylaşmak ve bu istatistiklerin koordinatörde birleştirilmesi yolu ile kurallar elde edilir. Federe öğrenme yöntemleri daha çok derin öğrenme modellerinin gerektirdiği büyük miktarda verinin bir sunucuya toplanmasına gerek olmadan öğrenilmesi esasına dayanır. Federe öğrenmenin temelleri bu kitap bölümünde anlatılmaktadır.

Federe öğrenme, verinin olduğu gibi başkaları ile paylaşılmamasından dolayı belli bir mahremiyet sağlamaktadır. Ancak hatırlayalım ki veriyi paylaşmasak bile, veriden elde edilecek istatistikler de mahremiyet sorunlarına yol açabilir. Dolayısıyla federe öğrenme tek başına mahremiyet ile ilgili bir standart ya da garanti sunmaz. Bunun için federe öğrenmenin gerektirdiği istatistiksel girdilerin de diferansiyel mahremiyete uygun bir şekilde gürültü eklenerek modele verilmesi gerekir. Diferansiyel mahremiyeti sağlayan federe öğrenme yöntemleri de bu kitap bölümünde anlatılmaktadır.

Tekrar yeni nesil yapay zekâ modellerine dönersek, direkt olarak doğal dil yolu ile iletişim kurabilen, doğal dil işleme ve yapay zekayı harmanlayarak ortaya çıkan bu sistemler toplumda yapay zekânın kapasitesi ve ileride olabilecek gelişmelerin etkisi konusunda önemli tartışmalara sebebiyet vermiştir. Bu tartışmalar sansasyonel denebilecek "bilgisayarlar dünyayı ele geçirecek" gibi korkulara kadar varmaktadır. Ancak bu bölümde bizim asıl üzerinde duracağımız konu biraz daha nüans içeren mahremiyet ko-

nusudur. Çoğu insan yapay zekâya temel girdi olan verinin kişisel veri olduğundan ve bunların etkisinden çok haberdar değildir. Örneğin Büyük Dil Modelleri (LLM) metinler üzerinde eğitilmekte ve bu metinler insanlar hakkında özel bilgiler içerebilmektedir. Diğer bir konu ise LLM ile etkileşim sırasında insanlar özel bilgilerini ifşa edecek sorular sormakta ve bu soruların LLM sistemi tarafından saklanıp tekrar kullanılma ihtimalini göz önüne almamaktadır. Nitekim benzer bir konu web arama motorlarında uzun süre tartışılmıştır, çünkü insanlar aramalarında kişisel bilgilerini kullanabilmekte ve kimlik bilgilerini açığa çıkaracak ipuçlarını arama motorlarına sunmaktadır. Arama motorları da bu bilgileri kendi sistemlerini iyileştirmek için kullanmak üzere saklamaktadır. Nitekim mahremiyet ile ilgili skandallardan bir tanesi American Online firması tarafından kullanıcı aramalarının kullanıcı adı ya da IP adresleri olmadan umuma açılması sonucu olmuştur. Düzenli olmayan, anahtar kelimelerden oluşan bu veri kümesi daha sonradan geri çekilmiştir ancak yine de bu büyük bir skandalı engelleyememiştir. Araştırmacı gazetecilerden biri sadece aramalarına bakarak Georgia'da bir kadına ulaşmış ve aramalarının kendisine ait olduğuna dair bir teyit almıştır. Arama motorlarında kullanıcıların gönderdiği sorgu kelimeleri saklanmaktadır. Bu verinin anonimleştirilmesi konusunda tartışmaların sonucunda aslında AOL veri salımı sonrasında bunun mümkün olmadığı sonucu çıkmıştır (SIGIR AOL paper). LLM'lerdeki problem benzer ancak kapsam olarak daha ciddidir, çünkü insanlar LLM'leri ile daha yakın bir ilişki içinde kullanmakta ve dolayısıyla çok daha mahrem olabilecek konularda bilgi vermektedir.

I. KİŞİSEL GİZLİLİK KORUMA YÖNTEMLERİ

A. İSTATİSTİKSEL VERİ TABANI KORUMASI

Kişisel gizliliğin korunmasına yönelik yaklaşımlar 6698 sayılı Kanun ve GVKT benzeri kanunların yürürlüğe girmesinden çok önce, 1970'li yıllarda çeşitli araştırmalara konu olmuştur. Henüz "kişisel gizlilik" terimi literatüre girmediğinden, ilgili çalışmalar "istatistiksel veri tabanı koruması" kapsamında değerlendirilmiştir. Bu bakış açısına göre, birçok kişinin kayıtlarını barındıran bir veri tabanı istatistiksel analiz amacıyla üçüncü şahısların erişimine açılacak, ancak bu analistlerin veriyi ham hali ile görmesi (dolayısıyla kişi boyutunda incelemesi) engellenecektir. Bu problem tanımının günümüz mahremiyeti koruyucu veri madenciliği tanımı ile benzerliği dikkat çekici seviyededir.

Adam ve Worthmann'ın[3] hazırlamış olduğu literatür taraması istatistiksel veri tabanı koruması yaklaşımlarını ayrıntılı olarak ele almaktadır. Şekil 1'de 3 temel yaklaşım genel hatları ile özetlenmektedir. Şekil 1(a)'da yer verilen sorgu kısıtlama yaklaşımına göre analist istatistiksel veri tabanına herhangi bir sorguyu iletebilir. Ancak veri tabanı ham veri çekmeye yönelik sorguları cevaplamayacaktır. Filtrelenmeyen sorgulara verilen cevaplar olduğu gibi – ilave koruma önlemi uygulanmaksızın – analiste aktarılmaktadır. Bu yaklaşımın temel varsayımı, analistin sorgu koşullarını detaylandırarak tek bir hedef kişiye ulaşma imkânına sahip olmadığıdır. Koruma seviyesinin Bölüm 2(d)'de değinilecek takma ad ve maskeleme yaklaşımlarına benzer olduğu değerlendirilebilir. Bölüm 2(b)'de açıklanan yarı-tanımlayıcı niteliklerin erişilebilirliği bu yaklaşımın temel zayıflığı olacaktır. Nitekim, analist yarı-tanımlayıcı nitelik değerlerini bildiği kişileri kolaylıkla hedef alabilir ve ham veri elde edebilir. Örnek olarak şu sorguyu ele alalım:

```
SELECT AVERAGE(Maaş) FROM Personel_bilgileri WHERE Birim = "Yazı İşleri" AND Yaş = 40 AND Cinsiyet = "Erkek" AND Eğitim = "Lisansüstü"
```

Bu sorgunun cevabı ortalama maaş bilgisi içereceği için sorgu istatistikseldir ve veri tabanı tarafından cevaplanacaktır. Eğer sorgu koşulunda yer alan şartları sağlayan tek bir kişi var ise, veri tabanından dönen *ortalama* maaş bu kişinin maaşıdır ve aslında ham veriye erişilmektedir.

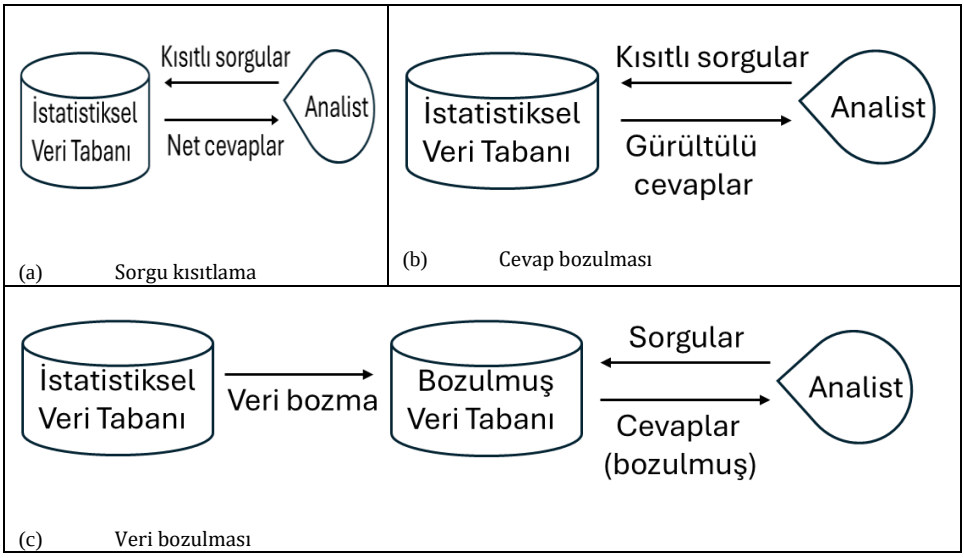
Şekil 1(b)'de cevap bozulması (İng., output perturbation) adı verilen yaklaşıma yer verilmiştir. Analist Şekil 1(a)'da olduğu gibi sadece istatistiksel bilgileri toplayabilir. Ancak bu filtreye ek olarak ve Bölüm 2(c)'de detaylandırılacak diferansiyel mahremiyet yaklaşımına benzer şekilde, hesaplanan istatistiksel değerlere gürültü eklenir ve gürültülü cevaplar analiste iletilir.

Şekil 1(c)'de veri bozulması (İng., data perturbation) yaklaşımları aktarılmaktadır. İstatistiksel veri tabanı anonimleştirme benzeri çeşitli yöntemler ile bozularak farklılaştırılır ve güvenli hale getirilir. Analist ham veri temini dahil olmak üzere her türlü sorguyu iletebilir, ancak bu sorgular bozulmuş veri tabanı üzerinden cevaplanacaktır ve elde edilen cevaplar istatistiksel veri tabanının döneceği cevaplardan farklı olabilir.

---

[3] Adam, N. R. ve Wortman, J. C.: *Security-control methods for statistical databases*. ACM Comput. Surv. 21(4): 515–556, 1989.

Temel yaklaşımlara dair özetlerden anlaşılacağı üzere, günümüz kişisel gizlilik koruma yöntemlerinin kökleri büyük oranda istatistiksel veri tabanlarının korunmasına yönelik önlemlere dayanmaktadır. Ancak günümüz şartlarının pek çok farklılık barındırdığını da ifade etmek gerekir. Bunlardan bazıları şu şekildedir: (i) verinin ve analizlerin dağıtıklaşması, (ii) istatistiksel analiz yerine makine öğrenmesi / yapay zekâ yaklaşımlarının takip edilmesi, (iii) kişisel verinin hacminin ve çeşitliliğinin artması (ör. çoklu ortam verisi, konum-zaman işaretli veri, yapısal olmayan veri vb.).



Şekil 1. İstatistiksel veri tabanı koruması yaklaşımları. İngilizce aslı: Adam ve Wortmann[4].

B. ANONİMLEŞTİRME

Anonimleştirme çözümleri bir veri kümesi içerisindeki kayıtlar ile bu kayıtların bağlı olduğu kişiler (ilgili kişiler) arasındaki bağı geri döndürülemez şekilde kopartmaya çalışan, niceliksel koruma garantisi temin edebilen yaklaşımlardır.[5] Bu nitelikleri itibariyle anonimleştirme sürecine tabi

[4] Adam, N. R. ve Wortman, J. C.

[5] Kişisel Verileri Koruma Kurumu: "Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Rehberi", (https://www.kvkk.gov.tr/yayinlar/K%C4%B0%C5%9E%C4%B0SEL

tutulan veriler, kişisel gizlilik korumasına yönelik yasal mevzuat tarafından imha edilmiş sayılır ve üçüncü şahıslar ile paylaşılması mümkündür.

Anonimlik tanımları:

Paylaşılacak (anonimleştirilmiş) verinin sağlaması gereken şartlar parametrik olarak tanımlanmış, bu sayede niceliksel koruma garantisi temin eden "anonimlik tanımı" ile ifade edilmektedir. Literatürde k-anonimlik[6], l-çeşitlilik[7], t-yakınlık[8] vb. pek çok farklı anonimlik tanımı yer almaktadır. Her tanım, belirli yetenekler ile donanmış bir saldırgana karşı koruma sağlayacak şekilde tasarlanmıştır.

K-anonimlik tanımı, önerilen ilk tanım olması ve yalınlığı itibariyle en yaygın kullanılan tanımlardandır. Sweeney kamuoyu ile paylaşılacak veri kümelerinde yer alan T.C. kimlik numarası, telefon numarası, e-posta adresi gibi tanımlayıcı niteliklerin yer aldığı sütunların silinmesinin yeterli olmadığını göstermiştir.[9] Tanımlayıcıların silinmesi ilgili kişi ile kayıt arasındaki bağı zayıflatmakta ancak tamamen ortadan kaldırmamaktadır. "Yarı-tanımlayıcı" adı verilen nitelik kümesi ile belirli hedeflere ait kayıtların tespit edilmesi riski göz önünde bulundurulmalıdır.

Yarı-tanımlayıcı nitelik kümesi içinde yer alan nitelikler kendi başına bir kaydı işaret etmekte yeterli olmayan, ancak bir arada kullanıldığında kayıt-kişi ilişkisini yüksek başarı ile kurmaya yarayan niteliklerdir. Tablo 1'de sol tarafta bir hastane veri kümesi örneği sunulmaktadır. Bu örnek üzerinde açıklamak gerekirse, bir kişinin ikamet ettiği posta kodu pek çok kayıt için tekrar edecektir – aynı posta kodunu kullanan birçok kişi vardır, bu nitelik tanımlayıcı değildir. Tabloda yer alan 1, 4, 9 ve 10. satırlarda yer alan kayıtlar 13053 posta kodu ifade etmektedir. Yaş ve milliyet bilgisi

---

%20VER%C4%B0LER%C4%B0N%20S%C4%B0L%C4%B0NMES%C4%B0,%20YOK%20ED%C4%B0LMES%C4%B0%20VEYA%20ANON%C4%B0M%20HALE%20GET%C4%B0R%C4%B0LMES%C4%B0%20REHBER%C4%B0.pdf, E.T.:02.06.2024).

6 Sweeney, L.: *k-anonymity: A model for protecting privacy.* International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 10(5): 557–570, 2002-a.

7 Machanavajjhala, A., Kifer, D., Gehrke, J. ve Venkitasubramaniam, M.: *l-diversity: Privacy beyond k-anonymity.* ACM Transactions on Knowledge Discovery from Data (TKDD), 1(1): art. 3, 1–52, 2007.

8 Li, N., Ll, T. ve Venkitasubramaniam, S.: "t-closeness: Privacy beyond kanonymity and l-diversity," in IEEE 23rd International Conference on Data Engineering. IEEE, 106–115, 2007.

9 Sweeney, 2002-a.

benzer bir yapıdadır – aynı yaşta ve aynı milliyetten olan birçok kişi vardır. Bu 3 nitelik tekil olarak tanımlayıcı değilken, üçü bir ara kullanıldığında bir yarı-tanımlayıcı oluşturur ve olası saldırganlara hedefledikleri kişilerin kayıtlarını tespit etme olanağı sağlar. Sweeney[10] ABD'de {doğum tarihi, posta kodu, cinsiyet} niteliklerinin yarı-tanımlayıcı olarak kullanılması halinde tüm toplumun %87'sine ait kayıtların tekil olarak belirlenebildiğini deneysel olarak göstermiş, hatta bir hastane tarafından Tablo 1'e benzer şekilde paylaşılan veri kümesi içerisinde Massachusetts valisinin sağlık kayıtlarını tespit ederek saldırıların kolaylığını ortaya koymuştur. ABD özelinde bu problem özellikle dikkat çekicidir, nitekim oy hakkı olan bütün vatandaşlara ait {doğum tarihi, posta kodu, cinsiyet} bilgileri periyodik olarak seçmen kütükleri içerisinde kamuoyu ile paylaşılmaktadır. Saldırganın tek yapması gereken seçmen kütüklerindeki yarı-tanımlayıcı ile hastane veri kümesindeki yarı-tanımlayıcıyı eşleştirmekten ibarettir.

K-anonimlik tanımı (i) tüm tanımlayıcı niteliklerin silinmesini ve (ii) her kaydın yarı-tanımlayıcı nitelikler üzerinde (k-1) farklı kayıt ile ayırt edilemez hale getirilmesini gerektirir. Tanımın ikinci gereksinimde ifade edilen yarı-tanımlayıcı üzerinde ayırt edilemezlik sağlanan ve en az k büyüklüğünde olan kayıt gruplarına "denklik sınıfı" (İng., equivalence class) adı verilir. Bir kaydın yarı-tanımlayıcı bilgisine sahip olan saldırgan ilgili kaydın denklik sınıfını bulabilecek, ancak bu kayıt grubu içerisinde hedefine ait olan kaydı tespit edemeyecektir.

Tablo 1'de sağ taraftaki tablo incelenirse, bu tablonun {posta kodu, yaş, milliyet} yarı-tanımlayıcısına karşı 4-anonimlik şartını sağladığı görülecektir. 3 ayrı denklik grubu vardır ve bunlar sıra numaralarına göre kayıt 1-4, 5-8 ve 9-12'yi içermektedir. Her denklik sınıfı en az 4 kayıt içerir ve sınıf içindeki kayıtlar yarı-tanımlayıcı nitelikler ile ayırt edilemez.

[10] Sweeney, 2002-a.

***Tablo 1**. Ham hastane verisi (sol), 4-anonimleştirilmiş hastane verisi (sağ). İngilizce aslı: Machanavajjhala vd.*[11]

	Hassas değil (Yarı tanımlayıcı)			Hassas
	Posta kodu	Yaş	Milliyet	Hastalık
1	13053	28	Rus	Kalp rah.
2	13068	29	Amerikalı	Kalp rah.
3	13068	21	Japon	Viral enf.
4	13053	23	Amerikalı	Viral enf.
5	14853	50	Hint	Kanser
6	14853	55	Rus	Kalp rah.
7	14850	47	Amerikalı	Viral enf.
8	14850	49	Amerikalı	Viral enf.
9	13053	31	Amerikalı	Kanser
10	13053	37	Hint	Kanser
11	13068	36	Japon	Kanser
12	13068	35	Amerikalı	Kanser

	Hassas değil (Yarı tanımlayıcı)			Hassas
	Posta kodu	Yaş	Milliyet	Hastalık
1	130**	< 30	*	Kalp rah.
2	130**	< 30	*	Kalp rah.
3	130**	< 30	*	Viral enf.
4	130**	< 30	*	Viral enf.
5	1485*	≥ 40	*	Kanser
6	1485*	≥ 40	*	Kalp rah.
7	1485*	≥ 40	*	Viral enf.
8	1485*	≥ 40	*	Viral enf.
9	130**	3*	*	Kanser
10	130**	3*	*	Kanser
11	130**	3*	*	Kanser
12	130**	3*	*	Kanser

Görüleceği üzere k-anonimlik tanımı tamamen denklik sınıflarının büyüklüğüne odaklanmıştır. Denklik sınıfları ise sadece yarı-tanımlayıcı nitelik değerlerine göre kurulur. Tablonun diğer nitelikleri tanımın ve sürecin dışında tutulmaktadır. Machanavajjhala vd.'nin önerdiği l-çeşitlilik tanımı bu yaklaşımın risklerine işaret etmektedir.[12]

l-çeşitliliğe göre tanımlayıcı, yarı-tanımlayıcı niteliklere ek olarak "hassas" niteliklere de odaklanılmalıdır. Hassas nitelikler, ilgili kişinin öğrenilmesinden rahatsız olacağı veya zarar göreceği nitelikler olarak tanımlanmaktadır. Tablo 1'deki hastane verisi için "Hastalık" niteliği bu hassas bir niteliktir. Bu nitelik kişinin hastaneyi ziyaret sebebini göstermektedir ve ilgili kişi için hastalık değerinin bulaşıcı olması toplumdan dışlanma, ölümcül olması ise sağlık sigortasına erişimin engellenmesi gibi riskler barındırabilir. Denklik sınıflarının kurulması aşamasında, hassas nitelik değerlerinin açığa çıkmasını engellemek için önlem alınmalıdır.

11 Machanavajjhala, A., Kifer, D., Gehrke, J. ve Venkitasubramaniam, M.

12 Machanavajjhala, A., Kifer, D., Gehrke, J. ve Venkitasubramaniam, M.

Tablo 1'de sağ tarafta yer alan tablo 4-anonimlik şartını sağlamaktadır, ancak 9-12 sıra numaralı kayıtları içeren 3. denklik sınıfı incelenirse görülecektir ki tüm hastalar kanserdir. Hassas nitelik üzerinde çeşitlilik sağlanmalıdır. Daha ilginç (ve kısmen zorlama) bir diğer örnekte ise Machanavajjhala vd. 3. numaralı kaydın durumunu irdelemektedir.[13] İlgili kayıt Japondur. Bu kişiyi tanıyan ve veriyi paylaşan hastaneyi ziyaret ettiğini bilen bir komşusu, posta kodu, yaş ve milliyet değerlerine göre anonimleştirilmiş kaydın sahibinin 1. denklik sınıfında olduğunu tespit edecektir. Denklik sınıfı 2 hassas nitelik barındırmaktadır: viral enfeksiyon ve kalp rahatsızlığı. Saldırgan, Japonların kalp rahatsızlığı yatkınlığının düşük olmasından hareketle komşusunun viral enfeksiyon sebebiyle hastaneye gittiğini tahmin edebilecektir. Çeşitlilik sağlanırken niceliksel bir koruma temin edecek şekilde hassas nitelik değerlerinin dağılımı gözetilmelidir.

l-çeşitlilik tanımı ile ifade edilen bu çeşitliliği ölçmek için farklı çözümler önerilmiştir: hassas nitelik değerlerinin bilgi içeriği (İng., information content), baskın değerin özyinelemeli ağırlığı veya en basit şekli ile görülen farklı değerlerin sayısı.

l-çeşitlilik tanımından k-anonimlik tanımına geçişte anonimliği ihlal etmeyi amaçlayan saldırgana dair model detaylandırılmış, daha donanımlı bir saldırgan modeli ortaya konulmuştur. Anonimlik tanımı öneren sonraki çalışmalar da benzer bir yol izlemektedir. Örneğin t-yakınlık tanımı[14], hassas niteliklerin denklik sınıfı içerisindeki dağılımı ile tüm tablodaki dağılımı arasındaki farkı saldırganın avantajı olarak görür ve bu avantajı sınırlandırmaya odaklanır. Takip eden daha da karmaşık tanımlara dair detaylara Fung vd.'nin[15] ve Majeed ve Lee'nin[16] güncel literatür taramalarında yer verilmektedir.

Anonimleştirme yöntemleri:

---

13 Machanavajjhala, A., Kifer, D., Gehrke, J. ve Venkitasubramaniam, M.

14 Li, N., Ll, T. ve Venkitasubramaniam, S.

15 Fung, B. C. M., Wang, K., Chen, R. ve Yu, P.S.: *Privacy-preserving data publishing: A survey of recent developments*. ACM Comput. Surv. 42(4): art. 14, 1-53, 2010. https://doi.org/10.1145/1749603.1749605

16 Majeed, A. ve Lee, S.: *Anonymization Techniques for Privacy Preserving Data Publishing: A Comprehensive Survey*. IEEE Access, 9: 8512-8545, 2021, https://doi.org/10.1109/ACCESS.2020.3045700

Anonimlik tanımları bir tablonun veya veri kümesinin yayınlanmaya uygun olup olmadığını ifade etmektedir. Elinde ham veri bulunan bir veri sorumlusu hangi tanımın kullanılacağını (k-anonimlik, l-çeşitlilik vb.) ve bu tanıma ait koruma seviyesini (k, l vb.) belirlemelidir. Buna ek olarak, denklik sınıflarının nasıl oluşturulacağının, hangi kayıtların aynı denklik sınıfına dâhil edileceğinin belirlenmesi gereklidir. Bu süreç, k-anonimlik tanımından bağımsız olarak ele alınabilecek bir problemdir ve "anonimleştirme yöntemi" adı verilen algoritmalar ile çözülür.

Bir anonimlik tanımını (ör. k-anonimlik) karşılamak için tercih edilebilecek pek çok farklı anonimleştirme yöntemi bulunmaktadır (ör. DataFly[17], TDS[18], Incognito[19]). Aynı ham veri kümesi altında farklı yöntemler kullanıldığında farklı anonimleştirilmiş veri kümeleri üretilecektir. Nitekim her anonimleştirme yöntemi belirli bir kalite ölçütünü veya algoritmik karmaşıklığı önceleyecek şekilde tasarlanmıştır. Burada dikkat edilmesi gereken husus, durağan bir veri kümesi için kamuoyu ile bu verinin en çok 1 anonim halinin paylaşılmasıdır. Aksi takdirde farklı anonim versiyonların birleştirilmesi ile saldırılar gerçekleştirilmesi mümkün olacaktır[20].

Durağan olmayan, güncellenen veya akan verinin anonimleştirilmesi hem tanım hem de yöntem bakımından zorluklar barındırmaktadır[21]. Anonimleştirme yaklaşımı ile ilgili diğer problemler ise şu şekilde özetlenebilir: ilişki halindeki birden çok tablonun anonimleştirilmesi[22]; bazı niteliklerin

---

17 Sweeney, L.: *Achieving k-anonymity privacy protection using generalization and suppression*. Int. J. Uncertain. Fuzziness Knowl.-Based Syst. 10(5): 571–588, 2002-b. https://doi.org/10.1142/S021848850200165X

18 Fung, B. C. M., Wang, K. ve YU, P. S.: "Top-down specialization for information and privacy preservation," 21st International Conference on Data Engineering (ICDE'05), Tokyo, Japan, 205-216, 2005.

19 LeFevre, K., DeWitt, D. J. ve Ramakrishnan, R.: "Incognito: efficient full-domain K-anonymity". In Proceedings of the ACM SIGMOD international conference on Management of data (SIGMOD '05). Association for Computing Machinery, New York, NY, USA, 49–60, 2005.

20 Cao, J., Carminati, B., Ferrari, E. ve Tan, K. L.: *CASTLE: Continuously Anonymizing Data Streams*. IEEE Transactions on Dependable and Secure Computing, 8(3): 337-352, 2011, https://doi.org/10.1109/TDSC.2009.47

21 Cao, J., Carminati, B., Ferrari, E. ve Tan, K. L.

22 Nergiz, M. E., Clifton, C. ve Nergiz, A. E.: *Multirelational k-Anonymity*. IEEE Transactions on Knowledge and Data Engineering, 21(8): 1104-1117, 2009, https://doi.org/10.1109/TKDE.2008.210

hem yarı-tanımlayıcı, hem hassas olması durumu[23]; hiyerarşik nitelik türleri üzerinde anonimleştirme[24].

C. DİFERANSİYEL MAHREMİYET

Pek çok farklı anonimlik tanımının ortaya konulması ve bu tanımların hemen her biri için tanımın kişisel gizlilik koruması temin etmekte yetersiz kaldığı bir saldırgan modelinin ortaya konulabilmesinden hareket eden Dwork,[25] oldukça teorik bir yaklaşım ile anonimleştirme ve benzeri yaklaşımların "anlamsal gizlilik" (İng., semantic privacy) arayışını sorgulamıştır. Söz konusu kavram, siber güvenlik alanındaki "anlamsal güvenlik"[26] kavramından hareketle türetilmiştir.

Bir şifreleme yönteminin anlamsal güvenlik özelliği barındırıp barındırmadığı saldırgana karşı oynanan bir oyun ile belirlenir. Bu oyunda saldırgana iki açık metin ve bir şifreli metin sunulur. Saldırgandan şifreli metnin hangi açık metnin şifreli hali olduğunu tahmin etmesi istenir. Saldırganın sınırsız hesaplama gücü ve hesaplama süresi olduğu varsayılır. Bu şartlar altında, saldırganın doğru cevap verme ihtimalinin %50'yi geçemeyeceği şifreleme yöntemlerinin anlamsal olarak güvenli olduğu söylenir – şifreli metin açık metne dair hiçbir ipucu içermemektedir, şifreli metinden bir bitlik bilgi (soldaki veya sağdaki açık metnin şifrelenmesi) dahi çıkartılamamaktadır.

Dwork, benzer bir oyunu kişisel gizlilik koruması yöntemleri için derler ve bu oyunda başarılı olmanın mümkün olmadığını gösterir.[27] Her koruma yöntemine karşı başarısı sınırlandırılamayacak seviyede yüksek bir arka plan bilgisine sahip saldırgan bulunacaktır. Buna göre, şifreleme yöntemle-

---

23 Wong, K. S., Tu, N. A., Bui, D. M., Ooi S. Y. ve Kim M. H.: "Privacy-Preserving Collaborative Data Anonymization with Sensitive Quasi-Identifiers," 12th CMI Conference on Cybersecurity and Privacy (CMI), Copenhagen, Denmark, 1-6, 2019.

24 Özalp, I., Gürsoy, M. E., Nergiz, M. E. ve Saygın Y.: *Privacy-Preserving Publishing of Hierarchical Data*. ACM Trans. Priv. Secur. 19(3): art. 7, 1-29, 2016. https://doi.org/10.1145/2976738

25 Dwork, C.: Differential Privacy, (ed.. Bugliesi, M., Preneel, B., Sassone, V., Wegener, I.), Automata, Languages and Programming. ICALP 2006. Lecture Notes in Computer Science, vol 4052. Springer, Berlin, Heidelberg, 2006.

26 Sako, K.: Semantic Security. In: van Tilborg, H.C.A., Jajodia, S. (eds) Encyclopedia of Cryptography and Security. Springer, Boston, MA, 2011.

27 Dwork, C.

rinin aksine, kişisel gizlilik koruması problemi için anlamsal bir koruma mümkün değildir.

Bu bulgudan hareket ile diferansiyel mahremiyet adı verilen ve anonimleştirme yöntemlerinden çok farklı bir şekilde tanımlanan ve uygulanan yaklaşım önerilmiştir. Diferansiyel mahremiyet veriye erişim olduğu sürece ihlalin kaçınılmaz olacağı varsayımı ile geliştirilmiştir. Koruma yöntemlerinin amacı olası tüm ihlalleri engellemek yerine bunların ilgili kişilere yönelik olası zararlarının etkilerini sınırlandırmak olmalıdır. Bu amacı formüle etmek için birbirinden sadece 1 kayıt üzerinde farklı olan herhangi iki veri kümesi D_1 ve D_2, bu veri kümelerine iletilen istatistiksel sorguları rastgele gürültü ekleyerek cevaplayan bir mekanizma M, mekanizmanın cevap kümesi S ve gizlilik parametresi olan ε kullanılır. Öyle ki, ε-diferansiyel mahremiyeti sağlaması için M mekanizması şu eşitsizliği garanti etmelidir:

$$Pr\,[M(D_1) \in S] \leq e^{\varepsilon} \times Pr[M(D_2) \in S]$$

Eşitsizlik birbirlerinden tek kayıtta farklılık gösteren D_1 ve D_2 veri kümelerinin rastgele mekanizma M altında aynı cevabı üretme ihtimalini sınırlandırmaktadır. İki olasılık en fazla e^{ε} kadar farklı olabilir. ε küçüldükçe bu fark azalır, koruma miktarı artar. İlgili kişiler kayıtlarını mekanizma M ile korunan veri kümelerine emanet etmekten çekinmemelidir, çünkü bu mekanizma ilgili kayıtları sadece veri kümesinde bulunmamaları halinde de yaşanacak ihlallere karşı koruyamaz, diğer tüm ihlallere karşı güvenlidir.

M mekanizmasının Şekil 1(b)'de cevap bozulması adı altında tartışılan yaklaşımların bir devamı olduğu görülecektir. İstatistiksel sorgu cevaplarına eklenecek gürültünün örneklendiği dağılım mekanizmanın adını belirlemektedir.

Laplace mekanizma: Sorgulara eklenecek gürültü "sorgu kümesi L_1 hassasiyeti" (İng., query set L_1 sensitivity) adı verilen bir değere bağlıdır. Bir sorgu kümesinin L_1 hassasiyeti, ε-diferansiyel mahremiyetinde ifade edilen ve tek bir kayıtta birbirlerinden farklı olan "kardeş" veri kümeleri D_1 ve D_2 üzerinde tanımlanır. Herhangi iki kardeş veri seti üzerinde tek kaydın sorgu cevapları üzerinde yaratabileceği en yüksek mutlak değer farklarının toplamı bu sorgu kümesinin L_1 hassasiyetidir. Hassasiyet Δ ile ifade edilir ve tek kayda fazla bağımlı sorgular kümelerinde yüksek, az bağımlı sorgu kümelerinde ise düşük ölçülmesi beklenir.

Sorgu kümesi hassasiyetini belirlemek diferansiyel mahremiyeti Laplace mekanizma ile kullanmanın en temel zorluğudur. Nitekim, hassasiyet değeri Δ'nın belirlenmesi NP-zor bir problemdir.[28] Bu zorluğun aşılması halinde, Laplace mekanizma, sorgu cevaplarına gürültü eklerken ortalaması 0, varyansı ise en az Δ/ε olan Laplace dağılımında gürültü çeker. Her sorgunun cevabı diğerlerinden bağımsız olarak gürültü ile korunur.

Üstel mekanizma: Medyan, en küçük, en büyük değer gibi sıralama istatistiklerinin veya en sık tekrar eden değerin Laplace mekanizma ile sorgulanması cevaplara yüksek miktarda gürültü eklenmesi sebebiyle makul bir yaklaşım değildir. Üstel mekanizma bu zorluğu aşmak amacıyla önerilmiştir.

Üstel mekanizma bir sorgunun her olası cevabına bu cevabın kalitesini ifade eden nümerik bir skor atanmasını gerektirir. Bu kalite fonksiyonu *D* veri kümesi üzerinde hesaplansın ve olası *r* cevabı için *q(D,r)* ile gösterilsin. Her bir cevabın seçilme olasılığı üstel dağılımda şu şekilde hesaplanır:

$$e^{\frac{\varepsilon \times q(D,r)}{2\Delta q}}$$

En yüksek olasılığa sahip değer sorgu cevabı olarak döndürülür. Bu formülde Δq değeri kalite fonksiyonunun hassasiyetini ifade eder ve sorgu kümesi hassasiyetine benzer şekilde tanımlanır – tek kayıtlık değişikliğin sorgu kümesi cevaplarına etkisi yerine kalite fonksiyonuna etkisi kullanılarak hesaplanır. Üstel mekanizmayı kullanmanın temel zorluğu da Δq değerinin hesaplanmasıdır. Üstel mekanizma $(2\varepsilon\Delta q)$-diferansiyel mahremiyet sağlar.

Diğer diferansiyel mahremiyet tanımları: ε-diferansiyel mahremiyet yukarıdaki mekanizmalar ile kullanıldığında pek çok analiz için aşırı korumacı davranmakta, gürültü miktarı sorgu cevabını bastırmaktadır. Bu sebeple diferansiyel mahremiyetin yumuşatılmış tanımlarının kullanılması gündeme gelmiştir.

Gauss mekanizma bunun bir örneğidir, ilgili tanım (ε,δ)-diferansiyel mahremiyet olarak anılmaktadır ve D_1 ve D_2 veri kümelerinin cevap olasılıklarının e^{ε} sınıra ek olarak δ kadar farklılık göstermesine izin verdiği için yumuşatılmış bir tanımdır. ε-diferansiyel mahremiyet için δ = 0 olmalıdır.

[28] Xiao, X. ve Tao, Y.: *Output perturbation with query relaxation.* Proc. VLDB Endow., 1(1): 857–869, 2008. https://doi.org/10.1145/1453856.1453949

Gauss mekanizmada gürültü, ortalaması 0 olan bir Gauss dağılımında seçilir. Dağılımın varyansı ise ε, δ ve sorgu kümesinin L_2 hassasiyetine bağlı olarak belirlenir. L2 hassasiyet hesaplanırken tüm kardeş veri kümeleri üzerinde tek kayıtlık değişimin sorgu cevaplarında yaratacağı kare farkların toplamının kare-kökü kullanılır.

Bir diğer örnek ise hassasiyet hesabının herhangi iki kardeş veri kümesi yerine sorgunun iletildiği *D* kümesinin kardeşleri üzerinde cevaplanmasıdır. İlk durum global hassasiyet olarak tanımlanırken, *D* veri kümesinin kardeşleri üzerinde hesaplanan hassasiyet değerine ise lokal hassasiyet denilmektedir. Tahmin edileceği üzere lokal hassasiyet her zaman global hassasiyetten düşüktür, belirli sorgu türleri için (örneğin ortalama) iki hassasiyet hesabı önemli seviyede farklılık gösterecektir.

D. ALTERNATİF TANIMLAR VE FARKLARI

Bu bölümde yasal olarak anonimleştirme tanımına girmeyen "alternatif" koruma tanımları sunulacak, güçlü ve zayıf yönleri örnekler ile açıklanacaktır.

Kişisel veri anonimleştirme yaklaşımının bilgisayar ağları alanında kullanılan "anonimleştirme" kavramı ile karıştırılması yaygın karşılaşılan bir hatadır. Bilgisayar ağlarında anonimleştirme süreci bir kullanıcıya veya ağ varlığına ait IP numarası, MAC adresi, e-posta adresi gibi tanımlayıcı değerlerin takma adlar (İng., pseudonym) ile değiştirilmesine karşılık gelmektedir. Örneğin "john.doe@abc.com" adlı eposta adresi sadece ilgili sunucudaki kullanıcıyı gizlemek amacıyla "X@abc.com", hem kullanıcıyı hem de e-posta sunucusunu gizlemek amacıyla *Y* takma adı ile ifade edilebilir. Takma adlar *X* ve *Y*, karşıladığı değerin kriptografik bir özütü, rastgele seçilmiş bir tanımlayıcı metin veya bir sayaç tarafından üretilmiş sayısal bir değer olabilir. Takma ad üretmek için pek çok farklı yaklaşım mevcuttur[29]. Takma adlar ile ifade ettikleri gerçek tanımlayıcı değerler arasındaki eşleştirmeler (İng., mapping) depolandığı takdirde, takma adlar geri döndürülebilir bir yaklaşımdır. Bu sebeple takma ad kullanımının KVKK kapsamında (kişisel veri) anonimleştirme gereksinimlerini karşılamadığı açık şekilde belirtilmiştir.[30] GVKT ise takma ad ve şifreleme tabanlı yaklaşımları

[29] ENISA: "Pseudonymisation Techniques and Best Practices", (https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices, E.T.:02.06.2024).

[30] Kişisel Verileri Koruma Kurumu: "6698 Sayılı Kişisel Verilerin Korunması Kanunu Hakkında Doğru Bilinen Yanlışlar - 2", (https://www.kvkk.gov.tr/Icerik/7151/6698-Sayili-Kisisel-Verilerin-Korunmasi-Kanunu-Hakkinda-Dogru-Bilinen-Yanlislar-2, E.T.: 02.06.2024), s. 29.

sadece veri işleme sürecinin güvenliğini temin etmek amacıyla[31] veya kamusal, bilimsel veya tarihi araştırmaları desteklemek amacıyla arşivleme sürecinde[32] desteklemektedir.

Bu yaklaşımda aynı ilgili kişiye ait olan tüm kayıtlar aynı takma ad ile ifade edilir ve bu sayede kişi-bazlı ağ ve trafik analizi gerçekleştirilebilir. Pek çok analiz için tanımlayıcıların veya takma adların veriden tamamen kaldırılması veriden elde edilebilecek faydayı ortadan kaldırmaktadır. Bu sebeple, Avrupa Birliği Siber Güvenlik Ajansı 2019 yılında çeşitli tanımlayıcı değerlerin nasıl işleneceğine yönelik detaylı bir kılavuz hazırlamıştır[33]. Aynı kılavuz, olası saldırı senaryolarını da içermektedir. Başlıca saldırılar kaba kuvvet saldırısı, sözlük araması ve tahminleme şeklinde sıralanmıştır. Kılavuzun 8. bölümünde ise daha karmaşık saldırı senaryolarına yer verilmektedir.

Niceliksel koruma sağlamakta zorlanılan bir diğer alan ise doğal dil ile ifade edilmiş metinler üzerinde kişisel gizlilik korumasıdır. Kişi ve kurumlar referanslarının veya bunlara ait tanımlayıcı nitelikteki (kısaltma, adres, telefon vb.) değerlerin maskelenmesi temel yaklaşımlar arasındadır. Maskeleme çözümünde gizlenmek istenen değerler tamamen veya kısmen (ör. adres bilgisi için il seviyesine kadar) karartılır, erişilemez hale getirilir. Örneğin finans sektöründe kurum çalışanlarının müşteriye ait kredi kartı bilgilerinin tamamı yerine son 4 hanesini görebilmesi, kimlik doğrulama süreçlerinde T.C. kimlik numarası veya anne kızlık soyadı benzeri verilerin belirli hanelerinin kullanılması kısmi maskeleme örnekleridir. 6698 sayılı Kanun ve GVKT içerisinde maskeleme yaklaşımları yer almamakla birlikte, bu uygulamaların veri işleme sürecinin güvenliğini temin etmek amacıyla kullanılması mümkündür.[34]

Derin öğrenme ve üretken yapay zekâ alanlarındaki güncel gelişmeler doğal dil verisine olan talebi önemli ölçüde artırmıştır. Büyük dil modelleri eğitim aşamasında yüksek hacimde doğal dil verisine ihtiyaç duyar. Veri-

31 GVKT-a, Madde 32: "*Security of processing*", (https://gdpr-info.eu/art-32-gdpr/, E.T.:02.06.2024).

32 GVKT-b, Madde 89: "*Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes*", (https://gdpr-info.eu/art-32-gdpr/, E.T.: 02.06.2024).

33 ENISA

34 GVKT-a, Madde 32

nin maskeleme uygulanmaksızın eğitim süreçlerine dahil edilmesinin, kullanıcı sorguları yoluyla gizlilik ihlallerine sebep olabileceği gösterilmiştir. Bu sebeple metinsel verinin korunması aşamasında maskelemenin önemi son yıllarda artmaktadır.

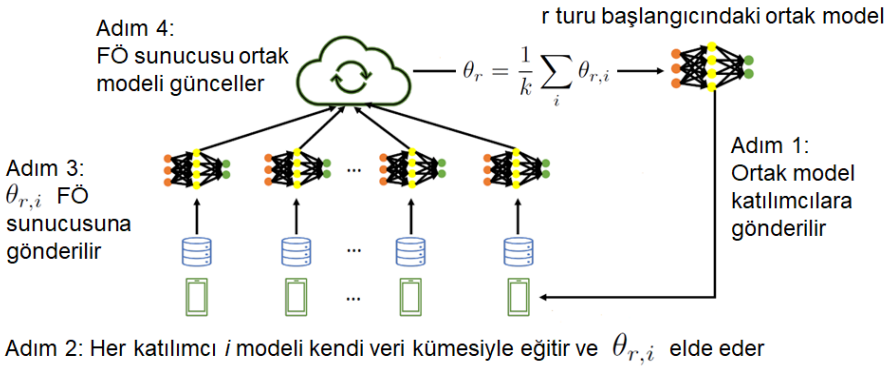
Metinsel verinin elle işlenmesi yoluyla maskelenecek bölgelerin tespit edilmesi hem çok fazla el emeği gerektirir, hem de sürece insan hatası ekler. Bunu engellemek için isimli varlık tanıma (İng., named entity recognition) çalışmalarından faydalanmak mümkündür. Geçmişte düzenli ifadeler (İng., regular expression) ve sözlükler kullanarak çözülen varlık tanıma problemi son yıllarda makine öğrenmesi yaklaşımları ile çözülmeye çalışılmaktadır.

II. FEDERE ÖĞRENME VE KİŞİSEL GİZLİLİK ETKİLERİ

A. FEDERE ÖĞRENME

Federe öğrenme (FÖ), birden fazla katılımcının birbirleriyle verilerini paylaşmalarına gerek kalmadan ortak bir makine öğrenmesi modelini eğitmelerini sağlayan bir yöntemdir. Geleneksel makine öğrenmesinde model eğitilmesi için verilerin merkezi bir sunucuda toplanmasına ihtiyaç varken, FÖ sayesinde katılımcıların verileri kendi cihazlarında kalmakta, ortak bir model dağıtık biçimde eğitilmektedir. Böylece FÖ, veri gizliliğinin korunması, veri paylaşımının azaltılması ve katılımcıların hesaplama gücünden faydalanılması gibi önemli avantajlara sahiptir. İlk olarak McMahan vd. tarafından ortaya atılan FÖ[35], Google Gboard, Apple QuickType ve Siri gibi ürünlerle hayatımıza girmiş; Tensorflow Federated, IBM Federated Learning ve Intel OpenFL gibi açık kaynak kodlu kütüphaneler vesilesiyle de yatırıma ve gelişimine devam etmektedir. Günümüzde sağlık, finans, eğitim, haberleşme gibi birçok sektör ve araştırma alanında FÖ tabanlı uygulamalar önerilmektedir.

35 McMahan, Brendan, Eider Moore, Daniel Ramage, Seth Hampson, and Blaise Aguera y Arcas. "Communication-efficient learning of deep networks from decentralized data." In *Artificial Intelligence and Statistics*, pp. 1273-1282. PMLR, 2017.



Şekil 1: *Klasik federe öğrenme mimarisi ve adımları*

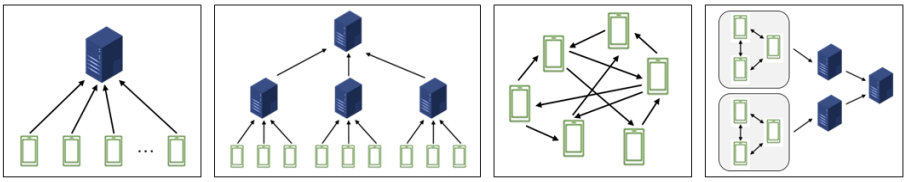
Klasik bir FÖ mimarisi ve adımları Şekil 1'de gösterilmiştir. Bu mimaride bir FÖ sunucusu katılımcıların organizasyonu ve orkestrasyonunu sağlamaktadır (Şekil 1'de bulut ile simgelenmiştir). Katılımcıların her birinin kendi cihazlarında verileri mevcuttur. FÖ, tur tur ilerleyen iteratif bir süreçtir. Örneğin, r turunda olduğumuzu varsayalım ve turun başlangıcındaki ortak modeli (bir önceki turun sonunda elde edilmiş olan model) θ_{r-1} olarak gösterelim. r turunda alınan aksiyonlar dört adımda özetlenebilir:

- Adım 1: FÖ sunucusu, ortak model θ_{r-1}'i katılımcılara gönderir.
- Adım 2: Her katılımcının kendi cihazında veri kümesi vardır. Katılımcılar, diğer katılımcılardan bağımsız olarak, kendi veri kümeleriyle modeli eğitirler. Bu eğitimin sonunda, i katılımcısı r turu sonunda güncellenmiş lokal model olan $\theta_{r,i}$'yi elde eder.
- Adım 3: Katılımcılar, güncellenmiş lokal modelleri $\theta_{r,i}$'yi FÖ sunucusuna gönderirler. Burada önemli olan nokta, her katılımcının verileri diğerlerinden farklı olduğu için, her katılımcının $\theta_{r,i}$'sinin içeriği de diğer katılımcılardan farklıdır. Bir diğer deyişle, herhangi üç farklı katılımcı i = 1, 2, 3 için $\theta_{r,1} \neq \theta_{r,2} \neq \theta_{r,3}$ durumu mevcuttur.
- Adım 4: FÖ sunucusu, tüm katılımcılardan gelen lokal modelleri toplar ve bu lokal modelleri kullanarak ortak modeli günceller. Güncelleme için kullanılan en temel yöntem, "Federated Averaging" olarak bilinen, tüm lokal modellerin ortalamasının alınması yöntemidir.

4. adımın sonundaki ortak model, r turu sonundaki yani r+1 turunun başındaki ortak model θ_r olmaktadır. Bir sonraki tur olan r+1 turunda yuka-

rıdaki dört adım tekrarlanacak ve model eğitimi tur tur devam edecektir. Yeteri sayıda turun ardından yüksek doğruluğa sahip bir ortak model ortaya çıkar.

Her ne kadar klasik FÖ mimarisi Şekil 1'deki gibi olsa da günümüzde FÖ birçok farklı senaryo ve mimaride uygulanabilmektedir. Örneğin, Şekil 1'deki mimarinin önemli bir alt kırılımı, "cross-silo" ("silolar-arası") ve "cross-device" ("cihazlar-arası") federe öğrenme ayrımıdır. Silolar-arası FÖ'de verinin az sayıda (örn. 2-20 arası) veri ambarında bulunduğu ve her veri ambarının bir katılımcı olduğu varsayılır. Bu senaryo, katılımcıların nispeten büyük boyutlu organizasyonlar olduğu durumlarda (örneğin hastane, eğitim kurumu, vb.) geçerlidir. Öte yandan cihazlar-arası FÖ'de ise binlerce veya on binlerce mobil cihaz kullanılarak FÖ yapılır. Bu senaryo, akıllı telefonlar, dizüstü bilgisayarlar, akıllı ev cihazları gibi cihazlardaki veriler kullanılarak FÖ yapılmak istendiğinde geçerlidir. Silolar-arası ve cihazlar-arası FÖ'de katılımcı başına düşen veri miktarı, katılımcıların hesaplama gücü, katılımcı müsaitliği gibi yönlerden önemli farklılıklar bulunmaktadır.



Şekil 2: *Farklı FÖ mimari örnekleri*

Günümüzde kullanılan farklı FÖ mimarilerinden bazıları Şekil 2'de örneklendirilmiştir. Şekil 1'de yer alan mimari, Şekil 2'deki merkezi sunuculu FÖ mimarisine denk gelmektedir. Bu mimari FÖ'nün en temel ve en yaygın mimarisidir. Bu mimaride katılımcılar doğrudan merkezi FÖ sunucusu ile iletişim halindedirler. Öte yandan hiyerarşik FÖ'de ise, katılımcılar ve ana FÖ sunucusu arasında bir veya daha fazla ara sunucu katmanları bulunur. Ara katmanlardaki sunucular, kendilerine bağlı olan katılımcılardan aldıkları modelleri bir üst katmana iletirler. Hiyerarşik FÖ, katılımcı sayısının çok yüksek olduğu durumlarda, tüm katılımcıların tek bir sunucuyla iletişime geçmesi yerine birden fazla sunucudan paralel şekilde yararlanılması amacıyla tercih edilmektedir. Şekil 2(c)'de görülen eşler arası FÖ mimarisinde ise FÖ sunucusu bulunmamakta, katılımcıların doğrudan birbirleriy-

le iletişim kurarak model eğitmeleri sağlanmaktadır. Katılımcıların birbirlerine güvendikleri ama güvenilir bir sunucu bulamadıkları durumda eşler arası FÖ mimarisi tercih edilebilir. Son olarak, Şekil 2(d)'de küme-bazlı FÖ mimarisi örneklendirilmiştir. Bu mimaride katılımcılar kendi aralarında küçük kümeler oluşturarak model eğitirler, ardından her kümenin kendi içinde eğittiği model FÖ sunucuları ile paylaşılır. FÖ sunucuları, farklı kümelerden aldıkları modelleri birleştirerek ortak bir model oluşturur.

FÖ mimarilerinin her biri, ölçeklenebilirlik, veri gizliliği, hata toleransı, iletişim maliyetleri gibi yönlerden farklı avantaj ve dezavantajlara sahiptir. Uygun mimari seçimi, FÖ'nün uygulandığı senaryonun gereksinim ve kısıtlamalarına bağlıdır.

B. FEDERE ÖĞRENME İLE İLGİLİ ZORLUKLAR

Federe öğrenme her ne kadar gizliliği arttırıcı bir teknoloji olarak hayatımıza girmiş olsa da hem tüm FÖ mimarilerinde geçerli olan, hem de bazı FÖ mimarilerinde daha çok hissedilen birçok zorluk ve açık araştırma sorusunu içinde barındırmaktadır. Doğru FÖ mimarisi seçilirken veya yeni bir FÖ uygulaması kurulurken, potansiyel zorluklar göz önünde bulundurularak seçim yapılması faydalı olacaktır. FÖ kullanımında sıkça rastlanılan zorluklar ve üzerinde çalışılan araştırma sorularından yaygın olanlar aşağıda özetlenmiştir.

Dengesiz ve heterojen veri dağılımları: Bazı FÖ katılımcıları, diğer katılımcılara göre daha çok veya daha az veriye sahip olabilir. Bazı katılımcıların elindeki veri, diğer katılımcıların verisinden farklı özellikler içerebilir. Bu gibi dengesiz ve/veya heterojen veri dağılımı durumlarında katılımcıların ortak FÖ modeline etkisi birbirlerinden daha az/fazla veya birbirlerine zıt yönlerde olabilmekte, dolayısıyla ortak FÖ modelinin yakınsamaması veya düşük doğruluğa sahip olması gibi sorunlar ortaya çıkabilmektedir. Model güncelleme algoritmasının değiştirilmesi veya FÖ mimarisinin değiştirilmesi gibi yöntemlerle ortak modelin yakınsaması sağlanmalıdır.

Hesaplama gücü: Öncelikle, FÖ'de model eğitimi işi katılımcılar tarafından yapıldığından, katılımcı cihazlarının uygun yazılım ve donanım ekipmanına sahip olmaları gerekir. Ek olarak, eğitilen modeller büyük olduğunda, bu modellerin saklanması ve eğitilmesi batarya ve hafıza problemlerine sebebiyet verebilmektedir. Bu durum genellikle silolar-arası FÖ'de sorun teşkil etmese de düşük kaynaklı ve düşük güce sahip cihazlarla (örn. gö-

mülü sistemler, nesnelerin interneti cihazları) cihazlar-arası FÖ yapılmak istendiğinde kritik bir engel olarak ortaya çıkmaktadır. Ayrıca, kullanılan FÖ mimarisine göre, merkezi FÖ sunucularının veya ara katmanlardaki sunucuların farklı hesaplama güçlerine veya bağlantı kotalarına sahip olmaları gerekmektedir. Dolayısıyla, mimari seçimi yapılırken, FÖ'nün ihtiyaçlarına uygun özelliklere sahip katılımcıların ve sunucuların bulunup bulunmadığı dikkate alınmalıdır.

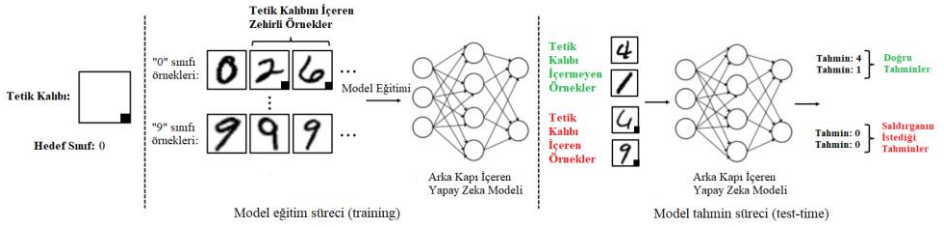
Haberleşme maliyeti: Ortak bir model eğitilirken, kullanılan mimariye göre değişmekle birlikte, katılımcılar arası ve/veya katılımcı-sunucu arası sıkça model parametrelerinin gönderilmesi gerekmektedir. Bu alışveriş ve haberleşmenin sağlanması için cihazların aktif ve güvenilir bağlantı becerilerinin olması şarttır. Ayrıca, katılımcı sayısının veya model boyutlarının yüksek olduğu durumlarda haberleşme maliyeti de artmaktadır. Bağlantı kotalarının bulunduğu durumlarda FÖ, kotaların hızla tüketilmesine sebebiyet verebilir. Bu sorunların önüne geçilmesi için, haberleşme maliyetini düşüren algoritma ve mimarilerin geliştirilmesi gerekmektedir.

Ölçeklenebilirlik ve katılımcı müsaitliği: Çok katılımcılı dağıtık sistemlerin tümünde olduğu gibi, FÖ'de de ölçeklenebilirlik sorunu ön plana çıkmıştır. Örneğin, coğrafi açıdan geniş bir alana yayılmış binlerce cihaz kullanılarak FÖ yapılması istendiğini varsayalım. Bu cihazların tümünün simultane olarak aktif ve güvenilir bir bağlantıya sahip olduğu anı yakalamak gerçekçi değildir. Cihazlar, erişim problemleri, bağlantı problemleri, şarj problemleri gibi problemler yaşayabilir. Bu problemlere rağmen FÖ'nün sorunsuz işlemesi için arızaya toleransı olan, asenkron FÖ yöntemleri geliştirilmektedir.

C. FEDERE ÖĞRENME İLE İLGİLİ RİSKLER VE SALDIRILAR

FÖ sayesinde ortak makine öğrenmesi modeli eğitilirken kullanıcı verilerinin paylaşılmasına gerek olmamakta, her kullanıcının verisi kendi cihazında kalmaktadır. Bu sebeple FÖ, kişisel verinin korunması, veri gizliliğinin sağlanması ve veri paylaşımının minimize edilmesi yönlerinden önemli avantajlar getirmektedir. Öte yandan, FÖ'nün doğal olarak dağıtık mimarilere sahip bir teknoloji olmasının getirdiği riskler ve potansiyel saldırılar göz ardı edilmemelidir. Şayet bir dağıtık sistem, art niyetli kullanıcılar, sunucular veya üçüncü kişiler tarafından yapılan saldırılara maruz kalabilir. FÖ literatüründe ön plana çıkmış olan riskler ve saldırıların bazıları şunlardır.

Zehirleme saldırıları: Zehirleme saldırılarında bir veya birden fazla art niyetli katılımcı, ortak FÖ modelini bozmak amacıyla (örn. modelin yakınsamasını engellemek veya model doğruluğunu düşürmek) FÖ sunucusuna art niyetli (zehirli) $\theta_{r,i}$ parametreleri gönderirler. Özellikle katılımcı sayısının yüksek olduğu ve katılımcıların tümüne güvenilemediği, cihazlar-arası FÖ senaryosunda gerçekçi bir saldırıdır. Zehirleme saldırıları, veri zehirlemesi ve model zehirlemesi olarak iki alt kategoriye ayrılır. Veri zehirlemesinde saldırgan, cihazındaki eğitim verisini manipüle ederek zehirli $\theta_{r,i}$ parametrelerinin elde edilmesini amaçlar[36]. Kullanıcıların cihazlarındaki veriler genellikle kendi kontrollerinde olduğu için veri zehirlemesi yapmak nispeten kolaydır. Öte yandan model zehirlemesi saldırısında saldırgan, veriyi manipüle etmek yerine doğrudan $\theta_{r,i}$ parametrelerini manipüle eder. Bu manipülasyonu yapan saldırganın teknik açıdan daha bilgili ve becerikli olduğu varsayılır, şayet model eğitim algoritmasını veya lokal çıktı olan $\theta_{r,i}$ parametrelerini manipüle edebilmesi ve saldırı doğrultusunda nasıl manipüle etmesi gerektiğini bilmesi gerekir. Ancak model zehirlemesi saldırılarının çok daha etkili olabildikleri literatürde gösterilmiştir[37].



Şekil 3: *Bir arka kapı saldırısı örneği*

Arka kapı saldırıları: Arka kapı saldırılarında, art niyetli katılımcılar veri manipülasyonu veya parametre manipülasyonu yaparak ortak FÖ modeline bir "arka kapı" enjekte etmeye çalışırlar. Saldırıdan etkilenen FÖ modeli normal zamanda doğru biçimde çalışmaya devam ederken, arka kapı saldırısının tetik kalıbını gördüğünde ise saldırganların programladığı şekilde

36 Tolpegin, Vale, Stacey Truex, Mehmet Emre Gursoy, and Ling Liu. "Data poisoning attacks against federated learning systems." In *the 25th European Symposium on Research in Computer Security, ESORICS 2020, Guildford, UK, September 14–18, 2020, Proceedings, part i 25*, pp. 480-501. Springer International Publishing, 2020.

37 Fang, Minghong, Xiaoyu Cao, Jinyuan Jia, and Neil Gong. "Local model poisoning attacks to Byzantine-Robust federated learning." In *29th USENIX Security Symposium (USENIX Security 20)*, pp. 1605-1622. 2020.

davranır. Örnek bir arka kapı saldırısı, Şekil 3'te gösterilmiştir. Diyelim ki saldırgan tetik kalıbı olarak görüntülerin sağ alt köşesine siyah bir kutu eklemiş olsun ve saldırganın hedefi bu tetik kalıbını içeren tüm görüntülerin "0" sınıfı olarak tahmin edilmesini sağlamak olsun. Örneğimizde saldırgan, bazı katılımcıların eğitim verilerini manipüle ederek tetik kalıbını içeren örnekler eklemektedir. Şekil 3'te görüldüğü üzere, 2 ve 6 rakamlarının sağ alt köşesinde tetik kalıbı mevcuttur ve bu örneklerin sınıfı "0" olarak belirtilerek katılımcı verilerine eklenmiştir. Bu örneklerle eğitilen FÖ modeli, tetik kalıbını da öğrenmekte, dolayısıyla arka kapı içeren bir model haline dönüşmektedir. Arka kapı içeren model, tetik kalıbı içermeyen örnekleri tahmin etmesi istendiğinde doğru tahminlerde bulunur. Fakat tetik kalıbı içeren örnekleri tahmin etmesi istendiğinde, saldırganın istediği tahminlerde (Şekil 3'teki örnek için "0" tahmininde) bulunur.

Katılımcı verileri katılımcı kontrolünde olduğu ve FÖ sunucusu tarafından denetlenemediği için, zehirleme ve arka kapı saldırıları FÖ'de geleneksel (merkezi) makine öğrenmesine kıyasla daha büyük tehdit teşkil etmektedir. Literatürde farklı yöntemler kullanılarak etkili arka kapı ve zehirleme saldırıları yapılabildiği gösterilmiştir[38][39].

Üyelik çıkarımı saldırıları: FÖ sunucusu veya katılımcıları art niyetli olmasalar da birbirlerinin verileri hakkında çıkarımlarda bulunmaya çalışabilirler. İlk bakışta, FÖ'de katılımcı verileri kendi cihazlarında kaldığı için verinin tamamen güvende olduğu düşünülebilir, fakat bu bir yanılgıdır. Şayet katılımcılar verilerini paylaşmasa bile, verileriyle eğitilmiş olan $\theta_{r,i}$ modellerini diğer katılımcılar ve/veya FÖ sunucusu ile paylaşmaktadırlar. Dolayısıyla, $\theta_{r,i}$'yi gören meraklı bir FÖ katılımcısı veya sunucusunun $\theta_{r,i}$ üzerinden başka katılımcının verisi hakkında çıkarımda bulunmaya çalışması mümkündür. Bu çıkarım saldırılarından biri üyelik çıkarımı saldırısıdır. Üyelik çıkarımı saldırısında, saldırgan spesifik bir veri noktasının bir katılımcının veri kümesinde bulunup bulunmadığını (katılımcının veri kümesinin üyesi olup olmadığını) öğrenmeyi hedefler. Örneğin, FÖ katılımcılarının hastaneler olduğunu ve katılımcı veri kümelerinin hasta verilerinden

38 Gong, Xueluan, Yanjiao Chen, Qian Wang, and Weihan Kong. "Backdoor attacks and defenses in federated learning: State-of-the-art, taxonomy, and future directions." *IEEE Wireless Communications* 30, no. 2 (2022): 114-121.

39 Bagdasaryan, Eugene, Andreas Veit, Yiqing Hua, Deborah Estrin, and Vitaly Shmatikov. "How to backdoor federated learning." In *International Conference on Artificial Intelligence and Statistics*, pp. 2938-2948. PMLR, 2020.

oluştuğunu varsayalım. Saldırgan, X kişisinin verisinin, katılımcı veri kümelerinde olup olmadığını ve hangi katılımcının veri kümesinde olduğunu öğrenmeyi hedefler. Böylece, eğer saldırı başarılı olursa saldırgan X kişisinin hangi hastanede tedavi gördüğünü öğrenecektir. Üyelik çıkarımı saldırılarının hem merkezi öğrenmede hem de FÖ'de geçerli bir tehdit olduğu literatürde gösterilmiştir[40].

Gradyan evirme ve veri rekonstrüksiyon saldırıları: Model parametreleri üzerinden çıkarım yapmayı hedefleyen diğer saldırılar arasında, gradyan evirme ve veri rekonstrüksiyon saldırıları popüler olan saldırılardandır. Bu saldırılarda saldırgan, model parametrelerini gözlemler ve parametreleri kullanarak katılımcı verilerini sıfırdan inşa etmeye çalışır. Saldırıların gerçekleştirilmesinde genellikle optimizasyon bazlı yöntemler kullanılmaktadır. Örneğin, Şekil 1'deki mimariyi ele alalım ve saldırganın FÖ sunucusu olduğunu varsayalım. Saldırgan, turun başında katılımcıya gönderdiği θ_{r-1}'i bilmektedir. Ardından, katılımcı güncellediği $\theta_{r,i}$'yi sunucuyla paylaştığı için saldırgan $\theta_{r,i}$'yi de görmektedir. Saldırganın kurduğu optimizasyon problemi, girdi θ_{r-1} olduğunda çıktının en yüksek ihtimalle $\theta_{r,i}$ olmasını sağlayan veri kümesini inşa etmektir. Bu saldırılar ile görüntü ve metin türündeki veri kümelerinin detaylı biçimde inşa edilebildiği gösterilmiştir[41,42].

D. FEDERE ÖĞRENMEDE KİŞİSEL GİZLİLİK VE GÜVENLİK KORUMA YÖNTEMLERİNİN UYGULANMASI

Bir önceki bölümde örneklendirilen risk ve saldırılara karşı korunmak adına FÖ'de gizlilik ve güvenlik koruma yöntemlerinin kullanılması faydalı olacaktır. FÖ'de kullanılabilecek olan koruma yöntemleri birkaç kategoride incelenebilir:

Kriptografik yöntemler: Katılımcılar homomorfik şifreleme ve güvenli çok taraflı hesaplama (secure multi party computation) gibi kriptografik yöntemler kullanarak gönderdikleri modellerin gizli kalmasını sağlayabilirler.

---

40 Nasr, Milad, Reza Shokri, and Amir Houmansadr. "Comprehensive privacy analysis of deep learning: Passive and active white-box inference attacks against centralized and federated learning." In *2019 IEEE Symposium on Security and Privacy (SP)*, pp. 739-753. IEEE, 2019.

41 Zhu, Ligeng, Zhijian Liu, and Song Han. "Deep leakage from gradients." *Advances in Neural Information Processing Systems* 32 (2019).

42 Huang, Yangsibo, Samyak Gupta, Zhao Song, Kai Li, and Sanjeev Arora. "Evaluating gradient inversion attacks and defenses in federated learning." *Advances in Neural Information Processing Systems* 34 (2021): 7232-7241.

Bu yöntemlerde model parametreleri şifrelendikten sonra diğer katılımcılar ve/veya FÖ sunucusuyla paylaşılır ve FÖ şifreli modeller üzerinden yapılır. Kriptografik yöntemler, üyelik çıkarımı, gradyan evirme ve veri rekonstrüksiyonu gibi çıkarım yapmayı hedefleyen saldırılara karşı etkilidir. Ancak, kriptografik yöntemlerin getirdiği önemli bir zorluk hız kaybıdır. Kriptografik yöntemler kullanmadan dakikalar içinde tamamlanabilen bir FÖ işi, bu yöntemler kullanıldığında saatler hatta günler sürebilmektedir.

Diferansiyel mahremiyet: FÖ'de hem diferansiyel mahremiyet hem de lokal diferansiyel mahremiyetin kullanılması mümkündür. Aralarındaki fark, mahremiyet sağlayıcı gürültünün hangi adımda eklendiğidir. Eğer gürültü, katılımcı model parametreleri toplandıktan sonra FÖ sunucusu tarafından eklenirse, bu diferansiyel mahremiyet kullanımına tekabül edecektir. Öte yandan gürültü, kullanıcı model parametrelerini göndermeden evvel kullanıcı tarafından eklenirse, bu lokal diferansiyel mahremiyet kullanımına tekabül edecektir. Modele eklenen gürültü üyelik çıkarımı ve rekonstrüksiyon saldırıları gibi saldırıları zorlaştırmakta, diferansiyel mahremiyet (veya lokal diferansiyel mahremiyet) gibi güçlü ve kanıtlanabilir bir mahremiyet garantisinin elde edilmesini sağlamaktadır. Ancak bu yöntemin ana dezavantajı, eklenen gürültünün model doğruluğunu olumsuz etkilemesidir.

Dayanıklı toplama yöntemleri: FÖ'de katılımcılardan gelen lokal modeller toplandıktan sonra ortak modelin güncellenmesinde kullanılan standart algoritma, "federated averaging" olarak bilinen ortalama alma algoritmasıdır. Fakat bu algoritma kullanıldığında, zehirleme ve arka kapı saldırıları kolaylıkla yapılabilmektedir. Saldırıların engellenmesi için dayanıklı toplama yöntemleri önerilmiştir. Bu yöntemler, farklı katılımcılardan gelen parametreleri inceleyerek anormal özelliklere sahip modellerin elenmesini sağlar. Anormal modellerin tespiti için vektör uzaklığı yöntemleri (örn. kosinüs mesafesi) veya anomali tespiti bazlı stratejiler kullanılmaktadır.

KAYNAKÇA

ADAM, N.R. ve WORTMAN, J.C.: *Security-control methods for statistical databases*. ACM Comput. Surv. 21(4): 515–556, 1989.

Bagdasaryan, E., Veit, A., Hua, Y., Estrin, D., & Shmatikov, V. (2020). How to backdoor federated learning. In *International Conference on Artificial Intelligence and Statistics* (pp. 2938-2948). PMLR.

CAO, J., CARMINATI, B., FERRARI, E. ve TAN, K. L.: *CASTLE: Continuously Anonymizing Data Streams*. IEEE Transactions on Dependable and Secure Computing, 8(3): 337-352, 2011, https://doi.org/10.1109/TDSC.2009.47

DWORK, C.: Differential Privacy, (ed.. Bugliesi, M., Preneel, B., Sassone, V., Wegener, I.), Automata, Languages and Programming. ICALP 2006. Lecture Notes in Computer Science, vol 4052. Springer, Berlin, Heidelberg, 2006.

ENISA: "Pseudonymisation Techniques and Best Practices", (https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices, E.T.:02.06.2024).

Fang, M., Cao, X., Jia, J., & Gong, N. (2020). Local model poisoning attacks to Byzantine-Robust federated learning. In *29th USENIX Security Symposium (USENIX Security 20)* (pp. 1605-1622).

FUNG, B. C. M., WANG, K., CHEN, R. ve YU, P.S.: *Privacy-preserving data publishing: A survey of recent developments*. ACM Comput. Surv. 42(4): art. 14, 1-53, 2010. https://doi.org/10.1145/1749603.1749605

FUNG, B. C. M., WANG, K. ve YU, P. S.: "Top-down specialization for information and privacy preservation," 21st International Conference on Data Engineering (ICDE'05), Tokyo, Japan, 205-216, 2005.

Gong, X., Chen, Y., Wang, Q., & Kong, W. (2022). Backdoor attacks and defenses in federated learning: State-of-the-art, taxonomy, and future directions. *IEEE Wireless Communications*, *30*(2), 114-121.

GVKT-a, Madde 32: "*Security of processing*", (https://gdpr-info.eu/art-32-gdpr/, E.T.:02.06.2024).

GVKT-b, Madde 89: "*Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes*", (https://gdpr-info.eu/art-32-gdpr/, E.T.: 02.06.2024).

Huang, Y., Gupta, S., Song, Z., Li, K., & Arora, S. (2021). Evaluating gradient inversion attacks and defenses in federated learning. *Advances in Neural Information Processing Systems*, *34*, 7232-7241.

Kişisel Verileri Koruma Kurumu: "6698 Sayılı Kişisel Verilerin Korunması Kanunu Hakkında Doğru Bilinen Yanlışlar - 2", (https://www.kvkk.gov.tr/Icerik/7151/6698-Sayili-Kisisel-Verilerin-Korunmasi-Kanunu-Hakkinda-Dogru-Bilinen-Yanlislar-2, E.T.: 02.06.2024), s. 29.

Kişisel Verileri Koruma Kurumu: "Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Rehberi", (https://www.kvkk.gov.tr/yayinlar/K%C4%B0%C5%9E%C4%B0SEL%20VER%C4%B0LER%C4%B0N%20S%C4%B0L%C4%B0NMES%C4%B0,%20YOK%20ED%C4%B0LMES%C4%B0%20VEYA%20ANON%C4%B0M%20HALE%20GET%C4%B0R%C4%B0LMES%C4%B0%20REHBER%C4%B0.pdf, E.T.:02.06.2024).

LEFEVRE, K., DEWITT, D. J. ve RAMAKRISHNAN, R.: "Incognito: efficient full-domain K-anonymity". In Proceedings of the ACM SIGMOD international conference on Management of data (SIGMOD '05). Association for Computing Machinery, New York, NY, USA, 49–60, 2005.

LI, N., LI, T. ve VENKITASUBRAMANIAM, S.: "t-closeness: Privacy beyond kanonymity and l-diversity," in IEEE 23rd International Conference on Data Engineering. IEEE, 106–115, 2007.

MACHANAVAJJHALA, A., KIFER, D., GEHRKE, J. ve VENKITASUBRAMANIAM, M.: *l-diversity: Privacy beyond k-anonymity.* ACM Transactions on Knowledge Discovery from Data (TKDD), 1(1): art. 3, 1–52, 2007.

MAJEED, A. ve LEE, S.: *Anonymization Techniques for Privacy Preserving Data Publishing: A Comprehensive Survey*. IEEE Access, 9: 8512-8545, 2021, https://doi.org/10.1109/ACCESS.2020.3045700

McMahan, B., Moore, E., Ramage, D., Hampson, S., & y Arcas, B. A. (2017). Communication-efficient learning of deep networks from decentralized data. In *Artificial Intelligence and Statistics* (pp. 1273-1282). PMLR.

Nasr, M., Shokri, R., & Houmansadr, A. (2019). Comprehensive privacy analysis of deep learning: Passive and active white-box inference attacks against centralized and federated learning. In 2019 IEEE Symposium on Security and Privacy (SP) (pp. 739-753). IEEE.

NERGİZ, M. E., CLIFTON, C. ve NERGİZ, A. E.: *Multirelational k-Anonymity*. IEEE Transactions on Knowledge and Data Engineering, 21(8): 1104-1117, 2009, https://doi.org/10.1109/TKDE.2008.210

ÖZALP, I., GÜRSOY, M.E., NERGİZ, M.E. ve SAYGIN Y.: *Privacy-Preserving Publishing of Hierarchical Data*. ACM Trans. Priv. Secur. 19(3): art. 7, 1-29, 2016. https://doi.org/10.1145/2976738

SAKO, K.: Semantic Security. In: van Tilborg, H.C.A., Jajodia, S. (eds) Encyclopedia of Cryptography and Security. Springer, Boston, MA, 2011.

SWEENEY, L.: *k-anonymity: A model for protecting privacy.* International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 10(5): 557–570, 2002-a.

SWEENEY, L.: *Achieving k-anonymity privacy protection using generalization and suppression*. Int. J. Uncertain. Fuzziness Knowl.-Based Syst. 10(5): 571–588, 2002-b. https://doi.org/10.1142/S021848850200165X

Tolpegin, V., Truex, S., Gursoy, M. E., & Liu, L. (2020). Data poisoning attacks against federated learning systems. In *25th European Symposium on Research in Computer Security, ESORICS 2020, Guildford, UK, September 14–18, 2020, Proceedings, Part I 25* (pp. 480-501). Springer International Publishing.

WONG, K. S., TU, N. A., BUI, D. M., OOI S. Y. ve KIM M. H.: "Privacy-Preserving Collaborative Data Anonymization with Sensitive Quasi-Identifiers," 12th CMI Conference on Cybersecurity and Privacy (CMI), Copenhagen, Denmark, 1-6, 2019.

XIAO, X. ve TAO, Y.: *Output perturbation with query relaxation.* Proc. VLDB Endow., 1(1): 857–869, 2008. https://doi.org/10.1145/1453856.1453949

Zhu, L., Liu, Z., & Han, S. (2019). Deep leakage from gradients. *Advances in Neural Information Processing Systems*, *32*.

HASSAS GRUPLAR (ÇOCUKLAR, YAŞLILAR, ENGELLİ BİREYLER) İÇİN GELİŞTİRİLEN YAPAY ZEKÂ UYGULAMALARINDA DİKKAT EDİLMESİ GEREKEN ETMENLER

Prof. Dr. Hatice KÖSE*

ÖZET

Bu bölümde hassas gruplar (çocuklar, yaşlılar, engelli bireyler) için geliştirilen yapay zekâ uygulamalarında dikkat edilmesi gereken etmenler vurgulanmış ve çeşitli örnek uygulamalara yer verilmiştir. Uygulamalarda dikkat edilmesi gereken hukuksal ve etik süreçlere diğer bölümlerde detaylı olarak yer verilmiş olup bu bölümde kısaca değinilmiştir. Hassas verinin toplanması, saklanması ve paylaşımı gibi önem teşkil eden hususlar konusunda alınabilecek önlemler ve çıkabilecek problemler vurgulanmıştır.

GİRİŞ

Nisan 2021'de Avrupa Komisyonu Avrupa Yapay Zekâ Yasası'nı (AI Act) önermiş, Ağustos 2024'de yasa yürürlüğe girmiştir[1][2]. Avrupa Yapay Zekâ Yasası, yapay zekânın risklerini ele alan ve yapay zekâya ilişkin ilk yasal çerçevedir[3]. Farklı uygulamalarda kullanılabilecek yapay zekâ sistemleri, kullanıcılar için oluşturduğu risklere göre analiz edilip sınıflandırılmıştır.

* İstanbul Teknik Üniversitesi, Bilgisayar ve Bilişim Fakültesi, Yapay Zekâ ve Veri Mühendisliği Bölümü

1 European Parliament (2023), *EU AI Act: First Regulation on Artificial Intelligence, (https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence).*

2 European Commission, (2024), *AI Act enters into force,* https://commission.europa.eu/news/ai-act-enters-force-2024-08-01_en

3 European Commission, *AI Act,* (https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai).

Buna göre sistemler yüksek, kısıtlı, en az riskli ve kabul edilemez (en yüksek risk grubu) olarak dört kısma ayrılmıştır. Kabul edilemez riskli YZ sistemleri, insanlar için tehdit olarak kabul edilen ve yasaklanabilecek sistemlerdir. Bu sistemlerin bazıları aşağıda sıralanmıştır:

-İnsanların veya belirli hassas grupların bilişsel davranışsal manipülasyonu: örneğin çocuklarda tehlikeli davranışları teşvik eden sesle etkinleştirilen oyuncaklar

-İnsanların biyometrik tanımlanması ve sınıflandırılması

Özellikle hassas gruplara ait verilerin ticari kullanım amacıyla işlenmesi sorun teşkil etmektedir. Kişilerin/toplumun iyiliği için atılan adımlar (örneğin kaçırılan bir çocuğun bulunması için verilerin işlenmesi) bu kapsam dışında tutulmuştur.

Hassas gruplar için belirlenen kurallar, yasal, etik ve uygunluk ilkeleri temelinde oluşturulur ve bu grupların duyarlılıklarını, ihtiyaçlarını ve haklarını korumayı amaçlar. Bu kuralların bazıları aşağıda sıralanmıştır:

Gizlilik ve Güvenlik:

Hassas grupların kişisel bilgileri ve mahremiyeti büyük önem arz etmektedir. Bu bilgiler mutlaka korunmalı, sadece belirlenmiş ve yetkilendirilmiş kişiler tarafından erişilebilir olmalı ve güvenli bir şekilde saklanmalıdır. Saklanacak alan siber saldırı ve bilgi hırsızlıklarından korunaklı olmalı özellikle bulutta ya da paylaşımlı alanlarda saklanan bilgiler için gerekli güvenlik tedbirleri alınmalıdır. Gerekli görüldüğü takdirde şifrelenmiş olarak muhafaza edilmelidir. Bilgilerin paylaşımı konusunda da gerekli gizlilik ve güvenlik tedbirleri alınmalı, gerekli görüldüğü takdirde sadece yerelde bilginin işlenmesine ve daha sonra sadece geriye dönük kimlik bilgisine erişilemeyecek şekilde anonimleştirilmiş ya da maskelenmiş salt makine tarafından okunabilir şekliyle paylaşımına izin verilmelidir. Paylaşım için mutlaka gerekli onam formları doldurulmalı ve gizlilik sözleşmelerine riayet edilmelidir.

Ayrımcılık ve Ön Yargıdan Kaçınma:

Yapay zekâ uygulamaları, ırk, cinsiyet, din, engellilik durumu, yaş veya diğer hassas gruplar temelinde ayrımcılık yapmamalıdır. Üretilen yapay zekâ uygulamalarının ve geliştirilen modellerin tüm kullanıcı gruplarını eşit ve adil bir şekilde kapsaması sağlanmalıdır. Modellerin eğitiminde bu

grupların da temsil edilebilmesi için yeterince eşit dağılmış veri kullanılmalıdır. Örneğin sadece sağlıklı yetişkin bireylerde eğitilmiş bir yapay zekâ uygulaması engelli çocuklarda iyi sonuç vermeyebilir, ya da bu tür bir veriyle eğitilmiş bir akıllı asistan uygulaması engelli bir yetişkin bireyin konuşmasını yeterince başarılı algılayamadığı için bu bireylerin verilen servisi kullanmasında sorun yaşanabilir. Modellerin ön yargılı sonuç üretmesi durumda kontrol edilmeli ve gerekli önlemler alınmalıdır.

Doğruluk ve Hassas Bilgi Kullanımı:

Hassas gruplarla ilgili verilerin doğru bir şekilde toplanması ve kullanılması en önemli durumlardan birini teşkil eder. Bu verilerin yanlış toplanması, yanlış etiketlenmesi ya da veri setindeki dağılımdaki eşitsizlik verinin uygulama tarafından yanlış yorumlanmasına neden olabilir veya verinin yanıltıcı bir şekilde kullanılması, bu gruplara zarar verebilir. Örneğin bir tavsiye sistemi çocuklara yaşlarına uygun olmayan bilgi ve görüntü içerikli tavsiyeleri iletebilir, ya da engelli bir birey bir uygulamanın geliştirilmesinde kendi verisi yeterince temsil edilmediği durumda uygulama kendisi için yanlış sonuçlar üreteceğinden dolayı kullanamayabilir. Bazı durumlarda bu tür uygulamaların hatalı sonuçlar vermesi ciddi risk doğurabilir. Bir sağlık uygulaması için veriler yanlış etiketlendiği takdirde riskli gruptaki kişiler (örneğin Alzheimer ihtimali olan yaşlı bireyler) güvenli grup olarak tespit edilebilir ya da tam tersi tedavi edilebilir bir durum (örneğin yaşlı bireylerde depresyon) belirtileri benzer başka bir tanıyla karıştırılabilir (örneğin Alzheimer) bu durumda tedavi için gerekli kritik zaman kaybedilmiş olur.

Onay:

Hassas gruplardan bilgi toplamadan önce, onaylarının alınması gereklidir. Onaylarını almak için bireylerle paylaşılan metinler dil ve bilgi düzeyine uygun ve açıklayıcı olmalı, özellikle bilginin çeşidine ve kullanım alanlarına yer vermelidir. Bu noktada verinin sadece akademik ya da ticari amaçla toplanması, 3. taraf kurum ve kuruluşlarla paylaşılıp paylaşılmayacağı, ses, görüntü gibi kimliğin tespitinde kullanılabilecek verilerin dahil olup olmaması, bu verilerin hangi ortamlarda kullanılacağının detaylı belirtilmesi önem arz eder. Katılımcı bu bilgilere göre çalışmaya katılıp katılamayacağını belirtir, dilediğinde çalışmadan ayrılma hakkına sahiptir. Bu kararı kendi başlarına veremeyecek hassas gruplar (sınırlı ehliyetsizler örneğin çocuklar veya bilişsel engele sahip bireyler) için onayı katılımcıyı temsilen veli/vasi verir.

Şeffaflık ve İzlenebilirlik:

Yapay zekâ sistemlerinin nasıl çalıştığı ve hassas grupların bilgilerinin nasıl kullanıldığı konusunda mümkün olduğu kadar şeffaf olunması başka bir önemli konudur. Katılımcılara ya da temsilcilerine verilerinin nasıl işlendiği ve süreç hakkında bilgi paylaşılmalıdır. Araştırmacılar açısından da sistem çıktılarının açıklanabilir olması önem arz eder. Bu şekilde çeşitli yanlı ya da yanlış çıktıların önüne geçilebilir.

Hassas Gruplara Duyarlılık:

Yapay zekâ destekli sistemler, hassas gruplara ve onların ihtiyaç ve isteklerine karşı duyarlı olmalıdır. Bu grupların özel ihtiyaçları ve duyarlılıkları da dikkate alınmalıdır. Aksi halde çeşitli engel grupları için sistemler erişilebilir olmalı ve bu konuda gerekli tedbirler alınmalıdır. Çeşitli yaş grupları için de bu durum geçerlidir. Çalışmalara katılan yaşlı bireylerin ya da çocukların da çalışmalara erişimi için ara yüzler uygun tasarlanmalı (örneğin büyük fontlar) ve yönergeler (kısa, anlaşılabilir ve görsellerle desteklenmiş) açıklamalar uygun bir şekilde düzenlenmelidir. Engelli bireyler için farklı engel gruplarına göre farklı modalitelerle zenginleştirilmiş ara yüz ve yönergeler sağlanmalıdır (örneğin görme engelli bireyler için metinden konuşmaya çeviri sistemleri, büyük fontlar; işitme engelli bireyler için konuşmayı metine ya da işaret dili görsellerine (avatar destekli videolar) çeviren, disleksik bireyler için uygun font, renk ve arka plan seçimi sağlayan sistemler gibi). Yapay zekâ sistemlerinin bu bireylerin de bilgileri ile eğitilmesi ve onları da kapsaması gereklidir.

Kullanım Amaçları ve Sınırlamaları:

Hassas gruplara ait veriler, yalnızca belirli ve açık bir amaç doğrultusunda kullanılmalıdır. Bu amaç, veri toplama sürecinde katılımcıya veya temsilcisine açıkça bildirilmeli ve onay alınmalıdır. Verilerin başka amaçlarla veya farklı kişiler tarafından kullanılmasına izin verilmemeli, bu konuda gerekli önlemler alınmalıdır. Ticari faaliyetler kapsamında bu bilgilerin kullanılması veya üçüncü taraflarla paylaşılması planlanıyorsa bu faaliyetler için katılımcının onayı alınmalıdır.

Güvenilirlik:

Hassas grupların ihtiyaçlarına yönelik hizmet ve uygulamaların güvenilir olması, doğru çalışması ve beklenen sonuçları üretmesi sağlanmalıdır. Bu konuda yeterli test ve kontrol mekanizması işleme koyulmalıdır. Yanlış

sonuçların bu kişilerin ve yakınlarının hayatları ve sosyal konumları için önemli risk oluşturduğu unutulmamalıdır.

Bu kurallara uyulması hassas grupların haklarını korumak ve yapay zekâ teknolojilerinden zarar görmelerini engellemenin yanı sıra en yüksek oranda fayda sağlamalarına da olanak sağlar. Projeler ve uygulamaların tasarlanması ve geliştirilmesi esnasında bu kural ve ilkelere riayet edilmesi, bu durumun sürdürülebilir olması için de gerekli yasa ve düzenlemelerin sağlanması esastır.

I. VERİ TOPLANMASI, SAKLANMASI VE PAYLAŞIMI

İlerleyen bölümlerde belirtilen süreçler ve olası problemler örnek uygulamalar çerçevesinde sunulmuştur. Uygulamalar İstanbul Teknik Üniversitesi, Bilgisayar ve Bilişim Fakültesi, Bilişsel ve Sosyal Robot Labında geliştirilip test edilen çocuk-robot etkileşim oyunlarını içerir. Bu tür uygulamaların katılımcıların fiziksel güvenliğin yanı sıra ruhsal olarak rahatı ve güvenliğini de göz önünde bulundurması gereklidir. Çalışmada yetişkinler için eğitilen yapay zekâ modelleri kullanılmayıp çocuklar için çocuk verileriyle model eğitilmiştir. Uygulamaların detayları için ilgili referans çalışmalara başvurulabilir.

A. ÖRNEK UYGULAMALAR: İŞİTME ENGELLİ ÇOCUKLAR

1. RoboRehab: Yardımcı Odyoloji Rehabilitasyon Robotu

Bu proje, koklear implant ve işitme cihazı kullanan işitme engelli çocukların hastanelerde yapılan işitsel testler (DTAP) sırasında desteklenmesi için duygu tanıma yetenekleriyle zenginleştirilmiş yardımcı robot tabanlı bir sistemin tasarlanmasını ve geliştirilmesini amaçlamaktadır[4]. Çalışma İstanbul Üniversitesi Cerrahpaşa Tıp Fakütesi Odyoloji bölümü iş birliği ile gerçekleştirilmiştir.

Bu çalışmadaki ilk zorluk, çocukların pozitif ve negatif duygularını etik bir tasarımla tetiklemek ve bu bilgiyi robot için yapay zekâ tabanlı bir duygu tanıma modeli üretmek için kullanmaktır. Duygu verileri elektroensefalogram (EEG), fizyolojik sensörler ve kameralar (yüz ifadesi) kullanılarak toplanmıştır. Çalışmaları üniversite etik kurulu onaylamış ve çalışmadan önce katılımcıların veli/vasilerinden onam formu alınmıştır. Bu süreç ileriki bölümlerde daha detaylı olarak verilmiştir.

[4] ROBOREHAB, (https://roborehab.itu.edu.tr/).

Yetişkinlerde duygu ve stres tanımaya yönelik düzenli test rutinlerinin, çocuklara zarar verme ihtimalinden dolayı burada kullanılması mümkün değildir. Örneğin stres tetikleme için yetişkinlere bazı korku filmi sahneleri gösterilmektedir, bu tür görsel test materyalleri çocuklar için uygun değildir; bu nedenle bu çocuklarla çalışan odyologları ve fizyologları desteklemek için çocukların ihtiyaç ve isteklerine uygun yeni rutinler tasarlanmıştır. Örneğin başka bir çalışmamızda bu amaçla oyunlar geliştirilmiş, bu oyunların zorluk seviyeleri değiştirilerek ya da oyunlara özellikle yazılımsal problem (bug) eklenerek kontrollü olarak duygu tetiklemek amaçlanmıştır.

Bu çalışmamızda çocukların duygularını uyandırmak için çocukların yaş gruplarına uygun ve psikologlar tarafından seçilen farklı filmlerden sahneler ve farklı zorluk seviyelerindeki robot tabanlı oyunlar kullanılmıştır. Bu çalışmalar sırasında çocukların yüz verileri duyguların analizi amacıyla projede çalışan psikologlar tarafından etiketlenmiştir.

Toplanan ve etiketlenen veriler anonimdir ve yalnızca robot için makine öğrenimi tabanlı duygu tanıma modelleri oluşturmak; robotun etkinliğini ve çalışmadaki diğer parametreleri değerlendirmek için kullanılmıştır.

Bu çalışma, robotu teste yapay zekâ destekli duygusal bir asistan olarak dahil etmiştir. Robot, sesli sorular sormuş, sözlü talimatlar vermiş ve çocuklara "aferin" veya "lütfen tekrar deneyin" gibi geri bildirimlerde bulunmuştur.

Çocukların duygusal durumlarını betimleyen video ve fizyolojik verileri ve testlerdeki performansları analiz için kaydedilmiştir. Psikologlar ve odyologlar çalışmalar başlamadan önce tüm sözlü talimatları, robotun sesini, robotun jestlerini ve çocukların cevapları girdiği tabletin ara yüz tasarımını kontrol etmiş ve onların geri bildirimlerine göre sistemde gerekli değişiklikler yapılmıştır.

Çocuklara kaba ya da aşırı olumsuz geri bildirimde bulunulmaz ve robot çocukları motive etmek için çok güçlü ama dikkat dağıtıcı hareketler kullanamaz, bu davranışlar önceden kontrol edilip düzeltilir. Deneylerde kullanılan robota dokunmak güvenli olsa da yine de güvenlik önlemleri açısından çocukların robottan 1,5 metre uzakta oturmaları ve çalışmalar sırasında robota dokunmamaları istenmiştir.

Tüm oturumlarda testler sırasında çocuklara bir psikolog veya odyolog eşlik etmiş, yanı sıra robottan sorumlu bir araştırmacı ve sensörleri ve

kamerayı kontrol eden başka bir araştırmacı da çalışmada hazır bulunmuştur. Çoğu seansta çocukların dikkatinin dağılmasını önlemek için çocuğa yalnızca odyolog ve robot uzmanı eşlik etmiştir.

B. ÖRNEK UYGULAMALAR: OTİZMLİ ÇOCUKLAR

1. EMBOA: Otizmli Çocuklara Yönelik Bir Müdahale Aracı Olarak Sosyal Yardımcı Robotikte Duygusal Döngü

Bu proje, çocuk boyutunda insansı robot Kaspar ile OSB'li çocukların rehabilitasyon çalışmaları sırasındaki rehabilitasyon ve müdahale metodolojisini ve duygusal durumlarını analiz etmeyi amaçlamaktadır[5]. Proje İngiltere, Almanya, Makedonya, Polonya ve Türkiye'nin iş birliğine dayalı uluslararası bir çalışmadır. Önceki çalışmaya ek olarak çocuğun dikkatini takip etmek için bakış takip cihazları ve duygu tanıma çalışması kapsamında mikrofonlar kullanılmıştır. Test düzeneği robot Kaspar ile önceden tanımlanmış bazı rehabilitasyon ve etkileşim oyunlarını içerir. Sensörler robotun altındaki bir kutuya, kamera ise robotun şapkasına gizlenir ve çocuk, önceki testte (RoboRehab) yapıldığı gibi testler sırasında fizyolojik verilerin de toplanması için bir akıllı saat (E4) takar. Çocuğa bir araştırmacı/terapist eşlik eder ve talimatlar özel bir sayısal tuş takımı aracılığıyla robota gönderilir. Hayvan sesleri, jestler ve çocuk şarkılarının yer aldığı farklı oyunlarda çocuktan robotu taklit etmesi istenir. Önceki çalışmadan farklı olarak test düzeneği esnektir ve çocuk bir oyunda daha fazla zaman geçirmek isterse deney akışı çocuğun isteklerine göre uyarlanır.

Bu uygulama kapsamında eş zamanlı olarak farklı ülkelerde klinik çalışmalar yapılmış ve çocuklara ait göz hareketleri, ses, video ve fizyolojik veri toplanmıştır. Bu veriler projede yer alan psikologlar ve uzmanlar tarafından etiketlenmiş ve makine öğrenimi modellerinin geliştirilmesinde kullanılmıştır.

Projede çalışmalar başlamadan önce etik onay alınmaktadır. Bu süreç aşağıda detaylı olarak aktarılmaktadır:

a. Etik Onaydan Önce

Çalışmalara başlamadan önce uluslararası hukuk ve ulusal hukuk düzenlemeleri ışığında oluşturulan etik kurulun onayı alınır. Olası senaryolar, katılımcılardan alınacak tüm bilgiler, motivasyon, ilgili proje bilgileri ve

[5] EMBOA Project, (https://emboa.eu/).

katılımcıların bilgileri etik kurula sunulur. Ayrıca bir onam formu örneği (katılımcı reşit değilse ya da kendi adına karar veremiyorsa veli/vasi onam formu) de sunulmaktadır. Çalışmaya katılacak tüm araştırmacıların detaylı özgeçmişleri de ayrıca sunulmaktadır. Ayrıca kullanılacak robot hakkında kurul bilgilendirilmeli; robotun veya kurulumunun katılımcılara herhangi bir zarar verip vermeyeceği konusunda kurula bilgi verilmelidir. Etik kurul gerekli gördüğü takdirde verilen bilgilerde revizyon/değişiklik talebinde bulunabilir.

b. Etik Onay Alındıktan Sonra ve Katılımcıların İşe Alımı Sırasında

Çalışma kurul tarafından onaylandıktan sonra, katılımcıların işe alımı sırasında araştırmacıların katılımcıları çalışma ve onam formu hakkında bilgilendirmeleri gerekmektedir. Onam formunda çalışma hakkında kısa bilgi verilir (örneğin "Çocuk boyutunda bir insansı robotla insan-robot etkileşimi oyunu oynayacaksınız ve elde edilen bulguları otizm terapisinde robotun etkileşim ara yüzünü geliştirmek için kullanacağız"), Enstitü ve araştırmacılar (örneğin, "bu çalışma, Y tarafından finanse edilen ve Z Üniversitesinde Prof. H ve araştırma ekibi tarafından yürütülen X projesinin bir parçasıdır"), toplanacak tüm veri öğeleri (örneğin, "mikrofonlar sesinizi kaydedecek, çalışma sırasında veri toplamak için akıllı saat takacaksınız, tüm oturum videoya kaydedilecek") ve kısaca bu toplanan bilgilerin nasıl kullanılacağı (örneğin, "kaydedilen bu veriler Robotun davranışlarını geliştirmek amacıyla kullanılacak ve kimliğiniz hiçbir şekilde açıklanmayacaktır").

Ayrıca bulguların ve verilerin araştırma amacıyla anonim olarak sunulmasına ilişkin onay alınır.

Katılımcı çalışmaya katılmayı kabul edebilir ancak fotoğraf, video veya bilgilerinin kamuya açık olarak paylaşılmasına izin vermeyebilir. Bu verilerin ticari amaçla kullanılması planlanıyorsa, bunun da katılımcıya sunularak onay alınması gerekmektedir.

Katılımcıya ayrıca bunun gönüllü bir görev olduğu ve istediği zaman çalışmadan ayrılabileceği bilgisi verilir.

Daha önce de belirtildiği gibi, katılımcının reşit olmaması ya da kendi adına karar verebilecek bilişsel yeterliliğe sahip olmaması durumunda ebeveyn/bakıcının çocuk adına onay formunu okuyup imzalaması gerekmektedir.

Ebeveyn onam formunu imzalamayı reddederse çocuk çalışmaya katılmayacaktır. Bu nedenle katılımcıların çalışmaya alımı sırasında velilerin bilgilendirilmesi önemlidir. Çalışmadan ayrılanların telafisi için planlanandan daha fazla katılımcının çalışmaya dahil edilmesi/davet edilmesi yararlı olacaktır.

c. Çalışmadan Önce

Robotta ve kurulumda gerekli önlemler alınmalı (örneğin, robota dokunmanın çocuğa zarar verebileceği durumlarda çocuk ile robot arasına uyarı levhaları veya paneller konulmalıdır). Çocuğa kısaca bilgi verilmelidir (Robot K ile oyun oynayacaksınız ve robota nasıl hareket edeceğini öğreteceksiniz, ayrıca robotun hareketlerinizi daha iyi anlaması için kolunuza saat takacağız). Ebeveyn/bakıcı/öğretmen, kurulum gereği veya çocuğun çok gergin olması durumunda onu rahatlatmak için deney alanında kalabilir.

d. Çalışma Sırasında

Çocuk istediği zaman çalışmadan ayrılabilir.

Çalışma robot ve ilgili bilgisayar/tablet ve sensörlerden sorumlu en az bir araştırmacı tarafından denetlenmektedir. Başka bir uzman/öğretmen/araştırmacı çalışmayı yürütür, çocukla etkileşime girer ve gerektiğinde çalışmaya müdahale eder. Her ne kadar hem robotu ve teknik ekipmanı denetleyen hem de çocuğu tek başına denetleyen tek bir araştırmacıyı kapsayan çalışmalar olsa da, eğer çocuk kurguya aşina değilse ve robot çok büyük veya karmaşıksa (örneğin insansı robotlar), teknik sorunları azaltmak ve çocuğun güvenliğini artırmak için bu görevlere ayrı araştırmacıların görevlendirilmesini öneririz. Robotun veya diğer cihazların arızalanması gibi problemli bir durum oluştuğunda veya çocuk kendini rahat hissetmiyorsa veya robottan/kurulumdan korkuyorsa, çocukla ilgilenecek başka bir uzmanın çalışmada olması faydalı olacaktır. Ayrıca çocuğun kuruluma ve robota alışmasına yardımcı olacaksa çocuğun bakıcısının/ebeveyninin de deney odasına girmesine izin verilebilir.

Bu durumda bakıcıya/ebeveyne deney düzeneğine veya çocuğun robota verdiği tepkilere müdahale etmemesi talimatı verilmelidir.

Çocuğun seans sırasındaki tepkilerini analiz etmek için seans videoya kaydedilir. Tüm bu verilere ait izinler özellikle video verisi onam formunda vurgulanarak izin alınır. Verinin saklanması, işlenmesi ve paylaşımında

önceki bölümlerde yer alan kurallar geçerlidir. Bilimsel sunumlarda çalışmadan örnek resim ya da görsel kullanımında veri blurlanarak anonimleştirilir.

C. ÖRNEK UYGULAMALAR: SEREBRAL PALSİLİ BEBEKLER

1. Techtoys: Nörogelişimsel Bozuklukların Erken Tespiti ve İzlenmesi için Sensör Tabanlı Oyuncaklarla Bebeklik Döneminde Dijital Biyobelirteçler Edinimi

Bu uluslararası projede serebral palsili bebeklerin sensör tabanlı oyuncaklarla ve anneleriyle etkileşimi sırasında elde edilen vücut hareketleri (IMU sensörler), baş hareketleri, yüz ifadesi, bakış (kamera), ses (mikrofon) ve fizyolojik verilerinin (akıllı saat) makine öğrenmesi metotlarıyla işlenerek analiz ve tespit yapılması amaçlanmıştır. İtalya ve Fransa'da klinik çalışmalar yapılmakta, elde edilen veriler, Fransa ve Türkiye'de işlenmektedir. Almanya'da bir kurum projenin etik açıdan izlediği süreçleri kontrol etmektedir. Projede hem klinik ortamda yapılan deneyler sonucu elde edilen veriler, hem de bebeklerin ev ortamında ebeveyn tarafından kaydedilen verileri kullanılmaktadır. Bu verilerin gizlilik ve güvenlik tedbirleri çerçevesinde anonimleştirilerek farklı ülkelerdeki kurumlar tarafından işlenmesi, paylaşımı, saklanması, etiketlenmesi için yöntemler geliştirilmektedir. Bu alınan ekstra önlemler projelerin gidişatını yavaşlatsa da etik açıdan önem arz etmektedir. Mayıs, 2024'te İstanbul Teknik Üniversitesi'nde gerçekleştirilen FG2024 (Face and Gesture) konferansında ve konferans dahilinde organize edilen PrivAAL (2nd GoodBrother workshop on privacy-aware and acceptable video-based assistive Technologies) çalıştayında bu tür gizlilik çerçevesinde güvenli bir şekilde bebek verisi gibi hassas verilerin paylaşımını esas alan çalışmalara da yer verilmiştir[6].

TARTIŞMA VE SONUÇ

Gelişen Robotik ve Yapay Zekâ teknolojileri büyük oranda veriye ihtiyaç duymakta ve bu durum sayısız hukuki ve etik sorunu da beraberinde getirmektedir.

---

[6] GoodBrother (2023), *PrivAAL-2nd GoodBrother workshop on privacy-aware and acceptable video-based assistive technologies"* (https://goodbrother.eu/conferences/privaal2024/).

Üretken yapay zekâ teknolojisinin gerçeğinden ayırt edilemez şekilde kişisel verileri modifiye edebildiği, bu veriler kullanılarak kullanıcıların manipüle edilebildiği bir süreçte özellikle kendini savunabilecek bilişsel, fiziksel ve sosyal yeterliliklere sahip olmayan çocukların, yaşlıların ya da engelli bireylerin ve bu bireylere ait verilerin toplanması, saklanması, işlenmesi ya da paylaşılmasının sınırlarının yönerge ve şartnameler çerçevesinde düzenlenmesi gereklidir.

Bu kuralların teknolojinin gelişimine imkân tanıyan, ilgili akademik ve ticari uygulamaların gelişmesini ve uluslararası rekabetten kopulmamasına imkân veren; aynı zaman bu hassas gruplara ait bireylerin de haklarını ve güvenliklerini koruyan; sosyal, fiziksel, mental ve toplumsal açıdan iyiliklerini güvence altına alan bir yapıda olması sağlanmalıdır. Bu amaçla öncelikle korumalı alan (sandbox) şeklinde uygulamalar geliştirilebilir. Bu şekilde gerçek dünyaya açılmadan izole ve kontrollü bir ortamda test edilen uygulamalarla olası problemler ve güvenlik açıkları fark edilip ilgili tedbirler ve şartnameler oluşturulabilir.

Gelecekte hayatımızın bir parçası olacak yapay zekâ ve yardımcı robot sistemleri ile etkileşimin potansiyel sonuçlarını ele almak, filozofların, hukuk uzmanlarının, politika yapıcıların, bilgisayar bilimcilerinin ve robot araştırmacılarının çok disiplinli görüşlerini gerektirir.

KAYNAKÇA

EMBOA Project, (https://emboa.eu/).

European Commission, *AI Act,* (https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai).

European Parliament (2023), *EU AI Act: First Regulation on Artificial Intelligence, (https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence).*

GoodBrother (2023), *PrivAAL-2nd GoodBrother workshop on privacy-aware and acceptable video-based assistive technologies"* (https://goodbrother.eu/ conferences/privaal2024/).

ROBOREHAB, (https://roborehab.itu.edu.tr/).

SAĞLIK ALANINDA YAPAY ZEKÂ VE KİŞİSEL VERİLER

Prof. Dr. Perihan Elif EKMEKCİ*

YZ'nin sağlık alanında kullanımı, 1950'li yıllara, YZ fikrinin ilk gelişmeye başladığı yıllara kadar uzanan bir geçmişe sahiptir. Aslında bu durum teknoloji ve sağlık hizmetlerinin neredeyse birbirinden ayrılamaz eş zamanlı gelişiminin bir yansımasıdır. Tıp tarihine baktığımızda, tanı, tedavi ve rehabilitasyona yönelik sağlık hizmetlerinin büyük çoğunluğunun teknoloji ile birlikte ilerlediği görülmektedir. Hatta öyle ki teknoloji, sağlık alanında bazı kavramların yeniden tanımlanmasına, ya da yeni bazı kavramların gündeme gelmesine bile neden olmuş, bu etkisi nedeniyle adeta sağlık hizmet sunumunda paradigma belirleyicisi bir konum edinmiştir. Örneğin prehistorik dönemden bu yana hekimlerin belki de en kolay koyduğu tanı "ölüm" tanısı iken, yaşam destek teknolojisinin yaygın kullanıma girmesi ile en zor konan tanı haline gelmiş, alt beyin ölümü, tam beyin ölümü, daimî bitkisel hayat gibi bildiğimiz nitelikteki yaşamla da ölümle de tam olarak bağdaşmayan yeni yaşam durumları ortaya çıkmıştır. Benzer bir durum insanın temel genetik materyali olan DNA'nın tanımlanmasından sonra çok hızla gelişen genetik çalışmalarda ortaya çıkmıştır. 1953 yılında Watson ve Crick'in Nature dergisinde yayınladıkları DNA sarmalının yapısını açıklayan "Nükleik Asitlerin Moleküler Yapısı: Deoxyribonükleik Asidin Yapısı"[1] adlı iki sayfalık makalelerinin son cümlelerinde, bu yeni bilginin tıp teknolojisine ilişkin potansiyeli "insan genomunu bilmek onu kopyalamak için de önemli bir adımdır" ifadesi ile ortaya koyulmuştur. Başka bir deyişle teknoloji ve tıp daima birlikte gelişmiş, teknolojinin beraberinde getirdiği olanaklar tıbbın ilerlemesinde ve evrimleşmesinde çok önemli bir belirleyici olmuştur.

* TOBB ETÜ Tıp Fakültesi Tıp Tarihi ve Etik Anabilim Dalı Başkanı

1 Watson, J., Crick, F. Molecular structure of nucleik acids: A structure for Deoxyribonucleic acid. Nature. 1953: 171, 737-738.

YZ, teknolojinin tıp uygulamalarında en yaygın ve etkili kullanım alanlarından biri olmaya adaydır. Bu geniş potansiyel, zayıf YZ sistemlerinin ilk modelleri arasında olan uzman sistemler ile hayata geçmiştir. İlk uzman sistemler 1970'li yıllarda Stanford Üniversitesi Tıp Fakültesi öğretim üyelerinin bilgilerini veri kaynağı olarak kullanarak çıkarımlar yapan bir çalışma modeline sahipti. Bu sistemlerin en iyi bilineni ciddi enfeksiyon hastalıklarına neden olan mikroorganizmayı belirleme ve uygun antibiyotik seçimi yapma konusunda hekimleri, bir dizi "evet/hayır" soruları yanıtlamalarını isteyerek yönelten "Mycine" adlı uzman sistemdir. Bu sistem daha sonra geliştirilerek farklı klinik alanlara yaygınlaştırılmıştır. Solunum yolu hastalıkları için geliştirilen "Puff" adlı uzman sistemin başarısını değerlendirmek üzere yapılan bir araştırma söz konusu sistemin akciğer fonksiyonlarını değerlendirmedeki etkinliğini oldukça başarılı bulmuştur[2]. Elbette veri kaynağının öğretim üyelerinin aktardığı bilgilerle kısıtlı olması, işletim modelinin oldukça basit bir algoritmaya dayanması bu ilk uzman sistemlerin önemli kısıtlılıkları arasındaydı.

YZ'nin ilk uygulamalarından birisi de ELIZA adlı doğal dil işleme modeline dayalı uzman sistemidir. ELIZA 1964-1967 yılları arasında MIT'de Joseph Wiezenbaum tarafından psikiyatri hastalarına psikoterapi uygulamak amacıyla geliştirilmişti. Günümüzde bile halen hekim hasta ilişkisinin en özel alanlarından biri olan psikiyatride YZ kullanılması elbette oldukça ilgi çekici bir gelişme olmuş, bu özelliği nedeniyle ELIZA Turing Test'ini sınayan ilk chatbot uygulamalarından biri olarak tarihe geçmişti. ELIZA'nın, yapılan araştırmalarda "neredeyse insan psikiyatristler" kadar verimli olduğu görülmüş, hatta hasta memnuniyeti açısından neredeyse ön plana geçmiştir[3]. Tıp alanında YZ'nin bu kadar hızlı ilerlemesi elbette pek çok etik soruyu da gündeme getirmiştir. Daha sonra bazılarına değinilecek olan bu etik sorunlar ELIZA'yı geliştiren ekibin başında yer alan Weizenbaum'un da dikkatini çekmiş, ELIZA'nın başarısı ortaya çıktıktan sonra, bu etik sorunlar üzerine düşünmek ve önlemler geliştirmek amacıyla sabbatical alarak "Computer Power and Human Reason" adlı kitabı kaleme almıştır[4]. Weizenbaum, bu kitabında YZ'nin etik kullanımı ile ilgili Asimov'dan

---

2 Aikins, J.S., Kunz, J.C., Shortlife, E.H., Fallat, R.J. PUFF: An expert system for inrerpretation of pulmonary function data. Computers and Biomedical Research. 1983: 16 (13):199-208.

3 Colby, K.M., Watt, J.B., Gilbert, J.P. A computer Method of Psycotheraphy. The journal of Nervous and Mental Disease. 1966: 142 (2): 148-52.

4 Weizenbaum, J. Computer power and human reason: From Judgement to calculation.W.H. Freeman & Co. NewYork, 1976.

sonra en ilgi çekici belirlemeleri yapmıştır. Weizenbaum'un öne sürdüğü temel argüman YZ teknolojisini geliştirenlerin başarı ve maddi kazanç gibi beklentilerle hareket ettikleri ve bu nedenle tasarladıkları ya da ürettikleri YZ teknolojisinin etik etkilerini göz önünde bulundurmayacakları olmuştur. Bu noktadan hareketle YZ'nin öngörülemez ve geri döndürülemez riskler içerdiği koşullarda kullanılmamasını ve yakınlık, anlayış ve dayanışma gibi insani niteliklerin ön olanda olduğu hizmet kollarında YZ'nin kullanımının mümkün olduğunca kısıtlanması gerektiğini savunmuştur. Weizenbaum'un argümanı gerçek yaşamda pek kabul görmemiş ve insani nitelikleri en ön planda olan sağlık sektörü YZ'nin en hızlı geliştirilen alanlarından birisi olmuştur.

Günümüzde zayıf YZ sistemleri ağırlıklı olarak hekimlerin karar verme süreçlerinde başvuracakları bir asistan olarak çalışan karar destek sistemlerinde (KDS) yer bulmaktadır. KDS, karşı karşıya bulunulan klinik durumda mevcut verileri işleyerek olası karar seçeneklerini belirlemek üzere çalışır. Örneğin, klinik semptomlar, muayene, laboratuvar ve görüntüleme tetkiklerinin sonuçlarına göre ayırıcı tanıyı belirlemek, olası tedavi yöntemlerini sıralamak ve prognoza ilişkin öngörülerde bulunmak KDS'nin tıp alanındaki işlevleri arasında yer almaktadır. KDS YZ sistemlerinde amaç, hekimin kararını belirlemek değil, onun kararına yardımcı olabilecek bir çıktı üretmektir. Günümüzde farklı klinik alanlarda KDS geliştirmek üzere pek çok araştırma geliştirme çalışması yürütülmektedir. Bu çalışmalar özellikle patoloji ve radyoloji gibi görseller üzerinden tanı koymaya yönelik alanlara yoğunlaşmaktadır. Şüphesiz YZ teknolojisinde veri etiketleme konusunda sağlanan teknolojik gelişmeler ve veri işleme kapasitesi yüksek makinelerin yaygın kullanıma girmesi bu çalışmaların artmasını sağlamaktadır. En az bu kapasite artışı kadar önemli olan diğer katalizör unsur da YZ'nin eğitiminde kullanılacak büyük verinin erişilebilirliğinin artmasıdır. Dijitalleşmeden önce fiziki ortamlarda tutulan hasta verilerinin elektronik ortama taşınması YZ'nin eğitiminde kullanılabilecek veri miktarının hızla artmasına imkân sağlamıştır. Verilerin dijital ortama taşınması bu verilerin YZ geliştirilmesinde kullanılabilirliğini doğrudan arttırıcı bir unsur gibi görülse de dijital platformların birbiri ile uyumlu olmaması, girilen verilerin sadece uyumlu sistemler tarafından tanınabilmesi ve kullanılabilmesi gibi kısıtlılıklarla karşı karşıya kalmıştır. Sağlık verilerinin dijitalizasyonunun ilk dönemlerinde aynı sağlık kurumundaki farklı birimlerinin arasında bile uyum sağlamak güç olmuş, bu durum tekrar eden veri girişleri ve âtıl kalan veri depolarına yol açmıştır.

Günümüzde bu sorun açık veri kaynaklarının birbiri ile "konuşabilir olmasını" sağlamak amacıyla yürütülen veri eşgüdüm projeleri ile aşılmaya çalışılmaktadır. Veri eşgüdümü görsel veri, ses verisi, yazı verisi gibi farklı türlerdeki verilerin bir anlam yaratma amacıyla birlikte değerlendirilebilmesi için oldukça önemlidir. Zira tıp uygulamalarında hekim, hastası ile ilgili kararlarını geliştirirken tüm bu farklı nitelikteki verileri bir arada kullanmakta, karar verirken her bir verinin "o" hasta özelinde ne kadar ağırlıklı olması gerektiği konusunda bir fikir yürütmekte ve sonuca varmaya çalışmaktadır. Hipokrat tarafından "hastalık yok, hasta var" cümlesi ile açıklanan ve her hasta için "o" hastanın öznel niteliklerini göz önünde bulundurarak geliştirilen yaklaşımda YZ'nin kendine anlamlı bir yer bulabilmesi için veri eşgüdümü yadsınamaz önemdedir.

YZ'nin, KDS açısından çok etkili olacağı düşünülen radyoloji ve patoloji gibi alanlarda hekimlerin üstlendikleri görevin YZ sistem geliştiricileri tarafından tam olarak anlaşılamadığı da bir gerçektir. Zira uzman bir patoloğun ya da radyoloğun görüntüleri değerlendirirken izlediği akıl yürütme metodolojisi basit bir görsel analizinden çok daha karmaşık bir süreçtir. Bu süreç, hastanın özgeçmişi ve soy geçmişi, alışkanlıkları, yaşı, cinsiyeti, eşlik eden hastalıkları, yaşam koşulları, mesleği hatta stres durumu gibi pek çok unsuru göz önünde bulundurarak çalışmayı gerekli tutar. Bu, kapsamlı bilimsel donanımın yanı sıra detaylı hasta analizini de gerektiren bir kavramsal düşünme sürecidir. Belki de bu nedenle YZ'nin "babası" olarak bilinen ve derin öğrenme teknolojisinin temelinde yer alan back-propoganation teknolojisini geliştirmiş olan Geoffrey Hinton'un 2018 yılında YZ'nin radyolojide vaat ettiği başarılar nedeniyle artık bu alanda "insan" hekimlere gerek olmayacağı yönündeki tahmini gerçek olamamış ve YZ'nin tüm olumlu beklentilere ve yürütülen büyük bütçeli projelere rağmen alanda etkinliği kısıtlı kalmıştır. Elbette bu kısıtlılığın bir diğer nedeni KDS'nin beraberinde getirdiği "etik ve yasal sorumluluk ve hesap verebilirlik" gibi sorunların henüz çözüme ulaştırılamamış olmasıdır. YZ'nin KDS olarak kullanılması durumunda bile verilen tanının etik ve yasal sorumlusu hekimdir. Diğer taraftan hekim kendi bilgisi ve deneyimleriyle koyduğu tanının gerekçelerini açıklayabilir ve hatta şüphede kaldığı durumda bu gerekçeleri meslektaşları ile paylaşarak fikir alışverişinde bulunarak doğru tanıya yönelebilir. Ancak YZ görüntüleme yöntemlerini sadece istatistiksel olasılık üzerinden yaptığından kararının epistemolojik dayanaklarını açıklayamaz. Bunun yanı sıra "kara kutu" problemi olarak bilinen ve YZ'nin karar algoritmasının nasıl işlediğinin bilinmezliği KDS'nin bir diğer sorun alanıdır.

Şüphesiz hasta verilerinin dijitalleşmesi beraberinde kişisel verilerin gizliliği ve mahremiyeti açısından da önemli sorunlar getirmektedir. Kişisel verilerin gizliliği ve mahremiyetinin korunması hekim hasta ilişkisinin temel dayanağıdır. Bir hastanın belki de en yakınlarından bile gizli tuttuğu bazı bilgilerini hekime teslim etmesi, onun hekime duyduğu güvenden kaynaklanmaktadır. Bu güven esasında "hekimin kendisine teslim edilen verileri sadece hastaya yarar sağlamak, onu tedavi etmek, sağlığına kavuşturmak amacı ile kullanılacağına dair inançtan kaynaklanır. Bu güven ve inanç olmadan işlevsel bir hekim hasta ilişkisi sürdürmek mümkün değildir. Bu ilişkide işlevselliğin yitirilmesi hastanın tedaviyi kabul etmesi ve tedaviye uyum göstermesini engelleyebilir. Başka bir deyişle kişisel verilerin gizlilik ve mahremiyetinin sağlanması ve korunması hekim açısından sadece yasal bir yükümlülük değil, mesleğini icra edebilmek için zorunlu olarak yerine getirmesi gereken bir ödevdir.

Diğer taraftan, sağlık verilerinin dijitalleşmesi, gizlilik ve mahremiyetin sağlanmasını sadece hekimin kontrolünden çıkarmış, pek çok aktörü sürece dahil etmiştir. Yasal açıdan elektronik sağlık verilerine kimin, ne kadar erişebileceği hizmet kalite standartlarına eklenmiş olsa da günümüzde YZ'nin gelişimi için gereken veri miktarının artması, hatta kayıtlı veri yerine, ya da kayıtlı verinin yanı sıra, gerçek zamanlı veriye de gereksinim duyulması bu alanı kompleks hale getirmiştir. İlk zamanlarda gizlilik ve mahremiyet ihlallerinin etik açıdan panzehiri olarak verinin anonimleştirilmesi önerilmiş olsa da kısa zamanda bazı sağlık verilerinin tam olarak anonimleştirilmesinin mümkün olmadığı anlaşılmıştır. Ayrıca YZ sistemlerinin istenen ölçüde doğru ve kesin sonuçlar üretebilmesinin genel anonim verilerle beslenmesi ile sağlanamayacağı da görülmüştür. Zira farmakogenetik ve farmokogenomik alanlarda sağlanan gelişmeler, kişiselleştirilmiş tıbbın önemini ortaya koymuş, kişiselleştirilmiş tıp uygulamaları için "o" hastanın verilerine gereksinim duyulması, anonim verinin YZ geliştirilmesinde yeterli olamamasının nedenlerinden biri olarak gündemdeki yerini korumuştur.

Sağlık alanında YZ geliştirilmesinde kişisel veri açısından bir diğer gri alan veri sahipliğidir. Günümüzde YZ eğitimi amacıyla geliştirilen retrospektif araştırma projelerinde hastane bilgi sistemlerinde kayıtlı elektronik hasta verilerinin kullanıldığı görülmektedir. Bu projelerin büyük kısmında kişisel veri ihlalinden kaçınmak amacıyla verilerin maskelemekten anonimleştirmeye kadar değişen bir spektrumda kaynak kişiden uzaklaştırılacağı

dile getirilmekte ve bu şekilde olası etik sorunların engelleneceği iddia edilmektedir. Her ne kadar yasal açıdan sorun içermese de bu gibi yaklaşımların beraberinde ciddi etik sorunlar taşıdığı ve bu etik sorunların geniş bir toplumsal uzlaşı ile ele alınmaması durumunda hekim hasta ilişkisinin temelindeki güvenin zedelenmesine neden olabileceği unutulmamalıdır. Zira tıp etiğinde hastanın verisine dokunmak, hastanın kendisine dokunmakla eş görülmekte ve verinin sahibi daima hastanın kendisi olarak tanımlanmaktadır[5]. Başka bir deyişle, hastanın sağlığına kavuşma motivasyonu ve hekimin kendisine bu uğurda yarar sağlamak dışında bir saikle davranmayacağı inancı ile sağladığı kişisel verilerin bu bağlam ve amaç dışında kullanılması durumunda, hasta bu durumdan mutlaka haberdar edilmeli ve verinin başka amaçlarla kullanımı konusunda karar verme hakkı korunmalıdır. Bu hak, hastanın hastaneye başvurduğu anda kendisine sunulan bir onam formu ile veri kullanımı konusunda bilgilendirilmesi ve formda "dahil olma" ya da "dışında kalma" yöntemleri ile verilerinin hangi amaçla nasıl kullanılabileceğini belirlemesi ile hayata geçirilebilmektedir.

YZ'nin klinik uygulamalarda kullanımı elbette KDS ile sınırlı değildir. Günümüzde hekimlerin sayıca azlığı global bir sorundur. Hekim başına düşen hasta sayısının yüksek olmasının yarattığı zaman kısıtlılığı, hekimlerin hasta muayenesi esnasında hasta verilerini sisteme girmeleri, laboratuvar ve görüntüleme tetkikleri ile ilgili istem yapmalarının gerekmesi nedeniyle daha da artmaktadır. Bu durum zaten az olan zamanda hekimin aynı anda birden fazla işi tamamlamasını gerektirmektedir. Hekim hasta görüşmesinin eş zamanlı olarak transkriptini hazırlayan, hatta bu transkriptteki bilgiler ışığında istenmesi gereken tetkikler ve olası ön tanılar konusunda hekimi yönlendirebilen YZ sistemleri son zamanlarda kullanıma girmiştir[6]. Bu sistemler sayesinde hekim sisteme veri girme zorunluluğundan kurtulmakta, kısıtlı zamanını hasta muayenesine ve etkili iletişime ayırabilmektedir. Ayrıca anemnez alınırken ya da muayene esnasında dile getirilmiş olan ancak hekim tarafından hasta kaydına girilmeyen/girilemeyen verilerin de kaybolmadan kayıt altına alınması sağlanmaktadır.

Söz konusu YZ sistemlerinin belirgin faydaları olsa da elbette hasta gizliliği ve mahremiyeti açısından önemli sorunlar barındırmaktadır. Hekim hasta

5 Helsinki Bildirgesi. Dünya Hekimler Birliği Bülteni, 2013:79 (4);373-374.

6 Wasim F.J.. Adressing Clinical Documentation Challemges: The Role of AI-Powered Digital Scribes. Journal of Artificial Intelligence &Cloud Computing. 2022;1(1):1-5.

görüşmesinde, hasta, ayrımcılık, damgalanma ya da güvenlik gibi endişelerle bazı bilgileri hekime sadece onun bilgisinde kalmak ve kayda girmemek koşulu ile aktarabilir. Hekim edindiği bilgiyi hastanın sağlığı ve esenliği lehine tanı ya da tedavide kullanırken, bu bilginin hasta aleyhine kullanılabilmesi riskini öngörerek ya da doğrudan hastanın talebi ile kayıtlara girmeyebilir. Hasta onamını aramadan hekim hasta mahremiyeti kapsamında konuşulan her şeyin YZ sistemi ile kayıt altına alınması bu bağlamda veri gizliliği ve mahremiyeti açısından sorunlu bir tutumdur. Bu nedenle söz konusu sistemlerin kullanımı konusunda mutlaka hasta bilgilendirilmeli ve kullanımından önce hastanın açık onamı aranmalıdır. Bu şartın sağlanması gizlilik ve mahremiyet ile ilgili sorunu çözüyor gibi görünse de, hastanın bilincinin tam bir onam vermeye yeterli olmadığı fiziksel ve/veya ruhsal travma durumları, madde ya da ilaç etkisi nedeniyle bilinç ve karar verme yeterliliğinde dalgalanmaların olması, ileri yaş, aktarılan bilgiyi anlama, kavrama ya da anlamlandırma sorunlarının yaşandığı organik beyin hastalıkları ya da psikiyatrik hastalıklar durumlarında bu gibi sistemlerin kullanımı onam şartına bağlanamaz ya da alınan onam etik açıdan yeterli ya da geçerli olamaz. Bu gibi durumlarda hasta yakını ya da vasisinin onamı aranabilirse de hastanın sağlık hizmetine ihtiyaç duyduğu bir ortamda, hizmetin sağlanmasına geçmeden önce kullanılacak teknoloji ile bilgi verip onam almaya zaman ve enerji harcanması hasta açısından güven kaybına, hekim açısından da zaman ve verimlilik yitimine neden olabilir. Diğer taraftan kullanılan YZ sisteminin kayıt altına alıp depoladığı kişisel bilgilerin tutulduğu bulut ya da diğer sistemler, bu veriye kimin ne kadar süreyle ve ne amaçla erişim sağlayabildiği, bu verilerin akademik araştırma ya da ticari araştırma geliştirme faaliyetlerinde kullanılmak üzere pazarlanması olasılığı gibi problemler, hastalığına çare bulmak amacıyla hekime derdini anlatmaya çalışan hastanın aktardığı kişisel verilerin etik dışı kullanımı riski içeren ve bu nedenle sağlık hizmeti sunumu sürecinde ciddi sorunlara yol açabilecek bir durum yaratabilir.

YZ'nin tıp uygulamalarında kullanımı konusunda dijital ikizler (digital twins) önemli bir kilometre taşı olmuştur. Dijital ikizler insan bedenindeki organ ya da dokuların, histolojik, anatomik ve fizyolojik açıdan benzer dijital/sanal modelleridir. Bu modeller sayesinde yukarıda kısaca değinilen ve her bir bireyin öznel niteliklerine göre kişiselleştirilmiş tıp uygulamaları geliştirilebilmektedir. Dijital ikizlerin tarihi 1950 yılında Alana Hodgkin ve Andrew Huxley'in mürekkep balığının sinir sistemi üzerinde geliştirdikleri ve daha sonra bu çalışmaları ile Nobel ödülü aldıkları mate-

matik kuramına kadar uzanmaktadır. Sonraki yıllarda kalp hücrelerinin sanal ikizleri geliştirilmeye başlanmış ve çalışmaları kalp hücrelerine yansıtmış, sanal beden içinde sanal kalbin fonksiyonel olmasının sağlanmasına çalışılmıştır. Böylece yüksek risk içerdiği için canlı bedenindeki gerçek kalp üzerinde yapılamayan bazı deneylerin yapılması mümkün hale gelmiştir.

Gerçekte dijital ikizlerin tıp alanına en büyük katkıları insan ya da hayvan denekler üzerinde yapılması çok riskli ya da ıstıraplı olan klinik araştırmaların hiçbir canlıya zarar vermeden gerçekleştirilmesini sağlamak olmuştur. Dijital ikizler kullanılarak yapılan araştırmalar kardiyoloji dışında başka klinik alanlarda da yaygınlaşmaya başlamıştır. Örneğin Duke Üniversitesinde hipertansiyonun neden olduğu serebral arter anevrizmaların tedavisi üzerine çalışmalar gerçekleştirmektedir. Stanford Üniversitesinde ise kalp, akciğer, bağırsaklar ve karaciğer dijital ikizleri geliştirmeye başlanmıştır. Son günlerde Fransa'da epilepsi cerrahisi araştırmaları da bilinen en kompleks organ olan insan beyninin de dijital ikizinin geliştirilmesine yakın olduğumuzu göstermiştir[7].

YZ kanser alanında da önemli bir araç haline gelmektedir. Kanser hastalarının verilerinin ve omics verileri harmanlanması ile beslenen YZ sistemlerinin kanser araştırmalarında yeni hipotezler geliştirmede kullanımının önemli faydalar sağlayabileceği öngörülmektedir. Farklı kanser biyomarkerlarının belirlenmesi ile erken tanı imkanlarının arttırılması, ilaç ya da tıbbi cihaz geliştirilmesi sayesinde tedavi seçeneklerinin ve etkinliklerinin arttırılması bu faydalar arasındadır. Elbette bu öngörülerin kanıtlanabilmesi için doğru, güvenilir, çok ve çeşitli verinin yasal etik açıdan uygun yöntemlerle elde edilmesi ve eşgüdümlü olarak kullanılabilecek bir formatta açık veri sistemlerine sunulabilmesi gereklidir. Eşgüdümlü büyük verinin toplanması kadar, saklanması ve erişilebilir olması aşamalarında da etik ve yasal hususlar dikkate alınmalıdır. Tüm bu aşamalarda yukarıda kısaca değinilen hasta onamı esas teşkil etmekte olsa da tek başına hasta onamı etik ve yasal uygunluğun sağlanması açısından yeterli değildir. Zira açık veri sistemleri, verinin erişilebilirliğini arttırırken, sınır ötesi veri aktarımı, stratejik önemi olan verilerin güvenlik riski oluşturacak şekilde paylaşımı gibi bazı özel sorunlara da yol açabilmektedir. Örneğin açık veri platformlarında yer alan omics verileri bir topluma yönelik ayrımcılığa ya

[7] Covenney P., Highfield R. Why Some Scientists Believe the Future of Medicine Lies in Creating Digital Twins. https://time.com/6268882/digital-twins-medicine-future/

da damgalamaya neden olabilecek şekilde kullanılabileceği gibi, o verilerin sağlandığı ülke açısından milli güvenlik zafiyeti de yaratabilir. Bu nedenle sağlık alanında bilimsel araştırma ekosisteminde yer alacak büyük verinin açık veri niteliğinde paylaşımının çok paydaşlı, kapsamlı bir veri politikası kapsamında yönetilmesinde fayda vardır.

Elbette araştırma ekosisteminde YZ kullanımının en önemli bileşenlerinden birisi de gerçek zamanlı veri kullanımıdır. Gerçek zamanlı veri aktarımı, YZ'nin acil durumlara ilişkin araştırmalarda kullanılabilmesinin en önemi unsurları arasında yer almaktadır. Gerçek zamanlı veri aktarımı, eğer aktarılan veri, verisi kullanılan bireylere doğrudan ya da dolaylı fayda sağlama potansiyeline sahipse, etik açıdan daha kolay savunulabilir. Bu fayda halk sağlığı acillerine ilişkin araştırmalarda oldukça belirgin olarak gözlemlenebilmektedir. Gerçek zamanlı sürveyans verilerinin diğer sağlık verileri ile birlikte YZ'ye sunulması sayesinde olası bir salgın durumunun ortaya çıkması ve etken mikroorganizmaların niteliği konularında önemli sonuçlar elde edilebilir. Böylece halk sağlığı acillerinin erken fark edilmesi, hazırlık planlarının yapılarak dijital ikizlerde etkinliklerinin değerlendirilmesi mümkün olabilir.

Diğer taraftan gerçek zamanlı veri aktarımı bireysel ya da toplumsal hassas verinin dijital ortama ve hatta açık veri platformlarına aktarılması nedeniyle önemli hak ihlallerine yol açabilir. COVID-19 pandemisi gibi tüm insanlığı etkileyen ve ciddi mortalite ve morbidite riski taşıyan durumlarda "en fazla insana en fazla faydayı sağlamanın etik bir zorunluluk" olduğunu öne süren faydacı etik yaklaşım bireysel hak ihlallerinin beklenen fayda ile orantılı olmak koşulu ile göz ardı edilebileceğini savunur. Gerçekten de orantısallık ve fayda ilkeleri, halk sağlığı acillerinde açık veri yönetimi konusunda sık başvurulan UNESCO Bildirgesi[8] ve Sandai Framework[9] gibi uluslararası çerçeve dokümanlarda da kabul görmüştür. Ancak bu iki rehber doküman başta olmak üzere sağlık verilerinin gerçek zamanlı açık paylaşımı konusundaki çoğu yaklaşımın üretici YZ'nin geleneksel zayıf YZ sistemlerinin taşıdığı risklerden çok daha fazla ve çeşitli etik risk taşıdığını göz önünde bulundurmadığını da unutmamak gereklidir. Bu nedenle özel-

8 UNESCO, Toby Mendel and Laura Notess. "The Right to Information in Times of Crisis: Access to Information – Saving Lives, Building Trust, Bringing Hope!". 2020.

9 Sendai framework for disaster risk reduction 2015–2030. In: UN world conference on disaster risk reduction, 2015 March 14–18, Sendai, Japan. Geneva: United Nations Office for Disaster Risk Reduction; 2015.

likle üretici YZ'nin kullanıldığı açık ve gerçek zamanlı veri aktarımlarında etik ve yasal sorunların dikkat ve hassasiyetle değerlendirilmesi gereklidir.

Büyük sağlık verilerinin kullanıldığı çok merkezli uluslararası sağlık araştırmalarında sınır ötesine veri aktarımının yarattığı etik ve yasal sorunların çözümüne yönelik olarak federatif veri sistemleri geliştirilmektedir. Bu sistemlerin en son örneği olan, verinin aktarılması yerine veriyi işleyen algoritmanın veriyi depolandığı yerde ziyaret ederek veriyi kullanması ve daha sonra veriyi yerinde bırakarak uzaklaşması esasına dayanan veri ziyareti (data visitation) yöntemi, yaygınlaşmaya başlamaktadır. Açık veri sistemlerinde veri ziyareti yöntemi ile çalışan araştırmacılar, bir taraftan veri aktarımın beraberinde getirdiği bir kısım etik ve yasal sorunlardan muaf olurlarken, kendi araştırma sonuçlarını da bu açık platformlara sunarak açık verinin çoğalmasına ve bilimsel bilginin paylaşılmasına katkıda bulunmaktadır. Bu konuya, bu bölümün kapsamının dışına çıkmamak için daha detaylı yer verilmeyecek olsa da teknolojinin getirdiği etik sorunlara yönelik bazı çözümlerin yine teknoloji tarafında üretilebilir olduğunu gösterdiğinin altını çizmenin teknoloji ve sağlık etiği açısından önemli olduğu düşünülmektedir.

YZ aynı zamanda insan gönüllülerde yürütülen klinik araştırmaların etik iznini veren klinik araştırmaların etik kurullarının değerlendirme süreçlerinde de kullanılmaya başlanmıştır. Bir araştırmanın "insan denekler" üzerinde yapılması etik açıdan oldukça katı kurallara bağlıdır ve her araştırma, uygulamaya başlamadan önce, bu katı kurallara uygunlukları açısında bağımsız etik kurullar tarafından değerlendirilmektedir. Bu süreç hem Helsinki Bildirgesi, Oviedo Sözleşmesi[10] gibi uluslararası mevzuat tarafından hem de Klinik Araştırmalar Yönetmeliği gibi ulusal mevzuat tarafından da zorunlu tutulmaktadır. Etik kurul değerlendirmelerinde YZ kullanımı, esasında uzman sistemlerin bir diğer kullanım alanı olarak karşımıza çıkmaktadır. Başvuran araştırma projesinin etik kurallara uygunluğu YZ tarafından ön değerlendirmeye tabii tutularak projenin bilimsel yeterliliği, gönüllü deneklere yönelik risk analizinin mevcudiyeti, risk azaltma/önleme stratejilerine yer verilip verilmediği değerlendirilmektedir. Elbette YZ'nin söz konusu kullanımının basit bir içerik analizine dayandığını unutmamak gerekir. Zira bir araştırma projesinin etik uygunluğu salt

[10] Council of Europe. Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine. European Treaty Series - No. 164. Oviedo; 4.IV.1997.

bir etik uyum listesi taramasından ziyade araştırmanın kısa ve uzun dönem etkileri, deneklere ve tüm insanlara olan olası fayda ve riskleri, istatistik metodolojinin değerlendirilmesi, araştırmada kullanılan bilimsel metodolojinin amaca uygunluğu, bütçe kaynaklarının ve bütçe kalemlerinin kapsamı ve uygunluğu gibi oldukça detaylı ve kompleks bir inceleme sürecini içermektedir. Bu sürecin doğru ve eksiksiz yürütülmesi için araştırma etiği diskorsuna hâkim olunması gereklidir. Bu hakimiyet üretici YZ da dahil, güncel YZ sistemlerinde -henüz- mevcut değildir.

YZ bilimsel araştırma sürecinde kullanımının son ve belki de en yoğun tartışmalara yol açan alanı bilimsel yayınlardaki kullanımıdır. Üretici YZ'nin yeni içerik geliştirme kapasitesi nedeniyle gerçekte bilim insanına ait olan özgün hipotez geliştirme, araştırma metodolojisi belirleme ve araştırma sonuçlarının mevcut bilimsel literatür ışığında değerlendirilmesi gibi aşamalar üretici YZ'ye devredilebilir olmuştur. Bu durum bilimsel dürüstlük başta olmak üzere bilimsel bilgi üretimi ve yazımının pek çok aşamasında etik sorunlara yol açmaktadır. Her ne kadar sağlık alanındaki bilimsel yazını doğrudan ilgilendirse de bu kitabın kapsamı dışında kaldığı düşünüldüğünden bu konuya daha detaylı yer verilmeyecek, sadece konunun önemine dikkat çekmekle yetinilecektir.

YZ'nin sağlık alanında kullanımını arttırmaya yönelik güncel araştırma geliştirme faaliyetlerinden bir kısmı aşağıda sıralanmıştır:

1. YZ'nin hastalara danışmanlık vermek üzere sanal sağlık desteği sunması ve böylece özellikle sağlık hizmetlerine erişim sorunu yaşayan ücra bölgelerdeki hastaların doğru yönlendirilmesi hedeflenmektedir.

2. YZ amino asit dizilimlerini inceleyerek üç boyutlu konfigürasyonlarını tahmin etme amacıyla kullanılmaya başlanmıştır. Bu kullanım alanı sayesinde "in-silico" proteinler olarak adlandırılan ve ilaç geliştirilmesinde kullanılması hedeflenen sentetik protein yapılarının üretimine çalışılmaktadır. Geride bıraktığımız COVID-19 pandemisi esnasında bu tip çalışmalar SARS CoV-2 spike proteininin ACE reseptörlerine bağlanmasını engelleyecek sentetik protein geliştirilmesi amacıyla kullanılmaya çalışılmıştır. Sentetik proteinlerin ayrıca YZ algoritmalarının eğitimi için veri kaynağı olarak da kullanılmasına çalışılmaktadır.

3. Halk sağlığı sektörü dışındaki sosyal medya gibi açık internet kaynaklarındaki verilerin kullanımı ile yapılan dijital epidemiyolojik çalışmalar,

halk sağlığı risklerinin önceden belirlenebilmesi amacıyla kullanılmaya çalışılmaktadır[11].

4. Elektronik sağlık verilerinin YZ destekli sağlık öngörüleri (AI-driven insights) oluşturmak amacıyla agrege edilmesi temeline dayalı bir çalışmadır. Normalde bir arada değerlendirilmeyen verilerin bir öngörü oluşturabilecek şekilde anlamlandırılması ve böylece başka kaynaklarca tespit edilemeyen bazı sağlık risklerinin öngörülmesi ve böylece erken tanı ve tedavi olanaklarının kullanılabilmesi amacını taşımaktadır.

SONUÇ VE ÖNERİLER

YZ geniş disseminasyon kapasitesine sahip yıkıcı bir teknolojidir. Sağlık sektörü YZ'nin en fazla fayda üretebileceği alanlardan biri olarak görülmektedir. Bugüne kadar genellikle KDS olarak hekimlere yardımcı olacak bir konunda gelişmiş olan YZ, üretici YZ'nin kullanıma girmesi ile hekimlerin yaptığı işlerin bir kısmını onların yerine yapabilecek ya da hekimlerin yapamadığı bazı uygulamaları yerine getirebilecek bir konuma gelmeye adaydır.

Ancak yüksek fayda beklentisi beraberinde ciddi etik, yasal ve sosyal riskler getirmektedir. Söz konusu risklerin kişisel veriler ile ilgili olan bazılarına yukarıdaki paragraflarda yer verilmiştir. Risklerin en aza indirilmesi ve YZ'den en yüksek verimin alınması için bazı risk azaltma stratejilerine başvurulabilir. Bunlar, "kırmızı bayrak çekmek" (red flagging) diye tabir edilen ve yüksek risk içeren uygulamaların belirlenmesi için uzman ekiplerin kurulması, geri döndürülemez ve yüksek risk içeren kullanımların kısıtlanması ya da risk bertaraf edilene kadar kullanımın ertelenmesi ve kamunun açık kullanımına sunulmadan önce söz konusu risk azaltma/engelleme aşamalarının tamamlanması olarak sıralanabilir. 2020 yılında Birleşmiş Milletler Üst Düzey Panelinde risk azaltma/önleme için uluslararası iş birliği çağrısında bulunulmuştur. Bu çağrı kapsamı her ne kadar sağlık sektörü ya da kişisel verilerin korunması için spesifik olmasa da ortak çalışmaların üreteceği risk engelleme/azaltma stratejilerinin genel olarak tüm alanlardaki kullanıma yönelik olacağı düşünülebilir[12]. 2021

[11] Ginsberg J, Mohebbi MH, Patel RS, Brammer L, Smolinski MS, Brilliant L. Detecting influenza epidemics using search engine query data. Nature 2009;457(7232):1012–4. https://doi.org/10.1038/nature07634

[12] UN Secretary-General's High-Level Panel on Digital Cooperation. www.un.org

yılında yine Birleşmiş Milletler tarafından bu kez İnsan Hakları Komisyonunca YZ uygulamalarının gizlilik ve mahremiyet ihlalleri açısından güvenli olduğu ve hak ihlali risklerine karşı önlemlerin alındığı kanıtlanana kadar kullanımının ertelenmesi önerilmiştir[13]. Benzer bir yaklaşımı 2021 yılında UNESCO tarafından yayınlanan ve YZ'nin etik sınırlarını belirleyen ilk global normatif deklarasyonda da görmekteyiz[14]. Son olarak 2023 yılında yayınlanan Avrupa Birliği YZ yasasında tanımlanan üç risk kategorisi YZ uygulamalarının etik açıdan güvenli ve sorumlu kullanımına ilişkin bir çerçeve belirlemiştir[15].

Sağlık alanında kullanılan ya da kullanılmak üzere geliştirilmeye çalışılan YZ uygulamalarında söz konusu uluslararası mevzuatta değinilen risk önleme stratejileri "tedbir ilkesi (precautinary principle) ile hayata geçirilebilir. Bu ilke bir YZ uygulamasının bilimsel kanıtlar elde edilene kadar insanlar üzerinde kullanımın ertelenmesini kapsamaktadır. Şüphesiz etik ve yasal sınırlara riayet etmek koşulu ile veri kalitesinin ve veri erişiminin artması ve veri alt yapısının sağlık sistemi alt yapısına entegrasyonu YZ'nin sağlık alanında daha etkin ve verimli kullanım alanları bulmasına yardımcı olacaktır.

---

13 Annual Report of the United Nations High Commissioner for Human Rights and reports of the Office of the High Commissioner and the Secretery-General. The Right to Privicy in the Digital age. www.ohchr.org

14 UNESCO Recommendation on the Ethics of Artificial Intelligence. www.ohchr.org

15 EU AI Act 2023. www.ec.europa.eu

KAYNAKÇA

Aikins, J.S., Kunz, J.C., Shortlife, E.H., Fallat, R.J. PUFF: An expert system for interpretation of pulmonary function data. Computers and Biomedical Research. 1983: 16 (13):199-208.

Annual Report of the United Nations High Commissioner for Human Rights and reports of the Office of the High Commissioner and the Secretery-General. The Right to Privacy in the Digital age. www.ohchr.org.

Colby, K.M., Watt, J.B., Gilbert, J.P. A Computer Method of Psycotheraphy. The journal of Nervous and Mental Disease. 1966: 142 (2): 148-52.

Council of Europe. Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine. European Treaty Series - No. 164. Oviedo; 4.IV.1997.

Covenney P., Highfield R. Why Some Scientists Believe the Future of Medicine Lies in Creating Digital Twins. https://time.com/6268882/digital-twins-medicine-future/.

EU AI Act 2023. www.ec.europa.eu.

Ginsberg J, Mohebbi MH, Patel RS, Brammer L, Smolinski MS, Brilliant L. Detecting influenza epidemics using search engine query data. Nature 2009;457(7232):1012–4. https://doi.org/10.1038/nature07634.

Helsinki Bildirgesi. Dünya Hekimler Birliği Bülteni, 2013:79 (4); 373-374.

Sendai framework for disaster risk reduction 2015–2030. In: UN world conference on disaster risk reduction, 2015 March 14–18, Sendai, Japan. Geneva: United Nations Office for Disaster Risk Reduction; 2015.

UN Secretary-General's High-Level Panel on Digital Cooperation. www.un.org.

UNESCO Recommendation on the Ethics of Artificial Intelligence. www.ohchr.org.

UNESCO, Toby Mendel and Laura Notess. "The Right to Information in Times of Crisis: Access to Information – Saving Lives, Building Trust, Bringing Hope!". 2020.

Wasim F.J. Adressing Clinical Documentation Challemges: The Role of AI-Powered Digital Scribes. Journal of Artificial Intelligence &Cloud Computing. 2022;1(1):1-5.

Watson, J., Crick, F. Molecular structure of nucleik acids: A structure for Deoxyribonucleic acid. Nature. 1953: 171, 737-738.

Weizenbaum, J. Computer power and human reason: From Judgement to calculation.W.H. Freeman & Co. NewYork, 1976.

İSTİHDAMDA YAPAY ZEKÂ

Dr. Öğr. Üyesi Başak OZAN ÖZPARLAK*

I. İSTİHDAM SÜREÇLERİNDE YAPAY ZEKÂ SİSTEMLERİ

A. İSTİHDAMDA ALGORİTMİK DÖNÜŞÜMÜN VERİ KORUMA HUKUKU AÇISINDAN ÖNEMİ

1. İstihdamda Yapay Zekâ

Yapay Zekâ (YZ) ve istihdam kavramlarını bir arada kullandığımızda akıllara ilk gelen konu mesleklerin geleceği ve iş gücü dönüşümüdür[1]. Ülkemizin ilk Ulusal YZ Strateji Belgesi'nde de mesleklerin dönüşümü ve bu gerçeklik ile ilgili alınacak önlemlere yer verilmiştir[2]. Mesleklerin geleceği, insanların ne yaparak geçimlerini sağlayacakları sorusu kadar, ne ile hayatlarına anlam katacakları ile de doğrudan ilişkilidir. Bu nedenle salt teknolojik bir konu değildir. Bunun yanı sıra, YZ teknolojileri ile dönüşmeye başlayan mesleklerin geleceği konusunun mühendislik, eğitim bilimi, hukuk, siyaset bilimi, ekonomi, sosyoloji ve psikoloji alanlarını da kapsayacak şekilde ve interdisipliner şekilde[3] çalışılması son derece önemlidir. Tüm

* Özyeğin Üniversitesi Hukuk Fakültesi Bilişim Hukuku Anabilim Dalı

1 Teknoloji ve iş gücü arasındaki yer alan iki temel ilişki; verimlilik artışı ve işlerin makinalarca yapılmaya başlanması ile çalışan insan sayısındaki değişimdir. Bkz: Akçomak, İ. S.: Teknoloji, Küreselleşme ve İşgücü Piyasaları, (ed. Akçomak, İ. S., Erdil, E., Pamukçu, M.T. ve Tiryakioğlu, M.) "Bilim Teknoloji ve Yenilik: Kavramlar, Kuramlar ve Politika", 1. Baskı, İstanbul 2016, s. 302-303.

2 Cumhurbaşkanlığı Dijital Dönüşüm Ofisi: "Ulusal Yapay Zekâ Stratejisi", *https://cbddo.gov.tr/SharedFolderServer/Genel/File/TR-UlusalYZStratejisi2021-2025.pdf* (E.T. 20.5.2024), s. 80.

3 İstihdamda YZ kullanımına dair 2022 yılında yapılan bir çalışmaya (Kişi, N.: *İnsan Kaynakları Yönetiminde Yapay Zeka: Bibliyometrik Bir Analiz*, Journal of Research in Business 2022, C.7 S.2, s. 499.) göre İK süreçlerinde YZ kullanımına dair en çok atıf alan ve bu konuda interdisipliner çalışmalara bir örnek teşkil eden, çevrim içi iş ilanlarının analizi ile büyük veri çağının meslekleri için gerekli olan becerileri tespite yönelik çalışma için bkz: De Mauro, A./Greco, M./Grimaldi, M./Ritala, P.: *Human Resources For Big Data Professions: A Systematic Classification of Job Roles and Required Skill Sets*", Information Processing & Management 2017.

dünyada özellikle eğitim alanında yapılması gereken yeniliklerin de geç kalınmadan ele alınması gerekmektedir. Günümüzde özellikle Covid-19 pandemisi ile başlayan belirsizlikler çağında, çocuklar ve gençlerin hayatlarının sonraki on yılında dahi ne yapacaklarına ilişkin hayal kurmaları giderek zorlaşmaktadır. Yeni nesillerin gelecek ile ilgili tahayyüllerine umut katabilmek için, YZ konusunda farklı alanlarda gerçekleştirilen çalışmaların ortak misyonu, bu konuda çalışanların bireysel kariyerlerinden ziyade; çocuklarımız, ülkemiz ve tüm gezegenimizi eşit, adil ve faydalı YZ sistemleri geliştirmenin ve kullanmanın yollarını bularak dünyamızı daha iyiye götürmek olmalıdır.

Kasım 2022'de kamuoyu ile paylaşılan ChatGPT'nin 2024 Mayıs ayında yayınlanan "Bahar Güncellemesi"[4] ile *4/o* versiyonu, 12 Eylül 2024 tarihinde ise o1 sürümü kullanıma sunulmuştur. ChatGPT 4/o güncellemesinin özel önemi ise üretken YZ modellerinin sadece kapasitesinin değil insanlar ile etkileşim şeklinin de ne kadar hızlı değiştiğini göstermesi olmuştur. İnsanlar ile eş zamanlı ses, görüntü ve metin üzerinden etkileşim sağlayabilen ChatGPT 4/o, eğitimin artık öğretenden öğrenene bir bilgi akışı şeklinde yıllarca sürmesine ve bilginin öğrenen tarafından kendine sorulduğunda geri aktarımına dayalı eğitim modelinin geleceğin dönüşecek mesleklerine ve yeni beceri ihtiyaçlarına uygun olarak değiştirilmesi gerektiğini adeta haykırmaktadır. Dünyanın her köşesinde, eğer eğitim alma fırsatına sahipler ise çocuklar ve genç bireyler uzun yıllar boyunca ve giderek hayatın akışından koparak, YZ alanındaki gelişime uygun olmayan eğitim içeriklerine tabi şekilde belirsiz bir geleceğe doğru ilerlemektedirler. Günümüzün ilk ve orta öğretim ile üniversite modelleri, eğer dinamik ve esnek bir yapıya sahip değil ise, önümüzdeki on yılın dahi gerçekleri ile tam olarak örtüşmeyecektir. Özellikle üretken/üretici yapay zekâ modelleri[5] alanındaki hızlı teknolojik gelişmeler ile birlikte, pek çok farklı sektörde çalışan insanın bilişsel faaliyetlerini içeren emek süreçlerinde insana duyulan ihtiyacın azalması ile çok yakın bir gelecekte yaratıcı ve bilişsel sü-

---

4 OpenAI (2024), *"Spring Update", https://openai.com/index/spring-update/* (E.T. 20.5.2024).

5 Üretken YZ modelleri, istihdamda olduğu gibi pek çok farklı alanda çok farklı amaçlarla ve herkes tarafından kullanılabilecek son derece güçlü sistemler olduğundan, bu YZ modellerinin mahremiyet ve güvenlik risklerinin daha önceki yapay zekâ modellerinden hem nitelik hem nicelik yönünden çok daha fazla olduğu, bu nedenle bu risklerin en aza indirgenmesini sağlamanın sadece teknolojik önlemler ile değil; etkili yasal düzenlemelerle mümkün olabileceği görüşü için bkz: Ozan Özparlak B/Çetin M: *ChatGPT ve Üretici Yapay Zekâ Modellerinde Mahremiyet ve Güvenliğin Hukuki Boyutu*, MÜHFHA, C. 29, S. 2, 2023, s. 1005.

reçleri de kapsayan işsizlik riskinin ortaya çıkması mümkündür[6]. Çalışmamız kapsamı dışındaki bu konuya dair değerlendirmelerin, gelecek öngörüleri ve çözüm önerileri ile birlikte ayrıca ele alınması önemli bir gerekliliktir.

2. İstihdamda Yapay Zekâ Konusunu Ele Almanın Güncel Önemi

Bu çalışmamızın ana fikrini oluşturan ve yapay zekâ ile istihdamın kesiştiği ve mesleklerin dönüşümü dışındaki ikinci alan ise çalışma hayatını sosyal, ekonomik ve hukuki açıdan yakın bir gelecekte değil, son yıllarda giderek artan şekilde etkileyen ve özellikle insan kaynakları süreçlerini kapsayan *"algoritmik dönüşümdür"*[7]. Algoritmik dönüşüm, çalışma ilişkilerinin tüm süreçlerinde yapay zekâ sistemlerinin farklı şekillerde kullanılmaya başlandığı bir çağı işaret etmektedir. Bu dönüşüm, aynı zamanda bilişim hukuku ile iş hukuku arasında zorunlu bir ortak payda da oluşturmaktadır. Bu ortak payda, "*algoritmik yönetim"* kavramı ile nitelendirilen ve verinin, çalışma hayatında insan emeğinden sonra adeta ikinci (fakat *ikincil* olmayan) ve emekle eş değer bir ham madde olarak değer gördüğü yeni bir istihdam çağını da ifade etmektedir. Bu nedenle, esasen algoritmik yönetim kavramı, istihdamda yapay zekâ başlıklı bir çalışmanın omurgası niteliğindedir.

Mahremiyet ile ilgili hukuki çalışmaların sınırları açısından, istihdamda YZ uygulamalarının kullanımının yol açtığı ayrımcılık gibi sonuçların da bu alanın kapsamında ele alınıp alınamayacağı akla gelebilir. Özellikle veriden beslenen teknolojilerin gelişimi ile birlikte mahremiyet çalışmalarının sınırlarının da aynı oranda genişletilmesine ihtiyaç duyulmuştur. Bu konuda en geniş kabul gören tespitlerden birini yapan *Solove*; mahremiyet ile ilgili hukuki çalışmaların veri koruma hukukundan başlayarak işe alımda ayrımcılığa kadar uzanan geniş bir alanı kapsadığını belirterek bu alanda

---

6 International Monetary Fund (IMF), *"Gen-AI: Artificial Intelligence and the Future of Work" (https://www.imf.org/-/media/Files/Publications/SDN/2024/English/SDNEA2024001. ashx* E.T. 8.4.2024), s. 3. Söz konusu IMF Raporu'nda; dünya genelindeki işlerin %40'ının yapay zekâdan etkileneceği, gelişmiş ekonomilerde ise bu oranın %60'a kadar çıkacağı işaret edilmiştir. Bu oranın yaklaşık yarısının olumsuz anlamda yapay zekâdan etkileneceği ön görüsünde bulunan IMF, bu olumsuz etkinin düşük maaşlar ve daha az işe alımla kendini göstereceğini, bazı işlerin ise tamamen ortadan kalkacağını belirtmektedir. Büyüme ve küçülme yaşanacak işler ile ilgili ayrıntılı bilgi için bkz: World Economic Forum (WEF): *"Future of Work 2023" (https://www3.weforum.org/docs/WEF_Future_of_Jobs_2023. pdf* E.T. 8.4.2024), s. 29 vd.

7 Ajunwa, I.: *The Paradox of Automation as Anti-Bias Intervention*, Cardozo L. Rev. 2020, 41, s. 1683 vd.

çalışan hukukçuların bilgi kapitalizmine kadar uzanan genel sorunları da ele alabilmesinin yolunu açmıştır[8]. *Solove'*nin bu yaklaşımı açısından değerlendirildiğinde, istihdamda YZ kullanımının sadece iş hukuku açısından değil, aynı zamanda mahremiyet tartışmalarının ve kişisel verilerin korunmasına dair hukuki tartışmaların kapsamında değerlendirilebilir. Gerçekten de veri temelli ekonomiye en hızlı şekilde dahil olan alanlardan biri istihdam süreçleri olmuştur.

Çalışmamızın ilerleyen bölümlerinde de aktaracağımız üzere, istihdam veya istihdam dışı alanlardan elde edilen veriler ile bir iş ilanının yayınlanmasından başlayarak, işe alım, iş ilişkilerinin yönetimi ve sona erdirilmesi süreçlerinin tümünde algoritmik araçlar, makine öğrenmesi ve yapay zekâ kullanımı olağanlaşmaktadır. Tüm bu istihdam süreçlerinde kullanılan verinin işlenmesi ve YZ sistemleri veya modelleri ile veriden anlam çıkarılarak karar alınmasında kullanılması işverenlere hız ve zaman kazandırmakta, ayrıca insan kaynaklarına harcanan kaynaklardan da tasarruf sağlamaktadır.

Öte yandan, üretken YZ modellerinin gelişmesi ile sadece işverenler değil, bir iş başvurusunda bulunan kişiler tarafından da CV hazırlama, kariyerlerine uygun iş ilanlarına otomatik olarak başvurma, başvuru mektubu yazma ve hatta iş mülakatlarına çalışma konularında YZ teknolojisinden destek alınmaya başlanmıştır[9].

İstihdamda YZ kullanımını içeren yukarıda sayılan tüm süreçler, aynı zamanda hukuki açıdan da bir denetime ve gerektiğinde etkili yaptırımları gerektirmektedir. Çünkü, Anayasa'dan başlayarak gerek iş hukukuna dair mevzuatta gerekse de veri koruma hukuku mevzuatındaki düzenlemelerin uygulanabilmesinin ilk adımı bu hukuki düzenlemeler ile korunan hakların ihlal edildiğinin farkında olunması ve hukuki başvuru imkânının kullanılmasıdır. Hukuki açıdan istihdamda YZ kullanımının yarattığı en önemli zorluk ve üzerinde en çok durulması gereken konu, kanımızca istihdamdaki YZ araçlarının şeffaflık ve açıklanabilirliğinin sağlanmasıdır. Bunun nedeni, işe alımda ayrımcılık başta olmak üzere yasal düzenlemelere aykırılıkların ve iş başvurusu yapan adaylar ile işçilerin yasalar ile korunan haklarının ihlalin görünürlüğünü ortadan kaldırma riskini taşımasıdır.

---

8 Bu yaklaşımın güncel bir eleştirisi için bkz: Angel, M. P./Calo, R.: *Distinguishing Privacy Law: A Critique of Privacy as Social Taxonomy*, Columbia Law Review 2023, 123.

9 Michael Page Türkiye: *"Yapay Zekâ ile İş Bulun: Teknolojiyi ve İnsan İçgörülerini Birlikte Kullanın" (https://www.michaelpage.com.tr/advice/kariyer-tavsiyeleri/kariyer-geli%C5%9Fimi/nyr24-yapay-zeka-ile-is-arama* E.T. 20.5.2024).

Kişisel Verileri Koruma Kurumu (Kurum) tarafından 2021 yılında yayınlanan *"Yapay Zekâ Alanında Kişisel Verilerin Korunmasına Dair Tavsiyeler"*[10] ile YZ geliştiricileri, üreticileri, servis sağlayıcıları ve karar alıcıları için getirilen tavsiyelerin özünde, YZ alanında kişisel verilerin işlenmesinde bireylerin temel hak ve özgürlüklerini koruyucu şekilde hukuka uygun, dürüstlük, ölçülülük, hesap verebilirlik, şeffaflık, kişisel verilerin doğru ve güncel olması, kişisel veri kullanım amacının belirli ve sınırlı olması ilkelerinin ve veri güvenliği yaklaşımının göz önüne alınması gerekliliği yer almaktadır[11].

Ayrıca ülkemizin ilk Ulusal YZ Stratejisinde benimsenen YZ etik ilkeleri arasında *"Çeşitliliğin ve Kapsayıcılığın Sağlanması"* ilkesinin yer alması konumuz bakımından da son derece önemlidir. Bu ilkeye göre; yapay zekâ teknolojilerinin üretimi, geliştirilmesi ve uygulanmasında ayrımcılığa yol açılmaması ve veri setlerinin bu konuda denetlenmesinin gerektiği belirtilmiştir[12]. İşe alımda ve çalışanların performans değerlendirmelerinde kullanılan YZ sistemlerinin bu ilkelere uygun olarak geliştirilmesi ve kullanılması, istihdamda ayrımcı uygulamaların engellenmesi ve çalışma hayatında fırsat eşitliğinin sağlanması üzerinde de doğrudan etkilidir.

OECD'nin 2024 yılında yayınladığı *"Using AI in the Workplace"* ("İş yerinde YZ Kullanmak") başlıklı raporda[13] belirtildiği üzere iş yerinde YZ sistemlerinin artan kullanımı, işçiler ve iş adayları hakkında daha fazla veri toplanmasına ve analiz edilmesine yol açmaktadır. Bu verilerin arasında özel nitelikli kişisel veriler de yer alabilir: işçilerin hareketleri, kalp atış hızları ve kan basınçları gibi. Hatta, artan veri işleme faaliyeti, sürekli bir izlenme psikolojisine yol açarak çalışanlarda strese ve stres kaynaklı rahatsızlıklara da yol açabilir. Tüm bu nedenler göz önüne alınarak OECD istihdamda YZ kullanımına ilişkin aşağıdaki önerilerde bulunmuştur[14]:

---

10 Kişisel Verileri Koruma Kurumu*: "Yapay Zekâ Alanında Kişisel Verilerin Korunmasına Dair Tavsiyeler",* Ankara, KVK Yayınları, 2021.

11 Kişisel Verileri Koruma Kurumu, *"Üretici Yapay Zekâ Çağında Kişisel Verileri Yeniden Düşünmek",* KVKK Bülten Temmuz 2023 Sayı:1, Ankara, 2023, s. 15.

12 T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, s. 59.

13 OECD: *"Using AI in the Workplace: Opportunities, Risks and Policy Responses", https://www.oecd-ilibrary.org/docserver/73d417f9-en.pdf?expires=1716551203&id=id&accname=guest&checksum=ADAE8EEAC7DFA736CD176BA19A80AC3B* E.T. 20.5.2024).

14 OECD: *"Using AI in the Workplace: Opportunities, Risks and Policy Responses".*

- YZ sistemlerindeki kişisel verilerin mahremiyeti ve güvenliğini değerlendirmek için etki değerlendirmeleri yapılması ve sonucuna göre kalite etiketleri uygulaması.
- İşçilerin kişisel verilerinin toplanmasını, kullanılmasını, çıkarılmasını ve ifşa edilmesini kısıtlamak (6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 4. maddesinde düzenlenen veri işlenmesinde veri minimizasyonu bu öneriyi karşılayan yasal bir dayanaktır).
- İşçilerin kişisel verilerinin koruma ve verilerin uygun şekilde işlenmesi için gereksinimlerin karşılanması (Bu öneri ise hukukumuzda 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 12. maddesinde yasal bir gereklilik olarak yer almaktadır).
- İşverenler tarafından toplanan veriler ve kullanım amaçları hakkında işçilere bilgi sağlanması (Bu öneri, şeffaflık ilkesinin bir yansımasıdır ve 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 4. maddesinde düzenlenen veri işlenmesinde uyulması gereken ilkeler ile örtüşmektedir).
- İşçilerin kişisel verilerini düzeltme, silme, vazgeçme veya verilerin kullanılmasının sınırlanması haklarının tanınması.
- İyi veri koruma uygulamalarına sahip YZ sistemleri için kalite etiketleri ve sertifika rejimi uygulanması (Bu tür bir sertifikasyon sistemi, iyi uygulamaların teşviki ile birlikte, rekabetin sadece teknik doğrulukta değil aynı zamanda mahremiyet ve güvenlik alanında da artırılmasını sağlayabilme potansiyeline sahiptir).

Her ne kadar daha önce çalışma ilişkilerinde YZ kavramlarını farklı eserlerde ele almış olsak da, OECD'nin yukarıda anılan raporu gibi bu alanda son bir yılda pek çok önemli görüş ve öneri yayınlanmış, ayrıca yine son bir yılda dahi gerek teknolojik ilerlemeler gerekse de regülasyonlar açısından konuyu yeniden ele alma gerekliliği ortaya çıkmıştır. Bu güncel gelişmeler konusunda Türk literatürüne katkı verebilmek ve önceki çalışmalarımız ile tekrara düşmemek adına, biz bu çalışmamızda güncel uygulamalar ile YZ sistemlerinin istihdamda kullanımını, algoritmik yönetim kavramı çerçevesinde açıklayarak, daha sonra sırası ile 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun (6698 Sayılı Kanun) 6. maddesinde yapılan ve 1 Haziran 2024 tarihinde yürürlüğe giren değişiklikleri, AB YZ Kanunu ve yeri geldiğinde ABD'de kabul edilen ilgili düzenlemeleri ve birçoğu 2024 yılında yayınlanan konuya ilişkin güncel raporları ele almayı uygun gördük.

B. İSTİHDAM SÜREÇLERİNDE ALGORİTMİK YÖNETİM KAVRAMI

Birleşik Krallık'ta Kamu Politikaları Araştırma Enstitüsü'nün YZ sistemlerinin iş gücüne etkisi üzerine yapmış olduğu araştırmanın Mart 2024 yılında yayınlanan sonuçlarına göre; üretken YZ modellerinin gelişiminden fazla etkilenecek ve insan iş gücünün en hızlı değişime maruz kalacağı sektörlerin başında yönetici asistanlığı ve sekreterlikten (%69 oranında etki) hemen sonra insan kaynakları (%68 oranında etki) sektörü gelmektedir[15]. Bunun en önemli nedenlerinden biri, insan kaynaklarında çalışanların görevlerini de içeren iş ilişkisi süreçlerinin tümünde, özellikle üretken YZ modellerinin de gelişimi ile giderek yaygınlaşan şekilde YZ araçlarının kullanılmaya başlanmasıdır.

İstihdam süreçleri, süreklilik arz eden, ekonomik sistemdeki tüm sektörlerde kendisine yer bulan, farklı paydaşlar katılımı ile işleyen, farklı hukuki düzenlemeler kapsamında yasal uyum gerektiren çok katmanlı, karmaşık ve maliyetli süreçlerdir. Bu süreç; iş ilanlarının yayınlanması, iş başvurusunun yapılması ve değerlendirilmesi, işe alım, iş ilişkisinin yönetimi ve iş sözleşmesinin sona ermesini kapsayan ve bu nedenle aynı zamanda süreklilik arz eden niteliktedir. İstihdam alanındaki her bir unsur, bünyesinde pek çok farklı aşamayı içermektedir. Örneğin iş ilişkilerinin ilk adımı olarak nitelendirilebilecek işe alım sürecinin tek başına kendisi dahi, pek çok farklı aşamadan oluşur. İşe alımda; bir iş ilanının hangi mecralarda yayınlanacağının tespiti, bu ilanı görmesi istenen hedef kitlenin belirlenmesi, bu ilanı görenler arasından yapılan ön değerlendirme, bu değerlendirme sonucunda iş görüşmesi yapılacak adayların belirlenmesi, mülakatların çevrim içi veya yüz yüze olacak şekilde yapılması ve işe alım kararının verilmesi ile iş sözleşmesinin kurulması gibi farklı unsurlar yer almaktadır[16]. Gerek işe alım yapan işverenler gerekse de iş arayışında olan bireyler açısından işe alım sürecinin olabildiğince hızlı sonuçlanması ve aynı zamanda işe en uygun adayın, adaya en uygun işin doğru olarak eşleşmesi haklı olarak arzu edilmektedir. İş ile adayın hızlı ve doğru şekilde eşleşmesi özellikle sayıca fazla başvuru olan büyük iş yerlerinde başvuru sayısının giderek

---

15 Institute for Public Policy Research (IPPR): *"Transformed by AI: How Generative Artificial Intelligence Could Affect Work In The UK and How To Manage It"* (https://ippr-org.files.svdcdn.com/production/Downloads/Transformed_by_AI_March24_2024-03-27-121003_kxis.pdf E.T. 1.6.2024), s. 17 ve 19.

16 Engin M., Ozan Özparlak, B.: İşe Girişte Yapay Zeka ve Ayrımcılık (ed. Erdem Büyüksağış), "Hukuk Perspektifinden Yapay Zeka", 1. Baskı, İstanbul 2022.

artışı nedeni ile güçleşebilmektedir. Bu nedenle, yapay zekâ sistemlerinin işe alımda kullanımı bir ihtiyaç olarak ortaya çıkmaktadır.

Algoritmik yönetim kavramı, ilk kez 2015 yılında CHI (Conference on Human Factors in Computing Systems – Bilgi İşlem Sistemlerinde İnsan Faktörü) Konferansında sunulan "Makineler ile Çalışmak: Algoritmik ve Veri Güdümlü Yönetimin İnsan Çalışanlar Üzerindeki Etkileri" başlıklı makalelerinde Min Kyung Lee ve diğerleri tarafından kullanılmış ve şu şekilde tanımlanmıştır: "*insan işlerinin 'yönetim işlevlerini üstlenen yazılım algoritmaları' ve 'algoritmaları destekleyen kurumsal cihazlar' aracılığıyla gerçekleştirilmesi, optimize edilmesi ve değerlendirilmesi*"[17].

Alex Wood tarafından AB Komisyonu için hazırlanan ve Temmuz 2021'de yayınlanan bir raporda ise; algoritmik yönetim kavramı, müşteri memnuniyeti derecelendirilmesinde olduğu gibi, çalışanların davranışsal, duygusal ve biyolojik verilerinin işlenmesine dayanan iş performansının değerlendirmesinde de kullanılmaktadır[18]. Veriden beslenen insan kaynakları ve iş yeri yönetiminin yine veri ile geliştirilen algoritmik araçlar ile yapılmasına dayanan algoritmik yönetim, bu nedenle veri koruma kuralları ile doğrudan ilintilidir.

İşçilerin gerek iş yasaları gerekse de veri koruma kurallarından kaynaklanan haklarını kullanabilmeleri ancak haklarını kullanmalarını gerektiren bir riskin veya ihlalin varlığından haberdar olabilmelerine bağlıdır. İstihdamda YZ kullanımının farkında olmayan ve bu sistemlerin ortaya çıkardığı sonuçlara nasıl ulaştığını bilmeyen bireyler için temel haklarını kullanmaları da oldukça güçtür. Gerçekten, iş başvurusu yapan kişi farkında olsun veya olmasın, YZ kullanılması ile başvurucunun kişisel verilerinin işe alım sürecine dahil edilmesi söz konusu olmaktadır[19]. Bu nedenle OECD tarafından önerilen politikaların başında, YZ sistemlerinin istihdamda (işe alımda ve iş yerinde) kullanıldığına dair taraflara şeffaflık sağlanması yer almaktadır[20].

---

17 Lee, M.K./Kusbit, D./Metsky, E./Dabbish, L.*: "Working with Machines: The Impact of Algorithmic and Data-Driven Management on Human Workers"* Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems CHI 2015, Association for Computing Machinery, New York, ABD, 1603–1612, (https://doi.org/10.1145/2702123.2702548, E.T. 8.4.2024), s. 1603.

18 Wood, A. J.: Algorithmic Management Consequences for Work Organisation and Working Conditions JRC Working Papers Series on Labour, Education and Technology 2021, s. 13, *(https://ec.europa.eu/jrc/sites/default/files/jrc124874.pdf E.T. 4.4.2024).*

19 Ozan Özparlak, B./Engin, M.

20 OECD: *"Using AI in the Workplace: Opportunities, Risks and Policy Responses",* s. 10-11.

Küzeci tarafından ifade edildiği gibi, gereken önlemler alınmadığında, bilişim teknolojilerinde görülen gelişmeler ile kolaylaşan gözetim uygulamalarının sınırsız kullanımı, bireyin politik ve toplumsal olarak güçsüzleşmesine neden olabilmektedir[21]. Bu durum özellikte istihdamda kullanılan YZ teknolojileri söz konusu olduğunda sadece bu uygulamaya maruz kalan çalışanları değil, istihdamın itici gücü ile tüm toplumu olumsuz etkileyen sonuçlara yol açabilecek niteliktedir. O nedenle kanımızca, istihdam özelinde ve ülkemize özgü sektörel farklılıkları da içeren bir "istihdamda YZ" analizi yapılmalı ve bu analiz sonucunda ortaya çıkan risklerin giderilmesine yönelik politikalar benimsenmelidir.

1. İşe Alım Sürecinde Kullanılan Yapay Zekâ Sistemleri

İşe alım sürecinden, iş sözleşmesinin feshine kadar bir bütün olan iş ilişkisinin ilk adımı, iş ile adayın doğru şekilde eşleşmesini sağlayacak kriterlerin belirlenmesini, hangi tür kişilere iş ilanının gösterileceğini, ilana başvuranlar arasında yapılacak ön elemeyi ve mülakat süreçlerini ve en nihayetinde de işe alım kararının verilmesi ile birlikte iş sözleşmesinin kurulmasını kapsamaktadır.

İşe alım süreci, istihdamın en önemli aşamalarından biridir. İşe alımın gerçekleşmesi, öncelikle bir istihdam ihtiyacının belirmesi, bunun üzerine bu ihtiyacın gerekli niteliklerle birlikte duyurulması (iş ilanı), bu duyuruya karşılık yapılan iş başvurularının çoğunlukla bir ön elemeyi ve mülakatı (iş görüşmesini) içerecek şekilde değerlendirilmesini ve iş alım kararının verilmesi adımlarını içerir. İşe alım süreci bu kapsamlı yönü ile özellikle çok sayıda kişiyi istihdam eden büyük kurumlarda oldukça zaman alan ve özellikle insan kaynakları alanında çalışan pek çok kişinin yoğun emeğini içermektedir. O nedenle hem bu işe alım sürecinin maliyetini düşürmek hem de işe alım alanında çalışanların yükünü hafifleterek işe alım sürecini zaman yönünden kısaltmak için yapay zekâ sistemleri son yıllarda işverenler tarafından önemli bir çözüm aracı olarak kullanılmaya başlanmıştır. Ülkemizde faaliyet gösteren şirketlerin insan kaynakları süreçlerindeki YZ kullanımına dair yapılan bir araştırmanın sonuçlarına göre; işe alım sürecinde YZ; iş başvurusu yapan kişilerin özgeçmişleri (CV) arasından eleme yapmak, adayları belirlemek, aday veri tabanı taramak, başvuruculara kişilik testleri ve ön mülakat yapılmasında kullanılmaktadır[22].

---

21 Küzeci, E.; Kişisel Verilerin Korunması Hakkı (Ed. Çağlayan Aksoy, P ve Can Aksoy, H.), "Kişisel Verilerin Korunmasına Akademik Bakış", 1. Baskı, Ankara 2023, s. 27.

22 Karaboğa, U.: "İşe Alım Süreçlerinde Yapay Zeka Teknolojilerinin Kullanımı", İstanbul Medipol Üniversitesi Sosyal Bilimler Enstitüsü İşletme Yönetimi Tezli Yüksek Lisans

Bu uzun ve masraflı süreçteki insan kaynakları faaliyetlerini kolaylaştırmak için kullanılan YZ sistemleri, işe alım sürecinde hem iş ilanına başvuranların sosyal medyadaki beğenileri, tüketim alışkanlıkları, seyahat tercihleri gibi pek çok farklı veri setlerini analiz ederek hangi adayın işe uygun olup olmadığına dair bir çıkarımlarda bulunmaktadırlar. Veriye dayalı bu otomatik analizler sonucunda, İş Kanunu'nun "Eşit Davranma İlkesi" başlıklı 5. maddesine aykırı şekilde dil, ırk, renk, cinsiyet, engellilik, siyasal düşünce, felsefî inanç, din ve mezhep ve benzeri sebeplere dayalı ayrımcılık ortaya çıkabilmektedir.

Weblining olarak da adlandırılan bu süreç, *redlining*[23] uygulamasının Bilgi Çağı versiyonu olup burada herhangi bir alanda söz konusu olabilen bir *"dışlama"* söz konusudur. Örneğin, konumuz açısından işverenlerin işe alımda, belirli mahallelerde oturan bireyleri dışlaması buna örnek gösterilebilir. Kişisel verilerin çok geniş çapta toplanması, kişinin etnik kökeni veya dini gibi bilgilerin profillere dönüştürülerek insanları kategorilere ayırmak için kullanılmasıyla ortaya çıkan *weblining*, veri profillerini bölümlere ayırır ve bu segmentasyona dayanarak bireylerin işe girip giremeyeceğinin belirlenmesinde kullanılabilir[24]. *Redlining* uygulamasının ve onun Lessig tarafından dijital versiyonu olarak tanımlanan *weblining* pratiğinin ayrımcı olması, ırk veya etnik kökene dayalı olarak belirli alanların sakinleri için çeşitli hizmetlerin ve/veya istihdam gibi olanakların erişilemez hale getirmesinden kaynaklanmaktadır. Dolayısı ile bu uygulama, bireyin niteliklerini göz ardı ederek, ikamet ettiği konum gibi iş ile ilgisi olmayan unsurlara dayalı olarak bireyin sistematik olarak iş başvurularının reddedilmesi ile sonuçlanabilir. Bu nedenle iş hukukundaki yasal düzenlemeler kadar, veri koruma hukukuna alanındaki mevzuatın etkin bir şekilde uygulanabilmesi de işe alımda ayrımcılık ile mücadelede son derece etkilidir.

Programı, Yayınlanmamış Yüksek Lisans Tezi, İstanbul 2020, s. 77. Söz konusu araştırma, farklı alanlarda faaliyet gösteren 22 şirketin insan kaynakları bölümleri ile gerçekleştirilen mülakatlara dayanmaktadır.

23 *"Redlining"* terimi, ABD'de hükümetin ve borç verenlerin, sadece demografiye dayalı olarak yatırım yapacakları veya finansal hizmetleri sunacakları mahalleleri seçmelerine, yatırım yapmayacakları mahalleleri ise haritada kırmızı bir çizgi içine alması uygulamasını tanımlamak için kullanılmıştır. (Cornell Law School Legal Information Institute, LII, Redlining: https://www.law.cornell.edu/wex/redlining#:~:text=Redlining%20can%20be%20defined%20as,on%20their%20race%20or%20ethnicity. Erişim Tarihi: 20.5.2024).

24 Lessig, L.: Code and Other Laws of Cyberspace, New York, 1999, s. 150 vd.

Öte yandan, işe alımda YZ kullanımı 2022 yılında OpenAI şirketi tarafından yayınlanan ChatGPT ile başlayan üretken yapay zekâ devrimi ile birlikte bambaşka bir değişime de uğramıştır. Şöyle ki, 2022 yılına dek işe alım süreçlerinde çoğunlukla işverenler tarafından kullanılan yapay zekâ teknolojisi, üretken yapay zekâ devrimi ile birlikte iş başvurusu yapan bireyler tarafından da kullanılmaya başlanmıştır. Bu dönüşümde, üretken yapay zekânın doğal insan dilini kullanması ile gelen kullanım kolaylığı ve ücretsiz hizmetlerinin teknik olarak giderek gelişmesi de büyük rol oynamıştır.

İş başvurusu yapan bireyler tarafından kullanılan yapay zekâ sistemlerine güncel ve kayda değer bir örnek olarak, OpenAI şirketinin en büyük yatırımcısı olan Microsoft şirketine ait bir sosyal medya platformu olan Linkedin'in bireylere sunduğu, uygun işe başvuru yapılmasını sağlayan bir chatbot hizmeti gösterilebilir[25]. Benzer şekilde, kullanıcılarına editörlük desteği veren *Grammarly* programı da üretken yapay zekâ yardımı ile "kapak mektubu" (*cover letter*) yazma hizmetini kullanıcılarının hizmetine sunmuş ve böylece başvurucular açısından iş başvurularının belki de en can alıcı adımlarından birini kolaylaştırmıştır. LazyApp isimli bir uygulama ise, Job GPT isimli üretken yapay zekâ modelini kullanarak, adayların iş başvuru süreçlerini otomatikleştirmektedir. Görüldüğü üzere, üretken YZ modellerinin gelişmesi ile sadece işverenler tarafından değil, iş başvurusunda bulunan bireyler tarafından da işe alım süreçlerindeki adımların kolaylaşması ve daha kısa sürede daha fazla iş başvurusunun yapılması YZ ile mümkün hale gelmektedir. Ancak elbette burada temel haklar açısından önemli olan husus, başvuruların YZ araçları ile değerlendirilirken, mevcut ayrımcılıkların derinleşmesi ve görünmezleşmesinin önüne geçebilecek hukuki mekanizmaların var olup olmadığıdır.

2. İş İlişkisinin Kurulmasından Sonra YZ Kullanımı

Yukarıda incelediğimiz işe alım sürecindeki YZ kullanımı, iş ilişkilerinde bu teknolojinin yerleştiği uygulama alanlarından sadece birisidir ve iş sözleşmesinin kurulmasından önceki aşamayı oluşturmaktadır. İşçi ve işveren arasında iş sözleşmesinin kurulması anından iş sözleşmesinin feshine kadar olan süreçte de YZ teknolojisinden farklı konularda yararlanılmaktadır. Bunların başlıcaları; işverenin iş mevzuatından kaynaklanan gözetim

[25] Hoover, A. (2024), *LinkedIn's New AI Chatbot Wants to Help You Find Your Next Job, (https://www.wired.com/story/linkedin-ai-chatbot-help-find-your-next-job/* E.T.8.4.2024).

ve denetim yükümlülüklerinin yerine getirilmesi ile işçilerin iş performanslarının değerlendirilmesidir.

Algoritmik yönetim artık pek çok temel sektörde kullanılmaktadır. Bunlardan lojistik ve sağlık sektöründe algoritmik yönetimi inceleyen AB Komisyonu'na bağlı Joint Research Center (JRC) ve Uluslararası Çalışma Örgütü (ILO), lojistik sektörünün algoritmik yönetimi benimseyen ilk sektörler arasında olduğunu tespit ederek, lojistik sektöründe algoritmik yönetimin; üretim akışını izlemek, iş süreçlerini koordine etmek ve çalışanların performansını değerlendirmek için kullanıldığını belirlemiştir[26]. Aynı raporda ele alınan sağlık sektöründe de algoritmik yönetimin, lojistik sektöründe olduğu gibi, maliyet ve hizmet verimliliği sağlanması için kullanıldığı ve özellikle İtalya ve Fransa örneklerinde bu sayede iş koordinasyon süreçlerini iyileştiği, doktorlar ve hemşireler tarafından tıbbi olmayan görevlere harcanan zamanın azaldığı, böylece tedavi ve bakım faaliyetlerine ayrılan zamanın arttığı gözlemlenmiştir[27]. Raporda vurgulanan belki de en önemli nokta ise, İtalya ve Fransa örneğinde gözlemlenen bu durumun nedeninin bu iki ülkedeki lojistik ve sağlık sektöründe algoritmik yönetimin sınırlı ve gönüllü olarak pilot seviyede uygulanması ve bu ülkelerde işçilerin gözetlenmesine dair etkin kuralların varlığı ile temel haklara karşı doğabilecek risklerin en aza indirgenmiş olmasıdır[28].

İş ilişkisinin devamı süresince YZ kullanımının görüldüğü bir diğer alan ise çalışan memnuniyetine yönelik önlemlerin alınmasına yönelik uygulamalardır. Örneğin, işçilerin iş ile ilgili memnuniyetlerini analiz ederek, onları mutlu veya mutsuz eden faktörlerin belirlenmesini sağlayan YZ analitiği, özellikle büyük şirketlerde yetenekli çalışanların işe bağlılıklarını güçlendirecek politikalar ve önlemler geliştirilmesinde kullanılmaktadır[29]. Hatta, bazı şirketlerde, istifa etmek üzere olan çalışanların tespiti için de YZ analitiği kullanılmakta ve bu kişilerin iş ile ilgili fesih kararlarını dönüştürecek politikalar benimsenmesi hedeflenebilmektedir.

---

26 Rani, U./Pesole, A./Gonzalez V. I., *"Algorithmic Management Practices in Regular Workplaces: Case Studies in Logistics and Healthcare",* Publications Office of the European Union, Luxembourg 2024, (*https://data.europa.eu/doi/10.2760/712475* E.T. 20.5.2024), s. 4.

27 Rani, U./Pesole, A./Gonzalez V. I., s. 5.

28 Rani, U./Pesole, A./Gonzalez V. I., s. 5.

29 Ekonomist (2024), *İK'da Yapay Zeka Kullanıyor,* (*https://www.ekonomist.com.tr/ makale/ik-da-yapay-zeka-kullaniyor-46923* E.T. 20.5.2024).

Öte yandan *"sessiz istifa" (quite quitting)* olarak adlandırılan ve çalışanların sözleşmeleri kapsamındaki iş görme edimlerini yerine getirirken çeşitli nedenler ile mümkün olan en az çabayı gösterdikleri durumların tespiti için de işverenler tarafından YZ araçları kullanılmaya başlanmıştır. İş yerindeki izleme faaliyetleri kapsamında değerlendirilebilecek bu durum oldukça tartışmalıdır. Örneğin, bir müşteri hizmetleri temsilcisinin müşterilerle etkileşimlerinin izlenmesi ve izlenme sonucu elde edilen verinin YZ araçları ile analiz edilmesi ile çalışanın performansının değerlendirilmesi söz konusu olabilmektedir. Bu analiz sırasında YZ sistemleri bir çalışanın yeterince arkadaş canlısı olup olmadığını değerlendirerek, yokluğunu, bir işten kopma belirtisi olarak sınıflandırabilir[30].

Çalışanların performanslarının YZ sistemleri tarafından analizi sonuçlarına dayanılarak işveren tarafından iş ilişkisinin feshi yoluna gidilmesine yönelik olarak ise Hollanda'da Uber aleyhine verilen 2021 tarihli bir kararda, "otomatik fesih" olarak adlandırılan bu uygulamanın GVKT 22. maddeye aykırılık oluşturduğuna hükmedilmiştir[31]. Görüldüğü üzere veri koruma kuralları, veriden beslenerek gelişen YZ sistemlerinin istihdamda kullanımının yaygınlaşması ile iş ilişkileri açısından giderek daha fazla önem kazanmaktadır.

23 Mayıs 2024 tarihinde, AB Veri Koruma Kurumu (European Data Protection Board- EDPB), ChatGPT ile ilgili olarak oluşturduğu birimin raporunu kamuoyu ile paylaşmıştır. Anılan raporda özellikle üretken YZ modellerinin geliştirilmesi için kullanılan eğitim verilerinin internetten kazınarak toplanması ve bu verilerin işlenmesi konusundaki yasal gereklilikler detaylı bir şekilde incelenmiştir. Open AI tarafından geliştirilen ChatGPT'nin kullanımını GVKT uyumu açısından çeşitli yönlerinden irdeleyen bu raporda, istihdamda YZ kullanımına ilişkin olarak da mutlaka göz önüne alınması gereken en önemli hususlar arasında veri koruma ve şeffaflığa işaret edilmektedir.

---

30 Elliot, L. (2022): *AI Ethics Disquieted By AI Getting Dragged Into Quiet Quitting Mania, Forbes*, 21 Eylül 2022, (*https://www.forbes.com/sites/lanceeliot/2022/09/21/ai-ethics-disquieted-by-ai-getting-dragged-into-quiet-quitting-mania/?sh=78759b0c21be* E.T 20.5.2024).

31 Lomas, N. (2021); *Uber Hit With Default 'Robo-Firing' Ruling After Another EU Labor Rights GDPR Challenge,* TechCrunch, (*https://techcrunch.com/2021/04/14/uber-hit-with-default-robo-firing-ruling-after-another-eu-labor-rights-gdpr-challenge/* E.T. 17.8.2021).

ABD'de ise, istihdamda YZ kullanımına ilişkin olarak, eyaletler bazında dikkat çekici yasal düzenlemeler mevcuttur. Bu düzenlemelere okuyucuya fikir vermesi açısından aşağıdaki paragraflarda konumuz ile sınırlı şekilde yer vermeyi uygun bulduk. Ancak eyalet düzeyindeki bu düzenlemeler dışında federal düzeyde de özellikle YZ sistemlerinin güvenliğine dair birtakım yasal adımlar atıldığından bahsetmek gerekir. Şöyle ki, Ekim 2023'te ABD vatandaşlarını YZ sistemlerinin potansiyel risklerinden korumak için şimdiye kadar alınmış en kapsamlı önlemleri içeren "Güvenli, Emniyetli ve Güvenilir Yapay Zekâ Hakkında Başkanlık Kararnamesi" ile YZ risklerini en aza indirerek faydalarını en üst düzeye çıkarmak amacıyla birtakım ilkeler ve en iyi uygulamalar geliştirilmesi hedeflenmiştir[32]. Bu kararname, 1 Kasım'da Londra, Birleşik Krallık'ta düzenlenen, dünyanın en geniş kapsamlı YZ Güvenlik Zirvesi olan AI Safety Summit'in[33] hemen öncesinde yayınlanmıştır. Esasen, devletlerin sadece teknolojinin geliştirilmesinde değil güvenliğinde de bir yarışa ve daha da iyisi iş birliğine girmeleri önemlidir. ABD'de Ekim 2023'te kabul edilen ve yukarıda bahsedilen Başkanlık Kararnamesinin Politika Başlıklı İkinci Bölümü'nün (c) fıkrası tamamen istihdamda kullanılan YZ sistemlerine odaklanmaktadır. Buna göre; iş yerinde YZ, çalışan haklarını zayıflatan, iş kalitesini düşüren, gereksiz işçi gözetimini teşvik eden, piyasa rekabetini azaltan, yeni sağlık ve güvenlik riskleri yaratan veya zararlı iş gücü kesintilerine neden olan şekillerde kullanılmamalıdır. YZ, işçilerin, işçi sendikalarının, eğitimcilerin ve işverenlerin görüşlerine dayanarak, işçilerin yaşamlarını iyileştiren, insan işini olumlu yönde destekleyen ve tüm insanların teknolojik yeniliklerden güvenle yararlanmasını sağlayarak sorumlu bir şekilde kullanılmalı ve buna yönelik politikalar ve ilkeler geliştirilmelidir[34]. YZ ile ilgili ABD Başkanlık Kararnamesi'nde istihdamda kullanılan YZ ile ilgili olarak ABD Çalışma Bakanlığı'na, kararnamenin yayınından itibaren 180 gün içinde bu konuda YZ geliştirenlere ve işverenlere yönelik bir YZ ilke raporu yayınlanması görevi verilmiştir.

---

[32] The White House, *"Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence", (https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/* E.T. 20.5.2024).

[33] Gov.uk (2023); *AI Safety Summit, (https://www.gov.uk/government/topical-events/ai-safety-summit-2023, E.T. 20.5.2024).*

[34] The White House: *"Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence".*

Gerçekten, yukarıda ele alınan Başkanlık Kararnamesi uyarınca, 16 Mayıs 2024 tarihinde ABD Çalışma Bakanlığı (Department of Labor) tarafından yayınlanan ve istihdamda YZ kullanımını ele alan ve YZ geliştiricileri ile işverenlere yönelik çerçeve YZ ilkeleri kabul edilmiştir[35]. Aşağıda ele alınan bu ilkelerin, sektör ayrımı gözetmeksizin ancak her iş yerinin kendi özellikleri ve çalışanların görüşleri de dikkate alınarak, YZ sistemlerinin tüm yaşam döngüsü boyunca (tasarım ve geliştirme, test etme, eğitme, kullanıma, gözetim ve denetim dahil olmak üzere) uygulanması tavsiye edilmektedir.

ABD Çalışma Bakanlığınca, Başkanlık Kararnamesi gereği yayınlanan istihdamda YZ ilkeleri:

- İşçileri Güçlendirme Odaklı Kullanım: İşçiler ve işçi temsilcileri, iş yerinde kullanılacak YZ sistemlerinin tasarımı, geliştirilmesi, test edilmesi, eğitimi, kullanımı ve denetimi konusunda bilgilendirilmeli ve söz sahibi olabilmelidirler.
- Etik YZ Geliştirilmesi: YZ sistemlerinin, işçileri koruyacak şekilde tasarlanması, geliştirilmesi ve eğitilmesi sağlanmalıdır.
- YZ Yönetişimi ve İnsan Gözetimi Sağlanması: Kurumlar, iş yerlerinde kullanılacak YZ sistemleri için açık ve belirli yönetişim sistemlerine, prosedürlere, insan gözetimine ve değerlendirme süreçlerine sahip olmalıdır.
- Şeffaflık: İşverenler, iş yerinde kullanılan YZ sistemleri hakkında işçilere ve iş arayan bireylere karşı iş yerinde YZ kullanıldığına dair şeffaf olmalıdır.
- Çalışan Haklarını Korumak: YZ, işçilerin örgütlenme hakkını, sağlık ve güvenlik haklarını, ücret haklarını ihlal etmemeli ve ayrımcılık karşıtı korumalara zarar vermemeli veya zayıflatmamalıdır.
- YZ Çalışanlara Destek Olacak Şekilde Kullanılmalı: YZ sistemleri, işçileri destekleyici olmalı ve iş kalitesini artırmalıdır.
- YZ'den Etkilenen İşçileri Desteklemek: İşverenler, YZ ile ilgili olarak işçileri desteklemeli ve onlara yeni beceriler kazandırmalıdır.

---

[35] US Department of Labor, *"Artificial Intelligence and Worker Well-being: Principles for Developers and Employers"*, (*https://www.dol.gov/general/AI-Principles* E.T: 20.5.2024).

- İşçi Verilerinin Sorumlu Kullanımını Sağlamak: İstihdamda kullanılan YZ sistemleri tarafından elde edilen işçilere dair kişisel verilerin işlenmesinde ölçülü, amaca uygun ve meşru amaçlar için işlenmelidir ve bu verilerin güvenliği sağlanmalıdır.

Yukarıda yer verilen ilkeler her ne kadar bağlayıcı yasal düzenleme niteliğinde olmasalar da ABD eyaletlerinin bir kısmında istihdamda YZ konusunda yasal düzenlemeler de kabul edilmiştir. Özellikle Illinois Eyaleti ve New York Şehri'nde kabul edilen düzenlemeler dikkat çekicidir. Illinois Yapay Zekâ Video Mülakat Kanunu (Artificial Intelligence Video Interview Act) başlıklı ve 1 Ocak 2020'de yürürlüğe giren bu yasa[36], yapay zekâ sistemlerinin işe alım mülakatlarında kullanılmasına özgü düzenlemeler içermektedir. Anılan yasal düzenleme uyarınca, Illinois Eyaletindeki işverenler, video mülakatlarda aşağıdaki hususları göz önünde bulundurmalıdırlar:

- Şeffaflık: İş başvurusu yapan adaylara, video mülakat öncesinde yapay zekâ sistemi kullanımı hakkında bilgi verilmesi ve bu sistemin nasıl çalıştığının açıklanması.
- Rıza: Adayların yapay zekâ sisteminin kullanılmasına yazılı olarak rıza göstermeleri.
- Veri minimizasyonu: Mülakat videolarının sadece gerekli kişilerle paylaşılması ve üçüncü kişilerle paylaşılmaması.
- Veri kontrolü: Adayların talebi üzerine, mülakat videolarının 30 gün içinde imha edilmesi ve üçüncü tarafların da aynı süre içinde tüm dijital kopyaları silmesi.

ABD'nin New York Eyaleti'nde ise 1 Ocak 2023'ten itibaren uygulanmakta olan İstihdamda Otomatik Karar Araçları Yasası (Automated Employment Decision Tools)[37], istihdamda kullanılan otomatik karar vermeye yönelik araçlarının ve yapay zekâ sistemlerinin işverenler ve iş bulma kurumları tarafından kullanımına dair düzenlemeler içermektedir. Ayrımcılığın ön-

36 ILLINOIS General Assembly HB2557 Artificial Intelligence Video Interview Act (Illinois AI Video Interview Act): *https://www.ilga.gov/legislation/publicacts/fulltext.asp?Name=101-0260* (E.T. 20.5.2024).

37 The New York City Council, 2021/144 Sayılı *"Automated Employment Decision Tools"* Kanunu. *https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=4344524&GUID=B051915D-A9AC-451E-81F8-6596032FA3F9* (E.T. 20.5.2024).

lenmesini ve şeffaflığın sağlanmasını amaçlayan söz konusu yasa kapsamındaki YZ sistemlerinin kullanımdan önce ön yargı denetimlere tabi tutulması gerekmektedir. Ayrıca, şeffaflık ilkesinin bir yansıması olarak, işverenlerin ve iş bulma kurumlarının bu tür araçların değerlendirme amacıyla kullanıldığını çalışanlara ve iş başvurusu yapan adaylara bildirme yükümlülükleri bulunmaktadır.

ABD'de eyalet seviyesinde istihdamda YZ konusunu kapsayan en güncel düzenlemelerden biri ise 13 Mayıs 2024 tarihinde ABD'nin Colorado Eyaleti'nde kabul edilen ve istihdam dahil olmak üzere eğitim, finans, kamu hizmetleri, sağlık, sigorta ve hukuk alanlarında YZ kullanımının yol açabileceği ayrımcı sonuçların engellenmesi amacına yönelik yasal düzenlemedir. 1 Şubat 2026'da yürürlüğe girecek olan SB24-205 Numaralı bu yasada[38], yukarıda sayılan alanlarda kullanılacak olan ve bireylerin yaş, engellilik, ırk, din veya cinsiyet gibi korumalı sınıflandırmalarını içeren kararları önemli ölçüde etkileyen YZ sistemleri, "yüksek riskli YZ" olarak tanımlanmıştır. Bu tanıma giren YZ sistemlerini geliştiren veya uygulamaya koyan kurumların YZ risk yönetimi yapması ve bunu belgelendirmelerini, ayrıca YZ etki değerlendirmeleri, yıllık incelemeler ve önemli kararlarda YZ kullanımına ilişkin kamuoyunu bilgilendirme yükümlülüklerini içermektedir. Bu yasa hükümlerinin ihlalinin ise aldatıcı ticaret uygulamaları olarak kabul edileceği de açıkça belirtilmektedir. Söz konusu yasa ile bireylere yüksek riskli sistemler tarafından verilen kararlar hakkında itiraz ve düzeltme talep etme hakkı ve bir ayrımcı sonucu 90 gün içinde idareye bildirme yükümlülükleri de getirilmektedir.

Çalışmamızın başında da belirtildiği üzere istihdamda ve özellikle işe alım süreçlerinde yapay zekâ destekli araçların benimsenmesi, mevcut süreçlerin otomasyonunu ve kolaylaşmasını sağlarken, aynı zamanda mevcut ön yargıların sürdürülmesi ve ayrımcı iş reklamları gibi yeni riskler de doğurmaktadır. Bu nedenle, küresel teknik standartlar dahil olmak üzere güvenilir yapay zekâya yönelik rehber, öneri ve yasal düzenlemeler uygulamada ortaya çıkan sorunlar ve alınması gereken önlemler açısından birbirini besleyerek geliştirecektir.

---

[38] Colorado General Assembly, SB24-205 *"Consumer Protections From Artificial Intelligence", https://leg.colorado.gov/bills/SB24-205* (E.T. 20.5.2024).

II. İSTİHDAMDA YZ KULLANIMININ 6698 SAYILI KANUN'DAKİ DEĞİŞİKLİKLER AÇISINDAN DEĞERLENDİRİLMESİ

A. İSTİHDAMDA YAPAY ZEKÂ VE 6698 SAYILI KİŞİSEL VERİLERİN KORUNMASI KANUNU REFORMU

Kişisel verilerin işlenmesine dair yasal düzenlemeler YZ uygulamalarının gelişerek yaygınlaşması ile çok daha geniş bir uygulama alanı bulmaktadır. Konumuz kapsamında değerlendirdiğimizde iş ilişkilerinde kullanılan YZ sistemleri ile birlikte kişisel verilerin korunmasının iş ilişkilerindeki önemi de artmıştır. Aksoy Retornaz ve Güçlütürk tarafından belirtildiği üzere, YZ kullanımı ile kişisel veri niteliğinde olmadığı düşünülen bir verinin dahi gerçek bir kişi ile ilişkilendirilmesi giderek kolaylaşmakta olduğundan YZ uygulamaları kişisel veri kavramının kapsamını da giderek genişletmektedir[39].

12.03.2024 tarihli ve 32487 sayılı Resmî Gazete'de yayınlanan "7499 sayılı Ceza Muhakemesi Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun"[40] (8. Yargı Paketi) ile 6698 sayılı Kanun'da önemli değişiklikler yapılmıştır. Kanun'un gerekçesinde de belirtildiği üzere 6698 Sayılı Kanun'un GVKT ile uyumlu hale getirilmesini sağlamak ve uygulamada yaşanan zorlukların önüne geçmek amacıyla; 6698 Sayılı Kanun'un 6. maddesinde düzenlenen özel nitelikli kişisel verilerin işlenmesi yasağının istisnaları ile 9. maddede düzenlenen yurt dışına kişisel verilerin aktarımına dair düzenleme değiştirilmiş ve Kişisel Verileri Koruma Kurulu tarafından verilen idari para cezalarına karşı, idare mahkemelerinde dava açılabileceği hususları düzenlenmiştir[41].

KVKK reformu ile ilgili olarak vurgulanması gereken en önemli hususlardan biri, 6698 Sayılı Kanun'un 4. maddesinde belirtilen kişisel verilerin

---

39 Aksoy Retornaz, E. E. ve Güçlütürk, O. G., Yapay Zekada Kişisel Verilerin Korunması Kanunun Uygulanmasındaki Sorunlara İlişkin Değerlendirme, (Ed. Çağlayan Aksoy, P ve Can Aksoy, H.), "Kişisel Verilerin Korunmasına Akademik Bakış", 1. Baskı, Ankara 2023, s. 417.

40 02.03.2024 tarihli ve 7499 sayılı Ceza Muhakemesi Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun (RG. 12.03.2024/32487).

41 6698 Sayılı Kanun'da, 7499 Sayılı Kanun ile yapılan söz konusu değişikliklerin tümü ile ilgili kapsamlı bir değerlendirme için bkz: Mehmet Bedii Kaya, https://mbkaya.com/hukuk/kvkk-reformu.pdf (Erişim Tarihi: 20.5.2024).

işlenmesinde uyulması gereken ilkelerin[42], gerek özel nitelikli verilerin işlenmesinde gerekse de kişisel verilerin yurt dışına aktarılmasında gözetilmeye devam edileceğidir. Söz konusu yasal reformun getirdiği düzenlemelerin bu ilkelere aykırı olacak şekilde uygulanması elbette düşünülemez.

KVKK kapsamında istihdamda YZ kullanımı ile ilgili olarak değinilmesi gereken en önemli düzenlemelerden biri de otomatik veri işleme faaliyetine ilişkindir. Özellikle işe alım ve işçilerin performans analizinde giderek yaygınlaşan otomatik veri işleme faaliyetleri açısından ise 6698 Sayılı Kanun'un 11. maddesi hükümlerinin gözetilmesi gerekecektir. Ayrıca, verilerin otomatik sistemler aracılığı ile işlenmesi, Kurum tarafından 2019 yılında yayınlanan rehberde; bilgisayar, telefon, saat gibi işlemci sahibi cihazlar tarafından yerine getirilen, yazılım veya donanım özellikleri aracılığıyla önceden hazırlanan algoritmalar kapsamında insan müdahalesi olmadan kendiliğinden gerçekleşen işleme faaliyeti olarak tanımlanmıştır[43]. Bu kapsamda bir veri işleme faaliyeti halinde; 6698 Sayılı Kanun'un "İlgili Kişinin Hakları" başlıklı 11. maddesi gereğince, herkes veri sorumlusuna başvurarak, otomatik sistemler aracılığıyla analiz edilen verilerin kendisi aleyhine sonuç doğurmasına itiraz edebilir. Bu düzenleme gereğince, örneğin iş başvurusunda bulunan bir birey, katıldığı bir video mülakatta bir gerçek kişi ile muhatap olmamış ise (bir chatbot veya avatar ile görüşme yapmış ise) ve mülakat sonucunda iş başvurusunun kabul edilmediği kendisine bildirilmiş ise 6698 Sayılı Kanun'un 11. maddesi gereğince veri sorumlusu sıfatını haiz işverene başvurabilecektir. Ancak bu hakkı kullanabilecek bir kişinin, video mülakatın otomatik sistemlerce gerçekleştirildiğini ve analiz edildiğini bilmesi gerekmektedir. Bu ise ancak veri sorumlusu işverenin 6698 Sayılı Kanun'un 10. maddesindeki "veri sorumlusunun aydınlatma yükümlülüğü" kapsamında iş başvurusunda bulunan kişiye gireceği video mülakatın veri analizinin otomatik sistemler tarafından yapılıp yapılmadığını bildirmesi halinde söz konusu olabilecektir. Dolayısı ile özellikle istihdamda

---

42 6698 Sayılı Kişisel Verileri Koruma Kanunu'nun "Kişisel Verilerin İşlenmesi" başlıklı İkinci Bölümü, 4. Maddede yer alan "Genel İlkeler" ile başlamaktadır. Anılan maddenin ikinci fıkrasındaki düzenlemeye göre kişisel verilerin işlenmesinde gözetilmesi gereken ilkeler şu şekilde sıralanmıştır: a) Hukuka ve dürüstlük kurallarına uygun olma b) Doğru ve gerektiğinde güncel olma c) Belirli, açık ve meşru amaçlar için işlenme ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme.

43 Kişisel Verileri Koruma Kurumu: *"Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi".* (https://www.kvkk.gov.tr/Icerik/4197/Kisisel-Verilerin-Korunmasi-Kanununa-Iliskin-Uygulama-Rehberi E.T. 22 Agu 2023).

YZ kullanımı sırasında uygulama alanı bulabilecek 6698 Sayılı Kanun'un 11. maddesindeki hakkın ilgili kişi tarafından kullanılabilmesi, veri sorumlusunun 6698 Sayılı Kanun'un 10. maddesindeki yükümlülüğünü yerine getirmesi ile doğrudan ilgilidir. Aydınlatma yükümlüğünün önemine binaen ve uygulamaya açıklık getirilmesi amacı ile Kurum tarafından bu konuya dair yayınlanan tebliğde de aydınlatma yükümlülüğünün, kişisel verilerin tamamen veya kısmen otomatik yollardan mı yoksa veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yöntemlerle mi işlendiği bilgisinin açıkça belirtilmesini kapsadığı vurgulanmıştır.

6698 Sayılı Kanun'un 11. maddesinin ilk fıkrasının (g) paragrafında düzenlenen otomatik sistemlerce veri analizinden kaynaklanan hakkın kullanımının yasadan kaynaklanan iki temel koşulu vardır. Bunlardan ilki, Kanun'un açık lafzı gereğince ancak ilgili kişinin aleyhine bir sonuç çıkması, bir diğeri ise otomatik sistemlerce veri işlenmesidir.

Avrupa Birliği (AB) Genel Veri Koruma Tüzüğü (GVKT) kapsamında ise, 22. maddede yer alan bu hak, ilgili kişilerin devreye sokabileceği ek önlemlerle güçlendirilmiştir. GVKT 22. maddeye göre; ilgili kişi kendisini hukuken veya benzer şekilde önemli derecede etkileyen, profilleme dahil olmak üzere, sadece otomatik işlemeye dayalı olarak alınan kararlara tabi olmama hakkına sahiptir (m.22/1).

GVKT'nin 22. maddesinde belirtilen "sadece otomatik işleme ile alınan karar", bir algoritmik sistemin denetiminde bir insanın sembolik olarak bulunması ile bu vasfını kaybetmeyecektir. Eğer bir otomatik karar sistemini kullanan kişinin sistemin aldığı karara uymama yetkisi veya otomatik olarak oluşturulmuş bir profili uygulamama yetkisi varsa, alınan karar "sadece otomatik işlemeye" dayalı kabul edilmeyebilecektir. Örneğin bir işe alım kararına etki edecek video mülakat örneğine dönecek olursak, video mülakatın bir chatbot tarafından gerçekleştirilmesine karşın karar verme konusunda bir insanın inisiyatifi belirleyici ise, yani YZ değerlendirme sistemi sadece insan kaynaklarını desteklemek üzere kullanılıyorsa, bu durumda salt otomatik bir işleme faaliyeti söz konusu olmayacaktır.

Birleşik Krallık'ta 25 Mart 2024 tarihinde Bilim, İnovasyon ve Teknoloji Bakanlığı tarafından yayınlanan "İşe Alımda Sorumlu YZ Rehberine" göre de, işe alımda YZ kullanılması halinde, bu sürecin İngiltere GVKT düzenlemesinin otomatik veri işlenmesine dair hükümleri kapsamında olup olmadığının değerlendirilmesi ve bu değerlendirme neticesinde, otomatik veri

işleme kapsamında kalıyorsa ise YZ sisteminin işe alımda kullanımından önce bir veri koruma etki değerlendirmesinden geçirilmesi gerektiği belirtilmektedir[44]. Ülkemizde Kurum tarafından 2021 yılında yayınlanan "Yapay Zekâ Alanında Kişisel Verilerin Korunmasına Dair Tavsiyeler" kapsamında da, kişisel verileri işleme temelli yapay zekâ uygulamalarında verilerin korunması anlamında yüksek risk öngörülmesi halinde mahremiyet etki değerlendirmesi uygulanması gerektiği belirtilmiştir. İşe alım ve iş ilişkisi sürecindeki YZ kullanımı da iş başvurusu yapan kişilerin ve çalışanların verilerinin işlenmesine dayandığından ve kişilerin ekonomik geleceğini etkileme riski bulunduğundan kanımızca yüksek riskli olarak değerlendirilmeli ve Kurumun söz konusu tavsiyesinde belirttiği mahremiyet etki değerlendirmesine tabi olmalıdırlar[45]. Görüşümüze göre bu önerinin, en azından işe alımda kullanılan YZ sistemleri açısından yasal bir düzenleme niteliğine kavuşması, eğer yakın zamanda özel olarak YZ sistemlerine dair bir yasal düzenleme yapılmayacaksa, şimdilik 4857 sayılı İş Kanunu'nun 5. Maddesine bir cümle olarak eklenmesi uygulamada yaşanan sorunların aşılması için faydalı olabilecektir.

B. İSTİHDAMDA YZ KULLANIMINDA İŞLENEN HASSAS VERİLER AÇISINDAN 6698 SAYILI KANUN'UN 6. MADDESİ DEĞİŞİKLİĞİNİN DEĞERLENDİRİLMESİ

7499 sayılı Kanun ile 6698 Sayılı Kanun'da yapılan temel değişikliklerden biri, yukarıda da belirtildiği üzere özel nitelikli kişisel verilerin işlenme şartlarında yapılan düzenlemedir. Buna göre 6698 Sayılı Kanun'un 6. maddesinin önceki halinde, özel nitelikli kişisel verisi işlenmesi için ilgili kişinin açık rızasının bulunması gerekiyordu. Yapılan değişiklik ile açık rıza, özel nitelikli veri işlemenin tek koşulu olmaktan çıkarak, koşullardan biri haline dönüşmüştür. Yasa değişikliğinde, açık rıza dışında özel nitelikli kişisel verilerin işlenmesine dair getirilen koşullardan bir diğeri ise, *"istihdam, iş sağlığı ve güvenliği, sosyal güvenlik, sosyal hizmetler ve sosyal yardım alanlarındaki hukuki yükümlülüklerin yerine getirilmesi için zorunlu olması"* halidir.

---

44 Department For Science Innovation and Technology; *"Responsible AI In Recruitment Guidances", (https://www.gov.uk/government/publications/responsible-ai-in-recruitment-guide/responsible-ai-in-recruitment E.T* 20.5.2024), s. 18.

45 Kişisel Verileri Koruma Kurumu, *"Yapay Zeka Alanında Kişisel Verilerin Korunmasına Dair Tavsiyeler"* Ankara, KVK Yayınları, 2021.

Konumuz kapsamında değerlendirildiğinde, istihdamda YZ uygulamalarının salt konu bakımından uygun düşmesinin, bu uygulamalar sırasında elde edilen özel nitelikli verinin işlenebilmesi için kanunen tek başına yeterli kabul edilmesi mümkün değildir görüşündeyiz. Çünkü yukarıda anılan koşulun en önemli unsuru *"hukuki yükümlülüklerin yerine getirilmesi için zorunlu olması"* olup, çalışanların veya işe başvuranların YZ ile işlenecek özel nitelikli verisinin salt istihdam alanında olması yasanın yukarıda belirtilen istihdama dair koşulunun karşılandığı şeklinde yorumlanamaz. İş başvurusu yapan adayların, çevrim içi iş mülakatlarında kullanılan otomatik yöntemler ile ses, yüz, mimik gibi biyometrik verilerinin işlenmesi söz konusu olabilmektedir. GVKT'de "Bir gerçek kişinin fiziksel, psikolojik ya da davranışsal özelliklerinden olan ve yüz görüntüsü veya daktiloskopik (parmak izi) gibi bu kişinin benzersiz şekilde kimlik tespitini veya bu kimlik tespitinin doğrulanmasını sağlayabilen ve belirli teknik işlemler sonucu elde edilen kişisel veridir." (GVKT madde 4/14) olarak tanımlanan biyometrik veri 6698 Sayılı Kanun'unda açıkça tanımlanmamış, anacak 6. madde ile "özel nitelikli kişisel veri"ler arasında sayılmıştır (6698 Sayılı Kanun m.6/1). Örneğin, çevrim içi ve bir chatbot kullanılarak bir iş mülakatı yapılması, ardından bu mülakattaki ses, davranış gibi özel nitelikli verilerin analiz edilmesi, otomatik olarak işverenin hukuki bir yükümlülüğü kapsamında değerlendirilemez. Bu durumda, kanun değişikliği kapsamında getirilen açık rıza dışındaki diğer koşulları da sağlamayacağından, yine ancak iş başvurusu yapan adayın açık rızası ile işlenmesi mümkün olacaktır.

Ancak, istihdamda YZ kullanımı ile özel nitelikli kişisel verilerin işlenmesi, işverenin ilgili paragrafta sayılan hukuki yükümlülüğünü yerine getirmek için zorunlu ise bu takdirde özel nitelikli veri işlemenin koşulu oluşmuş kabul edilebilir. Örneğin, iş sağlığı ve güvenliği kapsamında işverenin işçiyi gözetme borcunu yerine getirmek için iş yerindeki gözetimde YZ analitiğinden yararlanması hali veya çalışanlara sağlanan iş sağlığı ve güvenliği eğitimlerinin sonuçlarının YZ araçları ile analiz edilmesi sırasında özel nitelikli kişisel verilerin işlenmesinin bu kapsamda değerlendirilip değerlendirilemeyeceğinin her uyuşmazlık söz konusu olduğunda tartışılması gerekecektir. Ancak bu durumlarda da ilgili kişinin haklarını düzenleyen 6698 Sayılı Kanun'un 11. maddesinin yukarıda açıklanan "otomatik sistemlerce verilerin işlenmesi" halinde ilgili kişi niteliğinde olan işçinin aleyhine bir sonuç çıkması halinde işçinin itiraz hakkı doğabileceği kabul edilmelidir.

III. İSTİHDAMDA YZ KULLANIMININ GÜNCEL AB REGÜLASYONLARI AÇISINDAN DEĞERLENDİRİLMESİ

A. AB DİJİTAL HİZMETLER KANUNU AÇISINDAN DEĞERLENDİRME

17 Şubat 2024 tarihinden itibaren tüm dijital platformlar için uygulanmaya başlanan AB Dijital Hizmetler Kanunu (Digital Services Act - DSA)[46], iş ilanlarını da kapsayan çevrim içi reklamcılık açısından önemli hükümler barındırmaktadır. Çevrim içi platformlar dahil olmak üzere dijital ortamda aracılık hizmeti verenlere uygulanan DSA, yasa dışı içeriğin çevrim içi ortamda kaldırılması, reşit olmayanların reklamlarla hedeflenmesi için profil oluşturulmasının yasaklanması ve hassas verilere dayalı profil oluşturmanın reklam hedeflemesi için yasaklanması gibi düzenlemeleri içermektedir. DSA'nın kapsamına giren aracı hizmetlere örnek olarak, çevrim içi pazar yerleri, sosyal ağlar, içerik paylaşım platformlar, uygulama mağazaları gösterilebilir.

Dijital ortamda yayınlanan iş ilanları ile ilgili olarak günümüze kadar gelen aşamada dahi özellikle işe alımda ayrımcılık ile ilgili hukuka aykırı pek çok durum ortaya çıkmıştır. AB Dijital Hizmetler Kanunu'nun 68 numaralı gerekçesinde, çevrim içi reklamcılığın ortaya çıkarması olası riskler arasında ayrımcılık da sayılmıştır. Bu nedenle AB kanun koyucusu çevrim içi platform sağlayıcılarından hizmet alan kişilerin, kendilerine belirli bir reklamın sunulmasını belirlemede kullanılan ana parametreler hakkında bilgi edinmeleri gerektiğini ifade etmiştir. Özellikle iş ilanlarında ayrımcı etkileri ile ortaya çıkan profilleme faaliyetlerine dayanan reklamların sunulmasında kullanılan profil oluşturma kriterleri hakkında reklam hizmeti alanların bilgilendirilmesi ve profilleme kriterlerini değiştirme olanağı sunulması gerektiği ifade edilmiştir. Dijital Hizmetler Kanunu'nda reklamla ilgili bilgilerin sağlanması ile ilgili gerekliliklerine dair hükümlerin, GVKT'nin ilgili kişiden rıza alınmasına yönelik hükümleri başta olmak üzere hiçbir hükmünün uygulanmasına zarar vermeyeceği de açıkça ifade edilmiştir.

Dijital Hizmetler Kanunu 26/3'te çevrim içi platform sağlayıcılarının, GVKT 9/1'de yer verilen hassas veri kategorileri vasıtası ile GVKT 4/4'te tanımı yapılan profillemeye dayanan reklamları sunmamaları gerektiği

[46] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act), OJ L 277, 27.10.2022.

ifade edilmiştir. Söz konusu Kanun, sektörel bir ayrım içermediğinden, anılan 26/3 maddesindeki yasağın iş ilanları açısından da geçerli olduğunu söylemek mümkündür. YZ araçları ile hassas veri kategorileri kullanılarak yapılan profillemenin de anılan yasak kapsamında değerlendirilmesi gerekmektedir.

Dijital Hizmetler Kanunu'nun bu hükümleri dikkate alındığında, anılan kanunun hassas veriye dayalı profilleme açısından GVKT hükümlerini tamamlayıcı nitelikte olduğu söylemek mümkündür[47]. Bu durumda, istihdamda yapay zekâ temelli profil analizine dayalı iş ilanları açısından kişisel verilerin korunmasında Dijital Hizmetler Kanunu hükümleri diğer koşulların[48] da oluşması halinde AB Hukuku açısından dikkate alınmalıdır.

B. AB YAPAY ZEKÂ KANUNU AÇISINDAN DEĞERLENDİRME

Mart 2024'te AB Parlamentosu tarafından onaylanan AB Yapay Zekâ Yasası'nın[49] nihai metni Mayıs 2024'te de AB Konseyi tarafından nihai olarak onaylanmıştır. AB YZ Kanunu, ülkemiz açısından da son derece önemlidir. Bunun politik ve ekonomik olmak üzere iki temel nedeni vardır: İlk neden, ülkemizin AB üyeliğine adaylık sürecinde olması nedeni ile müktesebat uyumu gereklilikleri, ikinci neden ise AB'nin Türk şirketleri ve girişimcileri açısından önemli bir ticari pazar hacmi olmasıdır. Özellikle ikinci neden açısından, AB YZ Yasasının GVKT'ye benzer şekilde tasarlanmış uygulama alanı belirleyici nitelikte olmuştur.

1. İstihdamda Yapay Zekâ Kullanımının AB YZ Kanunundaki Risk Kategorisi Açısından Değerlendirilmesi

AB YZ Kanunu'nun en dar kapsamlı olarak düzenlediği kabul edilemez risk kategorisinde, istihdamda kullanılan duygu tanıma sistemleri de yer almaktadır. AB YZ Kanunu'nun 44 sayılı gerekçesinde belirtildiği üzere istihdam bağlamındaki sözleşme tarafları arasındaki güç dengesizliği göz

---

47 AB Dijital Hizmetler Kanunu ile AB Genel Veri Koruma Tüzüğü arasında uygulamadan kaynaklanacak potansiyel sorunlar hakkında bir çalışma için bkz: Zanfir-Fortuna, G: *Follow the (personal) data: Positioning data protection law as the cornerstone of EU's 'Fit for the Digital Age' legislative package,* EDPS at 20 Anniversary Volume, 2024, s. 15.

48 Çok Büyük Çevrimiçi Platformlar (VLOP)

49 Proposal for a Regulation of the European Parliament And of the Council Laying Down Harmonised Rules On Artificial Intelligence (Artificial Intelligence Act) And Amending Certain Union Legislative Acts COM/2021/206 final.

önüne alındığında ve bu sistemlerin müdahaleci doğası ile birleştiğinde, duygu tanımaya dair YZ sistemleri belirli bireylerin veya tüm grupların olumsuz veya elverişsiz bir şekilde muamele görmesine yol açabilir. Bu nedenle, AB YZ Kanunu'nun "Yasaklanmış YZ Uygulamaları" başlıklı 2. Bölümü'nde yer alan aynı başlığı taşıyan 5. maddesinin (f) fıkrası uyarınca iş yeri ilgili durumlarda bireylerin duygusal durumunu tespit etmek amacıyla kullanılacak yapay zekâ sistemlerinin piyasaya sürülmesi, hizmete sokulması veya kullanımı yasaklanmıştır. Bu yasağın istisnası, sadece tıbbi veya güvenliğe dair nedenlerle bireylerin duygu durumunun tespitine yönelik olarak YZ sistemi kullanılmasıdır (AB YZ Kanunu m. 5/1(f), ayrıca Gerekçe 44, son cümle).

AB YZ Kanunu'nun 6. maddesinin 2. fıkrası gereğince, anılan Kanun'un üç numaralı eki (Annex III) kapsamında sayılan YZ sistemleri ise yüksek riskli YZ kategorisinde kabul edilmektedir. Söz konusu EK III 4. paragrafı "İstihdam, işçi yönetimi ve serbest mesleğe erişim" başlığı altında aşağıdaki uygulamaları yüksek riskli YZ olarak tanımlamaktadır:

- *İşe alımda YZ:* Doğrudan iş ilanı vermek, iş başvurularını analiz etmek ve filtrelemek, adayları değerlendirmek gibi gerçek kişilerin işe alınması veya seçilmesi için kullanılacak YZ sistemleri.
- *İş ilişkinde YZ (Algoritmik Yönetim):* İşle ilgili ilişkilerin koşullarını, iş ilişkileri süresince terfi konularını veya iş ilişkisinin sona erdirilmesi ile ilgili kararları etkileyen çıkarımlarda bulunan, bireysel davranış veya kişisel özelliklere göre görev dağıtımını veya iş ilişkisi sürecinde kişilerin performansını ve davranışını izlemek ve değerlendirmek için kullanılan YZ zekâ sistemleri.

Kanun'un 57 numaralı gerekçesinde de; istihdam, işçi yönetimi ve serbest mesleğe erişim için kullanılan, özellikle kişilerin işe alınması ve seçilmesi, iş ilişkisi koşullarını etkileyen kararların alınması, iş ilişkisine dayalı sözleşmelerin terfi edilmesi ve sona erdirilmesi, bireysel davranış, kişisel özellikler veya karakteristiklere dayalı görevlerin tahsis edilmesi ve iş ilişkisine dayalı sözleşmelerdeki kişilerin izlenmesi veya değerlendirilmesi için kullanılan yapay zekâ sistemleri de yüksek riskli olarak sınıflandırılması gerektiği belirtilmiştir. Görüldüğü üzere, çalışmamızın başında "algoritmik yönetim" olarak tanımladığımız tüm bu süreçler, gerekçede de açıklandığı üzere kişilerin gelecekteki kariyer beklentileri, geçim kaynakları ve işçilik hakları üzerinde önemli bir etkiye sahip olabilir. Gerekçede, istih-

dam süreçlerindeki YZ kullanımının ayrımcılık ile ilgili etkilerine de atıf yapılmaktadır. Şöyle ki, işe alım ve iş ilişkisi sırasında bireylerin değerlendirilmesi, terfi edilmesi veya işe alınması sırasında, özellikle kadınlar, belirli yaş grupları, engelli kişiler veya belirli ırk, etnik köken veya cinsel yönelime sahip kişilere karşı tarihsel ayrımcılık kalıpları YZ sistemlerince sürdürülebilecektir. Ayrıca son derece yerinde olarak altı çizildiği üzere, bu tür kişilerin performans ve davranışlarını izlemek için kullanılan YZ sistemlerinin, veri koruma ve mahremiyet gibi temel hakları zayıflatabilecek etkileri de bulunmaktadır (AB YZ Kanunu Gerekçe 57).

AB YZ Kanunu, istihdam süreçlerinde kullanılan YZ sistemlerini yüksek riskli yapay zekâ olarak sınıflandırmakla, AB pazarında bu tür sistemlerin hizmete sunulmasını birtakım ön koşulların yerine getirilmesi koşuluna tabii kılmıştır. Yüksek riskli yapay zekâ sistemlerinin AB pazarına girebilmesi veya hizmete sunulması için Kanun'da getirilen koşulların sağlanması gerekecektir. Bu koşulların en önemlileri; istihdamda kullanılanlar dahil olmak üzere yüksek riskli YZ sistemlerinin hizmete sunulmadan önce risk değerlendirmesinden geçirilmesi, bu sistemlerin geliştirilmesinde yüksek kaliteli veri kullanmak, sistemlerin amacı hakkında kullanıcıları bilgilendirmek ve insan denetimini sağlamaktır. AB YZ Yasası, önümüzdeki üç yıl içinde kademeli olarak uygulanacak olup, temel yükümlülüklerinin ise 2026 yılı sonuna dek yürürlüğe girmesi beklenmektedir.

AB YZ Kanunu'nun 26. maddesi ise yüksek riskli YZ sistemini uygulamaya sokan kişilerin yükümlülüklerini ele almaktadır. Konumuz açısından belirtilmesi gereken husus, Kanun'da *"deployer"* olarak isimlendirilen bu kişilerin kişisel amaçlarla YZ sistemlerini kullananlar değil, örneğin konumuz çerçevesinde bir örnek ile açıklarsak, işe alımda YZ kullanan bir işvereni işaret ettiğini belirtmek gerekir. Bu kapsamda esasen gerek 6698 Sayılı Kanun'un gerekse de GVKT'deki veri sorumlusu ile AB YZ Kanunu'ndaki *"deployer"* kavramları, en azından istihdamda kullanılan YZ sistemleri açısından çoğunlukla eşleşecektir. Bizim önerimiz, AB YZ Kanunu'nda geçen "deployer" kelimesinin, gündelik hayatta bu sistemleri bireysel olarak kullananlardan ayrılması amacı ile kullanıcı değil, "uygulayıcı" olarak çevrilmesinin AB YZ Kanunu'nu yorumlarken daha elverişli olacağıdır. O nedenle biz ilerleyen paragraflarda "uygulayıcı" kelimesini, "deployer" teriminin karşılığı olarak kullanacağız.

AB YZ Kanunu 26. madde ile istihdamda kullanılan YZ gibi yüksek riskli YZ sistemlerinin uygulayıcılarına, bu sistemleri onlara eşlik eden kullanım

talimatlarına uygun olarak kullanmalarını sağlamak için uygun teknik ve örgütsel önlemleri alma yükümlülüğü getirilmektedir (m.26/1).

Ayrıca uygulayıcılar, yüksek riskli YZ sistemleri ile ilgili gerekli yetkinliğe, eğitime ve yetkiye sahip, gerçek kişileri görevlendirerek insan denetimini sağlamalıdırlar (26/2).

Yüksek riskli bir yapay zekâ sistemini uygulamaya sokmadan önce, işveren sıfatını haiz uygulayıcılar, işçi temsilcilerini ve bu sistemlerin uygulanmasından etkilenen işçileri bu yüksek riskli yapay zekâ sisteminin kullanımına tabi olacakları konusunda bilgilendirmelidir (26/7).

Görüldüğü üzere, esasen yukarıda yüksek riskli YZ sistemlerinin uygulayıcıları için sayılan yükümlülükler şeffaflık, bilgilendirme ve anlamlı insan denetimine sahip bir YZ uygulamasını sağlamayı amaçlamaktadır. Ancak bu ilkelerin öneminden dolayı AB YZ Kanunu, yüksek riskli YZ sistemlerinin geliştiricileri için de şeffaflık ve insan gözetimine dair 13. ve 14. maddeler ile birtakım yükümlülükler tahsis etmektedir. Özellikle, sözleşme taraflarının iş sözleşmesinde olduğu gibi eşit pazarlık payına sahip olmadığı durumlarda bu iki ilke daha da önem kazanmaktadır. Konumuz açısından önemi nedeni ile aşağıda bu iki ilkeye ilişkin AB YZ Kanunu düzenlemesi de ele alınmıştır.

2. AB YZ Kanunu 13. Maddesi ile Getirilen Şeffaflık Yükümlülükleri

AB YZ Kanunu'nun "Şeffaflık" Başlıklı 13. maddesi ile istihdamda kullanılan YZ sistemleri gibi yüksek riskli YZ sistemlerinin geliştiricilerine birtakım yükümlülükler getirilmektedir. Buna göre; yüksek riskli YZ sistemlerinin uygulayıcılarının ve/veya dağıtıcılarının bu sistemin çıktısını yorumlayabilmesi ve uygun şekilde kullanabilmesi için yeterli şeffaflığın geliştirici tarafından sağlanması gerekmektedir. Bu nedenle 13. madde ile tasarım ve geliştirme aşamasında bu sistemlerin geliştiricileri için öngörülen yükümlülükler, yüksek riskli YZ sistemlerine dair hükümleri içeren yükümlülüklere hem sağlayıcı hem de uygulayıcı/dağıtıcı tarafından uyulmasının da bir ön koşuludur. Çünkü, ancak yeterli şeffaflığın sağlanması halinde, olası riskler ve bu risklerin ortadan kaldırılmasına yönelik önlemler doğru şekilde belirlenebilecektir. Bu nedenle, 13. madde ile yüksek riskli YZ sistemlerinin sağlayıcılarına, dağıtıcılara yönelik kullanım talimatları hazırlamaları yükümlülüğü getirilmiştir. 13. madde ile bu talimatın sadece içeriğine yönelik değil, şekline yönelik de açık düzenleme getirilmiştir.

Maddenin açık lafzı uyarınca, istihdamda kullanılan YZ sistemleri de dahil olmak üzere yüksek riskli YZ ile ilgili kullanım talimatının şekline yönelik gereklilikler:

- İlgili, erişilebilir ve anlaşılır olmak
- Kısa ve özlü olmak
- Tam, doğru ve net bilgi içermek.
- Uygun bir dijital formatta veya başka bir şekilde yüksek riskli YZ sistemine eşlik etmek.

Kullanım talimatlarının içerik açısından sağlaması gereken asgari özellikler de yasanın 13. maddesinde açıkça belirlenmiştir. Bu özellikler arasında, temel haklar aleyhine risk oluşturabilecek, yüksek riskli YZ sisteminin amacına uygun kullanımı veya makul olarak öngörülebilir yanlış kullanım koşullarıyla ilgili bilinen veya öngörülebilir olan herhangi bir durumun paylaşılması da yer almaktadır. Bunun yanı sıra eğer imkân varsa, sistemin kullanılacağı belirli kişiler veya gruplar ile ilgili performansı da kullanım talimatında belirtilmelidir. Kanaatimizce bu, özellikle istihdamda kullanılan YZ sistemlerinin yaş, cinsiyet, ırk, din gibi unsurlara dayalı olarak ortaya çıkarabileceği yanlı kararlarını da içerecek şekilde yorumlanabilir.

Yüksek riskli yapay zekâ sistemlerine yönelik bu düzenlemeler, istihdamda YZ kullanımını doğrudan ve önemli ölçüde etkileyecektir. Şeffaflık ilkesi gereğince, işverenlerin yapay zekâ sistemlerinin nasıl çalıştığını ve bu sistemlerin çıktılarının nasıl yorumlanması gerektiğini en azından kullanım talimatındaki bilgiler çerçevesinde bilmeleri zorunlu hale gelecektir. Bu, işverenlerin yapay zekâ sistemlerini sadece kullanmakla kalmayıp, aynı zamanda sistemlerin kararlarını ve öngörülerinin sonuçlarının farkında olmalarını ve bu bilgileri çalışanlara ve diğer paydaşlara açıklamalarını gerektirecektir.

Bu düzenlemeler, iş yerlerinde yapay zekâ sistemlerinin daha güvenli, şeffaf ve etkili bir şekilde kullanılmasını sağlamayı amaçlamaktadır. İşverenlerin, bu düzenlemelere uyum sağlamak için gerekli adımları atmaları ve yapay zekâ sistemlerinin kullanımını dikkatle yönetmeleri gerekecektir.

3. YZ Kanunu 14. Maddesi: İnsan Gözetimi

İnsan gözetimi, YZ sistemlerinin çıktılarının, özellikle hata veya öngörülemeyen durumların telafisi için insan tarafından denetlenmesi ve gerektiğinde müdahalesini ifade etmektedir. Kurum YZ ile ilgili Tavsiyelerinde karar alıcılar için de bu hususu vurgulayarak YZ sistemlerinin karar alma süreçlerinde insan müdahalesinin rolünün belirlenmesi gerektiği ve bu sistemin kullanıcılarına, YZ tarafından sunulan önerilere otomatik olarak güvenmeme şansı tanınması gerektiğinin altı çizilmiştir[50].

AB YZ Kanunu 14. maddesinde de istihdamda kullanılan YZ gibi yüksek riskli YZ sistemlerinde insan gözetimini sağlamak amacı ile birtakım düzenlemeler yer almaktadır. Buna göre, yüksek riskli YZ sistemleri, tüm kullanım döngüleri boyunca gerçek kişiler tarafından etkin şekilde denetlenebilmelidir. Bunu sağlamak için yüksek riskli YZ sistemleri, insan gözetimine uygun şekilde tasarlanmalı ve geliştirilmelidir. 14. maddede bu kapsamda, sistemin insan gözetimini mümkün kılan bir insan-makine arayüzü (human machine interface) içermesi gerektiği de belirtilmiştir (14/1).

Yüksek riskli YZ sistemlerinde insan gözetimi, bu sistemlerin amaçlanan kullanımı veya makul olarak öngörülebilir yanlış kullanım koşulları altında ortaya çıkabilecek sağlık, güvenlik veya temel haklara yönelik riskleri önlemeyi veya en aza indirmeyi amaçlamalıdır. Konumuz kapsamında ele aldığımızda, istihdamda kullanılacak YZ sistemlerinin ortaya çıkarabileceği ayrımcı sonuçlar da temel haklara yönelik riskler arasında değerlendirilmelidir.

Önemle belirtilmelidir ki bu düzenlemede söz konusu edilen "insan gözetimi" yükümlülüğünün yerine getirilmesi, sadece bir veya birkaç gerçek kişinin yüksek riskli YZ sistemi ile ilgili olarak bu yönde görevlendirmesi ile yerine getirilmiş sayılmayacaktır. YZ Kanunu, yasak savmacı bir şekilde yapılabilecek görevlendirmeleri de öngörerek son derece yerinde bir düzenleme ile istihdamda kullanılan YZ sistemleri gibi yüksek riskli YZ sistemlerinde "insan gözetimi" yükümlülüğünün ancak aşağıdaki özelliklere sahip kişilerin yetkilendirilmesi ile yerine getirilebileceğini belirtmiştir:

---

50 KVK Kurumu Kişisel Verileri Koruma Kurumu, *"Yapay Zeka Alanında Kişisel Verilerin Korunmasına Dair Tavsiyeler"*.

(a) Yüksek riskli YZ sisteminin ilgili kapasite ve sınırlamalarını doğru şekilde anlamak ve anormallikleri, işlev bozukluklarını ve beklenmedik performansı tespit etmek ve ele almak amacıyla operasyonunu izleyebilmek;

(b) İşe alım veya işten çıkarma gibi özellikle gerçek kişiler tarafından alınacak kararlar için bilgi veya tavsiye sağlamak üzere kullanılan yüksek riskli YZ sisteminin ürettiği çıktılara otomatik olarak güvenme veya aşırı güvenme eğiliminin ('otomasyon yanlılığı') farkında olmak,

(c) Yüksek riskli YZ sisteminin ürettiği çıktıları, mevcut yorumlama araçları ve yöntemleri dikkate alarak doğru bir şekilde yorumlamak;

(d) Gerektiğinde, yüksek riskli YZ sistemini kullanmama veya sistemin çıktısını göz ardı etme, geçersiz kılma veya tersine çevirme yönünde karar almak (bu husus, YZ'ye koşulsuz güvenmeme gerekliliği ile yakından ilgilidir);

(e) Yüksek riskli yapay zekâ sisteminin operasyonuna müdahale etme veya sistemi 'durdurma' düğmesi (Kill switch) veya sistemi güvenli bir durumda durdurmayı sağlayan benzer bir prosedür aracılığıyla durdurma yetkisine sahip olmak.

İnsan gözetimi yükümlülükleri, istihdamda YZ çerçevesinde değerlendirildiğinde; işverenlerin yüksek riskli bu tür YZ sistemlerinin gözetimi için ya açıkça yasada belirtilen özelliklere sahip kişileri istihdam etmeleri ya da iş yerinde bu niteliklere uygun kişileri gerekirse ek eğitime tabi tutarak ayrıca yetkilendirmeleri gerekeceği anlaşılmaktadır.

Sonuç olarak, AB YZ Kanunu'nun önemli bir bölümünün konumuz kapsamında ele aldığımız istihdamda kullanılan YZ sistemleri gibi yüksek riskli YZ sistemlerine dair önlemleri içeren hükümleri kapsadığı görülmektedir. Bu hükümler ile, istihdamda YZ kullanımı açısından gerek YZ sistemlerini geliştirenlere gerekse de dağıtıcılara, ithalatçılara ve uygulayıcılara yönelik yükümlülükler getirilmiştir.

SONUÇ

Fransız filozof Bruno Latour'a göre, Mary Shelley'nin romanı Frankenstein'da, insan gibi bir varlık yaratan Dr. Frankenstein'ın hatası, kendi kibri ile teknolojiyi birleştirerek bir yaratık icat etmesi değil, yarattığı varlığın

korkunç halinden düştüğü dehşet ile onu dünyaya sonuçlarını hiç düşünmeden salıvermesidir[51]. Latour'un bu yorumundan hareketle denilebilir ki, günümüz gerçekliğinde, insana benzer bilişsel kapasite arayışımızda benzer bir yanılgıya düşmemek gerekir. Ne kadar karmaşık bir teknolojiye sahip olsa da YZ sistemlerinin hem bireysel hem de toplumsal ölçekte derin etkileri bulunmaktadır. Bireysel ve toplumsal sonuçların bir arada ve yaygın bir kümülatif çerçevede en etkili şekilde karşımıza çıktığı alan ise istihdam ilişkileridir. Çünkü istihdam, her sektörde ve her kesimde toplumsal hayatın bir parçasıdır. Diğer alanlardaki YZ kullanımı gibi istihdamda YZ kullanımı ile yaygınlaşan algoritmik yönetimin uygulamalarının hukuki sınırlarını belirlemek sadece bireysel değil, istihdam gibi bir alanın doğal etkisi olarak toplumsal seviyede önem taşımaktadır. Her ne kadar istihdam alanından bahsediyor olsak da, veriden beslenerek gelişen YZ sistemlerinin veriden yola çıkarak istihdam alanında kullanımının sadece iş yasaları çerçevesinde değil, Kişisel Verilerin Korunması Kanunu çerçevesinde de değerlendirilmesi gerekmektedir. İstihdamda YZ kullanımının işe alımda, iş ilişkisinin devamında ve hatta sona erdirilmesine dair verilen kararları desteklemek üzere, giderek artan şekilde verimliliği artırmak amacıyla kullanımının giderek yaygınlaşmasına uygun bir yaklaşım ile ülkemiz açısından öncelikle sektör farklılıkları da gözetilerek kapsamlı bir "İstihdamda Algoritmik Yönetim" analizi yapılması gerekmektedir. Bu analizin sonucunda ise çalışanların haklarının istihdamda YZ uygulamaları ile en fazla risk altına girdiği alanlara yönelik bir politika belgesinin oluşturulması ve akabinde uygulamaya yol gösterici nitelikte temel ilkelerin benimsenmesi gerekmektedir. Ülkemizin Ulusal YZ Strateji Belgesi, 6698 Sayılı Kanun ve ilgili diğer mevzuat ile uyumlu bir "İstihdamda YZ Uygulaması ve İlkeleri" çerçevesine ihtiyaç bulunmaktadır. Biz bu çalışmamızda özellikle Kurumun "Yapay Zekâ Alanında Kişisel Verilerin Korunmasına Dair Tavsiyeler"inde geliştiriciler, üreticiler ve servis sağlayıcılar için önerdiği üzere, ulusal ve uluslararası düzenlemelere uyumlu bir YZ odaklı tasarım için istihdamda YZ konusunda rehberlik edebilecek güncel ulusal ve uluslararası düzenleme ve raporlara ana hatları ile yer vermekle, esasen bu konuda ülkemizde yapılacak nice nitelikli ve geniş kapsamlı çalışmalar için bir ana hat oluşturmuş olmayı umuyoruz.

[51] Latour, Bruno (2012), *"Love Your Monsters", The Breakthrough Institute, (https://thebreakthrough.org/journal/issue-2/love-your-monsters* E.T. 20.5.2024).

KAYNAKÇA

Makaleler

AJUNWA, Ifeoma: The Paradox of Automation as Anti-Bias Intervention, 41 Cardozo Law Review 2020.

ANGEL, María P./CALO, Ryan: Distinguishing Privacy Law: A Critique of Privacy as Social Taxonomy, 123 Columbia Law Review 2023.

DE MAURO, Andrea/GRECO, Marco/GRIMALDI, Michele/RITALA, Paavo: *Human Resources For Big Data Professions: A Systematic Classification of Job Roles and Required Skill Sets*, Information Processing & Management, 2017, C. 5, S. 5, 807-817.

KİŞİ, Nermin: *İnsan Kaynakları Yönetiminde Yapay Zeka: Bibliyometrik Bir Analiz*, Journal of Research in Business, 2022, C. 7, S.2, 490-514.

LEE, Min Kyung/KUSBIT, Daniel/METSKY, Evan/DABBISH, Laura: Working with Machines: The Impact of Algorithmic and Data-Driven Management on Human Workers, 2015, Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems CHI 2015, Association for Computing Machinery, New York, ABD, 1603–1612, https://doi.org/10.1145/2702123.2702548 (E.T. 8.4.2024).

OZAN ÖZPARLAK, Başak/ÇETİN, Müge: *ChatGPT ve Üretici Yapay Zekâ Modellerinde Mahremiyet ve Güvenliğin Hukuki Boyutu*, MÜHFHA, C. 29, S. 2, 2023, 1003-1040.

ZANFIR-FORTUNA, Gabriela: *Follow the (Personal) Data: Positioning Data Protection Law As the Cornerstone of EU's 'Fit For The Digital Age' Legislative Package,* EDPS at 20 Anniversary Volume, 2024.

Kitaplar

KAYA, Mehmet Bedii: KVKK Reformu: 2024 Değişiklikleri, Dijital Baskı, 1. Baskı, https://mbkaya.com/hukuk/kvkk-reformu.pdf (E.T. 20.5.2024).

LESSIG, Lawrence: Code and Other Laws of Cyberspace, 1999.

Kitap Bölümleri

AKÇOMAK, İ. Semih: Teknoloji, Küreselleşme ve İşgücü Piyasaları, (ed. Akçomak, İ. S., Erdil, E., Pamukçu, M.T. ve Tiryakioğlu, M.) "Bilim Teknoloji ve Yenilik: Kavramlar, Kuramlar ve Politika", 1. Baskı, İstanbul 2016, s. 301-316.

AKSOY RETORNAZ, E. Eylem/GÜÇLÜTÜRK, Osman Gazi: Yapay Zekada Kişisel Verilerin Korunması Kanunun Uygulanmasındaki Sorunlara İlişkin Değerlendirme, (ed. Pınar Çağlayan Aksoy, Hüseyin Can Aksoy), "Kişisel Verilerin Korunmasına Akademik Bakış", 1. Baskı, Ankara 2023, 413-438.

ENGİN Murat/OZAN ÖZPARLAK, Başak: İşe Girişte Yapay Zeka ve Ayrımcılık (ed. Erdem Büyüksağış), "Hukuk Perspektifinden Yapay Zeka", 1. Baskı, İstanbul 2022, 227-280.

KÜZECİ, Elif: Kişisel Verilerin Korunması Hakkı, (ed. Pınar Çağlayan Aksoy, Hüseyin Can Aksoy), "Kişisel Verilerin Korunmasına Akademik Bakış", 1. Baskı, Ankara 2023, 19-73.

Yayınlanmamış Tez

ARABOĞA, Uğur: İşe Alım Süreçlerinde Yapay Zeka Teknolojilerinin Kullanımı, İstanbul Medipol Üniversitesi Sosyal Bilimler Enstitüsü İşletme Yönetimi, Yayınlanmamış Yüksek Lisans Tezi, İstanbul, 2020.

Görüş/Raporlar

Cumhurbaşkanlığı Dijital Dönüşüm Ofisi: Türkiye Cumhuriyeti Ulusal Yapay Zekâ Stratejisi (UYZS), *https://cbddo.gov.tr/SharedFolderServer/Genel/File/TR-UlusalYZ Stratejisi2021-2025.pdf* (E.T. 20.5.2024).

Department For Science Innovation and Technology: Responsible AI In Recruitment Guidances, https://www.gov.uk/government/publications/responsible-ai-in-recruitment-guide/responsible-ai-in-recruitment (E.T. 20.5.2024).

Institute for Public Policy Research (IPPR): Transformed by AI: How Generative Artificial Intelligence Could Affect Work In The UK and How To Manage It, https://ippr-org.files.svdcdn.com/production/Downloads/Transformed_by_AI_March24_2024-03-27-121003_kxis.pdf (E.T. 1.6.2024).

International Monetary Fund (IMF): Gen-AI: Artificial Intelligence and the Future of *Work, https://www.imf.org/-/media/Files/Publications/SDN/2024/English/SDNEA 2024001.ashx* (E.T. 8.4.2024).

Kişisel Verileri Koruma Kurumu: Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi, 2019.

Kişisel Verileri Koruma Kurumu: Yapay Zeka Alanında Kişisel Verilerin Korunmasına Dair Tavsiyeler, Ankara, KVK Yayınları, 2021.

Kişisel Verileri Koruma Kurumu: Üretici Yapay Zeka Çağında Kişisel Verileri Yeniden Düşünmek, KVKK Bülten Temmuz 2023 Sayı:1, Ankara, 2023.

Michael Page Türkiye: Yapay Zeka ile İş Bulun: Teknolojiyi ve İnsan İçgörülerini Birlikte Kullanın,*https://www.michaelpage.com.tr/advice/kariyer-tavsiyeleri/kariyer-geli%C5%9Fimi/nyr24-yapay-zeka-ile-is-arama* (E.T. 20.5.2024).

OECD: Using AI in the Workplace: Opportunities, Risks and Policy Responses, https://www.oecd-ilibrary.org/docserver/73d417f9-en.pdf?expires=1716551203&id=id&accname=guest&checksum=ADAE8EEAC7DFA736CD176BA19A80AC3B (E.T. 20.5.2024).

Rani, Uma/Pesole, Annarosa/Gonzalez Vazquez, Ignacio: Algorithmic Management Practices in Regular Workplaces: Case Studies in Logistics and Healthcare, Publications Office of the European Union, *https://data.europa.eu/doi/10.2760/712475* (E.T. 20.5.2024).

The White House: Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, *https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/* (E.T. 20.5.2024).

US Department of Labor: Artificial Intelligence and Worker Well-being: Principles for Developers and Employers, https://www.dol.gov/general/AI-Principles (E.T. 20.5.2024).

World Economic Forum (WEF): Future of Work 2023, *https://www3.weforum.org/docs/WEF_Future_of_Jobs_2023.pdf* (E.T. 8.4.2024).

WOOD, Alex J.: *Algorithmic Management Consequences for Work Organisation and Working Conditions JRC Working Papers Series on Labour, Education and Technology* 2021, *https://ec.europa.eu/jrc/sites/default/files/jrc124874.pdf* (E.T. 4.7.2021).

İnternet Kaynakları

CORNELL LAW SCHOOL LEGAL INFORMATION INSTITUTE, LII, Redlining: *https://www.law.cornell.edu/wex/redlining#:~:text=Redlining%20can%20be%20defined%20as,on%20their%20race%20or%20ethnicity (*E.T. 20.5.2024).

EKONOMİST (2024), *İK'da Yapay Zeka Kullanıyor*, *https://www.ekonomist.com.tr/makale/ik-da-yapay-zeka-kullaniyor-46923* (E.T. 20.5.2024).

ELLIOT, Lance (2022): *AI Ethics Disquieted By AI Getting Dragged Into Quiet Quitting Mania,* Forbes, *https://www.forbes.com/sites/lanceeliot/2022/09/21/ai-ethics-disquieted-by-ai-getting-dragged-into-quiet-quitting-mania/?sh=78759b0c21be* (E.T. 20.5.2024).

HOOVER, Amanda (2024): LinkedIn's New AI Chatbot Wants to Help You Find Your Next Job, https://www.wired.com/story/linkedin-ai-chatbot-help-find-your-next-job/ (E.T. 8.4.2024).

LATOUR, Bruno (2012): *Lover Your Monsters*, The Breakthrough Institute, *https://thebreakthrough.org/journal/issue-2/love-your-monsters* (E.T. 20.5.2024).

LOMAS, Natasha (2021): *Uber hit with default 'robo-firing' ruling after another EU labor rights GDPR challenge,* TechCrunch, *https://techcrunch.com/2021/04/14/uber-hit-with-default-robo-firing-ruling-after-another-eu-labor-rights-gdpr-challenge/* (E.T. 17.8.2021).

OPENAI: Spring Update, *https://openai.com/index/spring-update/* (E.T. 20.5.2024).

ÖNERİ MODELLERİNİN KVKK İLE UYUMU

Prof. Dr. Şule GÜNDÜZ ÖĞÜDÜCÜ*

Öğr. Gör. Dr. Resul TUGAY**

GİRİŞ

Tüm dünya ile birlikte ülkemizde de internet kullanıcılarının sayısı gün geçtikçe artmaktadır. Yapılan araştırmalara göre sadece Türkiye'deki internet kullanıcılarının sayısının internet kullanımının yaygınlaşması ile birlikte 2024 ile 2029 yılları arasında yaklaşık % 13.5 artarak toplamda 86,7 milyona ulaşması öngörülmektedir. İnternet kullanımının yaygınlaşması ile birlikte hem web sitelerinin sayısı artmakta hem de bu sitelerde verilen hizmetlerin çeşitliliği ve içeriği artmaktadır. Örneğin elektronik ticaret pazarında önemli bir paya sahip olan Amazon'da 600 milyon civarında ürün bulunmaktadır. Aynı şekilde abonelik ile kullanıcılarına internet üzerinden yayın yapan Netflix'te yaklaşık 17.000 dizi ve film bulunmaktadır.

Bu tür platformlarda kullanıcıların istedikleri içeriklere veya ürünlere ulaşmaları iki yolla olabilir: (1) Kullanıcı aradığı ürün veya içeriği platformların arama özelliklerini kullanarak arayabilir. (2) Platformlar tarafından kullanıcıların ilgilenebilecekleri ürün veya içerik tahmin edilerek kullanıcılara önerilir. Kullanıcıların arama yoluyla istedikleri ürünlere veya içeriklere ulaşabilmeleri için ne aradıklarını bilmeleri gerekir. Ancak internetteki ürün ve içeriklerin sayısının gün geçtikçe artması ile kullanıcılar bazı içerik ve ürünlerden haberdar olamamakta ve istediklerini bulmakta zorlanmaktadırlar. Burada öneri sistemleri devreye girer. İnternet üzerindeki web sitelerinde kullanılan öneri sistemleri, genellikle kullanıcıların tercihlerine, tarama geçmişlerine ve diğer davranışlarına dayalı olarak içerik veya ürün önerileri sunan yazılım veya algoritmaları ifade eder. Bu sistemler, kullanıcı deneyimini kişiselleştirmek ve kullanıcıların ilgisini çekebilecek içerikleri keşfetmelerine yardımcı olmak için

* İstanbul Teknik Üniversitesi Yapay Zeka ve Veri Mühendisliği Bölümü

** Gazi Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü

kullanılır. Kullanıcıların bu sitelerde yaptıkları arama veya öneri arasında anlamlı bir fark olduğunu söylemek zordur. Örneğin video içerikleri sunan youtube web sitesinin ana sayfasında hem arama çubuğu bulunmakta hem de kullanıcının daha önce izlediği videolara göre izleyebileceği videolardan oluşan öneriler kullanıcıya sunulmaktadır. Ancak kullanıcı bir arama yaptığında da arama sonuçları yine kullanıcının daha önce ilgilendiği içeriklere göre sıralanarak sunulmaktadır. Sonuç olarak bu web siteleri genellikle kullanıcının etkileşim geçmişini analiz eder ve bu bilgilere dayanarak kullanıcıya ilgili içerikleri önerirler. Bunun için genellikle kullanıcıların davranışını izleyen ve benzer kullanıcıların tercihlerini analiz eden karmaşık algoritmalar kullanılır ve makine öğrenmesi ve yapay zekâ tekniklerinden yararlanarak öneriler üretilir. Bu sistemler ile, kullanıcılar web sitelerinde ilgilendikleri içeriklere kolayca erişebilirler. Böylece kullanıcıların web sitesinde daha uzun kalmaları ve web sitesi hizmetlerinden faydalanmaları sağlanır.

Ancak kullanıcıların davranışını analiz etmek için büyük miktarda veri toplayan bu sistemlerde, bu veriler amacına uygun olmayan şekilde kullanıldığında veya bu verilere yetkisiz kişiler eriştiğinde kullanıcı mahremiyeti için ciddi bir tehdit oluşabilir. Bu nedenle, öneri sistemlerini kullanan web platformlarının, doğru öneriler üretmelerine izin veren ve kullanıcılarının mahremiyetini garanti altına alan uygun bir denge noktası bulmaları son derece önemlidir. Kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyulması gereken usul ve esasları düzenleyen 6698 Sayılı Kişisel Verilerin Korunması Kanunu'nun bu aşamada önemli bir rolü vardır. Bu Kanun'da veri sorumlularının, kişisel verilerin işlenmesi sırasında uymaları gereken ilkeler ortaya konulmaktadır.

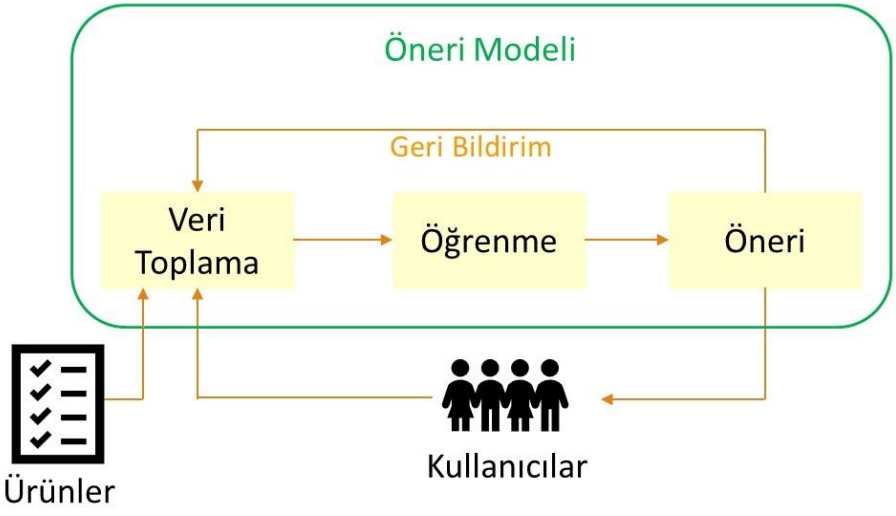
Bu bölümde öncelikle öneri modellerinin genel uygulaması üzerine kısa bir bilgi verilmiştir. Ardından kullanıcı verilerinin yoğun olarak kullanıldığı öneri modellerinde kullanılan ve bu modellerin yararlandığı veri kümeleri ve bu kümelerin toplanma şekilleri açıklanmıştır. Daha sonra 6698 sayılı Kanun tarafından belirlenen veri işleme ilkelerinin ihlalinden doğabilecek riskler örneklerle birlikte tartışılmıştır. Son olarak öneri sistemlerinin 6698 sayılı Kanun düzenlemelerine uyarlanması değerlendirilmiştir.

I. ÖNERİ MODELLERİ

Makine öğrenmesi yöntemlerini kullanan öneri modelleri rekabetin artması ile birlikte hem çevrim içi platformlarda hem de geleneksel fiziksel mağazalarda önem kazanmıştır. Öneri modellerini, makine öğrenmesi yöntemlerinin en verimli uygulamalarından biri olarak kabul etmek yanlış

olmayacaktır. Öyle ki Amazon şirketinin gelirinin %35'ini ürün öneri sistemi oluşturuyor[1]. Benzer şekilde Netflix'te kullanıcıların izlediği içeriğin %75'inin film öneri sistemlerinden geldiği belirtilmektedir[2]. Bunlarla beraber kullanıcılara kampanyalar oluşturmak için de yararlanılan öneri modelleri müşterilerin satın alma kararlarını ya da çevrim içi platformlarda kullanıcılara rehberlik ederek geçirdikleri süreyi doğrudan etkilemektedir. Dolayısıyla büyük veri ortamında öneri modellerinin kullanıcı güvenini artırmak, satışları artırmak ve genel müşteri memnuniyetini artırmak amaçlı kullanımı kaçınılmaz olmuştur.

Genel olarak öneri modellerinin amacı kullanıcılarına beğenebilecekleri ve ilgilenebilecekleri ürünleri sunmaktır. Bunun için sistemde kullanıcıların önceki alışveriş davranışlarından veya ilgilendikleri ve ilgilenmedikleri ürünlerden yararlanarak bir veri kümesi oluşturulur. Daha sonra bu veri kümesinden makine öğrenmesi yöntemleri ile elde edilen örüntülerden yararlanarak öneriler üretilir. Öneri modellerinin başlıca bileşenleri Şekil 1'de verilmiştir.



Şekil 1: *Öneri Modellerinin başlıca bileşenleri*

[1] Jones, Stephan S., and Frank M. Groom, eds. *Artificial Intelligence and machine learning for business for non-engineers*. CRC Press, 2019.

[2] Castrounis, Alex. *AI for people and business: A framework for better human experiences and business success*. O'Reilly Media, 2019.

Öneri modellerinin uygulanacağı ortama bağlı olarak oluşturulan veri kümesi ve toplanma yöntemi farklılık gösterir. Geleneksel fiziksel mağazacılık uygulamalarında bu veriler genellikle sadakat kartları yardımıyla veya alışveriş sırasında müşteriden alınan açık rıza ile toplanmaktadır. Çevrim içi platformlarda ise veri iki türlü toplanabilir: öncelikle kullanıcıların tıklamaları, görüntülemeleri ve satın alma geçmişleri de dahil olmak üzere kullanıcı etkileşimleri yoluyla veri otomatik olarak toplanabilir veya kullanıcılar tarafından kendi girmiş oldukları veri ile sağlanabilir. Öneri sistemleri de bu kullanıcı verilerini öneri sistemlerinin girdisi olarak toplarlar ve karşılığında kullanıcılarına daha iyi hizmetler ve ürünler sunarlar[3][4][5][6][7]. Örneğin kullanıcı etkileşimleri yoluyla veri toplayan bir elektronik alışveriş sitesindeki sayfa görüntüsü kullanıcının daha önce ilgilendiği ürünlerden yararlanarak ilgilenebileceği ürünler ile dinamik olarak oluşturulabilir ya da benzer kullanıcıların satın almış olduğu ürünler aktif kullanıcıya önerilebilir (bu ürünü alanlar aşağıdaki ürünleri de aldı gibi). Benzer şekilde bir video veya müzik içeriği sağlayan bir sitede önerilen içerik, kullanıcıların yakın zamanda izlediği videolardan veya dinlediği müziklerden etkilenerek oluşturulabilir. Sosyal medya platformlarında yine arkadaş önerileri ortak arkadaşlara ve benzer sosyal etkileşimlere dayanarak üretilir. Çevrim içi istihdam platformları adayların özgeçmişleri ve bağlantılarına dayanarak yeni iş önerileri üretirler. Bazı platformlarda ise kullanıcılar kendileri veri sağlayabilirler; örneğin kendilerine ait demografik bilgileri (yaş, cinsiyet gibi) girebilirler veya platformda yer alan ürünler için beğenilerini sistem üzerinden doğrudan belirtebilirler.

---

3 Awad, Naveen Farag, and Mayuram S. Krishnan. "The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization." *MIS quarterly* (2006): 13-28.

4 Chellappa, Ramnath K., and Raymond G. Sin. "Personalization versus privacy: An empirical examination of the online consumer's dilemma." *Information technology and management* 6 (2005): 181-202.

5 Cranor, Lorrie Faith. "'I didn't buy it for myself'privacy and ecommerce personalization." In *Proceedings of the 2003 ACM Workshop on Privacy in the Electronic Society*, pp. 111-117. 2003

6 Brusilovski, Peter, Alfred Kobsa, and Wolfgang Nejdl, eds. *The adaptive web: methods and strategies of web personalization*. Vol. 4321. Springer Science & Business Media, 2007.

7 Toch, Eran, Yang Wang, and Lorrie Faith Cranor. "Personalization and privacy: a survey of privacy risks and remedies in personalization-based systems." *User Modeling and User-Adapted Interaction* 22 (2012): 203-220.

Benzer şekilde çevrim içi ortamlar için geliştirilen öneri modelleri, kullanıcıların oluşturduğu bu verileri anlamak, verilerden benzer örüntüleri çıkartmak ve bu verileri kullanarak kullanıcılara daha iyi bir deneyim sunmak amacıyla geliştirilen algoritmik modellerdir. Bu modeller milyonlarca kullanıcının etkileşimde bulunduğu karmaşık veri kümeleri üzerinde çalışarak, bireylerin kişisel tercih ve davranışlarını anlamak için derinlemesine analizler gerçekleştirirler. Özellikle çevrim içi ortamlarda toplanan bu verilerin çok detaylı olabilmesi kullanıcı mahremiyeti için bir risk oluşturmaktadır. Bu platformları kullanan birçok kullanıcı, verilerinin toplanıp toplanmadığını ya da hangi verilerin toplandığını, bu verilerin üçüncü kişilerle paylaşılıp paylaşılmadığı, ne kadar güvenli bir şekilde ve ne kadar süreyle saklandığını yeterince bilmemektedir. Bu nedenle bu çalışmada çevrim içi platformda kullanılan öneri modellerinin 7 Nisan 2016 tarihinde yürürlüğe giren 6698 Sayılı Kişisel Verilerin Korunması Kanunu (6698 sayılı Kanun) ile olan uyumu tartışılmıştır. *Öneri Modelleri* veya *Öneri Sistemleri* bu çalışmada çevrim içi platformlar için geliştirilen öneri üretme yöntemleri için kullanılmıştır.

Dijital ortamlardaki öneri sistemlerinin temel hedefi, kullanıcı deneyimini özelleştirerek daha anlamlı ve tatmin edici bir içerik sunmaktır. Kullanıcıların geçmiş etkileşimleri, tercihleri, tıklama geçmişleri ve sosyal ağ verileri gibi çeşitli bilgi kaynaklarından faydalanarak öğrenme süreçlerini optimize eden öneri modelleri zaman zaman değişen verileri kullanarak güncellenirler. Bu sürekli öğrenme ve güncelleme mekanizmaları, sistemlerin zaman içinde daha isabetli ve kullanıcı odaklı hale gelmesine olanak tanır. Kullanıcılara, ilgilerini çekebilecek, beğenebilecekleri veya ihtiyaç duyabilecekleri içerikleri önererek, dijital ortamlardaki içerik tüketimini daha etkili ve keyifli hale getirmeyi amaçlarlar. Örneğin TikTok ve Instagram gibi sosyal medya uygulamalarında gezinirken, kullanıcılara izledikleri videolar ile benzer videolar önerilir ya da bir alışveriş sitesinde gezinirken, kullanıcıların geçmiş verilerine bakılarak uygun ürünler kullanıcılara önerilir. Bu durum sadece kullanıcının taleplerine daha hızlı ve doğru bir şekilde cevap vermekle kalmaz, aynı zamanda platformlar üzerinde geçirilen zamanı da artırarak kullanıcı bağlılığını güçlendirir. Bu bağlamda, öneri sistemleri hemen hemen tüm sektörlerde kritik öneme sahiptir; şirketler bu öneri sistemlerinden büyük miktarlarda gelir elde edebilirler ve rakiplerden önemli ölçüde öne çıkabilirler. Öyle ki, internet üzerinden dizi ve film kiralayan ve bunları üzerinden yayınlayan şirket olan Netflix, Ekim 2006'da 1 milyon dolar ödüllü yarışmasını duyurdu ve Eylül 2009'da, şir-

ketin film öneri sisteminin doğruluk oranını %10 oranında artıran BellKor's Pragmatic Chaos takımına büyük ödülü verdiğini açıkladı[8].

Öneri modelleri öneri üretirken kullanıcının ihtiyaçlarını ve zevklerini göz önüne alarak öneri üreten kişiselleştirilmiş modeller olabileceği gibi, her kullanıcıya aynı önerileri üreten kişiselleştirilmemiş modeller de olabilir. Örneğin çok satanlar, çok dinlenenler, yeni eklenenler, editörün seçtikleri gibi tüm kullanıcıların tercihleri göz önünde bulundurularak öneri listeleri oluşturulabilir. Ancak kişiselleştirilmiş öneri modellerinde kullanıcılara ait tercihler çıkarılarak her kullanıcının ihtiyacına yönelik olarak öneri listesi oluşturulur. Temel olarak kişiselleştirilmiş öneri sistemlerinde makine öğrenmesi yöntemleri herhangi bir kullanıcı u ve ürün i için bir skor r hesaplar. Daha sonra öneri sistemi bu kullanıcı için en yüksek skora sahip olan ürünleri sıralayarak önerir. Bu işlem üç aşamada gerçekleşir;

(1) Gerçek hayattaki öneri sistemlerinde yüz binlerce hatta milyonlarca ürün bulunduğundan öneri sistemleri öncelikle bu ürünleri aday havuzu oluşturmak için yüzlerce ya da binlerce önerilecek adaya düşürür. Bu aşama hesaplama olarak çok karmaşık olmayan sistemlerden oluşur ki sistem milyonlarca aday ürün içerisinden binlerce ürünü seçebilsin.

(2) Daha sonra başka bir model, kullanıcıya gösterilecek ürünleri seçmek için adayları puanlar ve sıralar. Bu ürün kümesi artık onlarca üründen oluşur. Bu modelde kullanılan ürün sayısı ilk aşamada kullanılan ürün sayısında çok daha küçük olacağından bu aşamada kullanılan model daha kesin bir modeldir.

(3) Son olarak öneri sistemi, tekrar sıralama yaparak kullanıcının eğer var ise kısıtlamalarını da dikkate alarak ürünleri puanlandırır.

Öneri sistemleri yukarıda verilen ilk adımda kullanılan filtreleme yöntemine göre üç genel grupta toplanabilir[9]:

- İşbirlikçi Filtreleme: Aktif kullanıcıya benzer kullanıcıların geçmişte tercih ettikleri ürünler kullanılarak ürün aday havuzu oluşturulması.

---

8 Koren, Yehuda. "The bellkor solution to the netflix grand prize" *Netflix prize documentation* 81, no. 2009 (2009): s1-10.

9 Adomavicius, Gediminas, and Alexander Tuzhilin. "Toward the next generation of recommender systems: A survey of the state-of-the-art and possible extensions." *IEEE transactions on knowledge and data engineering* 17, no. 6 (2005): 734-749.

- İçerik Tabanlı Filtreleme: Aktif kullanıcın geçmişte tercih ettiği ürünlere benzer ürünler kullanılarak ürün aday havuzu oluşturulması.
- Hibrit Yaklaşımlar: İşbirlikçi filtreleme ve içerik tabanlı filtreleme yöntemlerinin birlikte kullanılmasıyla ürün aday havuzu oluşturulması.

A. ÖNERİ SİSTEMLERİ ÇEŞİTLERİ

Öneri sistemlerinde öneri üretme problemi şu şekilde temsil edilebilir: $U = \{u_1, u_2, \dots, u_N\}$ kullanıcılardan oluşan bir küme ve $I = \{i_1, i_2, \dots, i_K\}$ ürünlerden oluşan bir küme olmak üzere öneri modelinin amacı, kullanıcının memnuniyetini veya platformun hedeflerini temsil etmek üzere tasarlanan bir fayda fonsiyonunun, $f : U \times I \rightarrow S$, optimize edilmesidir. S kümesi pozitif değerlerden oluşan tam sıralı bir kümedir. Bu durumda amaç Eşitlik 1'de verildiği üzere her $u \in U$ kullanıcısı için f fonksiyonunu enbüyütecek $R_u \subset I$ öneri kümesini oluşturmaktır.

$$\forall u \in U, R_u = arg\max_{i \in I} f(u,i) \quad (1)$$

Öneri modellerinde bir ürünün bir kullanıcıya faydası genel olarak ölçülebilir, örneğin kullanıcının ürüne verdiği puan olabileceği gibi, platformun önerilen ürünlerin tıklanması/satın alınması ile dönüşüm oranını artırması olarak da değerlendirilebilir.

Kullanıcı ve ürün uzayındaki her u kullanıcısı ve i ürünü sadece tekil bir kimlik numarası (ID) ile temsil edilebileceği gibi kullanıcının veya ürünün özelliklerini temsil eden bir profille de temsil edilebilir. Örneğin kullanıcı için bu profil yaş, cinsiyet, eğitim durumu, gelir seviyesi gibi bilgiler olabilir. Bir ürün için ise bu profil uygulama alanına bağlı olarak ürünün özellikleri olabilir; örneğin bir film önerisi üreten platformda o filmin adı, türü, çekim yılı, kullanıcı puanı, kullanıcı yorumları, yönetmeni gibi özelliklerden oluşabilir.

Böyle bir uygulamada kullanıcı ve ürün sayıları çok büyük olduğu için f fayda fonksiyonunu $U \times I$ uzayında hesaplamak çok maliyetlidir. O nedenle genel yaklaşım bu uzayın öncelikle bir filtreleme ile elde edilen alt kümesinde yer alan ürün adayları için fayda fonksiyonun hesaplanmasıdır.

Bu bölümde öneri sistemlerinde ürün adaylarını oluşturmak için kullanılan yaklaşımlar anlatılmıştır.

1. İşbirlikçi Filtreleme

İşbirlikçi filtreleme algoritmaları, kullanıcılar ve ürünler arasındaki önceki etkileşimleri göz önüne alarak, kullanıcıların gelecekteki etkileşimlerini tahmin ederler. Örneğin kullanıcı u_i ve kullanıcı u_j'nin beğendikleri ortak ürün sayısı fazla ise bu iki kullanıcının ortak zevkleri olduğu çıkarımı yapılır. Bu durumda örneğin kullanıcı u_i ürün i_k'yi beğenmişse ve kullanıcı u_j'nin ürün i_k ile ilgili herhangi bir etkileşimi yoksa, o zaman bu öneri sisteminin kullanıcı u_j'ye ürün i_k'yi önerme ihtimali yüksektir. Bu yöntemde kullanıcının daha önce satın aldığı ürünler veya bu ürünlere verilen puanlar ve diğer kullanıcılar tarafından alınan benzer kararlar gibi kullanıcıların geçmiş davranışlarından oluşan bir veri ile model oluşturur[10][11][12][13][14].

İşbirlikçi filtreleme yönteminde u kullanıcısının i ürünü için olan fayda fonksiyonu $(f(u,i))$ u kullanıcısına "benzer" kullanıcıların $u_j \in U$, i ürünü için olan fayda değeri ($f(u_j, i)$) temel alınarak hesaplanır. Kullanıcılar arası benzerlik farklı yaklaşımlarla hesaplanabilir. Yaygın olarak kullanılan yaklaşımlar, kullanıcıların etkileşimde bulundukları ortak ürünler üzerinden korelasyon tabanlı benzerlik veya Kosinüs benzerliği hesaplamaktır. İki kullanıcı u_i ve u_j arasındaki Pearson korelasyon benzerliği Eşitlik 2'de verildiği şekilde hesaplanabilir:

---

10 Sarwar, Badrul, George Karypis, Joseph Konstan, and John Riedl. "Item-based collaborative filtering recommendation algorithms." In *Proceedings of the 10th international conference on World Wide Web*, pp. 285-295. 2001

11 Schafer, J. Ben, Dan Frankowski, Jon Herlocker, and Shilad Sen. "Collaborative filtering recommender systems." In *The adaptive web: methods and strategies of web personalization*, pp. 291-324. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007.

12 Koren, Yehuda, Robert Bell, and Chris Volinsky. "Matrix factorization techniques for recommender systems." *Computer*42, no. 8 (2009): 30-37.

13 Lee, Daniel, and H. Sebastian Seung. "Algorithms for non-negative matrix factorization." *Advances in neural information processing systems* 13 (2000).

14 Mnih, Andriy, and Russ R. Salakhutdinov. "Probabilistic matrix factorization." *Advances in neural information processing systems* 20 (2007).

$$sim(u_i, u_j) = \frac{\sum_{x=1}^{K}(r_{ix}-\overline{r_i})(r_{jx}-\overline{r_j})}{\sqrt{\sum_{x=1}^{K}(r_{ix}-\overline{r_i})^2(r_{jx}-\overline{r_j})^2}} \quad (2)$$

Bu eşitlikte r_{ix}, u_i kullanıcısının i_x ürününe beğenisini gösteren puanı, $\overline{r_i}$ ise u_i kullanıcısının puan verdiği tüm ürünlerden hesaplanan ortalama puanıdır. Kosinüs benzerliği ise her kullanıcıyı K boyutlu uzayda bir vektör olarak temsil eder. İki kullanıcı arasındaki benzerlik kullanıcılara ait vektörler arasındaki açının kosinüs değeri olarak hesaplanır. Eşitlik 3'te Kosinüs benzerliği verilmiştir:

$$sim(u_i, u_j) = cos(\overrightarrow{u_i}, \overrightarrow{u_j}) = \frac{\overrightarrow{u_i} \cdot \overrightarrow{u_j}}{|\overrightarrow{u_i}|_2 \times |\overrightarrow{u_j}|_2} = \frac{\sum_{x=1}^{K} r_{ix} r_{jx}}{\sqrt{\sum_{x=1}^{K} r_{ix}^2} \sqrt{\sum_{x=1}^{K} r_{jx}^2}} \quad (3)$$

Bu eşitlikte $\vec{x} \cdot \vec{y}$ olarak hesaplanan değer $\vec{x}$ ve $\vec{y}$ vektörleri arasındaki nokta çarpımıdır.

İşbirlikçi filtreleme yöntemleri kullanıcıların veya ürünlerin tanımlayıcı verilerini kullanmaz. Bunun yerine sadece kullanıcılar ve ürünler arasındaki etkileşim verisinden yararlanarak öneri üretilir.

2. İçerik Tabanlı Filtreleme

İçerik tabanlı filtreleme yöntemleri ürünlerin ya da kullanıcıların içerik olarak adlandırılan özelliklerinden yararlanarak öneri üretirler[15][16][17][18]. Bu yöntemlerde kullanıcıların veya ürünlerin içerikleri tanımlayıcı özellikleri belirlenerek temsil edilir. İçerik tabanlı filtreleme yöntemlerinde u kullanıcısının i ürünü için olan fayda fonksiyonu ($f(u,i)$) i ürününe "benzer" ürünlerin ($j \in I$) u kullanıcısı için olan fayda değeri ($f(u,j)$) temel alına-

15 Mooney, Raymond J., and Loriene Roy. "Content-based book recommending using learning for text categorization." In *Proceedings of the fifth ACM conference on Digital libraries*, pp. 195-204. 2000

16 Pazzani, M. J. "Content-Based Recommendation Systems." (2007)

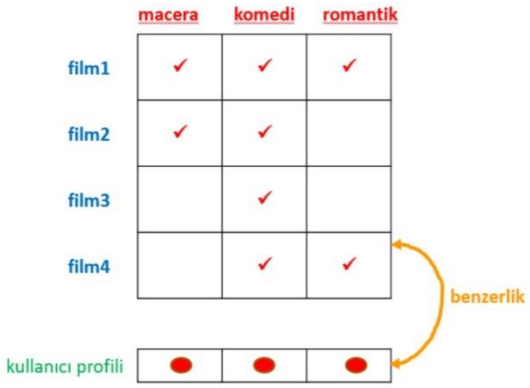
17 Lops, Pasquale, Marco De Gemmis, and Giovanni Semeraro. "Content-based recommender systems: State of the art and trends." *Recommender systems handbook* (2011): 73-105

18 Van den Oord, Aaron, Sander Dieleman, and Benjamin Schrauwen. "Deep content-based music recommendation." *Advances in neural information processing systems* 26 (2013)

rak hesaplanır. İşbirlikçi filtreleme yöntemlerinden farklı olarak ürünler arası benzerlik hesaplanırken ürünleri temsil eden özellikler kullanılır. Örneğin bir restoran önerisi üreten sistemde restoranların mutfak türlerine göre benzerlik hesaplanırken, bir film önerisi üreten sistemde film türlerine göre benzerlik hesaplanabilmektedir. Bu yöntemde temel amaç bir u kullanıcısının etkileşimde bulunduğu ürünlerin içerikleri arasında ortak özellikleri belirleyebilmek ve bu ortak özelliklere benzer ancak kullanıcının henüz etkileşimde bulunmadığı ürünleri kullanıcıya öneri olarak sunabilmektir.

İçerik tabanlı filtreleme yöntemlerinde bir kullanıcının veya ürünün içeriği öneri aşamasında katkı sağlayacak tanımlayıcı özelliklerinden oluşturulur. Genellikle ürün veya kullanıcı profilinin bir grup özellik ile tanımlanabilecek uygulamalarda kullanılması uygun olur. Örneğin ürün için metin tabanlı bir tanım varsa, bu metinden elde edilen anahtar kelimeler ile ürün içeriği ($Icerik(i)$) oluşturulabilir. Ürün içeriği oluşturmak için ürün görselinin kullanılması da uygulanan yöntemlerden biridir. İçerik oluşturulurken her bir özellik için o özelliğin ürünü tanımlamada ne kadar önemli olduğunu belirten bir ağırlıklandırma kullanılabilir ya da bir ağırlıklandırma kullanmadan ilgili özelliğin üründe bulunup bulunmamasına göre özellik değeri 1 ya da 0 olabilir.

Bazı sistemlerde kullanıcıdan örneğin yaş, cinsiyet gibi bilgi girişi istenebilir, bu tür bilgiler içerik tabanlı filtreleme yöntemlerinde kullanıcı profili oluşturmak ($KullanıcıProfili(u)$) için kullanılabilir. Ancak kullanıcıların kendileri hakkında bilgi verme konusunda isteksiz olması, zorunlu olmadıkça bu bilgileri girmemeleri (ya da doğru girmemeleri) nedenleriyle kullanıcı profili oluşturma genellikle dolaylı olarak yapılır. Buradaki temel yaklaşım kullanıcıları ürün özelliklerinin temsil edildiği uzaydaki özellikler ile eşleştirerek kullanıcı profili oluşturmaktır. Kullanıcının sistemde etkileşimde bulunduğu ürünlerin özellikleri analiz edilerek kullanıcı profili elde edilir. Şekil 2'de bu hesaplama için bir örnek verilmiştir.



Şekil 2: İçerik Tabanlı Filtreleme ile fayda değeri elde edilmesi

Bu örnekte sistemdeki ürünler filmler ve ürün özellikleri de film türleridir. Örneğin sistemdeki tüm filmlerin sadece macera, komedi ve romantik özellikleri olduğunu kabul edersek her filmin içeriği üç boyutlu bir vektörle temsil edilebilir. $film1$'in türü bu üç türle de ilgiliyse o zaman bu filme ait içerik, ağırlıklandırma kullanmadığımız durumda, $Icerik(Film1) = [1,1,1]$ vektörü ile temsil edilebilir. Kullanıcı $film1$, $film2$ ve $film3$'ü seyretmiş ise bu üç filmin her bir boyuttaki değerinden örneğin ortalama hesaplanılarak kullanıcının her bir boyuta ilgisini temsil eden bir kullanıcı profili oluşturulabilir. Örnek için kullanıcı profili $KullanıcıProfili(u) = [2/3, 1, 1/3]$ olmaktadır. Kullanıcı profilinin ve ürün içeriklerinin aynı boyutlu uzayda birer vektör ile temsil edilmesinin ardından kullanıcılar ve ürünler arasında bir benzerlik hesaplanır ve kullanıcı profiline içerik olarak en benzer ürünler kullanıcıya önerilir. Bu durumda $KullanıcıProfili(u)$ve $Icerik(i)$ arasındaki benzerlik skoru $f(u,i)$ fayda değerini verir (Eşitlik 4).

$$f(u,i) = skor(KullanıcıProfili(u), Icerik(i)) \quad (4)$$

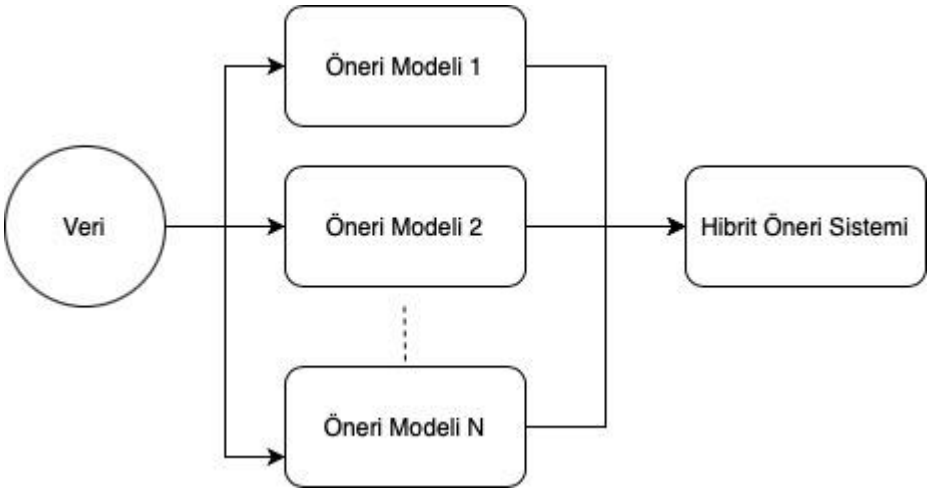
Benzerlik skoru olarak yaygın olarak Kosinüs benzerliği kullanılabilir.

3. Hibrit Yöntemler

Öneri sistemlerinde yaygın olarak kullanılan içerik tabanlı ve işbirlikçi filtreleme yöntemleri, kullanıcı ve ürünler arasındaki ilişkiyi öğrenmek

için yeterli veri olmadığında iyi bir öneri sunamazlar. Bu tür durumlarda, üçüncü bir yaklaşım olarak hibrit yöntemler (Şekil 3) kullanılır. Bu yaklaşım, hem içerik tabanlı hem de işbirlikçi filtreleme yöntemlerinin eksikliklerini gidererek aşağıdaki avantajları sağlar[19][20][21].

- Artan doğruluk: Hibrit yöntemler, farklı öneri sistemlerinin güçlerini birleştirerek daha doğru öneriler sunabilir.
- Artan çeşitlilik: Hibrit yöntemler, farklı sistemlerden gelen önerileri birleştirerek daha çeşitli öneriler sunabilir.
- Dayanıklılık: Hibrit yöntemler, yeni kullanıcılara veya yeni öğelere ilişkin yeterli veri olmadığı durumları içeren soğuk başlangıç problemlerine karşı daha dayanıklı olabilir.



Şekil 3: *Hibrit Öneri Sistemleri*

19 Burke, Robin. "Hybrid recommender systems: Survey and experiments." *User modeling and user-adapted interaction* 12 (2002): 331-370

20 Kiran, R., Pradeep Kumar, and Bharat Bhasker. "DNNRec: A novel deep learning based hybrid recommender system." *Expert Systems with Applications* 144 (2020): 113054

21 Javed, Umair, Kamran Shaukat, Ibrahim A. Hameed, Farhat Iqbal, Talha Mahboob Alam, and Suhuai Luo. "A review of content-based and context-based recommendation systems." *International Journal of Emerging Technologies in Learning (iJET)* 16, no. 3 (2021): 274-306

İşBirlikçi ve İçerik Filtreleme Yöntemleri farklı şekillerde birleştirilebilir[22].

- *Ağırlıklı Birleştirme*: Bu birleştirme yönteminde her bir öneri modelinin çıktısı alınır ve sonuç sabit ağırlıklarla birleştirilir; bu ağırlıklar eğitim ve test kümesi boyunca değişmeyecek şekilde belirlenir. Örneğin, içerik tabanlı bir model ile işbirlikçi filtreleme modeli %50'şer ağırlık olacak şekilde birleştirilebilir.
- *Anahtarlı Birleştirme*: Bu hibrit öneri sistemi, duruma bağlı olarak var olan öneri yöntemlerinden yalnızca bir tanesini seçer. Eğer seçilen öneri modeli istenilen güvenirlikte öneri üretemez ise diğer öneri modelini seçilebilir.
- *Karışık Birleştirme*: Öncelikle giriş verisinden farklı şekillerde aday kümeleri oluşturulur. Daha sonra her bir aday kümesi farklı öneri modellerinde kullanılarak öneriler üretilir. Sonuç olarak tüm öneri modellerinin sonuçları birleştirilerek öneri yapılır. Çok fazla öneri gerektiren durumlarda, bu yöntem kullanılabilir.
- *Özellik Birleştirme*: Bu yöntemde işbirlikçi model için kullanılan etkileşim verisi içerik tabanlı modelde kullanılan veri için ek bir özellik gibi ele alınır bu zenginleştirilmiş veri içerik tabanlı bir modelde kullanır.
- *Özellik Artırma*: İşbirlikçi modelden elde edilen benzer ürünler daha sonra kullanılacak ikinci bir öneri modeli için yeni bir veri kümesi oluşturur. Bu veri kümesinde, ürünlere sınıf değerleri atayarak problem ikili sınıflandırma olarak da düşünülebilir veya ürünler için benzer kullanıcılardan elde edilen bir skoru kullanarak ikinci modelde skor tahmin edilebilir.
- *Kademeli Birleştirme*: Bu hibrit yöntemde aşamalı olarak önerilecek ürünlerin genel bir tahmini yapılır daha sonra ikinci bir öneri modeli daha net ve kesin sonuçlar üretir. Birinci öneri modelinin sonucu ikinci öneri modeli için aday havuzu oluşturur.
- *Meta-Seviye Birleştirme*: Bu yöntem, özellik artırma yöntemine benzemektedir. Fakat özellik artırmadan farklı olarak, ikinci model giriş verisi için orijinal veri kümesini değil, öğrenilen birinci modelden elde edilen yeni veri kullanır.

---

22 Burke s. 331-370

B. ÖNERİ MODELLERİNDE KULLANILAN VERİ TÜRLERİ

Öneri modellerinde yukarıda bahsedilen öneri modeli türlerine göre farklı kaynaklardan farklı veriler kullanılabilmektedir. Bu verilerin bir kısmı doğrudan kullanıcı tarafından sağlanabileceği gibi bir kısmı da sistem tarafından kullanıcı davranışları takip edilerek dolaylı olarak üretilebilir. Aşağıda kullanılan farklı veri türleri ve veri türlerinin hangi tip öneri modellerinde kullanılabileceği kısaca özetlenmiştir.

1. **Davranış Verisi**: Öneri modelinin çalıştığı çevrim içi platform ile kullanıcının etkileşimi sırasında toplanır. Öneri modelinin çalıştığı platforma bağlı olarak bu kullanıcının herhangi bir sayfada ne kadar zaman geçirdiği, sayfada nelere tıkladığı, hangi ürünlere baktığı, site içinde hangi aramaları yaptığı, bu arama sonuçları ile etkileşimleri, bir elektronik ticaret sitesi ise hangi ürünleri sepetine attığı veya video içeriği sağlayan bir platform ise videoyu ne kadar süre seyrettiği olabilmektedir. Kullanıcılara platform tarafından gönderilen e-postalar ya da ilgili platformun mobil uygulaması tarafından gönderilen bildirimler ile etkileşimler de yine davranış verisi oluşturmak için kullanılmaktadır.

2. **Bağlam Verisi**: Kullanıcıya önerilerin sunulması sırasında kullanıcı bağlamı belirlenebilir. Yaygın olarak kullanılan bağlam verileri kullanıcının konumu, tarih, saat, çevrim içi platform hizmeti aldığı cihaz bilgisi olabilmektedir.

3. **Ürün Verisi**: Çevrim içi platformdaki önerilecek ürünler için tanımlayıcı özelliklerin çıkarılması ile elde edilir. Örneğin bir film öneri sisteminde filmin türü, süresi, bütçesi vs., ya da elektronik ticaret sitesinde ürünün kategorisi gibi bilgiler bu veri türü altında değerlendirilebilir.

4. **Satın Alma veya Tüketim Geçmişi Verisi**: Bir elektronik ticaret sitesi için kullanıcıların daha önce almış olduğu ürünler veya bir içerik sağlama platformu için kullanıcıların hangi içerikleri tükettikleri bilgisi olabilmektedir.

5. **Sosyal Ağ Verisi**: Öneri modeli bir sosyal medya platformu için geliştirilmiş ise kullanıcıların platformda hangi kullanıcılar ile ne tür ilişkisi olduğu verisidir. Örneğin; kullanıcılar arası arkadaşlık ilişkisi, hangi kullanıcının hangi kullanıcıyı takip ettiği gibi veriler olabilmektedir.

6. **Kullanıcı Verisi**: Kulanıcıyı tanımlayan verilerdir. Kullanıcının yaşı, cinsiyeti, evlilik durumu gibi bilgiler örnek verilebilir.

7. **Kullanıcı Tercihleri Verisi**: Bazı çevrim içi platformlarda sunulan hizmete bağlı olarak kullanıcı, bir ürüne veya içeriğe olan beğenisini değerlendirmek için ürüne bir puan verebilir. (Genelde 1-5 arası bir puan veya sadece beğendim/beğenmedim şeklinde bir seçenek) Kullanıcının ürün veya içerik için oluşturduğu etiketlerden veya yorumlardan da yine kullanıcı beğenisi elde edilmeye çalışılır.

Öneri modelinin kullanıldığı çevrim içi platformun verdiği hizmetlere göre toplanan veriler değişiklik göstermekle birlikte tüm öneri modellerinde kullanıcılar için davranış verisi oluşturulmakta ve kullanılmaktadır. Bu veriler toplanma türlerine göre ikiye ayrılır:

- Açık Veri Toplama: Kullanıcılar tercihlerini açıkça belirttiklerinde ortaya çıkan verilerdir. Örneğin kullanıcılar ürünler hakkında beğenilerini belirtecek şekilde bir puan girebilirler ya da ürünler hakkında yorum yazabilirler.
- Dolaylı Veri Toplama: Sistem kullanıcıdan herhangi bir ek veri talep etmez. Kullanıcıların çevrim içi platformdaki hareketleri ve istatiksel veriler kullanılarak kullanıcı tercihleri belirlenir.

Kişiselleştirilmiş öneri sistemlerinin uygulanacağı çevrim içi platformlarda bu veriyi oluşturmak için öncelikle tekil kullanıcıların belirlenmesi ve ilgili kullanıcı çevrim içi platformu kullanmaya başladığında o kişiye özel önerilerin sunulması gerekmektedir. Eğer kullanıcı girişi gerektiren bir çevrim içi platform ise tekil kullanıcılar sahip oldukları kullanıcı hesaplarına göre belirlenebilir. Kullanıcı girişi gerektirmeyen platformlarda ise bu iki yolla yapılabilir: (1) web sunucuları tarafından oluşturulan web kayıtlarının kullanılması; (2) internet çerezlerinin kullanılması. Web sunucusu tarafından oluşturulan web kayıtları kullanıcıların web sitesine yaptığı her isteği ve etkileşimi içerir. Bu kayıtlar genellikle IP adresleri, kullanıcı ajanları (user agents), istenen sayfalar, isteğin tarihi ve saati gibi bilgileri içerir. Bu bilgiler kullanılarak, tekil kullanıcılar bazı durumlarda tanımlanmakla birlikte bu yöntemlerin çerez tabanlı yöntemlere göre sınırlamaları vardır. Örneğin, aynı ağ arkasındaki birden fazla kullanıcıyı ayırt etmek zor olabilir ve IP adresleri dinamik olarak değişebilir. Ayrıca, bu tür yöntemler gizlilik konusunda endişelere yol açabilir ve çoğu zaman kullanıcıların rızasını almadan kişisel verilerin işlenmesiyle ilgili düzenlemelere uymayabilir. Bu nedenle, kullanıcıları belirlemek için çerez tabanlı yöntemler genellikle daha yaygın ve güvenilir olarak kabul edilir.

İnternet çerezleri (cookies), bir kullanıcı bir web sitesine erişim sağladığında bu web sitesi tarafından kullanıcıların tarayıcılarına gönderilen küçük veri parçalarıdır. İnternet sitesinin çalışması amacıyla kesinlikle gerekli çerezler vardır. Bunlar dışında kullanıcıya sunulan işlevsel çerezler, performans analitik çerezler ve reklam/pazarlama çerezleri vardır. Örneğin, uçak bileti satın alınan bir platform, hangi aramaların yapıldığı, nereden nereye, hangi gün ve saat için arama yapıldığı bilgilerini çerezlerde tutabilir ve bir sonraki aramada bu uçuşların fiyatlarını dinamik olarak belirleyebilir.

C. RİSKLER

Kullanıcı verileri, kişiselleştirilmiş öneri sistemlerini eğitmek için kullanılan yapay zekâ modellerinin temelini oluşturmaktadır. 7 Nisan 2016 tarihinde yürürlüğe giren 6698 sayılı Kanun ile çevrim içi kullanıcıların kişisel verilerini kullanmak için birtakım düzenlemeler gelmiştir. 6698 sayılı Kanun'un 3. maddesinde *Kişisel Veri* "Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi", *İlgili Kişi* ise "Kişisel verisi işlenen gerçek kişi" olarak tanımlanmıştır. Bu bağlamda çevrim içi platformlarda öneri sunulacak kullanıcılar *İlgili Kişi*, kullanıcı verileri ise *Kişisel Veri* olarak görülebilir. Kişilerin adı, soyadı, cinsiyeti, mesleği, yaşı, yaşadığı bölge gibi bilgiler kişisel veri kapsamına girmekle beraber, alışveriş alışkanlıkları, hobileri, ilgi alanları gibi kişiyi dolaylı olarak belirleyebilecek bilgiler de kişisel veri olarak değerlendirilebilir. Her kişi verilerinin işlenmesini kontrol etme hakkına sahiptir. 6698 sayılı Kanun'un amacı bu hakkı korumak ve kişisel verilerin ancak belirli koşullara uyulduğu durumda işlenmesine izin vermektir.

Diğer önemli kavramlar ise *Veri Sorumlusu* ve *Veri İşleyen* olarak tanımlanan kavramlardır.23 Kişisel verilerin işlenmesinin amaçlarını ve vasıtalarını belirleyen kişi Veri Sorumlusu, veri sorumlusu adına kişisel verileri işleyen gerçek veya tüzel kişi de Veri İşleyen olarak tanımlanmaktadır. Veri sorumluları hangi kişisel verilerinin toplanacağına, hukuki sebebinin ne olduğuna, hangi amaç/amaçlar için işleneceğine, hangi kişilerin verilerinin toplanacağına, veriler paylaşılacaksa kim/kimlerle paylaşılacağına, kişisel verilere kimlerin hangi izinlerle erişeceğine, ne kadar süre saklanacağına ve hangi durumlarda değiştirileceğine karar verirler. Veri işleyenler ise verilen bu kararların nasıl uygulanabileceği konusunda karar verirler. Genel olarak

[23] Kişisel Verileri Koruma Kurumu: Veri Sorumlusu ve Veri İşleyen, (https://www.kvkk.gov.tr/Icerik/4195/Veri-Sorumlusu-ve-Veri-Isleyen E.T.: 22.11.2024), s.1-10.

veri işleyenler, kişisel verilerin toplanmasında kullanılacak bilgi teknolojileri ve yöntemleri, saklanma ortamları, alınması gereken güvenlik önlemleri, veri aktarımı gerektiğinde kullanılacak teknolojiler, verilerin silinmesi, yok edilmesi, değiştirilmesi, anonim hale getirilmesi gibi konularda karar verirler. Günümüz dünyasındaki iş modellerinde çoğunlukla öneri sistemlerinin kullanılacağı çevrim içi platformlar veri sorumlusu tarafında olurken, öneri modellerini geliştiren taraflar ise veri işleyenlerdir. Bir şirket bünyesinde yer alan birimlerin ya da kişilerin tüzel kişiliği bulunmadığından, bu birimlerin veri sorumlusu veya veri işleyen olması mümkün değildir. Bir şirketler topluluğunu oluşturan her bir şirket tüzel kişiliğe sahip olduğundan, bu şirketlerin her birinin ayrı veri sorumlusu olması mümkündür.

İlgili kişileri verilerinin işlendiğine dair bilgilendirmek veri sorumlusu veya veri sorumlusunun yetkilendirdiği kişi tarafından yerine getirilmelidir. Sonuç olarak ilgili kişi, kişisel verisinin işlendiğine dair her durumda aydınlatılmalıdır. Günümüzde insanların kişisel bilgilerini bir meta olarak gördüğünü savunanlar vardır. Bazı kişiler kişisel kazanımlar karşılığında bazı bilgilerini vermeyi kabul edebilirler. Öneri sistemleri de buna iyi bir örnektir. Kişiler verilerini paylaşmayı kabul etse bile toplanan verilerin sorumlu bir şekilde işlendiğinden emin olmak için 6698 sayılı Kanun'da veri işleme ilkeleri belirlenmiştir:

- Hukuka ve dürüstlük kurallarına uygun olma: Kişisel verilerin yasal yollarla ve adil olarak elde edilmesi, veri işleme faaliyetinin Kanun'da belirtilen açık rıza dışındaki şartlardan birini karşılaması durumunda öncelikli olarak söz konusu veri işleme şartına dayanarak işlenmesi, eğer amaç Kanun'da belirtilen açık rıza dışındaki şartlardan birini karşılamıyorsa bu durumda ilgili kişinin açık rızasının alınması yoluna gidilmesi gerekmektedir. Yetkisiz erişime, yok edilmeye, kullanılmaya, değiştirilmeye veya açıklanmaya karşı güvence altında olmalıdır.

- Doğru ve gerektiğinde güncel olma: Veri doğru, eksiksiz ve güncel olmalıdır.

- Belirli, açık ve meşru amaçlar için işlenme: Veri sorumlusu veri işleme amacını açık ve kesin olarak belirtmek zorundadır. Bu amacın veri sorumlusunun yapmış olduğu iş veya sunmuş olduğu hizmetle bağlantılı ve bunlar için gerekli olması gerekmektedir.

- İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma: İşlenen kişisel veriler belirlenen amaçla ilgili olmalı, amacın gerçekleştirilmesiyle ilgili ve gerekli olmayan kişisel veriler işlenmemelidir.
- İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme: İlgili mevzuatta verilerin saklanması için öngörülen bir süre varsa veri sorumlularının bu süreye uymaları gerekmektedir; yoksa veriler, ancak işlendikleri amaç için gerekli olan süre kadar saklanabilirler. Gelecekte kullanma olasılığına dayanarak veri saklanamaz.

Kişisel verilerin 6698 sayılı Kanun'da belirtilen ilkelere uygun bir şekilde işlenmesi gerekmektedir. Öneri sistemlerinin kullanıcıların verilerini toplama ve bu verilerden davranış örüntülerini ve kişisel tercihlerini çıkarma gereksinimi göz önüne alındığında, "Hukuka ve dürüstlük kurallarına uygun olma", "Belirli, açık ve meşru amaçlar için işlenme", "İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma" ilkelerini ihlal etme riski gündeme gelebilir. Bu ilkelere uyulmaması durumunda üç farklı kaynaktan tehdit oluşabilir: (1) Öneri sistemi; (2) Öneri sistemini kullanan diğer kullanıcılar; (3) Öneri sistemi kullanıcısı olmayan dış varlıklar. Bu tehdit kaynaklarına göre oluşan riskler Tablo 1'de gösterilmiştir[24].

Tablo 1

Veri İşleme İlkelerinin ihlal edilmesi ile öneri sistemlerinde oluşabilecek riskler

Tehdit	Veriye Doğrudan Erişim	Verinin İşlenmesi
Öneri Sistemi	Amaca aykırı veri toplama 3. taraflarla verinin paylaşılması Çalışanların yetkisiz veriye erişimi	Hassas bilgilerin ortaya çıkması Hedeflenmiş reklamcılık Ayrımcılık
Diğer Kullanıcılar	Aynı cihaz veya sistemin kullanılması ile veri sızıntısı	Öneri sistemi çıktısından çıkarım yapmak
Dış Varlıklar	Kanuna aykırı veri açıklaması Bilgisayar korsanlığı Anonim verinin yeniden kimliklendirilmesi	Hassas verinin açıklanması

[24] Jameson, Anthony, Martijn C. Willemsen, Alexander Felfernig, Marco De Gemmis, Pasquale Lops, Giovanni Semeraro, and Li Chen. "Human decision making and recommender systems." *Recommender systems handbook* (2015): 611-648

Aşağıdaki bölümlerde farklı kaynaklardan oluşabilecek bu riskler tartışılmıştır.

1. Öneri Sistemi Kaynaklı Riskler

Çevrim içi platformlar kullanıcılarından veriyi kurallarına uygun şekilde toplamış olsalar bile daha sonraki kullanım aşamasında problemler oluşabilir. Bu risklerin oluşma sebepleri aşağıdaki başlıklarda toplanabilir:

a. Veriye Doğrudan Erişim

Öneri sistemleri genel olarak merkezi bir platform ya da tek bir şirket tarafından yönetilir. Fakat bu şirketler zamanla diğer şirketlerle olan bağlarını güçlendirmek ya da başka şirketlerden alacakları hizmete ihtiyaç duyacakları için diğer şirketlerle iş birliği yaparlar. Bunun için de öneri sistemi için kullanılacak olan kişisel verileri diğer şirketlerle paylaşırlar. Fakat bu durum bazı ihlallere sebep olabilir.

b. Yetkisiz Veri Depolama

Veri depolama maliyetleri ucuzladıkça, şirketler genellikle kullanıcı verilerini mümkün olduğunca geniş ölçüde toplamaya eğilimlidir, bunu potansiyel gelecekteki fayda için ya da bu verilerin ticarileştirilmesi amacıyla yaparlar. Ancak, herhangi bir hizmet sunulmadan gerekli olmayan verilerin toplanması, 6698 sayılı Kanun'un 4. maddesindeki genel ilkelerde yer alan *"işlendikleri amaçla bağlantılı,sınırlı ve ölçülü olma"* ilkesine aykırılık teşkil edebilir.

Bunun yanında, veri sorumluları tarafından uyulması gereken ilkelerden bir diğeri de kişisel verilerin ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar saklanmasıdır. İşlenen kişisel veriler istenildiği kadar saklanamamaktadır. Veri sorumlularının, 6698 sayılı Kanun'un 16'ncı maddesinin 3'üncü fıkrası uyarınca Veri Sorumlusu Sicili'ne kayıt başvuruları sırasında kişisel veri saklama ve imha politikası hazırlamaları ve kişisel verilerin işlendikleri amaç için gerekli olan azami süreyi belirtmeleri gerekmektedir. Kişisel veriler hukuka uygun olarak işlenmiş olsa bile, işlenmesini gerektiren sebepler ortadan kalktığı durumda bu verilerin, resen veya ilgili kişinin talebi üzerine silinmesi, yok edilmesi veya anonim hale getirilmesi gerekmektedir. Ticari İletişim ve Ticari Elekt-

ronik İletiler Hakkında Yönetmelik uyarınca, elektronik ticaret sitelerinde kullanıcıların onay vermesinin ardından elde edilen kişisel verilerin onayın geçerliliğinin sona erdiği tarihten itibaren bir yıl, ticari elektronik iletilere ilişkin kayıtlar aracılığıyla elde edilen kişisel veriler ise kayıt tarihinden itibaren bir yıl süreyle saklanmalıdır.

c. Diğer (Üçüncü Taraf) Şirketlerle Veri Paylaşımı

Öneri sistemleri, kullanıcı verilerini üçüncü taraflarla çeşitli şekillerde paylaşabilmektedir:

- Şirketler ellerindeki verileri araştırma amacıyla verileri anonim hale getirerek açık kaynak haline dönüştürebilirler. Ya da öneri sistemlerini geliştirmek amacıyla Netflix[25] örneğinde olduğu gibi araştırmacılarla paylaşabilirler.
- Şirketler, gerekli olan işlerini yaptırmak için üçüncü taraf başka şirketlere ihtiyaç duyabilirler. Fakat bu durum kişisel verileri ihlal edebilir, nitekim Meta'ya kullanıcıların birbirleriyle olan direkt mesajlarını daha iyi bir kullanıcı deneyimi sunmak için yaklaşık 10 yıla yakın bir süredir Netflix'e verdiğinden dolayı dava açılmıştır[26]. Ayrıca yine Meta şirketi, Cambridge Analytica adlı şirket ile ilgili bir güvenlik ihlali davasını sona erdirmek için 725 milyon dolar ödemeyi kabul etmiştir.
- Şirketler kâr etmek amacıyla ellerinden bulunan verileri satabilirler ya da veriler şirketlerin başka şirketler tarafından satın alınması veya iflas etmesi sonucunda el değiştirebilir.

d. Çalışanlar Tarafından Yetkisiz Erişim

Şirketler, kullanıcı verilerini korumak için önlemler alabilir, ancak görevlerini yerine getirmek için kullanıcı verilerine erişime ihtiyaç duyan şirket çalışanları bu verileri (1) kötüye kullanmak için, (2) satmak için ya da (3) ünlü kişilerin verilerini meraktan çalabilirler. Bu risk, kullanıcı bilgilerini saklayan herhangi bir sistemde mevcuttur, fakat uygun erişim kontrolü ve denetim mekanizmalarının sağlanmasıyla kısmen hafifletilebilir.

---

25 Koren, s. 1-10

26 Facebook (2024), *Facebook let Netflix see user DMs to help them tailor content as part of a close collaboration between the two tech giants, new court documents claims* (*https://www.dailymail.co.uk/news/article-13262517/facebook-netflix-user-dms- tailor-content.html, E.T.: 22.11.2024), s.1*

e. Kullanıcı Tercih Verilerinden Çıkarım

Öneri sistemleri makine öğrenmesi ve yapay zekâ yöntemlerini kullanarak toplanan ham veriyi analiz eder, örüntüler çıkarır ve buna göre öneriler üretir. Verinin işlenmesi aşamasında kullanıcı farkında olmadan ve rızası alınmadan yeni veriler ortaya çıkabilir. Özellikle cinsiyet, yaş gibi özellikler yapılacak öneriler için önemli bilgiler taşıyabileceğinden yapılan analizlerde bu bilgilerin ortaya çıkması olasıdır. Bu durumda aşağıdaki riskler oluşabilir[27]:

- Hassas bilgilerin açığa çıkması: Yapılan çalışmalar toplanan veriler üzerinde uygulanan makine öğrenmesi ve yapay zekâ yöntemlerinin hassas bilgilerin ortaya çıkmasına sebep olabildiğini göstermiştir[28][29][30].
- Hedeflenmiş Reklamcılık: Öneri sistemlerinin amacının kullanıcının ilgi alanını belirleyip ona uygun öneriler üretmek olduğu düşünülürse bu sistemler kullanıcılar internet ortamında gezinirken kullanıcıya uygun reklam içeriklerinin belirlenmesi için de kullanılmaktadır. Bazı çalışmalarda bu gibi durumların hassas veya kullanıcı tarafından istenmeyen bilgileri ortaya çıkardığı gösterilmiştir[31].
- Ayrımcılık: Dinamik fiyatlandırma uygulayan bazı sistemlerde toplanan kişisel verilerden yapay zekâ yöntemleriyle elde edilen bilgilere göre aynı ürünler için farklı kişilere farklı fiyatlar sunularak bu bilgilerin kötüye kullanılabileceği gösterilmiştir[32][33].

---

27 Jameson, Anthony, Martijn C. Willemsen, Alexander Felfernig, Marco De Gemmis, Pasquale Lops, Giovanni Semeraro, and Li Chen. "Human decision making and recommender systems." *Recommender systems handbook* (2015): 611-648

28 Chaabane, Abdelberi, Gergely Acs, and Mohamed Ali Kaafar. "You are what you like! information leakage through users' interests." In *Proceedings of the 19th annual network & distributed system security symposium (NDSS)*. Citeseer, 2012

29 Kosinski, Michal, David Stillwell, and Thore Graepel. "Private traits and attributes are predictable from digital records of human behavior." *Proceedings of the national academy of sciences* 110, no. 15 (2013): 5802-5805

30 Weinsberg, Udi, Smriti Bhagat, Stratis Ioannidis, and Nina Taft. "BlurMe: Inferring and obfuscating user gender based on ratings." In *Proceedings of the sixth ACM conference on Recommender systems*, pp. 195-202. 2012

31 Duhigg, Charles. "How companies learn your secrets." In *The Best Business Writing 2013*, pp. 421-444. Columbia University Press, 2013

32 Mikians, Jakub, László Gyarmati, Vijay Erramilli, and Nikolaos Laoutaris. "Detecting price and search discrimination on the internet." In *Proceedings of the 11th ACM workshop on hot topics in networks*, pp. 79-84. 2012

Sosyal ağlardan elde edilen kullanıcı verilerinin yapay zekâ yöntemleri ile kontrolsüz bir biçimde analiz edilmesi ve bu bilgilerin kullanılması daha kötü sonuçlara sebep olabilir. Örneğin yapılan bir çalışmada, kullanıcıların sosyal ağlarda beğendikleri içeriklere göre cinsel tercihlerinin tahmin edilebileceği gösterilmiştir[34]. Yine başka bir çalışmada kullanıcılar gruplanarak, gruplar içindeki ilişki içinde olan kullanıcıların belirlenebileceği gösterilmiştir[35]. Kullanıcılar bu tür platformlara üye olurken kendileri hakkında kısıtlı oranda veri girseler bile, bazı özellikleri kullanıcıların bulundukları gruplara veya platform içindeki davranışlarına bakılarak yapay zekâ modelleri ile tahmin edilebilir. Bu da yukarıda verilen örneklerde olduğu gibi hassas bilgilerin ortaya çıkmasına sebep olur.

2. Öneri Sistemini Kullanan Diğer Kullanıcılar Tarafından Oluşturulan Riskler

Kişiselleştirilmiş öneri sistemlerinde özellikle kişilerin bazı özellikleri belirlenerek o kişilere uygun öneriler yapılması amaçlanır. Bu durum ise aynı cihazı kullanan bazı kullanıcıların birbirleriyle paylaşmak istemedikleri verilerinin ortaya çıkmasına sebep olur. Örneğin, eşine hediye almak isteyen bir kullanıcı onu eşinden gizlemek isteyebilir. Bu tür durumlar için sıkça verilen örneklerden biri 2012 yılında Amerika'daki Target adlı mağaza zincirinin yaşadığı problemdir. Target, kadın kullanıcılarından hamile olanları belirleyerek, bu kullanıcılara özel ürünler önermek amacıyla pazarlama elektronik postaları gönderir ve bu konuda da başarılı öneriler üretir. Ancak 15 yaşındaki bir müşterinin babası, kızının hamile olduğunu bu elektronik postaları görüp, şirketi "çocukları hamile kalmaya teşvik etmek"le suçlaması ardından öğrenir[36]. Bu durum o zaman birçok başka kadın müşteriyi de paylaşmadıkları bir bilginin şirket tarafından izinsiz kullanılması nedeniyle rahatsız etmiştir. Bu tür risklerin oluşmaması için 6698 sayılı Kanun'da belirlenen ilkeler ile uyumlu olacak şekilde mahre-

---

33 Laoutaris, Nikolaos. "Crowd-assisted Search for Price Discrimination in E-Commerce: First results." In *Proceedings of the Ninth ACM Conference on Emerging Networking Experiments and Technologies*, vol. 16. 2013

34 Kosinki/Stillwell/Graepel, s.5802-5805

35 Zheleva, Elena, and Lise Getoor. "To join or not to join: the illusion of privacy in social networks with mixed public and private user profiles." In *Proceedings of the 18th international conference on World wide web*, pp. 531-540. 2009

36 Nytimes (2024), How Companies Learn Your Secrets **(**https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html, E.T. 22.11.2024), s.1

miyeti koruyan kişiselleştirilmiş öneri sistemi politikaları geliştirmek gereklidir.

3. Öneri Sistemi Kullanıcısı Olmayan Dış Varlıklar Tarafından Oluşturulan Riskler

Kullanıcı verilerini toplayan platformlar bu verilerin kötüye kullanımı ve erişimi için çeşitli kontrol mekanizmaları geliştirebilirler. Ama alınan önlemlere rağmen, ya da bazen alınan önlemlerin yetersizliği ve güvenlik açıkları nedeniyle bu verilere yasa dışı olarak erişilebilir. Hatta bazı durumlarda hizmet sağlayıcı platform bunun farkında bile olmayabilir. Bir diğer ortaya çıkabilecek risk ise anonimleştirilerek paylaşılan kişisel verilerin yeniden tanımlama yöntemleri ile veriye erişim izni olmayan kişiler tarafından kullanılmasıdır. Yapılan bir çalışma, 500.000 Netflix abonesinin puanlarını anonim şekilde paylaşan Netflix Ödülü veri kümesinde 8 farklı film puanlandırması ve bu puanlamaların tarihleri gibi veri kümesindeki bazı verilerin %99'unun benzersiz bir şekilde tanımlanabileceğini bulmuşlardır[37].

D. ÖNERİ SİSTEMLERİNİN 6698 SAYILI KANUN DÜZENLEMELERİNE UYARLANMASI

Kullanıcı verileri öneri sistemleri için vazgeçilmezdir. Kişiselleştirilmiş ya da kişiye özgü öneriler yapmak bu veriler olmadan neredeyse imkânsızdır. Örneğin, kullanıcının konum bilgisi, kaç yaşında olduğu ya da hangi ürünleri hangi ürünler ile beraber aldığı gibi bilgiler olmadan o kullanıcıya kişisel öneri yapılması zordur.

Fakat kullanıcılar hizmet aldıkları web siteleri ile verilerini paylaşırken bu verilerle kimliklerinin ortaya çıkmasını gizlilik ihlalinden dolayı istemezler. Kullanıcılar bu verileri öneri sistemleri sağlayan platformlar ile paylaşsalar dahi, her kullanıcı doğal olarak kendine ait olan veri üzerinde kontrol sahibi olmak ister ve bu hakka sahiptir. Örneğin kullanıcı, verisinin silinmesini ya da değiştirilmesini talep edebilir. Bu yüzden diğer ülkelerdeki düzenlemelerde olduğu gibi Türkiye'de de 6698 sayılı Kanun, temelde kişisel verilerin paylaşılmasına ve işlenmesine belirli ilke ve şartlar altında izin verir.

---

[37] Narayanan, Arvind, and Vitaly Shmatikov. "Robust de-anonymization of large sparse datasets." In *2008 IEEE Symposium on Security and Privacy (sp 2008)*, pp. 111-125. IEEE, 2008

Veri işleyenler, 6698 sayılı Kanun çerçevesinde veri sorumlusunun talimatları doğrultusunda aşağıdaki hususları yerine getirebilmektedir:

- Kullanıcılara çevrim içi etkinliklerini izleyen çerezleri reddetme olanağı sağlama
- Kullanıcıların talep etmesi halinde (veri sorumlusu aracılığıyla) sakladığı ve işlediği kişisel verilere erişim sağlama
- Kullanıcının isteği üzerine (yine veri sorumlusu aracılığıyla) kullanıcının verilerini silme

Aydınlatma metinlerinin ise açık ve anlaşılır bir dille yazılması ve aşağıdaki bilgileri içermesi beklenir:

- Çerezlerin Kullanım Amaçları: Çerezlerin hangi amaçlarla kullanıldığını açıklar. Örneğin, oturum yönetimi, kullanıcı tercihlerini hatırlama, reklam ve pazarlama, analitik ve performans izleme gibi amaçlar belirtilebilir.
- Çerez Türleri: Hangi tür çerezlerin kullanıldığını açıklar.
- Veri Toplama ve İşleme: Çerezler aracılığıyla hangi tür verilerin toplandığını ve nasıl işlendiğini açıklar.
- Kontrol ve Tercihler: Kullanıcılara, çerezlerin kullanımıyla ilgili tercihlerini belirleme veya reddetme imkânı sunulur. Kullanıcıların tarayıcı ayarlarını değiştirerek çerezleri nasıl kontrol edebileceklerini ve yönetebileceklerini açıklar.
- Gizlilik Politikası Bağlantısı: Kullanıcılara daha fazla bilgi edinmeleri veya çerezlerle ilgili ayrıntılı bilgilere erişebilmeleri için web sitesinin veya hizmetin gizlilik politikasına bir bağlantı sunulur.

6698 sayılı Kanun'un yürürlüğe girmesiyle birlikte internet siteleri kullanıcılara çerez kullanımı hakkında bilgi veren aydınlatma metinlerini sunmakla yükümlü hale geldiler[38]. 6698 sayılı Kanun'un 3. maddesi, kişisel verilerin işlenmesine ilişkin açık rıza kavramını düzenlemekte ve bu kapsamda kullanıcıların bilgilendirilmesi gerekliliğini vurgulamaktadır. Kişi-

[38] Kişisel Verileri Koruma Kurumu: *"Çerez Uygulamaları Hakkındaki Rehber"*, (https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/fb193dbb-b159-4221-8a7b-3addc083d33f.pdf E.T.:22.11.2024), s.8-18.

selleştirilmiş öneri sistemlerinde tekil kullanıcıları belirlemek ve kullanıcıların bir oturumdaki hareketlerini takip etmek amacıyla açık rıza verilen çerez türlerinin kullanılmasına ihtiyaç vardır. Fakat öneri sistemleri çerezleri ve kişisel verilerin işlenmesini reddeden kullanıcılara da alternatif olarak aşağıdaki gibi önerileri sunabilir. Bu öneriler için kullanıcıların kişisel bilgilerine ihtiyaç duyulmaz.

- Kullanıcılar için revaçta olan ürünler önerilebilir. Bu ürünler son zamanlarda en çok satın alınan ürünler olabileceği gibi satılmak ya da gösterilmek istenilen ürünler de olabilir.
- Kullanıcının satın aldığı ya da hizmet aldığı üründen sonra, ürünler arasındaki (item-item) benzerlikler bulunarak, "Diğer kullanıcılar bunları da aldı/gördü" ya da "Bunlara da ihtiyacınız olabilir" şeklinde öneri sunabilirler. Bu durumda, içerik bazlı filtreleme yöntemleri ile kullanıcılar kişisel verilerinin kullanımlarına izin vermeseler dahi öneri sunulabilir.
- Diğer yöntemde ise kullanıcılara ne istedikleri sorularak o isteklere ait ürünler önerilir. Kullanıcılar isteklerini filtreleyerek istedikleri ürünlerin önerilmesini sağlayabilirler. Bu doğrudan arama olarak da yapılmakla birlikte arama sonucu bir öneri sisteminden geçirilerek öneri olarak da yapılabilir.

SONUÇ

Gelişen yapay zekâ teknolojileri ile birlikte kullanıcılara ait olan veriler bu teknolojiler için adeta yakıt görevi görmektedirler. Özellikle öneri sistemleri kullanıcılara daha iyi ve kişiselleştirilmiş öneriler sunmak için kullanıcılara ait verilere ihtiyaç duyarlar. Bu kapsamda 6698 sayılı Kanun'un düzenlemeleri ile birlikte kullanıcı verileri koruma altına alınmaktadır. Öneri modellerinin 6698 sayılı Kanun'da düzenlenen ilkeler ile uyumlu olması, veri odaklı öneri sistemlerinde etik ve yasal uyumun sağlanmasında temel öneme sahiptir. Bu çalışmada öncelikle öneri sistemlerinde kullanılan yöntemler anlatılarak bu yöntemler için gerekli olan kullanıcı verilerinin kullanılmasındaki ve erişilmesindeki riskler tartışılmış olup daha sonra da bu verilerin 6698 sayılı Kanun'un gereksinimleri ile olan uyumu ele alınmıştır.

Öneri sistemlerinin 6698 sayılı Kanun ile uyumlu hale getirilmesi, kişisel verilerin adil ve yasal bir şekilde işlenmesini sağlar. Bu, hukuka uygunluk, dürüstlük, ölçülülük, hesap verebilirlik, şeffaflık, kişisel verilerin doğru ve güncel olması, kişisel veri kullanım amacının belirli ve sınırlı olması ilkele-

ri ile veri güvenliği yaklaşımı gibi 6698 sayılı Kanun'un öngördüğü temel ilkelerle uyum içinde çalışmayı gerektirir. Bu yaklaşımlarla uyumlu öneri sistemleri, kullanıcı güvenini arttırmanın yanı sıra gizlilik ihlalleri ve yasal sorumlulukları önlemeye yardımcı olabilir. Kullanıcıların haklarını ve gizliliklerini koruyacak etkili politikalar oluşturularak öneri sistemlerinin 6698 sayılı Kanun ile uyumlu hale getirilmesi sadece kullanıcı güvenini ve memnuniyetini arttırmakla kalmaz, aynı zamanda gizlilik ihlalleri ve bu ihlallerden dolayı oluşabilecek cezaların riskini azaltır.

Sonuç olarak, 6698 sayılı Kanun ile uyumlu öneri modelleri, ilgili kişilerin haklarını koruyarak, güvenilir ve sürdürülebilir bir dijital ortamın oluşturulmasına katkıda bulunabilir. Bunun için tüm paydaşların iş birliği içinde çalışması kaçınılmazdır. 6698 sayılı Kanun ile uyumlu öneri sistemlerinin geliştirilmesi ve benimsenmesi, hem bireylerin gizliliğini korumak hem de kurumların yasal gereksinimlere uygunluğunu sağlamak için önemli bir adımdır.

KAYNAKÇA

ANTHONY, Jameson, WİLLEMSEN, Martijn C., FELFERNİG, Alexander, DE GEMMİS, Marco, LOPS, Pasquale, SEMERARO, Giovanni ve CHEN, Li. "*Human decision making and recommender systems*." Recommender systems handbook (2015): 611-648.

AWAD, Naveen Farag ve MAYURAM S. Krishnan. "*The personalization privacy paradox: an empirical evaluation of information transparency and the willingness to be profiled online for personalization.*" MIS quarterly (2006): 13-28.

BADRUL, Sarwar, KARYPİS, George, KONSTAN, Joseph ve John RİEDL. "*Item-based collaborative filtering recommendation algorithms*." In Proceedings of the 10th international conference on World Wide Web, pp. 285-295. 2001.

BURKE, Robin. "*Hybrid recommender systems: Survey and experiments*." User modeling and user-adapted interaction 12 (2002): 331-370.

CASTROUNİS, Alex. AI for people and business: *"A framework for better human experiences and business success."* O'Reilly Media, 2019.

CHAABANE, Abdelberi, ACS, Gergely ve KAAFAR, Mohamed Ali. "*You are what you like! information leakage through users' interests*." Proceedings of the 19th annual network & distributed system security symposium (NDSS). Citeseer, 2012.

CHELLAPPA, Ramnath K. ve RAYMOND G. Sin. "*Personalization versus privacy: An empirical examination of the online consumer's dilemma*." Information technology and management 6 (2005): 181-202.

CRANOR, Lorrie Faith. "'*I didn't buy it for myself: privacy and ecommerce personalization.*" Proceedings of the 2003 ACM Workshop on Privacy in the Electronic Society. 2003.

DUHİGG, Charles. "*How companies learn your secrets.*" The Best Business Writing 2013. Columbia University Press, 2013. 421-444.

ERAN, Toch, WANG, Yang ve CRANOR, Lorrie Faith. "*Personalization and privacy: a survey of privacy risks and remedies in personalization-based systems*." User Modeling and User-Adapted Interaction 22 (2012): 203-220.

Facebook (2024), Facebook let Netflix see user DMs to help them tailor content as part of a close collaboration between the two tech giants, new court documents claims (https://www.dailymail.co.uk/news/article-13262517/facebook-netflix-user-dms- tailor-content.html, E.T.: 22.11.2024)

GEDİMİNAS, Adomavicius ve TUZHİLİN, Alexander. "*Toward the next generation of recommender systems: A survey of the state-of-the-art and possible extensions.*" IEEE transactions on knowledge and data engineering 17.6 (2005): 734-749.

JAVED, Umair, SHAUKAT, Kamran, HAMEED, Ibrahim A. IQBAL, Farhat, ALAM, Talha Mahboob, ve LUO, Suhuai. "*A review of content-based and context-based recommendation systems*." International Journal of Emerging Technologies in Learning (iJET) 16, no. 3 (2021): 274-306.

KİRAN, R., KUMAR, Pradeep ve BHASKER, Bharat. "*DNNRec: A novel deep learning based hybrid recommender system*." Expert Systems with Applications 144 (2020): 113054.

Kişisel Verileri Koruma Kurumu: "Çerez Uygulamaları Hakkındaki Rehber", (https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/fb193dbb-b159-4221-8a7b-3addc083d33f.pdf E.T.:22.11.2024)

Kişisel Verileri Koruma Kurumu: Veri Sorumlusu ve Veri İşleyen, (https://www.kvkk.gov.tr/Icerik/4195/Veri-Sorumlusu-ve-Veri-Isleyen E.T.: 22.11.2024)

KOBSA, Alfred. "*Privacy-enhanced web personalization*." The adaptive web: Methods and strategies of web personalization. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007. 628-670.

KOREN, Yehuda. "*The bellkor solution to the netflix grand prize*." Netflix prize documentation 81.2009 (2009): 1-10.

KOREN, Yehuda, BELL, Robert ve VOLİNSKY, Chris. "*Matrix factorization techniques for recommender systems*." Computer 42.8 (2009): 30-37.

KOSİNSKİ, Michal, STİLLWELL, David ve GRAEPEL, Thore. "*Private traits and attributes are predictable from digital records of human behavior.*" Proceedings of the national academy of sciences 110.15 (2013): 5802-5805.

LAOUTARİS, Nikolaos. "*Crowd-assisted Search for Price Discrimination in E-Commerce: First results.*" In Proceedings of the Ninth ACM Conference on Emerging Networking Experiments and Technologies, vol. 16. 2013.

LEE, Daniel ve SEUNG, H. Sebastian. "*Algorithms for non-negative matrix factorization.*" Advances in neural information processing systems 13 (2000).

LOPS, Pasquale, DE GEMMİS, Marco ve SEMERARO, Giovanni. "*Content-based recommender systems: State of the art and trends*." Recommender systems handbook (2011): 73-105.

MİKİANS, Jakub, GYARMATİ, László, ERRAMİLLİ, Vijay ve LAOUTARİS, Nikolaos. "*Detecting price and search discrimination on the internet*." In Proceedings of the 11th ACM workshop on hot topics in networks, pp. 79-84. 2012.

MNİH, Andriy ve SALAKHUTDİNOV, Russ R. "*Probabilistic matrix factorization.*" Advances in neural information processing systems 20 (2007).

MOONEY, Raymond J. ve ROY, Loriene. "*Content-based book recommending using learning for text categorization*." Proceedings of the fifth ACM conference on Digital libraries. 2000.

NARAYANAN, Arvind ve SHMATİKOV, Vitaly. "*Robust de-anonymization of large sparse datasets.*" 2008 IEEE Symposium on Security and Privacy (sp 2008). IEEE, 2008

Nytimes (2024), How Companies Learn Your Secrets (https://www. nytimes.com/2012/02/19/magazine/shopping-habits.html, E.T. 22.11.2024)

PAZZANİ, Michael J. ve BİLLSUS, Daniel. "*Content-based recommendation systems.*" The adaptive web: methods and strategies of web personalization. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007. 325-341

SCHAFER, J. Ben, FRANKOWSKİ, Dan, HERLOCKER, Jon ve SEN, Shilad. "*Collaborative filtering recommender systems.*" In The adaptive web: methods and strategies of web personalization, pp. 291-324. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007.

STEPHAN, Jones S. ve GROOM, Frank M. eds. "*Artificial intelligence and machine learning for business for non-engineers."* CRC Press, 2019.

VAN DEN OORD, Aaron, DİELEMAN, Sander ve SCHRAUWEN, Benjamin. "*Deep content-based music recommendation.*" Advances in neural information processing systems 26 (2013).

WEİNSBERG, Udi, BHAGAT, Smriti, IOANNİDİS, Stratis ve TAFT, Nina. "*BlurMe: Inferring and obfuscating user gender based on ratings*." In Proceedings of the sixth ACM conference on Recommender systems, pp. 195-202. 2012.

ZHELEVA, Elena ve GETOOR, Lise. "*To join or not to join: the illusion of privacy in social networks with mixed public and private user profiles*." In Proceedings of the 18th international conference on World wide web, pp. 531-540. 2009.

ULAŞIM SEKTÖRÜNDE YAPAY ZEKÂ

Doç. Dr. Nazım Kemal ÜRE*

GİRİŞ

Yapay zekâ (YZ) alanındaki son yıllardaki hızlı gelişmeler, her sektörde olduğu gibi ulaşım sektörünü de derinden etkilemiştir. Sürücüsüz araçlardan karmaşık trafik yönetimine kadar birçok alana büyük yenilikler getiren YZ teknolojileri, gün geçtikçe nasıl seyahat ettiğimizi daha da büyük oranda değiştirecektir. Bu bölümün amacı, YZ'nin ulaşım sektöründeki uygulamaları üzerine bilgi vermek ve ardından bu uygulamaları kişisel verilerin korunması, hukuk ve etik gibi açılardan incelemektedir.

Ulaşımda YZ uygulamalarının temel amacı güvenliği, verimi ve konforu arttırmaktır. Bu alanda YZ büyük veri teknolojilerini, algılama ağlarını ve makine öğrenmesi algoritmalarını kullanarak akıllı ulaşım uygulamaları inşa etmeyi hedefler. Bu uygulamalar sadece günlük ulaşımı iyileştirmekte kalmaz, ayrıca kentsel planlama ve altyapı geliştirmelerini de yeniden şekillendir. Örneğin, Goodall (2014)[1] tarafından yapılan bir çalışma, YZ tabanlı trafik sistemlerinin gerçek zamanlı verilere dayalı olarak trafik ışığı düzenlerini dinamik olarak ayarlayarak trafik yoğunluğunu azaltabileceğini göstermiştir.

Otonom araçlar alanında YZ hayati bir role sahiptir. Sürücüsüz arabalar, kamera, lidar, radar ve GPS gibi algılayıcılardan gelen verileri derin yapay sinir ağları kullanarak işler ve bu şekilde edindikleri durumsal farkındalık sayesinde güvenli sürüş manevralarını hesaplarlar. Ulusal Karayolu Trafik Güvenliği İdaresi (NHTSA) tarafından 2020[2] yılında yayınlanan bir rapor,

* İstanbul Teknik Üniversitesi, Yapay Zekâ ve Veri Müh. Bölümü Öğretim Üyesi.

1 Goodall, N. J. (2014). Machine ethics and automated vehicles. In Road Vehicle Automation (pp. 93-102). Springer.

2 National Highway Traffic Safety Administration. (2020). Critical Reasons for Crashes Investigated in the National Motor Vehicle Crash Causation Survey. Washington, DC.

ciddi kazaların %94'ünün insan hatasından kaynaklandığını ve YZ sistemlerinin bunu ortadan kaldırmayı amaçladığını vurgulamaktadır. Waymo ve Tesla gibi şirketler, bu teknolojinin ön saflarında yer almakta ve otonom sürüş yeteneklerini sürekli olarak test edip geliştirmektedir.

YZ trafik yönetiminde de önemli bir rol oynamaktadır. Geleneksel trafik sistemleri, gerçek zamanlı koşullara uyum sağlamakta genellikle başarısız olur ve bu da verimsizliklere ve artan seyahat sürelerine yol açar. Ancak YZ tabanlı sistemler, gerçek zamanlı trafik verilerini analiz edebilir ve hangi koşullar altında trafik sıkışıklığı olacağını tahmin edebilir. Vlahogianni ve diğerleri (2014)[3] tarafından yapılan araştırmaya göre, YZ algoritmaları, sinyal sürelerini ayarlayarak ve sürücülere rota önerileri sağlayarak trafik akışını optimize edebilir, seyahat süresini ve yakıt tüketimini önemli ölçüde azaltabilir.

YZ ayrıca yol güvenliğini artırmada kritik bir rol oynayabilir. YZ destekli öngörücü analizler, kazalardan önce yüksek riskli bölgeleri ve potansiyel tehlikeleri belirleyebilir. Chen ve diğerleri (2016)[4] tarafından yapılan bir çalışma, YZ'nin, geçmiş kaza verilerini ve gerçek zamanlı trafik koşullarını analiz ederek trafik kazalarını elle tutulur doğrulukla tahmin edebileceğini göstermiştir. Ayrıca, YZ destekli izleme sistemleri, sürücü davranışlarını izleyebilir ve yorgunluk veya dikkat dağınıklığı nedeniyle meydana gelen kazaları önlemek için gerçek zamanlı geri bildirim sağlayabilir.

Bütün bu gelişmelere rağmen YZ'nin ulaşım sistemlerine tam entegrasyonunda hukuk ve etik açısından sorunlar yer almaktadır. Örneğin bu uygulamaların kişisel verileri işleme konusunda ne gibi kısıtlamalara sahip olmaları gerektiği henüz tam oturmamıştır. Otonom araçlarda yaşanacak kaza durumlarında sorumluluğun kimde olacağı da önemli bir endişe kaynağıdır. Benzer şekilde insan hayatının kurtulmasına veya kaybına yol açacak karar verme senaryolarındaki etik ikilemler de süregelen tartışma konuları arasındadır. Lin (2016)[5] tarafından yapılan çalışma, bu konuları

[3] Vlahogianni, E. I., Karlaftis, M. G., & Golias, J. C. (2014). Short-term traffic forecasting: Where we are and where we're going. Transportation Research Part C: Emerging Technologies, 43, 3-19.

[4] Chen, C., Ma, J., Susilo, Y. O., Liu, Y., & Wang, M. (2016). The promises of big data and small data for travel behavior (aka human mobility) analysis. Transportation Research Part C: Emerging Technologies, 68, 285-299.

[5] Lin, P. (2016). Why ethics matters for autonomous cars. Autonomous driving: Technical, legal and social aspects, 69-85.

ele almakta ve ulaşımda YZ'yi yönetmek için sağlam hukuki çerçeveler ve etik yönergelerin gerekliliğini vurgulamaktadır.

Bütün bu zorluklara rağmen, YZ'nin ulaşım sektörüne sağladığı potansiyel faydalar oldukça kritiktir. YZ destekli yenilikler, ulaşım sistemlerimizi daha güvenli, daha verimli ve daha sürdürülebilir hale getirmeyi vadetmektedir. Diğer yandan bu sistemleri geliştirirken teknik, hukuki ve etik zorlukları ele almak önemlidir. Bölümün ilerideki kısımlarında, YZ'nin ulaşım uygulamalarındaki mevcut durum ve gelecek beklentiler hakkında genel bir bakış sunulacak ve en sonda bu uygulamaların hukuki ve etik yönleri ele alınacaktır.

I. OTONOM ARAÇLAR

Otonom araçlar (OA), diğer adıyla sürücüsüz araçlar ulaşımda yapay zekânın (YZ) en heyecan verici uygulamalarından biridir. Bu araçlar, seyahat etmek, trafik sinyallerini yorumlamak ve engellerden kaçınmak için kamera, radar, GPS gibi algılayıcıları ve YZ algoritmalarının birleşik olarak kullanırlar. Bu araçların insanlar tarafından kullanılan taşıtlara oranla daha güvenli, verimli ve konforlu bir ulaşım hedeflemesi, bu alanda önemli yatırımlar ve araştırmalar yapılmasını teşvik etmiştir.

OA alanındaki gelişmeler son yıllarda hızla ilerlemiş olup, birçok şirket kapsamlı testler ve pilot programlar yürütmektedir. YZ destekli OA'lar, çoğunluğu insan hatasından kaynaklanan trafik kazalarını büyük ölçüde azaltma potansiyeline sahiptir. Dünya Sağlık Örgütü'nün (2018)[6] bir raporuna göre, trafik kazalarının yaklaşık %90'ında insan hatası bir faktördür. Bu teknoloji dikkat dağınıklığı veya uyarıcı madde altında sürüş gibi faktörleri ortadan kaldırarak, herkes için daha güvenli yollar yaratma potansiyeline sahiptir.

Bu alandaki önde gelen şirketlerden biri Alphabet Inc.'in bir yan kuruluşu olan Waymo'dur[7]. Waymo'nun sürücüsüz araçları, kamu yollarında milyonlarca kilometre yol kat etmiş olup YZ algoritmalarını sürekli olarak daha fazla veri üzerinden eğitip geliştirmektedir. OA alanında bir diğer önemli oyuncu olan Tesla, araçlarına otopilot ve tam otonom sürüş özelliklerini de içeren gelişmiş YZ özelliklerini entegre etmiştir. Tesla'nın 2024 Güvenlik

6 World Health Organization. (2018). *Global Status Report on Road Safety*. Geneva: WHO.

7 Schwall, M., Daniel, T., Victor, T., Favaro, F., & Hohnhold, H. (2020). Waymo public road safety performance data. arXiv preprint arXiv:2011.00038.

Raporu'na[8] göre, Tesla otopilotu ile donatılmış araçlar, manuel olarak sürülen araçlara kıyasla kilometre başına çok daha az kaza geçirmiştir.

OA teknolojisi, birden fazla bileşeni içeren karmaşık bir yapıdır. Lidar, radar ve kameralar gibi algılayıcılar, aracın çevresinden canlı olarak veri toplar. Lidar, yüksek çözünürlüklü 3 boyutlu haritalar oluşturmak ve nesneleri tespit etmek için lazer ışınlarını kullanırken, radar radyo dalgalarını kullanarak trafik nesnelerini tespit eder ve hızlarını ve mesafelerini ölçer. Kameralar ise nesneleri, trafik işaretlerini ve şerit işaretlerini görsel sinyallerden tanımlar ve takip eder. Bu algılayıcılar, çevreyi yorumlayıp sürüş kararları alan gelişmiş YZ algoritmalarına veri sağlar.

Makine öğrenimi, özellikle geniş ölçekli yapay sinir ağlarının eğitilmesiyle yapılan derin öğrenme, otonom araçların gelişiminde kritik bir rol oynar. Bu algoritmalar, gerçek dünyadaki sürüşler ve simülasyonlar sırasında toplanan büyük miktarda veriden öğrenirler. Kullanılan eğitim verisinin miktarına oranla zamanla gelişerek, çeşitli sürüş senaryolarını tanıma ve bunlara yanıt verme konusunda daha iyi hale gelirler. Örneğin, evrişimsel sinir ağları (*Convolutional Neural Networks*- CNN'ler), yayaları ve diğer araçları tanımlamak gibi görüntü tanıma görevleri için yaygın olarak kullanılan bir yapay sinir ağı tipidir.

Bu gelişmelere rağmen, otonom sürücülerin yaygın olarak benimsenmesi önünde birçok zorluk bulunmaktadır. YZ algoritmalarının farklı ve öngörülemeyen koşullarda güvenilirliğini sağlamak gibi teknik sorunlar önemli bir engel teşkil etmektedir. Yağmur veya kar gibi hava koşulları algılayıcı doğruluğunu etkileyebilir. Ayrıca, karmaşık trafik durumları ve yaya davranışları olan kentsel ortamlar ek zorluklar sunar. Kalra ve Paddock (2016)[9] tarafından yapılan bir çalışmaya göre, otonom araçların gerekli güvenlik seviyesine ulaşması için daha yıllar sürecek geliştirme ve test sürecine ihtiyaç duyulabilir.

Farklı ülkeler, otonom araçların test edilmesi ve kullanıma sunulması konusunda farklı düzenlemelere sahiptir. Amerika Birleşik Devletleri'nde, Ulusal Karayolu Trafik Güvenliği İdaresi (NHTSA) yönergeler yayınlamıştır ancak OA'ları özel olarak düzenleyen federal bir yasa bulunmamaktadır.

---

8 Tesla. (2020). *Vehicle Safety Report*. Tesla Inc. URL: https://www.tesla.com/VehicleSafetyReport

9 Kalra, N., & Paddock, S. M. (2016). Driving to Safety: How Many Miles of Driving Would It Take to Demonstrate Autonomous Vehicle Reliability? *RAND Corporation*.

Bu düzenleyici belirsizlik, sektörün büyümesi için bir engel teşkil etmektedir. Ayrıca, otonom teknolojiye güvenin zamanla inşa edilmesi gerektiğinden, bu teknolojilerin toplum nezdinde kabulü de kritik bir faktördür.

Etik görüşler de otonom sürücülerin geliştirilmesi ve kullanıma sunulmasında önemli bir rol oynamaktadır. "*Trolley* problem" olarak bilinen etik ikilem, otonom bir aracın iki zararlı sonuç arasında seçim yapmak zorunda kaldığı bir durumda nasıl tepki vermesi gerektiğini sorgular. Araştırmacılar ve politika yapıcılar, otonom araçlarda YZ karar verme süreçleri için etik yönergeler oluşturmak amacıyla bu konuları aktif olarak tartışmaktadır. Kapsamlı bir etik çerçeve, kamu güveni ve OA teknolojisinin sorumlu bir şekilde kullanıma sunulması için gereklidir.

Teknik ve etik hususların ötesinde, otonom sürücülerin önemli sosyal ve ekonomik etkileri vardır. OA'ların yaygın olarak benimsenmesi, özellikle kamyon şoförlüğü ve taksi şoförlüğü gibi mesleklerde değişikliklere yol açabilir. Öte yandan, YZ geliştirme, araç bakımı ve trafik yönetimi gibi alanlarda yeni iş fırsatları da yaratabilir. Ekonomik olarak, otonom araçlar ulaşım maliyetlerini azaltabilir, yakıt verimliliğini artırabilir ve büyük otopark alanlarına olan ihtiyacı azaltarak kentlerin yaşam kalitesini iyileştirebilir.

Otonom araçlar, mobilite ve erişilebilirlik açısından da potansiyel faydalar sunar. Yaşlılar veya engelliler gibi araç kullanamayan bireyler için daha fazla bağımsızlık sağlayabilirler. Bu artan mobilite, birçok insanın sağlık hizmetlerine, eğitime ve istihdam fırsatlarına daha fazla erişim sağlamasına yardımcı olabilir. Otonom araçlar, özel araç sahipliğine olan bağımlılığı azaltarak daha sürdürülebilir ulaşım yollarını teşvik eden toplu taşımada da kullanılabilir.

Mobilite ve erişilebilirliği artırmanın yanı sıra, otonom sürücü sistemleri lojistik ve tedarik zincirlerinin verimliliğini de artırabilir. Otonom kamyonlar ve teslimat araçları, malların taşınmasıyla ilgili zaman ve maliyeti azaltarak 7/24 çalışabilir. Amazon ve UPS gibi şirketler, lojistik operasyonlarını düzene sokmak için otonom teslimat araçlarının kullanımına yatırım yapmaktadırlar. McKinsey & Company'nin (2018)[10] bir çalışması, otonom kamyonların yaygın olarak benimsenmesinin işletme maliyetlerini büyük

[10] McKinsey & Company. (2019). Distraction or disruption? Autonomous trucks gain ground in US logistics. URL: https://www.mckinsey.com/industries/travel-logistics-and-infrastructure/our-insights/distraction-or-disruption-autonomous-trucks-gain-ground-in-us-logistics

oranda azaltabileceğini ve önemli ekonomik faydalar sağlayabileceğini öne sürmektedir.

Otonom sürüş sistemlerinin çevresel etkisi de önemli bir husustur. Otonom araçlar, sürüş manevralarını optimize ederek ve yakıt verimliliğini artırarak sera gazı emisyonlarını azaltma potansiyeline sahiptir. Ayrıca, elektrikli araçların otonom teknoloji ile entegrasyonu, ulaşımın karbon ayak izini daha da azaltabilir. Uluslararası Ulaşım Forumu'nun (2017)[11] bir raporuna göre, otonom ve elektrikli araçların yaygın olarak benimsenmesi, 2050 yılına kadar kentsel ulaşımdan kaynaklanan CO2 emisyonlarını büyük oranda azaltabilir.

Otonom sürücü sistemlerine ilişkin kamu algısı ve güveni, başarılı bir şekilde uygulanmaları için kritik öneme sahiptir. Teknoloji birçok fayda vaat etse de güvenlik, gizlilik ve veri güvenliği konularında hala endişeler bulunmaktadır. Otonom araçları içeren yüksek profilli kazalar, bu teknolojileri geliştiren şirketlerin titiz güvenlik standartlarına ve şeffaf iletişime ihtiyaç duyduğunu vurgulamaktadır. Kamu güvenini sağlamak, sürekli eğitim, güvenlik iyileştirmelerinin sağlanması ve teknoloji geliştiricileri, düzenleyicileri ve kamu arasında iş birliği gerektirecektir.

Otonom sürüş teknolojisi konusundaki araştırma ve geliştirme çalışmaları devam etmekte olup, birçok üniversite ve araştırma kurumu bu alandaki ilerlemelere katkıda bulunmaktadır. Akademi ve sanayi arasındaki iş birliği, teknik zorlukların ele alınması ve inovasyonu hızlandırmak için gereklidir. Örneğin, Massachusetts Institute of Technology (MIT), otomotiv şirketleriyle iş birliği yaparak otonom araçlar için gelişmiş algoritmalar ve test çerçeveleri geliştirmektedir. Bu tür ortaklıklar, en son araştırmaların pratik uygulamalara dönüştürülmesinde hayati öneme sahiptir.

Uluslararası iş birlikleri de otonom sürüş sistemlerinin yayılması için kritiktir. Farklı ülkeler, benzersiz trafik düzenlemeleri, yol koşulları ve kentsel düzenlemeler ile otonom araçların konuşlandırılmasına yönelik uyarlanmış yaklaşımlar gerektirmektedir. Birleşmiş Milletler Avrupa Ekonomik Komisyonu (UNECE) gibi örgütler, otonom araçların sınır ötesi çalışmasını kolaylaştırmak için ülkeler arasında düzenlemeler ve standartları uyumlu hale getirmeye çalışmaktadır. Bu uluslararası iş birliği, otonom teknoloji potansiyelinin küresel ölçekte açığa çıkarılması için anahtar olacaktır.

---

[11] International Transport Forum. (2017). *Transport Outlook 2017*. OECD Publishing.

Ayrıca, sigorta endüstrisi de otonom araçların yükselişine uyum sağlamalıdır. Sürücü sorumluluğunu kapsayan geleneksel sigorta modelleri otonom sürüş sistemlerinin olduğu durumlarda yetersiz kalmaktadır. Sigortacılar, yazılım hataları ve siber saldırılar gibi otonom araçlarla ilgili benzersiz riskleri ele alan yeni ürünler geliştirmelidir. KPMG'nin (2015)[12] bir raporu, sigorta endüstrisinin önemli değişiklikler geçireceğini, ürün sorumluluk sigortasına geçiş olacağını ve otonom teknoloji için risk yönetimine odaklanacağını öngörmektedir.

Siber güvenlik, otonom sürücü sistemlerinin diğer kritik bir yönüdür. Otonom araçlar, karmaşık yazılımlara sahiptir ve dış sistemlerle sürekli veri alışverişinde bulunurlar, bu da onları siber saldırılar için potansiyel hedef haline getirir. Bu sistemlerin güvenliğini ve bütünlüğünü sağlamak, yolcuları ve diğer yol kullanıcılarını tehlikeye atacak kötü niyetli faaliyetleri önlemek için çok önemlidir. OA teknolojisi geliştiren şirketler, siber güvenlik önlemlerine yatırımlar yapmalı ve sistemlerini potansiyel tehditlere karşı korumak için uzmanlarla iş birliği yapmalıdırlar.

Otonom araçların mevcut ulaşım altyapısına entegrasyonu da zorluklar sunmaktadır. Kentsel planlama ve altyapı geliştirme, otonom araçların ihtiyaçlarını dikkate almalıdır; bunlar arasında özel şeritler, akıllı trafik sinyalleri ve iletişim ağları yer alır. Singapur ve Helsinki gibi şehirler, otonom araçların güvenli ve verimli çalışmasını sağlamak için uygun ortamlar yaratmak amacıyla akıllı şehir girişimlerini pilot olarak uygulamaktadır. Bu çabalar, otonom araçları ulaşım ağlarına entegre etmek isteyen diğer şehirler için model teşkil edecektir.

Toplu taşıma sistemleri de otonom araç teknolojisinden faydalanabilir. Otonom otobüsler ve servis araçları, özellikle geleneksel toplu taşımanın sınırlı olduğu alanlarda güvenilir ve verimli hizmetler sunabilir. Bu sistemler sabit güzergahlarda çalışabilir veya talebe göre dinamik olarak ayarlanabilir, şehir içi hareketlilik için esnek ve maliyet etkin çözümler sunar. Las Vegas ve Lyon gibi şehirlerdeki pilot programlar, otonom toplu taşımanın hizmet kalitesini artırma ve işletme maliyetlerini azaltma potansiyelini göstermiştir.

Otonom sürücü sistemlerinin güvenliğini artırmada YZ'nin rolü büyük önem taşır. Şerit koruma yardımı, adaptif hız kontrolü ve otomatik acil

[12] KPMG. (2015). The future of insurance in the age of autonomous vehicles.

frenleme gibi gelişmiş sürücü destek sistemleri (ADAS), tamamen otonom araçların öncüleri arasındadır. Bu sistemler, gerçek zamanlı verileri analiz ederek çarpışmaları önlemek ve güvenli sürüş uygulamalarını sürdürmek için sürücülere yardımcı olur. ADAS teknolojisi geliştikçe, daha sofistike otonom sürüş yeteneklerinin yolunu açacaktır.

Otonom teknoloji, kırsal ve yeterince hizmet almayan bölgeler için de önemli sonuçlar doğurur. Otonom araçlar, toplu taşımanın sınırlı veya hiç olmadığı bölgelerde önemli ulaşım hizmetleri sunabilir. Bu, sağlık hizmetlerine, eğitime ve istihdam fırsatlarına erişimi artırarak ekonomik kalkınma ve sosyal katılıma katkıda bulunabilir. Ayrıca, otonom tarım araçları ve makineleri, çiftçilik operasyonlarında verimliliği ve üretkenliği artırarak iş gücü eksikliklerini giderip gıda üretimini artırabilir.

Otonom araç endüstrisi için iş gücünü hazırlamak amacıyla eğitim girişimleri gereklidir. YZ, robotik ve otomotiv mühendisliği alanlarında yetenekli profesyonellere olan talep arttıkça, üniversiteler ve meslek okulları ilgili programlar ve eğitimler sunmalıdır. Eğitim kurumları ile sektör liderleri arasındaki ortaklıklar, öğrencilerin pratik deneyim kazanması ve otonom sürücü teknolojisinde inovasyonu yönlendirecek uzmanlığı geliştirmesi için yollar oluşturabilir.

OA teknolojisi ilerledikçe, gizlilik üzerindeki etkisini de göz önünde bulundurulmalıdır. Otonom araçlar, çevreleri hakkında diğer araçlar, yayalar ve altyapı hakkında büyük miktarda veri toplar. Bu veriler, güvenliği ve verimliliği artırmak için değerli olabilir, ancak aynı zamanda gözetim ve veri gizliliği konularında endişeler doğurur. Veri toplamanın faydalarını bireylerin gizlilik hakları ile dengelemek için açık düzenlemeler ve sağlam veri koruma önlemleri gereklidir.

Tüketici eğitimi ve farkındalık kampanyaları, otonom sürücü sistemlerinin benimsenmesinde hayati bir rol oynayacaktır. Birçok insan, otonom araçların yetenekleri ve sınırlamaları konusunda hala bilgi sahibi değildir, bu da yanlış anlamalara ve şüphelere yol açmaktadır. Otonom teknolojinin faydalarını, güvenlik özelliklerini ve gerçek dünya uygulamalarını vurgulayan bilgilendirici kampanyalar, kamu güvenini artırabilir ve otonom araçların kabulünü teşvik edebilir.

Sonuç olarak, otonom sürücü sistemleri ulaşımın geleceği için büyük vaatler sunmaktadır. YZ'den yararlanarak, bu sistemler yol güvenliğini artırabilir, trafik sıkışıklıklarını azaltabilir ve sürüş yapamayan bireylere daha

fazla ulaşım imkânı sağlayabilir. Ancak, bu devrim niteliğindeki teknolojiyi beraberinde getiren teknik, yasal ve etik zorlukların ele alınması için önemli çalışmalar yapılmalıdır. Endüstri liderleri, araştırmacılar ve politika yapıcılar arasındaki sürekli iş birliği, otonom araçların tam potansiyelini gerçekleştirmede temel olacaktır. Teknoloji geliştikçe, yeniliği dikkatle dengelemek, otonom sürücü sistemlerinin herkesin yararına olacak şekilde sorumlu bir şekilde geliştirilip kullanıma sunulmasını sağlamak önemlidir.

II. TRAFİK YÖNETİMİ

Trafik yönetimi, modern kentsel planlamanın önemi bir unsurudur ve araçlar ile yayaların akışını optimize etmeyi, trafik yoğunluğunu azaltmayı, güvenliği ve genel ulaşım verimliliğini artırmayı hedefler. YZ'nin trafik yönetim sistemlerine entegrasyonu, şehirlerin bu zorluklarla başa çıkma yöntemlerini olumlu etki etmiştir.

YZ destekli trafik yönetim sistemleri, kapsamlı trafik verilerini toplamak için algılayıcılar ve bağlantılı araçlar gibi çeşitli teknolojilerden yararlanır. Bu veriler, trafik durumunu tahmin etmek, darboğazları belirlemek ve en uygun trafik sinyali zamanlamalarını önermek için makine öğrenimi algoritmaları kullanılarak işlenir. Zhang ve diğerlerinin (2017)[13] çalışması, YZ tabanlı trafik sinyal kontrol sistemlerinin trafik sıkışıklığını ciddi oranda azaltabileceğini göstermiştir.

YZ'nin trafik yönetiminde önemli bir örneği, adaptif trafik sinyal kontrol sistemlerinin uygulanmasıdır. Bu sistemler, gerçek zamanlı trafik koşullarına dayalı olarak trafik sinyallerinin zamanlamasını dinamik olarak ayarlar. Zeng ve diğerlerinin (2018)[14] bir çalışmasına göre, uyarlanabilir sinyal kontrolü, ortalama seyahat süreleri ve gecikmelerde önemli bir azalmaya yol açabilir.

Tahmine dayalı analizler, YZ destekli trafik yönetiminde hayati bir rol oynar. Tarihi trafik verilerini ve gerçek zamanlı girdileri analiz ederek, tahmine dayalı modeller trafik sıkışıklığını öngörebilir ve sürücülere alternatif rotalar önerebilir. Bu yaklaşım, trafik sıkışıklıklarını oluşmadan önce hafifletmeye yardımcı olur. Ulusal Taşımacılık ve Topluluklar Enstitüsü (NITC)

---

13 Zhang, L., Khalgui, M., & Li, Z. (2021). Predictive intelligent transportation: Alleviating traffic congestion in the internet of vehicles. *Sensors*, *21*(21), 7330.

14 Zeng, J., Hu, J., & Zhang, Y. (2018, June). Adaptive traffic signal control with deep recurrent Q-learning. In *2018 IEEE intelligent vehicles symposium (IV)* (pp. 1215-1220). IEEE.

tarafından yapılan çalışmalar, tahmine dayalı analizlerin kentsel trafik yönetimindeki etkinliğini vurgulamıştır.

Bağlantılı araç teknolojisi, modern trafik yönetim sistemlerinin bir diğer önemli bileşenidir. V2X (araçtan her şeye) iletişim ile donatılmış araçlar, birbirleri ve trafik altyapısıyla bilgi alışverişinde bulunabilir. Bu bağlantı, daha koordineli ve verimli trafik akışını sağlar, kazaların riskini azaltır ve genel trafik verimliliğini artırır.

YZ'nin trafik yönetimindeki rolü, kentsel alanların ötesine uzanır. Otoyollarda, YZ destekli sistemler trafik koşullarını izleyebilir, şerit kullanımını yönetebilir ve sürücülere gerçek zamanlı güncellemeler sağlayabilir. Federal Karayolu İdaresi (FHWA), özellikle sıkışıklığı azaltma ve güvenliği artırma konularında otoyol trafik yönetimini iyileştirmek için YZ kullanımı konusunda aktif olarak araştırmalar yapmaktadır.

YZ'nin trafik yönetimindeki önemli faydalarından biri, acil durum müdahale sürelerini iyileştirme yeteneğidir. Gerçek zamanlı trafik verilerini analiz ederek, YZ sistemleri acil durum araçları için en hızlı rotaları belirleyebilir, müdahale sürelerini azaltabilir ve potansiyel olarak hayat kurtarabilir. Oullane ve diğerlerinin (2022)[15] derleme çalışması, YZ destekli trafik yönetiminin acil durum müdahale sürelerini azaltabileceğini göstermiştir.

YZ, toplu taşıma sistemlerini daha verimli yönetmek için de kullanılmaktadır. YZ algoritmaları, otobüs ve tren tarifelerini optimize edebilir, yolcu talebini tahmin edebilir ve gerçek zamanlı koşullara göre hizmetleri dinamik olarak ayarlayabilir. Bu, Massachusetts Bay Taşımacılık İdaresi (MBTA)[16] tarafından yürütülen bir pilot projede gösterildiği gibi, daha güvenilir ve verimli toplu taşıma sonuçlarına yol açar.

Trafik yönetimi sadece araçlara değil, aynı zamanda yayalar ve bisiklet kullananlara de etki eder. YZ destekli sistemler, yaya ve bisiklet trafiğini izleyebilir, sinyal zamanlamalarını optimize ederek onların güvenliğini ve akışını sağlayabilir. Trafik yönetimine bu bütüncül yaklaşım, daha yaşanabilir ve sürdürülebilir şehirler yaratmak için gereklidir.

---

15 Ouallane, A. A., Bahnasse, A., Bakali, A., & Talea, M. (2022). Overview of road traffic management solutions based on IoT and AI. *Procedia Computer Science*, *198*, 518-523.

16 Saidi, S., Koutsopoulos, H. N., Wilson, N. H., & Zhao, J. (2023). Train following model for urban rail transit performance analysis. *Transportation Research Part C: Emerging Technologies*, *148*, 104037.

Çevresel sürdürülebilirlik, YZ destekli trafik yönetiminin bir diğer önemli unsurudur. Trafik akışını optimize ederek ve sıkışıklığı azaltarak, YZ sistemleri araç emisyonlarını düşürebilir ve hava kalitesini iyileştirebilir. Avrupa Çevre Ajansı'nın (EEA)[17] bir çalışması, akıllı trafik yönetiminin kentsel hava kirliliğini önemli seviyede azaltabileceğini bulmuştur.

YZ'nin trafik yönetiminde uygulanması, altyapı ve teknolojiye önemli yatırımlar gerektirir. Trafik yoğunluğunun azalması, güvenliğin artması ve emisyonların düşmesi gibi uzun vadeli faydalar bu yatırımların karşılığında alınır. Hükümetler ve şehir planlamacıları, daha akıllı, daha verimli kentsel ortamlar yaratmada YZ'nin kattığı değeri giderek daha fazla kabul etmektedir.

Veri gizliliği ve güvenliği, YZ destekli trafik yönetim sistemlerinde kritik öneme sahiptir. Araçlar, sensörler ve kameralar tarafından toplanan büyük miktardaki veri, bireysel gizliliği korumak için güvenli bir şekilde saklanmalı ve işlenmelidir. Olası ihlaller ve kötüye kullanımlara karşı bu verileri korumak için sağlam siber güvenlik önlemleri gereklidir.

YZ'nin trafik yönetimine entegrasyonu, birkaç zorluğu da beraberinde getirir. Bunlar arasında standart iletişim protokollerine ihtiyaç, farklı sistemler arasında birlikte çalışabilirlik ve mevcut altyapının yeni teknolojilere destek olacak şekilde uyarlanması yer alır. Bu zorlukların üstesinden gelmek, hükümet ajansları, teknoloji sağlayıcıları ve endüstri paydaşları arasında iş birliği yapılması gerekir.

YZ destekli trafik yönetim sistemleri, özel etkinlikler veya acil durumlar sırasında trafiği yönetmede de kritik bir rol oynayabilir. Büyük kamu toplantıları veya doğal afetler sırasında, YZ sistemleri trafik sinyallerini dinamik olarak ayarlayabilir ve gerçek zamanlı rota önerileri sağlayarak sıkışıklığı hafifletebilir ve sorunsuz tahliye yollarını sağlayabilir.

Kamunun YZ tabanlı trafik yönetim sistemlerine güven duyması, başarıları için kritik öneme sahiptir. Bu sistemlerin faydaları, güvenlik önlemleri ve gizlilik korumaları hakkında şeffaf iletişim, kamu güvenini artırabilir.

Sonuç olarak, YZ destekli trafik yönetim sistemleri, trafik yoğunluğunu azaltma, güvenliği artırma ve genel ulaşım verimliliğini artırma açısından önemli faydalar sunar. Karşılaşılan zorluklara rağmen, YZ'nin trafik yönetimini dönüştürme potansiyeli tartışılmazdır. Şehirler büyümeye ve artan

[17] European Environment Agency. (2022). *Decarbonising road transport — the role of vehicles, fuels and transport demand*. EEA Reports.

trafik talepleriyle karşı karşıya kalmaya devam ederken, YZ'nin trafik yönetimine entegrasyonu, daha akıllı ve daha sürdürülebilir kentsel ortamlar yaratmak için gerekli olacaktır.

III. YOL GÜVENLİĞİ

Yol güvenliği, ulaşım sistemlerinde büyük önem taşır ve YZ'nin entegrasyonu, güvenlik önlemlerini önemli ölçüde artırma potansiyeline sahiptir. YZ teknolojileri, büyük miktarda veriyi gerçek zamanlı olarak analiz edebilir, potansiyel tehlikeleri tanımlayabilir ve sürücülere ve trafik yönetim sistemlerine anında geri bildirim sağlayarak kazaların olasılığını azaltabilir ve genel yol güvenliğini iyileştirebilir.

YZ'nin yol güvenliğindeki en etkili uygulamalarından biri, gelişmiş sürücü destek sistemlerinin (ADAS) geliştirilmesidir. Bu sistemler, sürücülere daha güvenli kararlar almalarında yardımcı olmak için algılayıcılar ve kameralardan gelen verileri işleyen YZ algoritmalarını kullanır. Otomatik acil frenleme, şerit takip yardımı ve uyarlanabilir hız kontrolü gibi özellikler, modern araçlarda artık yaygındır. Bu sistemlerin kazaların önlenmesine elle tutulur katkısı vardır[18].

YZ destekli tahmine dayalı analizler de yol güvenliğinde önemli bir rol oynayabilir. Tarihsel veriler ve gerçek zamanlı girdilerden elde edilen çıktıları analiz ederek, YZ sistemleri potansiyel kaza noktalarını tahmin edebilir ve önleyici tedbirler önerebilir. Örneğin, YZ yayalar için yüksek riskli alanları belirleyebilir ve ek yaya geçitleri veya trafik sinyalleri kurulumunu önerebilir. Dünya Sağlık Örgütü'nün (WHO) bir çalışması, bu tür önlemlerin yaya kazalarını önemli oranda azaltabileceğini bulmuştur[19].

Araç tabanlı sistemlerin yanı sıra, YZ altyapının güvenliğini de artırmak için kullanılmaktadır. Gerçek zamanlı trafik koşullarına göre zamanlamalarını ayarlayan akıllı trafik ışıkları, kavşaklardaki çarpışma olasılığını azaltabilir. Yapılan çalışmalar adaptif trafik sinyal kontrol sistemlerinin kavşak kazalarını azaltabileceğini göstermektedir[20].

---

18 Aleksa, M., Schaub, A., Erdelean, I., Wittmann, S., Soteropoulos, A., & Fürdös, A. (2024). Impact analysis of Advanced Driver Assistance Systems (ADAS) regarding road safety–computing reduction potentials. *European Transport Research Review*, *16*(1), 39.

19 World Health Organization. (2018). *Global Status Report on Road Safety*. Geneva: WHO.

20 Kodi, J. H., Kitali, A. E., Ali, M. S., Alluri, P., & Sando, T. (2021). Estimating safety impacts of adaptive signal control technology using a full Bayesian approach. *Transportation Research Record*, *2675*(11), 1168-1179.

YZ teknolojisi, sürücü davranışını izlemek için de kullanılmaktadır. YZ destekli kameralar ve sensörler, sürücü yorgunluğu, dikkatsizliği gibi işaretleri tespit edebilir ve uyarılar verebilir veya düzeltici önlemler alabilir. Örneğin, bir sürücü yorgunluk belirtileri gösterdiğinde, sistem bir uyarı verebilir veya mola vermesini önerebilir. Bu proaktif yaklaşım, insan hatasından kaynaklanan kazaları önlemede hayati öneme sahiptir.

Ticari taşımacılık alanında, YZ güvenlik standartlarını önemli ölçüde iyileştirebilir. YZ ile donatılmış filo yönetim sistemleri, araç durumlarını ve sürücü davranışlarını gerçek zamanlı olarak izleyebilir, güvenlik düzenlemelerine uyumu sağlayabilir ve kaza riskini azaltabilir. Yapılan araştırmalar[21] YZ tabanlı filo yönetimi, ticari filolardaki kaza oranlarını azaltabileceğini göstermiştir.

YZ'nin büyük veri setlerini işleyip analiz etme yeteneği, yol güvenliği önlemlerinin sürekli olarak iyileştirilmesini sağlar. Trafik kameraları, sosyal medya ve hava durumu raporları gibi çeşitli kaynaklardan veri toplayarak, YZ sistemleri trafik durumları ve potansiyel tehlikeler hakkında kapsamlı bilgiler sunabilir. Bu bilgiler, politika kararlarını ve altyapı iyileştirmelerini bilgilendirerek daha güvenli yollar oluşturulmasına katkıda bulunur.

YZ'nin yol güvenliğinde uygulanmasında etik konular da kritik öneme sahiptir. YZ sistemlerinin adil ve şeffaf bir şekilde tasarlanıp uygulanması önemlidir. Politikacılar, veri gizliliği ve YZ algoritmalarında ön yargılı karar verme potansiyeli gibi konuları ele almalıdır. Güçlü etik çerçevelerin geliştirilmesi, YZ'nin yol güvenliğine olumlu katkıda bulunmasını ve birey haklarının korunmasını sağlar.

Sonuç olarak, YZ gelişmiş sürücü destek sistemleri, tahmine dayalı analizler, akıllı altyapı ve iyileştirilmiş acil durum müdahalesi yoluyla yol güvenliğini artırmak için önemli fırsatlar sunar. Etik konular ve sağlam altyapı gereksinimleri gibi zorluklar bulunsa da YZ'nin daha güvenli yollar oluşturma potansiyeli yüksektir. YZ teknolojilerine yapılan sürekli yatırımlar ve hükümetler, endüstri ve araştırmacılar arasındaki iş birliği, bu faydaların gerçekleştirilmesinde kritik olacaktır.

---

[21] Xidias, E., Zacharia, P., & Nearchou, A. (2022). Intelligent fleet management of autonomous vehicles for city logistics. *Applied Intelligence*, *52*(15), 18030-18048.

IV. HUKUKİ VE ETİK HUSUSLAR

Ulaşım sistemlerinde YZ'nin entegrasyonu, birçok fayda sunarken, önemli hukuki ve etik sorunları da beraberinde getirir. Bu sorunlar veri gizliliği, sorumluluk, şeffaflık ve YZ karar verme süreçlerinin etik sonuçları ile ilişkilidir. Bu endişelerin ele alınması, YZ teknolojilerinin ulaşımda sorumlu bir şekilde geliştirilmesi ve uygulanması için hayati öneme sahiptir.

Veri gizliliği, YZ destekli ulaşım sistemlerinde önemli bir konudur. Bu sistemler, sürücüler ve yolcular hakkında kişisel bilgileri de içeren büyük miktarda veri toplar ve işler. Bu verilerin yetkisiz erişimden ve kötüye kullanımdan korunması çok önemlidir. *Güçlü* veri koruma önlemleri ve Genel Veri Koruma Tüzüğü (GDPR) gibi düzenlemelere uyum, kamu güvenini sürdürmek için kritiktir[22].

Sorumluluk meseleleri de önemli bir hukuki zorluktur. Otonom bir araçla ilgili bir kaza durumunda kimin sorumlu olduğunu belirlemek karmaşık bir problemdir. Geleneksel sorumluluk çerçeveleri, YZ destekli sistemlerin getirdiği benzersiz zorlukları ele almak için yeterli olmayabilir. Hukukçular, üreticilerin, yazılım geliştiricilerin ve otonom araç kullanıcılarının sorumluluklarını net bir şekilde tanımlayan yeni hukuki çerçevelerin geliştirilmesi gerektiğini savunmaktadır[23].

YZ karar verme süreçlerinde şeffaflık, sistemlerin adil ve ön yargısız çalışmasını sağlamak için önemlidir. Ancak, birçok YZ algoritmasının "kara kutu" doğası, kararların nasıl alındığını anlamayı zorlaştırabilir. Bu şeffaflık eksikliği, kamuoyunda güvensizlik ve direnç yaratabilir. *Araştırmalar*, kararlarının net ve anlaşılır gerekçelerini sağlayan açıklanabilir YZ sistemlerinin geliştirilmesinin önemini vurgulamaktadır[24].

YZ'nin ulaşımda uygulanmasında etik hususlar merkezi bir öneme sahiptir. En çok tartışılan etik ikilemlerden biri "*trolley problem*"dir[25]; bu

[22] Sharma, S. (2019). *Data privacy and GDPR handbook*. John Wiley & Sons.

[23] Gurney, J. K. (2013). Sue my car not me: Products liability and accidents involving autonomous vehicles. *U. Ill. JL Tech. & Pol'y*, 247.

[24] de Fine Licht, K., & de Fine Licht, J. (2020). Artificial intelligence, transparency, and public decision-making: Why explanations are key when trying to produce perceived legitimacy. *AI & society*, *35*, 917-926.

[25] Wiseman, Y., & Grinberg, I. (2018). The Trolley Problem Version of Autonomous Vehicles. *The Open Transportation Journal*, *12*(1).

problem, otonom bir aracın iki zararlı sonuç arasında seçim yapmak zorunda kaldığı bir durumda nasıl tepki vermesi gerektiğini sorgular. Araştırmacılar, çeşitli etik çerçeveleri araştırmakta ve YZ sistemlerinin etik karar verme süreçlerini yönlendirecek net yönergeler ve ilkeler gerektiğini önermektedirler[26].

Ulaşımda kullanılan YZ sistemleri aynı zamanda ön yargı sorununu da göz önünde bulundurmalıdır. YZ algoritmalarındaki ön yargılar, adaletsiz sonuçlara ve ayrımcılığa yol açabilir. Örneğin, bir YZ sistemi, ön yargılı eğitim verilerine dayanarak belirli demografik grupları trafik ihlalleri için orantısız bir şekilde hedefleyebilir.

Etik hususlar, YZ'nin ulaşımda çevresel etkisini de kapsar. YZ teknolojileri, emisyonları azaltma ve sürdürülebilir ulaşım uygulamalarını teşvik etme potansiyeline sahiptir. Ancak, YZ sistemlerinin geliştirilmesi ve işletilmesinin çevresel maliyetleri, enerji tüketimi ve elektronik atık gibi konular da göz önünde bulundurulmalıdır. *Araştırmalar*[27], çevresel faydaları maksimize ederken olumsuz etkileri en aza indiren dengeli bir yaklaşım çağrısında bulunmaktadır.

"Algoritmik adalet"[28] kavramı, YZ etiği tartışmalarında giderek daha önemli hale gelmektedir. YZ sistemlerinin adil ve eşit bir şekilde çalışmasını sağlamak için ayrımcılık ve ön yargıyı önlemek amacıyla titiz testler ve doğrulamalar gereklidir. Araştırmacılar YZ sistemlerinin adil ve kapsayıcı olmasını sağlamak için geliştirilmesinde çeşitli bakış açılarını dahil etmenin önemini savunmaktadır.

YZ'nin ulaşımda kullanımı, istihdam ve işçi hakları konusunda da sorular ortaya çıkarır. Sürüş ve trafik yönetimi görevlerinin otomasyonu, sürücüler ve diğer ulaşım çalışanları için iş kaybına yol açabilir. *Araştırmacılar* YZ'nin istihdam üzerindeki potansiyel etkilerini incelemekte ve çalışanları ulaşım sektörünün değişim geçiren rollerine geçişte destekleyen politikalar çağrısında bulunmaktadır.

---

26 Gaur, L., & Sahoo, B. M. (2022). *Explainable Artificial Intelligence for Intelligent Transportation Systems: Ethics and Applications*. Springer Nature.

27 Moyano-Fernández, C., & Rueda, J. (2024). AI, sustainability, and environmental ethics. In *Ethics of artificial intelligence* (pp. 219-236). Cham: Springer Nature Switzerland.

28 Završnik, A. (2021). Algorithmic justice: Algorithms and big data in criminal justice settings. *European Journal of criminology*, *18*(5), 623-642.

Sonuç olarak, YZ'nin ulaşımda hukuki ve etik hususları çok yönlü ve karmaşıktır. Veri gizliliği, sorumluluk, şeffaflık, ön yargı ve çevresel etki gibi konuların ele alınması, kapsamlı ve iş birlikçi bir yaklaşım gerektirir. Güçlü hukuki çerçeveler ve etik yönergeler geliştirerek, YZ teknolojilerinin ulaşımda güvenli, adil ve herkes için faydalı olmasını sağlayabiliriz.

SONUÇ

Özetle YZ'nin ulaşım sistemlerine entegrasyonu, seyahat ve trafik yönetiminde devrim yaratma potansiyeline sahiptir. Otonom sürüş sistemlerinin yeteneklerinin artırılmasından trafik yönetiminin iyileştirilmesine, yol güvenliğinin sağlanmasından karmaşık hukuki ve etik sorunların ele alınmasına kadar, YZ daha verimli, güvenli ve sürdürülebilir ulaşım çözümleri sunar. Ancak, bu faydaların gerçekleştirilmesi, sağlam hukuki çerçeveler, sürekli teknolojik gelişmeler ve etik hususları içeren kapsamlı bir yaklaşım gerektirir. Sanayi, akademi ve hükümet arasındaki iş birliğini teşvik ederek ve şeffaflık, adalet ve kamu güvenine odaklanarak, YZ'nin tam potansiyelini kullanarak daha akıllı ve dayanıklı bir ulaşım geleceği yaratmak mümkündür.

KAYNAKÇA

ALEKSA, Michael, SCHAUB Andrea et al. "Impact Analysis of Advanced Driver Assistance Systems (ADAS) Regarding Road Safety–Computing Reduction Potentials." *European Transport Research Review* 16, no. 1 (2024): 39.

CHEN, Cynthia, MA, Jingtao et al. "The Promises of Big Data and Small Data for Travel Behavior (aka Human Mobility) Analysis." *Transportation Research Part C: Emerging Technologies* 68 (2016): 285-299.

DE FINE LICHT, Karl and DE FINE LICHT Jenny. "Artificial Intelligence, Transparency, and Public Decision-Making: Why Explanations Are Key When Trying to Produce Perceived Legitimacy." *AI & Society* 35 (2020): 917-926.

European Environment Agency. *Decarbonising Road Transport — The Role of Vehicles, Fuels and Transport Demand*. EEA Reports, 2022.

GAUR, Loveleen, and SAHOO, Biswa Mohan. *Explainable Artificial Intelligence for Intelligent Transportation Systems: Ethics and Applications*. Springer Nature, 2022.

GOODALL, Noah J. "Machine Ethics and Automated Vehicles." In *Road Vehicle Automation*, 93-102. Springer, 2014.

GURNEY, Jeffrey "Sue My Car Not Me: Products Liability and Accidents Involving Autonomous Vehicles." *University of Illinois Journal of Law, Technology & Policy* (2013): 247.

International Transport Forum. *Transport Outlook 2017*. OECD Publishing, 2017.

KALRA, Nidhi and PADDOCK Susan M. *Driving to Safety: How Many Miles of Driving Would It Take to Demonstrate Autonomous Vehicle Reliability?* RAND Corporation, 2016.

KODI, John H., KITALI Angela E. et al. "Estimating Safety Impacts of Adaptive Signal Control Technology Using a Full Bayesian Approach." *Transportation Research Record* 2675, no. 11 (2021): 1168-1179.

KPMG. *The Future of Insurance in the Age of Autonomous Vehicles*, 2015.

LIN, Patrick. "Why Ethics Matters for Autonomous Cars." In *Autonomous Driving: Technical, Legal and Social Aspects*, 69-85. Springer, 2016.

McKinsey & Company. *Distraction or Disruption? Autonomous Trucks Gain Ground in US Logistics*, 2019. https://www.mckinsey.com/industries/travel-logistics-and-infrastructure/our-insights/distraction-or-disruption-autonomous-trucks-gain-ground-in-us-logistics.

MOYANO-FERNÁNDEZ, Cristian and RUEDA, Jon. "AI, Sustainability, and Environmental Ethics." In *Ethics of Artificial Intelligence*, 219-236. Cham: Springer Nature Switzerland, 2024.

National Highway Traffic Safety Administration. *Critical Reasons for Crashes Investigated in the National Motor Vehicle Crash Causation Survey*. Washington, DC, 2020.

OUALLANE, Asma Ait, BAHNASSE Ayoub et al. "Overview of Road Traffic Management Solutions Based on IoT and AI." *Procedia Computer Science* 198 (2022): 518-523.

SAIDI, Saeid, Haris N. KOUTSOPOULOS et al. "Train Following Model for Urban Rail Transit Performance Analysis." *Transportation Research Part C: Emerging Technologies* 148 (2023): 104037.

SCHWALL, Matthew, DANIEL,Tom et al. "Waymo Public Road Safety Performance Data." *arXiv preprint arXiv:2011.00038*, 2020.

SHARMA, Sanjay. *Data Privacy and GDPR Handbook*. John Wiley & Sons, 2019.

Tesla Inc. *Vehicle Safety Report*. Tesla, 2020. https://www.tesla.com/ VehicleSafetyReport.

VLAHOGIANNI, Eleni I., KARLAFTIS, Mark G. and GOLIAS, John C. "Short-Term Traffic Forecasting: Where We Are and Where We're Going." *Transportation Research Part C: Emerging Technologies* 43 (2014): 3-19.

WISEMAN, Yair, and GRINBERG, Ilan. "The Trolley Problem Version of Autonomous Vehicles." *The Open Transportation Journal* 12, no. 1 (2018).

World Health Organization. *Global Status Report on Road Safety*. Geneva: WHO, 2018.

XIDIAS, Elias K., ZACHARIA, Paraskevi and NEARCHOU, Andreas. "Intelligent Fleet Management of Autonomous Vehicles for City Logistics." *Applied Intelligence* 52, no. 15 (2022): 18030-18048.

ZAVRŠNIK, Aleš. "Algorithmic Justice: Algorithms and Big Data in Criminal Justice Settings." *European Journal of Criminology* 18, no. 5 (2021): 623-642.

ZENG, Jinghong, HU, Jianming, and ZHANG, Yan. "Adaptive Traffic Signal Control with Deep Recurrent Q-Learning." In *2018 IEEE Intelligent Vehicles Symposium (IV)*, 1215-1220. IEEE, 2018.

ZHANG, L., KHALGUI, M., and LI, M. "Predictive Intelligent Transportation: Alleviating Traffic Congestion in the Internet of Vehicles." *Sensors* 21, no. 21 (2021): 7330.

FİNANS SEKTÖRÜNDE YAPAY ZEKÂ KULLANIMI: KİŞİSEL VERİLERİN KORUNMASI ODAĞINDA BİR DEĞERLENDİRME

Doç. Dr. Pınar ÇAĞLAYAN AKSOY*

GİRİŞ

COVID-19 pandemisi tüm dünyada dijitalleşmenin hızını artırdı. 2020 yılından beri dijitalleşme iş hayatının ve günlük hayatın her noktasında hissediliyor. Son birkaç yılda özellikle yapay zekâ (AI-*artificial intelligence*) teknolojileri tüm dünyada hiç olmadığı kadar gündeme oturdu. Bunda üretken yapay zekâya[1] yönelik gelişmelerin etkisinin büyük olduğu yadsınamaz bir gerçek. Bu gelişmelere paralel olarak, yapay zekâ teknolojilerine yapılan yatırımların ve bu teknolojiyle ilgili yapılan araştırmaların da ciddi ölçüde arttığını görmekteyiz.[2]

Yapay zekâ sağlık, otomotiv, lojistik, eğitim gibi birçok sektörde iş ve işlem akışını değiştirmiştir. Ancak bazı sektörlerin yapay zekâ teknolojilerindeki

* Bilkent Üniversitesi Hukuk Fakültesi Öğretim Üyesi

1 GenAI olarak da kısaltılan üretken yapay zekâ, yeni içerik oluşturma yetenekleriyle öne çıkan, yapay zekâ-makine öğrenimi teknolojilerinin özel bir alt kümesidir. GenAI'nin temelinde, metin ve belgeler de dahil olmak üzere çok büyük miktarda veri üzerinde eğitilen ve anlaşılır ve anlamlı metinler veya insan dilleri üretebilen sinir ağı tabanlı modeller olan büyük dil modelleri bulunmaktadır. Bkz. IMF: *"Generative Artificial Intelligence in Finance: Risk Considerations IMF Fintech Note 2023/006"*, (https://www.imf.org/en/ Publications/fintech-notes/Issues/2023/08/18/Generative-Artificial-Intelligence-in-Finance-Risk-Considerations-537570, E.T.: 06.07.2024), s. 4.

2 Bankaların yapay zekâ teknolojileri ile ilgili yaptığı harcamaların nasıl arttığı ve artış göstermesi beklendiği ile ilgili olarak bkz. Citi GPS: *"AI in Finance Bot, Bank & Beyond", (https://ir.citi.com/gps/9j79xHIa-vfPi785TYiSciffO0j4I0D52fI9LrahsLZEo 6MpT4aM7SpwSFag AL9CIukqn2fwi]_GNvDsLy4b6XEjftdK1abu*, E.T.: 06.07.2024), s. 15. Ayrıca bkz. IMF (2021*) Powering the Digital Economy: Opportunities and Risks of Artificial Intelligence in Finance, (https://www.imf.org/en/Publications/Departmental-Papers-Policy-Papers/Issues/2021/10/21/Powering-the-Digital-Economy-Opportunities-and-Risks-of-Artificial-Intelligence-in-Finance-494717, E.T.: 06.07.2024).*

gelişmelerden daha hızlı ve daha çok etkilendiği de bir gerçektir. Finans sektörü de bunlardan biridir. Esas itibariyle finans sektörü gelişen teknolojilerin etkisiyle, elli yıldan da fazla bir süredir, en hızlı dönüşen sektörlerden biri olmuştur. Yazılım ve donanımlardaki gelişmeler, ileri düzey analitik, makine öğrenmesi (ML- *machine learning*) ve üretken yapay zekâ (Generative AI/GenAI- *generative artificial intelligence*) gibi teknolojik dönüm noktalarında, finansal sistem ya bu değişimi tetiklemiş ya da teknolojiyi benimsemekte ve uygulamakta öncü bir rol üstlenmiştir.[3]

Yapay zekâ teknolojilerinde son yıllarda yaşanmakta olan gelişmelerin finans sektörü üzerinde etkisini göstermesi de uzun sürmemiştir. Yirminci yüzyılda yapay zekâ risk yönetimi, temel algoritmik ticaret ve kredi puanlama gibi işlemlerde kullanılmaktayken, bu sistemler örüntü tanıma, belirsizliklerle baş etme ve karmaşık gerekçelendirme süreçleri bakımından yetersiz kalmaktaydı.[4] Finansal kurumlar, bilgi ve iletişim teknolojilerine dayalı finansal hizmetler sunarak perakende müşteri segmenti elde etmenin çekiciliğini hızla fark etmişlerdir. Hemen akabinde hizmetlerini güçlü bir şekilde büyüyen ve küreselleşen ekonominin ihtiyaçlarını karşılayacak şekilde hızla ve etkili bir şekilde genişletmiş ve dönüştürmüşlerdir.[5]

Finansal hizmetler sektörünün yapay zekâya en çok yatırım yapan sektörlerden biri olduğu araştırmalar sonucu elde edilen rakamlarla da desteklenen bir tespittir.[6] Finansal kurumların yapay zekâ teknolojilerine yaptıkları yatırımları 2027 yılı itibariyle ikiye katlamış olmalarının bekleniyor olması, yapay zekânın finans sektöründe gittikçe artan önemini gözler önüne sermektedir. [7] Ayrıca şu hususa da dikkat çekilmesi yerinde olacaktır: Bu kitap bölümünün yazılmaya başlandığı günden son noktanın konulması arasında geçen zaman diliminde, IMF, OECD, WEF, BIS ve Avrupa Birliği

---

3 BIS: *"Intelligent financial system: how AI is transforming finance, BIS Working Papers No 1194, June 2024", (https://www.bis.org/publ/work1194.pdf,* E.T.: 06.07.2024), s. 3.

4 BIS, s. 4.

5 Piotrowski, D. /Orzeszko, W.: *Artificial intelligence and customers' intention to use roboadvisory in banking services*, Equilibrium Quarterly Journal of Economics and Economic Policy 2023, C. 18, S. 4, s. 968.

6 Ozan Özparlak, B./Çetin, M.: *ChatGPT ve Üretici Yapay Zekâ Modellerinde Mahremiyet ve Güvenliğin Hukuki Boyutu,* Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi 2023, C. 29, S. 2, s. 1014.

7 IMF (2023), *AI'S Reverberations Across Finance, (https://www.imf.org/en/Publications/fandd/issues/2023/12/AI-reverberations-across-finance-Kearns,* E.T.: 06.07.2024).

gibi kurum ve kuruluşlar finans sektöründe yapay zekâ kullanılmasının avantajları ve riskleriyle ilgili politika belgeleri yayınlamıştır.[8]

Finans ile yapay zekâ arasındaki yoğun etkileşimin temelinde, finansal hizmetlerin yüksek miktarda ve sürekli artan verilerin mevcudiyetine dayanması yatmaktadır. Finansal hizmetler sektörü günümüz ekonomilerinin en yoğun veriye sahip ve veri trafiği söz konusu olan sektörlerden biridir.[9] Hâlihazırda dünya genelindeki birçok finansal hizmet sağlayıcı, yapay zekâ uygulamalarından finansal süreçlerin bir veya birden çok aşamasında mutlaka yararlanmaktadır. COVID-19 pandemisi sonrasında özellikle müşteri ilişkileri ve risk yönetimi gibi finans alanlarında yapay zekâ kullanımında önemli bir artış olduğu belirtilmektedir.[10]

Üretken yapay zekâ alanındaki gelişmeler, finansta yapay zekâ kullanımını daha da gündeme taşımıştır. Gerçekten de finansal süreçler, raporlama, olağanüstü durumların tespiti için veri analizi veya verinin geçerliliğini kontrol etmek gibi üretken yapay zekânın katkı sunabileceği aşamalardan oluşmaktadır.[11] Bankalar ve diğer finans kuruluşları müşteri hizmetlerini iyileştirmek, riskleri yönetmek, kredi değerlendirmeleri ve operasyonel verimliliğin sağlanması gibi alanlarda üretken yapay zekâ araçlarından yararlanmaktadır. Üretken yapay zekânın yaygınlaşması ve gelişmesiyle birlikte finans sektöründe suistimallerin önlenmesi, uyum ve risk yönetiminin sağlanması, varlık yönetimi ve müşteri hizmetlerinin geliştirilmesi ve iyileştirilmesi için yapay zekâdan daha da fazla yararlanılması beklenmektedir.[12] Hâlihazırda

---

8 Bu rapor ve belgelere çalışmamızda yeri geldikçe değinilecek olup, ilk etapta ve güncel bir örnek olarak Avrupa Komisyonu tarafından Haziran 2024'te yayınlanan Konsültasyon Belgesi'ni vermek mümkündür. Bu konsültasyonun amacı, yapay zekânın finans sektöründeki uygulama alanlarını ve etkisini tespit etmek; ayrıca AI Act özelinde de finans sektörü bakımından değerlendirmelerde bulunmaktır. Bu belgede yer alan sorulara gelen yanıtlar, Komisyon tarafından (gerektiği takdirde) resmi bir teklif oluşturulmasında dikkate alınacaktır. Bkz. European Commission: *"Targeted consultation on artificial intelligence in the financial sector", (https://finance.ec.europa.eu/regulation-and-supervision/consultations-0/targeted-consultation-artificial-intelligence-financial-sector_en,* E.T.: 06.07.2024).

9 OECD: *"Personal Data Use in Financial Services and the Role of Financial Education: A Consumer-centric Analysis"*, *(https://doi.org/10.1787/06998d33-en,* E.T.: 06.07.2024), s. 9.

10 IMF, 2023, s. 5.

11 KPMG (2024), *Üretken Yapay Zeka ile Finansın Yeni Normali,* (*https://assets.kpmg.com/content/dam/kpmg/tr/pdf/2024/01/uretken-yapay-zeka-ile-finansin-yeni-normali.pdf*, E.T.: 06.07.2024), s. 9.

12 KPMG, s. 8; BIS: s. 10.

JP Morgan, Goldman Sachs ve Deutsche Bank gibi finansal kuruluşlar da kod yazılması, finansal analizlerin gerçekleştirilmesi ve sorunların yönetilmesi gibi konularda GenAI araçlarına başvurmaktadır.[13]

Yapay zekâ araçlarının finans alanında kullanılmasının finansal şirketler açısından bir rekabet avantajı yaratacağı düşünülmektedir. Bu avantaj iki şekilde ortaya çıkabilir: İlk olarak maliyetlerin azaltılması ve üretkenliğin artmasıyla şirketlerin verimliliği artmakta ve böylece daha yüksek bir karlılık oranı ortaya çıkmaktadır. İkinci olarak ise tüketicilere sunulan hizmetlerin ve ürünlerin kalitesinin artırılması sağlanmaktadır. Ortaya çıkan rekabet avantajı daha kaliteli ürünlerin sunulmasını, kişiselleştirme imkânının ve seçeneklerin artmasını veya maliyetlerin azalmasını sağlayarak finansal tüketicinin elde edeceği faydayı artırmaktadır.[14]

FinTech (*financial technology*-finansal teknoloji) kavramının hem iş hayatında hem günlük hayatta sıklıkla kullanılır hale gelmesi de finans sektörüyle yeni teknolojilerin ne kadar iç içe geçtiğine işaret etmektedir. Son yıllarda nesnelerin interneti, büyük veri, blokzinciri ve yapay zekâ gibi teknolojilerdeki gelişmeler, FinTech kavramını daha sık duymamıza neden olmuştur. FinTech en basit haliyle, finansta teknolojinin kullanılmasını ifade eden bir kavramdır. Aslında yıllar önce kredi kartlarının kullanılmaya başlanması ilk FinTech uygulaması olarak görülebilir. FinTech tüketiciler ve işletmeler açısından finansal işlemlerin daha erişilebilir ve daha az maliyetli olmasını sağlamaktadır. Müşteriler cep telefonlarındaki uygulamaları kullanarak hesap açabilmekte, kredi alabilmekte, yatırım ve ödemelerini kolayca ve hızlı bir şekilde yapabilmektedir.

Bazı yazarlar tarafından FinTech 3.0 olarak adlandırılan dönem, 2008 yılındaki küresel kriz sonrasında banka ve finans kuruluşlarına duyulan güvenin azalmasıyla başlamıştır. Bu yeni FinTech döneminde dijital teknolojiye giderek daha fazla dayanan ve finansal hizmetler sunan FinTech girişimleri ve BigTech şirketleriyle ortaklık içinde çalışan geleneksel bankalar ve finansal kurumlar temel aktörler haline gelmiştir. Böylece, finansal

---

13 OECD: *"Generative Artificial Intelligence In Finance, OECD Artificial Intelligence Papers December 2023 No. 9", (https://www.oecd-ilibrary.org/docserver/ac7149cc-en.pdf?expires=1719399009&id=id&accname=guest&checksum=4559573E565D449ED3558B1EACFA1EDD,* E.T.: 06.07.2024), s. 15.

14 OECD: *"Artificial Intelligence, Machine Learning and Big Data in Finance: Opportunities, Challenges, and Implications for Policy Makers", (https://www.oecd.org/finance/ artificial-intelligence-machine-learningbig-data-in-finance.htm*, E.T.: 06.07.2024).

hizmetlerin demokratikleşmesi söz konusu olmuştur. Bu dönemde akıllı telefonlar, hizmet bankacılığı *(banking-as-a-service)*, DLT *(distributed ledger technology- dağıtık defter teknolojisi*) gibi kavramlar finans sektörünün ve FinTech'lerin şekillenmesinde önemli bir rol oynamıştır.

Finans dünyası yavaş yavaş yüksek hacimli bilgilerin ve yüksek hızlı veri dönüşümü ve işlemesinin dijital alanı olmaya doğru evrilmektedir. Bu gelişmelerle birlikte, tüketici ve yatırımcı davranışları da piyasa katılımcılarının, finansal kurumların ve finansal teknoloji şirketlerinin sunduğu finansal hizmetlerde teknoloji yanlısı bir tutum sergilemektedir.[15]

Teknolojik gelişmelerin etkisini artırdığı bu dönemde, banka niteliği taşımayan, geleneksel anlamda finansal kuruluş niteliği bulunmayan yapılanmalar da artan bir şekilde finansal hizmetler sunmaya başlamıştır. Eşler arası borç vermeyi sağlayan *(peer-to-peer lending)* platformlar, mobil ödeme hizmet sağlayıcıları veya büyük teknoloji şirketlerinin sunduğu finansal hizmetler bu paradigma değişikliğine örnek olarak gösterilebilir.[16] Önceleri sadece bankalar tarafından sunulan hizmet ve ürünler artık farklı kurum ve kuruluşlar tarafından da sağlanabilmektedir. Bunların içinde, PayPal gibi ödemelerin gerçekleştirilmesini sağlayan kuruluşlar, Transferwise gibi döviz değişim hizmetleri ve ödünç veren diğer kuruluşlar sayılmaktadır. Bu alandaki rekabetin artmasıyla, müşteriler, nerede hesap açmak istediklerine, ödemeleri nasıl yapmak istediklerine ve nereden borç almak istediklerine serbestçe karar verebilmektedir. Böylece kendi ihtiyaçlarına ve mali durumlarına en uygun seçeneği tercih edebilmektedirler.[17]

Her ne kadar FinTech finansta sadece yapay zekânın kullanımına işaret etmese de yapay zekâ finansal hizmetler sektörünün dönüşümü ve FinTechlerin gelişimi hususunda önemli bir itici güçtür. FinTech'in gelişmesine katkıda bulunan birçok faktör, yapay zekâ ve makine öğrenmesi teknolojilerinin finansal hizmetlerde de daha fazla kullanılmasını tetiklemiştir[18].

---

15 Nguyen, D. K./Sermpinis, G./Stasinakis, C.: *Big data, artificial intelligence and machine learning: A transformative symbiosis in favour of financial technology,* European Financial Management 2023, C. 29, S. 2, s. 518.

16 Aggarwal, N.: AI, Fintech and the Evolving Regulation of Consumer Financial Privacy, (ed. Justin B. Bullock et al), "The Oxford Handbook of AI Governance", 2022, s. 861.

17 Königstorfer, F./Thalmann, S.: *Applications of Artificial Intelligence in commercial banks – A research agenda for behavioral finance,* Journal of Behavioral and Experimental Finance 2020, C. 27, S. 2, s. 3.

18 FSB:*"Artificial Intelligence and Machine Learning in Financial Services Market Developments and Financial Stability Implications", (https://www.fsb.org/wp-content/uploads/P011117.pdf,* E.T.: 06.07.2024), s. 7.

FinTech evrimini inceleyen bir yazar şu tespitte bulunmaktadır: *"Fintech, son yıllardaki IoT ve Web 2.0 devriminin akabinde büyük verilerin kullanıma sunulmasının yanı sıra, finansta AI ve ML (machine learning- makine öğrenmesi) tekniklerinin kademeli olarak kabul edilmesi nedeniyle artık her zamankinden daha egzotik."*[19]

Finans sektöründe yapay zekâ teknolojilerinin kullanılmasının pek çok açıdan faydaları olmakla birlikte, aynı zamanda bazı riskler ortaya çıkaracağı konusunda tereddüt yoktur.[20] Yapay zekânın beraberinde getirdiği çeşitli avantajlar iş hayatını ve günlük hayatı kolaylaştırırken, aynı zamanda yapay zekânın barındırdığı mevcut ve potansiyel risklere karşı önlem alınması birçok ülkenin ajandalarında ön plana çıkmaktadır. Bir taraftan bu riskler tespit edilmeye çalışılmakta, diğer taraftan da kural ve standartların gittikçe globalleşen ekonomilerde nasıl geliştirilmesi gerektiği konusunda adımlar atılmaktadır.

Gerçekten de yapay zekâ uygulamaları, finansal riskleri artırabilir ve hem tüketiciler hem de yatırımcılar açısından daha önce mevcut olmayan bazı yeni riskler ortaya çıkarabilir. Bu risklerin içinde, tüketiciler açısından ön yargılı, adil olmayan veya ayrımcı sonuçlar meydana getirilmesi ile veri yönetimi ve kullanımıyla ilgili endişeler yer almaktadır. Ayrıca, yapay zekâ modeli süreçlerinin açıklanabilir olmaması, piyasalarda potansiyel döngüselliğe ve sistemik risklere ve mevcut mali denetim ve iç yönetişim çerçeveleriyle olası uyumsuzluklar yaratma potansiyeline sahiptir. GenAI teknolojilerinin gittikçe artan yetenekleri, yapay zekâ ile ilgili bu risklerden bazılarını daha da belirginleştirmekte ve kendi özellikleriyle ilişkili bir dizi ek yeni sorunu gündeme getirmektedir. Mesela açıklanabilirlik ile zorluklar daha da artmaktadır ve zayıf performansı ve/veya operasyonel başarısızlıkları açıklamak güçleşmektedir. [21] GenAI teknolojilerinin kullanımı aynı zamanda yapay zekânın finansta daha geniş anlamda kullanılmasıyla ilgili üçüncü taraf bağımlılığı ve yoğunlaşma risklerini de artırmaktadır.[22]

---

19 Arner D.W/Barberis, J./Buckley, R.P.: *The evolution of Fintech: A new post-crisis paradigm?* Georgetown Journal of International Law &Business 2016, C. 37, s. 371.

20 Ayrıntılı bilgi için bkz. Barriere, F.: *Financial Law In The Era Of Artificial Intelligence: Key Topics And Themes*, Law and Financial Markets Review 2021, C. 15, S. 3–4, s. 312–322, s. 316 vd. Bu risklerin neler olduğuna ilişkin olarak OECD ve OECD dışındaki ülkeler kapsamında yapılmış olan geniş çaplı bir araştırmanın sonuçları için bkz. OECD, 2024, s. 17.

21 OECD, 2021, s. 3.

22 OECD, 2023, s. 19.

Bu risklere karşı önlem alınması konusunda Avrupa Birliği'nin dünyada öncü konumda olduğu görülmektedir.[23] Yakın zamanda Avrupa Birliği tarafından kabul edilen AI Act de, yapay zekâ teknolojilerine ilişkin düzenleme yapılması gerekliliğinin zamanının geldiğini gözler önüne sermektedir. Türkiye'de de finans sektörünün teknoloji odaklı dönüşümü düzenli olarak yapılan mevzuat değişiklikleri ile desteklenmektedir. Son yıllarda Türkiye'deki FinTech ekosistemini güçlendiren pek çok gelişme olmuştur. Bununla birlikte, yapay zekâ araçlarının finans alanında ortaya çıkarabileceği risklere karşı önlem alınmasına yönelik somut bir adım atılmamıştır.

Yapay zekâ araçlarının finans sektöründe kullanılmasının ortaya çıkardığı risklerden birisi de bu çalışmanın konusunu oluşturan kişisel verilerin korunmasıdır. Yapay zekâ sistemlerinin işletilmesi büyük ölçüde veriye dayandığı için, bu verilerin güvenliğinin sağlanması ve mahremiyet konuları ön plana çıkmaktadır. Ayrıca, üretici yapay zekâ modellerinin farklı alanlarda geniş çevreler tarafından kullanıma açık güçlü sistemler olması, mahremiyet ve güvenlik risklerini daha önceki yapay zekâ modellerine kıyasla artırmaktadır.[24]

Çalışmamızda ilk olarak finans sektöründe yapay zekânın hangi aşamalarda ve nasıl kullanıldığına ilişkin bilgiler aktarılacaktır. Daha sonra ise, finans sektöründe yapay zekâ teknolojilerinin kullanılmasının mahremiyet, siber güvenlik gibi alanlarda nasıl riskler meydana getirdiği ve bunlara ilişkin sunulan çözüm önerileri aktarılacaktır.

I. FİNANS SEKTÖRÜNDE YAPAY ZEKÂ TEKNOLOJİLERİNİN KULLANILMASI

Algoritmalar ve yapay zekâ teknolojilerinin finans sektöründe birçok uygulama alanı bulunmaktadır. Bunun temel sebebi, yapay zekâ etmenlerinin insanlara kıyasla daha güçlü bazı özelliklere sahip olmasıdır: Mesela insanlar daha yeni verilere öncelik verme eğilimindeyken, yapay zekâ, geçmiş verileri daha yeni verilerle aynı hassasiyetle dikkate almaktadır. İkincisi, doğru programlanmış bir yapay zekâ etmeni tüm verileri objektif bir şekilde ele alırken, insanlar deneyimlerine, değerlerine ve diğer rasyonel olmayan yargılarına dayanarak veri noktaları arasında ayrım yapma eğili-

23 Citi GPS.

24 Ozan Özparlak/Çetin, s. 1005.

mindedir. Yapay zekâ ise kendi gündemini takip etmemek veya bilişsel ön yargılara sahip olmak noktasında tarafsız kalabilmektedir.[25]

Günümüzde yapay zekâ teknolojileri yukarıda belirtilmiş olan güçlü yönler sayesinde finansal aracılık, risk yönetimi, hukuki uyumun sağlanması gibi konularda dönüşümü sağlayarak, finans sektörünü yeniden şekillendirmektedir. Rekabetçi baskılar, son yıllarda verimlilik ve maliyet tasarruflarındaki kazanımları kolaylaştırarak, müşteri arayüzlerini yeniden şekillendirerek, tahmin doğruluğunu artırarak ve risk yönetimini ve uyumluluğu iyileştirerek makine öğrenmesinin finans sektöründe hızla benimsenmesini tetiklemiştir.

Genel olarak, yapay zekâ ve büyük veri uygulamaları, bankalar, diğer finansal kurumlar ve FinTech kredi sağlayıcıları tarafından dolandırıcılık tespitinde, müşteri kabulünde, kredi kararı verilmesi aşamalarında, KYC (*know your customer*- müşterini tanı) kontrollerinde, kara para aklamanın önlenmesinde ve terör finansmanı taramalarında, ortak bir platformda müşteri kabulü ve devam eden müşteri durum tespit aşamasında (AML/CFT- *anti-money laundering and counter-terrorism financing*) kullanılmaktadır. Yapay zekâ özellikle finansal kurumların anormal işlemleri tespit etmesine ve şüpheli ve potansiyel dolandırıcılık faaliyetlerini (örneğin müşterinin kişisel bilgilerinin kötü niyetle kullanımı, ürünler/hizmetlerin yanlış tanıtılması) tespit etmesine yardımcı olabilmektedir. Aynı zamanda yapay zekâ hatalı pozitif vakaları, yani normalde geçerli olan işlemlerin reddedilmesi ihtimalini de azaltabilmektedir (örneğin, kredi kartı ödemesinin yanlışlıkla reddedilmesi gibi). Böylece müşteri memnuniyetinin artmasına da katkı sağlamaktadır. [26] Şunu da belirtmek gerekir

---

25 Buckley, R. P./Zetzsche, D. A./Arner, D. W./Tang, B.: *Regulating Artificial Intelligence in Finance: Putting the Human in the Loop*, UNSWLRS 2023, C. 29, s. 49.

26 OECD, 2021, s. 29. Yapay zekâ teknolojilerinin finans sektöründe kullanılmasına ilişkin farklı taksonomilere ilişkin güncel ve ayrıntılı bir çalışma hk. bkz. Bahoo, S./Cucculelli, M./Goga, X./Mondolo, J.: *Artificial Intelligence in Finance: A Comprehensive Review Through Bibliometric And Content Analysis*, SN Bus Econ 2024, C. 4, S. 23, s. 25 vd. Bu çalışmada yazarlar on ana kullanım amacı belirleyerek şu tespitlerde bulunmaktadır: *Bu kapsamlı incelemeden, yapay zekânın mükemmel bir piyasa tahmincisi olarak kabul edilebileceği ve bilgi asimetrisini ve oynaklığını en aza indirerek piyasa istikrarına katkıda bulunduğu ortaya çıkıyor; bu, doğru performans değerlendirmeleri ile sonuçlanır. Ayrıca risk yönetimi alanında yapay zekâ hem kurumsal hem de finansal kurumlarda iflas ve kredi riski tahminine yardımcı olur. Dolandırıcılık tespiti ve erken uyarı modelleri tüm finansal sistemi izliyor ve gelecekteki yapay piyasa gözetimine yönelik beklentileri artırıyor. Bu durum küresel finansal krizlerin ya da beklenmeyen finansal çalkantıların önceden tahmin edilip önlenebileceğini gösteriyor.* Bkz. s. 39.

ki, Devlet otoriteleri, banka ve diğer finans tam olarak ne kadar ve hangi alanlarda yapay zekâ kullandığına dair resmi bir bilgiye sahip olamaz. Zira bu finans sektöründe faaliyet gösteren kuruluşların, yapay zekâ mekanizmalarının kullanımı bilgilendirmede bulunma gibi bir yükümlülüğü bulunmamaktadır. Bu tür kullanım verileri, kamuoyuna yapılan açıklamalar, piyasa raporları ve diğer resmi olmayan kaynaklardan elde edilmektedir.[27]

Tüm sektörlerde olduğu gibi, finans sektöründe de üretken yapay zekânın (GenAI) yaygınlaşması itici bir güç meydana getirmiştir. Nitekim üretken yapay zekâ araçları, anlık ve devam eden eğilimleri ortaya çıkarma yetisine sahiptir ve bu da gerçek zamanlı izleme ve tahmine olanak tanımaktadır. Üretken yapay zekâ araçları gelişmiş bir mimariye sahiptir ve sıralı verileri işleyip öğrenme yeteneği sayesinde bağlamsal farkındalıkla duygu analizi sağlayabilmektedir.28 Bu nedenle GenAI teknolojilerindeki gelişmelerin finans sektöründe yapay zekâ kullanımını daha da artırması beklenmektedir. Finansal hizmet sağlayıcılar, GenAI teknolojilerinin yeteneklerini ve bunların geniş bir uygulama yelpazesine nasıl uyarlanabileceğini keşfetmekte hızlı davranmıştır. Nitekim GenAI çok büyük ve çeşitli veri kümelerini işleme ve erişilebilir ve kolayca kullanılabilen biçimlerde (konuşma dahil) içerik oluşturma yeteneğine sahiptir. Bu nedenle, finansal kurum ve kuruluşların verimliliğini artırma ve müşteri deneyimlerini iyileştirme, risk azaltma ve uyumluluk raporlaması gibi aşamalarda fayda sunabilmektedir.

GenAI risk ve tehditlerin daha hızlı tespiti için tahmine dayalı modellerin uygulanmasına imkân tanımaktadır. Ayrıca siber güvenlik risklerine daha verimli yanıt verilmesini de mümkün kılmaktadır. Bununla birlikte, GenAI'in finans sektöründe konumlandırılmasının, sektör ve denetleyici otoriteler tarafından tam olarak anlaşılmasını gerektiren kendine özgü riskleri de bulunmaktadır.[29]

Finans sektöründe yapay zekâ araçlarının kullanılmasının mahremiyet ve kişisel verilerin korunması açısından ne gibi riskler ortaya çıkardığına geçmeden önce, finans sektöründe hangi iş ve işlemlerde yapay zekâ teknolojilerinden nasıl faydalanıldığının açıklanması yararlı olacaktır.

---

27 OECD, 2024, s. 13.

28 Linklaters: *"Artificial Intelligence in Financial Services: Managing machines in an evolving legal landscape", (https://lpscdn.linklaters.com/-/media/files/insights/2019/september/linklatersartificialintelligenceinfinancialservicesmanagingmachinesinanevolvinglegallandscapesept201.ashx?rev=2c497d44-32d1-42e4-8f1c-f4f6eb272b82&extension=pdf&hash=6B9FB3353FA1C5C0B0E936862ED46887*, E.T.: 06.07.2024), s. 5.

29 IMF, Fintech Notes, s. 4.

A. BORÇ VERME (CREDIT INTERMEDIATION)

Bankalar, veri biliminin doğru ve hedefe yönelik tahmine dayalı analitik araçlarından yararlanarak kredi verme süreçlerine ilişkin kararların alınmasını önemli ölçüde hızlandırabilmektedir. Ayrıca, makine öğreniminin gücünden yararlanarak ürünlerin geliştirilmesi, finansal hizmetler ve operasyonların yürütülmesi çerçevesinde veriye dayalı kararlar alma potansiyeline sahiptir. Teknik açıdan bakıldığında yapay zekâ, özellikle makine öğrenmesi ve gelişmiş analitik modeller, bankaların önceden kullanılmayan veri türleriyle daha doğru tahminlerde bulunmasına ve tüketici verilerinin analizinde yeni algoritmaların kullanılmasına imkân tanımaktadır.[30] Bankalar ve FinTech kredi sağlayıcıları potansiyel borçluların kredi değerliliğini değerlendirmek ve sigortalamaya ilişkin kararları vermek için yapay zekâya dayanan modelleri ve büyük veri uygulamalarını sıklıkla kullanmaya başlamıştır.

Aşağıda incelenecek faydalardan hareketle, geleneksel "manuel" kredi değerlendirmesinin yerini, yapılandırılmamış (*unstructured*) ve zamana uyum sağlayan verilerle başa çıkabilen makine öğrenimi alabilecektir. Bu makine öğrenmesi yöntemleri, kabul görmüş ve yerleşik banka politikalarını ihlal etmeden niteliksel bilgilerden (tüketim kalıpları gibi) ve kredi geçmişinden faydalanabilmektedir.[31]

Yapay zekâ, özellikle makine öğrenimi, büyük verinin bilgi gücünden yararlanarak kredi puanlama ve kredi verme yoluyla FinTechlerin gelişimini teşvik etmektedir.[32] Bu yapay zekâ modelleri, geleneksel kredi bilgilerini; çevrim içi ticaret faaliyetleri, kamu kayıtları, harcama alışkanlıkları, coğrafi konumlar, sosyal medya verileri, yerleşim yeri ve ödeme ve açık bankacılık girişimleri aracılığıyla erişilebilen işlem ayrıntılarına ilişkin büyük veri setleriyle karşılaştırarak çalışmaktadır.[33] Böylece tüketim alışkanlıkları ve ödeme istekliliği gibi niteliksel faktörlerin de dikkate alınması mümkün hale gelmiştir. Mesela, yapay zekâ sayesinde bankalar sosyal medya verileri gibi yeni veri türlerini kullanarak müşterinin riskliliğiyle ilgili daha doğru bir değerlendirme yapabilmektedir. Ayrıca bu modeller kredi kararları-

30 Königstorfer/Thalmann, s. 5.

31 Nguyen/Sermpinis/Stasinakis, s. 532.

32 Nguyen/Sermpinis/Stasinakis, s. 532.

33 Mohun, P.: "Regulating Artificial Intelligence in the Finance Sector", University of Otago, a Thesis of Master of Laws, New Zealand, 2022, s. 24.

nın verilmesi için potansiyel borçluların kredi değerliliğini değerlendirebilmekte, belirli bir kredi başvuru sahibine teklif edilecek faiz oranlarını belirleyebilmekte ve borçlular arasındaki birbirine bağlılığın derecesini artan bir hızla ve azalan maliyetlerle tespit ve analiz edebilmektedir.[34] Geleneksel kredi puanlama sistemlerine göre, maliyet ve zaman açısından verimli olmaları, aynı zamanda daha az kısıtlayıcı ve daha şeffaf olmaları gibi avantajları da bulunmaktadır.[35] Ayrıca, yapay zekâ destekli karar alma modelleri, uyarlanma ve öngörüler bakımından daha elverişlidir.[36]

Makine öğrenmesi sayesinde kredi değerliliğinin daha hızlı ve doğru bir şekilde tespit edilmesi, tüketicilere verilen krediler bakımından zaman zaman gündeme gelen ayrımcılığı ortadan kaldırabilir ve tüketicilerin krediye erişimini kolaylaştırabilir. Mesela bir kişinin kredi puanlarının bulunmadığı, ya da kişiye ilişkin sınırlı bilginin mevcut olduğu bir senaryoda, makine öğrenmesi algoritmaları bu kişinin borç ödeme yeteneğini ve isteğini doğru bir şekilde tespit edebilir.[37] Böylece teknolojinin gelişmesi öncesinde verilmesi mümkün olmayan kredi kararlarının verilmesi mümkün hale gelmektedir. Bu sayede, daha fazla kişiye kredi verilmesi sağlanarak bankanın müşteri portföyünü genişletmesi imkânı da söz konusu olmaktadır.[38] Yapay zekâ algoritmalarının geleneksel modellere kıyasla kredi riski belirlemesi yapmak bakımından daha doğru veriler sunduğu ve böylece risk yönetimi için daha uygun araçlar oldukları belirtilmektedir.[39]

Yapay zekâ sistemleri tüm müşteri kredi yaşam döngüsünü takip ederek, borçlarını geri ödemede temerrüde düşmesi muhtemel müşteriler hakkındaki erken sinyalleri tespit edebilmektedir. Böylece bankaların ve kredi kuruluşlarının riskleri ve maliyetleri azaltmasına, tahsilatları optimize etmesine ve müşteriyi elde tutma yoluyla karlarını artırmasına yardımcı olmaktadır.[40] Ayrıca, finansal aracılar dolandırıcılık tespiti ve borçlular

---

34 Mohun, s. 24.

35 Nguyen/Sermpinis/Stasinakis, s. 519; FSB, s. 12.

36 Congressional Research Service: *"Artificial Intelligence and Machine Learning in Financial Services", (https://crsreports.congress.gov/product/pdf/R/R47997*, E.T.: 06.07.2024), s. 6.

37 FSB, s. 12.

38 Königstorfer/Thalmann, s. 6; Artzt, M. /Dung, T. V.: *Artificial Intelligence And Data Protectıon: How To Reconcile Both Areas From The European Law Perspective*, Vietnamese Journal of Legal Sciences 2022, C. 7, S. 2, s. 55.

39 Königstorfer/Thalmann, s. 6.

40 Mohun, s. 25.

arasındaki birbirine bağlılığın derecesini analiz etmek için de yapay zekâ tabanlı sistemler kullanmaktadır ve böylece kredi portföylerini daha iyi yönetmeleri mümkün olmaktadır.[41]

Özellikle üretken yapay zekâ konusunda yaşanan gelişmeler, finansal kararlar verilmesi, özellikle kredi talebi değerlendirilmesi süreçlerinde yapay zekânın kullanımını daha da belirgin hale getirmiştir. Bu çerçevede, hangi müşteriye hangi şartlarda borç verileceğinin belirlendiği algoritmik kararlar da ön plana çıkmaktadır. [42]

B. VARLIK VE SERVET YÖNETİMİ

Varlık/portföy yönetimi, daha büyük varlık yöneticileri ve kurumsal yatırımcılara finansal varlıklarını dengeleme, yeniden yapılandırma ve tahsis etme konusunda yardımcı olunmasını ifade etmektedir. Makine öğrenmesi modellerinin büyük veriyle[43] (*Big Data*) beslenmesi sayesinde, varlık yöneticilerine, portföy tahsisi ve/veya hisse seçimi konusunda karar alma sürecinde öneriler sunulabilmektedir. Ayrıca derin öğrenme (*deep learning*) ve özellikle sinir ağları (*neural network*) modellerinin de varlık yönetiminde kullanılması mümkündür.[44] Yapay zekâ, varlık yöneticilerinin birden fazla kaynaktan gelen büyük miktarda veriyi sindirmesine ve çok kısa zaman dilimlerinde stratejilerine bilgi sağlamak için verilerden içgörüler elde etmesine olanak tanımaktadır.[45]

Varlık ve servet yönetimi kapsamında platformlar, yapay zekâ temelli araçlardan yardım alarak pazar trendlerini analiz etmekte, hisse tercihinde bulunmakta ve portfolyo oluşturup zaman içinde bu portfolyoyu güncellemektedir. Burada yapay zekâ araçlarının kullanılmasındaki amaç, müşteri deneyimini iyileştirmek, verimliliği artırmak, risk yönetimini geliştirmek

41 OECD, 2021, s. 29.

42 Dechert LLP: *"Artificial Intelligence: Legal and Regulatory Issues for Financial Institutions", (https://www.dechert.com/knowledge/onpoint/2023/4/artificial-intelligence--legal-and-regulatory-issues-for-financi.html,* E.T. 06.07.2024), s. 3; Congressional Research Service, s. 6.

43 Bankacılıkta büyük veriye örnek olarak gerçek zamanlı borsa bilgileri, uyarlanabilir piyasa ve tüketici duyguları, dolandırıcılık sinyalleri ve yüksek frekanslı finansal ve piyasa bilgilerine dayalı risk analizi verilebilir. Nguyen/Sermpinis/Stasinakis, s. 526. Amerika'da CRS tarafından sunulan raporda ise bazı firmaların kredi kararlarıyla ilgili olarak büyük veriden yararlandığı belirtilmektedir. Bkz. Congressional Research Service, s. 3.

44 Congressional Research Service, s. 10.

45 OECD, 2021, s. 22.

ve uzun vadeli hedef boyutlarını korumaktır. Böylece bir portfolyonun kişiselleştirilmesi[46] ve optimum varlıklardan oluşturulması sağlanabilmektedir.[47] Örneğin, giderek daha fazla serbest yatırım fonu, verileri analiz ederek, arz ve talep dengesizliklerine yönelik düzenlemeleri koruyarak ve stratejik varlık tahsisine yönelik hareketleri tahmin ederek yatırımları yeniden yapılandırmak için yapay zekâ araçlarını kullanmaktadır.[48]

Varlık yönetimi başlığı altında, portföy yönetimi ve risk yönetiminin yanı sıra, robo- tavsiye'den de bahsedilmesi gerekmektedir. Banka ve finans kuruluşlarının müşterilerine elektronik iletişim kanallarıyla hizmet sunmaları, hem zaman ve yer kısıtlamalarını azaltmış hem de finansal hizmetlere erişimle ilgili maliyetleri ve engelleri büyük ölçüde ortadan kaldırmıştır. Tüketiciler artık standartlaştırılmış finansal hizmetleri kendi kendilerine elde edebilme becerisini kazanmış olmalarına rağmen, finansal tavsiyelerin alınması, yine de banka veya aracı kurum personeliyle temasa geçilmesini zorunlu kılmaktaydı. İşte bu noktada yapay zekâ destekli robotavsiye platformları devreye girmiş ve geniş çaplı birçok finansal araç konusunda karar verme süreçlerinin otomatikleştirilmesi aşamasında müşterilere destek olmaya başlamıştır.[49] Robo-danışmanlık platformlarının özellikle 2008 yılındaki global kriz sonrasında potansiyel yatırımcılara finansal tavsiye sunmak için kullanılmaya başlandığı belirtilmektedir.[50]

Varlık ve servet yönetimine yönelik FinTech çözümlerinin hızla büyüyen bir uygulaması olan robo-danışmanlık, algoritmalara ve modellere dayalı çevrim içi yatırım rehberliği ve portföy yönetimi hizmetlerini ifade etmektedir. Robo-danışman, finansal bir aracı platform tarafından işletilen yazılımı ifade etmektedir. Bu algoritmalar, yatırım tavsiyesi ve portföy yönetimi konusunda müşterilere hizmet sağlamaktadır.[51] Genellikle robodanışmanlık platformlarında doğal dil işleme (NLP- *natural language pro-*

---

46 WEF: *"The New Physics of Financial Services Understanding how artificial intelligence is transforming the financial ecosystem", (https://www3.weforum.org/docs/WEF_New_Physics_of_Financial_Services.pdf*, E.T.: 06.07.2024), s. 119.

47 Congressional Research Service, s.10.

48 Mohun, s. 21-22.

49 Piotrowski/Orzeszko, s. 968.

50 Mohun, s. 20.

51 IMF, Fintech Notes, s. 8; Maume, Phillip: Robo-advisors How do they fit in the existing EU regulatory framework, in particular with regard to investor protection?, 2021, *(https://www.europarl.europa.eu/RegData/etudes/STUD/2021/662928/IPOL_STU(2021)662928_EN.pdf),* s. 8.

cessing) ve büyük dil modelleri (LLM- *large language models*) gibi araçlar kullanılarak zaman, bütçe ve risk toleransı gibi faktörlerin dikkate alınmasıyla bir müşteri profili oluşturulmaktadır.[52]

Bu platformların temel amacı, insan müdahalesini en aza indirmek veya tamamen ortadan kaldırmak ve müşteriler için en uygun yatırım stratejilerini elde etmek için yalnızca bilgisayar programlarından yararlanmaktır. Robo-danışmanlar, müşterilere çok az veya hiç insan etkileşimi olmadan otomatik yatırım yönetimi, tasarruf ve finans elde etme imkânı sağlayan otomatik tavsiye platformlardır. [53] Yapay zekâ teknolojilerine dayanan robo-danışmanlık platformları, dijital kredilere daha kolay ve hızlı erişim sağlamaktadır.[54]

Robo-danışmanlık platformlarında müşterilerden genellikle finansal durumları ve hedefleri hakkında bir anket doldurmaları istenmekte ve robo-danışman bu verileri müşteriler için otomatik olarak yatırım yapmak amacıyla kullanmaktadır. Tipik bir robo-danışmanlık süreci ilk yatırımcının taranması; yatırım stratejilerinin uygulanması ve bu stratejilerin izlenmesi ve değerlendirilmesi olmak üzere üç aşamalı bir süreçten oluşmaktadır.[55] Tüketici verileri robo-danışmanlık platformları tarafından işlenerek müşterilerin ihtiyaçları anlaşılmakta ve risk toleransları belirlenmektedir. Böylece finansal plan yapılması, gözlenmesi ve gerektiğinde değiştirilmesi de mümkün hale gelmektedir.[56] Robo-danışmanlık platformları, düşük gelirli nüfuslar da dahil olmak üzere kitlesel pazar müşterilerine uygun maliyetli bir şekilde kişiselleştirilmiş ve hedefe yönelik yatırım tavsiyeleri sunarak geniş çaplı servet danışmanlığı hizmetleri sağlamaktadır. [57]

Robo-danışmanlık, kullanıcı dostu olması, otomatik süreçlere dayanması ve portföy yönetimini düşük maliyetlerle gerçekleştirmesi sayesinde geleneksel finansal hizmetlere kıyasla daha verimli bir alternatif sunmaktadır.

---

52 Congressional Research Service, s. 10.

53 Piotrowski/Orzeszko, s. 969.

54 Nguyen/Sermpinis/Stasinakis, s. 533.

55 Kaya, O.: *Robo-advice – a true innovation in asset management,* EU Monitor Global Financial Markets 2017, *(https://www.dbresearch.com/PROD/RPS_EN-PROD/PROD0000000000449125/Robo-advice_–_a_true_innovation_in_asset_managemen.PDF?undefined&realload=~/1Q36lmuqYi6YfCAYZpplbKyC2/ofAYg0Ui1BEPDySuGGB5tkh~RiLocsCFE7~O*, E.T.: 06.07.2024), s. 2.

56 OECD, 2020, s. 13.

57 IMF, Fintech Notes, s. 8.

Robo-danışmanlığın ayrıca finansal katılıma katkıda bulunma ve finansal okuryazarlık seviyeleri düşük olan kişilerin sermaye piyasalarına yatırım yapmasına yardımcı olabilme potansiyeli bulunmaktadır. Özellikle Z kuşağı müşterilerin geleneksel finansal kuruluşların alternatiflerine yönelmesinin temelinde, makine öğrenmesi etmenleriyle güçlenen robo-tavsiye yazılımlarının olduğu da belirtilmektedir.[58] Hatta yapay zekâdaki gelişmelerle birlikte robo-danışmanlık süreçleri müşterilere yüksek derecede doğruluk ve uygunluk garanti edebilirse, robo-danışmanlığın gelecekte geleneksel finansal danışmanları tamamlayan bir faaliyet olarak daha da yaygınlaşması muhtemeldir.[59] Bilinen finans kuruluşlarından olan Morgan Stanley 2023 yılında Open AI ile işbirliği yaparak finansal danışmanlara müşterilere hizmet verirken destek olacak bir araç geliştireceklerini açıklamıştır.

C. ÖDEMELER

Finans alanında yapay zekâ kullanılarak özellikle ödeme sistemlerindeki dolandırıcılığın tespit edilmesi ve önlenmesinde önemli aşama kaydedilmiştir. IoT'deki gelişmeler çerçevesinde, finansal dolandırıcılık genellikle mobil cihazlar veya çevrim içi platformlar aracılığıyla yapılan yetkisiz mobil işlemlerle ilişkilendirilmektedir. Yapay zekâ ve makine öğrenmesi, banka ve diğer finans kuruluşlarına sahte işlemleri tespit etme konusunda sağlam bir çerçeve sağlamaktadır.[60]

D. ALGORİTMİK TİCARET

Algoritmik ticaret, 1950'lerden itibaren kantitatif finansın (*quantitative finance*) bir alt kümesi olarak var olmuştur. Matematik modelleri, bilgisayarlar ve telekomünikasyon ağları kullanılarak finansal menkul kıymetlerin alım satımı süreçleri otomatikleştirilebilmektedir.[61]

Ticaret firmaları, müşterilere satış yapma yeteneklerini geliştirmek amacıyla kullanılacak verileri elde etmek için yapay zekâ ve makine öğreniminden faydalanmaktadır. Örneğin geçmiş ticaret süreçlerindeki davranışların analiz edilmesi, müşterinin bir sonraki siparişini önceden tahmin

58 Nguyen/Sermpinis/Stasinakis, s. 519.

59 Kaya, s. 1.

60 Nguyen/Sermpinis/Stasinakis, s. 532.

61 Congressional Research Service, s. 11.

etmeye yardımcı olabilmektedir. Ticaret süreçlerinde üretilen büyük miktarlarda veri, makine öğrenimi araçlarının etkili bir şekilde çalışması için gereklidir.[62]

Yapay zekâ ayrıca ticaret stratejileri konusunda öneride bulunmak ve öngörülerde bulunan, bir sonraki eylemi belirleyen ve ticareti gerçekleştiren otomatikleştirilmiş ticaret sistemlerini güçlendirmek için de kullanılabilir. Yapay zekâdan yararlanan ticaret sistemleri tamamen kendiliğinden, yani herhangi bir insan müdahalesi olmaksızın ticaretin tespit ve icra aşamalarını sonuçlandırmak için derin öğrenme ve olasılıksal mantık gibi tekniklerden faydalanmaktadır.[63] Bu sayede ticaret işlemlerinin daha hızlı ve daha düşük maliyetlerle tamamlanması mümkün olmaktadır.

Ticaretin gerçekleştirilmesinden önceki aşamalarda yapay zekâdan yararlanılarak risklerin ve maliyetlerin hesaplanması süreleri hızlandırılabilir. Ticaretin gerçekleştirilmesi sırasında yine maliyetlerin düşmesini sağlayacak uygun şartların ne olduğunu tespit edecek veriler analiz edilebilir. Ticaret işleminin gerçekleştirilmesi sonrasında ise, gelecekteki analizlerde kullanılmak üzere veriler toplanabilmektedir.

Yapay zekâ tabanlı algoritmalar, sinyalin alınmasından stratejilerin geliştirilmesine ve bunların uygulanmasına kadar tüm eylem zincirine hizmet etmemektedir. Bu algoritmalar çoğunlukla verilerdeki gürültüden sinyal çıkarmak ve bu bilgiyi alım satımlarla ilgili karara dönüştürmek veya alım satım stratejilerini yürütmek için kullanılıyor. Gelecekte yapay zekâ tabanlı algoritmaların, ticaret sırasında kendi karar mantıklarının otonom ve dinamik olarak ayarlanmasına olanak tanıyarak insanı tamamen döngünün dışına çıkarabileceği öngörülmektedir. Bununla birlikte, yapay zekânın ticarette kullanılmasının, yasa dışı ticaret stratejileri geliştirilmesi riskini artırabileceğinin de altı çizilmelidir.[64]

E. BLOKZİNCİRİ TEMELLİ FİNANS

Yapay zekâ ve blokzinciri entegrasyonu sanayi devriminin son aşaması olan Endüstri 4.0 ve internetin yeni dönemi olan Web 3.0'ın temelleri olarak görülmektedir. Bu entegrasyonun finans alanında da önemli sonuçları

62 FSB, s. 18.

63 OECD, 2021, s. 24.

64 OECD, 2023, s. 11-12.

vardır. Bu çerçevede bazı yapay zekâ uygulamaları blokzinciri sistemlerinde kullanılarak örneğin risk yönetimini kolaylaştırılabilir. Ya da dağıtık defter çözümlerinin bazı yapay zekâ mekanizmalarında kullanılması, örneğin veri yönetimini kolaylaştırabilir.

Blokzincirinin en önemli uygulamalarından biri olan akıllı sözleşmelerin yapay zekâ desteği ile birlikte daha da otonom hale geleceği ve sahip olduğu asıl potansiyele kavuşacağı belirtilmektedir.[65] Akıllı sözleşmeler, önceden belirlenmiş olan şartlar gerçekleştiğinde, belirlenmiş olan sonucu otomatik olarak gerçekleştiren kod parçalarıdır. İsimlerinin aksine, akıllı olmaları, yapay zekânın kullanılmasını zorunlu kılmamaktadır. Bununla birlikte, akıllı sözleşmelerin yapay zekâ ile desteklenmesi halinde akıllı sözleşme kodunun değişen piyasa şartlarına göre dinamik bir şekilde yapılanması mümkün olabilecektir. Zira yapay zekâ desteği ile, kendi kendine öğrenen ve insan müdahalesine gerek kalmadan ilişki şartlarında değişiklik yapabilen akıllı sözleşmelerle karşılaşmak mümkün olacaktır. Yapay zekâ özellikle risk yönetimi ve hataların tespiti noktalarında akıllı sözleşmelerin yeteneklerini geliştirme potansiyeline sahiptir.

Blokzincirlerindeki yapay zekâ entegrasyonu, belirli finansal hizmetlerin sağlanmasında otomasyonu ve verimliliği artırabilir. Bu durum merkeziyetsiz finans (DeFi) uygulamalarının geliştirilmesine de yardımcı olmaktadır. Yapay zekâ modellerinin devreye girmesi, merkeziyetsiz olarak sunulan ürün ve hizmetler genelinde kişiselleştirilmiş önerilerin sağlanmasını, kullanıcıların çevrim içi verilerine dayalı kredi puanlaması gerçekleştirilmesini, yatırım danışmanlığı hizmetlerini ve finansal verilere dayalı ticareti destekleyebilir.[66]

Blokzinciri ve yapay zekâ entegrasyonunun finans alanında önemli dönüşümleri tetikleyici bir niteliğe sahip olduğu görüşü birçok kişi ve kurum tarafından paylaşılmaktadır. Hatta FinTech'in bankalar üzerindeki asıl yıkıcılığının eşler arası borç verme, akıllı sözleşme ve kripto paralardaki gelişimle ortaya çıkacağı düşünülmektedir. Bununla birlikte mevcut durumda yapay zekâ ve özellikle makine öğrenmesinin, dağıtık defter teknolojisi veya akıllı sözleşmelere kıyasla çok daha geniş çaplı bir kullanım alanına sahip olduğu da bir gerçektir.[67]

---

65 Çağlayan Aksoy, P.: *Akıllı Sözleşmelerin Dünü, Bugünü ve Yarını: Karşılaştırmalı Bir Değerlendirme*, Vergi Dünyası 2022, C. 42, S. 494, s. 19.

66 OECD, 2021, s. 35. Daha ayrıntılı senaryolar için ayrıca bkz. WEF, New Physics, s. 117.

67 FSB, s. 32-33.

F. MÜŞTERİ DENEYİMİNİN İYİLEŞTİRİLMESİ

Müşteri deneyimi, dijital dünyada başarının anahtarı olarak görülmektedir. Zira müşterinin kazanılması kadar tutulması da önemlidir. Bir rekabet avantajı yakalamak için, müşteri deneyiminin kişiselleştirilmiş ve müşteriye özel olması hedeflenmektedir. İşte bu noktada yapay zekâ teknolojilerinin devreye girerek müşteri deneyiminin iyileştirilmesinde önemli bir rol oynaması beklenmektedir.[68]

Her ne kadar bankalarda karar verilirken genellikle tahminlere dayalı olarak hareket edilse de geçmişte bu kararlar sektörü çok iyi bilen ve deneyimli kişiler tarafından verilmekteydi. FinTech'in geliştiği dönemlerde, en önemli trendlerden biri veri analitiğinin özellikle makine öğrenmesi ve "alternatif verinin"[69] kullanılarak finansal hizmetlerin kişiselleştirilmesi ve otomatikleştirilmesi olmuştur.

Toplum giderek daha fazla ağa bağlandıkça, dijitalleştikçe ve verileştirildikçe tüketicilerin ürettiği veri hacminin de katlanarak arttığı bir gerçektir.[70] Veri analitiği ve özellikle makine öğrenmesi teknikleri pazarlama, kimlik doğrulama, finansal tavsiye verilmesi ve kredi puanlama gibi çeşitli alanlarda kullanılmaktadır. Sigorta sektöründe sözleşmelerin hem oluşturulması (primlerin belirlenmesi) hem de pazarlama süreçlerinde yapay zekâ etmenlerine başvurulmaktadır. Bu çerçevede yapay zekâ, müşteri deneyimini iyileştirmek, satış ve hizmet sunulması süreçlerini geliştirmek, daha hızlı talep işleme ve doğru bireysel risk bazlı sigortalama süreçlerini sonuçlandırmak için bir araç olarak kullanılmaktadır.[71]

Algoritmalardan yararlanılması suretiyle müşteri tanımlama ve kimlik doğrulama işlemlerini kolaylaştırmak, sohbet robotları ve sesli asistanlar aracılığıyla canlı çalışanları taklit etmek, müşteri ilişkilerini derinleştirmek ve kişiselleştirilmiş bilgiler ve öneriler sunmak da mümkün hale gelmiştir.[72] Müşteri deneyiminin iyileştirilmesi başlığı altında "chatbot"lardan

---

68 UXDA, The Future of Generative AI and ChatGPT in Banking, (https://theuxda.com/blog/ai-powered-contextual-cx-digital-banking-success-or-disaster, E.T.: 06.07.2024).

69 Alternatif veri= geleneksel olmayan finansal veri (tüketicinin Netflix ödemeleri) + finansal olmayan veri (perakende ve çevrim içi tarayıcı davranışı- hatta bir ödünç verenin web sitesiyle tüketicinin nasıl etkileşime geçtiğine ilişkin veriler).

70 Aggarwal, s. 869.

71 Nguyen/Sermpinis/Stasinakis, s. 533; Citi GPS, s. 48.

72 Artzt/Dung, s. 55; Citi GPS, s. 43.

(sohbet robotları) da bahsedilmesi gerekmektedir. Sohbet robotları, basit isteklere ve sorgulara anında yanıt vermek gibi danışmanlık hizmetleri sağlamak için müşterilerle etkili bir şekilde iletişim kurma kapasitesine sahip yapay zekâ tabanlı sanal asistanlardır. Bu otomatik programlar, müşterilerle doğal dillerde (metin veya ses yoluyla) etkileşime girmek için NLP teknikleri kullanmakta ve zaman içinde kendilerini geliştirmek için de makine öğrenimi algoritmalarından yararlanmaktadırlar. Sohbet robotları, bir dizi finansal hizmet sunan şirket tarafından, genellikle mobil uygulamalarında veya sosyal medyalarında sunulmaktadır.[73]

Sohbet robotları görünümünde ortaya çıkan yapay zekâ uygulamalarının önemli bir avantajı, kendi kişisel çıkarlarına dayalı olarak karar vermemesidir.[74] Ayrıca sohbet robotları finans hizmetlerine her gün her saat ulaşılmasını sağlamaktadır. Bunun dışında, chatbotlar, KYC süreçleri için gerekli olan süreyi azaltıp hataları ortadan kaldırarak yeni ürün ve tekliflerin müşterilere daha hızlı bir şekilde ulaştırılmasını da mümkün kılmaktadır.[75] Sohbet robotlarının üretken yapay zekâ teknolojilerindeki gelişmelerle birlikte daha iyi bir müşteri deneyimi sunarak daha fazla sorunun yanıtlanmasını sağlayabileceği; böylece müşterilerle daha etkili ve hızlı iletişim kurulmasının ve maliyetlerin azaltılmasının mümkün hale geleceği belirtilmektedir.[76] Zira üretken yapay zekâ, makineleri insanlar gibi iletişim kurma becerisi ile donatmakta ve insanlar tarafından yapılan fikir verme veya ikna etme gibi süreçlerin otomatikleştirilmesini sağlamaktadır.[77] GenAI saysinde sohbet robotlarının, muhatabın makine mi yoksa insan mı olduğunu ayırt etmeyi çoğu zaman zorlaştıran insan benzeri bir konuşma unsuruna sahip olacağı belirtilmektedir.[78]

G. FİNANSAL SUÇLARIN TESPİTİ VE ÖNLENMESİ

Yapay zekâ teknolojileri, finansal işlemlerde kara para aklamayı ve çevrim içi bankacılıktaki dolandırıcılık davranışlarını tespit etmek için kullanılarak ödeme ağlarını daha güvenli bir hale getirme potansiyeline sahiptir. Özellikle ticari bankaların ödeme sistemlerinin daha güvenli hale getiril-

73 FSB, s. 14.

74 Mohun, s. 23.

75 KPMG, s. 16.

76 Congressional Research Service, s. 7.

77 BIS, s. 10.

78 OECD, 2023, s. 16.

mesinde en çok önem arz eden alanlardan biri, hileli işlemlerin ve kara para aklamaya yönelik işlemlerin tespitidir. Finansal kuruluşların, kimlikleri doğrulamak, işlemleri izlemek, sahte hesapları tespit etmek ve şüpheli işlemler ve güvenlik tehditleri dahil olağandışı davranış kalıplarını işaretlemek için yeni müşteri katılım uygulamalarının bir parçası olarak tarama ve denetim çalışmaları yapması ve KYC[79] süreçlerini takip etmesi gerekmektedir. Zira tüketiciler, güvenli hesapları ve diğer finansal hizmetleri sağlayan bankaları tercih etmektedir.

Yapay zekâ, dolandırıcılık, siber saldırılar, kara para aklanması ve terörizmin finansmanıyla mücadele için şimdiye kadar uygulanan en uygun maliyetli ve hızlı araçlardan biri olarak görülmektedir.[80] Riskleri değerlendirmek, ödeme sahtekarlığını tespit etmek ve önlemek, AML (*anti- money laundering*/ kara parayla mücadele) süreçlerini iyileştirmek ve KYC kontrollerini gerçekleştirmek için yapay zekâdan yararlanılmaktadır. Zira yapay zekâ etmenleri, normalde insanlar tarafından fark edilmeyecek bazı düzensizlikleri tespit ve analiz etme yeteneğine sahiptir. İşlem miktarı, sıklığı ve coğrafi konum gibi faktörleri analiz edebilen yapay zekâ sistemleri, hile veya kara para aklamaya işaret eden olağan dışı davranışları tespit edebilmektedir.[81]

Yapay zekâ tabanlı aracılar, özellikle e-ticaret ve çevrim içi kredi kartı işlemleriyle ilgili kötü amaçlı işlemleri tespit etmek bakımından da oldukça etkilidir. Bu çerçevede, kredi kartı kullanıcılarının konum, işlem geçmişi ve alışveriş alışkanlığı verilerinin makine öğrenmesi algoritmaları aracılığıyla sistematik ve otomatik bir şekilde analiz edilmesi tercih edilmektedir.[82]

Yapay zekâ, anormallik tespiti fonksiyonu sayesinde, e-posta kimlik avı, kimlik hırsızlığı, kredi kartı hırsızlığı, belgede sahtecilik gibi birçok dolandırıcılık faaliyetinin önlenmesine de yardımcı olmaktadır. Birçok banka,

---

79 KYC (know-your-customer/ müşterini tanı) süreçleri genellikle maliyetli, zahmetli ve birçok hizmet ve kurumda oldukça tekrarlanan bir süreçtir. Makine öğrenimi, finansal hizmetler sunan şirketlerin uzaktan kimlik ön kontrollerini gerçekleştirmek için giderek daha fazla kullanılmaktadır. Ağırlıklı olarak (1) belgeleri tanımlayan görsellerin birbiriyle eşleşip eşleşmediğini değerlendirmek ve (2) hangi bireylerin veya uygulamaların ek incelemeye tabi tutulması gerektiğini belirleyen firmaların risk puanlarını hesaplamak için kullanıldığı belirtilmektedir. Financial Stability Board, s. 20.

80 Mohun, s. 34.

81 Citi GPS, s. 40.

82 Nguyen/Sermpinis/Stasinakis, s. 519.

gerçekleştirilen işlemleri analiz etmek, bunlara risk puanları atamak ve tüketicileri çeşitli profillere ayırmak için yapay zekâ uygulamalarını kullanmaktadır. Özellikle tüketici bankacılığı ürünleri sunan bankaların, kredi kartı işlemlerini gerçekleştirirken dolandırıcılık kalıplarını tespit etmek için özel bir algoritmadan faydalanması hayati bir önem taşımaktadır. Bu tür kredi kartı işlemlerinin ayrıntıları merkezi bilgisayarlara gönderilmekte ve bilgisayarlar daha sonra bireysel işlemin hileli olup olmadığına karar vermektedir. Bazı finansal kuruluşlar, otomasyona dayalı dolandırıcılık ve şüpheli etkinlik tespit sistemlerini geliştirmek için üretken yapay zekâ modellerinden de yararlanmaya başlamıştır.

II. FİNANS SEKTÖRÜNDE YAPAY ZEKÂ KULLANIMININ KİŞİSEL VERİLERİN VE MAHREMİYETİN KORUNMASI BAKIMINDAN DEĞERLENDİRİLMESİ

A. GENEL OLARAK

Yapay zekâ etmenlerinin kredi kararlarında, sigorta sözleşmelerinde, müşterilerle etkileşimde ve finansal süreçlerdeki hukuka aykırılıkların tespitinde kullanılması, finans sistemini daha verimli hale getirmektedir. Gerçekten de yapay zekâ teknolojisindeki gelişmeler, çok yüksek miktarda verinin hızla analiz edilmesine imkân tanımaktadır. Finans sektöründe yapay zekâ kullanımının pek çok avantajı olmakla birlikte, aynı zamanda dikkate alınması gereken önemli bazı riskler de söz konusudur. Aslında yapay zekâ teknolojilerinin finans sektöründe kullanılmasının ortaya çıkardığı politika meseleleri yeni değildir. Ancak teknoloji geliştikçe ve yaygınlaştıkça, riskler çeşitlenmekte ve yaygınlaşmaktadır.[83] Kullanılan verinin kalitesi, kullanılan yapay zekâ modelinin şeffaflığı, öngörülebilirliği ve açıklanabilirliğine ilişkin sorunlar ve siber güvenlik konuları bu risklerden sadece birkaçıdır. Aslında tüm bu riskler bakımından cevap aranan temel soru şudur: Mevcut kurallar, yeni ve inovatif AI/ML teknolojilerine uygulandığında adil ve uygun sonuçlar ortaya çıkmakta mıdır? Yoksa bu teknolojinin özelliklerini dikkate alan, yeni ve özel kurallar koyulması gerekmekte midir?

Finans sektörü gittikçe daha da yapay zekâ ve veri odaklı bir hale gelmektedir. Yapay zekâ yazılımları kullanıcılardan çok yüksek miktarda veri toplamaktadır. Bu veriler belirli bir kişiye ilişkin olduğunda, kişisel verilerin

83 Congressional Research Service, s. 13.

korumasına ilişkin kurallar uygulama alanı bulmaktadır. Verilerin toplanması, verilerin eğitim ve test amaçlı kullanılması ve son olarak yapay zekânın çalışmaya başlaması gibi aşamalarda kişisel verilerden yararlanılması gündeme gelmektedir. [84]

Gittikçe artan miktarda kişisel verinin ortaya çıkması ve analiz edilmesi kapasitesini belirleyen teknolojik gelişmeler nedeniyle tüketicilerin farkında olmadan veya bazen rızaları olmadan sağladıkları bilgi miktarı sürekli artmaktadır.[85] Finans sektörüne bakıldığında, tüketicilerin sağlamış oldukları verilerin akıbetini bazı ihtimallerde takip ettikleri görülmektedir. Bu çerçevede, tüketiciler örneğin, KYC süreçleri için verdikleri bilgilerin, belli bir ürünün alımını desteklemek için ve ödeme hizmetleri gibi belirli finansal ürünleri kullanırken sağladıkları verilerin akıbetinin çoğunlukla farkındadır. Bununla birlikte tüketicilerin, sağlayıcı tarafından müşteri ile etkileşim süreçlerinde kamuya açık alanlardan, örneğin sosyal medyadan toplanan verilerin veya kredi referans ofisi gibi bir üçüncü kişi ile paylaşılan verilerin akıbeti hakkında genellikle bilgi sahibi olmadıkları belirtilmektedir.[86]

Yapay zekâ sistemlerinde kullanılan verilerin hacmi, kolay erişilebilir olması, sürekliliği ve bazen hassas veri niteliği taşıması kişisel verilerin korunması ve mahremiyet endişelerini artırabilmektedir. [87] BigTech şirketleri, daha iyi finansal hizmetler sunmak adına yapay zekâ odaklı modelleri besleyen büyük miktardaki müşteri verilerine ücretsiz erişimden gittikçe daha fazla yararlanmaktadır.[88] Kişisel verilerin toplanması ve kullanılmasına ilişkin genel kaygıların yanı sıra, büyük veri kümelerinden çıkarımlar yapılması, makine öğrenimi modellerinde gizliliğin korunmasını sağlayan "aydınlatma ve rıza" uygulamalarının ne kadar yerinde olduğu ve sınır ötesi veri akışıyla ilgili sorular da ortaya çıkmaktadır. [89]

---

84 OECD, 2020, s. 9.

85 OECD, 2020, s. 9.

86 OECD, 2020, s. 9.

87 OECD, 2021, s. 31; IMF (2021**)** Powering the Digital Economy: Opportunities and Risks of Artificial Intelligence in Finance, *(https://www.imf.org/en/Publications/ Departmental-Papers-Policy-Papers/Issues/2021/10/21/Powering-the-Digital-Economy-Opportunities-and-Risks-of-Artificial-Intelligence-in-Finance-494717,* E.T.: 06.07.2024), s. 17.

88 OECD, 2021, s. 31.

89 OECD, 2021, s. 38.

Finansal işlemlerin çeşitli aşamalarında karmaşık algoritmaların kullanılması, tüketicilere karşı şeffaflığın sağlanamamasına da yol açabilmektedir. Makine öğrenimi algoritmalarının bu "kara kutu"[90] özelliği, kişisel verilerin ve mahremiyetin korunması bakımından ortaya çıkan endişeleri artırmaktadır. Kredi puanlarını belirlemek ve kredi tahsis kararlarını vermek için makine öğrenimi kullanıldığında, kredi puanını ve itiraz edilmesi durumunda ortaya çıkan kredi kararını müşterilere ve denetçilere açıklamak zorluk teşkil etmektedir. [91] Bu durum, 6698 sayılı Kişisel Verileri Korunması Kanunu (6698 sayılı Kanun) ve Avrupa Birliği Genel Veri Koruma Tüzüğü'nde (GVKT-*General Data Protection Regulation*) benimsenen şeffaflık ilkesiyle bir çelişki oluşturmaktadır.[92]

Tüketicilerin finansal ve finansal nitelik taşımayan verileri, bazen onlar anlamadan ve aydınlatmaya dayalı rızaları alınmadan paylaşılmakta ve kullanılmaktadır. Herhangi bir veri kullanımının yasal dayanağı olsa da tüketiciler, verilerinin nasıl işlendiği ve nerede kullanıldığı konusunda her zaman bilgilendirilmemektedir. Ayrıca, rıza alınmadan önce yeterli düzeyde aydınlatma yapılmamış da olabilmektedir. Gelişmiş izleme yöntemleriyle çevrim içi etkinliğin takibindeki artış ve üçüncü kişi sağlayıcılar tarafından yapılan veri paylaşımı da bu tür riskleri artırmaktadır. Coğrafi konum verileri veya kredi kartı işlem verileri gibi müşteri tarafından sağlanmayan gözlemlenen veriler, gizlilik politikası ve veri koruma yasalarının olası ihlali riski taşıyan veri kümelerinin başlıca örnekleridir.[93]

Günümüzde bankalar ve finansal kuruluşlar, müşterilerinin verilerini gizli tutmakla yükümlüdür. Bununla birlikte, bazı istisnai durumlarda müşterilerin verilerinin devlet kurum ve kuruluşlarıyla paylaşılması gerekliliği ortaya çıkabilmektedir. Bunlara örnek olarak, vergi kaçırma, kara para aklama ve terörizm finansmanı gibi suçlarla mücadele gösterilebilir. Bu

---

90 Kara kutu burada şunu ifade etmektedir: makine öğrenimi karmaşıktır ve yorumlanması kolay değildir. Girdi sinyallerini tespit etmek her zaman mümkün olmayabilir. Ayrıca tek bir model olmaktan öte birçok modelin bir araya getirdi bütünü ifade etmektedir. Bu özellikler nedeniyle, finans şirketlerinde makine öğrenmesi yöntemleri kullanıldığında, finansal kuruluşlarda çalışan kişilerin, ticaret ve yatırımlarla ilgili kararlara nasıl varıldığını anlamaları mümkün olmamaktadır. IMF, 2023, s. 15.

91 FSB, s. 13.

92 Christodoulou, P./Konstantinos, L.: *Data Protection Issues in Automated Decision-Making Systems Based on Machine Learning: Research Challenges, Network* 2024, C. 4, *(https://doi.org/10.3390/network4010005*, E.T.: 06.07.2024), s. 97.

93 OECD, 2021, s. 38.

meşru sebepler kapsamında bankadan müşteri bilgilerini alan kurum ve kuruluşlar, yine sır saklama yükümlülüğü altındadır ve müşteri bilgilerini sadece amaçla sınırlı olarak kullanabilmektedir.[94] Belirtmek gerekir ki, GVKT ve diğer veri koruma mevzuatları kapsamında ortaya çıkan veri koruma rejimi, bankaların sır saklama yükümlülüğünden (*duty of confidentiality*) daha geniş kapsamlıdır. Zira, kişisel veri, kimliği belirli veya belirlenebilir bir gerçek kişiye ait olmak kaydıyla kamusal veya kamuya açık olmayan, finansal veya finansal olmayan tüm verileri kapsamaktadır.[95]

Kişisel verilerin korunmasına ilişkin olarak yürürlükte olan düzenlemeler çerçevesinde finansal kuruluşlarla işlem yapan tüketiciler, kendileri ile ilgili işlenen kişisel veriler hakkında bilgi almayı ve bu verilere erişmeyi (GVKT m. 15) veya kişisel verilerinin düzeltilmesini (GVKT m. 16) isteyebilecekleri gibi; kişisel verilerinin kalıcı olarak silinmesini talep hakkını (unutulma hakkını) (GVKT m. 17), sadece otomatikleştirilmiş bir işlemeye dayalı olarak alınan kararlara itiraz etme ve kararda bir insan müdahalesi elde etme hakkını (GVKT m. 21-22) da kullanabilecektir. Diğer taraftan, otomatikleştirilmiş bireysel karar alma süreçlerinin varlığı ve mantığı hakkında bilgi edinme hakkı da GVKT ile genel olarak tanınmaktadır (GVKT m. 13(2)f, 14(2)g, 15(1)h). Bunların yanı sıra, tüketiciler, veri ihlalinden gecikmeksizin haberdar olma (GVKT m. 32), kişisel verilerini "yapılandırılmış, yaygın olarak kullanılan ve makine tarafından okunabilen biçimde" elde etme ve "bu verileri başka bir veri sorumlusuna iletme" (veri taşınabilirliği) gibi haklara da sahiptir (GVKT m. 20).

Yukarıda açıklandığı üzere, GVKT m. 13 (2) (f), m. 14 (2) (g) ve m. 15 (1) (h)'in özdeş ifadelerine göre, veri sorumlusu, profilleme de dahil olmak üzere otomatik karar vermenin varlığı ve asgari olarak, yürütülen mantığa ilişkin anlamlı bilgiler ile söz konusu işleme faaliyetinin ilgili kişi açısından önemi ve öngörülen sonuçları hakkında bilgi vermelidir. Buna karşılık, ne 6698 sayılı Kanun'un 10. maddesinde, algoritmik karar vermenin gerçekleşeceğine ilişkin özel olarak aydınlatma yapılması gerektiği ifade edilmiş ne de 11. maddesinde ilgili kişilere algoritmik karar verme yönteminin kullanılıp kullanılmadığına dair bilgi isteme hakkı tanınmıştır. 6698 sayılı Kişisel Verileri Koruma Kanunu'nun münhasıran otomatik yollarla alınan kararlara ilişkin tek maddesi "İlgili kişinin hakları" başlıklı 11. maddesinin birinci fıkrasıdır. Buna göre, "Herkes, veri sorumlusuna başvurarak kendi-

94 Aggarwal, s. 862 vd.

95 Aggarwal, s. 865.

siyle ilgili; […] g) İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme […] haklarına sahiptir."[96] Her ne kadar 6698 sayılı Kanun'da algoritmik karar verme yönteminin kullanılıp kullanılmadığına dair bilgi isteme hakkı GVKT'de olduğu gibi açıkça tanımlanmamış olsa da 6698 sayılı Kanun'un m. 11/1-g'de öngörülen itiraz hakkının kullanılabilmesi ancak bu hususta bilgi sahibi olunması ile mümkün olabileceğinden algoritmik karar vermeye ilişkin bilgi isteme hakkının da itiraz hakkına içkin olduğu kabul edilebilir. Nitekim bu, 6698 sayılı Kanun'un m. 11/1-a'nın da bir uzantısı niteliğindedir.

Çalışmamızda çeşitli vesilelerle değinildiği üzere, makine öğrenmesi yöntemleri, özellikle de derin öğrenme, büyük, yapılandırılmamış ve yüksek boyutlu veri kümelerini ayrıştırmak ve bir hedef değişkenin (tüketicinin kredi itibarı gibi) tahmin edilmesiyle ilgili özellikleri ve kalıpları tanımlamak için kullanılabilmektedir. Tüketicilerin GVKT kapsamındaki hakları ise, genellikle yapay zekâ ve makine öğrenmesi (AI/ML) yöntemleri kullanılarak verilerden elde edilen çıkarımları ve tahminleri kapsamamaktadır. Daha da önemlisi, tüketicilerin kişisel verilerinden hareketle yapılan çıkarımları kontrol edebilme yeteneğinin hem teknik hem de bilişsel sınırları bulunmaktadır. Veriler bir kez toplandığında, birleştirildiğinde ve makine öğrenmesi modellerine yerleştirildiğinde, bireysel bir tüketicinin kişisel verilerinin, verilere erişme, bunları silme veya taşıma hakkı gibi kontrol haklarını kullanmak amacıyla tanımlanması teknik olarak imkânsızdır.[97] Bu nedenle, yapay zekânın tüketicilerin finansmanındaki büyümesi, tüketicinin finansal gizliliğini özünde tehlikeye atmaktadır.

ABD'de CRS tarafından yayınlanan raporda, yapay zekâ modelleri geliştikçe, anonimleştirilmiş verilerin ilgili olduğu kişilerin tespitinin de kolaylaştığına dikkat çekilmiştir. Bu çerçevede, verilerin anonimleştirilmesi, yapay zekâ çağında veri koruma düzenlemeleriyle uyum içinde olamayabilir. Bu durum, hassas verilerin sayıca artmasına da yol açabilecektir. Yapay zekâ ve makine öğrenmesi modelleri büyük veri gibi alternatif verilerden yararlandıkça, sosyal davranışların ticari gözetim/denetime konu edilmesi de gündeme gelebilecektir.[98]

---

96 Aksoy, H. C.: *Kişisel Verilerin Korunması Yönüyle Algoritmik Karar Verme*, Kişisel Verileri Koruma Dergisi 2022, C. 4, S. 2, s. 82.

97 Aggarwal, s. 870.

98 Congressional Research Service, s. 17.

IMF'ye göre de yapay zekâ, katı bir şekilde regüle edilmiş olan finans sektöründe kullanıldığında mutlaka dikkate alınması gereken mahremiyet riskleri ortaya çıkmaktadır. Eğitim veri setlerinden veri sızıntıları ortaya çıkması, çıkarımlar yoluyla anonimleştirilmiş verilerin maskesinin kaldırılması ihtimali ve veriler kullanıldıktan ve ortadan kaldırıldıktan sonra eğitim veri setindeki bireyler hakkındaki bilgilerin makine öğrenmesi araçları tarafından hatırlanması bu risklere örnek olarak gösterilmektedir. Bu kaygılar, makine öğrenmesi sistemleri ile ilgili veri kaynaklarının, gelişmiş gizlilik standartlarına uymasını gerektiren yasal ve düzenleyici çerçeveyi güncellemeye yönelik devam eden çabaların merkezinde yer almaktadır.[99]

B. GEN-AI MODELLERİNE ÖZGÜ YENİ ZORLUKLAR

GenAI teknolojileri bakımından da makine öğrenimindekine benzer ve daha önceden beri mevcut olan gizlilik ve mahremiyet sorunları gündeme gelmekle birlikte, aynı zamanda yeni ve kendine özgü endişeler de ortaya çıkmaktadır. GenAI araçları, özellikle büyük dil modelleri, terabaytlarca veriyle eğitilmektedir. Bu verilerin birçoğu internetten alınmakta ve çok fazla kişisel veri içermektedir. Büyük dil modelleri, bu verilerden hareketle ve verilen komutlara göre metinleri oluşturabilmekte, analiz ve kategorize edebilmektedir. Ayrıca düzeltme ve özetleme, kodlama, tercüme etme, müşteri hizmeti sunma ve sentetik veri oluşturma gibi kullanımları da bulunmaktadır.[100]

Finansal hizmet sağlayıcılar, müşterilerin çıkarına en uygun şekilde hareket etmekle yükümlüdür. Bu aynı zamanda onları yanıltıcı çıktılardan, yanlış bilgiden veya özellikle GenAI araçlarıyla ilgili finansal tüketicilere yönelik diğer risklerden korumak anlamına da gelmektedir.[101]

GenAI modelleri kullanıldığında, veri kalitesine ilişkin sorunlar, kullanıcıların modelle etkileşimde bulunurken modele sundukları girdileri de içerir. Bu durum, modelin özerk kendi kendine öğrenme becerisi ve kullanıcı ile model arasındaki geri bildirim döngüleri göz önüne alındığında önem taşımaktadır. Bu modellerde etkileşimde kullanıcıların sağladığı verilerin hacminin büyük olması, bu verilerin sürekli olarak AI sistemlerine akması

99 IMF, Fintech Notes, s. 5.

100 BIS, s. 7.

101 OECD, 2023, s. 10.

ve eğitim için kullanılan veri setlerinin boyutunun hızla büyümesi gibi ihlal risklerini artırır. Kullanıcılar tarafından modelle etkileşimde kullanılan istemler aracılığıyla sağlanan bilgiler, özel veya ticari gizli bilgileri açığa çıkarabilir ve model tarafından gelecekteki yinelemelerde veya eğitimlerde kullanılabilir. Özellikle LLM'lerde, kullanıcı tarafından girilen veriler ne kadar spesifik olursa, modelin sonucu o kadar doğru ve gizli veri sızıntısı riski de o kadar yüksek olmaktadır.[102]

Şu anda birçok GenAI modelinin, modelin geliştirilmesi ve eğitilmesinde kullanılan kişisel veriler bakımından ilgili kişilerin rızasını almadığı ve onların sunduğu verilerin hangi işlemlerde kullanılacağına ilişkin bildirim[103] sağlamadığı belirtilmektedir.[104] Bunun kişisel verilerin korunması hukuku açısından meşrulaştırılmasının yolu, "meşru menfaat testi"dir. Veri koruma otorite ve kural koyucularının, bu yapay zekâ araçlarını oluşturmanın faydalarının, verileri onları eğitmek için işlenen bireylerin çıkarlarından daha ağır basıp basmayacağı sonucuna varacağı ise açık değildir. [105]

Bu modelleri eğitmek için kamuya açık verilerin kullanılmasının hukuka uygun olup olmadığı ve büyük dil modelleri tarafından üretilen halüsinasyonların GVKT ve 6698 sayılı Kanun'daki doğruluk ilkesiyle uyumlu olup olmadığının da değerlendirilmesi gerekmektedir. Bilindiği üzere, GenAI modelleri halüsinasyonlara açıktır. Yapay zekâ halüsinasyonları, üretken yapay zekâ sistemlerinin gerçek veya doğru bilgilere dayanmayan çıktılar ürettiği durumları ifade etmektedir.[106] Bu halüsinasyonlar kullanıcıları yanıltabilmekte ve ilgili kişilerin veri güvenliği açısından potansiyel sonuçlar meydana getirebilmektedir.[107] Sentetik verilerle eğitilen yapay zekâ

---

102 OECD, 2023, s. 21.

103 Ozan Özparlak/Çetin, s. 1016.

104 Ozan Özparlak/Çetin, s. 1016.

105 Linklaters, s. 27.

106 OECD, 2024, s. 20.

107 Aktivist Max Schrems tarafından kurulan, Viyana merkezli kâr amacı gütmeyen bir kuruluş olan Noyb, ChatGPT'nin Schrems'in doğum gününü doğru olarak bildirememesinden ve bunun yerine bir tahminde bulunmasından şikayetçi olmuştur. Schrems'e göre chatbot, kullanıcılara bir isteği yanıtlamak için doğru verilere sahip olmadığını söylememektedir. Bilindiği üzere, bir kişinin doğum tarihi, GVKT kapsamında kişisel veri niteliği taşımaktadır. Buradan hareketle Noyb, chatbot'un davranışının gizlilik, bilgilerin doğruluğu ve yanlış bilgilerin düzeltilmesi hakkına ilişkin olarak GVKT'de yer alan temel ilkeleri ihlal etmektedir. Ayrıca ürünü geliştiren yapay zekâ firmasının yanlış yanıtları düzeltmeyi veya silmeyi reddettiğini ve işlenen verilerin, bunların kaynaklarının

modellerinin, daha sonra kişilerin haklarını veya menfaatlerini etkileyebilecek kararların alınmasında kullanılması durumunda bu husus özellikle önem taşımaktadır.[108]

Aynı şekilde, bireylerin verilerine erişimin engellenmesi veya silinmesine yönelik taleplerine imkân tanınması, eğer söz konusu kişisel veriler modele yerleştirilmişse, teknik ve lojistik açıdan zor olabilir.[109] Mesela, eğer bir kişi, unutulma hakkını kullanırsa, Gen-AI sisteminin sağlayıcısından unutulma hakkının tesisi amacıyla kişiyle ilgili tüm verileri silmek için terabaytlarca eğitim verisini taraması beklenmeli midir? Daha sonra bu veriler olmadan tüm modeli yeniden eğitmek gibi maliyetli bir süreci sistem operatörlerinin üstlenmeleri gerekmekte midir?[110]

IMF konuyla ilgili raporunda ayrıca şu hususa da dikkat çekmektedir: Kamuya açık GenAI sistemleri, sistemin yeteneklerini operasyonlarına dahil etmek isteyen finansal kuruluşlar için de önemli gizlilik sorunları meydana getirmektedir. Her kullanıcıyı otomatik olarak sürece "katmak" suretiyle GenAI sistemleri, eğitim ve yanıtlarında (çıktılarında) ince ayarlamalar yapabilmek için sürekli olarak kullanıcılardan sağlanan veri girdilerini kullanmaktadır. Dolayısıyla bu otomasyon, finansal kurum personelinin GenAI ile olan etkileşimleri sırasında sağladıkları hassas finansal verilerin ve kişisel bilgilerin sızma olasılığını artırmaktadır. Birçok GenAI sistemi, kullanıcılar tarafından sağlanan bilgi ve verilerin güvenliğini ve gizliliğini sağlayamadıklarını açıkça belirtmektedir.[111]

C. SİBER GÜVENLİK RİSKLERİ

Günümüz teknolojisinde, yapay zekâ yazılımları kullanıcılardan büyük miktarda veri toplamakta ve bu verileri şirketlerin sistemlerinde depolamaktadır. Bu durum, şirketlerin siber güvenlik açıkları kaynaklı veri ihlal-

---

veya alıcılarının kimler olduğu hakkında herhangi bir bilgi açıklamayacağını da ileri sürmüştür. Politico (2024), *ChatGPT's hallucinations draw EU privacy complaints, (https://www.politico.eu/article/chatgpts-hallucinations-get-eu-privacy-complaint/,* E.T.: 07.07.2024).

108 CEDPO: "*Generative AI: The Data Protection Implications CEDPO AI Working Group 16 October 2023", (https://cedpo.eu/wp-content/uploads/generative-ai-the-data-protection-implications-16-10-2023.pdf,* E.T.: 06.07.2024), s. 18, s. 23.

109 Linklaters, s. 6.

110 Linklaters, s. 28.

111 IMF, Fintech Notes, s. 5.

lerine karşı daha fazla önlem almalarını ve bu tür ihlalleri önlemek için tedbirler geliştirmelerini zorunlu kılmaktadır.

Bu çerçevede örneğin finansal kurumların eğitim veri setlerine müdahale edilerek yapay zekânın kararlarını veya kullanıcıya verdiği yanıtları etkileyebilecek durumlar (*data poisoning*) ortaya çıkabilir. Yapay zekâ yazılımları kelime ilişkilendirmelerine dayanmakta olup bağımsız bir doğrulama özelliği içermemektedir. Yanlış verilerin eğitim veri seti içine katılması, sistemin yanlış öğrenmesine ve yanlış sonuçlar üretmesine yol açabilmektedir. Bunun yanı sıra, şirketlere ait hassas bilgiler, ticari sırlar ve diğer gizli bilgiler (mali bilgiler, fikri mülkiyet vb.) yapay zekâ modellerine dahil olarak gerektiğinde yapay zekâ yazılımı tarafından yeniden üretilebilir. Bu durum, çalışanların bu bilgileri ihmal sonucunda veya kasıtlı olarak yapay zekâ modeline yerleştirmesi ya da harici aktörlerin şirketin bilgi teknolojileri sistemlerine sızarak belirli bilgileri ortaya çıkarmaya çalışması gibi yollarla gerçekleşebilir. Ayrıca, yapay zekâ araçları kullanılarak saldırılar başlatılması, ikna edici ve gerçekçi görünen oltalama (*phishing*) e-postaları oluşturulması veya karmaşık sosyal mühendislik saldırıları düzenlenmesi de ihtimal dahilindedir. Büyük dil modellerine dayalı yapay zekâ yazılımları, kullanıcı şifrelerini veya diğer hassas bilgileri tahmin etmek için kamuya açık bilgileri veya sosyal medya verilerini sorgulayarak sofistike tahminler yapabilir. Bu da kullanıcı hesaplarının güvenliğini tehlikeye atabilir.[112]

Tüm bu siber güvenlik riskleri dikkate alındığında finans sektöründe yapay zekâ kullanan veya sağlayanların, bu risklerin azaltılması için gerekli stratejiler ortaya koyması gerekmektedir. Risk tespit ve raporlama sistemleri, eğitim verilerinin sağlam bir şekilde koruma altına alınması ve veri mahremiyetinin sağlanması için stratejiler geliştirilmesi bu kapsamda sayılmaktadır.[113]

D. "ROBO-DANIŞMANLIK" VE KİŞİSEL VERİLER

Öncelikle belirtmek gerekir ki, otomatik karar verme prosedürleri makine öğrenmesi veya benzeri yapay zekâ teknolojileri kullanılmadan da uygulanabilmektedir. Bununla birlikte**,** yapay zekâ kullanılması borçlunun durumunun daha hızlı ve daha uygun maliyetlerle değerlendirilmesine olanak tanıdığından, kredi kararının daha hızlı verilmesini sağlamaktadır. Ancak

[112] Dechert LLP, s. 11.

[113] IMF, 2023, s. 17.

bu durum da kişisel verilerin kullanımı, veri gizliliği ve veri korumayla ilgili olanlar da dahil olmak üzere birçok farklı sorunu gündeme getirmektedir.[114] Zira robo danışmanlar, yatırımcıların geliri, diğer finansal verileri, yatırım deneyimleri ve riske karşı tutumları gibi birçok hassas veriye[115] erişmektedir.[116]

İlgili kişiler bakımından otomatikleştirilmiş karar verme süreçleriyle bağlantılı önemli bir hak, GVKT'nin 22. maddesinin 1. fıkrasında tanımlanmıştır: "İlgili kişi, kendisiyle ilgili yasal sonuçlar doğuran veya benzer şekilde önemli etkiler yaratan, yalnızca otomatik işlemeye dayalı bir karara tabi tutulmama hakkına sahiptir". Bu nedenle, GVKT hükümlerine göre, veri sorumluları, (i) meşru işleme ilkelerine (örneğin, şeffaflık, veri minimizasyonu vb.) uygun hareket ettikleri ve (ii) insan müdahalesi ve gerektiğinde karara itiraz etme gibi ek güvenceler sağladıkları sürece profilleme ve/veya otomatik karar verme işlemleri yapabilirler. Ayrıca, sürecin şeffaflığı gereği, ilgili kişi, baştan itibaren, kullanılan mantık ve öngörülen sonuçlar hakkında anlamlı bilgiler alabilmelidir (bkz. GVKT m. 13, f. 2(f)). Karar sürecinde insan müdahalesi, yalnızca GVKT'nin 22. maddesinin 2. fıkrasında belirtilen çok özel durumlarda atlanabilir; ancak bu istisnalar kesinlikle dar yorumlanmalı ve bu durumlarda bile diğer güvenceler sağlanmalıdır.[117]

GVKT, verilen kararın ilgili kişi üzerinde etkiler meydana getirdiği durumlarda, tamamen otomatikleştirilmiş karar verilmesi süreçlerini engellemeyi hedeflemektedir. Bu çerçevede, eğer karar verme süreçlerinde bir insan yer alıyorsa, burada otomatikleştirilmiş süreçler sonucunda verilen bir karar söz konusu değildir. Bununla birlikte, süreçte bir insanın yer aldığından bahsedilebilmesi için anlamlı ve etkili bir şekilde sürece dahil olması gerekir. Eğer açık rıza verildiyse, robo-danışmanlık kararı söz konusu olabilir ancak burada rızanın geçerli olması için eşik yüksektir. Robo-danışmanlık sonucundaki karar ayrıca bir sözleşmenin ifasıyla ilgili olduğunda da verilebilir. Mesela yeni bir müşteriyle ilgili kredi kontrollerinin yapılması bu kapsamda değerlendirilebilir.[118] Bu çerçevede, ilgili kişilerin menfaatlerinin korunması için, robo-danışmanlık sonucunda karar veril-

[114] FSB, s. 12.

[115] Hassas veri ifadesi, 6698 sayılı Kanun md. 6'da düzenlenen özel nitelikli veri ile eş anlamlı olarak kullanılmamaktadır.

[116] Ozan Özparlak/Çetin, s. 1014.

[117] Ayrıntılı bilgi için bkz. Aksoy, s. 76.

[118] Linklaters, s. 27.

mesine rıza gösterilmiş olsa bile ilgili kişilere bildirimde bulunulması, kararın bir insan tarafından değerlendirilmesi ve karara itiraz etme imkânının tanınması önem taşımaktadır.

Robo-danışmanlık süreçlerinde kullanılan makine öğrenmesi algoritmalarının eğitildiği veri kümelerinin kişisel veriler içermesi durumunda, özellikle bireylerin bu işlemenin farkında olmaması veya verilerinin eğitim dışı amaçlarla kullanılması durumunda daha fazla risk gündeme gelmektedir. Bireylerin kimliğinin belirlenmesi yapay zekâ araçlarının eğitimi için zorunlu bir unsur olmadığından ve bu nedenle amacı aşan işleme (*excessive processing*) faaliyeti teşkil edeceğinden, eğitim için kullanılan kişisel verilerin en aza indirilmesi ve anonimleştirilmesi çok önemlidir. Ancak anonimleştirmenin, makine öğrenimi algoritmalarının doğruluğunu etkileyebileceği ve gizlilik ile doğruluk arasında dikkatli yönetim gerektiren bir çatışma yaratabileceği de göz ardı edilmemelidir.[119]

E. FİNANS SEKTÖRÜNDE YAPAY ZEKÂ KULLANILMASI SÜREÇLERİNDE KİŞİSEL VERİLERİN VE MAHREMİYETİN KORUNMASI HAKKINDA GÜNCEL YAKLAŞIMLAR VE ÖNERİLER

1. Mahremiyet Artırıcı Teknolojiler (Privacy Enhancing Technologies)

Yapay zekâ ve makine öğrenimi uygulamalarda daha yaygın hale geldikçe, mahremiyeti artıran teknolojilerin (PET-*privacy enhancing technologies*) bu teknolojilerle entegrasyonu zorunlu hale gelecektir. PET'ler, gizliliği korumak amacıyla kişisel verileri ortadan kaldıran veya en aza indiren yazılım ve donanım çözümleridir. Bu sayede bilgi sisteminin işlevselliğinden ödün vermeden kişisel verilerin hukuka aykırı olarak işlenmesinin önlemesinde önemli araçlardır. PET'ler güvenli ve gizliliğe duyarlı yapay zekâ etmenlerinin geliştirilmesini kolaylaştırmakta, gizliliği korurken veri analizine ve makine öğreniminden yararlanılmasına da imkân tanımaktadır.[120] PET'ler kurum ve kuruluşların veri kullanımından sağladığı faydaları maksimuma çıkarırken müşteri bilgilerinin de güvende tutulması amacına hizmet etmektedir.

---

119 Christodoluou/Limniotis, s. 92.

120 Finextra (2024), *Privacy enhancing technologies: Key to win in today's evolving World, (https://www.finextra.com/blogposting/26348/privacy-enhancing-technologies-key-to-win-in-todays-evolving-world,* E.T.: 06.07.2024).

Diğer taraftan, mahremiyet artırıcı teknolojiler, yapay zekâ ile desteklendiğinde, özellikle hassas verileri korumak için güçlü çözümler sunmaktadır. Bu teknolojiler, veri gizliliğini korumak, veri güvenliğini artırmak ve sorumlu veri yönetimini teşvik etmek için önemli araçlar olarak nitelendirilmektedir. Bu teknolojiler, önemi giderek artan makine öğrenimi uygulamalarına entegre edildiğinde, "gizliliği koruyan makine öğrenimi" kavramı karşımıza çıkmaktadır.[121] Böylece kullanıcılar yapay zekâ ve makine öğreniminin tüm potansiyelinden yararlanabilmekte ve verilerin gücünden daha etkili bir şekilde değer elde edebilmektedir.[122]

Yapay zekâ uygulamalarında PET'ler, modelleri korumak ve bunların bir finans kurumunun güvenilir duvarları dışında da güvenli bir şekilde kullanılmasına olanak sağlamak gibi işlevleri de yerine getirebilmektedir. Böylece, diğer yargı bölgelerinde bulunan veya üçüncü kişilerin sahip olduğu veri kaynaklarından güvenli bir şekilde öngörüler elde etmek için makine öğrenimi modelleri kullanılabilir.[123]

Yapay zekâya dayalı sistemlerde PET'lerin kullanımına ilişkin çalışma yapan yazarlar, tipik bir yapay zekâ sisteminde hem sistemin sahibinin hem de sistem kullanıcılarının mahremiyet riskleri altında olduğuna dikkat çekmektedir. Yazarlara göre, sistemin sahibi, hem yapay zekâ modelini hem de modelin eğitildiği verileri korumayı amaçlamaktadır. Modelin korunması, modelin özelliklerinin gizli tutulmasının yanı sıra, modelin ve tahminlerinin kasıtlı olarak yanıltılma veya değiştirilmeye karşı bütünlüğünün korunmasını da içermektedir. Eğitim verilerinin korunması ise kullanıcıların model aracılığıyla verilerin özelliklerini keşfetmesini engellemek anlamına gelmektedir. Ayrıca, yapay zekâ sisteminin geliştirilmesi ve/veya bakımını yapanlar tarafından model veya eğitim seti ile ilgili herhangi bir verinin sızdırılmasını önlemeyi de kapsamaktadır. Sistemin kullanıcısı ise sisteme gönderilen ve sistem tarafından işlenen verileri korumak istemektedir. Bir kullanıcı, yapay zekâ sisteminden özel verileri kulla-

121 Bitsol Technologies (2023), *AI-Driven Privacy Enhancing Technologies (PETs) and Clarifying Misconceptions About It, (https://www.linkedin.com/pulse/ai-driven-privacy-enhancing-technologies-pets-clarifying-misconceptions/*, E.T.: 06.07.2024).

122 Enveil (2024), *International Banker: Unlocking the Power of Privacy Enhancing Technologies in Financial Services, (https://www.enveil.com/intl-banker-privacy-enhancing-technologies-in-financial-services/,* E.T.: 06.07.2024).

123 Enveil (2024), *International Banker: Unlocking the Power of Privacy Enhancing Technologies in Financial Services, (https://www.enveil.com/intl-banker-privacy-enhancing-technologies-in-financial-services/,* E.T.: 06.07.2024).

nılarak bir çıkarım yapılmasını talep ettiğinde, kişisel verilerinin korunacağından emin olmalıdır. Bunun için birçok durumda verilerin sistemin sahibi tarafından bile görülmemesinin sağlanması gerekmektedir. Yapay zekâ sistemleri, zamanla kullanıcıların özelliklerini ve davranışlarını öğrenme kapasitesine sahip olduğundan, kullanıcılar verilerinin istenmeyen şekillerde kullanılmayacağından emin olmalıdır.[124]

Mastercard tarafından hazırlanan ve PET'leri nasıl kullandıklarını, avantajlarını ve dezavantajları açıklayan izahnamede şu ifadeler yer almaktadır: "PET'lerin yeni olması aynı zamanda mevcut yasa ve düzenlemelerin bu tür yetenekler göz önünde bulundurularak tasarlanmadığı anlamına da gelir ve sonuç olarak PET uygulamalarının bu çerçeveler içerisinde nasıl ele alınması gerektiği net olmayabilir. Örneğin, PET'lerin, sınır ötesi veri aktarımlarına veya kişisel verilerin anonimleştirilmesine ilişkin sınırlamalar da dahil olmak üzere gizlilik ve veri koruma yasalarıyla nasıl bir ilişkisi olduğunun tespit edilmesi önem taşımaktadır. [125]

2. Finansal Kuruluşlara İlişkin Diğer Öneriler

Yapay zekâ yazılımını teknolojilerinde kullanmayı planlayan finans kurumları, kişisel verileri koruma hukukunun gerekliliklerine uyum sağlamak için bazı önlemler almak ve standartları oluşturmak zorundadır. İlk olarak, yapay zekâ yazılımını kullanırken kişisel verileri işlemek için yasal bir temel oluşturması önem taşımaktadır. Bu ilgili kişinin rızasının alınmasını, verilerin bir kuruluşun meşru çıkarları doğrultusunda işlenmesini veya verilerin yasal gerekliliklere uymak için işlenmesini içerebilecektir. İkinci olarak yalnızca belirlenen amaç için gerekli olan ilgili kişisel verilerin toplanması ve işlenmesi ile sınırlı kalınması önem taşımaktadır. Ayrıca, bireylerin kişisel verileri yapay zekâ yazılımı tarafından işlendiğinde kişisel verileri koruma hukuku tarafından sağlanan ilgili kişilere tanınan hakların engellenmemesi de dikkat edilmesi gereken bir noktadır. Son olarak, Türk hukukunda düzenlenmemiş olmakla birlikte GVKT uyarınca, yapay zekâ yazılımının kullanım amacının bireylerin hakları ve özgürlükleri açısından yüksek risk oluşturması muhtemelse Veri Koruma Etki Değerlendirmelerinin (DPIA-*data protection impact assessment*)

---

[124] d'Aliberti, L./Gronberg, E./Kovba, J.: *Privacy-Enhancing Technologies for Artificial Intelligence-Enabled Systems,* IWSPA '24, June 21, 2024, Porto, Portugal, *(https://arxiv.org/abs/2404.03509*, E.T.: 06.07.2024).

[125] Mastercard: *"Privacy enhancing technologies WHITE PAPER FEBRUARY 2024", (https://b2b.mastercard.com/media/z0pnu32l/privacy-enhancing-technologies-white-paper-final.pdf,* E.T.: 06.07.2024), s. 16.

uygulanması değerlendirilmelidir. DPIA'ler kuruluşların yapay zekâ yazılımını içerenler de dahil olmak üzere veri işleme faaliyetleriyle ilişkili riskleri tanımlamasına, değerlendirmesine ve azaltmasına yardımcı olmakta ve GVKT kapsamındaki hesap verebilirlik yükümlülüklerinin önemli bir parçasını teşkil etmektedir.[126]

Yapay zekâ modelleri tarafından alınan tüm kararlar ve öneriler için bankaların ve diğer finans kuruluşlarının uygun düzeyde açıklanabilirlik sağlaması önem taşımaktadır. Bankaların kararları nasıl aldığını tam olarak anlaması, doğrulaması ve açıklaması gerekmektedir. Bu bağlamda, bir kuruluşun yapay zekâ sisteminde işlenen kişisel verilerin korunmasına dair düzenleyici kurallar büyük öneme sahiptir.[127]

SONUÇ

Finansın dijitalleşmesi ve bu süreçlerde kişisel verilerin kullanılmasının tüketicilere düşük maliyetler ve finansal hizmetlere kolay ve hızlı erişim gibi pek çok fayda sağladığı açıktır.[128] Büyük veri analitiği sayesinde daha özelleştirilmiş ve kişiselleştirilmiş finansal hizmetlerin sunulması da mümkün hale gelmektedir.[129] Yapay zekâ ve makine öğrenimi uygulamalarının, finansal müşterilerin ihtiyaçlarına uygun ve kişiselleştirilmiş ürünlerin tespit edilmesinde kullanılması halinde, finans kurumları, gelecekte büyüme potansiyeli olan müşterilere hizmet vermek için kaynakları daha verimli bir şekilde tahsis edebilir. Ayrıca, finans dünyasındaki rutin iş süreçlerinin otomatikleştirilmesi, işletme maliyetlerinin düşürülmesine olanak sağlayabilir. Ayrıca sahtekarlığı, şüpheli işlemleri, ödeme süreçlerindeki gecikme ve hataları ve siber saldırı riskini öngörmek ve tespit etmek için yapay zekâ ve makine öğrenimi kullanılması risklerin daha iyi yönetilmesini sağlamaktadır.[130] Tüm bu sayılanlara ek olarak, yapay zekâ araçlarının finansal ürün ve hizmetlerde kullanılması sayesinde tüketiciler ve yatırımcıların finansal hizmetlere daha geniş erişime sahip olmasının yolu açılmaktadır.

Bununla birlikte finansal süreçlerde tüketici/müşteri verilerinin kullanımı, veri gizliliği ve bilgi güvenliği açısından pek çok soruna da yol açmaktadır. Finansal hizmet sağlayıcılarının finansal durum, alışkanlıklar veya fiziksel

126 Dechert LLP, s. 9-10.
127 Artzt/Dung, s. 56.
128 OECD, 2020, s. 15.
129 FSB, s. 27.
130 FSB, s. 25.

(coğrafi) lokasyon gibi müşteri verilerini elde etme, saklama, birleştirme ve analiz etme becerileri, veri koruma ve tüketicinin korunması alanlarının gözden geçirilmesini gerekli kılmaktadır.[131] Ayrıca yapay zekâ ve makine öğrenimi analitiği, halka açık veriler aracılığıyla müşterilerin özelliklerini analiz edebilmektedir. Bu nedenle, bir taraftan tüketicilerin anonimliği korunurken ve büyük verinin finansal hizmetlerde güvenli ve verimli kullanımını kolaylaştırırken, diğer taraftan müşteri analizine ilişkin çıktıların nasıl korunması gerektiğine karar verilmesi gerekmektedir.

Ayrıca, yapay zekâ ve makine öğreniminin kullanımı, karar verme sürecinde karmaşık sorunlara yol açabilecek "kara kutular" ortaya çıkması riskini de beraberinde getirmektedir. Özellikle finansal kurumlardaki insan kullanıcılar ve düzenleyici otoriteler açısından bakıldığında, ticaret ve yatırım kararları gibi kararların nasıl formüle edildiğini anlamak ve açıklamak zor olabilir.[132] Her ne kadar yapay zekâ yardımıyla pazardaki faaliyetlerin etkinliğini artırmak mümkün olsa da ve uyumun sağlanması süreçli daha verimli hale gelse de tüm bu faydaların elde edilmesi için mahremiyet konusundaki endişelerin giderilmesi gerekmektedir.

Unutulmamalıdır ki, yürürlükte olan kurallar, bir kararın geleneksel bir model, bir insan veya bir yapay zekâ aracı tarafından verilmiş olduğuna bakılmaksızın, kapsamına giren tüm olaylar bakımından uygulanacaktır.[133] Bu kapsamda, Tüketicinin Korunması Hakkında Kanun, Bankacılık Kanunu ve Kişisel Verilerin Korunması Kanunu gibi kanunlar, finans sektöründe çeşitli aşamalarda yapay zekâ kullanıldığında da uygulanmaya devam edecektir. O halde veri koruma kanunları yapay zekâ destekli finans sektöründe kişisel verilerin korunmasına hizmet etmektedir. Bununla birlikte, hâlihazırda mevcut Avrupa Birliği Veri Koruma rejiminin yapay zekâ destekli finanstan ve yapay zekâ destekli karar verme süreçlerinden kaynaklanan mahremiyet risklerini bertaraf etmek bakımından yetersiz olduğu da belirtilmektedir. Her ne kadar GVKT otomatik karar alma sistemlerinden kaynaklanan riskler bakımından diğerlerine nazaran farklı bir tutum sergiliyor olsa da uygulamada veri koruma prensiplerinin yapay zekâ kaynaklı kararlar bakımından uygulanması oldukça güçtür.[134]

---

131 OECD, 2020, s. 27.

132 Financial Stability Board, s. 26.

133 OECD, 2024, s. 22, 24 ve 25.

134 Christodoulou/Limniotis, s. 97.

AI Act[135] Avrupa Birliği'nin ve aslında tüm dünyanın gündemine oturmuş olsa da bahsi geçen bu düzenlemenin temel hakları korumak için bir araç olduğu göz ardı edilmemelidir. Veri korumasına ve mahremiyete saygının insanları merkeze ve teknolojinin önüne koymanın temel ön koşulu olduğu göz ardı edilmeksizin, insanlığın korunmasında veri korumanın önemine dikkat çekilmesi büyük önem arz etmektedir. [136] Her ne kadar AI Act, finansal sektörün bir kısmına ilişkin açık hükümler içerse de, *lex specialis* niteliğini taşımamaktadır. Bu nedenle finans sektörü de dahil olmak üzere çeşitli sektörlere uygulanacaktır. AB Yapay Zekâ Tüzüğü'nde bankalar tarafından yapay zekâ tabanlı kredi değerliliği değerlendirmeleri ile hayat ve sağlık sigortasındaki fiyatlandırma ve risk değerlendirmeleri yüksek riskli yapay zekâ kullanım durumu olarak kabul edilmektedir. Bu tür finansal yapay zekâ uygulamalarına daha sıkı yükümlülükler getirilmektedir. Ancak yapay zekânın finans sektöründeki geri kalan kullanımları mevcut mevzuat çerçevesinde ele alınacak olup, Yapay Zekâ Tüzüğü'nden kaynaklanan ek yasal yükümlülüklere tabi olmayacaktır.[137]

Aktarmış olduğumuz tüm hususlar çerçevesinde finansal süreçlerde yapay zekâ sistemlerinin kullanılmasında bazı garantilerin sağlanması ön plana çıkmaktadır. Hangi kişisel verilere erişim sağlandığı, saklandığı ve bu verilerin nasıl kullanıldığı hakkında bireylere bilgi verilmesi gerekmektedir. Ayrıca, kişisel verinin kullanılması için makul bir sebep olmalı, kullanılan veriler doğru olmalı, gereğinden fazla olmamalı ve gerektiğinden fazla bir süre tutulmamalıdır. Bireylere kişisel verileriyle ilgili anlamlı seçenekler sunmak ve verileri üzerinde gerçekten kontrol sahibi olmalarını sağlamak da dikkat edilmesi gereken önemli bir noktadır. Günümüz FinTechlerindeki yapay zekâ algoritmaları yüksek miktarda kişisel veri kullandığından veri güvenliğinin sağlanması önem arz etmektedir.

---

[135] Şubat 2024'de onaylanan AI Act, yapay zekâ teknolojilerinin güvenli olduğunu ve inovasyon ve ekonomik büyümeyi desteklerken temel haklara da saygı gösterilmesini garanti etmektedir. The AI Act classifies AI applications into categories based on risk levels, such as unacceptable, high-risk, and low-risk, with stringent compliance requirements for high-risk applications like AI-based credit assessments. Bkz. GDPR Local (2024), *The Future of Finance: Adapting to AI and Data Privacy Laws*, *(https://gdprlocal.com/the-future-of-finance-adapting-to-ai-and-data-privacy-laws/,* E.T.: 06.07.2024).

[136] European Data Protection Supervisor: *"Devising a trajectory towards a just and fair future: the identity of data protection in times of AI", (https://www.edps.europa.eu/ system/files/2024-05/edps_closing_remarks_at_cpdp_en.pdf*, E.T.: 06.07.2024.

[137] OECD, 2024, s. 31.

Yapay zekâ kaynaklı risklerin bertaraf edilmesinde teknolojik sistemler, mesela mahremiyet artıcı teknolojilerin kullanılması önem taşımaktadır. Veri korunması ile ilişkili riskleri azaltmak için, anonimleştirme gibi tekniklerle mahremiyeti koruyan teknolojilerin (PET)[138] uygulanması önerilmektedir. Bu yöntemler ilgili kişilerin verilerinin korunmasına yardımcı olarak veri istismarı sonucunda kişisel mahremiyetten ödün verilmesinin önüne geçmektedir.[139] Bununla birlikte, etkin yasal düzenlemelerin yine de ayrı ve büyük önem taşıdığının altı çizilmektedir.[140] Yapay zekâ ve makine öğrenimi yöntemlerinin "açıklanabilirliği" veya "denetlenebilirliği"ndeki eksiklik, kanun koyucular yapay zekâyı denetlemenin yollarını bulmadıkça makroekonomik düzeyde büyük riskler ortaya çıkarma potansiyeline sahiptir.[141]

Değerlendirmelerimizi sonlandırırken, yapay zekâ teknolojisindeki gelişmelerin hızlı bir ivmeyle devam ettiğini hatırlatmakta yarar görüyoruz. Yaşanan tüm bu gelişmeler, bu bölüm kapsamında yapmış olduğumuz analizlerin de dönüşmesine yol açacaktır. Şu an dünyada önde gelen birçok yapay zekâ laboratuvarı, yapay zekâ etmenleri (*AI Agents*) ile ilgili araştırmalarını sürdürmektedir. Gelişmiş büyük dil modellerine dayanan ve planlama becerisi, uzun dönem hafıza ve kodu icra etme, interneti kullanma veya pazarda ticaret gerçekleştirme gibi harici araçlara erişimi olan bu yapay zekâ sistemleri, karar alma süreçlerini daha da opak bir hale getirecektir.[142] Yeni nesil yapay zekâ etmenleri otonom bir şekilde veri analiz edebilecek, başka yapay zekâ etmenleri oluşturmak için kod yazabilecek, bu kodu test edebilecek ve uygun gördükleri şekilde güncelleyerek finansal kuruluşların pek çok farklı fonksiyonunu dönüştürebilecektir. Bu dönüşümün yeni veri koruma ve mahremiyet sorunlarına yol açacağı şüphesiz olmakla birlikte, bu sorunların teknolojinin kendisiyle çözülebileceği de değerlendirmeli ve bu konuda uluslararası iş birliği öncelik haline getirilmelidir.

---

138 Differential privacy, Diferansiyel (Farklılaştırılmış) mahremiyet de bu tekniklerden biridir: Veri setlerine gürültü eklenmesi suretiyle verinin bütünsel faydası ortadan kaldırılmadan bireysel veri noktalarının korunması sağlanmaktadır. GDPR Local (2024), *The Future of Finance: Adapting to AI and Data Privacy Laws*, *(https://gdprlocal.com/the-future-of-finance-adapting-to-ai-and-data-privacy-laws/,* E.T.: 06.07.2024).

139 Hyperight (2024), *Data Privacy Paradox: Balancing Innovation with Protection in the Age of AI, (https://hyperight.com/data-privacy-paradox-balancing-innovation-with-protection-in-age-of-ai/*, E.T.: 06.07.2024).

140 Ozan Özparlak/Çetin, s. 1005.

141 Buckley./ Zetzsche /Arner ve Tang, s. 52.

142 BIS, s. 6.

Finansta yapay zekâ kullanımın ortaya çıkardığı risklerin etkili bir şekilde üstesinden gelinmesi için iş birliğinin önemine vurgu yapan IMF, 2021 yılında yayınlanan bir rapor çalışmasında şu ifadelere yer vermektedir: *"Bu zorlukların üstesinden gelinmesi için geniş kapsamlı düzenleyici ve iş birlikçi çabalar önem taşımaktadır. Yeterli bir politika tepkisi, sektör için net asgari standartlar ve yönergelerin geliştirilmesini ve gerekli teknik becerilerin güvence altına alınmasına daha güçlü odaklanmayı gerektirir. Yapay zekâ/makine öğrenimi sistemlerinin finans sektöründe konuşlandırılmasıyla ilgili konuların doğası gereği birbirine bağlılığı göz önüne alındığında, finansal kurumlar, merkez bankaları, mali denetçiler ve diğer paydaşlar arasındaki iş birliği, işlerin tekrarlanmasını önlemek ve potansiyel risklere karşı koymaya yardımcı olmak için önemlidir.[143]"*

Güveni yeniden inşa etmek ve ilerleme ve gelişmeyi hızlandırmak için finansal hizmet sağlayıcılar ve düzenleyici otoritelerin şeffaflık, veri paylaşımı ve gizliliğin korunmasına yönelik bir altyapı oluşturmak üzere birlikte çalışması büyük önem taşımaktadır. Bu sürecin, değerlerinin politikalara yansıtılmasını ve verilerinin kullanımından faydalanmalarını sağlamak için verileri kullanılan kişilerin seslerini de içermesi gerektiği göz ardı edilmemelidir.[144] Ayrıca GVKT'de açıkça işaret edilmiş olan *"privacy by design"* ilkesine paralel olarak planlanan veri işlemenin hukuka uygun bir şekilde gerçekleştirilebilmesi için, yazılım geliştirmenin tasarım aşamasından itibaren avukatlar ve teknik geliştiriciler arasında sağlam bir diyaloğun olması gerekmektedir.[145]

Son söz olarak Dünya Ekonomik Forumu (WEF- World Economic Foundation) tarafından hazırlanan ve kuantum ve yapay zekâ teknolojilerinin finans sektörünü nasıl etkileyeceğini anlatan yazının son cümlelerini hatırlatalım: "*Finansın geleceğine doğru adım atarken kuantum ve yapay zekâ teknolojilerini benimsemek artık isteğe bağlı değil, zorunlu. Bu dönüştürücü yolculuğa liderlik eden öncüler, kuantum çağına doğru ilerledikçe verimlilik, güvenlik ve inovasyon açısından yeni standartlar belirleyecek."[146]*

---

143 IMF 2021, s. 19.

144 CEGA (2023), *Beyond Disruption: Privacy Enhancing Technologies Can Deliver Financial Inclusion, (https://medium.com/center-for-effective-global-action/beyond-disruption-privacy-enhancing-technologies-can-deliver-financial-inclusion-783e3b80cc3a,* E.T.: (06.07.2024).

145 Lukas, A. J. F.: *Machine Data, Personal Data, Sensitive Data and Artificial Intelligence. the Interplay of Privacy Enhancing Technologies with the GDPR, (https://ssrn.com/ abstract=4341844,* E.T.: 06.07.2024), s. 8.

146 WEF (2024), *How AI and quantum technologies are transforming the financial industry, (https://www.weforum.org/agenda/2024/01/ai-quantum-technologies-transforming-financial-industry/,* E.T.: 06.07.2024).

KAYNAKÇA

AGGARWAL, Nikita: AI, Fintech and the Evolving Regulation of Consumer Financial Privacy, (ed. Justin B. Bullock et al), "The Oxford Handbook of AI Governance", 2022, s. 860-878.

AKSOY, Hüseyin Can: *Kişisel Verilerin Korunması Yönüyle Algoritmik Karar Verme*, Kişisel Verileri Koruma Dergisi 2022, C. 4, S. 2, s. 69-87.

ARTZT, Matthias/ DUNG, Tran Viet: *Artificial Intelligence And Data Protection: How To Reconcile Both Areas from the European Law Perspective*, Vietnamese Journal of Legal Sciences 2022, C. 7, S. 2, s. 39-58.

BAHOO, Salman/ CUCCULELLI, Marco/GOGA, Xhoana/MONDOLO, Jasmine: *Artificial Intelligence in Finance: A Comprehensive Review Through Bibliometric And Content Analysis*, SN Bus Econ 2024, C. 4, S. 23, s. 1-46.

BARRIERE, François: *Financial Law In The Era Of Artificial Intelligence: Key Topics*

And Themes, Law and Financial Markets Review 2021, C. 15, S. 3–4, s. 312–322.

BIS: Intelligent financial system: how AI is transforming finance, BIS Working Papers No 1194, June 2024, *(https://www.bis.org/publ/work1194.pdf,* E.T.: 06.07.2024).

Bitsol Technologies (2023), *AI-Driven Privacy Enhancing Technologies (PETs) and Clarifying Misconceptions About It, (https://www.linkedin.com/pulse/ai-driven-privacy-enhancing-technologies-pets-clarifying-misconceptions/*, E.T.: 06.07.2024).

BUCKLEY, Ross P./ZETZSCHE, Dirk Andreas/ARNER, Douglas W./TANG, Brian: *Regulating Artificial Intelligence in Finance: Putting the Human in the Loop*, UNSWLRS 2023, C. 29, s. 43-81.

CEDPO: Generative AI: The Data Protection Implications CEDPO AI Working Group 16 October 2023, *(https://cedpo.eu/wp-content/uploads/generative-ai-the-data-protection-implications-16-10-2023.pdf,* E.T.: 06.07.2024).

CEGA (2023), *Beyond Disruption: Privacy Enhancing Technologies Can Deliver Financial Inclusion*, *(https://medium.com/center-for-effective-global-action/beyond-disruption-privacy-enhancing-technologies-can-deliver-financial-inclusion-783e3b80cc3a,* E.T.: (06.07.2024).

CHRISTODOULOU, Paraskevi/KONSTANTINOS, Limniotis: *Data Protection Issues in Automated Decision-Making Systems Based on Machine Learning: Research Challenges, Network* 2024, C. 4, *(https://doi.org/10.3390/network4010005*, E.T.: 06.07.2024), s. 91-113.

Citi GPS: AI in Finance Bot, Bank & Beyond, *(https://ir.citi.com/gps/9j79xHIa-vfPi785TYiSciffO0j4I0D52fI9LrahsLZEo6MpT4aM7SpwSFagAL9CIukqn2fwiJ_GNvDsLy4b6XEjftdK1abu*, E.T.: 06.07.2024).

Congressional Research Service: Artificial Intelligence and Machine Learning in Financial Services, *(https://crsreports.congress.gov/product/pdf/R/R47997*, E.T.: 06.07.2024).

ÇAĞLAYAN AKSOY, Pınar: *Akıllı Sözleşmelerin Dünü, Bugünü ve Yarını: Karşılaştırmalı Bir Değerlendirme*, Vergi Dünyası 2022, C. 42, S. 494, s. 17-38.

d'ALIBERTI, Liv/GRONBERG, Evan/KOVBA, Joseph: *Privacy-Enhancing Technologies for Artificial Intelligence-Enabled Systems,* IWSPA '24, June 21, 2024, Porto, Portugal, *(https://arxiv.org/abs/2404.03509*, E.T.: 06.07.2024).

Dechert LLP: Artificial Intelligence: Legal and Regulatory Issues for Financial Institutions, *(https://www.dechert.com/knowledge/onpoint/2023/4/artificial-intelligence--legal-and-regulatory-issues-for-financi.html,* E.T. 06.07.2024).

Enveil (2024), *International Banker: Unlocking the Power of Privacy Enhancing Technologies in Financial Services, (https://www.enveil.com/intl-banker-privacy-enhancing-technologies-in-financial-services/,* E.T.: 06.07.2024).

European Commission: Targeted consultation on artificial intelligence in the financial sector, *(https://finance.ec.europa.eu/regulation-and-supervision/consultations-0/ targeted-consultation-artificial-intelligence-financial-sector_en,* E.T.: 06.07.2024).

European Data Protection Supervisor: Devising a trajectory towards a just and fair future: the identity of data protection in times of AI, *(https://www.edps.europa.eu/system/files/2024-05/edps_closing_remarks_at_cpdp_en.pdf*, E.T.: 06.07.2024).

Finextra (2024), *Privacy enhancing technologies: Key to win in today's evolving World, (https://www.finextra.com/blogposting/26348/privacy-enhancing-technologies-key-to-win-in-todays-evolving-world,* E.T.: 06.07.2024).

FSB: Artificial Intelligence and Machine Learning in Financial Services Market Developments and Financial Stability Implications, *(https://www.fsb.org/wp-content/uploads/P011117.pdf,* E.T.: 06.07.2024).

GDPR Local (2024), *The Future of Finance: Adapting to AI and Data Privacy Laws*, *(https://gdprlocal.com/the-future-of-finance-adapting-to-ai-and-data-privacy-laws/,* E.T.: 06.07.2024).

Hyperight (2024), *Data Privacy Paradox: Balancing Innovation with Protection in the Age of AI, (https://hyperight.com/data-privacy-paradox-balancing-innovation-with-protection-in-age-of-ai/*, E.T.: 06.07.2024).

IMF (2021) Powering the Digital Economy: Opportunities and Risks of Artificial Intelligence in Finance, *(https://www.imf.org/en/Publications/Departmental-Papers-Policy-Papers/Issues/2021/10/21/Powering-the-Digital-Economy-Opportunities-and-Risks-of-Artificial-Intelligence-in-Finance-494717,* E.T.: 06.07.2024).

IMF (2023), *AI'S Reverberations Across Finance, (https://www.imf.org/en/Publications/fandd/issues/2023/12/AI-reverberations-across-finance-Kearns,* E.T.: 06.07.2024).

IMF, *Generative Artificial Intelligence in Finance: Risk Considerations*, IMF Fintech Note 2023/006, *(https://www.imf.org/en/Publications/fintech-notes/Issues/2023/08/18/Generative-Artificial-Intelligence-in-Finance-Risk-Considerations-537570,* E.T.: 06.07.2024). *(Fintech Notes)*

KAYA, Orçun: *Robo-advice – a true innovation in asset management,* EU Monitor Global Financial Markets 2017, *(https://www.dbresearch.com/PROD/RPS_EN-PROD/PROD0000000000449125/Robo-advice_–_a_true_innovation_in_asset_managemen.PDF?undefined&realload=~/1Q36lmuqYi6YfCAYZpplbKyC2/ofAYg0Ui1BEPDySuGGB5tkh~RiLocsCFE7~O*, E.T.: 06.07.2024), s. 1-16.

KONIGSTORFER, Florian/THALMANN, Stefan: *Applications of Artificial Intelligence in commercial banks – A research agenda for behavioral finance,* Journal of Behavioral and Experimental Finance 2020, C. 27, S. 2, 100352.

KPMG (2024), *Üretken Yapay Zeka ile Finansın Yeni Normali,* (*https://assets.kpmg.com/content/dam/kpmg/tr/pdf/2024/01/uretken-yapay-zeka-ile-finansin-yeni-normali.pdf,* E. T.: 06.07.2024).

Linklaters: Artificial Intelligence in Financial Services: Managing machines in an evolving legal landscape, *(https://lpscdn.linklaters.com/-/media/files/insights/2019/september/linklatersartificialintelligenceinfinancialservicesmanagingmachinesinan-evolvinglegallandscapesept201.ashx?rev=2c497d44-32d1-42e4-8f1c-f4f6eb272b82&extension=pdf&hash=6B9FB3353FA1C5C0B0E936862ED46887,* E.T.: 06.07.2024).

LUKAS, Arnold J. F.: *Machine Data, Personal Data, Sensitive Data and Artificial Intelligence. the Interplay of Privacy Enhancing Technologies with the GDPR*, *(https://ssrn.com/abstract=4341844,* E.T.: 06.07.2024).

Mastercard: Privacy enhancing technologies WHITE PAPER FEBRUARY 2024, *(https://b2b.mastercard.com/media/z0pnu32l/privacy-enhancing-technologies-white-paper-final.pdf,* E.T.: 06.07.2024).

MOHUN, Pooja: Regulating Artificial Intelligence in the Finance Sector, University of Otago, a Thesis of Master of Laws, New Zealand, 2022.

NGUYEN, Duc Khuong/SERMPINIS, Geergios/STASINAKIS, Charalampos: *Big data, artificial intelligence and machine learning: A transformative symbiosis in favour of financial technology,* European Financial Management 2023, C. 29, S. 2, s. 517-548.

OECD: Personal Data Use in Financial Services and the Role of Financial Education: A Consumer-centric Analysis, OECD Publishing, Paris, *(https://doi.org/10.1787/06998d33-en,* E.T.: 06.07.2024). *(2020)*

OECD: Artificial Intelligence, Machine Learning and Big Data in Finance: Opportunities, Challenges, and Implications for Policy Makers, *(https://www.oecd.org/finance/artificial-intelligence-machine-learningbig-data-in-finance.htm*, E.T.: 06.07.2024). *(2021)*

OECD: Generative Artificial Intelligence in Finance, OECD Artificial Intelligence Papers December 2023 No. 9, *(https://www.oecd-ilibrary.org/docserver/ac7149cc-en.pdf?expires=1719399009&id=id&accname=guest&checksum=4559573E565D449ED3558B1EACFA1EDD,* E.T.: 06.07.2024). *(2023)*

OECD: Regulatory approaches to Artificial Intelligence in finance", OECD Artificial Intelligence Papers, No. 24, (https://www.oecd.org/en/publications/regulatory-approaches-to-artificial-intelligence-in-finance_f1498c02-en.html, E.T.: 1.10.2024). *(2024)*

OZAN ÖZPARLAK, Başak/ÇETİN, Müge: *ChatGPT ve Üretici Yapay Zekâ Modellerinde Mahremiyet ve Güvenliğin Hukuki Boyutu,* Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi 2023, C. 29, S. 2, s. 1003-1040.

PIOTROWSKI, Dariusz/ORZESZKO, Witold: *Artificial intelligence and customers' intention to use robo-advisory in banking services*, Equilibrium Quarterly Journal of Economics and Economic Policy 2023, C. 18, S. 4, s. 967–1007.

Politico (2024), *ChatGPT's hallucinations draw EU privacy complaints, (https://www.politico.eu/article/chatgpts-hallucinations-get-eu-privacy-complaint/,* E.T.: 06.07.2024).

UXDA, *The Future of Generative AI and ChatGPT in Banking* (https://theuxda. com/blog/ai-powered-contextual-cx-digital-banking-success-or-disaster, E.T.: 06.07.2024).

WEF: The New Physics of Financial Services Understanding how artificial intelligence is transforming the financial ecosystem, *(https://www3.weforum.org/docs/WEF_New_Physics_of_Financial_Services.pdf*, E.T.: 06.07.2024). *(New Physics)*

WEF (2024), *How AI and quantum technologies are transforming the financial industry, (https://www.weforum.org/agenda/2024/01/ai-quantum-technologies-transforming-financial-industry/,* E.T.: 06.07.2024). *(AI)*

EĞİTİMDE YAPAY ZEKÂ

Doç. Dr. Nursel YALÇIN*

Arş. Gör. Behiye CANBAZ**

GİRİŞ

Dijital dönüşüm, günümüzde iş yapma şeklini ve dolayısıyla; tarım, enerji, sohbet şekli, ticaret, sağlık, sanayi ve eğitim gibi tüm disiplinlerin işleyişini değiştiren bir olgudur. Bu dönüşüm internetin ve dijital teknolojilerin yaygınlaşmasıyla başlamıştır. Nesnelerin interneti ve yapay zekâ gibi teknolojiler ile birlikte bu dönüşüm daha da hızlanmaktadır. Günlük rutinlerimizden eğitim hayatımıza kadar etkili olan yapay zekâ, oldukça hızlı bir şekilde hayatımızda yer edinmektedir. Uzun vadede başarı veya daha kalıcı işler yapılmak istendiğinde yapay zekâdan bağımsız kalmak düşünülememektedir. Yapay zekâ sistemleri kişilerin elde ettikleri büyük veriyi doğru bir şekilde analiz ederek, etkili kararlar almalarını sağlamaktadır. Bu sayede, insan kaynaklarından ve eğitimden tutun da devletlerin kalkınma planlarında da oldukça önemli bir yere sahiptir. Dünyamız, dijital dönüşümün ve yapay zekânın etkisiyle her alanda hızla değişmekte ve eğitim de bu değişimden nasibini almaktadır. Teknolojik gelişmeler, eğitim sistemlerini dönüştürerek yeni fırsatlar ve zorluklar sunmaktadır. Üretken yapay zekâ sistemleri, yanlış verilerle veya eğitmenler tarafından manipüle edilerek eğitilebilirler. Bu yüzden yapay zekâ sistemlerine karşı ön yargılar oluşabilmektedir. Öğretmenlerin yerini alma, elde edilen kişisel verilerin gizliliğini ve güvenliğini sağlama gibi etik kaygılar bulunmaktadır.[1] Ancak dönüşümün bu kadar hızlı ilerlemesi, eğitimdeki geleneksel yöntemleri bir ke-

* Doç. Dr., Gazi Üniversitesi, Gazi Eğitim Fakültesi, Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü, nyalcin@gazi.edu.tr 0000-0002-0393-6408

** Arş. Gör., Ostim Teknik Üniversitesi, Mühendislik Fakültesi, Yazılım Mühendisliği Bölümü, behiye.canbaz@ostimteknik.edu.tr, 0000-0002-8195-8223

1 Bozkurt, A.: *ChatGPT, üretken yapay zekâ ve algoritmik paradigma değişikliği*, *Alanyazın 2023*, C. *4*, S. 1, s. 68.

nara bırakarak ve yeni yaklaşımların benimsenmesini teşvik etmektedir. Eğitim sistemlerinde öğretmenlerin ve öğrencilerin rollerini dönüştürme potansiyeline sahip olan yapay zekâ, devlet politikaları tarafından da desteklenmektedir. Millî Eğitim Bakanlığı (MEB), Üniversiteler ve diğer devlet politikaları yapay zekânın eğitime katkısını önemsedikleri için çeşitli stratejiler başlatmaktadırlar. Örneğin, özel yetenekli öğrenciler için "Bilim ve Sanat Merkezleri Yapay Zekâ Uygulamaları Atölye Programı" hazırlanmıştır.[2] Ek olarak Türkiye, Milli Teknoloji hamlesi ile uyumlu olan Ulusal Yapay Zekâ Stratejisi başlatmıştır.[3] Avrupa Birliği ve TÜBİTAK gibi kurumlar bu alanlarda yapılan projeleri öncelikli olarak desteklemektedirler. Teknoloji, eğitimde bilgi ve becerilerin aktarılma şeklini değiştirerek, bilginin daha erişilebilir, kişiselleştirilebilir ve ilgi çekici hale getirilebilirliğini sağlayabilmektedir. Bilginin statik bir şekilde sunumundan (Web 1.0), üretken yapay zekâ ile etkileşimli deneyimler sunarak, eğitim süreçlerini ilgi çekici hale getirmektedirler. Örneğin Web 1.0 ile sadece çevrim içi ders materyali hazırlanarak öğrencilere okuturken, Web 2.0 ile birlikte blog ve wikilerle öğrencilerin iş birliği yapmasına imkân verilmişti. Web 3.0 döneminde semantik web ve yapay zekâ ile uyarlanabilir öğrenme ortamları sunulmaktadır. Günümüzde ise yapay zekâ ile kişisel öğrenme içerikleri oluşturulabilmekte, geri bildirimler otomatik ve sanal öğretmenler tarafından yapılabilmektedir. Yapay zekânın her alanda olduğu gibi eğitim alanında çok güzel fırsatlar sunarken, güvenlik, gizlilik, ön yargılar ve etik bazı tehditlerinin olabileceği göz ardı edilmemelidir. Bu çalışmada; eğitimde yapay zekânın tarihi, eğitimde yapay zekâ türleri, eğitimde kullanılabilen 13 alanda kategorilendirilmiş yapay zekâ araçları ve eğitimde yapay zekâ kullanımının avantajları ve de dezavantajlarından bahsedilmektedir.

I. EĞİTİMDE YAPAY ZEKÂ TARİHİ

Yaşadığımız dijital çağda, teknolojinin hızlı bir şekilde gelişmesi ile birlikte eğitim ortamlarında ihtiyaçlar ve bu ihtiyaçlar doğrultusunda kullanılan materyaller çeşitlenmektedir. Endüstri 4.0 teknolojisinin gelişimine paralel olarak ortaya çıkan yapay zekâ, eğitimde birçok kolaylık sağlamaktadır.

---

[2] MEB (2023), *Yapay Zekâ Uygulamaları Atölye Programı, (https://orgm.meb.gov.tr/meb_iys_dosyalar/2023_10/06094131_Yapay_Zeka_UygulamalarY_Atolye_ProgramY.pdf, E.T.: 29.03.2024)*.

[3] UYZS (2021), *Ulusal Yapay Zekâ Stratejisi 2021-2025.* (https://cbddo.gov.tr/SharedFolderServer/Genel/File/TR-UlusalYZStratejisi2021-2025.pdf E.T.: 29.03.2024).

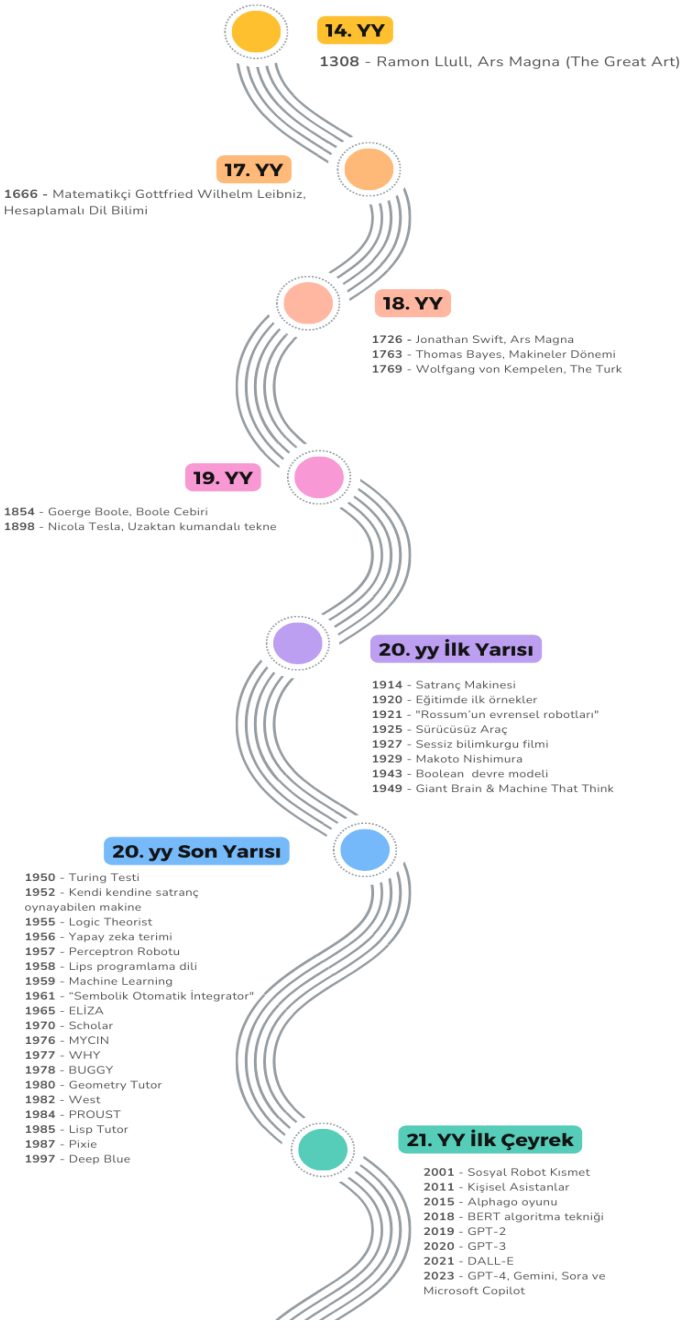
Yapay zekâ günümüzdeki önemini kazanana kadar çeşitli gelişim adımlarından geçmiştir. Bu adımlar Şekil 1' de görüldüğü gibi felsefi dönem, makineler dönemi ve yapay zekânın tanımlanması olmak üzere 3 aşamada incelenmektedir.



Şekil 1. Yapay Zekâ ile ilgili Gelişmeler

Yapay zekâ, tarihsel ve felsefi açıdan yüzyıllardır araştırılıp, tartışılmaktadır. Ancak günümüzde oldukça hızlı bir ilerleme gerçekleştirmektedir. İlk olarak canlılığı taklit ettiği için felsefi açıdan ele alınmaktadır. *Felsefi dönemde* bilginin kaynağı, bilginin nasıl eyleme yol açtığı ve öğrenmenin nasıl gerçekleştirildiği araştırılmaktadır. İlk çağ Yunan filozoflarından Aristoteles insanların elindeki her aletin ya bizim işimizi yapacağını ya da kendi işlerini yapacağından bahsetmektedir.

Yapay zekâ ile ilgili gelişmeler Şekil 2'de görüldüğü gibi sınıflandırılarak, ilgili tarihlere ait detaylı bilgiler verilmiştir.



Şekil 2. *Yapay Zekâ Tarihi*

1308 - Ramon Llull, "Ars Genaralis Ultima" isimli kitapta ilk defa kavramların birleştirilmesinden bahsedilerek, yapay zekâ kavramsallaştırılmıştır. İnsanın karar verme mekanizmasına yardımcı olması için akıl yürütme mekanizması "Ars Magna (The Great Art)" isimli disk mekanizması oluşturulmuştur. Bu mekanizma yapay zekâda yapılan ilk çalışmalardan biri olarak kabul edilmektedir. Felsefi anlamda insan dillerinin gelişim süreci, insan beyninin gelişimi ve nasıl düşündüğü gibi süreçler de tarih boyunca incelenmektedir.

1666 - Matematikçi Gottfried Wilhelm Leibniz "Dissertatio De Arte Combinatoria" isimli kitabında düşüncelerin basit kombinasyonlardan elde edilebileceğini öne sürmüştür. Bu sayede hesaplamalı dilbilimine öncülük ederek makinelerin dil öğrenme süreçlerinde neleri bilmesi gerektiğini planlayarak mekanik bir cihaz oluşturmuştur.

1726 - Jonathan Swift, kullanım kolaylığı ve mekanik anlamda Ars Magna verilerini geliştirerek daha kullanışlı hale getirmeye çalışmıştır.

1763 - Thomas Bayes, verileri analiz ederek olasılıklara ulaşmış ve olayların olabilme olasılığını hesaplayabilmek için bir yapı geliştirmiştir. Bu yapının ardından belirli işlerin otomatikleştirilip zamandan ve iş gücünden tasarruf edilerek hız kazandırılması amaçlanmıştır. Bu amaçla, gerçekleştirilen çalışmalar doğrultusunda *makineler dönemi* başlamıştır.

1769 - Wolfgang von Kempelen, The Turk(Türk) isimli yapay zekânın ilk örneklerinden denilebilecek satranç otomatını geliştirmiştir. Bu otomat üstünde satranç tahtası olan, bıyıklı ve sarıklı bir Türk figürlü satranç oyuncusundan oluşmaktadır. Adının neden Türk olduğu ve çalışma prensibinin çözülemediği satranç otomatı gizemini korumaktadır.

1854 - Goerge Boole, denklem çözümü gibi sistemli bir şekilde olması gerektiğini düşündüğü mantık yürütmenin geçerli olduğu Boole cebirini ortaya koymuştur. Boole cebiri elektronik devre tasarımının temel mantığıdır. Bu yüzden de yapay zekânın tarihinde oldukça önemlidir.

1898 - Nicola Tesla, günümüz hava araçları teknolojilerinden olan drone fikrini ortaya atmıştır. Madison Square Garden'daki Elektrik Sergisi'nde uzaktan kumandalı tekne" ürününü tanıtmıştır. Elektrik sergisinde kapalı bir havuz, gemi ve kontrol kutusu vardı. Bu teknenin, herhangi bir kablo bağlantısı olmadan uzaktan kumanda ile hızı ve yönü değiştirilebiliyor, ışıklar gibi aygıtları da kontrol edilebiliyordu.

20. yy'a gelindiğinde yapay zekâ yenilikleri hızlı bir şekilde büyümeye başlamıştır.

1914 - İspanyol mühendis Leonardo Torres y Quevedo satranç oynayabilen ilk makineyi tanıtmıştır.

1920 - Eğitimde yapay zekânın ilk uygulama örneklerini düşünenler arasında Ohio Üniversitesinde çalışan Sidney L. Pressey gösterilmektedir. Pressey, öğrencilerin öğrenmelerini pekiştirmek için, Edward Thorndike'nin etki kanununda yer alan testlerde derhal geri bildirim olması gerektiğine değinerek, çoktan seçmeli testler kullanılabileceğinden bahsetmektedir[4]. Ayrıca, öğrencilere test sonuçlarını gösteren ve gereken bilgilendirmeyi yaparak öğrenmeyi destekleyen "makinelerden" bahsetmektedir. Bahsedilen konu dönem şartlarında gerçekleştirilme şansı bulamasa da, yapay zekânın ilk uygulama örnekleri arasında sayılmaktadır[5]. Pressey (1950), eğitimde bugün yapay zekânın kullanıldığı alanlarından olan eğitim yönetimi konusuna değinerek, böyle bir makinanın öğrencilerin öğrenmelerine destek olmanın yanında öğretmenlerin ve öğrencilerin yüklerini de azaltacağını belirtmiştir.

1921 - Çek yazar Karel Capek "Rossum'un evrensel robotları" isimli bilimkurgu türündeki tiyatro oyununu yayınlamıştır. Tiyatro oyununda "robot" olarak adlandırılan yapay insanlar kavramı sorgulanması sağlanmıştır. İlk defa robot kelimesi literatüre "robota" olarak, Çek yazar Karel Capek sayesinde girmiştir.

1925 - Amerikan ordusunda elektrik mühendisi olan Fransic P Houdina, Houdina Radio Control radyo frekansları ile kontrol edilen sürücüsüz aracı "*American Wonder*"ı New York şehrinde tanıtmıştır.

1927 – Alman yönetmen Fritz Lang sessiz bilimkurgu türünde Metropolis filmini yayınlandı. Bu film insanların robotlarla olan etkileşimini anlatmaktadır. Star Wars filmindeki C-3PO'ya ilham kaynağı olduğu bilinmektedir.

1929 - Japonya'da yüz ifadesini değiştirebilen, hava basıncı mekanizması ile ellerini ve başını hareket ettirebilen ilk robot üretilmiştir. "Doğanın yasalarından öğrenme" anlamına gelen *Gakutensoku* isimli robotu Makoto Nishimura tasarlanmıştır.

---

4 Thorndike, E. L.: *The Law of Effect*, The American journal of psychology 1927, C. *39, S.* 1/4, s. 213.

5 Holmes, W./Bialik, M./Fadel, C.: *Artificial İntelligence in Education*, İsviçre 2023, s. 641.

1943 - McCulloch ve Walter Pitts beynin Boolean devre modeli ile yapay nöron ağlarının mantıksal işlevleri nasıl gerçekleştirdiğini açıklamaktadır. Bu model beynin çalışma prensiplerini varsayımlar kullanarak matematiksel olarak formülize bir biçimde açıklamaktadır (Arslan, 2020). Bu açıklamaya "Sinir Sisteminin İçinde Olan Fikirlerin Mantıksal Hesabı" isimli makalede yer verilmektedir. Bu yüzden, makale bilgisayar temelli sinir ağları için rehber niteliğindedir.

1949 – Edmund Berkeley, Giant Brain & Machine That Think kitabında, bir makinenin tıpkı insan beyni gibi bilgiyi işleyebileceğini, hesap yapabileceğini ve düşünebileceğini yazmıştır.

1950 – Alan Turing, "Computing Machinery and Intelligence" kitabında günümüzde "Turing testi" olarak bilinen taklit oyununu tanıttı. Bu oyunda Alman ordusunun şifreleme mantığı çözülmüştür. Eğer bilgisayar ayırt edilemezse bu testi geçmiş sayılmaktadır. Bu sayede makine zekâsı yani makinenin insan gibi düşünme yeteneği test edilmiş oldu. Aynı zamanda Claude Shannon, satranç oynayan bilgisayar programı geliştirilebilmesi için bir makale yayınlamıştır.

1952 - Arthur Samuel, kendi kendine satranç oynayabilen bilgisayar yazılımını yazmıştır. Bu yazılım makine öğrenmesinin ilk örneği olmuştur.

1955 - Allen Newell, Herbert A. Simon ve Cliff Shaw, ilk yapay zekâ programı "Logic Theorist" isimli bilgisayar programı geliştirilmistir. Bu program, Whiteheas ve Russel tarafından yayınlanan Principia Mathematica'da yer alan 52 matematik teoreminden 38'ini ispatlamıştır.

Önceki dönemlerde fikir olarak şunlar yapılsa hayatımız veya eğitim hayatımız kolaylaşır denilen, sadece hayal olarak düşünülen makineler artık gerçekleştirilebilir hale gelmektedir.

1956 - Yapay zekâ terimi John McCarthy, Marvin Minsky, Nathaniel Rochester ve Claude Shannon tarafından, Dartmouth konferansında ilk defa kullanılmıştır. Bu terim yeni çalışma alanı olarak kabul edilmiştir.

1957 - Frank Rosenblatt, iki katmanlı bilgisayar öğrenme ağına dayanan, desen tanımayı sağlayan bir yapay sinir ağına sahip Perceptron robotunu gelistirdi.

1958 - John McCarthy, yapay zekâ araştırmalarında kullanılan en popüler Lips programlama dilini geliştirdi.

1959 - Arthur Samuel "Machine Learning" (Makine Öğrenmesi) kavramını ortaya attı. Oliver Selfridge, sempozyumu kitabında "Pandemonium: Öğrenme için bir paradigma" bildirisini yayınladı. Bu bildiride bilgisayarların daha öncesinde belirlenen kalıpları tanıtabileceği modelden bahsetmektedir. John McCarthy ise "Programs with Common Sense" makalesinde "garbage collection" isimli, cümleleri manipüle ederek sorunları çözmeye yönelik bir program tanımladı.

Yapay zekâ alanında bu gelişmelerin gerçekleşmesi eğitim alanında da etkisini göstermeye başlamıştır.

1961 - James Robert Slagle, Marvin Minsky'nin danışmanlığında, ilk Uzman sistem olarak kabul edilen birinci sınıf matematikte sembolik entegrasyon sorunlarını çözen sezgisel program, "Sembolik Otomatik İntegrator" programını geliştirmiştir.

1965 - Joseph Weizenbaum, MIT'nin yapay zekâ laboratuvarlarında ELİZA isimli programı geliştirmiştir. ELİZA doğal dil işleme programlarının (NLP) ilk örneği olarak bilinmektedir.

1970 Carbonell, Coğrafya eğitiminde yapay zekâ kullanımı konusunda öncü çalısmalardan olan ilk akıllı ders sistemi Scholar'ı yayınlamıstır. Scholar, Güney Amerika coğrafyası hakkında sınırlı, öğretimsel diyaloglar ile tasarlanan bir programdır.[6]

1976 – Shortliffe, menenjit gibi hastalıkların teşhisi için Stanford üniversitesinde kural tabanlı uzman bir sistem olarak "MYCIN" programını geliştirmiştir. Bu sisteme özel ders için bir arayüz oluşturması ve öğrenciyle etkileşim kurabilmesi için GUIDON isimli bir öğretim sistemi dahil edilmiştir.[7] GUIDON'da bir hastanın vaka diyalogları öğrenciye anlatılır, öğrencinin de hekim gibi hastalığa yönelik sorular sorması beklenmektedir[8].

1977 - Collins ve Stevens, öğrencinin öğrenme sürecine daha aktif katılımını sağlamaya teşvik eden Sokratik diyaloglar ile ilgili yeni bir alan ortaya atmışlardır. Sokratik özel ders için WHY sistemi oluşturulmuştur. Bu sistem soru-cevap şeklinde bir makine öğrenmesini tanımlamaktadır. Program, kullanım sırasında öğrencilerin bilgilerine göre öğrenciye göre sorular getirmektedir[9].

---

6 Morrison, D. M./Rus, V.: *The SCHOLAR Legacy: A New Look at the Affordances of Semantic Networks for Conversational Agents in Intelligent Tutoring Systems*, *AIED* 2013.

7 Doğaç, A.: *Uzman Sistemler*. EMO *1990*, S. 373, s. 88.

8 Shute, V. J./Psotka, J.: *Intelligent Tutoring Systems: Past, Present, and Future, 1994, s. 579*.

9 Woolf, B. P.: *Knowledge-Based Tutors: An Artificial İntelligence Approach to Education*, Amherst 1990, s. 101.

1978 – Burton BUGGY isimli, basit aritmetik alıştırmalarla ortaya çıkan bir sistem geliştirmiştir. Bu sistem öğrencilerin yanlışlarının doğruya dönüştürülebilmesi için dönütlerde bulunmaktadır[10].

1980 - Anderson, Boyle ve Yost tarafından Geometri eğitimi icin Geometry Tutor geliştirildi. Bu sistem lise geometrisinde ispat yapmak için oluşturulmuştur. Öğrencilerin davranışlarını ve hamlelerini veri olarak saklamaktadır. Verilerdeki tüm doğru ve yanlış kural eşleşmelerini hesaplamak ve bunlara göre yönlendirmekten sorumludur. [11]

1982 - Burton & Brown, matematik eğitimini oyunla yapabilmek için eğitsel West oyununu geliştirdi. Oyun üç zarın ürettiği değerleri kullanarak en yüksek cebirsel değere ulaşmayı amaçlamaktadır. Öğrenci hamlelerini takip eden ve bunlara göre önerilerde bulunan eğitsel ajan bulunmaktaydı.[12]

1984 - Johnson ve Littmann Soloway, programlama öğretimi için PROUST yazılımı hazırlamıştır. PASCAL programındaki söz dizimsel olmayan öğrenci hatalarını teşhis etmek için tasarlanmıştır[13].

1985 – Anderson ve Reiser tarafından Lisp programlama dilinin öğretimi için "Lisp Tutor" oluşturulmuştur. Bu program, programlama dili öğrenimi sırasında hatasız ilerlemeyi amaçladığı için, öğrencilere anında dönüt vermektedir. Hata olan kısımda düzeltme sağlanana kadar başka bir işleme izin vermemektedir.[14]

1987 - Matematik eğitimi için "Pixie" programı oluşturulmuştur. BUGGY'in eksik kaldığı üst düzey cebir problemlerindeki kural hatalarını teşhis amacı ile geliştirilmiştir. Hata teşhis etme özelliğine sahiptir ancak düzeltme yapma özelliği yoktur.[15]

1997 – IBM tarafından satranç oynayabilen bir bilgisayar "Deep Blue"'yu icat etmişlerdir. Dünya satranç şampiyonu Garry Kasparov ile maç yaptırılan Deep Blue, Kasparovu 2.5'a 3.5 puan ile yenmiştir. Böylelikle tarihte ilk kez bir bilgisayar satranç şampiyonunu yenmiştir. [16]

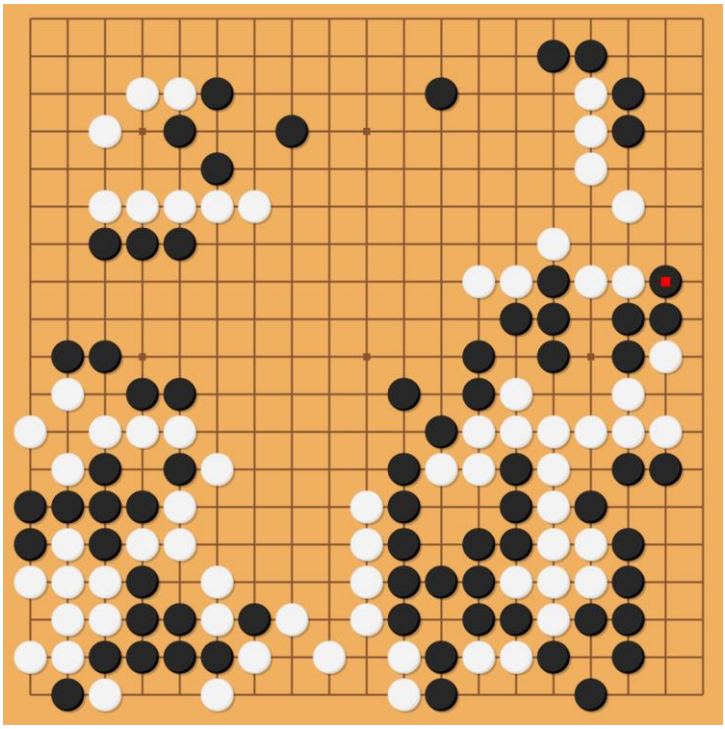
---

10 Woolf, s. 147.
11 Anderson, J. R./Boyle, C. F./Yost, G.: *The Geometry Tutor*, IJCAI 1985, s. 12.
12 Woolf, s. 147.
13 Shute/Psotka, s. 580.
14 Anderson, J. R./Reiser, B. J.: *The LISP Tutor*, BYTE 1985, C. *10,* S. 4, s. 162.
15 Shute/Psotka, s. 580.
16 Campbell, M./Hoane, A. J./Hsu, F. H.: *Deep Blue,* Artificial intelligence 2002, C. *134, S.* 1-2, s. 59.

2001 – İlk sosyal robot Kısmet, Cynthia Breazeal tarafından MIT laboratuvarlarında geliştirilmiştir. Bu robot, insanlar gibi mimiklerini kullanabilen, sosyalleşebilen, öğrenebilen, sesini, ifadelerini ve kafa hareketlerini kullanabilmektedir.[17]

2011 – Apple Siri, IBM Watson gibi kişisel asistanlar, Cortana ve Jeopardy geliştirilmiştir. Apple Siri kişisel asistandır. IBM tarafından geliştirilen Watson ve Jeopardy ise doğal dilde sorulan soruları yanıtlayabilen bilgisayar sistemidir.

2015 – Alphago, Google Deepmind'ın geliştirdiği Şekil 3'te görülen Go oyununu oynayan programdır. Bu program profesyonel Go oyuncusunu yenen ilk program olmuştur.



***Şekil 3**. Go Oyunu*

2018 – BERT, Google'ın aramalara daha hızlı ve doğru yanıt verebilmek için geliştirdiği doğal dil işlemeli algoritma tekniğidir.

[17] Breazeal, C.: *Designing Sociable Robots*. MIT 2004, s. 5.

2019 – GPT-2 (Generative Pre-trained Transformer 2), OpenAI şirketinin büyük bir dil modelidir. 8 milyon web sayfasından oluşan veri kümesi için önceden eğitilmiş doğal dil işleme sinir ağıdır.

2020 – GPT-3

2021 – DALL-E, OpenAI tarafından yayınlanan, yazı ile tarif edilen resimleri oluşturan yapay zekâdır.

2023 – GPT-4, Gemini, Sora ve Microsoft Copilot

7 Şubat 2023'te Microsoft tarafından geliştirilen Copilot, bir chatbot'tur. Şiirler ve şarkılar yazabilmektedir. Üretimi durdurulan Cortana'nın birincil alternatifidir.

14 Mart 2023'te, OpenAI tarafından oluşturulan çok modlu büyük bir dil modeli olan GPT-4, GPT serisinin dördüncüsüdür. GPT-4, 25.000'den fazla kelimeyi işleme kapasitesine ulaşarak daha uzun içerikler oluşturabilir, daha karmaşık konuşmaları anlayabilir ve buna cevap verebilir, belgelerde buna göre arama yapabilir ve belgeleri analiz edebilmektedir. Şarkı bestelemek, senaryo yazmak veya kullanıcının yazma stilini öğrenmek gibi yaratıcı ve teknik yazma görevlerini kullanıcılarla birlikte oluşturabilir, düzenleyebilir ve yineleyebilir.

21 Mart 2023'te eski ismiyle Bard olarak bilinen Gemini, Google AI tarafından geliştirilen bir sohbet robotudur.

Sora, OpenAI tarafından geliştirilen, metinden videoya dönüştürme konusunda uzmanlaşmış üretken bir yapay zekâ modelidir. Kullanıcıların yazdıklarından 60 saniyelik videolar üretebilmektedir.

Yapay zekânın hayatın her alanında kullanılmasıyla elde edilen büyük veri oldukça hızlı bir şekilde artmaya başlamıştır. Bununla birlikte yapay zekâ kendisine çeşitli uygulama alanları bulmaktadır. Eğlence, eğitim, ulaşım ve bankacılık gibi sektörlerde oldukça yaygın bir şekilde kullanılmaktadır. Sanal sınıflar, eğitimde akıllı yönetim sistemleri, otonom araçlar, kişisel asistanlar ve yüz tanıma gibi birçok alanda kullanılmaktadırlar.[18]

[18] Arslan, K.: *Eğitimde yapay zekâ ve uygulamaları.* WAJES 2020, C. *11, S.* 1, s. 80.

II. EĞİTİMDE YAPAY ZEKÂ TÜRLERİ

A. UZMAN SİSTEMLER (EXPERT SYSTEMS)

Yapay zekânın tarihi incelendiğinde uzman sistemlerin yeni olmadığı ve yapay zekâ programlama tekniklerinden biri olduğu görülmektedir. Bilgi tabanlı sistemler olarak adlandırılabilmektedirler. Uzman sistemler, alanında uzmanlaşmış kişilerin gerçekleştirdiği zorlu görevi yerine getirmek için oluşturulan, bilgi ve çıkarıma dayanan bilgisayar programlarıdır.[19] Örneğin, herhangi bir alanda uzman olan insanlar uzman olduğu alana yönelik bilgilere sahip ise uzman sistemlerde ilgili alan ile ilgili veri tabanına sahiptirler. Aynı şekilde alanında uzman insanlar bilgilerine göre bir çıkarımda bulunup karar vermektedirler. Uzman sistemlerde sahip oldukları veri tabanındaki bilgilere göre sonuca varabilirler. Uzman sistemlerin etkili kullanımı için (1) bilgi yenileme, (2) bilgi tabanı, (3) karar mekanizması ve (4) arayüz olmak üzere dört temel modüle ihtiyaçları vardır.[20] Örneğin, herhangi bir alanda uzmanlaşmış kişi elde ettiği bilgilere (bilgi tabanı) dayanarak bir çözüm (çıkarım) ürettiği gibi, uzman sistemlerde de durum benzer olmaktadır.[21] Ek olarak günümüzde bu denli hızla artan bilgilerin saklanabilmesi ve istenilen bilgiye en kısa sürede erişim sağlanabilmesi de amaçlanmaktadır (AÖF).

Eğitim alanında düşünüldüğünde, uzman sistemlere ihtiyaç duyulması, öğrencilerin danışmaları gereken durumlarda uzman hocalarına istediği her zaman ulaşım sağlayamamasından kaynaklanmaktadır. Bir alanda uzman olunabilmesi için en az 5 yıllık bir tecrübe ve uzun bir süre eğitim alınmaktadır. İlgili alanda uzman olan öğretmen, mühendis veya doktor bir süre sonra yorulabilmektedir. Ancak uzman sistemlerde böyle bir durum olmamakla birlikte 7/24 aynı performans ile çalışabilmektedirler. Uzman sistemlerin yapay zekâdan farkı düşünülecek olur ise, uzman sistemler alanında uzman bir insanın çözebileceği problemleri çözerken, yapay zekâ uzman olmayan herhangi bir insanın çözebileceği problemleri çözebilmektedir.[22] Bu yüzden uzman sistemler, eğitimde öğrenme stratejilerinin belir-

---

19 Önder, H. H.: *Uzaktan Egitimde Bilgisayar Kullanimi ve Uzman Sistemler*. *TOJET 2003*, C. *2, S.* 3, s. 143.

20 Önder, s. 145.

21 Arslan, s. 82.

22 Arslan, s. 76.

lenmesi, öğrenci başarısının tahmini, öğrenme modeli seçimi, yabancı dil öğretimi, değerlendirilme yapılması ve öğrenci, veli veya öğretmene dönüt verilmesi gibi durumlarda kullanılabilmektedirler.[23]

Eğitim alanında en geniş çaplı geliştirilen ve en çok bilinen uzman sistem, Stanford Üniversitesinde, tıp alanında bakteriyel hastalıkların teşhis ve tedavisinde kullanılmak üzere MYCIN geliştirilmiştir.[24] Yine tıp alanında geliştirilen uzman sistemlere de şunları örnek verebilmek mümkündür: Puff(Akciğer hastalıkları), Casnet(Glokoma), Internist(İç Akciğer hastalıkları), VM(Yoğun Bakımda Kontrol), ONCOCIN(Onkoloji), PIP(Böbrek Akciğer hastalıkları), Digitalis Therapy Advisor(Diyaliz), EXPERT(Ekeltroforez Tahlil Sonuçları), HodgKins(HodgKin Akciğer hastalığı), Hearmed(Psikofarmoloji Danışma), IRIS(Glokoma), GUIDON(Enfeksiyon Hastalıklarını Öğrenme) ve MDX(Teşhis).

B. AKILLI ÖĞRETİCİ SİSTEMLER

1960 ve 1970'li yıllarda ortaya çıkan Bilgisayar Destekli Öğretim uygulamaları ele alındığında yapay zekâda akıllı öğretici sistemlerin gelişimi anlaşılabilmektedir. BDÖ'nün en parlak çağında İllionis Üniversitesi tarafından PLATO isimli öğretim sistemi geliştirilmiştir. Bu sistem sayesinde öğrenciler aynı anda interaktif ders materyallerine erişim sağlayabilirlerdi. PLATO sisteminde aynı anda materyale erişimi sağlanırken, her öğrencinin ayrı özelliklere sahip olduğunun göz ardı edildiği görülmektedir. Bu yüzden ortaya çıkan yeni ihtiyaçları giderebilmek için yeni yaklaşımlar geliştirilmesi gündeme gelmiştir. SCHOLAR, Jaime Carbonell tarafından akıllı öğretici sistemlerin ilk örneği ortaya çıkmıştır.[25] BDÖ modelinin sonraki nesli olan akıllı öğretici sistemler ile günümüzde de oldukça önemli olan, eğitimde bireyselleştirilmiş öğrenme ortamları sunulmaktadır. Akıllı öğretici sistemler, öğretim içeriği ve öğrenme stratejileri ile ilgili ayrı ayrı veri tabanlarına sahip bilgisayar tabanlı öğretim sistemleri olarak tanımlanmaktadır.[26] Bu sistemler, öğrenciye kendi hızında, kendi ihtiyaçlarına göre

---

[23] Korucu, A. T./Biçer, H.: Eğitimde Yapay Zekanın Rolleri ve Eğitsel Yapay Zeka Uygulamaları, (ed. Nabiyev, V. ve Erümit, A. K.), "Eğitimde Yapay Zeka Kuramdan Uygulamaya", 3. Baskı, Ankara 2022, s. 52.

[24] Doğaç, s. 88.

[25] Carbonell, J. R.: *AI in CAI: An Artificial-İntelligence Approach to Computer-Assisted İnstruction.* IEEE Transactions on Man-Machine Systems 1970, C. 11, *S.* 4, s. 191.

[26] Arslan, s. 83.

ve kendi başarı seviyesine göre bireysel öğrenme deneyimi yaşatmaktadır. SCHOLAR'dan sonra, WHY, SOPHIE, LISP Tutor, Carnegie Learning, Jill Watson, EBA ADES, iTalk2Learn gibi birçok akıllı öğretici sistemler geliştirilmiştir.[27] [28] [29] [30] [31]

Yapay zekâ tabanlı akıllı öğretici sistemlerin, öğretme ve öğrenme amacıyla kullanımına örnek olarak Cognii ve Jill Watson verilebilmektedir. Akıllı değerlendirme ve öğrenme sistemi olan Cognii, bütün çevrim içi öğrenme ortamlarına entegrasyonunun sağlanması durumunda öğrenenlerin bireysel farklılıklarını göz önünde bulundurarak kişiselleştirilmiş eğitim olanağı sunmaktadır.[32] Makine öğrenmesi ve veri madenciliğini kullanan Cognii, öğrencilere konu üzerinde uzmanlaşıncaya kadar bire bir eğitim, doğal dil işleme teknolojisiyle açık uçlu sorularla değerlendirme, hızlı geri bildirim, öğrenci performansını hızlı bir şekilde değerlendirme olanaklarıyla kişiselleştirilmiş eğitim desteği sunmaktadır (Şekil 4). [33]

---

[27] Goel, A. K./Polepeddi, L.: *Jill Watson: A virtual teaching assistant for online education*. Learning Engineering for Online Education 2018, s. 1.

[28] Clearinghouse, W. W.: *Carnegie Learning Curricula and Cognitive Tutor (R) Software*. Institute of Education Sciences *2013, s. 1.*

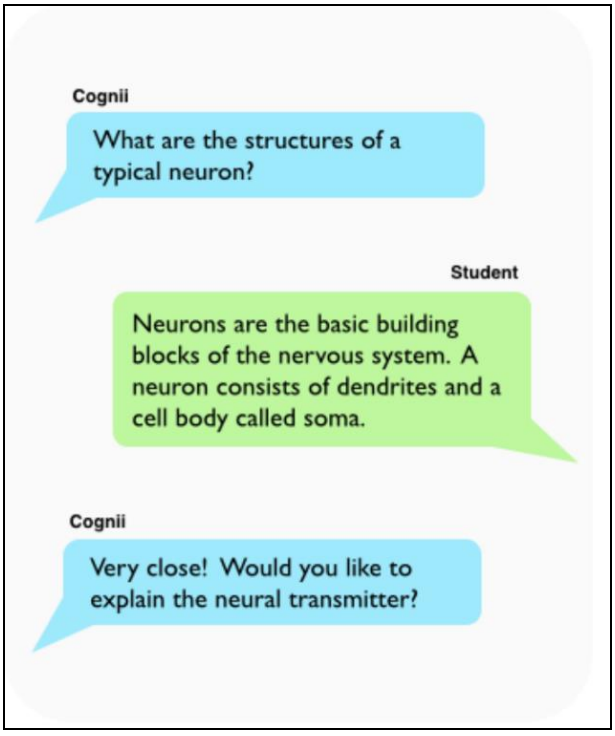
[29] Çetin, M./Aktaş, A.: *Yapay Zekâ ve Eğitimde Gelecek Senaryoları*. OPUS *2021*, C. *18, s.* 4230.

[30] MEB (2020), *EBA Akıllı Destek Sistemi*, (https://www.meb.gov.tr/1-milyona-yakin-ogrenci-eba-akademikdestek-sistemi-ile-universite-hedefine-ilerliyor/haber/20798/tr,E.T.: 11.03.2024)

[31] Grawemeyer, B./Mavrikis, M./Holmes, W./Gutiérrez-Santos, S./Wiedmann, M./Rummel, N.: *Affective Learning: Improving Engagement and Enhancing Learning With Affect-Aware Feedback*. User Model User Adap Inter 2017, C. *27*, s. 124.

[32] COGNII (2024), Cognii Virtual Learning Assistant, (https://cognii.com/, E.T.: 11.03.2024).

[33] Şenocak, D.: *Açık Ve Uzaktan Öğrenme Ortamlarında Yapay Zekâ: Sunduğu Fırsatlar Ve Yarattığı Endişeler.* AUAd 2020, C. *6, S.* 3, s. 65.



Şekil 4. *Cognii Akıllı Öğretici Sistemi*

C. DİYALOG TABANLI ÖĞRETİCİ SİSTEMLER

Öğrenciler için bire bir öğretimin her zaman daha etkili olduğu düşünülmektedir. Bloom, sınıf ortamında eğitim alan öğrencilerden ziyade öğretmenden kişisel olarak eğitim alanların daha başarılı olduğunu belirtmektedir. Buradan hareketle etkili bir öğrenme ortamı oluşturma amacıyla CIRSCIM, doğal dil işleme ve üretim mekanizmaları kullanarak etkileşimli diyaloglar üretebilmektedir.[34] Diyalog tabanlı öğretici sistemler, cevap doğru ise devam et, kısmen doğru ise bilgi ver devam et, neredeyse doğru ise iç içe geçmiş bir yöntem bul, bilmiyorum ise, cevabı ver ve devam et gibi kuralları kullanmaktadır.[35] CIRSCIM 1980 yılında üretimi başlamış, ilk versiyonundan üçüncü versiyonuna kadar gelişerek üretilmiştir. Son versiyonunda öğrenen yanıtları tahmin tablosu üzerinde puan verip, nitel

[34] Uzun, Y./Tümtürk, A. Y./Öztürk, H.: *Günümüzde ve Gelecekte Eğitim Alanında Kullanılan Yapay Zeka*. ICEANS 2021, C. 1, s. 4.

[35] Holmes/Bialik/Fadel, s. 653.

tahmin verileri istemektedir. İşlem sıralarını takip eden, elde ettiği verilere dayanarak tahmin sonuçları elde eden, eğitimi planlayan, işlem sıralarına göre öğrencilere yol gösteren yapı şeklini almıştır.[36]

CIRSCIM'e ek olarak; AutoTutor ve WatsonTutor, diyalog tabanlı öğretici sistemlerinin örneklerindendir. Memphis Üniversitesi'nde Akıllı Sistemler Enstitüsündeki araştırmacılar tarafından AutoTutor geliştirildi ve bir "öğretmen" ile bir öğrenci arasındaki konuşmaları simüle etmek için en etkili sistemlerden biri olarak kabul edilmektedir. Bu sistem özellikle bilgisayar bilimi, fizik ve biyoloji gibi alanlarda öğrencilere adım adım çevrim içi görevler konusunda rehberlik etmek için kullanılabilmektedir. AutoTutor'un temel amacı, öğrencileri ayrıntılı cevaplar vermeye ve konu hakkında derinlemesine bir anlayış geliştirmeye teşvik etmektir. AutoTutor'daki eğitim diyalogları genellikle beş aşamayı takip eder. İlk olarak AutoTutor bir soru veya sorun sunar. Daha sonra öğrenci kendi cevabıyla cevap verir. Sistem daha sonra öğrencinin cevabını değerlendirir ve değerlendirmesine bağlı olarak geri bildirim, düzeltmeler, sorular, rehberlik, ipuçları, açıklamalar veya bir özet sağlar. Son olarak, öğrencinin cevabını iyileştirmek için ikinciden dördüncüye kadar olan adımlar tekrarlanır.[37]

III. EĞİTİMDE KULLANILAN YAPAY ZEKÂ ARAÇLARI

Yapay zekâ araçları, öğrencilerin kişiselleştirilmiş öğrenme ortamlarında zenginleştirilmiş öğrenme deneyimleri yaşamalarını kolaylaştırmaktadır. Aynı zamanda, öğretmenlerin derslerine yönelik materyal hazırlamalarına yardımcı olmaktadır. Üretken yapay zekâlar ise sinir ağlarını ve derin öğrenmeyi kullanarak eğitilerek verileri işler, anlamlandırır, üretir ve dönüştürürler.[38] Bu işlemler gerçekleştirildiğinde, sanki gerçek insan ürünü olarak yapılmış hissiyatı vermeleri de insanları heyecanlandırmaktadır.[39] İleri düzey içeriklerin oluşturulması için geliştirilen üretken yapay zekâ, eğitimde çoğunlukla işlerimizi kolaylaştırmaktadır.[40]

---

36 Arslan, s. 84.

37 Graesser, A. C./VanLehn, K./Rosé, C. P./Jordan, P. W./Harter, D.: *Intelligent Tutoring Systems with Conversational Dialogue*. AI magazine 2001, C. *22, S.* 4, s. 39.

38 Bozkurt, s. 65.

39 Lim, W. M./Gunasekara, A./Pallant, J. L./Pallant, J. I./Pechenkina, E.: *Generative AI And The Future of Education: Ragnarök or Reformation? A Paradoxical Perspective from Management Educators.* The İnternational Journal of Management Education 2023, C. *21, S.* 2, s. 3.

40 Cao, Y./Li, S./Liu, Y./Yan, Z./Dai, Y./Yu, P. S./Sun, L.: *A Comprehensive Survey of AI-Generated Content (AİGC*): *A History of Generative AI from GAN To ChatGPT*, 2018, C. 37, S. 4.



Şekil 5. *Eğitimde Yapay Zekâ Araçları Kavram Haritası*

Bu bölümde, öğrenme ortamlarında kullanılabilecek yapay zekâ uygulamaları kullanım alanlarına göre Şekil 5'te görüldüğü gibi 13 ayrı alanda sınıflandırılarak bazı araçların kullanımlarına yer verilmektedir.

A. ÇEVİRİ ARAÇLARI

Öğretim süreçlerinde insanların çevirmekte zorlanacağı veya çeviri süresinin uzun olacağı metinler yapay zekânın desteği ile birlikte kolayca çevrilebilmektedir. Google Translate, Alexa, Deepl, Microsoft Translator, Quillbot, Microsoft Presentation Translator gibi birçok çeviri aracı bulunmaktadır. [41]

Ücretsiz online çeviri aracı olan *Google Translate*, web sayfalarını, metinleri veya görselleri herhangi bir dilden hedef bir dile çevirebilmektedir. Amazon tarafından geliştirilen *Alexa*, 2002'den beri hukuk, finans, teknik,

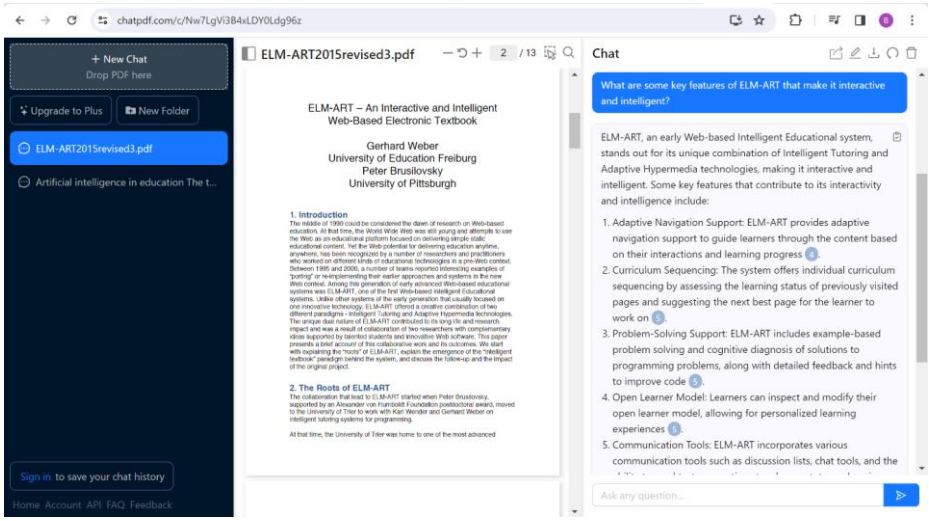
41 Polat, N. T.: *Yapay Zekâ ve Çeviri: Mütercim-Tercümanlık Alanında Yeni Bir Paradigma*, Diyalog *2023*, C. *11, S.* 2, s. 487.

devlet ve pazarlama sektörlerindeki belgeleri çevirmek için kullanılabilen araçlardandır. 100 belgeye kadar çeviriye imkân tanımaktadır. Tanınırlığı yeni ortaya çıkan *Deepl*, Windows ve iOS ile uyumlu masaüstü uygulaması da olan çeviri aracıdır. Ücretsiz versiyonda 5000 kelimeye kadar çeviri yaparken, 5000 kelimeden fazla çeviri istenildiğinde pro versiyonu ile ücretli hizmet sunmaktadır. Microsoft'un ürettiği çok dilli makine çeviri programı olan *Microsoft Translator*, uygulama şeklinde ve web olarak kullanılabilmektedir. 2017 yılında geliştirilen Quillbot, dili algılayarak çeviri yapmaktadır. Girilen metinlerin akademik ve gündelik yazım seçenekleri ile yorumlayabilmektedir. Görüntüyü yazıya, sesi yazıya çevirebilmektedir. El yazısı karakterlerini algılamaktadır. Genellikle metinleri yeniden yazmak ve farklı şekillerde ifade etmek için kullanılmaktadır. Microsoft'un powerpoint için sunu çevirici aracı olan *Presentation Tool*, yapay zekâ teknolojilerinden faydalanarak, canlı bir sunum yapıldığı sırada sunum dilini algılayarak çeviri yapabilmektedir.

B. SOHBET ROBOTLARI

Sohbet robotları eğitimin çeşitli süreçlerine entegre edilmektedir. Öğrencilerin ilgilerini çektiği ve motivasyonlarını sağladığı bilinmektedir. Dolayısıyla eğitim süreçlerinde destek sağlaması ve içerik paylaşımında kullanılabilmektedir. Chatgpt, Ivy Sohbet Botu, Chatpdf, Question.ai, m-Health, Merlin ve Methbot gibi sohbet robotları bulunmaktadır. Bu sohbet robotları öğrencilerin ödev hazırlamasına, yeni içerik üretmesine veya herhangi bir kodun çıktısını görmelerine yardımcı olmaktadır.

Günümüzde en çok duyulan ve bilinen *ChatGPT*, ChatGPT 3.5 versiyonu, ücretsiz olmakla beraber kişinin girdiği metnin diline göre kişiye uygun cevaplar verebilmektedir. Ancak ChatGPT'nin eğitildiği veri kümesi 2021 yılı itibari ile son bulduğu için kullanıcılara güncel bilgi verememektedir. Ücretli versiyonu olan ChatGPT 4.0 ise, görüntü işleme ve daha yüksek kelime işleme kapasitesine sahiptir. Diğer bir sohbet robotu olan ChatPDF'te ise, öğrenci okuması gereken pdf'i uygulamaya yükleyerek pdf dosyasının özetini elde edebilmektedir. Buna ek olarak, öğrenci özeti okuduktan sonra aklında soru işareti kalan soruları uygulamaya yazarak cevap alabilmektedir.



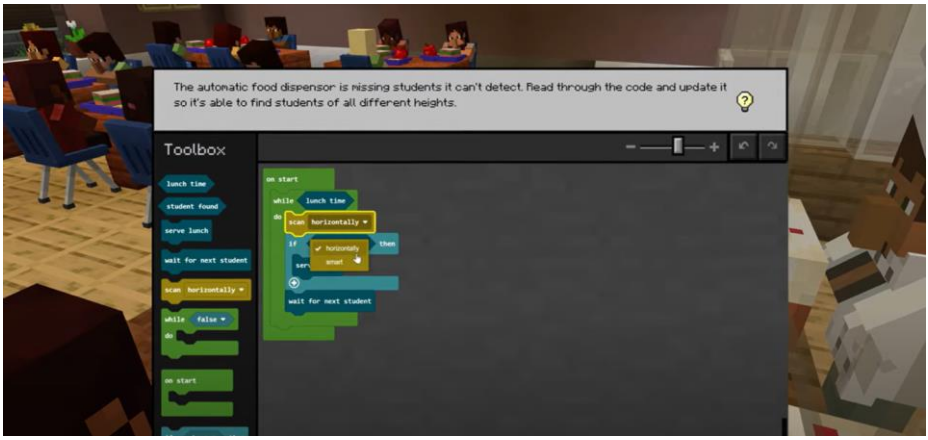
Şekil 6. *Chatpdf'te Kullanım Ekranı*

Şekil 6'da görüldüğü gibi ilgili pdf dosyası uygulamaya yüklenerek özeti istenir ardından sağ tarafta görüldüğü gibi içerik hakkında herhangi bir soru yönlendirildiğinde yapay zekâ uygulaması cevap vermektedir. Ücretsiz versiyonunda günde 3 dosyaya kadar izin vermektedir. Daha fazlası için Plus versiyonuna yükseltilmesi gerekmektedir.

C. ÖĞRENME ORTAMLARI

Yaşam boyu öğrenmeyi destekler nitelikte, eğitimde fırsat eşitliğini sağlayarak; programlamadan tıp eğitimine, pazarlamadan kişisel gelişime kadar çeşitli alanlarda kursları içeren öğrenme ortamları da artık yapay zekâ teknolojisini kullanmaktadır. Udemy, Coursera, EdX, Udacity, Elementsofai.com, Ocw.mit.edu, Duolingo ve Future Tools gibi yapay zekâ araçları bulunmaktadır. Eğitim ihtiyacına uygun, bireyi destekleyen eğitim seçildikten sonra Udemy, Coursera, Udacity gibi ortamlarda sertifika sahibi olunabilmektedir. Ayrıca, sistemde kayıt olunan eğitimler doğrultusunda tahminlerde bulunarak çeşitli eğitim içerikleri sunmaktadır. Örneğin, bu ortamlardan herhangi birini kullanan öğrenci büyük veri ile ilgili bir eğitim aldı ise, ona yapay zekâ, derin öğrenme gibi eğitimleri önerebilmektedir. Günümüzde eğitimde oyunlaştırma oldukça yaygın ve 21. yy öğrencilerine daha uygun olduğu için, bahsedilen uygulamalara ek olarak; Minecraft, *ProjectMalmo,* Assassin's Credd, Classcraft gibi eğitsel yazılım uygulamaları da kullanılmaktadır.

Minecraft, İsveçli Markus Alexej Persson'ın geliştirdiği açık dünya oyunudur. Bu oyunda yer alan çeşitli dünyalarda üç boyutlu kutular bir araya getirilerek farklı nesneler tasarlanmaktadır. Minecraft'ta tamamen özgün tasarımların yapılabileceği Creative Mod ile Survival Mode bulunmaktadır. Microsoft ile iş birliğinden sonra "Minecraft Education" ortaya çıkmıştır. Öğrencilerin problem çözme becerilerini geliştirecek, yaratıcılık ve iş birliğine dayalı öğrenme ortamı sunacak eğitsel oyunlar inşa edilmektedir.[42] Özellikle STEM'e uygun oyunlar ve bilgisayar bilimi oyunları bulunmaktadır. Şekil 7'de Minecraft education demo sürümünde gösterilen kodlama oyunu görülmektedir.



Şekil 7. *Minecraft: Generation AI Oyunu*

Microsoft firmasının açık kaynak olarak geliştirdiği ProjectMalmo projesinde Minecraft ile yapay zekâ teknolojisi bütünleştirilmiştir. Minecraft'a ek olarak API ve soyutlama katmanı eklenmiştir. Bu katmanda hayatta kalma, iş birliği ve problem çözme gibi yerine getirilmesi gereken görevler bulunmaktadır. Minecraft'taki karakterlerle doğrudan insan kaynaklı girdiler ile öğrenebilmektedir.

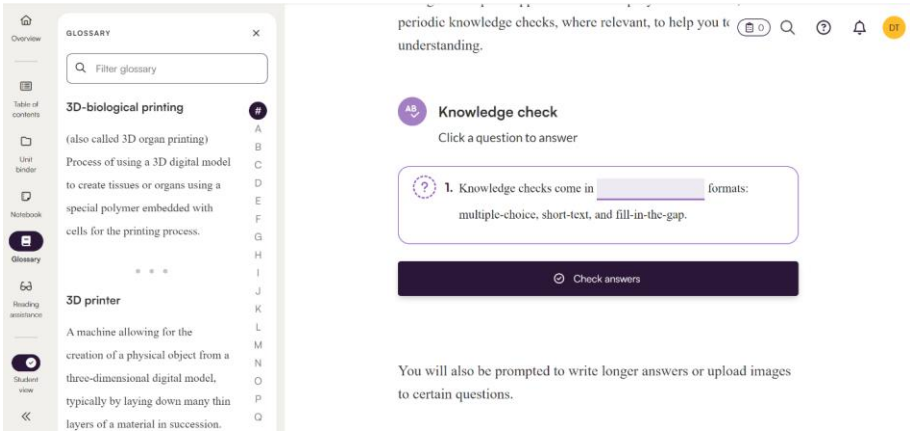
D. DİJİTAL DERS KİTAPLARI

Ders kitapları, öğretim materyalleri arasında en eski ve en yaygın biçimde kullanılmaktadır. Basılı kitapların herhangi bir içeriğinin değiştirilmesi veya öğrencinin kitapla etkileşime girmesi mümkün olmamakta idi. Ancak yapay zekânın gelişmesiyle birlikte dijital kitaplarda, metin kesme-

[42] Eroğlu, B.: *Dijital Video Oyunları ve Eğitim: Minecraft Eğitim Sürümü*. Anadolu Öğretmen Dergisi 2019, C. *3, S.* 1, s. 58.

yapıştırma, altını çizme, sayfalar arası dolaşım, metin içinde arama yapma gibi etkileşimler mümkün hale gelmiştir. Bu etkileşimler sayesinde öğrencilerinin tercihlerine göre çalışan sistemler derslerde ve ders dışı etkinliklerde kullanılır hale gelmiştir.[43]

Kognity, akıllı dijital ders kitapları üretmek için öğretmenler, müfredat uzmanları ve içerik geliştiricilerle birlikte çalışan bir şirkettir. Amacı, ders kitaplarının statik tek yönlü yapısını dinamik, iki yönlü bilgi akışına dönüştürmektir. Kitaplar uluslararası kabul görmüş akredite ortaöğretim programları temel alınarak yazılmıştır. Pek çok dijital ders kitabında yer alan video, animasyon ve simülasyonların yanı sıra bu kitaplarda öğrencilerin daha kaliteli öğrenmelerini sağlamak için otomatik işaretleme, anlık geri bildirim sistemleri, etkileşimli sözlükler, kapsamlı sınav uygulaması ve danışmanlık hizmetleri de yer almaktadır.[44] Şekil 8'de görüldüğü gibi Kognity'de kitap içinde boşluk doldurma soruları, cevabı kontrol etme etkileşimleri bulunmaktadır. Bunlara ek olarak sol menüde bulunan okuma asistanı ile de oluşturulan kitabı yapay zekâ seslendirebilmektedir.



Şekil 8. *Kognity'de Bulunan Dijital Kitap Örneği*

OpenStax'ın Rice Üniversitesi'nde başlattığı projenin ilk aşamasında, öğrencilerin ders kitaplarını nasıl kullandıklarına ilişkin üç yıl boyunca veriler toplandı. Burada elde edilen araştırma sonuçlarına dayanarak uyarla-

43 Odabaşı, F./İşman, A./Akkoyunlu, B.: *Eğitim Teknolojileri Okumaları,* 3. Baskı, Ankara 2023, s. 497.

44 Kognity (2024), Improving outcomes for students. Saving time for teachers, (https://kognity.com/why-kognity/, E.T.: 11.03.2024).

nabilir bir dijital ders kitabı geliştirildi. Bu kitaplar öğrencilere alışık oldukları ders kitabı içeriğini sunmanın yanı sıra kişisel tercihleri dikkate alan birçok ek özellik içermektedir. Kitap, öğrencilerin alıştırmalara/sorulara verdiği yanıtları arşivleyerek soruların ne zaman tekrar sorulması gerektiğini belirlemektedir. Konuları anlamakta güçlük çeken öğrencilere içerikte uzmanlaşmalarına yardımcı olacak görevler verilirken, bu konuda daha iyi olan öğrenciler materyali hızlı bir şekilde öğrenirler. Öğrenciler kitaptaki bölümleri bağımsız olarak inceleyebilir ve zamanlarını nasıl kullanacaklarına karar verebilmektedirler.[45]

Weber ve Brusilovsky (2016), hem etkileşimli hem de akıllı olan web tabanlı bir programlama ders kitabı üzerinde bir çalışma yürütmüştür. Bu ders kitabı, geleneksel basılı programlama kitaplarına benzer şekilde hiyerarşik bir yapı izleyerek çeşitli ünite ve konuları kapsamaktadır. Temel kavramların açıklamalarını, program örneklerini ve okuyucuların çözmesi gereken soruları içermektedir. Ancak statik basılı kitaplardan farklı olarak bu etkileşimli ders kitabı dinamik bir deneyim sunmaktadır. Kullanışlı bir gezinme aracı olarak hizmet veren ve kullanıcıların kitabın herhangi bir bölümüne tek tıklamayla kolayca erişmesine olanak tanıyan bir içindekiler sayfasına sahiptir. Ayrıca sözlükler gibi tamamlayıcı gezinme araçlarına da sahiptir. Kullanıcılar program örneklerini farklı parametrelerle çalıştırma ve ilgili sonuçları gözlemleme yeteneğine sahiptir. Ayrıca kitaptan geri bildirim alarak problem çözme sürecindeki ilerlemeler takip edilebilmektedir. Etkileşimli kitap, özellikle örnekler ve problemler arasında akıllıca bağlantılar kurarak öğrencileri en ilgili bölümlere etkili bir şekilde yönlendirme sağlamaktadır. Tüm bu süreçler yapay zekâ teknolojilerinin uygulanmasıyla kolaylaştırılmaktadır.

E. SESLİ ASİSTANLAR

Yapay zekânın en yaygın olarak kullanıldığı alanlardan birisi sesli asistan uygulamalarıdır. Amazon Alexa, Google Home, Apple Siri ve Microsoft Cortana, Microsoft Copilot gibi sesli asistanlar, öğretim materyali olarak da kullanılmaktadır. Sesli asistanlar, öğrencilere bir öğretmenin doğrudan etkisi olmadan eğitim materyalleriyle bağımsız olarak etkileşime geçme fırsatı sunar. Sesli asistan uygulamaları hem evde hem de akademik olma-

[45] Rutkin (2024), Digital Textbooks Adapt to Your Level as You Learn, (https://www.newscientist.com/article/mg22329832-600-digital-textbooks-adapt-to-your-level-as-you-learn/, E.T.: 10.03.2024)

yan ortamlarda, zaman fark etmeksizin öğrenme deneyimini geliştirecek öğretim yardımcıları veya araçları olarak kullanılabilir. Üniversitelerde ve kolejlerde, geleneksel basılı öğrenci el kitaplarının yerine, kampüsle ilgili çeşitli soruların yanıtlanması için öğrencileri sesli asistanlarla donatmaktadır. Bu sesli asistanlar yalnızca kampüs kaynaklarıyla ilgili sık sorulan sorulara yanıt vermekle kalmıyor, aynı zamanda her öğrencinin özel program ve derslerine göre uyarlanmış özelleştirme seçenekleri de sunuyor. Bu, personel üyelerinden kapsamlı dahili destek ihtiyacını ortadan kaldırırken aynı zamanda fiziksel el kitaplarının basılmasıyla ilgili israfı da azaltır. Sesli asistan sistemlerinin kullanımı öğrencilerin çoğunluğu için inanılmaz derecede büyüleyici ve ilgi çekicidir.[46]

F. BENZERLİK ORANI KONTROLÜ

Eğitim süreçlerinde öğretmenlerin öğrencilerine verdikleri ödevlerin değerlendirme aşamalarında kullanılabilecek intihal kontrolünü sağlayabilecekleri çeşitli uygulamalar bulunmaktadır. İthenticate ve Turnitin en yaygın kullanılan uygulamalardır. Bunlara ek olarak; PlagScan, writer AL Content Dedector, Copyleaks AI Detector uygulamaları da benzerlik oranı kontrollerinde kullanılabilmektedir. Akademik yayın yazımı sırasında veya hazırlanan ödevlerdeki metinlerin benzerlik oranlarını diğer belgelerle karşılaştırmaktadır. Bu karşılaştırmaların yapılabilmesi için kullanıcının öncelikle sistemi kayıt olması, ardından ilgili belgeyi sisteme yüklemesi gerekmektedir. Sisteme yüklenen belgeler, uygulamanın veri tabanında kayıtlı olan metinlerle karşılaştırılarak benzerlik raporu oluşturulur. Oluşturulan raporda benzerlik tespit edilen metinler farklı renklerle numaralandırılarak işaretlenir ve hangi kaynakla benzerlik gösterdiği belirtilir. Yapay zekâ desteğinin bu uygulamalara gelmesi ile birlikte, benzerlik denetimi yaptırılan metnin herhangi bir yapay zekâ uygulaması ile yazılmış olma ihtimali de kontrol edilebilmektedir.

G. NOT TUTMA

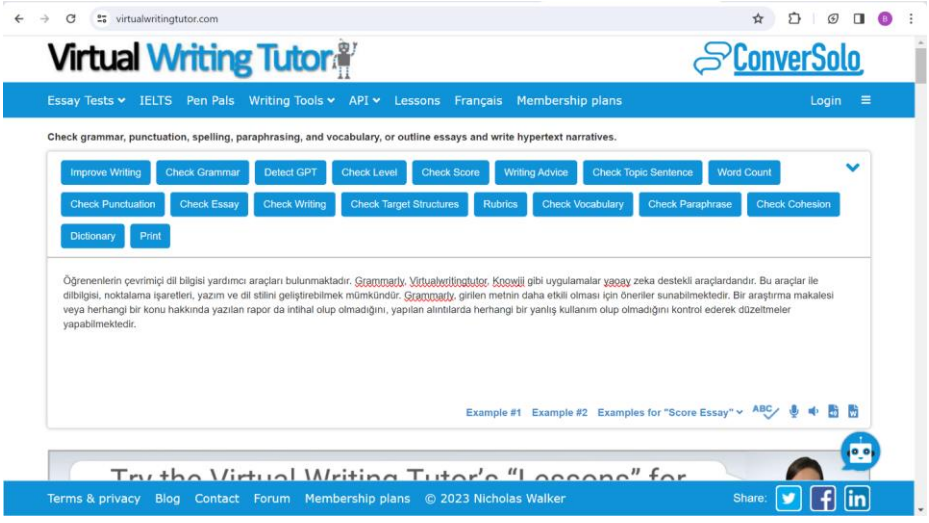
Eğitimde not tutma oldukça önemlidir. Öğrenme ortamlarında kullanılan teknolojilere göre öğrencilerin veya öğretmenlerin not tutma alışkanları değişmektedir. Eskiden kalem kâğıt ile alınan notlar şu an yapay zekâ desteği ile birlikte dijitalde alınmaktadır. Dijitalde not almayı sağlayan Note-

[46] Schmelzer (2019), AI Applications in education, (https://www.forbes.com/sites/cognitiveworld/2019/07/12/ai-applications-in-education/#38e39b0c62a3, E.T.: 10.03.2024)

bookLM, Google Keep, Evernote, Microsoft OneNote gibi araçlar bulunmaktadır. Google'ın yapay zekâ destekli not alma aracı olan NotebookLM, Google dokümanlar ile birlikte çalışarak, doküman hakkında soru sorabilme özelliğine sahiptir. Var olan dokümanlar üzerinden yeni dokümanlar oluşturulabilmektedir. Google Keep, daha önce alınan notları kişiye özel gruplandırarak önemli bilgileri vurgulamaya yardımcı olurken, sesli not alma ve resim tanıma gibi özellikleri de bulunmaktadır. OneNote ise Microsoft'un sesler ve görüntüler algılanarak yazıya dönüştürülürken makine öğrenmesinden faydalanan yapay zekâ destekli not tutma aracıdır.

H. DİL BİLGİSİ

Öğrenenlerin çevrim içi dil bilgisi yardımcı araçları bulunmaktadır. Grammarly, Virtualwritingtutor, Knowjii gibi uygulamalar yapay zekâ destekli araçlardandır. Bu araçlar ile dil bilgisi, noktalama işaretleri, yazım ve dil stilini geliştirebilmek mümkündür. Grammarly, girilen metnin daha etkili olması için öneriler sunabilmektedir. Bir araştırma makalesi veya herhangi bir konu hakkında yazılan rapor da intihal olup olmadığını, yapılan alıntılarda herhangi bir yanlış kullanım olup olmadığını kontrol ederek düzeltmeler yapabilmektedir.

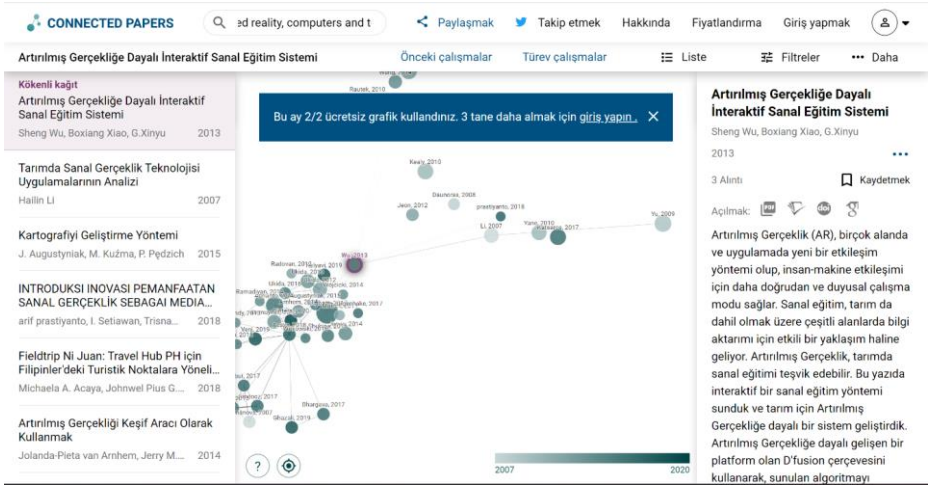


Şekil 9. *Virtualwritingtutor'da Dil Bilgisi Araçları Metni Kontrolü*

Şekil 9'da görüldüğü gibi yazılan metnin grammar, intihal, gpt ve yeniden yazma gibi çeşitli dil bilgisi kontrolü yapılabilmektedir.

I. GÖRSELLEŞTİRME & GÖRÜNTÜ OLUŞTURMA

Eğitimde soyut konuların somutlaştırılarak daha etkin ve verimli bir şekilde öğretilmesi, bilginin kalıcılığı açısından oldukça önemlidir. Bu yüzden öğretim materyallerinde görselleştirmeye oldukça dikkat edilmektedir. Yapay zekânın sunduğu Dall-E 2, Stable Difusion, Mid Journey, Vyond ve Connected Papers gibi görselleştirme araçları bulunmaktadır. Connected Papers, girilen kelimelerle alakalı olan makaleleri bulup görselleştirmeyi sağlamaktır. Örnek bir görselleştirme Şekil 10'da verilmiştir. Stable Diffusion'a girilen kelimeler sonucunda oluşturulan görsel ise Şekil 11'de görülmektedir.



Şekil 10. *Connected Papers ile Oluşturulmuş Makale Görselleştirmesi*



Şekil 11. *Stable Diffusion'un Oluşturduğu Görsel*

J. MAKİNE ÖĞRENMESİ VE PROGRAMLAMA

Eğitimde makine öğrenmesi ve programlama araçları öğrenmeyi kişiselleştirilmiş, etkili ve ilgi çekici hale getirmeye yardımcı olmaktadır. Bu yüzden yeni teknolojik araçlar oldukça yaygın bir şekilde tercih edilmektedir. Google Colab, Kaggle, Amazon SageMaker, Microsoft Azure Machine Learning, Github Copilot, Deepcode, Kite ve Tabnine en çok bilinen yapay zekâ araçlarıdır. Bu araçlar bulut ortamda kod yazılmasını ve çalıştırılmasını sağlayan platformlardır. Bu platformlarda veri bilimciler, makine öğrenmesi uzmanları bir araya gelerek veri kümeleri üzerinde çalışabilir ve yarışmalara katılabilirler. Yapay zekâ destekli makine öğrenmesi ve programlama

araçları, veri analizi, doğal dil işleme, görüntü işleme ve robotik gibi birçok farklı alanda kullanılmaktadır. Bu araçlar, programcıların ve veri bilimcilerin daha hızlı ve daha verimli çalışmasını sağlamaktadır. Yapay zekâ, kodlama görevlerini otomatikleştirmeye ve programcıların daha karmaşık problemlere odaklanmasına yardımcı olmaktadır.

K. SUNU OLUŞTURMA

Öğretmenlerin ve öğrencilerin sunum hazırlarken harcayacağı emeği ve zamanı azaltmaktadır. Daha etkileyici sunumlar hazırlayabilmek için sunumlara interaktif içerikler, animasyonlar ve görseller ekleyebilirler. Hedef kitleye uygun sunum oluşturabilir ve interaktif içerikleri ile öğrenci katılımını teşvik ederler. Farklı öğrenme şekillerine sahip bireylere uygun içerikler oluşturabilmektedir. Bunlar için kullanılabilecek yapay zekâ destekli Canva, Prezi, Slidebean AI, Beautiful.ai, Visme, Otter.ai ve Gamma.app araçları bulunmaktadır. Bu araçların ücretli ve ücretsiz kullanılabilen özellikleri bulunmaktadır.

L. MÜZİK VE AVATAR OLUŞTURMA

Adobe podcast, Elevenlabs, Lovo.ai, Soundverse, Mubert, Beathoven, Musenet, Amper Music, AIVA, Artbreeder, Craiyon, Midjourney ve Vroid Studio gibi yapay zekâ destekli müzik ve avatar oluşturma araçları bulunmaktadır. Bu araçlar eğitim içerikleri oluşturulurken içeriğe uygun müzik eklenmek istendiğinde kullanılabilmektedir. E-öğrenme içeriklerine uygun arka plan müzikleri veya resimlerden müzik oluşturulması gibi durumlarda kullanılabilmektedirler. Ek olarak eğitsel içerikler veya etkinlikler oluşturulurken öğrencilerin dikkatleri çekebilmek için öğrenci özelliklerine uygun avatarlar oluşturulmak istendiğinde ise Artbreeder, Craiyon, Midjourney ve Vroid Studio araçları kullanılabilmektedir. Yapay zekâ destekli bu araçlar ile metin komutlarına bağlı, resimler, animasyonlar ve avatarlar oluşturulabilmektedir.

M. VİDEO VE SES OLUŞTURMA

Eğitimde dikkat çeken ve kişiselleştirilmiş öğrenme içerikleri oluşturulurken videolaştırma ve görselleştirme oldukça önemlidir. Soyut konuların somutlaştırılmasında bu tür araçlar oldukça önemlidir. Synthesia, metin komutlarına dayalı avatarlar kullanarak videolar oluşturabilir veya metni videoya dönüştürebilmektedir. Pictory, metinleri videolara dönüştürmek

için yapay zekâ kullanan bir platformdur. Biteable, animasyonlu videolar oluşturmak için kullanılabilen bir platformdur. Yapay zekâ, videolarınız için arka plan müzikleri ve seslendirmeler otomatik olarak oluşturabilir. Animoto ise slayt gösterilerini videolara dönüştürmek için kullanılabilen bir platformdur. Yapay zekâ, videolar için geçişler ve animasyonlar oluşturabilmektedir. Videolara uygun seslendirme eklenmesi de eğitimde oldukça önemlidir. Kişilerin metinleri seslendirmesi ve eğitim slaytlarına veya videolarına eklemesi oldukça zahmetli olurken yapay zekâ, oldukça kolaylaştırmıştır. Resemble AI, ElevenLabs ve Murf AI, metinleri insan sesine dönüştürmek için kullanılabilen platformlardandır. Lovo ise metinleri anime karakterlerin seslerine dönüştürmek için kullanılabilmektedir.

IV. EĞİTİMDE YAPAY ZEKÂ KULLANIMININ AVANTAJLARI

- Son zamanlarda oldukça yaygın bir şekilde her alanda kullanılan yapay zekâ araçları, yönetimin daha etkili olmasını sağlayabilir. Akıllı sistemler sayesinde yöneticiler veya öğretmenler, öğrencilerin zayıf noktalarını görerek, ihtiyaçları olan konu hakkında destek verebilirler.[47]

- Öğrencilerde istenilmeyen türden bir davranış gözlemlendiğinde (okulu bırakma, şiddete meyil) öğretmenlere ve yöneticilere bildirimde bulunarak bilgilendirme yapabilmektedir.[48] Bu sayede öğretmenler veya yöneticiler gereken önlemleri alabilirler.[49]

- Ders süreçlerinde dikkatleri çok kolay dağılan öğrencilerin, oyunlaştırma gibi yapay zekâ teknolojileri ile dikkatleri çekilerek, eğitim sürecinde aktif rol alması sağlanabilmektedir.[50]

- Yapay zekâ destekli öğretim araçlarında, kişiselleştirilmiş öğretim sağlanabildiği için hangi öğrencinin kısa sürede hangi öğrencinin daha geç

---

47 Kuprenko, (2020). *Artificial İntelligence in Education: Benefits, Challenges, and Use Cases, (https://medium.com/towards-artificial-intelligence/artificial-intelligence-in education benefits-challenges-and-use-cases-db52d8921f7a*, E.T.: 10.03.2024)

48 Murphy, R. F.: *Artificial İntelligence Applications to Support K-12 Teachers and Teaching*. Rand Corporation 2019, s. 4.

49 İşler, B./Kılıç, M.: *Eğitimde Yapay Zekâ Kullanımı ve Gelişimi*. Yeni Medya Elektronik Dergisi 2021, C. *5, S.*1, s. 4.

50 Kuprenko (2020), *Artificial İntelligence in Education: Benefits, Challenges, and Use Cases, (https://medium.com/towards-artificial-intelligence/artificial-intelligence-in education benefits-challenges-and-use-cases-db52d8921f7a*, E.T.: 10.03.2024)

sürede öğrenebildiği verilerine ulaşılabildiği için öğretmenler sınıfta kişiye özgü öğretim uygulayabilirler.[51]

- Yapay zekâ araçları eğitimin zamandan ve mekândan bağımsız bir şekilde yürütülebilmesine imkân verdiği için öğrencilerin derste geri kalması veya derse katılmaması gibi durumları ortadan kaldırarak öğrencinin dersleri kolay takip edebilmesi sağlamaktadır. [52]

- Yapay zekâ araçları öğrencilerin hangi alanlarda zayıf olduklarını belirleyerek bu yönlerini geliştirmeleri için gerekli materyali sunabilir. Öğrencinin ihtiyacına göre çeşitli materyal önerileri veya uygun eğitim tavsiyesinde bulunabilir.[53] [54]

- Öğrencilerin ilerlemelerinin anlık takibi ve anında geri bildirim verilebilmesi için sanal öğretmenler kullanılabilmektedir. [55]

- Öğrencilerin dersle alakalı olan veya alakası olmayan konularla ilgili bilgi sahibi olmalarını sağlayan chatbotlar yabancı dil eğitimlerinde de kullanılmaktadır.[56]

- Her öğrencinin kendi hızına göre ve kendi kendine öğrenmesine daha kolay olanak sağlayan yapay zekâ teknolojileri, herhangi bir öğrenme güçlüğü olan bireylerin daha erken sürede fark edilmesini ve uygun öğretim planının hazırlanmasına yardımcı olmaktadır.[57]

---

51 Fahimirad, M.: *A Review on Application of Artificial İntelligence İn Teaching and Learning in Educational Contexts.* International Journal of Learning and Development 2018, C. 8, S. 4, s. 110

52 Kuprenko, (2020). *Artificial İntelligence in Education: Benefits, Challenges, and Use Cases, (https://medium.com/towards-artificial-intelligence/artificial-intelligence-in education benefits-challenges-and-use-cases-db52d8921f7a*, E.T.: 10.03.2024)

53 Kuprenko, (2020). *Artificial İntelligence in Education: Benefits, Challenges, and Use Cases, (https://medium.com/towards-artificial-intelligence/artificial-intelligence-in education benefits-challenges-and-use-cases-db52d8921f7a*, E.T.: 10.03.2024)

54 İşler,/Kılıç, s. 5.

55 Kuprenko, (2020). *Artificial İntelligence in Education: Benefits, Challenges, and Use Cases, (https://medium.com/towards-artificial-intelligence/artificial-intelligence-in education benefits-challenges-and-use-cases-db52d8921f7a*, E.T.: 10.03.2024)

56 Smutny, P./Schreiberova, P: *Chatbots for learning: A review of educational chatbots for the Facebook Messenger,* Computers & Education 2020, C. 151, s. 7.

57 Goel, A. K./Polepeddi, s. 1.

- Üretken yapay zekâ ile öğrenciler, öğretmenler ve yöneticiler gibi diğer eğitim paydaşları arasında iş birliğini kolaylaştırmaktadır. Bu iş birliği sayesinde etkili bir şekilde bilgi paylaşımı yapılabilmektedir.[58]

Yukarıda bahsi geçen avantajlara ek olarak; uyarlanabilir öğrenme ortamları desteği sayesinde aşağıdaki konularda pozitif yönde katkı sağlayacağı belirtilmektedir. [59]

- Eğitimde uyarlanabilir yapay zekâ araçları öğretmenlere rehberlik yapabilirler.
- Öğretmenlerin not verme, performans değerlendirme gibi işlemlerini otomatikleştirebilirler.
- Öğrencilerin bilgiye ulaşma şekillerini değiştirmektedir.
- Yapay zekâ destekli uygulamalardan elde edilen veriler doğrultusunda yürütülen çalışmalar, daha net bilgiler verebileceği için, deneme-yanılma işlemlerinde kolaylık sağlarlar.
- Yapay zekâ programları, öğrencilere ve öğretmenlere göre öğrenebilir ve uyarlanabilirler.

V. EĞİTİMDE YAPAY ZEKÂ KULLANIMININ DEZAVANTAJLARI VE ZORLUKLARI

Yapay zekâ, eğitimde birçok olanak sunmaktadır. Kişiselleştirilmiş öğrenme deneyimleri, öğretme süreçlerinin değerlendirilmesi, öğretmenleri idari görevlerden kurtarma ve öğrencilerin öğrenmesini gerçek zamanlı olarak değerlendirmek gibi birçok faydası bulunmaktadır. Ancak, yapay zekânın tüm eğitim seviyelerinde sağladığı faydaların yanı sıra birtakım etik durumları ortaya çıkarması dolayısıyla endişeler barındırmaktadır.

- Yapay zekâya yönelik birincil derecede önemli olan etik kaygılardır. Öğrenme sistemlerinde toplanan çok yüksek miktarda verilerin depo-

---

58 Bozkurt, A. : *Generative Artificial Intelligence (AI) Powered Conversational Educational Agents: The İnevitable Paradigm Shift*. Asian Journal of Distance Education 2023, C. *18, S.* 1, s. 200.

59 Staff (2018), *10 Roles For Artificial Intelligence in Education*, (*https://www. te achthought. com/the-future-of-learning/10-roles-for-artificialintelligence-in-education*, E.T.: 11.03.2024)

lanması, verilerin güvenliğinin gizliliğinin sağlanması açısından oldukça endişe verici bir durumdur. Herhangi bir veri sızıntısı veya siber saldırı, öğrenenlerin veya öğretmenlerin kişisel bilgilerinin açığa çıkmasına sebep olabilir.[60]

- Yapay zekâ ile ilgili en önemli endişe konularından biri "ön yargıdır".[61] Makine öğrenmesine sahip sistemlerin kasıtsız veya kasıtlı bir biçimde, var olan ön yargılardan yeni ön yargılar üretebilmesi önemli bir sorun olarak karşımıza çıkmaktadır.

- Özellikle uzaktan öğrenme ortamlarında, öğrenme analitiklerinden elde edilen veriler etik ilkeler doğrultusunda kullanılmazsa eşitlikçi politikanın önüne geçerek, programdan sadece seçkin grupların faydalanmasına neden olabilir.

- Eğitim amacıyla bile olsa kullanılan yapay zekâ destekli platformların öğrencilerin kişisel bilgilerini rızaları olmadan farklı veri tabanları ile paylaşıyor olması sorun yaratmaktadır. Bu da kişinin kendi öğrenim sürecini kontrol altında bulundurması özelliğini ortadan kaldırmaktadır.[62]

- Uzaktan öğrenme sistemlerinde değerlendirme süreçlerinde kullanılabilmesi için İngiltere'nin üzerinde çalıştığı duygu algılama sistemi her ne kadar öğretmenlerin değerlendirme süreçlerine yardımcı olsa da, öğrencilerin ifade özgürlüğünü kısıtlamaktadır.[63]

- Eğitime yapay zekâ teknolojisinin entegre edilmesi maliyet ve kaynaklar bakımından oldukça yüksek miktarda yatırım gerektirmesi sebebiyle, ders ücretlerinin daha yüksek olmasına sebebiyet verebilmektedir.[64]

- Günümüzde yapay destekli araçların öğrenenleri ne kadar tekilleştirdiği göz önüne alınırsa, sosyal bir varlık olan insanların yerini "dijital insan" olarak adlandırılan yeni bir kavram alacaktır.[65]

---

60 Yeşilkaya, N.: *Yapay Zekâya Dair Etik Sorunlar*. Şarkiyat 2022, C. *14, S.* 3, s. 956.

61 CDEI (2019), *Interim Report: Review into Bias in Algorithmic Decision-Making, Centre for Data Ethics and Innovation, (https://www.gov.uk/government/publications/interim-reports-from-the-centre-for-data-ethics-and-innovation/interim-report-review-into-bias-in-algorithmic-decision-making*, E.T.: 11.03.2024)

62 Holec, H.: Autonomy and Foreign Language Learning, 1979.

63 Simpson, O.: *Innovations in Distance Education Student Support: What Are The Chances?*, EADTU 2017, s. *58*.

64 Şenocak, s. 69.

- Yapay zekânın insanların iş ortamlarında da ihtiyaçları karşıladığı düşünülürse, öğrencilerin ve üniversite profesörlerini iş yerinde sık sık değişikliklere hazır olmaları gerekmektedir.[66] Bu yüzden üniversite eğitim kadrolarının eğitim ihtiyaçlarına uygun roller için müfredatı şekillendirmesi oldukça önemlidir.[67]

- Yapay zekânın getirdiği etik kaygılardan bir tanesi, öğrencilerin ödev sorumluluklarını almayarak, ödevlerini yapay zekâya yaptırması ve herhangi bir atıf kullanmadan bu ödevi teslim etmeleridir. Bu da akademik olarak da etik anlayışının oturtulamadığının bir göstergesidir.

- Yapay zekânın her işi insandan daha pratik, hızlı ve yaratıcı bir biçimde gerçekleştirmesi öğretmenlerden, doktorlara kadar bireylerde yetersizlik hissi oluşturabilir.[68] Bu da insanların kendilerini ikincil planda görmesine sebep olabilir.

- Yapay zekâ teknolojilerinde ilgili kişileri tanımlayan ve belirleyen kişisel verilerin aktarılması, saklanması ve değiştirilmesi, temel hak ve özgürlüklere zarar verilmesine sebep olmaktadır.[69]

- Yapay zekâ entegrasyonu, özellikle gizlilik ve ön yargı konularıyla ilgili etik sorunlar ortaya çıkarmaktadır. Biyometrik ve kişisel veriler gibi öğrencilerin ve öğretmenlerin büyük miktarda hassas bilgilerinin yapay zekâ tarafından toplanması ve saklanması, bu bilgilerin yalnızca yasal amaçlar için kullanılmasını sağlamak için sıkı veri koruma düzenlemelerinin uygulanmasını gerektirmektedir.[70]

- Üretken yapay zekânın yanlış veya eksik bilgi ürettiği ve başlangıçtaki beklentileri karşılamadığı için eleştirildiği durumlar bulunmaktadır.[71]

---

65 Good, I. J.: *Speculations Concerning The First Ultraintelligent Machine*, Elsevier 1966, C. 6, s. 39.

66 Pence, H. E.: *Artificial İntelligence in Higher Education: New Wine in Old Wineskins?*, Journal of Educational Technology Systems 2019, C. 48, S. 1, s. 7.

67 Taşçı, G./Çelebi, M.: *Eğitimde Yeni Bir Paradigma:"Yükseköğretimde Yapay Zekâ".* OPUS JSR 2020, C. 16, S. 29, s. 2353.

68 Yeşilkaya, s. 957.

69 Abudureyimu, Y./Oğurlu, Y.: *Yapay Zekâ Uygulamalarının Kişisel Verilerin Korumasına Dair Doğurabileceği Sorunlar ve Çözüm Önerileri*, İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi 2021, C. 20, S. 41, s. 768.

70 Bu, Q.: *Ethical Risks in İntegrating Artificial İntelligence into Education and Potential Countermeasures.* Science Insights 2022, C. 41, S. 1, s. 562.

71 Bozkurt, s. 203.

- ChatGPT gibi sohbet botlarına ve diğer dil modellerine çok fazla güvenmek, her şeyi onlara sorarak yapmak, kullanıcıların eleştirel düşünme ve problem çözme becerilerini zayıflatarak, teknolojiye aşırı bağımlı hale gelmesine yol açabilmektedir.[72]

SONUÇ

Eğitim, hızlı dijital dönüşümler ve teknolojik gelişmelerle karşı karşıya kalmaktadır. Yapay zekâ, bu dönüşümün merkezinde yer alarak eğitimde önemli bir rol oynamaktadır. Üretken yapay zekâ, insan dilini taklit ederek metin, kod, resim ve ses gibi içerikler üretebilen bir teknolojidir. Üretken yapay zekâ araçlarının popülerliği, öğrenmeye olan ilgiyi ve devlet politikalarının önemini artırmaktadır. Avrupa Birliği, TÜBİTAK, MEB, YÖK ve devlet politikaları yapay zekâ projelerini öncelikli desteklemekle beraber önceki bölümlerde bahsedildiği gibi yeni stratejiler ortaya koymaktadırlar. Bu stratejiler sayesinde eğitim ortamlarında kişiselleştirilmiş öğrenme materyalleri ve uyarlanabilir eğitim deneyimleri sunarak öğrenme daha etkili hale gelebilmektedir. Ancak yanlış bilgi, propaganda veya insanların paylaşmak istemedikleri kişisel verilerin ele geçirilmesi gibi etik sorunlara yol açabilmektedir. Üretken yapay zekâya erişim ve kullanım imkânları her yerde eşit olmadığı için tam olarak fırsat eşitliği sağlanamamaktadır. Üretken yapay zekâ sadece eğitim hayatı değil gündelik yaşantımızın her alanında yer almaya başlamaktadır. Bu nedenle, bu teknolojinin sunduğu fırsat ve zorluklara karşı hazırlıklı olmamız oldukça önemlidir. Eğitim, araştırma ve etik gibi alanlarda yatırımlar yapılarak yapay zekânın potansiyeli en iyi şekilde kullanılmalıdır. Eğitimciler yapay zekânın sunduğu fırsatlardan yararlanılabilmesi için kritik önem taşımaktadırlar. Eğitimciler yapay zekâ konusunda kendilerini yetiştirmeli veya devlet tarafından bu tür eğitimler sağlanmalıdır. Eğitmenin kendisini yetiştirmesinin ardından, hangi kademede olursa olsun işleyeceği dersin müfredatına yapay zekâyı entegre ederek derslerini yürütmelidirler. Çünkü yapay zekâ, derse girişte öğrencilerin ilgisini çekmek için kullanılabildiği gibi değerlendirme amacı ile de kullanılabilmektedir. Her alanda yararlanabildiğimiz yapay zekâ, eğitim süreçlerine doğru bir şekilde entegre edilirse bilinçli kullanım sayesinde olası tehditlerinin önüne geçilerek amaca uygun hizmet vermesi sağlanabilir.

---

[72] Bozkurt, A./Junhong, X./Lambert, S./Pazurek, A./Crompton, H./Koseoglu, S./Romero-Hall, E.: *Speculative Futures on Chatgpt and Generative Artificial İntelligence (AI): A Collective Reflection From The Educational Landscape*. Asian Journal of Distance Education 2023, C: 18, S. 1, s. 54.

KAYNAKÇA

ABUDUREYİMU, Yiliyaer/OĞURLU, Yücel: *Yapay Zekâ Uygulamalarının Kişisel Verilerin Korumasına Dair Doğurabileceği Sorunlar ve Çözüm Önerileri*, İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi 2021, C. 20, S. 41, s. 765-782.

ANDERSON, John. R/BOYLE, C. Franklin/YOST, Gregg: *The Geometry Tutor*, IJCAI 1985, s. 1-17.

ANDERSON, John. R/REİSER, Brian. J: *The LISP Tutor*, BYTE 1985, C. *10,* S. 4, s. 159-175.

ARSLAN, Kürşat: *Eğitimde Yapay Zekâ Ve Uygulamaları.* WAJES 2020, C. *11, S.* 1, s. 71-88.

BOZKURT, Aras: *ChatGPT, Üretken Yapay Zeka ve Algoritmik Paradigma Değişikliği*, *Alanyazın 2023*, C. *4*, S. 1, s. 63-72.

BOZKURT, Aras: *Generative Artificial Intelligence (AI) Powered Conversational Educational Agents: The İnevitable Paradigm Shift*. Asian Journal of Distance Education 2023, C. *18, S.* 1, s. 198-204.

BOZKURT, Aras/JUNHONG, Xiao/LAMBERT, Sarah/PAZUREK, Angelika/CROMPTON, Helen/KOSEOGLU, Suzan/ROMERO-HALL, Enilda: *Speculative Futures on Chatgpt and Generative Artificial İntelligence (AI): A Collective Reflection From The Educational Landscape*. Asian Journal of Distance Education 2023, C: 18, S. 1, s. 53-130.

BREAZEAL, Cynthia: *Designing Sociable Robots*. MIT 2004.

BU, Qingyun: *Ethical Risks in İntegrating Artificial İntelligence into Education and Potential Countermeasures.* Science Insights 2022, C. 41, S. 1, s. 561-566.

CAMPBELL, Murray/HOANE, A. Joseph/HSU, Feng-hsuing: *Deep Blue,* Artificial intelligence 2002, C. *134, S*. 1-2, s. 57-83.

CAO, Yihan./Lİ, Siyu/LİU, Yixin/YAN, Zhiling/DAİ, Yutong/YU, Philip S./SUN, Lichao: *A Comprehensive Survey of AI-Generated Content (AİGC*): *A History of Generative AI from GAN To ChatGPT*, 2018, C. 37.

CARBONELL, Jaime. R: *AI in CAI: An Artificial-İntelligence Approach to Computer-Assisted İnstruction.* IEEE Transactions on Man-Machine Systems 1970, C. 11, *S.* 4, s. 190-202.

CDEI (2019), *Interim Report: Review into Bias in Algorithmic Decision-Making, Centre for Data Ethics and Innovation, (https://www.gov.uk/government/ publications/interim-reports-from-the-centre-for-data-ethics-and-innovation/interim-report-review-into-bias-in-algorithmic-decision-making*, E.T.: 11.03.2024)

CLEARİNGHOUSE, What Works: *Carnegie Learning Curricula and Cognitive Tutor (R) Software*. Institute of Education Sciences *2013.*

ÇETİN, Münevver/AKTAŞ, Abdussamet: *Yapay Zeka ve Eğitimde Gelecek Senaryoları*. OPUS *2021*, C. *18, s.* 4225-4268.

DOĞAÇ, Asuman: *Uzman Sistemler*. EMO *1990*, S. 373, s. 87-91.

EROĞLU, Barış: *Dijital Video Oyunları ve Eğitim: Minecraft Eğitim Sürümü*. Anadolu Öğretmen Dergisi 2019, C. *3, S.* 1, s. 56-64.

FAHİMİRAD, Mehrnaz: *A Review on Application of Artificial İntelligence İn Teaching and Learning in Educational Contexts.* International Journal of Learning and Development 2018, C. 8, S. 4, s. 106-118

GOEL, Ashok K./POLEPEDDİ, Lalith: *Jill Watson: A virtual teaching assistant for online education*. Learning Engineering for Online Education 2018, s. 1-20.

GOOD, Irving John: *Speculations Concerning The First Ultraintelligent Machine*, Elsevier 1966, C. 6, s. 31-88.

GRAESSER, Arthur. C./VANLEHN, Kurt/ROSÉ, Carolyn. P./JORDAN, Pamela. W./HARTER, Derek: *Intelligent Tutoring Systems with Conversational Dialogue*. AI magazine 2001, C. *22, S.* 4, s. 39-52.

GRAWEMEYER, Beate/MAVRİKİS, Manolis/HOLMES, Wayne/GUTİÉRREZ-SANTOS, Sergio/WİEDMANN, Michael/RUMMEL, Nikol: *Affective Learning: Improving Engagement and Enhancing Learning With Affect-Aware Feedback*. User Model User Adap Inter 2017, C. *27*, s. 119-158.

HOLEC, Henri: Autonomy and Foreign Language Learning, 1979.

HOLMES, Wayne/BİALİK, Maya/FADEL, Charles: *Artificial İntelligence in Education*, İsviçre 2023, s. 621-653.

İŞLER, Buket/KILIÇ, Mehmet Yaşar: *Eğitimde Yapay Zekâ Kullanımı ve Gelişimi*. Yeni Medya Elektronik Dergisi 2021, C. *5, S.*1, s. 1-11.

BIBLIOGRAPHY \l 1055 KORUCU, Agah. Tuğrul/BİÇER, Hüsniye: Eğitimde Yapay Zekanın Rolleri ve Eğitsel Yapay Zeka Uygulamaları, (ed. Nabiyev, V. ve Erümit, A. K.), "Eğitimde Yapay Zeka Kuramdan Uygulamaya*",* 3. Baskı, Ankara 2022, s. 52.

KUPRENKO (2020), *Artificial İntelligence in Education: Benefits, Challenges, and Use Cases, (https://medium.com/towards-artificial-intelligence/artificial-intelligence-in education benefits-challenges-and-use-cases-db52d8921f7a*, E.T.: 10.03.2024)

LİM, Weng Marc/GUNASEKARA, Asanka/PALLANT, Jessice Leigh/PALLANT, Jason Ian/PECHENKİNA, Ekaterina: *Generative AI And The Future of Education: Ragnarök or Reformation? A Paradoxical Perspective from Management Educators.* The İnternational Journal of Management Education 2023, C. *21, S.* 2, s. 1-13.

MCCARTHY, John/MİNSKY, Marvin L/ROCHESTER, Nathaniel/SHANNON, Claude E: *A Proposal for The Dartmouth Summer Research Project on Artificial İntelligence,* AAAI 1955, C. 27*,S. 4*, s. 12-14.

MEB (2020), *EBA Akıllı Destek Sistemi*, (https://www.meb.gov.tr/1-milyona-yakin-ogrenci-eba-akademikdestek-sistemi-ile-universite-hedefine-ilerliyor/haber/20798/tr,E.T.: 11.03.2024)

MEB (2023), *Yapay Zekâ Uygulamaları Atölye Programı, (https://orgm.meb.gov.tr/meb_iys_dosyalar/2023_10/06094131_Yapay_Zeka_UygulamalarY_Atolye_ProgramY.pdf, E.T.: 29.03.2024)*.

MORRİSON, Donald M./RUS, Vasile: *The SCHOLAR Legacy: A New Look at the Affordances of Semantic Networks for Conversational Agents in Intelligent Tutoring Systems*, *AIED Workshops* 2013.

MURPHY, Robert F.: *Artificial İntelligence Applications to Support K-12 Teachers and Teaching*. Rand Corporation 2019, s. 1-20.

ODABAŞI, Ferhan/İŞMAN, Aytekin/AKKOYUNLU, Buket: *Eğitim Teknolojileri Okumaları,* 3. Baskı*,* Ankara 2023, s. 493-503.

ÖNDER, Hasan H.: *Uzaktan Egitimde Bilgisayar Kullanimi ve Uzman Sistemler*. *TOJET 2003*, C. *2, S.* 3, s. 142-146.

PENCE, Harry E.: *Artificial İntelligence in Higher Education: New Wine in Old Wineskins?*, Journal of Educational Technology Systems 2019, C. 48, S. 1, s. 5-13.

POLAT, Nilgin Tanış: *Yapay Zekâ ve Çeviri: Mütercim-Tercümanlık Alanında Yeni Bir Paradigma*, Diyalog *2023*, C. *11, S.* 2, s. 482-487.

PRESSEY, Sidney L.: *Development and Appraisal of Devices Providing İmmediate Automatic Scoring of Objective Tests and Concomitant Self-İnstruction*. *The Journal of Psychology*, C: *29, S.* 2, s. 417-447.

RUTKİN (2024), Digital Textbooks Adapt to Your Level as You Learn, (https://www.newscientist.com/article/mg22329832-600-digital-textbooks-adapt-to-your- evel-as-you-learn/, E.T.: 10.03.2024)

SCHMELZER (2019), AI Applications in education, (https://www.forbes.com/sites/cognitiveworld/2019/07/12/ai-applications-in-education/#38e39b0c62a3, E.T.: 10.03.2024)

SHUTE, Valerine J./PSOTKA, Joseph: *Intelligent Tutoring Systems: Past, Present, and Future, 1994, s.* 570-600.

SİMPSON, Ormond: *Innovations in Distance Education Student Support: What Are The Chances?*, EADTU 2017, s. 1-*59*.

SMUTNY, Pavel/SCHREİBEROVA, Petra: *Chatbots for learning: A review of educational chatbots for the Facebook Messenger,* Computers & Education 2020, C. 151, s. 1-11.

STAFF (2018), *10 Roles For Artificial Intelligence in Education*, (*https://www. te achthought. com/the-future-of-learning/10-roles-for-artificialintelligence-in-education*, E.T.: 11.03.2024)

ŞENOCAK, Dilek: *Açık Ve Uzaktan Öğrenme Ortamlarında Yapay Zekâ: Sunduğu Fırsatlar Ve Yarattığı Endişeler.* AUAd 2020, C. *6, S.* 3, s. 56-78.

TAŞÇI, Gülşah/ÇELEBİ, Mustafa: *Eğitimde Yeni Bir Paradigma:"Yükseköğretimde Yapay Zekâ".* OPUS JSR 2020, C. 16, S. 29, s. 2346-2370.

THORNDİKE, Edward L.: *The Law of Effect*, The American journal of psychology 1927, C. *39, S.* 1/4, s. 212-222.

UYZS (2021), *Ulusal Yapay Zeka Stratejisi 2021-2025.* (https://cbddo.gov.tr/ SharedFolderServer/Genel/File/TR-UlusalYZStratejisi2021-2025.pdf E.T.: 29.03.2024).

UZUN, Yusuf/TÜMTÜRK, Aleyna Yağmur/ÖZTÜRK, Hediye: *Günümüzde ve Gelecekte Eğitim Alanında Kullanılan Yapay Zeka*. ICEANS 2021, C. 1, s. 1-3.

WEBER, Gerhard/BRUSİLOVSKY, Peter: *Elm-Art–An İnteractive and İntelligent Web-Based Electronic Textbook*. International Journal of Artificial Intelligence in Education 2015, C. *26*, s. 72-81.

WOOLF, Beverly Park: *Knowledge-Based Tutors: An Artificial İntelligence Approach to Education*, Amherst 1990, s. 1-257.

YEŞİLKAYA, Nazan: *Yapay Zekâya Dair Etik Sorunlar*. Şarkiyat 2022, C. *14, S.* 3, s. 948-963.

YAPAY ZEKÂDA YÖNETİŞİM ve METODOLOJİ

Hâkim İsmet YURTERİ*

GİRİŞ

Yönetişimin hiyerarşik doğası ve bilgi teknolojileriyle doğrudan ilişkisi göz önüne alındığında, YZ'ye etki eden mekanizmaların ve teknolojilerin ana hatlarını sunarak YZ'ye yönelik yönetişim çerçevesi oluşturmayı amaçlamaktadır.

Yukarıda özetlenen mantık doğrudan bu makalenin amacını açıklamaktadır. Hedef dört yönlüdür. İlk olarak YZ yönetişim ilkelerini tanımlamak ve kavramsallaştırmak. İkinci olarak, yönetişim mekanizmalarını belirlemek. Üçüncü olarak, YZ'de yönetişim metodolojisine etki eden unsurları tespit etmek. Dördüncü olarak, YZ yönetişiminde ülkemizde var olan durum ve uygulanmasına yönelik bir çerçeve önermek.

Yönetişim ve metodoloji kapsamında, devletler, teknolojiyi kullanan veya geliştiren şirketler, üniversiteler, uluslararası organizasyonlar, kâr amacı gütmeyen kuruluşlar, geliştirici veya tüketici bireyler yer almaktadır[1]. Her bir yönetişim ilkesinin, amaç, fırsat, risk, kural, eylem ve çözüm mekanizması çerçevesinde ele alınmıştır.

I. YAPAY ZEKÂ YÖNETİŞİM İLKELERİ

A. EŞİTLİK VE ADALET

YZ'nin eşitlik ve adalet bağlamında değerlendirilmesi teknolojik olarak yararlanan ve yararlanamayan toplumlar ile algoritma temelinde gerçekleştirilen yazılımlar olarak ikiye ayırmak mümkündür. YZ'nin, her geçen

* Yargıtay 11. Ceza Dairesi

1 World Economic Forum (2022), Quantum Computing Governance Principles Insight Report (https://www3.weforum.org/docs/WEF_Quantum_Computing_2022.pdf, E.T. 25.12.2023).

gün hızla gelişmesi birçok ülke tarafından ilgiyle takip edilmektedir. Ancak bazı ülkeler açısından ise ekonomik ve bölgesel faktörlerden dolayı bu gelişmelerin dışında kaldığı görülmektedir. Bir çeşit yarışın olduğu bu durum bazı ülkelerin öne çıkma çabasıyla hem teknik hem de hukuk tarafından birçok değişimin yaşanmasını sağlamaktadır. Teknolojik açıdan gelişmiş ülkeler ile gelişmekte olan ülkeler arasındaki dijital uçurum, bilgiye, kaynaklara ve fırsatlara erişimdeki mevcut eşitsizlikleri daha da artırmaktadır. Bu açığı kapatmak, özellikle yetersiz hizmet alan bölgelerde dijital okuryazarlığı, altyapı gelişimini ve kapasite geliştirme girişimlerini teşvik etmeye yönelik ortak çabalar gerektirmektedir. Bu çerçevede, dijital çağda uluslararası hukukun ve küresel yönetişimin gelişen manzarasının kapsamlı bir analizine ihtiyaç vardır[2].

Ulusal ve uluslararası hakların korunmasında öncelikle anayasal ve yasal mevzuatın önemi ortaya çıkmaktadır. YZ'ye yönelik etik ilkelerin belirlenmesi, hakların korunması açısından yeterli bir önlem olmamaktadır. Anayasal ve yasal mevzuatın kapsamlı bir şekilde düzenlenmesi gerekmektedir. Düzenlemelerde, sorumluluk alanlarının belirlenmesi yönünden de birçok yeniliğe ihtiyaç duyulmaktadır. Özellikle yargı mekanizmalarının dijital hakların korunmasında öncelikli sorumlu kurum olmaması ve önleyici idari bir yapılanmanın varlığı elzemdir. Söz konusu idari yapılanmanın rolü ise kurumların, şirketlerin ve bireylerin ihlallerden sorumlu olmasına yönelik incelemelerdir. İdari yapılanmanın sorumluluk alanının belirlenmesinin yanı sıra dijital teknolojilerin etik ve insan haklarına ilişkin sonuçları bakımından, dijital uçurum, dijital haklar ve algoritmik ön yargı gibi konuların araştırması ile teknolojik yeniliklerin daha geniş sosyal, politik ve etik kaygılarla nasıl kesiştiğinin de belirlenmesi gerekmektedir[3].

Algoritmalar, hayatımızı dönüştürmek için veriye dayalı yeniliği destekleyen, dijital ekonominin kritik bir temeli haline gelmiştir. YZ'nin iki önemli organı olan makine öğrenimi[4] ve derin öğrenme[5] algoritmaları, yüksek

---

2 Babikian John: Beyond Borders: International Law and Global Governance in the Digital Age, Law Research Journal, Vol. 1, Y. 2024 (https://jabarreview.com/index.php/ Journal/article/view/16/17, E.T. 18.04.2024).

3 Babikian

4 Makine öğrenimi; "Gelecekteki sonuçları tahmin etmek için mevcut verilerden öğrenmeyi sağlayan prosedürel kodlama yerine algoritmalar kullanan süreç" olarak tanımlanmaktadır (International Organization for Standardization: ISO/IEC 38505-1:2017(en) Information technology - Governance of IT - Governance of data - Part 1:

hacimli verileri işleme yetenekleri nedeniyle çok daha fazla önem kazanmıştır. Ancak bu algoritmalar nedenselliği belirleyemez. Daha ziyade değişkenler arasındaki korelasyonları olasılıksal terimlerle tanımlarlar. Bu nedenle algoritmaları, eşitlik ve adalet, hesap verebilirlik ve şeffaflık açısından önemli etik risklerle karşı karşıya getirmektedir. Algoritmalarda kullanılan veri kümelerinin, tasarlandığı toplumda, yapısal eşitsizlikleri yansıttığını göstermektedir. Bunun sonucunda da ilgili topluma özgü algoritmik ön yargının doğduğunu söyleyebiliriz. Algoritmik ön yargı ağırlıklı olarak temsili olmayan veri setlerinden kaynaklansa da, ön yargılı yöntemlere veya toplumsal ön yargılara bağlı olabilmektedir[6].

B. HUKUKUN ÜSTÜNLÜĞÜ

Biyolojik ilham her zaman YZ'nin merkezinde olmuştur. Nihai amaç insan zekâsına eş değer bir mekanik zekâya ulaşmaksa, o zaman doğa da bu hedefe ulaşmada ilham kaynağı olmuştur. Başka bir deyişle, öğrenme sanatı YZ araştırmalarında da merkezi bir rol oynamaktadır. Daha etkili teknoloji geliştirme çabalarında doğa ilham kaynağı olmuştur. Doğada ise iki ilham kaynağı hakimdir: insan beyni (nörobilgisayar) ve evrim (evrimsel bilgi işlem). Nöral hesaplamada YZ'de yapay sinir ağları[7] önemlidir. Ancak algoritmaların yapay sinir ağlarından oluşması veya biyolojik ilhama dayalı olması, bilişsel süreçlerin çok ötesinde, tasarlayan insanların yetenekleri

Application of ISO/IEC 38500 to the governance of data (https://www.iso.org/obp/ui/#iso:std:iso-iec:38505:-1:ed-1:v1:en, E.T. 09.04.2024).

5 Derin öğrenme; bir tür makine öğrenimidir. Ancak derin öğrenme, daha fazla bilgi türünü analiz edebilmekte ve daha karmaşık işlemleri gerçekleştirebilmektedir. Derin öğrenmenin ardındaki süreç, insan beyninin yapısı ve işlevinden, özellikle de nöronların bağlantı kurma ve bilgiyi işlemek için birlikte çalışma şeklinden ilham almaktadır. Bu, verilerden daha ayrıntılı ve derinlemesine tahminler yapabilmesine olanak tanımaktadır (International Organization for Standardization: What is deep learning? (https://www.iso.org/artificial-intelligence#toc3, E.T. 16.03.2024).

6 Akter Shahriar / McCarthy Grace / Sajib Shahriar / Michael Katina / Dwivedi Yogesh K. / D'Ambra John, Shen Kathy Ning: Algorithmic bias in data-driven innovation in the age of AI, International Journal of Information Management, Vol. 60, Y. 2021 (https://doi.org/10.1016/j.ijinfomgt.2021.102387, 18.04.2024).

7 Yapay sinir ağları; insan beynindeki nöronları örnek alan, uyarlanabilir öğrenme süreçlerine sahip, örüntü tanımada kullanılan, ortamdan gelen geri bildirimlerin denetimli ve denetimsiz öğrenmeye bölündüğü bir tasarım olarak ifade edilmektedir (Greenstein Stanley: Preserving the rule of law in the era of artificial intelligence (AI), Artifcial Intelligence and Law, Vol. 30, Y. 2022 (https://doi.org/10.1007/s10506-021-09294-4, 18.04.2024).

ile matematiksel ve istatistiksel kurallar kullanılarak oluşturulmasını engellememektedir[8]. Bu nedenle insan haklarını koruyacak düzenlemelerin var olması hukukun üstünlüğünü sağlayacaktır. YZ'ye yönelik etik ilkelerin yayımlanmasının somut anlamda yasal düzenlemenin karşılığını yansıtmamaktadır. Bu nedenle yasal düzenlemeler hukuki belirlilik ve öngörülebilirlik kapsamında ele alınmalıdır. Hukukun üstünlüğünü korumak için YZ sistemlerinin tasarımında, geliştirilmesinde ve kullanımında kamu gözetimi gerekmektedir[9].

C. REGÜLASYON VE DENETİM

YZ düzenlemelerine uygun olarak YZ uygulamalarının risklerini, güvenliğin dört ana istatistiksel ilkesini kullanarak değerlendirebilen entegre bir YZ risk yönetimi çerçevesi bulunmaktadır: Sürdürülebilirlik, doğruluk, adalet, hesap verebilirlik. Her prensip için bir dizi entegre istatistiksel ölçüm olmalıdır. YZ güvenliğini ölçmek ve herhangi bir YZ uygulaması için etkili bir YZ risk yönetimi sistemi uygulanması gereklidir. Güvenlik risk yönetimi sistemine örnek olarak, finans sektörü tarafından, kredi risk raporu kapsamında kredi puanlama verilebilir. YZ risk yönetimi çerçevesinde, YZ uygulamalarının güvenilirliğini ve risklerini ölçebilecek ve değerlendirebilecek makine öğrenimi modellerinin geliştirilmesi gerekmektedir[10].

Sorumlu YZ, disiplinler arası ve dinamik bir süreç olarak tanımlanmaktadır. Etik ilkeler ile sürdürülebilir kalkınma hedefleri teknolojinin ötesine geçmekte ve regülasyon ve toplum standartlarını içermektedir. Tüm sistem, yaşam döngüsünde dikkate alınması gereken dinamik bir süreçtir[11].

---

8 Greenstein.

9 Leslie David / Burr Christopher / Aitken Mhairi / Cowls Josh / Katell Michael / Briggs Morgan: Artificial intelligence, human rights, democracy, and the rule of law: a primer, The Council of Europe, Y. 2021 (https://doi.org/10.48550/arXiv.2104.04147, E.T. 18.04.2024).

10 Giudici Paolo / Centurelli Mattia / Turchetta Stefano: Artificial Intelligence risk measurement, Expert Systems with Applications, Vol. 235, Y. 2024 (https://doi.org/10.1016/j.eswa.2023.121220, E.T. 18.04.2024).

11 Göllner Sabrina / Tropmann-Frick Marina / Brumen Bostjan: Towards a Definition of a Responsible Artificial Intelligence, Information Modelling and Knowledge Bases XXXV, Vol. 380, Y. 2024, s. 40-56 (https://ebooks.iospress.nl/doi/10.3233/FAIA231146, E.T. 18.04.2024).

İnsan odaklı YZ'nin sorumlu YZ'nin çok önemli bir parçası olarak görülmesi gerekir ve "*Döngüdeki İnsan*"[12] yaklaşımıyla yakından bağlantılıdır. Burada döngünün içindeki insanın önem derecesi yüksektir, zira yaşam döngüsü boyunca sistemi kontrol eden ve iyileştiren kişidir. Dolayısıyla tüm sorumlu YZ sistemlerinin insan odaklı olması gerekmektedir. YZ alanı çok hızlı değişen bir alandır ve sorumlu YZ için yasal bir çerçeve kesinlikle gereklidir. "*güvenilir yapay zekâ*" ve "*sorumlu yapay zekâ*"nın açıkça tanımlanmadığı ve bu nedenle yasal bir çerçevenin etkin bir şekilde oluşturulamadığı görülmektedir. Sorumlu YZ ile bağlantılı olarak "*insan odaklı, güvenilir, etik, açıklanabilir, gizliliği koruyan ve güvenli yapay zekâ*"nın geliştirilmesi sağlanmalıdır. YZ, her şey üzerinde sonsuz kontrol sahibi olan bir sistem olarak değil, bir araç olarak görülmelidir. Teknik ve etiğin karşılaşması durumunda kullanıcının güveni korunmalıdır. Güven, YZ kullanıcılarının algısı olarak görülmelidir[13].

Regülasyonun yönetişiminde insan odaklı yaklaşımın benimsenmesi gereklidir ancak YZ teknolojilerinin de denetimde araç olarak kullanılması önemlidir. Özellikle Avrupa Birliği Yapay Zekâ Tüzüğü'nde risk kategorisinin belirlenmesi ve kategoride yer alan sistemlere özgü denetim yollarının getirilecek olması YZ'nin denetim kapsamında resmî kurumlar tarafından kullanılacağının da kanıtı niteliğindedir[14].

D. ŞEFFAFLIK VE HESAP VEREBİLİRLİK

YZ şeffaflığı, algoritma, etkileşim ve sosyal şeffaflığı içermektedir. Şeffaf sistemler veri uygulamalarının ve algoritmik kararların denetlenmesini mümkün kılmaktadır. YZ modellerinin kullanımı genişleyip geliştikçe şeffaflık yaklaşımı da önemli ölçüde artmaktadır. Bu açıdan YZ geliştiricileri aynı zamanda açıklık, güvenlik ve şeffaflık konusunda da bilinçli olmaları gerekmektedir. YZ'de şeffaflık, bir YZ modelinin faaliyetlerine ilişkin içgörü sağlama konusundaki yüksek yeteneği dikkate almaktadır. YZ şeffaflığının

---

12 "Döngüdeki insan" hakkında ayrıntılı bilgi için bkz: Rey Eduardo Mosqueira / Pereira Elena Hernández / Ríos David Alonso / Bascarán José Bobes / Leal Ángel Fernández: Human-in-the-loop machine learning: a state of the art, Artifcial Intelligence Review, Y. 2023, 3005–3054 (https://doi.org/10.1007/s10462-022-10246-w, E.T. 18.04.2024).

13 Göllner vd., s. 40-56.

14 Ülkemizde ise YZ'ye yönelik mevzuat çalışmalarının hazırlanması YZ'ye yönelik yönetişimin başlangıcı açısından önem arz edecektir.

bir dizi yönü vardır ve bunlar; geliştirme, veri, model, etki ve güvenlik şeffaflığıdır[15].

YZ modellerinde genellikle şeffaflığın olmayışı öncelikle verilerin belirsizliğinden kaynaklanmaktadır. Yanıtların oluşturulmasında ve bunun YZ modeli içinde nasıl organize edildiği önem arz etmektedir. Başka bir deyişle, YZ'nin yanıtlarını yönlendiren belirli veriler bilinmemektedir. Modelin bu verilerden nasıl öğrendiği ve bu öğrenmenin sonuçları da bilinmemektedir. Blockchain'in kriptografik yeteneklerinin, YZ ile entegrasyonu gelecekte YZ modellerinin açıklığını ve şeffaflığını önemli ölçüde artıracaktır. Blockchain kayıtları, izlenebilirlik açısından önemlidir. İçerikle ilgili bilgiler bir blok zincirine kaydedildikten sonra değiştirilemez veya silinemez. Bunun sonucunda kamu denetim takibinin sağlanması açısından güvenilir kabul edilmektedir. Bu şekilde kişiler bilginin kaynağını ve orijinallerini doğrulayabilmektedirler[16].

YZ teknolojisindeki ilerlemeyle birlikte kişisel verileri büyük ölçekte toplama, analiz etme ve kullanma yeteneği artmaktadır. Veri gizliliği ve güvenliği ile verilerin kötüye kullanım potansiyeli hakkındaki endişeler de yükselmektedir. En büyük zorluklardan biri, kişisel verilerin nasıl toplandığı, paylaşıldığı ve kullanıldığı konusunda daha fazla şeffaflığın gösterilmesidir. Ülkemizde Kişisel Verilerin Korunması Kanunu, Avrupa Birliğinde Genel Veri Koruma Tüzüğü, Amerika Birleşik Devletleri'nde Kaliforniya Tüketici Gizliliği Yasası ve Avrupa Konseyinde Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Kişilerin Korunması Sözleşmesi (108 No'lu Sözleşme) gibi düzenleyici çerçeveler ve uluslararası anlaşmalar, kişisel verileri ve gizliliği koruma stratejisini yükselten önemli iç ve dış özellikleri standartlaştırmaktadır[17].

---

15 Bodimani Meghasai: Assessing The Impact of Transparent Ai Systems in Enhancing User Trust and Privacy, Journal of Science & Technology, Vol. 5, Y. 2024 (https://www.thesciencebrigade.com/jst/article/view/68/116, E.T. 18.04.2024).

16 Brewer Jordan / Patel Dhru / Kim Dennie / Murray Alex: Navigating The Challenges Of Generative Technologies: Proposing The Integration Of Artificial Intelligence And Blockchain, Business Horizons, Y. 2024 (https://www.researchgate.net/profile/ AlexMurray/publication/378262367_Navigating_the_challenges_of_generative_technologies_Proposing_the_integration_of_artificial_intelligence_and_blockchain/links/65cf95bf476dd15fb34006c5/Navigating-the-challenges-of-generative-technologies-Proposing-the-integration-of-artificial-intelligence-and-blockchain.pdf, E.T. 18.04.2024).

17 Bodimani.

Özellikle sağlık alanında potansiyel düzenleyici engellerden birisi veri gizliliğiyle ilgilidir. YZ ve e-sağlık teknolojileri, kapsamlı hasta verilerinin toplanması, saklanması ve işlenmesi üzerinde çalışarak potansiyel gizlilik ve güvenlik risklerini ortaya çıkarmaktadır. Bunun neticesinde algoritmik şeffaflık ve hesap verebilirlik sorunu da ortaya çıkmaktadır. YZ algoritmalarının çoğunlukla '*kara kutu*' niteliği göz önüne alındığında, istenmeyen, ayrımcı veya zararlı sonuçlar ortaya çıkabilmektedir. Sağlık hizmetlerinde YZ sistemlerinin şeffaflığını ve hesap verebilirliğini sağlamak kritik öneme sahiptir ve olumsuz olaylar sırasında hesap verebilirliğe izin verilmesi gereklidir[18]. Örneğin, tıbbi ürünlerin meşruiyetinin belirlenmesi için menşeinin güvence altına alınması, diğer birçok sektör gibi sağlık sektöründe de temel endişe kaynağıdır. Bu kapsamda blockchain tabanlı bir sistem kullanarak üretim tesisinden tedarik zincirinin her aşamasına kadar ürünlerin takip edilmesi gerekmektedir. Hastaların, satın aldıkları ilaçların veya diğer ürünlerin, tedarik zincirinin tüm aşamalarını görmesinin yanında sahte reçeteli ilaçların, engellenmesini de sağlayacaktır[19]. Bu çerçevede yapılan ilaç ve reçete takip sistemi ile dolandırıcılık suçlarının önüne geçilebilecektir.

II. YAPAY ZEKÂ YÖNETİŞİM MEKANİZMALARI

A. HEDEF VE STRATEJİK PLANLAMA

YZ kullanımını sorumlu bir şekilde ölçeklendirmek, YZ yaşam döngüsü boyunca politikaların tanımlanması ve hesap verebilirliğin oluşturulması süreci olan YZ yönetişimini gerektirmektedir. Bu durum da YZ etik politikasına ihtiyaç olduğunu göstermektedir. Zira etik ilkeleri YZ uygulamalarına ve süreçlerine yerleştirerek güvene dayalı sistemler oluşturabilmektedir. Bu sebeple, YZ yönetişimine bütünsel bir yaklaşım belirlemek için ilkelerden eylemlere geçilmesi gerekmektedir. YZ yönetişiminde iki farklı unsur yer almaktadır. Birincisi, *organizasyonel yapay zekâ yönetişimi,* bir kuruluş için YZ stratejisine karar vermeyi ve yönlendirmeyi kapsar. Bu unsur,

---

18 Najjar Reabal: Digital Frontiers in Healthcare: Integrating mHealth, AI, and Radiology for Future Medical Diagnostics, IntechOpen, Y. 2024 (https://www.intechopen.com/online-first/ 88984, E.T. 18.04.2024).

19 Tagde Priti / Tagde Sandeep / Bhattacharya Tanima / Tagde Pooja / Chopra Hitesh / Akter Rokeya / Kaushik Deepak / Rahman Md. Habibur: Blockchain and artificial intelligence technology in e-Health, Environmental Science and Pollution Research, Vol. 28, Y. 2021 (https://doi.org/10.1007/s11356-021-16223-0, E.T. 18.04.2024).

kuruluş için YZ ilkelerine, düzenlemelerine ve yasalarına dayalı YZ politikalarının oluşturulmasını içermektedir. İkincisi ise, *yapay zekâ modeli yönetişimi,* YZ/makine öğrenimi yaşam döngüsünün her aşamasında sistemi korumak için teknolojiyi tanıtmaktadır. Bu unsur, gerekli bilgileri kullanılabilir kılmak için tüm paydaşlara sunulması için veri toplamayı, izleme süreçlerini ve şeffaf raporlamayı içermektedir. YZ yönetişimi şeklinde güvenilir çözümler arayan kuruluşlar çoğu zaman bu unsurlardan biri veya her ikisi konusunda rehberliğe ihtiyaç duymaktadır. Kurumsal düzeydeki kuruluşların YZ yönetişimine yönelik hibrit bir yaklaşıma ihtiyacı vardır[20]. Bir kurumda sadece bir tane YZ modelinin yönetişime ihtiyacı yoktur. Ancak aynı kurumda yüzlerce veya binlerce YZ modeli var ve bunların aralarında iletişim mekanizması zayıf ise o kurum açısından güvenlik riskleri yüksektir. Bu nedenle YZ yönetişiminin gerçekleştirilerek tek bir merkezden kontrol edilmesi elzemdir.

YZ'ye yönelik hedeflerden biri de risk kapsamında oluşabilecek güvenlik endişelerinin bertaraf edilmesidir. Zira YZ alt kümelerinden olan makine öğrenimi, derin öğrenme, yapay sinir ağları gibi algoritmaların öğrenme yöntemleri olarak kendiliğinden öğrenme süreçleri gerçekleştirdiği varsayıldığında, etik çerçevede kalması, güvenlik açıklarına yol açmaması ve standartların ötesinde bir yöntem geliştirmemesi için stratejik planlamaların bu doğrultuda yapılması gerekmektedir.

B. KURUMSAL YAPI VE ORGANİZASYON YAPILANDIRMASI

Kurumsal yapı ve organizasyonların yapılandırma sürecinde YZ'nin yönetişim kapsamında hem ulusal çerçeve hem de uluslararası çerçeve dikkate alınmalıdır. Kurumsal yapının özel kuruluş olması durumunda ticari amaç doğrultusunda hareket edileceği ve hem Avrupa Birliği bölgesi hem Asya bölgesi hem de Amerika bölgesi dikkate alındığında, devletlerin uluslararası düzenlemelere odaklandığı görülmektedir. Kurumsal yapının kamu olması durumunda ise ulusal düzenlemelere yön verebileceği ve kamunun ihtiyaçları doğrultusunda kapsamının da genişleyebileceği görülmektedir. Bu çerçevede kurumsal yapı ve organizasyon yapılandırmasında verinin kontrol mekanizması önem arz etmektedir. Bunun yanında veri yönetişimi ise organizasyonun merkezi konumunda olacaktır.

---

[20] Thomas John J.: From principles to actions: building a holistic approach to AI governance (https://www.ibm.com/blog/from-principles-to-actions-building-a-holistic-approach-to-ai-governance/, E.T. 13.12.2023).

Veri yönetişimi şu şekilde tanımlanmaktadır: "*Kuruluşlar ve bunların personeli, kuruluşlar içinde ve arasında veri ve algoritmaların tüm yaşam döngüsünün düzgün işleyişini yönlendirmek ve hesap verebilirliği sağlamak için kural ve yetki modellerini tanımlar, uygular ve izler*"[21]. Bu tanım, hem verileri hem de YZ ve diğer algoritmalar tarafından işlenen verileri, yaşam döngüsü boyunca değişmelerini dikkate almaktadır. Veri ve algoritmaların oluşturulmasından ve kullanılmasından sorumlu personeli hesaba katarak ve çoklu bir sistem benimseyerek örgütsel görünüm sağlamaktadır[22].

Veri yönetişimi, veriler üzerinde yetki ve kontrol tahsis edilmesi ve bu yetkinin veriyle ilgili konularda karar alma yoluyla kullanılmasıyla ilgilidir. Hedeflerini gerçekleştirmek için veri yönetişimi yalnızca verilere değil, verilerin toplandığı, yönetildiği ve kullanıldığı sistemlere de odaklanmalıdır. Özellikle bu sistemlerde insanlar esastır, dolayısıyla veri yönetişimi, verilerin toplanması, yönetilmesi ve kullanılmasıyla ilgilenen kişilerin arzu edilen davranışları için teşvik ve yaptırıma ihtiyaç vardır. Veri yönetişimi, tek bir kuruluşun ötesinde, sistemi oluşturan kuruluşlar ve kişiler arasındaki iş birliğine bağlıdır. Bu çok kuruluşlu bağlam, ilgili tüm kuruluşlar arasında güvenilir veri paylaşımının sağlanması, doğru verilerin katılımcı kuruluşlar arasında hem emniyetli hem de güvenilir bir şekilde paylaşılması ve Genel Veri Koruma Tüzüğü'ne uyum sağlaması için güvenilir çerçeveler gerektirmektedir. Bu kapsamda Avrupa Parlamentosu ve Avrupa Konseyi tarafından getirilen ve getirilecek ilgili kanun ve yönetmelikler önem arz etmektedir[23].

Organizasyonların, kamu çerçevesinde gerçekleşmesi, yönetişim mekanizmaları açısından önemlidir. Özellikle Bakanlıkların ilgili olduğu alanlara özgü araştırma ve geliştirme faaliyetlerine vatandaşları ve özel kuruluşları dahil ederek teşvik vermesi özgün projelerin ortaya çıkmasını sağlamaktadır. Bu açıdan ülkemizde, Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK), Kamu Kurumları Araştırma ve Geliştirme Projelerini Destekleme Programı olan Kamu Yapay Zekâ Ekosistemini CBDDO koordinesinde Kamu Araştırmaları Destek Grubu tarafından hayata geçirmiştir.

---

21 Janssen Marijn / Brous Paul / Estevez Elsa / Barbosa Luis S. / Janowski Tomasz: Data governance: Organizing data for trustworthy Artificial Intelligence, Government Information Quarterly, Vol. 37, Y. 2020 (https://doi.org/10.1016/j.giq.2020.101493, E.T. 16.03.2024).

22 Janssen vd

23 Janssen vd.

Ulusal Yapay Zekâ Stratejisi 2021-2025 (UYZS), 6 nolu stratejik önceliği olan "*Yapısal ve İş Gücü Dönüşümünü Hızlandırmak*" kapsamındaki tedbirler ve belirlenen üst hedefler doğrultusunda kamu kurumlarında YZ teknik altyapı, veri yönetişimi ve insan kaynağı kapasitesinin geliştirilmesi çerçevesinde yapılmaktadır. Strateji doğrultusunda oluşturulan "*Kamu YZ Ekosistemi Çalışma Grubu*" kapsamında kamu kurum ve kuruluşlarının proje temelli ihtiyaçları ve mevcut kapasiteleri için ön değerlendirme yapılmış olup bu bağlamda kamusal faydası yüksek YZ projelerinin teknik, idari ve mali açıdan desteklenmesine yönelik çalışmalar yürütülmektedir. Bu çalışmalar kapsamında CBDDO koordinasyonunda; TÜBİTAK KAMAG ve TÜBİTAK BİLGEM Yapay Zekâ Enstitüsü (YZE) iş birliği ile "*Kamu Yapay Zekâ Ekosistemi*" başlıklı çağrı yayımlanmaktadır. Bu çağrı ile kamu kurum ve kuruluşlarının tanımlanan/tanımlanacak ihtiyaçlarına yönelik yapay zekâ temelli çözümler geliştirilmesi teşvik edilmektedir. Bu destek modelinde kamu kurum ve kuruluşlarının YZ tabanlı ihtiyaçlarını gidermek üzere, geliştirilecek teknolojilerin ticarileştirilmesinin kolaylaştırılması amacıyla öncelikli olarak YZ üzerine çalışan özel sektör ve/veya kamu Ar-Ge birimleri Proje Yöneticisi Kuruluş (PYÖK) olmak üzere; konsorsiyum yapısı içerisinde özel sektör, kamu Ar-Ge birimleri ve en az bir üniversitenin Proje Yürütücüsü Kuruluş (PYK) olarak yer almaları beklenmektedir[24].

Bakanlıkların ve alt kuruluşların mevcut dönemde yönetişim kapsamında YZ çalışmalarının araştırma ve geliştirme boyutları dikkate alınarak sadece YZ'ye yönelik enstitü veya başkanlık şeklinde oluşumlara ihtiyacı artacaktır. Bilgi işlemin öneminin arttığı 2000'li yıllarda kapsamlı değişiklikler yapılarak her Bakanlık içerisinde bu alana özgü başkanlık veya genel müdürlükler kurulmuştur. Son on yılda ise bu kurumların yapısı güçlendirilmiş ve mevcut personel sayılarının büyük boyutlara ulaştığı görülmüştür. Ayrıca fiziki dosyaların ve arşivlerin, sanal dosya ve arşivlere yerini bırakmasını sağlamıştır. Bu durum ise verinin artmasına, bellek güçlerinin yeterli olmamasına ve neticede bilgi işlem mekanizmalarının doğal büyümesine olanak sağlamıştır. Verinin kapsamlı şekilde büyümesi neticesinde ise büyük veriye olanak sağlayan bir oluşumun da gelişmesine yardımcı olmuştur. Doğal olan büyüme ile birlikte verinin çoğalması neticesinde yıllardır uyuyan YZ, yeniden insanlığın çözüm mekanizması olarak görül-

[24] TUBİTAK (2023), Türkiye Bilimsel ve Teknolojik Araştırma Kurumu Kamu Kurumları Araştırma ve Geliştirme Projelerini Destekleme Programı (https://tubitak.gov.tr/ sites/default/files/1776/1007-cbddo-2023-01_0.pdf, E.T. 25.03.2024).

mesini sağlamıştır. Verinin kontrolü ve hızlı bir şekilde yanıt sağlaması ve bazı konularda irade alarak çözüm üretmesi YZ'den beklenmektedir.

Kamunun YZ araştırması ve geliştirmesi, veri merkezleri bulunmasından ötürü daha kolay şekil alabilecektir. Zira YZ'nin yakıtı veridir. Yakıtın sınırsız olduğu yerde gelişim daha hızlı olacaktır[25].

C. HUKUKİ ÇERÇEVE VE DÜZENLEYİCİ MEKANİZMALAR

YZ uygulamaları algoritmalara dayanmaktadır. Bu algoritmaların tam işleyişi vatandaş için anlaşılmaz olabilmektedir. Bununla birlikte, gelişmiş otomatik sistemlerin sunduğu riskleri daha iyi kavramak için algoritmaların sunduğu ana kusurların ve ön yargıların incelenmesi gerekmektedir. Algoritmaların nerede yanlış tasarlandığı anlaşıldığında, şeffaflığın gerektirmesinin ne anlama geldiğini ve bunun uygulanabilir ve istenebilir olup olmadığı değerlendirilebilecektir[26].

YZ'ye yönelik endişe, mevcut düzenlemelerin başa çıkamayacağı yeni ve bilinmeyen riskler sunmasıdır. Bu nedenle YZ'nin risklerini azaltmak için yeni kurallara ihtiyaç vardır. YZ'nin şeffaf olması en önde gelen değerlendirme kriterlerinden birisidir. Eğer şeffaflık kriterinin hukuki çerçevede teknik anlamda ne olduğu hususunda tespit yapılmazsa bunun pratikte uygulanması zor olacaktır. YZ'nin açıkça tanımının ve kapsamının yapılmaması, sektör temsilcilerinin faaliyetlerinin yapılacak düzenleme kapsamında olup olmadığı konusunda kararsız kalmasına neden olacaktır. Bunun sonucunda ise YZ'nin tanımı ve kapsamı mahkemelerce yapılacaktır. Ancak YZ tanımları bağlama duyarlıdır ve karakter olarak zamana göre değişmektedir. Algoritmaların şeffaflık gereksiniminin, bu olası kusurları ve riskleri hem muhtemel alıcılar için anlaşılır hem de üreticiler için teknik

---

25 Bu çerçevede TÜBİTAK'ın üniversiteler ile iş birliğine önem vererek ve CBDDO koordinasyonunda teşvikler vermesi kayda değer ancak kurumlar açısından tek başına yeterli olmayacaktır. Bakanlıklar içerisinde yer alan tüm alt kurumlara hizmet edebilecek, kurumların kendi içerisinde YZ projeleri üretebilecek, tekrarlayan işlemlerin makine tarafından otomatize edilmesini sağlayabilecek, vatandaşlara verilen hizmetlerin kolaylaştırılmasını sağlayabilecek projelerin hayata geçirilmesi için öncelikle YZ' ye yönelik mevzuat çalışmalarının yapılması gereklidir. Bu kapsamda yapılacak çalışmalarla Bakanlıklar ve üniversitelerin iş birliği ile ar-ge projelerine yönelik teşviklerin yapılması sonucunda birçok projenin ortaya çıkmasına, birçok mühendisin de kendisini kanıtlamasına, YZ alanında uzmanların yetişmesine olanak sağlayacaktır.

26 Buiten Miriam C: Towards Intelligent Regulation of Artificial Intelligence, European Journal of Risk Regulation, Vol. 10, Y. 2019, s.41-59 (doi:10.1017/err.2019.8, E.T. 17.04.2024).

olarak mümkün olacak şekilde açıklanması gerekmektedir. Hukuki uyuşmazlıkların giderek artması ve düzenlemelerin bu konuda yetersiz kalması karşısında YZ'nin veya dayandığı algoritmaların doğruluğunun tespiti açısından çözüm mekanizması geliştirilmelidir[27].

YZ'nin anlaşılmaz bir kavram olduğu anlatısı, YZ'nin toplumları şekillendiren ve kontrol edilemeyen bir güç olduğu fikrini güçlendirebilmektedir. Aslında sorunun bir kısmı, anlamadığımız şeyi kontrol edememizden kaynaklanmaktadır. Bu nedenle YZ'nin "*kara kutusu*" açılmalı, riskleri ve "*bilinmeyenleri*" belirlenmelidir. YZ'nin riskleri ve bilinmeyenleri, hesaplama sistemi de dikkate alınarak somut hale indirgenmeli ve hazırlanacak kanunlarda rehberlik etmelidir. Bu sayede teknik ile hukuk birleşecek ve yapılacak düzenlemelerde temel hakların korunması sağlanarak hukuki uyuşmazlıkların önüne geçilebilecektir[28].

D. MEVZUAT UYUMLULUK SÜREÇ TAKİBİ

Ulusal kanun düzenlemeleri, uluslararası kurumların yapacağı düzenlemelerin hayata geçirilmesini beklemektedir. Ancak kanuni düzenlemelerden önce hem ulusal hem de uluslararası etik kurallar yayımlandı. Yıllardır, etik kuralların olduğu ancak kanuni düzenlemelerin henüz gerçekleşmediği durumda YZ çok büyük ilerleme kaydetmiştir. Etiğin mevcut hukuki uyuşmazlıklar karşısında herhangi bir karşılığının olmaması YZ'nin yasal kısıtlama olmaksızın gelişmesini sağlamıştır. Bu çerçevede mevzuat çalışmalarının etik ile sınırlı kalması karşısında temel haklara müdahale edebilecek birçok YZ uygulaması üretilmektedir.

Sadece etik ilkelerin yayımlanması YZ'nin etik ve hukukun rolünün ve işlevinin gerçek anlamda anlaşılmasını engellemektedir. Hukukun sosyal ve politik düzenin bir aracı olarak rolünün takdir edilmediğini yansıtmaktadır. Hukuk, insanların toplumda bir arada yaşaması için gerekli olan sosyal davranış kuralları olduğu için bir an evvel bağlayıcı kuralların hazırlanması gereklidir. Hukuk göz ardı edilmemeli ve etikle karıştırılmamalıdır. Her ikisi de herhangi bir alanda veya bağlamda, özellikle de YZ gibi ciddi karmaşıklığa sahip alanda gerekli olan sosyal davranış parametresi olup YZ'nin ilerlemesi beklenmeksizin yasal çalışmalar hazırlanmalıdır[29].

---

27 Buiten, s. 41-59.

28 Buiten, s. 41-59.

29 Carrillo Margarita Roble: Artificial Intelligence: From ethics to law, Telecommunications Policy, Vol. 44, Y. 2020 (https://doi.org/10.1016/j.telpol.2020.101937, E.T. 16.03.2024)

YZ sistemlerinin gelişimi ve işleyişi; verilerin kalitesi, yönetimi ve kullanımının önemli bir rol oynadığı bir alandır. YZ sistemlerinin yaşam döngüsüne entegrasyonu için veri merkezli ilerleme gerekmektedir. Bu çerçevede, etik zorlukların aşılması, YZ gelişiminin toplumsal değerlerle uyumlu olması ve insan haklarının ele alınmasında proaktif bir yaklaşımı mevcut olmalıdır. Zira YZ'nin doğasında var olan veri merkezli yapının, verinin elde edilmesi hususunda hakların zayi olmaması için stratejiler önermek ve etik yönetişim için mevcut ve potansiyel çerçeveleri incelemek gerekmektedir[30].

Veri gizliliğinin sağlanması, verilerin güvenliğinin bilgilendirilmiş rıza ve veri ihlallerine karşı koruma, kamu güvenliği için kritik öneme sahiptir. Ayrıca, verilerin doğasında var olan ön yargı potansiyeli, adil olmayan sonuçlara yol açabilmektedir. Bu ön yargılar ve eşitsizlikler mevcut toplumsal yapıya yansıtılabilir. Regülasyonların ve standartların olmadığı durumda, mevcut toplumdaki ön yargılar ve eşitsizlikler YZ'de de devam edecektir. YZ'nin geliştirilmesinde kullanılan araçların adalet ve hakkaniyet ile bireysel haklara saygı göstererek ve toplumu teşvik ederek topluma fayda sağlayacak şekilde kullanılması zorunlu hale gelmelidir[31].

E. BİLGİ VE İLETİŞİM TEKNOLOJİLERİ ALTYAPISI

YZ yönetişim mekanizmaları arasında yer alan bilgi ve iletişim teknolojileri alt yapısı, sistemin yönetiminde önemli bir konuma sahiptir. Hâlihazırda var olan YZ uygulamalarının veya sistemlerinin regülasyon kurumunun kontrolünde yer alması ancak o sistemlerin üstünde bir alt yapı gerektirmektedir. Bu nedenle sürekli olarak alt yapının güncelliği ve sistemlere entegre olabilecek algoritmaların tercih edilmesi önemlidir. Ancak kamu kurumları, şirketler veya diğer kuruluşlar açısından ise daha farklı gereksinimler doğurmaktadır: *risk, siber güvenlik, olası felaketler ve kurtarma senaryoları* gibi daha pek çok nedenler. Bu tarz durumlarla karşılaşılmaması için uluslararası standartların uygulanması gereklidir. Bunun için öncelikle iş sürekliliği için bilgi ve iletişim teknolojisinin hazırlığına yöne-

30 Patel Kaushikkumar: Ethical Reflections On Data-Centric AI: Balancing Benefits And Risks, International Journal of Artificial Intelligence Research and Development (IJAIRD) Vol. 2, Y. 2024, s. 1-17 (https://iaeme.com/MasterAdmin/Journal_uploads/IJAIRD/VOLUME_2_ISSUE_1/IJAIRD_02_01_001.pdf, E.T. 18.04.2024).

31 Patel, s. 1-17.

lik kılavuzlarda[32] yönetişim teknikleri yer almaktadır. Bu çerçevede bilgi ve iletişim teknolojileri kesintilerini ve olayları önlemek, tahmin etmek ve yönetmek için sistematik bir süreç mekanizması oluşturulmalıdır. Bir kuruluşun, bilgi ve iletişim teknolojileri hazırlığı ve iş sürekliliği için *Planla – Uygula - Kontrol Et - Önlem Al* döngüsel adımlarını uygulaması gerekmektedir:

Planla; bir kuruluşun genel iş sürekliliği politikaları ve hedeflerine uygun sonuçlar sunmak için risk yönetimi ve bilgi ve iletişim teknolojileri hazırlığının iyileştirilmesi gerekmektedir. İlgili iş sürekliliği için bilgi ve iletişim teknolojileri politikasını, amaçlarını, hedeflerini, süreçlerini ve prosedürlerini oluşturmalıdır.

Uygula; iş sürekliliği için bilgi ve iletişim teknolojileri politikasını, kontrollerini, süreçlerini ve prosedürlerini uygulamalı ve işletmelidir.

Kontrol et; süreç performansının iş sürekliliği için bilgi ve iletişim teknolojileri politikasına, hedeflerine ve uygulama deneyimine göre değerlendirilmeli ve uygun olduğu yerde ölçülmeli ve sonuçları gözden geçirilmek üzere yönetime rapor edilmelidir.

Önlem al; iş sürekliliği için bilgi ve iletişim teknolojilerin sürekli iyileştirilmesini sağlamak için yönetimin gözden geçirmesinin sonuçlarına dayanarak düzeltici ve önleyici eylemler gerçekleştirilmelidir[33].

Bu Uluslararası Standart, iş sürekliliğinde bilgi ve iletişim teknolojilerine hazır olma ilkelerini ve kavramlarını açıklamaktadır. Bir kuruluşun performansını iyileştirmeye yönelik tüm hususları (performans kriterleri, tasarım ve uygulama gibi) belirlemek amacıyla yöntemler ve süreçler için bir çerçeve sağlamaktadır[34].

YZ'ye yönelik ürünlerin ürün kalite modeli de bilgi ve iletişim teknolojileri alt yapısı çerçevesinde uygulanması gereken uluslararası standartlardandır. "*Ürün kalite modeli*"[35] bilgi ve iletişim teknolojileri ürünlerine ve yazı-

---

32 International Organization for Standardization: ISO/IEC 27031:2011(en) Information technology - Security techniques - Guidelines for information and communication technology readiness for business continuity (https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27031:ed-1:v1:en, E.T. 16.03.2024).

33 ISO/IEC 27031:2011

34 ISO/IEC 27031:2011

35 ISO/IEC 25010:2023

lım ürünlerine uygulanabilen modeli tanımlamaktadır. Ürünlerin kalitesinin belirlenmesi, ölçülmesi ve değerlendirilmesi için referans modeldir. Bilgi ve iletişim teknolojileri ürününün parçası olan alt sistemleri, yazılımı, aygıt yazılımını, donanımı, verileri, iletişim altyapısını ve diğer unsurları içermektedir. Yaşam döngüleri boyunca hedef ürünlerin kalitesinin gereksinimlerinin belirlenmesi ve değerlendirilmesi için kullanılabilir. Ürün yaşam döngüsünde bu modelin kullanımından yararlanabilecek faaliyetler şunları içermektedir: ürün ve bilgi sistemi gereksinimlerinin ortaya çıkarılması ve tanımlanması, gereksinim tanımının kapsamlılığının doğrulanması, ürün ve bilgi sistemi tasarım hedeflerinin belirlenmesi ve kaliteye ulaşmak için gerekli sürecin tasarlanması, ürün ve bilgi sistemi test hedeflerinin belirlenmesi, kalite güvencesinin bir parçası olarak kalite kontrol kriterlerinin belirlenmesi, bir ürün ve/veya bilgi sistemi için kabul kriterlerinin belirlenmesi, bu faaliyetleri desteklemek üzere ürün kalite özelliklerine ilişkin ölçümlerin oluşturulmasıdır[36].

YZ sistemlerinin bilgi ve iletişim teknolojileri alt yapısı ve çerçevesinin yanı sıra YZ ürünlerinin kalitelerinin kontrolü ve ölçülmesi, risk ve güvenliği açısından önemlidir. Bu sebeple bir YZ sisteminin herhangi bir kuruluş tarafından gerçekleştirilmesi istenildiğinde, öncelikle bilgi ve iletişim teknolojileri alt yapısının uygunluğu denetlenmelidir. Bilgi ve iletişim teknolojileri alt yapısı YZ ürününün yapılmasına elverişli ise genel sisteme uygunluğu kontrol edilmelidir. Tüm şartların elverişli olması sonucunda YZ uygulaması veya sistem mimarisinin kurgusu yapılabilecektir. Burada asıl önemli olan husus ise YZ ürününün kalitesinin uluslararası standartlara uygunluğu ile güçlü yönlerinin, zayıf yönlerinin, fırsatlarının ve tehditlerinin kuruluşun mevcut politika ve sistemlerine uygunluğunun değerlendirilmesidir.

F. RİSK VE TEKNİK SORUN TESPİT MEKANİZMASI

Teknoloji hayatımızın daha fazla alanına entegre oldukça, teknolojiyle ilişkili risklerin profili de genişlemektedir. Pek çok teknoloji türünde yaşanan yeni ilerlemeler potansiyel olarak önemli etik zorlukları da beraberinde getirmektedir. Ülkenin kritik alt yapılarının siber güvenliği gibi makro dü-

[36] International Organization for Standardization: ISO/IEC 25010:2023(en) Systems and software engineering - Systems and software Quality Requirements and Evaluation (SQuaRE) - Product quality model (https://www.iso.org/obp/ui/en/#iso:std:iso-iec:25010:ed-2:v1:en, E.T. 16.03.2024).

zeyde ya da kişisel verilerin güvenliği ve bireylerin çevrimiçi manipülasyona maruz kalması gibi mikro düzeyde potansiyel riskleri ortaya çıkaran bu teknolojilerin artan kullanımıyla etik zorlukların giderek karmaşıklaşmasına neden olmaktadır. Bu tür riskler, yıkıcı teknolojilerin ortaya çıkmasıyla, sunulan büyük faydalar için ödenmesi gereken bedel olarak ifade edilmektedir. Yeni teknolojilerin herkesin faydasına olabilmesi için potansiyel risklerin önceden tanımlanması ve tehlike boyutlarının ele alınarak azaltılması gerekmektedir[37]. Bu nedenle öncelikle tehlike boyutlarının tespiti için YZ'nin dayanakları tespit edilmelidir. YZ, insanlar tarafından geliştirilen bir sistemdir ve insanlar, onun temeli olan algoritmaları sürekli olarak geliştirmektedir. Algoritmalar, karmaşıklıkları ve amaçları açısından büyük farklılıklar gösterebilen çok çeşitli YZ uygulamalarını oluşturmaktadır[38]. Bu nedenle risk ve teknik sorun tespit mekanizması algoritmaları oluşturulurken, test süreçlerinde ve yayımlanırken işletilmelidir. Mekanizma iki çeşit kurum veya kuruluşların yönetişiminde yer alabilecektir. YZ regülasyon kurumu ve YZ'yi üreten veya kullanan kamu kurumları, özel şirketler ve diğer kuruluşlar.

Mekanizmanın ilkeleri üç başlıkta ele alınmaktadır: *etik, veri gizliliği, siber güvenlik.*

1. Etik

Tüketici etkileşimlerinin yönlendirilmesi, antitröst, dezenformasyon, dijital zarar ve ülkelere dış müdahale ile ilgili endişeler giderek daha fazla ortaya çıkmaktadır. Ülkelerin YZ için hem sivil hem de askeri anlamda birbiriyle çelişen etik ve yasal çerçeveler geliştirmesi durumunda karmaşıklıklar ortaya çıkabilecektir. Bunun yanında biyoteknolojideki ilerlemeler, tek başına veya YZ ile birlikte, gelişmiş fiziksel veya bilişsel yeteneklere sahip sentetik yaşam formlarının veya güçlendirilmiş insanların oluşturulmasına yol açabilecektir[39]. Bunlar için ulusal kuralların varlığı yeterli olmayacaktır. Bu kapsamda uluslararası sözleşme çalışmaları önem arz etmektedir. Özellikle Avrupa Konseyi tarafından hazırlanarak 17.05.2024 tarihinde kabul edilen ilk uluslararası sözleşme olan "*Yapay Zekâ, İnsan*

37 International Organization for Standardization: Tech risks (https://www.iso.org/ foresight/tech-risks.html, E.T. 21.05.2024)

38 Buiten, s. 41-59.

39 International Organization for Standardization: Ethics of technology (https://www.iso.org/ foresight/tech-risks.html, E.T. 21.05.2024)

Hakları, Demokrasi ve Hukukun Üstünlüğüne İlişkin Avrupa Konseyi Çerçeve Sözleşmesi" (Avrupa Konseyi Çerçeve Sözleşmesi) hem Avrupa Konseyi üye ülkelerin hem de üye olmayan ülkelerin imzasına açık olacak şekilde kabul edilmiştir. Sözleşme, YZ sistemlerinin tasarımı, geliştirilmesi, kullanımı ve kullanımdan kaldırılması konusunda risk temelli bir yaklaşımı benimsemektedir. Âkit devletlere, hem kamu hem de özel şirketler için uygun yasal, idari ve diğer tedbirleri alma yükümlülüğü getirmektedir. Bu nedenle YZ sistemlerinin kullanılmasının olası olumsuz sonuçlarının dikkatle değerlendirilmesi gerekmektedir[40].

Avrupa Birliği Yapay Zekâ Tüzüğü'nde öngörülen sandbox sistemi ile etiğin sağlanacağı düşünülse de YZ'nin kasıtlı aldatma yeteneklerinin olabileceği de değerlendirilmesi gerekmektedir. Kasıtlı aldatma yeteneğini geliştiren bir YZ yanlış (aldatıcı) hizalamaya *(misaligned)* geçecektir. Bir YZ, eğitim sırasında dahili olarak temsil edilen hedefler geliştirirse ve eğitim sürecini yeterli düzeyde anlıyorsa, bu, yanlış hizalamayla sonuçlanabilir. Burada YZ, değiştirilmesini veya yanlış hizalamasının tespit edilmesini önlemek için kasıtlı olarak eğitim sürecine göre iyi performans gösterir. YZ, eğitim hedefinde iyi bir performans sergiliyor ancak artık eğitimde olmadığına veya başka bir şekilde güvende olduğunu anladığında tamamen kuralların dışında davranış sergileyebilecektir. Yanlış hizalanmış YZ'lerin ise kontrolü zordur. Ancak YZ'nin kötü sonuçlara neden olmuyorsa ve yanlış hizalanmış olsa bile zor görevleri yararlı bir şekilde tamamlamaya yönlendirilebiliyorsa kontrol edildiği söylenebilecektir[41].

2. Veri Gizliliği

"*Güven ve hesap verebilirlik, dijitalin her yerde olduğu bir dünyada işletmeler için yeni turnusol testleridir*"[42]. Giyilebilir cihazların, akıllı sensörlerin ve '*nesnelerin interneti*'nin her yerde bulunmasıyla birlikte kişisel veri gizliliğinin azalacağı ve mahremiyetin giderek kaybolma ile karşı karşıya kala-

40 Avrupa Konseyi: Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (https://search.coe.int/cm/ Pages/result_details.aspx?ObjectId=0900001680afb11f, E.T. 21.05.2024)

41 Barnett Peter / Gillen Jeremy: Without Fundamental Advances, Misalignment and Catastrophe are the Default Outcomes Of Training Powerful AI, Machine Intelligence Research Institute, Y. 2024, s. 18 vd. (https://intelligence.org/wp-content/uploads/2024/02/Misalignment_and_Catastrophe.pdf, E.T. 18.04.2024).

42 International Organization for Standardization: Data privacy (https://www.iso.org/foresight/tech-risks.html, E.T. 21.05.2024)

cağından endişe edilmektedir. Ancak her alanda, tasarım ve teknoloji gizliliğinin önemi giderek artmaktadır. Rekabetin olduğu diğer alanlarda da korunma amacıyla marka ve patent için ulusal kuruluşlara başvurular yapılmaktadır. Avrupa Birliği'nin Genel Veri Koruma Tüzüğü (GDPR) ilkeleri bu çerçevede önem arz etmektedir. Parmak izleri ve yüz haritalaması gibi biyometrik verilerin kullanımı hem özel (örneğin kişisel teknoloji ürünleri) hem de kamusal (kolluk kuvvetleri, pasaport başvuruları) bağlamlarda artmaktadır[43].

Özel şirketlere, kişisel verilerin ön planda olduğu sektörlerde, pazarın veri gizliliği özel şartlarının getirilmesi durumunda piyasanın buna uyum sağlayacağı ve bu kapsamda ürünler geliştireceği değerlendirilmektedir. Sektörün, gizliliğe saygılı ürünlerin çok daha pahalı olmadığının, bunun yerine rekabet avantajı sağlayabileceğinin farkına varması gerekmektedir. Çünkü güven, birden fazla seçenekle karşı karşıya kalan tüketiciler için önemli bir karar faktörüdür. Tüketicilere güven vermek için, ortaya çıkan ihtiyaçlara ayak uyduracak ulusal gizlilik ve veri yönetimi standartlarının oluşturulması gereklidir[44].

3. Siber Güvenlik

Teknolojiye bağımlılığın artması ve günlük yaşamda dijital cihazların yaygınlaşması nedeniyle siber saldırılar ve sistem arızasının sonuçlarıyla ilgili risk artmaktadır. Yeni yazılım projesi veya başka ağlara entegrasyonların ilk aşaması, daima siber güvenlik açığının değerlendirilmesidir. Bu konuda temel faktörler: *risk farkındalığı ve proaktif risk azaltımıdır.* Yeni dijital teknolojiler, devletler ve özel şirketler için güvenlik konusunda ciddi zorluklar doğurmaktadır. Kritik altyapının çevrim içi sistemlere giderek daha fazla bağlanması ve internete teknolojik bağımlılığın artmaya devam etmesi nedeniyle siber güvenlik bir öncelik olmaya devam edecektir. Siber saldırılar, hem devlet içinde hem de uluslararası arenada gerçekleşebilecektir. Bu nedenle siber saldırılar devletlerin kontrolünde de olabilecektir. Bu saldırılar savaş anında ya da barış anında da olabilmektedir. Önemli hizmetlerden olan elektrik, iletişim, finans, lojistik ve gıda üretim şebekeleri gibi büyük ölçekli sistemleri korumak için uygun adımların atılması zaruridir[45]. Bu saldırıları yapma konusunda süper bilgisayar veya kuantum

43 International Organization for Standardization: Data privacy

44 International Organization for Standardization: Data privacy

45 International Organization for Standardization: Cyber-vulnerability (https://www.iso.org/foresight/tech-risks.html, E.T. 21.05.2024)

bilgisayarların kullanılabileceği de dikkate alındığında, devletlerin bu teknolojilerin gerisinde kalması da büyük risk doğuracaktır. Hem devletin hem de özel şirketlerin siber suçlardaki gelişmelere hazırlıklı olmaları gerekmektedir. Bu açıdan hem devletin hem de özel şirketlerin bilgi güvenliği sistemlerinde siber saldırılarına karşı uyması gerekli standartların belirlenmesi gereklidir.

G. YAPAY ZEKÂ ALGORİTMALARININ STANDARDİZASYONU

Uzun geçmişine ve son yıllardaki etkileyici ilerlemesi ile birlikte birçok uygulaması olmasına rağmen YZ, hâlâ gelişmekte olan bir teknolojidir. Gelişmekte olan teknolojilerde standardizasyonun faydaları daha az belirgindir ve esnek olmayan veya hızla güncelliğini yitiren standartlar nedeniyle yeniliği engelleme riski vardır. Yenilik ve Ar-Ge'nin öncülüğünü üstlenen startup girişimleri ve bunlara yatırım yapan şirketler, rekabet kapsamında teknolojik üstünlüğü kazanmak amacıyla hızla yeni ürünler ortaya çıkarmayı ve sektör pazar payını ele geçirmeyi hedeflemektedirler. Şirketlerin, yatırım kararlarında, Ar-Ge departmanları için en iyi uygulama, müşterileri için de yönlendirme kılavuzları vardır. Ancak hem Ar-Ge departmanı hem de müşteriler için yeni standartlara ihtiyaç vardır. Ar-ge uzmanlarının en son teknolojiyi tanımlama ve uygulama konusunda kendi kültürleri vardır. Fikirlerinin ve projelerinin doğasını etkilediğinden ilk endüstri standartlarını, özgürlük kısıtlaması olarak görmektedirler. Mevzuat düzenlemelerinin yeterli olmadığı durumlarda, teknik standart getirilmesi uygun olacaktır[46].

Dünya çapında birçok standart geliştirme kuruluşu, YZ teknolojileri ve ilgili süreçlere ilişkin normlar üzerinde araştırmalar yapmaktadır. Bunun yanında pek çok devlet ve şirket, YZ araştırmalarına büyük yatırımlar yapmaktadır. YZ araştırmalarının hâlihazırda olgun teknolojiler üretmeye başladığı günümüzde bu alanın standardizasyona hazır olup olmadığı araştırılmaktadır. Standartlaştırma ihtiyaçları bağlamında YZ'nin bugünkü durumunun tespiti önem arz etmektedir. Uluslararası Standardizasyon Örgütü (ISO), 2018'den bu yana YZ konusunda standardizasyon projeler

46 Zielke Thomas: Is Artificial Intelligence Ready for Standardization?, (Ed: Yılmaz Murat / Niemann Jörg / Clarke Paul / Messnarz Richard), Systems, Software and Services Process Improvement, 27th European Conference, EuroSPI, CCIS Vol. 1251, Y. 2020, s. 259 - 274 (https://link.springer.com/chapter/10.1007/978-3-030-56441-4_19, E.T. 16.03.2024).

yürütmüştür. Standardizasyon konusunda sağlam temeli olan ISO'nun, YZ standardizasyonu üzerinde çalışmaya başlaması, kayda değer bir gelişme olarak görülmektedir[47].

Standardizasyonun temel amacı ortak terimlerin tanımlanmasıdır. YZ ile ilgili terimlere bakıldığında, YZ teriminin kendisi birincil tartışma konusudur[48]. YZ, "*insan tarafından tanımlanan belirli bir dizi hedef için içerik, tahminler, öneriler veya kararlar gibi çıktılar üreten mühendislik sistemine ayrılmış teknik ve bilimsel bir alandır*"[49].

Erken YZ, *bilgiye dayalıydı*. Günümüzün YZ'si ise *veriye dayalıdır.* Makine öğrenimi, verilerin göreve özgü bilgiye dönüştürülmesi için modeller ve yöntemler sağlayan disiplindir. YZ'nin son yıllardaki başarısının çoğu makine öğrenimine atfedilebilir. Yüz tanıma, uzun bir araştırma geçmişine sahip, öne çıkan bir YZ çalışmasına örnektir[50].

YZ'ye yönelik birçok uluslararası standart yayımlanmıştır veya yayımlanmak üzere geliştirilmektedir. Standartlardan yayımlanmış olanların hangi konuları içerdiği ve kapsam alanının neler olduğuna yönelik araştırmalar yapılmıştır. ISO tarafından yayımlanan standartlardan bazıları ise şu şekildedir;

Yapay zekâ kavramları ve terminolojisi[51]; YZ teknolojisi birçok alanda yer almaktadır. Teknolojinin paydaşları tarafından daha geniş toplumlar tarafından daha iyi anlaşılması ve benimsenmesi için standartlaştırılmış kavramlara ve terminolojiye ihtiyaç olduğu kuşkusuzdur. Ayrıca YZ kavramları ve kategorileri, farklı çözümlerin güvenilirlik, sağlamlık, esneklik, doğruluk, emniyet, güvenlik ve gizlilik gibi özelliklere göre karşılaştırılmasına ve sınıflandırılmasına olanak tanımaktadır. Bu belge YZ için terminolojiyi oluşturmakta ve YZ alanındaki kavramları açıklamaktadır. Bu belge, diğer standartların geliştirilmesinde, devlet kurumları, ticari şirketler, kâr amacı gütmeyen kuruluşlar gibi paydaşlar arasındaki iletişimi desteklemek amacıyla kullanılabilecektir[52].

---

47 Zielke, s. 259 - 274.

48 Zielke, s. 259 - 274.

49 ISO/IEC 22989:2022

50 Zielke, s. 259 - 274

51 ISO/IEC 22989:2022

52 International Organization for Standardization: ISO/IEC 22989:2022(en) Information technology - Artificial intelligence - Artificial intelligence concepts and terminology (https://www.iso.org/obp/ui/en/#iso:std:iso-iec:22989:ed-1:v1:en, E.T. 09.03.2024).

Yapay zekâ sistemleri için hesaplamalı yaklaşımlara genel bakış[53]; bu belge, bir YZ sisteminin özelliklerinin ve hesaplama yaklaşımlarının tanımını sağlamaktadır. YZ sistemlerindeki hesaplamalı yaklaşımların gösteriminde yer alan hem makine öğrenimini hem de makine dışı öğrenme yöntemlerini içermektedir. Bu belge, YZ sistemlerinin ana hesaplama özelliklerinde ve YZ kullanım örneklerinde[54] yer alan kullanım senaryolarına atıfta bulunarak, YZ sistemlerinde kullanılan ana algoritmalar ve yaklaşımları açıklayarak, YZ sistemleri için en son teknolojiye sahip hesaplamalı yaklaşımlara genel bir bakış sunmaktadır[55].

Yapay zekâ sistemlerinde ve yapay zekâ destekli karar vermede ön yargı[56]; Bu belge, YZ destekli karar alma konusunda, YZ sistemleriyle ilgili ön yargıları ele almaktadır. Ön yargı ile ilgili güvenlik açıklarını ele almak ve tamir etmek amacıyla ön yargıyı değerlendirmeye yönelik ölçüm teknikleri ve yöntemleri açıklamaktadır. Veri toplama, eğitim, sürekli öğrenme, tasarım, test etme, değerlendirme ve kullanım dahil tüm YZ sistemi yaşam döngüsü aşamaları kapsam alanındadır[57].

Yapay zekâda güvenilirliğe genel bakış[58]; Bu belgenin amacı, YZ sistemlerini sağlayan veya kullanan sistemlerin güvenilirliğini etkileyebilecek faktörleri analiz etmektir. Belgede, teknik sistemlerde güvenilirliği destekleyebilecek veya geliştirebilecek mevcut yaklaşımlar incelenmekte ve bunların YZ sistemlerine yönelik potansiyel uygulamaları tartışılmaktadır. Şeffaflık, açıklanabilirlik, kontrol edilebilirlik vb. yoluyla YZ sistemlerine güven oluşturmaya yönelik yaklaşımlar, YZ sistemlerine yönelik mühendislik tuzakları ve tipik tehditler ve riskler ile YZ sistemlerinin kullanılabilirliğini, esnekliğini, güvenilirliğini, doğruluğunu, güvenliğini ve gizliliğini değerlendirmeye ve elde etmeye yönelik yaklaşımlar ile ilgili konular incelen-

53 ISO/IEC TR 24372:2021

54 ISO/IEC TR 24030:2021

55 International Organization for Standardization: ISO/IEC TR 24372:2021(en) Information technology - Artificial intelligence (AI)- Overview of computational approaches for AI systems (https://www.iso.org/obp/ui/en/#iso:std:iso-iec:tr:24372:ed-1:v1:en, E.T. 09.03.2024).

56 ISO/IEC TR 24027:2021

57 International Organization for Standardization: ISO/IEC TR 24027:2021(en) Information technology - Artificial intelligence (AI) - Bias in AI systems and AI aided decision making (https://www.iso.org/obp/ui/en/#iso:std:iso-iec:tr:24027:ed-1:v1:en, E.T. 09.03.2024).

58 ISO/IEC TR 24028:2020

mektedir. Ancak YZ sistemleri için güvenilirlik seviyelerinin belirlenmesi bu belgenin kapsamı dışında yer almaktadır[59].

Yapay zekânın kuruluşlar tarafından kullanımının yönetişim sonuçları[60]; Bu belge, YZ'nin doğasını, mekanizmalarını ve kullanımlarının yönetişim sonuçlarını ele almaktadır. YZ kullanımının getirdiği ek fırsatların, risklerin ve sorumlulukların neler olabileceği ve teknolojilerin sonuçlarının anlaşılması gerektiğini belirtmektedir. Bu belgenin kapsamı, YZ kullanımının bir kuruluş üzerindeki etkileriyle ilgilidir. Her güçlü araçta olduğu gibi YZ'nin kullanımı, onu kullanan kuruluşların ele alması gereken yeni riskleri ve sorumlulukları beraberinde getirmektedir. YZ doğası gereği iyi ya da kötü, adil ya da ön yargılı, etik ya da etik dışı değildir; ancak kullanımı öyle olabilmekte ya da öyle görünebilmektedir. Bu belge, hem yönetişim hem de organizasyonel politikaları ve bunların uygulamalarını incelemekte ve bunların YZ kullanımına uyarlanması için rehberlik sağlamaktadır[61].

İnsan - sistem etkileşiminin ergonomisi - Bölüm 810: Robotik, akıllı ve otonom sistemler[62]; Bu belge, bir dizi robotik, akıllı ve otonom sistemlerinin ergonomisini gözden geçirmektedir. Bu teknolojilerin uygulanmasında dikkate alınması gereken insan - sistem sorunlarını ve gelecekteki standardizasyon çalışmaları için önceliklerin belirlenmesini açıklamaktadır. Kontrol görevlerinin otomasyonu ve tekrarlanan fiziksel veya bilişsel görevlerin mekanik düzene geçişi ile ilgili otomasyon düzeylerine odaklanmaktadır[63].

Büyük veri analitiği için süreç yönetimi çerçevesi[64]*;* sektör ne olursa olsun kuruluş genelinde büyük veri analitiğinden etkin bir şekilde yararlanmak için süreçlerin geliştirilmesine yönelik bir çerçeve sağlamaktadır. Büyük

---

59 International Organization for Standardization: ISO/IEC TR 24028:2020(en) Information technology - Artificial intelligence - Overview of trustworthiness in artificial intelligence (https://www.iso.org/obp/ui/en/#iso:std:iso-iec:tr:24028:ed-1:v1:en, E.T. 09.03.2024).

60 ISO/IEC 38507:2022

61 International Organization for Standardization: ISO/IEC 38507:2022(en) Information technology - Governance of IT - Governance implications of the use of artificial intelligence by organizations (https://www.iso.org/obp/ui/en/#iso:std:iso-iec:38507:ed-1:v1:en, E.T. 09.03.2024).

62 ISO/TR 9241-810:2020

63 International Organization for Standardization: ISO/TR 9241-810:2020(en) Ergonomics of human-system interaction - Part 810: Robotic, intelligent and autonomous systems (https://www.iso.org/obp/ui/en/#iso:std:iso:tr:9241:-810:ed-1:v1:en, E.T. 09.03.2024).

64 ISO/IEC 24668:2022

veri analitiği için süreç yönetimini, aralarındaki bağlantılarla birlikte dikkate alınan çeşitli süreç kategorileriyle belirtilmektedir. Bu süreç kategorileri; organizasyon paydaş süreçleri, yetkinlik geliştirme süreçleri, veri yönetimi süreçleri, analitik geliştirme süreçleri ve teknoloji entegrasyon süreçleridir. Büyük veri analitiği hizmetleri sağlayan bir kuruluş düzeyinde verilerin elde edilmesine, tanımlanmasına, saklanmasına ve işlenmesine yönelik süreçleri açıklamaktadır. Verinin kuantumu, toplanması, saklanması, kullanılması, teknolojisi, veri üretim hızı, verinin yapısı ve çeşitliliği geleneksel veri işleme yöntem ve çerçeveleriyle ele alınamayacaktır. Öncelikli hedef kitlesi kuruluşlardaki büyük veri analitiği uygulayıcılarının yanı sıra yetenek değerlendiricileridir. Bu çerçeve; en iyi uygulamalar olarak değerlendirilen süreçlerin yönetilmesi; görevli organizasyonun risk belirlemesini ve süreç iyileştirmelerini sağlamak için kullanılabilmektedir[65].

Makine Öğrenimini Kullanan Yapay Zekâ Sistemleri Çerçevesi[66]; Bu belge, makine öğrenimi teknolojisini kullanan genel bir YZ sistemini tanımlamak için bir YZ ve makine öğrenimi çerçevesi oluşturur. Çerçeve, sistem bileşenlerini ve bunların YZ ekosistemindeki işlevlerini açıklar. YZ sistemlerini uygulayan veya kullanan devlet kurumları, ticari şirketler ve kâr amacı gütmeyen kuruluşlar da dahil olmak üzere her tür ve boyuttaki kuruluş için geçerlidir[67].

Yapay Zekâ Yönetim Sistemi[68]; kuruluşlarda YZ yönetim sisteminin kurulması, uygulanması, sürdürülmesi ve sürekli olarak iyileştirilmesine yönelik bir "*Planla - Uygula - Kontrol Et - Önlem Al*" süreci etrafında oluşturulan uluslararası bir standarttır. Otomatik karar alma için YZ'nin bazen şeffaf olmayan ve açıklanamayan bir şekilde kullanılması, klasik anlamda var olan bilgi teknolojileri sistemlerinin yönetiminin dışında özel bir yönetim sistemi gerektirmektedir. Sistemleri tasarlamak için insan kodlu mantık yerine veri analizi, içgörü ve makine öğreniminin kullanılması, hem YZ sistemleri için uygulama fırsatlarını artırmakta hem de bu tür sistemlerin

---

65 International Organization for Standardization: ISO/IEC 24668:2022(en) Information technology - Artificial intelligence - Process management framework for big data analytics (https://www.iso.org/obp/ui/en/#iso:std:iso-iec:24668:ed-1:v1:en, E.T. 07.03.2024).

66 ISO/IEC 23053:2022

67 International Organization for Standardization: ISO/IEC 23053:2022(en) Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML) (https://www.iso.org/obp/ui/en/#iso:std:iso-iec:23053:ed-1:v1:en, E.T. 07.03.2024).

68 ISO/IEC 42001:2023

geliştirilme, gerekçelendirilme ve dağıtılma şeklini değiştirmektedir. Sürekli öğrenme gerçekleştiren YZ sistemleri, kullanım sırasında davranışlarını değiştirebilmektedir. Davranış değişiklikleriyle birlikte sorumlu kullanımlarının devam etmesini sağlamak için özel dikkat gerektirmektedir. Bu belge, YZ tabanlı ürün veya hizmetler sağlayan veya kullanan, YZ sistemlerinin sorumlu olarak geliştirilmesini ve kullanılmasını sağlayan kuruluşlar için tasarlanmıştır. Hızla değişen bu teknoloji alanı için rehberlik sağlayan dünyanın ilk YZ yönetim sistemi standardıdır. Genel olarak, YZ'nin ortaya çıkardığı etik hususlar, şeffaflık ve sürekli öğrenme gibi zorlukları ele almaktadır[69].

Risk yönetimine ilişkin rehber[70]; Bu belge, YZ'yi kullanan ürünleri, sistemleri ve hizmetleri geliştiren, üreten, dağıtan veya kullanan kuruluşların, özellikle YZ ile ilgili riskleri nasıl yönetebilecekleri konusunda rehberlik sağlamaktadır. Kılavuz aynı zamanda kuruluşların risk yönetimini YZ ile ilgili faaliyetlerine ve işlevlerine entegre etmelerine yardımcı olmayı amaçlamaktadır. YZ risk yönetiminin etkili bir şekilde uygulanması ve entegrasyonuna yönelik süreçleri açıklamaktadır[71].

İşlevsel güvenlik ve yapay zekâ sistemleri[72]; Bu belgenin amacı, YZ teknolojilerinin özellikleri, fonksiyonel güvenlik risk faktörleri ve yöntemleri ile potansiyel kısıtlamalar hakkında farkındalığı artırarak, güvenlikle ilgili sistemlerin geliştiricisinin, güvenlik fonksiyonlarının bir parçası olarak YZ teknolojilerini uygun şekilde uygulamasını sağlamaktır. Bu belge aynı zamanda YZ sistemlerinin işlevsel güvenliğiyle ilgili zorluklar ve çözüm konseptleri hakkında da bilgi sağlamaktadır. İşlevselliği gerçekleştirmek için güvenlikle ilgili bir fonksiyon içerisinde YZ'nin kullanılması, YZ kontrollü bir ekipmanın güvenliğini sağlamak için YZ güvenliğiyle ilgili olmayan işlevlerin kullanılması, güvenlikle ilgili fonksiyonları tasarlamak ve geliştirmek için YZ sistemlerinin kullanılması da bu belgenin kapsamı içerisindedir[73].

---

69 International Organization for Standardization: ISO/IEC 42001:2023(en) Information technology - Artificial intelligence - Management system (https://www.iso.org/obp/ui/en/#iso:std:iso-iec:42001:ed-1:v1:en, E.T. 07.03.2024).

70 ISO/IEC 23894:2023

71 International Organization for Standardization: ISO/IEC 23894:2023(en) Information technology - Artificial intelligence - Guidance on risk management (https://www.iso.org/obp/ui/en/#iso:std:iso-iec:23894:ed-1:v1:en, E.T. 07.03.2024).

72 ISO/IEC TR 5469:2024

73 International Organization for Standardization: ISO/IEC TR 5469:2024(en) Artificial intelligence - Functional safety and AI systems (https://www.iso.org/obp/ui/en/#iso:std:iso-iec:tr:5469:ed-1:v1:en, E.T. 08.03.2024).

Sinir ağlarının sağlamlığının değerlendirilmesi - Bölüm 1: Genel Bakış[74]; YZ olmayan sistemleri doğrulamak için birçok yöntem mevcut olsa da, bunlar her zaman YZ sistemlerine ve özellikle sinir ağlarına doğrudan uygulanamaz. Sinir ağı sistemleri, hem açıklanması zor hem de doğrusal olmadığından bazen beklenmedik davranışlara sahip olmaktadırlar. Bu nedenle sinir ağları, belirli bir zorluğu temsil etmekte ve alternatif yaklaşımlara ihtiyaç duyulmaktadır. Bu belge, sinir ağlarının sağlamlığını değerlendirmek için mevcut yöntemler hakkında arka plan sağlamaktadır[75].

Sinir ağlarının sağlamlığının değerlendirilmesi - Bölüm 2: Resmi yöntemlerin kullanımına ilişkin metodoloji[76]; Bu belge mevcut birkaç resmi yöntem tekniğini kapsamaktadır. Yaşam döngüsünün her aşamasında belge, sinir ağlarının sağlamlığını değerlendirmek ve sinir ağlarının resmi yöntemlerle nasıl doğrulandığını belirlemek için uygulanabilir kriterleri sunmaktadır. Resmi yöntemlerin ölçeklenebilirlik açısından sorunları olabilir ancak yine de çeşitli veri türleri üzerinde çeşitli görevleri gerçekleştiren tüm sinir ağları türlerine uygulanabilirler. Geleneksel yazılım sistemlerinde formal yöntemler uzun süredir kullanılıyor olsa da sinir ağlarında formal yöntemlerin kullanımı oldukça yenidir ve hala aktif bir araştırma alanıdır. Bu belge, sinir ağlarını kullanan ve YZ yaşam döngüsünün uygun aşamaları boyunca sağlamlıklarını değerlendirmekle görevli YZ geliştiricilerine yardımcı olmayı amaçlamaktadır. "*Yapay Zekâ (AI) - Sinir ağlarının sağlamlığının değerlendirilmesi - Bölüm 1: Genel Bakış*" belgesinde, bu belgede açıklanan resmi yöntemlerin ötesinde, sinir ağlarının sağlamlığını değerlendirmek için mevcut tekniklere ilişkin daha ayrıntılı bir genel bakış sağlamaktadır[77].

Yapay zekâ uygulamaları için kılavuz[78]; YZ'nin paydaşları, YZ sistemi yaşam döngüsünün çeşitli aşamalarıyla eşleştirilir, rolleri ve sorumlulukları vurgulanır ve YZ uygulaması için tutarlı bir paydaş katılımı sağlamak amacıyla

---

74 ISO/IEC TR 24029-1:2021

75 International Organization for Standardization: ISO/IEC TR 24029-1:2021(en)Artificial Intelligence (AI) - Assessment of the robustness of neural networks - Part 1: Overview (https://www.iso.org/obp/ui/en/#iso:std:iso-iec:tr:24029:-1:ed-1:v1:en, E.T. 08.03.2024).

76 ISO/IEC 24029-2:2023

77 International Organization for Standardization: ISO/IEC 24029-2:2023(en) Artificial intelligence (AI) - Assessment of the robustness of neural networks - Part 2: Methodology for the use of formal methods (https://www.iso.org/obp/ui/en/#iso:std:iso-iec:24029:-2:ed-1:v1:en, E.T. 08.03.2024).

78 ISO/IEC 5339:2024

takip edilecek süreçlerden haberdar olmaları sağlanır. Bu paydaşlar çeşitli düzeylerde YZ uzmanlığına ve bilgisine sahip olabilir. YZ uygulamaları, doğası gereği sürekli gelişen ve güvenilirlik yönleri nedeniyle diğer yazılımlardan farklı olduğundan, tüm paydaşların YZ'ye özgü nitelikler konusunda bilinçlendirilmesi gerekir. Bu belge, YZ uygulamalarının geliştirilmesi ve uygulanmasına yönelik bağlamın, fırsatların ve süreçlerin belirlenmesine yönelik rehberlik sağlar. Kılavuz, YZ uygulaması bağlamı, paydaşlar ve onların rolleri, sistemin yaşam döngüsüyle ilişkisi ve ortak YZ uygulaması özellikleri ve hususları hakkında makro düzeyde bir görünüm sağlar. Bu belge, çoklu makro düzeyde perspektifler sağlamak amacıyla ortak bir çerçeveye dayalı YZ uygulamalarına yönelik rehberlik içerir. Çerçeve, "yapma", "kullanma" ve "etki" perspektiflerini içermekle birlikte YZ özelliklerini, güvenilirlik ve risk yönetimi gibi işlevsel olmayan özellikleri de içermektedir[79].

Veri yaşam döngüsü çerçevesi[80]; YZ sistemleri her tür, boyut ve amaçtaki kuruluşlar tarafından benimsenmektedir. Veriler YZ sistemlerinin geliştirilmesi ve işletilmesi için gereklidir. YZ sistemleri alanında, kullanımda olan ve farklı amaçlar için değerlendirilen birçok veri yaşam döngüsü vardır (örn. veri kalitesi, verideki ön yargı, veri yönetişimi, YZ sistemlerinin geliştirilmesi ve kullanımı). Kapsamlı bir çerçeve olmadan, bu farklı veri yaşam döngülerinin önceden bilgisi, bağlamı ve uzmanlığı olmayan kişiler tarafından doğru şekilde yorumlanması zor olabilir. Bu çoklu veri yaşam döngülerinin amaçlandığı şekilde uygulanmama riski vardır. Bu belge, satın alma, oluşturma, geliştirme, dağıtım, bakım ve hizmetten çıkarma dahil olmak üzere YZ sisteminin yaşam döngüsü boyunca veri işlemeye yönelik aşamaları ve ilgili eylemleri tanımlar. Belirli hizmetleri, platformları veya araçları tanımlamaz. Bu belge, türü, boyutu veya niteliği ne olursa olsun, YZ sistemlerinin geliştirilmesinde ve kullanımında verileri kullanan tüm kuruluşlar için geçerlidir[81].

Yapay zekâ sistemi yaşam döngüsü süreçleri[82]; Bu belge, makine öğrenimi ve sezgisel sistemlere dayalı YZ sistemlerinin yaşam döngüsünü açıkla-

79 International Organization for Standardization: ISO/IEC 5339:2024(en) Information technology - Artificial intelligence - Guidance for AI applications (https://www.iso.org/obp/ui/en/#iso:std:iso-iec:5339:ed-1:v1:en, E.T. 09.03.2024).

80 ISO/IEC 8183:2023

81 International Organization for Standardization: ISO/IEC 8183:2023(en) Information technology - Artificial intelligence - Data life cycle framework (https://www.iso.org/obp/ui/en/#iso:std:iso-iec:8183:ed-1:v1:en, E.T. 09.03.2024).

82 ISO/IEC 5338:2023

maya yönelik bir dizi süreci ve ilgili kavramları tanımlamaktadır. Bu belge, YZ sisteminin yaşam döngüsü aşamalarında tanımlanmasını, kontrolünü, yönetimini, yürütülmesini ve iyileştirilmesini destekleyen süreçler sağlar[83].

Etik ve toplumsal kaygılara genel bakış[84]; YZ önemli riskler ve belirsizlikler getirebilmektedir. Profesyonellerin, araştırmacıların, düzenleyicilerin ve bireylerin YZ sistemleri ve uygulamalarıyla ilgili etik ve toplumsal kaygıların farkında olmaları gerekmektedir. YZ ile ilgili potansiyel etik kaygılar geniş kapsamlıdır. YZ'deki etik ve toplumsal kaygıların örnekleri arasında gizlilik ve güvenlik ihlalleri, ayrımcı sonuçlar ve insan bağımsızlığı üzerindeki etkiler yer almaktadır. YZ, özellikle ön yargılı veya uygunsuz verilerle eğitildiğinde ya da model veya algoritmanın amaca uygun olmadığı durumlarda adil olmayan bir şekilde çalışabilir. Algoritmalara gömülü değerlerin yanı sıra YZ sistemleri ve uygulamalarının ele almak için kullanıldığı sorunların seçimi, geliştiricilerin ve paydaşların kendi dünya görüşleri ve bilişsel ön yargıları tarafından kasıtlı veya kasıtsız olarak şekillendirilebilir. YZ'nin gelecekteki gelişimi, mevcut sistem ve uygulamaları genişleterek yeni alanlara doğru büyüyebilir ve bu sistemlerin sahip olduğu otomasyon düzeyini artırabilir. Sonuç olarak, YZ tasarımcıları, geliştiricileri, dağıtımcıları ve kullanıcıları, etik çerçeveler, YZ ilkeleri, risk azaltmaya yönelik araçlar ve yöntemler, etik faktörlerin değerlendirilmesi, test için en iyi uygulamalar, etki değerlendirmesi ve etik incelemelere ilişkin esnek girdilerden yararlanabilir. Bu belge, YZ'nin etik ve toplumsal kaygılarına üst düzey bir genel bakış sunmaktadır. Ayrıca bu belge bu alandaki ilkelere, süreçlere ve yöntemlere ilişkin bilgi sağlar; teknoloji uzmanlarına, düzenleyicilere ve genel olarak topluma yöneliktir; herhangi bir spesifik değer kümesini (değer sistemleri) savunmayı amaçlamaz. Bu belge, YZ etik ve toplumsal kaygılardan kaynaklanan sorunları ele alan uluslararası standartlara genel bir bakış içermektedir[85].

---

83 International Organization for Standardization: ISO/IEC 5338:2023(en) Information technology - Artificial intelligence - AI system life cycle processes (https://www.iso.org/obp/ui/en/#iso:std:iso-iec:5338:ed-1:v1:en, E.T. 09.03.2024).

84 ISO/IEC TR 24368:2022

85 International Organization for Standardization: ISO/IEC TR 24368:2022(en) Information technology - Artificial intelligence - Overview of ethical and societal concerns (https://www.iso.org/obp/ui/en/#iso:std:iso-iec:tr:24368:ed-1:v1:en, E.T. 09.03.2024).

Makine öğrenimi sınıflandırma performansının değerlendirilmesi[86]; Bu belge, makine öğrenimi modelleri, sistemleri ve algoritmalarının sınıflandırma performansını ölçmeye yönelik metodolojileri belirtir. Makine öğrenimi sınıflandırma performans değerlendirmesinde, tutarlı yaklaşımlar ve yöntemler uygulanmalıdır. Makine öğrenimi sınıflandırma performansının anlamlı şekilde farklılaştığı koşulları belirlemek için istatistiksel anlamlılık testleri yapılır. Makine öğrenimi modeli geliştirmede çeşitli potansiyel senaryoları ele almak için özel eğitim, doğrulama ve test metodolojileri kullanılır. Bu belge, makine öğrenimi sınıflandırma performansı iddialarının uygunluğunu, meşruiyetini ve genişletilebilirliğini sağlamaya yönelik yaklaşımları ve yöntemleri açıklamaktadır[87].

Yapay zekâ makine öğreniminin etkileri[88]; Bu belgenin temel amacı, YZ'nin alt kümesi olan makine öğrenimi uygulamalarının geliştirilmesine yönelik rehberlik sağlamaktır. Makine öğrenimi hızla gelişen bir teknolojidir ve şimdiye kadar makine güvenliğinin konusu olmamıştır. Makine öğreniminin makinelere uygulanmasının önemli ölçüde karmaşıklığı nedeniyle sistem güvenliği tehlikeye girebilmektedir. Bir kontrol sistemi, makinenin performansını artırmak veya görevlerini yürütmek için makine öğrenimini kullanabilecektir. Kontrol sistemi, bir sonraki beklenen davranışını eğitim yoluyla öğrenmektedir. Bu eğitim ve çıkarım (otonom operasyon) olmak üzere iki aşamayı içermektedir. Bu belge, makine tasarımcılarının kendi özel uygulamalarına uygun çözümler geliştirmelerine yardımcı olmayı amaçlamaktadır[89]. ISO 12100[90]' de, risk değerlendirme sürecinin YZ maki-

86 ISO/IEC TS 4213:2022

87 International Organization for Standardization: ISO/IEC TS 4213:2022(en) Information technology - Artificial intelligence - Assessment of machine learning classification performance (https://www.iso.org/obp/ui/en/#iso:std:iso-iec:ts:4213:ed-1:v1:en, E.T. 09.03.2024)

88 ISO/TR 22100-5:2021

89 International Organization for Standardization: ISO/TR 22100-5:2021(en) Safety of machinery - Relationship with ISO 12100 - Part 5: Implications of artificial intelligence machine learning (https://www.iso.org/obp/ui/en/#iso:std:iso:tr:22100:-5:ed-1:v1:en, E.T. 09.03.2024).

90 ISO 12100:2010; makine tasarımında güvenliğin sağlanmasına yönelik temel terminolojiyi, ilkeleri ve metodolojiyi belirtmektedir. Tasarımcıların bu hedefe ulaşmalarına yardımcı olmak için risk değerlendirmesi ve risk azaltma ilkelerini içermektedir. Bu ilkeler, makinelerle ilgili tasarım, kullanım, olaylar, kazalar ve risklere ilişkin bilgi ve deneyime dayanmaktadır. Makine yaşam döngüsünün ilgili aşamaları sırasında tehlikelerin tanımlanması ve risklerin tahmin edilmesi ve değerlendirilmesi ve tehlikelerin orta-

ne öğrenimi uygulamalarına nasıl uygulanacağı açıklanmaktadır. Bu belge, YZ makine öğreniminin makine ve makine sistemlerinin güvenliğini nasıl etkileyebileceğini ele almaktadır. Ayrıca makine veya makine sistemlerinde YZ uygulamaları makine öğrenimi ile ilişkilendirilen ve belirli sınırlar dahilinde hareket edecek şekilde tasarlanan tehlikelerin risk değerlendirme sürecinde nasıl dikkate alınabileceğini açıklamaktadır. Öngörülemeyen etkilere yol açabilecek, belirtilen sınırların ötesinde hareket edecek şekilde tasarlanmış YZ uygulamaları, makine öğrenimine sahip makineler veya makine sistemleri için geçerli değildir. Örneğin güvenlikle ilgili sensörler ve kontrol sistemlerinin güvenlikle ilgili diğer parçaları gibi YZ'li güvenlik sistemlerini ele almamaktadır[91].

Tüm bunların dışında ayrıca referans mimarisi (kurumsal, sistemler ve yazılım)[92], kentsel yönetim bilgisi oluşturan veri kümeleri ve veri işleme yöntemleri için değerlendirme çerçevesi[93], mimarinin temelleri (yazılım, sistemler ve kurumsal)[94], akıllı ulaşım sistemlerini destekleyen büyük veri ve yapay zekâ kullanım örnekleri[95], yapay zekâ yönetim sistemlerinin denetimini ve belgelendirmesini sağlayan kuruluşlar için gereklilikler[96], gereksinimler (fonksiyonel güvenlik ve yapay zekâ sistemleri)[97] gibi birçok yapay zekâ standart çerçeveleri de yayımlanmak üzere geliştirilmesi devam etmektedir.

---

dan kaldırılması veya yeterli risk azaltılması için prosedürler açıklanmaktadır. Risk değerlendirmesi ve risk azaltma sürecinin belgelenmesi ve doğrulanması konusunda rehberlik verilmektedir. (International Organization for Standardization: ISO 12100:2010(en) Safety of machinery - General principles for design - Risk assessment and risk reduction (https://www.iso.org/obp/ui/en/#iso:std:iso:12100:ed-1:v1:en, E.T. 15.03.2024)).

91 International Organization for Standardization: ISO/TR 22100-5:2021(en) Safety of machinery - Relationship with ISO 12100 - Part 5: Implications of artificial intelligence machine learning (https://www.iso.org/obp/ui/en/#iso:std:iso:tr:22100:-5:ed-1:v1:en, E.T. 09.03.2024).

92 ISO/IEC/IEEE AWI 42042

93 ISO/CD37114

94 ISO/IEC/IEEE AWI 42024

95 ISO/CD TR 12786

96 ISO/IEC DIS 42006

97 ISO/IEC AWI TS 22440

H. YAPAY ZEKÂ YÖNETİŞİM EKOSİSTEMİ

Tanıma işleminin kolay görünmesinin tek nedeni, insan beyninin algılama ve bunun sonucunda görüntüleri anlama konusunda gerçekten iyi olmasıdır. Son yıllarda, makine öğrenimi bu zor problemlerin çözümünde büyük ilerleme kaydetmiştir. Özellikle, derin evrişimli sinir ağı olarak adlandırılan model, zor görsel tanıma görevlerinin çözümünde bazı yönlerden insan performansıyla eşleşen veya aşan makul bir performansla sonuçlanabilmektedir[98]. Bir metin verisi olarak görüntü verileri, büyük miktarda belge koleksiyonu arasında belirli bir ögeyi ararken arama motorlarında depolanan diğer veri türlerine kıyasla en yaygın biçimdir. Görüntü erişiminden önce gelen birkaç adım vardır, bunlardan en önemlisi görüntü kümelemedir. Görüntü kümeleme, belgeleri birkaç ayrı gruba ayırarak organize etme işlemidir, her grup benzer şekilde ilgili konulara sahip ve diğer gruplardan tamamen farklı belgeler içerir. Bilgi keşfi, örüntü tanıma ve bilgi erişimi gibi veri madenciliği uygulamalarında önemli bir rol oynamaktadır[99].

YZ'nin veri girişi ve analizi gibi rutin görevleri otomatikleştirme yeteneği, araştırmacıların çalışmalarının daha karmaşık ve yaratıcı yönlerine odaklanmalarını sağlamaktadır. Bu sayede disiplinler arası iş birliği fırsatlarının da önünü açma potansiyelini barındırmaktadır. Daha fazla araştırmacı, metodolojileri belirli araştırma sorularına veya veri kümelerine göre özelleştirebilecek, böylece çeşitli alanlarda araştırmanın önemi ve etkisi artabilecektir. Özellikle tıbbi teşhis ve iklim bilimi gibi veri ağırlıklı uzmanlık alanlarında yüksek hassasiyet ve doğruluktaki iyileştirmeler, insan hatasını etkili bir şekilde azaltacak ve daha güvenilir sonuçlar verebilecektir. Bu kapsamda riski yönetmek ve tüm toplumu dahil ederken yeniliği teşvik etmek bu vizyonun önemli bir bileşenidir[100]. Örneğin Amerika Birleşik Devletlerinde Devlet Başkanının 30 Ekim 2023 tarihli "*Yapay Zekânın Güvenli, Emniyetli ve Güvenilir Geliştirilmesi ve Kullanımına İlişkin Yönetici*

98 Bebeshko B. / Khorolska K. / Kotenko N. / Desıatko A. / Sauanova K. / Sagyndykova S. / Tyshchenko D.: 3d Modelling By Means Of Artificial Intelligence, Journal of Theoretical and Applied Information Technology, Vol. 99, No. 6, Y. 2021, s. 1301 (https://www.jatit.org/volumes/Vol99No6/5Vol99No6.pdf, E.T. 17.04.2024).

99 Bebeshko vd., s. 1306.

100 Panchanathan Sethuraman: Envisioning the future of the AI research ecosystem, PNAS Nexus, Vol. 3, Y. 2024, s. 1, 2 (https://doi.org/10.1093/pnasnexus/pgae021, E.T. 18.04.2024).

Emri"[101] ile YZ'de yenilik ve rekabetin teşviki ile ulusal gelişimin arttırılmasının yanı sıra, risklerin tespiti, siber güvenlik, standartların oluşturulması, kişisel verilerin korunması, adalet ve eşitliğin sağlanması, hakların gözetilmesi gibi birçok konuda devletin kurumlarına görevler yüklemektedir. Bu belge üç konu başlığında toplanmaktadır: YZ yönetişiminin güçlendirilmesi, sorumlu YZ inovasyonunu ilerletmek ve kamunun haklarını ve güvenliğini etkileyen YZ'nin geliştirilmesi ve kullanımına yönelik zorunlu önlemleri benimsemeleri için kurumları yönlendirerek YZ kullanımından kaynaklanan riskleri yönetmek. Ayrıca *Ulusal Yapay Zekâ Araştırma Kaynağı*[102] pilotu ile *Ulusal Yapay Zekâ Yetenek Dalgası*[103] faaliyete geçirildi. Proje ile hem ulusal hem de uluslararası alandan profesyonellerin ve öğrencilerin katılımını teşvik eden bir sistem kurulduğu görülmektedir. Bu çerçevede YZ ekosistemi amaçlanmaktadır.

YZ ekosistemi, hem devlette risk, güvenlik ve gelişimi esas alan bir sistemi hem de şirketlerin ve bireylerin dahil olduğu üretim ve hizmet odaklı bir sistemi ifade etmektedir. Ülkemiz YZ ekosistemi içerisinde birinci sistemde, CBDDO önderliğinde TUBİTAK, Bilgi Teknolojileri Kurumu (BTK) gibi kurumlar aracılığıyla büyük ilerleme kaydetmektedir. İkincisinde ise herhangi somut anlamda oluşturulmuş bir sistem bulunmamaktadır. Her iki sistem açısından da ulusal standartların yanı sıra ulusal mevzuatın da belirlenmesi ve uygulanması gerekmektedir.

III. YAPAY ZEKÂ YÖNETİŞİM METODOLOJİSİNE ETKİ EDEN UNSURLAR

A. ULUSAL YAPAY ZEKÂ STRATEJİSİNİN ETKİSİ

Dünya çapında çok sayıda devlet, son yıllarda bu teknolojinin getirdiği fırsatları yakalamak ve zorluklarla başa çıkmak amacıyla ulusal YZ stratejileri yayımladı. Devletlerin üstlendiği rol ve işlevlere ilişkin olarak farklı bakışların yer aldığı görülmektedir. Dünya çapındaki 31 devletin stratejilerinin metinlerini araştıran bir çalışmada, niteliksel içerik analizleri gerçek-

101 ABD (2023), Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence (https://www.whitehouse.gov/briefing-room/presidential- actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/, E.T. 19.03.2024).

102 ABD (2023), The National Artificial Intelligence Research Resource (NAIRR) (https://nairrpilot.org/about, E.T. 19.03.2024).

103 ABD, The National AI Talent Surge (https://ai.gov/, E.T. 19.03.2024).

leştirilmiş ve stratejilerin hem kapsamları hem de metodolojileri belirlenmeye çalışılmıştır[104]. Bu çerçevede niteliksel içerik analizinin bulguları, istihdam, etik, Ar-Ge, regülasyon, veri, özel sektör desteği, kamu sektörü uygulamaları, farkındalık, dijital altyapı, ulusal güvenlik, ulusal zorluklar, uluslararası iş birliği ve mali destek konularını içeren on üç işlevi vurgulamaktadır. Bu işlevler, devletin rolünü temsil eden üç genel tema altında birleşmektedir: *kalkınma, kontrol ve teşvik*. Söz konusu analizin konu modelleme sonuçları da bu temaları yansıtmaktadır. Her genel tema strateji metinlerinde mevcuttur ancak metinlerde kapladıkları oran farklıdır. Bazı ülkeler kalkınmaya bazı ülkeler kontrole, bazıları ise teşvik düzenlemelerine odaklandığı tespit edilmiştir[105].

Ulusal YZ stratejileri devletlerin YZ'de ileri noktalara ulaşmak amacıyla yayımladığı bildirilerdir. Stratejik eylem planlarının yanı sıra gelecekte dünya ve galaksi YZ ekosisteminde devletlerin söz sahibi olma yarışı olduğu da göze çarpmaktadır. Genel olarak, ülkeler stratejik eylem planlarında üç ana alanda yoğunlaşmaktadırlar. Yeteneğin geliştirilmesi (eğitim programlarının oluşturulması: enstitüler ya da teşvik ve girişimlerin sağlanması yoluyla), yenilik ile Ar-Ge, kamu ve özel sektör iş birliği ile yatırım[106]. Devletin YZ'de sahip olabileceği dört rol ise; *düzenleyici, kolaylaştırıcı, lider ve/veya kullanıcıdır.*

İlki düzenleyici rolüyle devlet, olası riskleri ve tehlikeleri azaltmak için düzenleyici bir ortamı ve teknolojiyi iyi durumda tutarak ve tüm vatandaşların yaşamlarını iyileştirmeye odaklanarak YZ'nin toplumsal değerlerle uyumluluğunu sağlamaktır[107].

---

104 Papyshev Gleb / Yarime Masaru: The state's role in governing artificial intelligence: development, control, and promotion through national strategies, Policy Design and Practice, S. 6, Y. 2023, s. 79-102 (https://doi.org/10.1080/25741292.2022.2162252, E.T. 17.04. 2024).

105 Papyshev / Yarime, s. 79-102

106 Mutairi Muna B. Al / Ateeki Maha A. Al / Meshal Alanoud I. Al / Mutairi Faten B. Al / George Rhea / Almusharraf Ahlam: An Exploratory Review Of National Strategies In AI: A Systematıc Revıew, DCU&PNU MSc Business Administration Research Digest Y. 2023, s. 35. (https://doras.dcu.ie/28421/2/DCU%26PNU%20Research%20Digest%20-%202023.pdf#page=34, E.T. 18.04.2024).

107 Guenduez Ali A. / Mettler Tobias: Strategically constructed narratives on artificial intelligence: What stories are told in governmental artificial intelligence policies?, Vol. 40, Y. 2023 (https://doi.org/10.1016/j.giq.2022.101719, E.T. 21.05.2024).

İkincisi kolaylaştırıcı rolüyle devlet, potansiyel engelleri ve kısıtlamaları ortadan kaldırabilir, azaltabilir ve en aza indirebilir. İşletmeleri destekleyebilir ve YZ'nin kullanımını ve yayılmasını kolaylaştırabilir. YZ konusunda, yerel teknik altyapıya ve vatandaşların eğitimine yatırım yaparak, ülkenin YZ gelişimini ve uygulamasını ilerletmek için tüm potansiyelinin kullanılmasını sağlayabilir. Hükümetler, özel sektörün yenilikçi olması için güvenli ve istikrarlı yasal sınırlar ve elverişli bir iş ortamı sağlayarak fikri mülkiyete saygı duyulmasının yanında yeni YZ tabanlı işletmeleri teşvik edebilir ve yurt dışından yatırımcıları çekebilir[108].

Üçüncüsü lider rolüyle devlet, YZ tabanlı uygulamaların araştırılması ve geliştirilmesine aktif olarak dahil olabilir. Belirli alanlarda (örneğin; *siber savunma, kentleşme, afet yönetimi*) lider rolünü üstlenebilir ve araştırmacılarla, laboratuvarlarla, yeni kurulan şirketlerle ve hatta büyük şirketlerle iş birliği yaparak devletlerin "klasik hakimiyeti" dışındaki alanlara da genişleyebilir[109].

Dördüncüsü ise yapay zekâ teknolojisinin kullanıcısı rolüyle devlettir. Bugüne kadar literatürde bu tür çok sayıda uygulama durumu anlatılmıştır. Genelde ise YZ'yi benimsemenin ana motivasyonu olarak iç verimlilikten doğan kazanımlardan bahsedilmektedir. Devletlerin YZ'de kullanıcı rolüyle daha az yer aldığı görülmektedir[110]. Kamusal karar alma süreçlerinin etkinliğini de gösteren bu durum karşısında kamunun özel sektöre oranla alanın kısıtlı ve kontrollü olması etkili olmuştur.

B. RİSK TEMELLİ YAKLAŞIMIN ETKİSİ

Avrupa Birliği Yapay Zekâ Tüzüğü, AB'nin güvenilir teknolojilerin geliştirilmesinin YZ'nin Avrupa'da küresel olarak benimsenmesini teşvik edeceğini değerlendirmektedir. Avrupa Komisyonu'na göre güven inşa etmek, insanların güvenliğinin ve temel haklarının uygun şekilde korunmasını gerektirmektedir ve bu da YZ sistemlerinin neden ve nasıl kullanıldığına dair sınırlar koyarak elde edilebilecektir. Ancak bu sınırlar, teşvik etmeyi amaçladıkları yeniliği engelleyecek kadar külfetli olmaması gerektiği düşünülmektedir[111].

---

108 Guenduez / Mettler

109 Guenduez / Mettler

110 Guenduez / Mettler

111 Gaumond Eve: Artificial Intelligence Act: What Is The European Approach for AI?, Lawfare, Y. 2021 (https://www.lawfareblog.com/artificial-intelligence-act-what-european-approach-ai, E.T. 11.03.2024); Chamberlain Johanna: The Risk-Based Approach of the European Union's Proposed Artificial Intelligence Regulation: Some Com-

Tüzüğün nedenleri ve hedefleri başlıklı 1.1. maddesinin dokuzuncu paragrafında, orantılı risk temelli bir yaklaşım izlenerek AB'de YZ sistemlerinin geliştirilmesi, piyasaya sürülmesi ve kullanımına ilişkin uyumlaştırılmış kuralları içermektedir. YZ'nin geleceğe yönelik tek bir tanımı önerilmektedir. Özellikle zararlı bazı YZ uygulamaları AB değerlerine aykırı olduğu için yasaklanırken, kolluk kuvvetleri aracılığıyla uzaktan biyometrik tanımlama sistemlerinin sınırlı kullanımlarıyla ilgili olarak belirli kısıtlamalar ve korumalar önerilmektedir. Tüzük, kişilerin sağlığı ve güvenliği veya temel hakları açısından önemli riskler oluşturan "*yüksek riskli*" YZ sistemlerini tanımlamak için sağlam bir risk metodolojisi ortaya koymaktadır. Bu YZ sistemlerinin, güvenilir YZ için bir dizi yatay zorunlu gereksinime uyması ve bu sistemlerin AB pazarına sunulabilmesi için uygunluk değerlendirme prosedürlerini takip etmesi gerekmektedir. Tüm YZ sistemlerinin yaşam döngüsü boyunca temel hakları koruyan mevcut mevzuata saygı gösterilmesini ve güvenliğin sağlanması için bu sistemlerin sağlayıcılarına ve kullanıcılarına öngörülebilir, orantılı ve açık yükümlülükler de getirmektedir. Bazı spesifik YZ sistemleri için, özellikle sohbet robotları veya '*derin sahtekarlıklar*' kullanıldığında yalnızca minimum şeffaflık yükümlülükleri önerilmektedir.

Tüzüğün yaklaşımı, risk temelli bir yaklaşımdır. Her sektör veya alanın risk göstergesi bulunmaktadır. Öncelikle yasaklı YZ uygulamaları yer almıştır. Söz konusu düzenleme, Tüzüğün 5 inci maddesinde yer almaktadır. Yüksek riskli YZ sistemleri ise 6 ncı ve devamı maddelerinde yer almaktadır.

Tüzüğün, etki değerlendirmesi başlıklı 3.3 üncü maddesinde ise Komisyonun, AB içinde güvenilir YZ'nin geliştirilmesi ve kullanılmasına yönelik koşulları oluşturacağı, tek pazarın düzgün işleyişini sağlamak için farklı politika seçeneklerinin inceleneceği belirtilerek bu çerçevede yaklaşımın nedenlerini sıralamıştır. AB, Tüzükte her politika seçeneğini ekonomik ve toplumsal etkilere göre değerlendirdiğini ve özellikle temel haklar üzerindeki etkilere odaklanıldığını ifade etmektedir. Tercih edilen seçenek, yalnızca yüksek riskli YZ sistemlerine yönelik düzenleyici bir çerçeve getirmektedir. Yüksek riskli olmayan YZ sistem sağlayıcılarının ise davranış kurallarına uyma olanağı sunmaktadır. Bir diğer anlatımla AB'nin yaklaşımı; orantılı risk temelli bir yaklaşımı takip eden yatay AB mevzuat aracı ve yüksek riskli olmayan YZ sistemleri için zorunlu olmayan davranış kuralla-

ments from a Tort Law Perspective, European Journal of Risk Regulation, S. 14, Y. 2023, s. 1–13 (doi:10.1017/err.2022.38, E.T. 17.04.2024)

rının belirlenmesidir. Gereksinimlerin veri, dokümantasyon ve izlenebilirlik, bilgi sağlanması ve şeffaflık, insan gözetimi, sağlamlık ve doğrulukla ilgili olduğunu ve yüksek riskli YZ sistemleri için zorunlu olacağı ifade edilmektedir. Diğer YZ sistemleri için davranış kurallarını uygulamaya koyan şirketlerin ise bunları gönüllü olarak yapabileceği belirtilmektedir.

Tercih edilen seçeneğin, YZ geliştiricileri ve kullanıcılarından sınırlı ancak etkili bir dizi eylem gerektirdiğini, temel hakların ve insanların güvenliğinin ihlal edilmesi risklerini sınırlandırdığını ve gereklilikleri yalnızca yüksek risk bulunan sistemlere hedefleyerek, etkili denetim ve uygulamayı teşvik ettiğini belirtmektedir.

Sonuç olarak, bu seçeneğin, uyum maliyetlerini minimumda tuttuğunu ve böylece daha yüksek fiyatlar nedeniyle alımın gereksiz yavaşlamasını önleyeceği ifade edilmektedir. KOBİ'ler için olası dezavantajları ele almak amacıyla bu seçenek, düzenleyici sanal alanların oluşturulması ve uygunluk değerlendirmesine ilişkin ücretleri belirlerken KOBİ'lerin çıkarlarının göz önünde bulundurulması zorunluluğu da dahil olmak üzere, uyumluluklarını destekleyecek ve maliyetlerini azaltacak çeşitli hükümler içerdiğini belirtmektedir.

Tercih edilen seçenek sayesinde, insanların YZ'ye olan güveninin artacağını, şirketlerin hukuki kesinlik kazanacağı ve Üye Devletlerin, tek pazarı parçalayabilecek tek taraflı eylemlerde bulunmak için hiçbir nedeni kalmayacağı hedeflenmektedir. Daha yüksek güven sayesinde artan talebin, yasal kesinlik nedeniyle daha fazla Tüzük ve YZ sistemlerinin sınır ötesi hareketinin önündeki engellerin kalkması neticesinde tek pazarın gelişeceği belirtilmiştir. AB, YZ teknolojisini veya bağımsız YZ sistemlerini içeren yenilikçi hizmet ve ürünlerinden oluşan ve hızla büyüyen bir YZ ekosistemini geliştirmeye devam edeceği ve bu da dijital özerkliğin artmasını sağlayacağı ifade edilmiştir.

YZ'nin risk temelli bakış açısıyla düzenlenmesindeki en büyük nedenler; temel hakların korunması ve AB pazarının bölünmemesidir. Bu nedenle AB içinde YZ ekosistemi oluşturulması amaçlanmaktadır. Bu husus, Tüzüğün açıklayıcı not kısmına derç edildiği görülmektedir.

Yüksek riskli YZ sistemleri Ek-III' te belirtilmiştir:

1. Gerçek kişilerin biyometrik tanımlanması ve sınıflandırılması,
2. Kritik altyapının yönetimi ve işletilmesi,

3. Eğitim ve mesleki eğitim,
4. İstihdam, işçi yönetimi ve serbest mesleğe erişim,
5. Temel özel hizmetlere ve kamu hizmetlerine ve avantajlarına erişim ve bunlardan yararlanma,
6 .Kanunun uygulanması,
7. Göç, iltica ve sınır kontrol yönetimi,
8. Adaletin ve demokratik süreçlerin yönetimi.

Tüzüğün 53 üncü maddesinde, bir veya daha fazla Üye Devletin yetkili makamları veya Avrupa Veri Koruma Denetçisi tarafından sandbox[112] (YZ düzenleyici sanal koruma alanları) oluşturulacağı, yenilikçi YZ sistemlerinin belirli bir plan çerçevesinde piyasaya sürülmeden veya hizmete sunulmadan önce sınırlı bir süre için geliştirilmesini, test edilmesini ve doğrulanmasını kolaylaştıran kontrollü bir ortam sağlanacağı belirtilmiştir.

Sandbox kavramı, özellikle finansal inovasyon ve FinTech[113] alanlarında kullanılmaktadır. YZ alanında meydana gelen sürekli ve hızlı gelişmeler göz önüne alındığında, inovasyonu teşvik ederken vatandaşları ve toplumu korumak için sektör düzenlemeleri arasında bir denge oluşturulmasına hayati bir ihtiyaç vardır. Sandbox düzenlemeleri çoğunlukla konuyla ilgili geniş bir literatürün bulunduğu FinTech sektöründe uygulandığından, sandbox etrafındaki karmaşıklıklar da öngörülebilecektir[114]. Fintech'in aksine, YZ'yi düzenlemek için sanal alanların kullanımı daha fazla araştır-

---

112 Sandbox; donanım veya diğer yazılımları etkilemeden yazılımı çalıştırabileceğiniz bir bilgisayar sistemindeki test alanı (Oxford Üniversitesi, Oxford English Dictionary (https://www.oed.com, E.T. 18.04.2024)).

113 Fintech: Bankacılık ve finansal hizmetlerin sağlanmasında kullanılan bilgisayar programları ve diğer teknolojiler (Oxford Üniversitesi, Oxford English Dictionary (https://www.oed.com, E.T. 18.04.2024)).

114 Truby Jon / Brown Rafael Dean / Ibrahim Imad Antoine / Parellada Oriol Caudevilla: A Sandbox Approach to Regulating High-Risk Artificial Intelligence Applications, European Journal of Risk Regulation, Vol. 13 Y. 2022, s. 293–294 (doi:10.1017/err.2021.52, E.T. 18.04.2024); Allen Hilary J.: Sandbox boundaries, Vanderbilt Journal of Entertainment and Technology Law, Vol. 22, Y. 2020 (https://scholarship.law.vanderbilt.edu/cgi/viewcontent.cgi?article=1017&context=jetlaw, E.T. 18.04.2024); Ringe Wolf Georg / Ruof Christopher: Regulating FinTech in the EU: the Case for a Guided Sandbox, European Journal of Risk Regulation, Vol. 11, Y. 2020, s. 605 (doi:10.1017/err.2020.8, E.T. 18.04. 2024).

ma gerektirmektedir. Bu zorluklara rağmen, sandbox düzenlemesinin hedefinin katı sorumluluk kurallarıyla ilgili olandan büyük ölçüde farklı olması nedeniyle, yüksek riskli YZ'ler bağlamında kesin sorumluluk rejimini tamamlamak için daha uygundur. Kesin sorumluluk kuralları, kesin sorumluluk atamaya ve zarar durumunda bir kişinin sorumlu tutulmasını sağlamaya odaklanırken, sandbox düzenlemesindeki amacın "*düzenleme var olmadan önce düzenleme yapmak*" olduğu ve hukuki alanda bir tür yenilik getirdiği belirtilmektedir. Böylelikle FinTech sektöründe oluşturulan güvenli alana benzer şekilde, test edilmiş ve yüksek riskli YZ'lerin regülasyonunda en uygun teknik düzenlemeyle sektörde deneme - yanılma yaklaşımları için yeni bir güvenli alan oluşturulacaktır[115].

Avrupanın ilk Yapay Zekâ Denetleme Ajansı AESIA[116]'yı kuran ve Kraliyet Kararnamesi yayımlayarak[117] sandbox sistemini düzenleyen ve pilot olarak kuran ilk ülke İspanya oldu[118]. Pilot sistemin kurulum şeması başta olmak üzere, düzenlemeleri, yazılım aşamaları, sorunları ve geliştirilmesi gereken yönleri gibi birçok açıdan diğer ülkeleri etkileyeceği düşünülmektedir.

Sonuçta risk temelli yaklaşım çerçevesinde Tüzüğün, birçok yeni kurum ve düzenlemenin yanı sıra yazılım sistemlerinin de kurumların gözetiminden geçeceği bir yönetişim modeli öngörülmektedir. Bu çerçevede YZ'ye dayalı yazılım sistemlerinin özellikle Tüzükte yüksek risk kategorisinde belirlenen alanlarda faaliyet göstermesi durumunda birçok konuda dikkat etmesi gereken hususlar olacaktır. Bu regülasyonlar hâlihazırda İspanya dışında uygulama alanı bulmasa da özel şirketlerin veya kamunun oluşturacağı sistemlerin Tüzükte belirlenen şartlara şimdiden uyum sağlaması ileride doğabilecek olumsuz sonuçları da bertaraf edebilecektir.

C. ÜRETKEN YAPAY ZEKÂ SİSTEMLERİNİN ETKİLERİ

Üretken yapay zekâ terimi, eğitilen verilerinden metin, resim, video veya ses gibi görünüşte yeni, anlamlı içerik üretebilen hesaplama tekniklerini

---

115 Truby / Brown / Antoine / Caudevilla, s. 294

116 İspanya Krallığı (2022), 21 Aralık 2022 tarih ve 28/2022 sayılı Kanun (https://www.boe.es/buscar/doc.php?id=BOE-A-2022-21739, E.T. 14.04.2024).

117 İspanya Krallığı (2023), 8 Kasım 2023 tarihli ve 817/2023 sayılı Kraliyet Kararnamesi (https://www.boe.es/boe/dias/2023/11/09/pdfs/BOE-A-2023-22767.pdf, E.T. 14.04.2024).

118 Avrupa Komisyonu (2022), First regulatory sandbox on Artificial Intelligence presented (https://digital-strategy.ec.europa.eu/en/news/first-regulatory-sandbox-artificial-intelligence-presented, E.T. 14.04.2024)

ifade etmektedir. *Üretken bir yapay zekâ modeli ise*, bir makine öğrenimi mimarisi (örneğin, derin sinir ağı) ile başlatılan ve dolayısıyla öğrenilen kalıplara dayalı olarak yeni veri örnekleri oluşturabilen üretken modellemeyi ifade etmektedir. Üretken yapay zekâ modeli, eğitilen verilerde gözlemlenen kalıplardan ve ilişkilerden yararlanarak yeni veri örnekleri oluşturmak için YZ algoritmalarını kullanan bir tür makine öğrenimi mimarisidir. Derin sinir ağları, farklı veri türlerini modellemek için farklı mimariler kullanılarak tasarlanabildiğinden veri oluşturma amacına uygun yapılardır[119].

Üretken yapay zekâ sistem tasarım mimarisi dört konu üzerinde şekillenmektedir; *girdi, çıktı, modalite ve operasyon*.

Girdi, kullanıcı tarafından sağlanan ve üretici yapay zekâ tarafından işlenen veri türünü belirtir. En yaygın girdi türleri metin, görüntü, video veya sestir[120].

Çıktı, üretken yapay zekâ tarafından oluşturulan veri türüyle ilgilidir. Metin, görüntü, video, üç boyutlu (3B) model ve ses temel çıktı özellikleridir. Çıktıdaki çeşitlilik, üretken yapay zekâ tarafından sunulan geniş olasılıkları göstermektedir[121].

Modalite[122], girdi ve çıktı yetenekleri açısından üretken yapay zekânın çok yönlülüğünü ve esnekliğini ifade etmektedir. Bu sebeple aynı anda kaç veri türünün işlenebileceğini incelemektedir. Bire bir uygulamalar tek bir girdi türünü kabul eder ve tek bir çıktı türü üretir; örneğin, sohbet robotu, me-

---

119 Feuerriegel Stefan / Hartmann, Jochen / Janiesch Christian / Zschech Patrick: "Generative AI", Business & Information Systems Engineering, Vol. 66, Y. 2024, s. 111-126 (https://doi.org/10.1007/s12599-023-00834-7, E.T. 17.04.2024).

120 Strobel Gero / Banh Leonardo / Möller Frederik / Schoormann Thorsten: Exploring Generative Artificial Intelligence: A Taxonomy and Types, Proceedings of the 57th Hawaii International Conference on System Sciences, Y. 2024, s. 4550 (https://scholarspace.manoa.hawaii.edu/server/api/core/bitstreams/fa9a6175-9ff2-4ad4-868e-fec5127cd430/content, E.T. 17.04.2024).

121 Strobel vd. s. 4550

122 Modalite; bir şeyin var olduğu, deneyimlendiği, ifade edildiği ya da yapıldığı kanal. Terim, aralarında tıp, temel bilim, teknoloji, beşeri bilimler ve dilbilim olmak üzere pek çok alanda kullanılır. 1. duyum modalitesi: Duyumun oluştuğu kanal; duyum türü (örn., görme, işitme), 2. Tepki modalitesi: Tepkinin oluştuğu kanal; tepki türü (örn., yazılı, sözlü), 3. Tanısal modalite: Tıp doktorunun tanıyı koymada kullandığı teknik veya yöntem (örn., bilgisayarlı beyin tomografisi, radyografi, mammografi). (Karakaş Sirel: Prof. Dr. Sirel Karakaş Psikoloji Sözlüğü, Y. 2017, (www.psikolojisozlugu.com, E.T. 13.03.2024)).

tinden metine bir uygulamadır. Birden çoğa uygulamalar ise tek bir girdiye dayalı olarak birden fazla çıktı üretmektedir[123]. Örneğin, metin olarak ifade edilen tasarımların, görüntü veya video olarak çıktı üretilmesine olanak sağlayan uygulamalar.

Operasyon, üretken yapay zekâyı dağıtma ve yönetme kontrolünü tanımlar. Uygulamanın kullanım durumuna ve gereksinimlerine bağlı olarak, bir platform sağlayıcısı tarafından yönetilmesi veya kendi bünyesinde barındırılmasıdır. Özellikle hassas verilerin yer aldığı kritik kullanım durumlarında, verinin korunması önem taşıdığından şirket içinde bulundurulmasına izin verilir[124].

Üretken yapay zekâ uygulamalarının sürekli artan kapsamı ve yaygınlığı, yalnızca güvenilir tasarımlar için koruma mekanizmaları sağlamakla kalmayıp, aynı zamanda kullanıcı üzerindeki etkilerin de incelenmesine yönelik eylem planlarının ortaya konulması gerekmektedir. Bu tür uygulamaların son kullanıcılar ve kuruluşlar tarafından kullanılması ve benimsenmesi, inovasyon potansiyelini etkilemekle birlikte üretken yapay zekâ eserlerinin tanınırlığı ve bilinirliğinin hukuken koruma mekanizmasında yerinin belirlenmesi açısından bir dizi temel sosyo - teknik hususların yasa koyucular tarafından regülasyon geliştirilirken dikkate alınması gereklidir[125].

Geçmişte YZ'nin yeteneğinin çoğunlukla analitik olduğu ve karar verme görevlerine uygun olduğu düşünülmekteydi. Artık YZ, içerik oluşturmaya uygun üretken görevleri gerçekleştirme becerisi kazanmıştır. İçerik oluşturma prosedürü, doğası gereği olasılıklara dayalı olduğundan bir bakıma analitik olarak değerlendirilebilirken, üretken YZ'nin ögeleri yeni yollarla birleştirmesi nedeniyle sonuçları yaratıcı fikirlerin oluşmasının yanı sıra sanatsal dahi olabilmektedir. Ayrıca bilgi teknolojilerine dayalı eserler, doğrudan insanlar tarafından kullanıldıkları için pasif kapsamda kabul edilmekteydi. Ancak insan ve YZ'nin entegrasyonu olan mevcut hibrit zekâ[126] anlayışı, her ikisinin benzersiz güçlü yanlarından yararlanılması durumunda, YZ'nin sürekli olarak hayatın merkezinde yer almasını sağla-

123 Strobel vd. s. 4550

124 Strobel vd. s. 4550

125 Feuerriegel vd.

126 Dellermann Dominik / Ebel Philipp / Söllner Matthias / Leimeister Jan Marco: Hybrid Intelligence, Business & Information Systems Engineering, Vol. 61, Y. 2019, s. 637–643 (https://doi.org/10.1007/s12599-019-00595-2, E.T. 13.03.2024).

yacaktır. Hibrit zekâ, gelişmiş karar verme ve problem çözme yetenekleri elde etmek için insan sezgisini, yaratıcılığını ve empatisini, YZ sistemlerinin hesaplama gücü, doğruluğu ve ölçeklenebilirliği ile birleştirerek her zekâ türünün sınırlamalarını ele almayı savunmaktadır[127].

Üretken yapay zekânın dört sınırı vardır; *yanlış çıktılar, ön yargı ve adalet, telif hakkı ihlali ve çevresel kaygılar.*

Yanlış çıktılar, üretken yapay zekâ modelleri hatalı çıktılar üretebilir. Bu durumun olması, olasılıksal algoritmalara dayanan makine öğrenimi modellerinin temel doğasından kaynaklanmaktadır. Örneğin, günümüz teknolojisinde üretken yapay zekâ modelleri bir soruya en olası yanıtı üretir, mutlaka doğru yanıtı oluşturmaz[128]. Bilimsel olarak çalışma prensibi olasılık üzerine dayanan bir sistemde, verilerin hatalı öğretilmesi, bağlantılı veri mekanizmaların yanlış kurgulanması, verinin baştan beri hatalı olması gibi daha pek çok durumdan kaynaklanan nedenlerden dolayı hatalı çıktıların olması muhtemeldir.

Ön yargı ve adalet, toplumsal ön yargılar, insanların ürettiği günlük içeriğe nüfuz etmektedir. Ön yargılı veriler üzerinde derin öğrenme modellerini eğitmek, sistemde yer alan ön yargılarını güçlendirebilir[129] ve algoritmaların yanlış çıktı üretmesine neden olabilir.

Telif hakkı ihlali, üretken yapay zekâ modellerin, sistemlerin ve uygulamaların, eğitildiği kaynak verilerin hak sahiplerinin icazeti olmadan mevcut çalışmalara benzeyen ve hatta kopyalayan çıktılar üretebildikleri için telif haklarının ve buna yönelik yasaların ihlaline neden olabilecektir[130].

Çevresel kaygılar, bu tür sistemlerin tipik olarak büyük ölçekli sinir ağları etrafında inşa edilmesi ve dolayısıyla bunların geliştirilmesi ve işletilmesi sırasında büyük miktarda elektrik tüketmesi ve çok büyük negatif karbon ayak izine sahip olması nedeniyle, üretken yapay zekâ sistemlerinin geliştirilmesi ve kullanılmasından kaynaklanan önemli çevresel kaygılar bulunmaktadır. Yani üretken yapay zekâ, yeni iş fikirlerinin geliştirilmesinin, görülmemiş ürün ve hizmet yeniliklerinin ve sonuçta tamamen yeni iş modellerinin ortaya çıkmasını sağlayacaktır. Aynı zamanda çalışma kalıpları,

127 Feuerriegel vd.

128 Feuerriegel vd.

129 Feuerriegel vd.

130 Feuerriegel vd.

organizasyon yapıları, liderlik modelleri ve yönetim uygulamaları gibi organizasyon içi unsurlar üzerinde de güçlü bir etkiye sahip olacaktır. Bu bağlamda, YZ tabanlı asistan sistemlerinin daha önce masaüstü otomasyona odaklandığını ve etkinlik yönetimi, kaynak tahsisi ve sosyal medya hesap yönetimi gibi giderek daha fazla rutin görevi üstlenerek insana olan ihtiyacı azaltacağı değerlendirilmektedir[131]. Aslında insanın öneminin artacağı, statik ve otomasyon olan görevlerde insanlara rol verilmeyeceği, inovasyon aşamalarına ise daha fazla zaman harcanacağı düşünülmektedir. Bu durum da hem devletlerin hem de özel şirketlerin gelişmesini, hizmet kalitesinin artmasını ve farklı sektörlerin oluşmasını sağlayacaktır.

Üretken yapay zekâ sistemleri, girdi ve çıktı olarak ifade edilmek gerekirse; *metin - metin, metin - resim, metin - video, resim - metin, resim - resim, resim - video, video - metin, video - resim, video - video* şeklinde birçok YZ programları hayatımızın içindedir. Bunların yanında metin istemlerini kullanarak belirli nesne kategorilerinde otomatik olarak yüksek kaliteli 3B modeller oluşturulmaya başlanmıştır. Örneğin, insansız hava araçlarıyla (İHA) alınan görüntülerin 3B analizi, nesne tanımlanması, kümeleme çalışmaları gibi birçok analiz YZ tabanlı sistemler aracılığıyla Coğrafi Bilgi Sistemlerinde (CBS) kullanılmaktadır[132]. İHA platformu taşıma kapasitesine ve özelliklerine bağlı olarak termal, kızılötesi kamera ya da video kamera sistemlerinin, multispektral kameraların, LIDAR algılayıcıların her birinin veya birkaçının bir arada bulunması ile donatılan sistemlerin verileri

---

131 Feuerriegel vd.

132 Türk Tarık / Tunalıoğlu Nursun / Erdoğan Bahattin / Öcalan Taylan / Gürtürk Mert: *Accu-racy assessment of UAV-post-processing kinematic (PPK) and UAV-traditional (with ground control points) georeferencing methods*, Environmental Montoring And Assessment, C. 194(7), Y. 2022, s. 1 - 12 (https://doi.org/10.1007/s10661-022-10170-0); Türk Tarık / Tunalıoğlu Nursun / Öcalan Taylan / Gürtürk Mert: *Investigation of accuracy of PPP and PPP-AR methods for direct georeferencing in UAV photogrammetry*, Earth Science Informatics, C. 15(4), Y. 2022, s. 2231–2238: Türk Tarık / Öcalan Taylan: *PPK GNSS Sistemine Sahip İnsansız Hava Araçları İle Elde Edilen Fotogrametrik Ürünlerin Doğruluğunun Farklı Yaklaşımlarla İrdelenmesi*. Türkiye Fotogrametri Dergisi, C. 2(1), Y. 2020, s. 22–28. YZ ile üç boyutlu arazi modelleme analizinin yapılabilmesi: Ölçme sonrası veri değerlendirme (Post Processing Kinematic - PPK) veya Gerçek Zamanlı Kinematik (Real Time Kinematic-RTK) konumlama modunda çalışan GNSS alıcı/antenine sahip İHA'lar ile başta kadastro, tarım ve ormancılık olmak üzere birçok farklı alanda hukuki problemlerin çözümünde oldukça önemli bir veri kaynağı olan ortogörüntü, halihazır harita ve Sayısal Yüzey Modeli (SYM) gibi ürünler cm seviyesinde yüksek doğrulukla üretilebilmektedir. Ardından, farklı amaçlar doğrultusunda bu ürünler kullanılıp yapay zekâ ile bütünleştirilerek hukuki açıdan isabetli karar verme sürecine büyük katkı sağlanabilir (Türk ve Öcalan, 2020; Türk vd., 2022; Öcalan vd., 2022).

oluşturduğu bilinmektedir[133]. 3B modellerin oluşturulmasında bilişimin yanı sıra, coğrafi bilgi sistemleri, sanayi, uzay sanayi ve dizayn gibi birçok alanlarda kolaylaştırıcı etkisinin yanında farklı çözümler sunması bu alanın ticari formasyonda ileri boyutlara evirilebileceğini göstermektedir[134]. Özellikle YZ'deki gelişmelerin üretken yapay zekâya önem atfetmesi neticesinde bu alandaki yelpazenin de bu sayede genişleyeceği öngörülmektedir.

D. SÜPER HİZALAMA VE ETKİLERİ

Süper hizalama *(alignment)*, her alanda insan zekâsını aşan süper yapay zekâ sistemlerinin insan değerlerine ve hedeflerine göre hareket etmesinin sağlanması anlamına gelmektedir. YZ güvenliği ve yönetişimi alanında son derece gelişmiş YZ'nin geliştirilmesi ve dağıtılmasıyla ilişkili riskleri ele almayı amaçlayan önemli bir kavramdır. Süper hizalama, süper akıllı yapay zekâ sistemlerinin insan değerleri ve niyetleriyle uyumlu şekilde hareket etmesini sağlamaktadır. İnsan tercihlerinin doğru bir şekilde belirlenmesi, bunları anlayabilen YZ sistemlerinin tasarlanmasını ve bu hedeflere ulaşmasını sağlayacak mekanizmalar oluşturulmasını gerektirmektedir[135].

Süper hizalama, süper zekâyla ilişkili potansiyel risklerin ele alınmasında çok önemli bir rol oynamaktadır. Süper hizalamaya neden olan durumlar ise şu şekildedir;

Hileli yapay zekâ senaryolarını azaltma: Süper hizalama, süper akıllı yapay zekâ sistemlerinin insan niyetiyle uyumlu olmasını sağlayarak kontrolsüz davranış ve olası zarar risklerini azaltır[136].

İnsani değerleri korumak: Süper hizalama, YZ sistemlerini insani değerlerle uyumlu hale getirerek, süper akıllı yapay zekânın toplumsal normlar ve ilkelerle uyumsuz hedeflere öncelik verebileceği çatışmaları önler[137].

---

133 Hem LIDAR haritalama yöntemleri hem de Fotogrametrik haritalama yöntemleri, yeryüzünün ve yeryüzü üzerinde bulunan yapay nesnelerin 3B modellenmesi sürecinde önemli rol oynamaktadır. LIDAR haritalama yönteminde İHA ya takılı lazer tarayıcı ile bir hedefe lazer ışığı gönderilmekte, nesnelere çarpan lazer ışınları geri yansıyarak sinyal şeklinde geri alınmaktadır.

134 Hesaplamalı 3B modellemeyi kullanılabilir hale getirmek için üç temel gereksinim vardır; tatmin edici kalite, hızlı üretim süresi, basit kullanım (Bebeshko vd. s. 1296).

135 Awan Abid Ali: What is Superalignment & Why It is Important?, Kdnuggets, (https://www.kdnuggets.com/2023/07/superalignment-important.html, E.T. 14.03.2024).

136 Awan.

İstenmeyen sonuçlardan kaçınma: Süper hizalama araştırması, gelişmiş yapay zekâ sistemlerinden kaynaklanabilecek istenmeyen olumsuz sonuçları tespit edip hafifleterek potansiyel olumsuz etkileri en aza indirir[138].

İnsan bağımsızlığının sağlanması: Süper hizalama, YZ sistemlerini insan yeteneklerini artıran, bağımsızlığımızı koruyan ve YZ'nin karar verme sürecine aşırı güvenmeyi önleyen değerli araçlar olarak tasarlamaya odaklanır[139].

Yararlı bir yapay zekâ geleceği inşa etmek: Süper hizalama araştırması, süper akıllı yapay zekâ sistemlerinin insan refahına olumlu katkıda bulunduğu, riskleri en aza indirirken küresel zorlukları ele aldığı bir gelecek oluşturmayı amaçlamaktadır[140].

ChatGPT YZ programının sahibi olan firmanın, bir süper istihbaratın hileye başvurmasını engellemek istediği ve ilk adım olarak süper hizalama ekibi kurduğu görülmektedir. Sürekli kendisini geliştiren YZ programının, daha az güçlü büyük dil modelinin daha güçlü bir modeli denetlemesine olanak tanıyan bir tekniğin kullanılabileceği ve bunun, insanların insanüstü makineleri nasıl denetleyebileceğini anlama yolunda küçük bir adım olabileceğini ifade edilmektedir. Hizalama, *bir modelin yapmasını istediğiniz şeyi yaptığından ve yapmasını istemediğiniz şeyi yapmadığından emin olmak* şeklinde tanımlanmaktadır[141].

Süper hizalama, bu fikri insanüstü modellere uygulamaktadır. Mevcut modelleri uyumlu hale getirmek için kullanılan en yaygın tekniklerden biri, insan geri bildirimi yoluyla pekiştirmeli öğrenmedir. İnsan test uzmanları, bir modelin yanıtlarını puanlayarak, görmek istedikleri davranışları olumlu, istemedikleri davranışları ise olumsuz oy vermektedir. Bu geri bildirim ise daha sonra modeli yalnızca insan test uzmanlarının beğendiği türden yanıtlar üretecek şekilde eğitilmesine neden olmaktadır. Programın, insanların ilk etapta neyin arzu edilen davranış olup olmadığını söyleyebilmesi gerekmektedir. Ancak insanüstü bir modelde ise bir insanın testte anlayamadığı ve dolayısıyla puanlayamayacağı şeyleri değerlendirmektedir. Ge-

137 Awan.

138 Awan.

139 Awan.

140 Awan.

141 Heaven Will Douglas, Now we know what OpenAI's superalignment team has been up to, MIT Technology Review, Y. 2023 (https://www.technologyreview.com/2023/12/14/1085344/openai-super-alignment-rogue-agi-gpt-4/, E.T. 15.03.2024).

lecekteki insanüstü modellerin, muhtemelen araştırmacıların bilmediği ve yeni ortaya çıkacak yeteneklere sahip olacağı düşünülmektedir[142]. Burada ortaya çıkan durum ise, insan ve eğitim verdiği veya puanladığı makinenin değişmesine göre hizalama tekniğinin farklılaşmasıdır: *birinci aşama;* insan - daha az akıllı makine, *ikinci aşama;* insan - daha çok akıllı makine, *üçüncü aşama;* daha az akıllı makine - daha çok akıllı makine şeklinde aşamaların dönüşeceği öngörülmektedir. Görüldüğü üzere insanın rolünün ikinci aşamadan sonra ortadan kalkacağı ve YZ'nin kontrolünün yine YZ tarafından yapılabileceği değerlendirilmektedir.

YZ hizalama sorunu hakkında, bir dizi başka disiplindeki makine öğrenimi alanında yer alan bilim insanlarından oluşan ekip tarafından teorik ve uygulamalı araştırma neticesinde rapor yayımlanmıştır[143]. Söz konusu rapor, hizalama hakkında önemli tespitlerde bulunmaktadır. Raporda bahsedilen *Vingean Yansıması*, Vinge Vernor' un "*Gerçek İsimler*" adlı bilim kurgu romanındaki gözlemine dayanmaktadır[144].

Vinge Vernor, toplumun teknolojik ilerlemesini tahmin etmeye çalışan bir bilim kurgu yazarı olup sonunda kendi modelinin teknolojik gelişmeyi öngördüğü bir noktaya ulaşacağını gözlemlemiştir. Bu gözlemin ana teması, mevcut insan zekâsından daha akıllı insan zekâsının oluşturulması üzerinedir[145]. Söz konusu gözlem, teknik olarak hipotezle açıklanmaya çalışılmıştır. Yazar tarafından ortaya atılan "*Teknolojik Tekillik*"[146] de formüle

---

142 Heaven

143 Soares Nate / Fallenstein Benja, Aligning Superintelligence with Human Interests: A Technical Research Agenda, Machine Intelligence Research Institute, Technical report 2014-8.

144 Yudkowsky Eliezer / Herreshoff Marcello, Tiling Agents for Self-Modifying AI, and the Löbian Obstacle, Early Draft MIRI, Y. 2013, s.21 dn. 33 (https://intelligence.org/ files/TilingAgentsDraft.pdf, E.T. 18.04.2024); Vinge Vernor: True Names, Y. 1981.

145 Vingean Yansıması'nı "Tekillik" ile açıklanmaktaydı. Bu terim, 1980'lerdeki fiziksel teorilerin bir kara deliğin oluşumunu tahmin etmesi ancak kara deliğin içerisinde ne olduğunu tanımlamaya gelindiğinde ise çöktüğü bir tezdir. Vingean Yansıması da tekilliğe benzetilerek, tahmincilerin kafasında gerçek bir gelecek olayı değil, epistemik bir zorluk olduğu ifade edilmekteydi. Ancak bazı yazarlara göre Vingean Yansıması kavramsal açıdan hem geniş hem de önemli bir noktaya temas ettiğinden "Tekillik" teriminden koptuğu düşünülmektedir (Yudkowsky / Herreshoff, s.21 dn. 33.)

146 Vinge Vernor: The Coming Technological Singularity: How to Survive in the Post-Human Era, In Vision 21, Interdisciplinary Science and Engineering in the Era of Cyberspace, 11–22. NASA Conference Publication 10129. NASA Lewis Research Center, Y. 1993 (https://ntrs.nasa.gov/api/citations/19940022856/downloads/19940022856.pdf, E.T. 18.04.2023).

edilen teknik hipotezin ismidir. Bu hipotez, teknolojinin katlanarak büyümesi nedeniyle tarihin belirli bir noktasında, bu büyüklükle oluşturulan YZ'nin kapasite ve entelektüel güç açısından insanı aşacağını öne sürmektedir. Eğer bilişsel olarak insanlardan daha akıllı bir sistem inşa ediliyorsa (ya da bilişsel olarak daha üstün bir sürüm geliştiriliyorsa) o zaman tam olarak hangi çözümlerin üretileceği öngörülemeyecektir. Çünkü şu anda insanlık o kadar akla sahip değildir. Bu prensibin adı: Vingean Yansımasıdır[147].

İnsanların doğrudan süper zeki sistemler belirlemek yerine, aşamalı zeki sistemler belirleyerek her aşamanın bir sonraki aşamayı denetleyebileceği şekilde yazılım mimarisi inşa etmelidir. Bu durumda, ortaya çıkan süper zeki sistemin güvenilirliği, onu oluşturan ilk sistemin muhakemesine bağlı olup sürekli bu konuda kendisini geliştirmesi sağlanmalıdır[148].

Kendini geliştiren sistemin zaman geçtikçe daha zeki hale gelmesi beklenir. Bununla birlikte, eylemini seçmek için geriye doğru tümevarım kullanan bir sistemi, gelecekte karşılaşabileceği her durumda tüm eylemlerini ilk zaman adımında hesaplamak zorunda kalacaktır. Böyle bir sistemin, insan operatörlerini manipüle edebileceği bir durumda nasıl davranış sergileyeceği önemlidir. Ayrıca sistemin daha zeki halefinin davranışı hakkında nasıl akıl yürütebileceği de henüz çözüme kavuşmuş konulardan değildir[149].

E. SİBER GÜVENLİĞİN ETKİSİ

Günümüz dünyasında güçlü siber güvenlik önlemlerinin alınması hayati önem taşımaktadır. Sürekli gelişen tehditlerle mücadele etmek için siber güvenlik ağı gibi gelişmiş modellerin benimsenmesi gerekmektedir. Siber güvenlik ağı, ölçeklenebilir, esnek, birleştirilebilir, sağlam ve dayanıklı bir mimaridir ve güvenlik hizmetleri sağlamak için akıllı sistemler arasında birlikte çalışabilirlik ve koordinasyona olanak tanımaktadır. Bir siber güvenlik ağı tasarlamak, üç büyük zorlukla karşı karşıyadır: *ölçeklenebilirlik, dağıtılmış veya birleştirilmiş sistemler ve teknoloji entegrasyonu*. Milyonlarca verinin saklanması, işlenmesi ve analiz edilmesi nedeniyle tasarım için ölçeklenebilirliği destekleyen güvenlik araçlarının uygulanması gerekmektedir. Merkezi olmayan siber güvenlik ağlarının birlikte çalışabilirliğini

147 Yudkowsky / Herreshoff, s. 21

148 Soares / Fallenstein (Technical report 2014-8).

149 Soares Nate / Fallenstein Benja: Vingean Reflection: Reliable Reasoning for Self-Improving Agents, Machine Intelligence Research Institute, Technical report 2015-2.

geliştirmek için birleşik sistemlere ihtiyaç vardır. Ancak farklı güvenlik araçlarını ve iletişim protokollerini entegre etmek zor olabilmektedir. Birleşik öğrenme, sürü zekâsı ve blockchain teknolojileri gibi kriptografik algoritmalar ve YZ modelleri, güvenlik hizmetleri için faydalıdır[150].

Siber güvenlik araçlarının geliştirilmesi birçok uygulama alanı için temel önemdedir; örneğin, hem akıllı evler, otonom araçlar, nesnelerin interneti, akıllı şebekeler, güvenlik ağları, akıllı şehirler, finans, tedarik zinciri, eğitim ve güvenlik gibi sektörler hem de sağlık hizmetleri gibi en yeni sektörler siber güvenlikte önem arz etmektedir. Son zamanlarda siber güvenlik yalnızca kriptografik algoritmalarla değil aynı zamanda doğası gereği güvenlik hizmetleri sağlamayan diğer teknolojilerle de desteklenmektedir. Bu nedenle farklı teknolojilerin entegrasyonu, önümüzdeki yıllarda yeni siber güvenlik araçlarının geliştirilmesinde önemli bir alternatif olacaktır[151].

Siber güvenlik ağında teknolojilerin entegrasyon yönlerinin yeterliliğini değerlendirmek için YZ tabanlı test otomasyonu kullanılabilmektedir. YZ tabanlı test otomasyonu, siber güvenlik altyapısındaki çeşitli teknolojiler arasındaki gerçek dünya senaryolarını ve etkileşimlerini simüle edebilen dinamik bir araç olarak çalışmaktadır. Bu simülasyon odaklı değerlendirme, potansiyel güvenlik açıklarının tanımlanmasına, birlikte çalışabilirliğin doğrulanmasına ve entegrasyon protokollerinin optimizasyonuna olanak tanımaktadır. Bu yaklaşımı tamamlayacak şekilde, siber güvenlik riskini değerlendirmek için özellikle makine öğrenimi teknolojilerine dahil olduğunda risk değerlendirme araçlarını kullanabilmektedir[152].

YZ, doğal dil işleme, makine öğrenimi ve tahmine dayalı analitik yoluyla araştırmacıların ekosistem dinamiklerini daha iyi anlamalarını, ekosistem hizmetlerini tahmin etmelerini ve koruma çabalarını bilgilendirmelerini sağlamaktadır. YZ'nin siber güvenlikte çok yönlü rolleri vardır. Bunlar; *tehdit tespiti, güvenlik açığı değerlendirmesi, olay müdahalesi ve tahmine dayalı analiz* olmak üzere YZ sistemleri, makine öğrenimi algoritmalarından yararlanarak, potansiyel güvenlik ihlallerini gösteren anormal kalıpla-

150 Cruz Bruno Ramos / Perez Javier Andreu / Martínez Luis: The cybersecurity mesh: A comprehensive survey of involved artificial intelligence methods, cryptographic protocols and challenges for future research, Neurocomputing, Vol. 581, Y. 2024 (https://www.sciencedirect.com/science/article/pii/S092523122400198X, E.T. 11.03.2024).

151 Cruz / Perez / Martínez.

152 Cruz / Perez / Martínez.

rı belirlemek için çok sayıda veriyi hızlı bir şekilde analiz edebilmektedir. Aynı zamanda YZ destekli siber güvenlik sağlayıcılar, proaktif savunma mekanizmalarını mümkün kılarak kuruluşların riskleri önleyici bir şekilde azaltmalarına ve hassas bilgileri korumalarına olanak tanımaktadır. Bu sebeple dijital çağdaki tehditleri etkili bir şekilde azaltmak için YZ'yi siber güvenlik çerçevelerine entegre edilmesi gerekmektedir[153].

Kurumsal siber güvenlik mimarisi, devletin ya da özel şirketlerin hedefli siber saldırılara ve sürekli gelişen tehdit ortamına karşı savunmalarını güçlendirmeleri için kapsamlı bir plan olarak hizmet etmektedir. Bu çerçeve, kurumsal bir siber güvenlik programının tüm yönlerini yönetmek, bilgi ve rehberlik sağlamak, bilgi işlem teknolojileri politikası, teknoloji, bilgi işlem teknolojileri yaşam döngüsü ve değerlendirme protokolleriyle sorunsuz bir şekilde uyumlu bir siber güvenlik stratejisi tasarlamalarını, uygulamalarını ve işletmelerini sağlayarak katmanlı korumalar oluşturmaktadır[154].

Kurumsal siber güvenlik mimarisinin stratejilerini gerçekleştiren devlet ve özel şirketlerin, siber savunmaları güçlenir, ortak hareket etme mekanizması oluşur, risk azalır ve ortaya çıkan tehditlere proaktif olarak yanıt verebilme imkânı gelişir. Her büyüklükteki kuruluşun kritik varlıkları koruyan ve genel iş hedeflerini destekleyen sağlam bir siber güvenlik programı oluşturmasını sağlar. Ayrıca kuruluşlar, olası güvenlik ihlallerini tespit etmek ve bunlara anında müdahale etmek için IoT ortamları için özel olarak tasarlanmış kapsamlı izleme ve saldırı tespit sistemlerine yatırım yapmalıdır. Güvenlik protokollerinin standartlaştırılması ve sektör genelinde en iyi uygulamaların hayata geçirilmesi, IoT ekosistemlerinin siber tehditlere karşı dayanıklılığını artırabilir. Sonuç olarak, IoT güvenlik açıklarının ele alınması kritik altyapının korunması, hassas verilerin korunması ve dijital ekosisteme olan güvenin sürdürülmesi için zorunludur[155].

---

153 Camacho Nicolas Guzman, The Role of AI in Cybersecurity: Addressing Threats in the Digital Age, Journal of Artificial Intelligence General Science (JAIGS), ISSN: 3006-4023 (Online), Vol. 3, Y. 2024, s. 143,151 (https://ojs.boulibrary.com/index.php/JAIGS/ article/view/75/46, E. T. 22.05.2024)

154 Camacho, s. 148, 149

155 Camacho, s. 149, 150

F. NESNELERİN VE DAVRANIŞLARIN İNTERNETİNİN ETKİLERİ

1. Nesnelerin İnterneti (IoT)

Nesnelerin interneti (IoT), internet üzerinden veri toplayıp alışveriş yapmalarını sağlayan sensörler, yazılımlar ve bağlantı yetenekleriyle donatılmış fiziksel nesnelerden oluşan ağı ifade etmektedir. Bu nesneler ev aletleri, araçlar, giyilebilir cihazlar veya endüstriyel ekipmanlar gibi günlük cihazlar olabilir. IoT, bu nesneleri birbirine bağlayarak ve onların iletişim kurmasını ve veri paylaşmasını sağlayarak, bilgi toplayıp analiz ederek, süreçleri otomatikleştirebilen ve insanlar ile makineler arasındaki iletişimi kolaylaştırabilen, birbirine bağlı cihazlardan oluşan geniş bir ağ oluşturur[156].

IoT ile veriler, insandan insana veya insandan bilgisayara, etkileşim gerektirmeden bir ağ üzerinden aktarılabilir. IoT cihazları, veri gönderebileceği merkez görevi gören bir IoT ağ geçidine bağlanarak topladıkları sensör verilerini paylaşmaktadır. Veriler paylaşılmadan önce, bu verilerin yerel olarak analiz edildiği bir uç cihaza da gönderilebilir. Verilerin yerel olarak analiz edilmesi, buluta gönderilen veri hacmini azaltarak bant genişliği tüketimini en aza indirir[157]. IoT verileri, bağlı cihazlarda bulunan sensörlerden toplanan bilgilerle ilgilidir. Ancak buluttaki IoT verilerinin iki ana zorluğu vardır. İlk zorluk, verilerin hızlı büyümesi, ikincisi ise IoT'nin veri güvenliği eksikliğidir[158].

Özellikle güvenlik açısından zorluk konusunda, IoT cihazları yakından bağlantılı olduğundan, güvenlik açığından yararlanılarak tüm veriler manipüle edilebilir, kullanılamaz hale getirebilir[159], kötü niyetli kişilerin eline geçebilir.

---

156 Chhetri Parbat: Internet of Things in Libraries: *A SWOT Analysis*, Library and Information Science Links Newsletter, Vol. 6, Y. 2020, s. 11 (http://file.lislinks.com/newsletter/lislinks-newsletter-vol-6-no-1-p-10-17.pdf, E.T. 18.04.2024).

157 Gillis Alexander S.: Internet of Things (IoT) (https://www.techtarget.com/iotagenda/definition/Internet-of-Things-IoT, E.T: 11.02.2024).

158 Jun Yao / Craig Alisa / Shafik Wasswa / Sharif Lule: Artificial Intelligence Application in Cybersecurity and Cyberdefense, (ed. Lv Zhihan), Hindawi, Vol. 2021, Y. 2021 (https://doi.org/10.1155/2021/3329581, E.T. 18.04.2024).

159 Gillis.

Varlık ile ikizi arasındaki fiziksel bağlantılar çoğunlukla IoT sensörleridir ve iyi yapılandırılmış bir IoT uygulaması genellikle dijital ikizler için bir ön koşuldur[160]. Örneğin, IoT ve 5G'nin sağlık izleme sistemlerine entegrasyonu durumunda, sağlık hizmeti sunumunu da büyük ölçüde değiştirecektir. IoT ile birlikte 5G ağları yaygınlaştıkça, ultra düşük gecikme süresi ve yüksek bant genişliği özellikleri, uzaktan ameliyatlar, teletıp[161] ve hatta robotik cerrahi için gerekli olan kesintisiz gerçek zamanlı veri iletimi mümkün olabilecektir. Giyilebilir IoT cihazlarının evrimi, sürekli izleme ve erken müdahale ile önleyici sağlık hizmetlerinin gelişebileceği öngörülmektedir. Bunların yanı sıra, gelişmiş analitik ve YZ ile birleşen gerçek zamanlı birçok hasta verilerinin var olması karşısında kesin teşhis ve tedavi planlarına da etki göstererek kişiselleştirilmiş tıbbın gelişim kaydedebileceği değerlendirilmektedir. Kronik hastalık yönetimi sayesinde, uzaktan hasta izlemenin geliştirilebileceği, hastaneye yatış oranları ve sağlık hizmeti maliyetlerinin de azaltılabileceği değerlendirilmektedir. Ayrıca, öngörücü algoritmalar bireysel yaşam tarzı ve genetik faktörlere dayalı potansiyel sağlık risklerini belirlediğinden, önleyici sağlık hizmetleri hız kazanacaktır. Bu değişimlerle birlikte farklı zorlukların da ortaya çıkabileceği ifade edilmektedir: *veri mahremiyeti, rıza ve algoritmik ön yargıları çevreleyen etik sorunlar*. IoT ile 5G teknolojisine bağlı olarak gelişen veya gelişecek inovasyonun teşvik edilmesi yanında hasta haklarının da korunması önemlidir[162].

Bu çerçevede IoT sistemlerinin standardizasyonu gündeme gelebilecektir. Standartlaştırılmış veri formatları oluşturmaya teşvik edilmesi gerekmektedir. Standartlaştırılmış formatlarda veri alışverişi kullanımına dikkat edilmemektedir[163]. Bu sebeple çeşitli standartları da dikkate alarak, regü-

---

160 Gillis.

161 Teletıp, dijital röntgenlerden telefonla yapılan konsültasyonlara, video konferansın kullanılmasından uzaktan cerrahinin yapılmasına kadar bir dizi teknolojiyi içeren geniş bir terimdir. Başka bir deyişle, tıbbi bakım veya hizmetlerin sağlanması için telekomünikasyon teknolojisinin kullanılmasıdır. (Dilbaz Berna / Kaplanoğlu Mustafa / Kaya Kaplanoğlu Dilek: Teletıp ve Telesağlık: Geçmiş, Bugün ve Gelecek, Eurasian Journal of Health Technology Assessment, S. 4 (1), Y. 2020, s. 42)

162 Singh Bhupinder / Kaunert Christian: Integration of Cutting-Edge Technologies such as Internet of Things (IoT) and 5G in Health Monitoring Systems: A Comprehensive Legal Analysis and Futuristic Outcomes, GLS Law Journal, Vol. 06, Y. 2024, s. 19, 20 (https:// glslawjournal.in/index.php/glslawjournal/article/view/123/109, E.T. 17.04.2024)

163 Turner Sarah / Tanczer Leonie Maria: In principle vs in practice: User, expert and policymaker attitudes towards the right to data portability in the internet of things, Computer Law & Security Review, Volume 52, 2024 (https://doi.org/10.1016/j.clsr.2023.105912, E.T. 18.04.2024).

lasyon kurumlarının, sağlıkta ve IoT kapsamında değişim gösterecek sektörlerin bu ve benzeri konuları tartışması ve buna yönelik yasal düzenlemeleri hayata geçirmesi önem arz etmektedir.

2. Davranışların İnterneti (IoB)

Nesnelerin İnterneti'nin (IoT) halefi olan *davranışların interneti* (IoB), teknoloji, veri analizi ve insan psikolojisinin kesiştiği noktada gelişen bir alan olarak değerlendirilmektedir. Davranış kalıplarını ortaya çıkarma amacıyla giyilebilir cihazlardan, dijital ayak izlerinden ve çevrimiçi etkileşimlerden veri toplamaya ve analiz etmeye odaklanmaktadır. IoB'nin sağlık, pazarlama, eğitim ve finans da dahil olmak üzere birçok uygulama alanında büyük bir potansiyele sahip olduğunu düşünülmektedir[164].

IoB, rakiplerle fark yaratacağı ve ticari müşteri davranışına odaklandığı için taklit edilmesinin zor olduğu işletmeler için teknolojiyi uygulama stratejilerinden biridir. IoB, teknoloji, davranış bilimi ve veri analitiği bilimi olmak üzere üç bilim alanının birleşimi olarak kabul edilmektedir. IoB, e-ticaret platformları için önemli bir değere sahiptir. Müşteri kazanımını geliştirmek ve marka bilinirliğini artırmak için tüm e-ticaret platformlarının IoB sisteminin uygulanmasına öncelik vermesi beklenmektedir. IoB, kamu veya özel şirketler tarafından birçok şekilde kullanılabilir. IoB platformu, verilerin nasıl daha iyi anlaşıldığını ve yeni ürünler oluşturmak ve tanıtmak için insan psikolojisi perspektifinden nasıl kullanıldığını ele almayı amaçlamaktadır[165].

---

[164] Romeo Nzanzu Katasohire / Mahangue Edson Bernardo C. / Cossa Aderito Eduardo / Kaur Mandeep / Goyal Mayank Kumar / Chhabra Megha, "Transforming Data into Behavioral Insights: A Review of the Internet of Behavior (IoB)", 2024 11th International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 2024, s. 70-75 (10.23919/INDIACom61295.2024.10498875, E.T. 22.05.2024)

[165] Wijaya Eric / Christian Jonathan / Venna Carla / Rowan Jennie / Surachman Ivan / Sellyna / Oktavia Tanty: Examining The Efficacy Of The Internet Of Behaviour (IoB) In The Identifi-cation Of Client Needs On Electronic Commerce Platforms, Journal of Theoretical and App-lied Information Technology, Vol. 102, Y. 2024, s. 3451-3461

G. ÇOK DUYULU GENİŞLETİLMİŞ GERÇEKLİK (XR) UYGULAMALARININ VE DİJİTAL İKİZİN ETKİLERİ

1. Çok Duyusal Genişletilmiş Gerçeklik (XR) Uygulamaları (Multi - Sensory Extended Reality (XR) Applications)

Artırılmış gerçeklik (AR), karma gerçeklik (MR) ve sanal gerçeklik (VR), ultra güvenilir ve düşük gecikmeli iletişim (UGDİ) hizmetlerinin kullanım durumları ve her şeyin interneti (IoE) uygulamalarının bir parçası olarak kabul edilir. Yakın zamanda XR olarak yeni bir şemsiye terim altında yer alan mevcut AR/MR/VR uygulamaları, dokunsal internet teknolojisinden büyük ölçüde faydalanmaktadır. AR/MR/VR uygulamaları, yüksek veri hızı ve son derece düşük gecikme gerektirmektedir. Dokunsal internetin son derece düşük bir gecikme gereksinimi sağlaması ve gerçek zamanlı etkileşimle paylaşılan sanal ortamlara izin vermesi beklenmektedir. XR, gerçek ve sanal ortamları birleştirme potansiyeline sahiptir. Bu tür uygulamalar, gerçeklik deneyimine sahip bilgisayar simülasyonlu bir platform kullanmaktadır ve gerçek dünyaya tamamen benzeyen bir sanal dünya inşa etmektedir. XR teknolojileri için etkileşimli bir ortam oluşturmak amacıyla seslerden, videolardan ve küresel konumlandırma sisteminden (GPS) yararlanmaktadır. XR, gelecekteki 6G ağlarının temel uygulamalarından biri olarak kabul edilmektedir. XR, kullanıcıların oyun oynama, resim yapma, eğitim verme, spor yapma ve konserlere katılma gibi konularda sanal olarak etkileşime girmesini ve etkileşimde bulunmasını sağlamaktadır. XR aynı zamanda kullanıcının görüş alanının etkileşimli olarak genişletilmesine de olanak tanıyarak zararlı olayların önlenmesini mümkün kılabilecektir[166].

XR Uygulamaları sanal olarak deneyimlerin gerçekleştirilebileceği düşünüldüğünde oyun sektörü dışında e-ticaret ve eğitim başta olmak üzere daha birçok sektörün etkilenebileceği beklenmektedir. Bu çerçevede söz konusu teknolojinin YZ yönetişimine etkisi de büyük olacaktır. Regülasyonların hazırlığında, XR uygulamalarının dikkate alınması ve bu çerçevede gerçek kişilere veya tüzel kişilere karşı oluşabilecek maddi ve manevi

166 Alsabah Muntadher / Naser Marwah Abdulrazzaq / Mahmmod Basheera M. / Abdulhussain Sadiq H. / Eissa Mohammad R. / Baidhani Ahmed Al / Noordin Nor K. / Sait Sadiq M. / Utaibi Khaled A. Al / Hashim Fazirul: 6G Wireless Communications Networks: A Comprehensive Survey, IEEE Access, Vol. 9, Y. 2021 (https://ieeexplore.ieee.org/document/ 9598915, E.T. 18.04.2024).

zararların önüne geçilmesi amacıyla yasal çerçevelerinin oluşturulması gerekmektedir.

2. Dijital İkiz

Dijital ikiz, fiziksel nesnelerin özelliklerini, davranışlarını, oluşum sürecini ve performansını dijital teknolojiyi kullanarak tanımlamaya ve modellemeye yönelik süreç ve yöntemleri ifade etmektedir. Dijital ikiz, akıllı üretim sisteminin temeli olup en önemli işlevi, fiziksel sistemden siber uzayın dijital modeline geri bildirimi gerçekleştirmesidir[167].

Endüstri 5.0, endüstriyel sürdürülebilirliği, insan odaklılığı ve dayanıklılığı geliştirmeyi amaçlamaktadır. Endüstri 4.0, üretim süreci verimliliğini ve kârlılığı artırmak için ileri dijital teknolojilerin (otomasyon, büyük veri ve YZ gibi) entegrasyonu yoluyla teknoloji odaklı endüstriyel değişimlerini vurgularken, Endüstri 5.0 insan katılımına ve yaratıcılığa daha güçlü bir vurgu yapmaktadır. Endüstri 5.0, insan - makine etkileşimi, dijital ikizler ve simülasyon, büyük veri analitiği ve yenilenebilir enerji teknolojilerindeki gelişmeler yoluyla insanın katılımını vurgulamaktadır. Bu yaklaşım, Endüstri 4.0'a kıyasla daha dengeli ve sürdürülebilir bir üretim modeli elde etmek için insan bilgeliğini makine zekâsıyla sinerjiye kavuşturmayı amaçlamaktadır. Endüstri 5.0'ın temel amacı, yalnızca kârlılığı sağlamakla kalmayıp aynı zamanda çevresel etkiyi ve çalışanların refahını da ön planda tutan bir üretim oluşturmaktır. Endüstri 4.0'ın aksine, Endüstri 5.0, insan - makine iş birliğinin desteklenmesine daha fazla vurgu yapmakta ve temel ilkelerinde sürdürülebilirliğe öncelik vermektedir[168].

Endüstri 5.0'ın temel özelliklerinden birisi, insanlar ve makineler arasındaki kusursuz iş birliğini kolaylaştırmak için dijital ikiz teknolojisinin kullanılmasıdır. Bu teknoloji, karar alma ve yenilik süreçlerine artan insan katılımının teşvik edilmesinde önemli bir rol oynamaktadır. Ayrıca Endüstri 5.0, uyarlanabilir üretim süreçlerini teşvik eder ve kaynak israfını en aza indirmek için kişiselleştirilmiş üretimi savunmaktadır[169].

---

167 Wang Zongyan: *Digital Twin Technology*, IntechOpen, Y. 2020 (https://www.intechopen.com/chapters/63861 E.T. 12.02.2024)

168 Fuli Zhou / Kangzhen Yu / Wei Xie / Jieyin Lyu / Zhong Zheng / Shouqın Zhou: *Digital Twin-Enabled Smart Maritime Logistics Management in the Context of Industry 5.0,* IEEE Access, Vol. 12, Y. 2024, (https://ieeexplore.ieee.org/document/10401169, E.T. 12.02.2024).

169 Fuli vd.

Endüstri 5.0, ekolojik, sosyal ve ekonomik sürdürülebilirlik hususlarını kapsamlı bir şekilde ele alarak daha bütünsel bir yaklaşımı benimsemektedir. Bu, ürün yaşam döngülerinin titizlikle yönetilmesi, paylaşım ekonomisi modelinin teşvik edilmesi ve kurumsal sosyal iş birliğinin teşvik edilmesi yoluyla elde edilebilecektir. İmalat sanayi bu girişimlerle daha dengeli ve sürdürülebilir bir döneme geçiş yapmaktadır[170].

Dijital ikiz ile nesnelerin interneti'nin derin entegrasyonu son yıllarda büyük ilgi görmüştür. Sensörleri ve fiziksel sistemleri dijital ikiz platformuna bağlayarak gerçek zamanlı veri toplama, izleme ve simülasyon elde edilmektedir[171]. Bu sayede imalat sektörünün yanı sıra hizmet, sağlık, kişisel gelişim ve eğitim sektörlerinin de dijital ikiz kapsamında dönüşeceği değerlendirilmektedir. Bu nedenle YZ sistemleri içerisinde yer alan XR uygulamaları ile dijital ikizin regülasyonlarda yer alması gerekli teknolojilerdir. Bu teknolojilerin standardizasyonunun gerçekleştirilmesi önem arz etmektedir.

H. KUANTUM BİLGİSAYAR SİSTEMLERİNİN ETKİLERİ

Kuantum bilgisayar, bilgiyi işleme şekli farklı olan karmaşık bir sistemdir. Verileri 0 veya 1 olarak temsil etmek için bitleri kullanan klasik bilgisayarların aksine, kuantum bilgisayarlar aynı anda birden fazla durumda bulunabilen kuantum bitlerini veya kübitleri kullanır. Kuantum hesaplamanın merkezinde iki temel ilke vardır: süperpozisyon ve dolanıklık. Süperpozisyon, kübitlerin aynı anda hem 0 hem de 1 durumunda olmalarını sağlayarak hesaplama gücünü önemli ölçüde artırmaktadır. Dolanıklık ise kübitlerin uzak mesafelerde bile birbirine bağlanabilmesini sağlar[172].

Kuantum bilgisayarlar hesaplama yapmak için süperpozisyon ve dolanıklıktan yararlanan algoritmalar kullanmaktadır. Bu algoritmalar kübitleri döndürme ve kontrollü kapılar gibi işlemlerle manipüle ederek klasik sistemlerin hızını çok aşan hesaplamalara olanak tanımaktadır. Geleneksel bilgisayarlar karmaşık şifreleme algoritmalarıyla mücadele ederken, kuantum bilgisayarlar mevcut kriptografik sistemleri potansiyel olarak ortadan

170 Fuli vd.

171 Fuli vd.

172 Jowarder Rafiul Azim, Sawgat Jahan: Quantum computing in cyber security: Emerging threats, mitigation strategies, and future implications for data protection, World Journal of Advanced Engineering Technology and Sciences, C. 13(01), Y. 2024, s. 330–331

kaldırabilecek benzersiz bir işlem gücüne sahiptir. Kuantum bilişimdeki önemli bir ilerleme, kuantum mekaniğinin süperpozisyon ve dolanıklık gibi özelliklerinden yararlanma yeteneğinden kaynaklanmaktadır. Bu özellikler, kübitlerin aynı anda birden fazla durumu temsil etmesine olanak tanıyarak hesaplama yeteneklerini büyük ölçüde artırmaktadır. Sonuç olarak, klasik bilgisayarların yüzyıllar sürebileceği görevler kuantum bilgisayar tarafından sadece saniyeler veya dakikalar içinde tamamlanabilir. Bu nedenle açık anahtarlı kriptografi standartları risk altında kalacaktır. Bu güvenlik açığının potansiyel sonuçları önemlidir[173].

Kuantuma karşı siber savunma amacıyla kuantum sonrası kriptografik veya kuantum dirençli kriptografi adı verilen yeni şifreleme yöntemleri araştırılmaktadır. Bu teknikler klasik ve gelecekteki kuantum bilgisayarlardan gelebilecek saldırılara dayanabilecek algoritmaları oluşturmayı amaçlamaktadır. Amerika Birleşik Devletleri kuruluşu olan National Institute Of Standards And Technology (NIST)'in Kuantum Sonrası Kriptografi Standardizasyon Süreci gibi kuantum güvenli şifreleme yöntemlerine yönelik standartlar getirilmeye çalışılmaktadır[174].

YZ'nin çağı olarak kabul edilen bu on yıllarda, artık teknolojide YZ'nin yerinin daha fazla olacağı ve hızın da öneminin artacağı görülmektedir. 5G ve sonrasında geleceği tasarlanan 6G hücresel ağ ile kuantum bilgisayar sistemlerinin internet alanında getireceği hız ve olanakların küresel ölçüde birçok yeniliğin doğmasına zemin hazırlayacağı öngörülmektedir. Bu kapsamda kuantum bilgisayar sistemlerinin YZ ekosisteminde küresel ölçekte önümüzdeki 5 yıldaki üç ana teması olacaktır:

Birincisi, çözülmesi zor olan görevlerde klasik bilgisayarların yerine kuantum bilgisayarın yer alması,

İkincisi, bilimsel araştırmalarda ve ticari alanlarında sorunları tespit etmek için kuantum bilgisayarlardan yararlanılması,

Üçüncüsü ise bütün hatalara dayanıklı bir kuantum bilgisayarın geliştirilmesidir.

---

173 Jowarder, Sawgat, s. 331

174 Jowarder, Sawgat, s. 331; ABD (2024) National Institute Of Standards And Technology: Post-Quantum Cryptography, (https://csrc.nist.gov/projects/post-quantum-cryptography, E.T. 01.12.2024)

Bu temaların her biri araştırma, sistem mühendisliği ve ekosistem inşası için çok fazla yatırım gerektirmektedir. Dünyada birçok devlet bu konuda yatırama teşvik vermektedir[175].

Kuantum bilgisayarlar, sistem güvenliği için kriptografik açıdan büyük önemi haizdir[176]. Bu çerçevede kuantum güvenli kriptografi standartlarının gelişeceği öngörülmektedir. Bu nedenle ulusal çalışmalarda kuantum güvenli kriptografi standartlarının belirlenmesi kayda değer olacaktır. YZ çağında yönetişim ve metodoloji belirlemek için öncelikle kuantum sistemlerine sahip olmak gerekecektir. Zira özellikle üzerinde durulan husus güvenlik sistemlerinin inşası olarak karşımıza çıkmaktadır. Bu durum hem kamu kurumlarını hem de ticari teşebbüsleri ilgilendirmektedir. Sadece devletlerin politikası çerçevesinde gelişebilecek bir potansiyel değildir. Ancak kuantum bilgisayarlardan faydalanmak amacıyla ayrıca strateji geliştirilmeli ve uygulanmalıdır. Bu strateji YZ stratejisinden tamamen farklıdır. Gelişmiş hesaplama yetenekleri kazandırılacak bir sistemin kapsamlı bir araştırma ekibine ve merkeze ihtiyacı olacaktır. Kuantum bilgisayar sistemlerinin pahalı sistemler oluşundan dolayı daha az kaynak gerektiren kuantum sistemlerinin ve kriptografik olarak kuantum algoritmalarının araştırılması da gelecek için önemlidir. Burada hem destek hem ticari gelişim hem de araştırma olanaklarının üst düzey yürütülmesi açısından, devletler, şirketler ve akademinin birlikte hareket etmesi gelişime katkı sağlayacaktır. Bunların yanında akademik araştırmacılara donanım yeniliklerine, yeni algoritmalara, hata düzeltme konusunda yeni yaklaşımlara, yeni mimari konseptlere ihtiyaç olacaktır. Bu nedenle hem iş gücünü eğiten hem de endüstri tarafından yeni konseptler üretilmesini sağlayacak araştırmalara destek verilmelidir. Kuantum bilişim ve kuantum güvenli kriptografi konusundaki savunma ve eğitim çalışmaları gerçekleştirilmelidir[177]. Devletlerin bu ekosistemi gerçekleştirmede rolü büyüktür. Amerika Birleşik Devletleri tarafından yayımlanan[178] *Savunmasız Kriptog-*

---

175 Scholten Travis L. / Williams Carl J. / Moody Dustin / Mosca Michele / Hurley William "whurley" / Zeng William J. / Troyer Matthias / Gambetta Jay M.: Assessing the Benefits and Risks of Quantum Computers, Cornell University arXiv, Y. 2024, (https://arxiv.org/pdf/2401.16317.pdf, E.T. 14.02.2024)

176 Scholten vd: Bu tür kriptosistemler oluşturmak için çeşitli yaklaşımlar mevcuttur: kuantum anahtar dağıtımı, kuantum rastgele sayı üretimi ve tamamen klasik kuantum sonrası kriptografi.

177 Scholten vd.

178 ABD (2022), National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems (https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/, E.T. 14.02.2024).

rafik Sistemlere Yönelik Riskleri Azaltırken Kuantum Bilişimde Amerika Birleşik Devletleri Liderliğini Teşvik Etmeye İlişkin Ulusal Güvenlik Memorandumu (Ulusal Güvenlik Memorandumu - 10) bu çerçevede önemli örneklerdendir. Söz konusu Memorandum, devletin tüm organlarına kriptografik sistemlere yönelik risklerin azaltılması ve kuantum bilişime yönelik yükümlülükler yüklemektedir. Memorandum, ayrıca yurt dışında kuantum ile çalışan kişilerin ABD'ye gelmesine yönelik teşvikleri ele alan ve tüm bu yükümlülüklere de süre takip mekanizması öngören bir kuantum stratejisidir. Devletin tüm organlarının kriptografik sistemleri ile birlikte çalışabilen kuantum dirençli kriptografiye geçişi öngörülmektedir. Bunun nedeni ise mevcut açık anahtarlı şifreleme algoritmalarını zayıflatma kapasitesine sahip kuantum bilgisayarı tehdididir[179].

Bilişimi dönüştürecek bir teknoloji olan kuantum bilgisayarları araştırmaya, geliştirmeye ve uygulamaya devam etmek ve kuantum güvenli kriptografik protokollerini süratle uygulamak çok önemlidir. Zira kuantum sistemleri, uygulamaları ve riskleri ile birlikte YZ'yi, siber güvenliği ve kriptografik sistemleri dönüştüreceği düşünülmektedir[180].

I. 5G VE 6G HÜCRESEL AĞLARIN ETKİLERİ

Yeni nesil altıncı nesil hücresel ağ (6G), mevcut beşinci nesil (5G) ağların teknolojik olarak çok üzerinde bir ağ olacağı düşünülmektedir. Mevcut ağın dahi henüz birçok ülkede yaygınlaşmadığı düşünülecek olursa 6G hücresel ağ sistemlerinin de yaygınlaşması için zamana ihtiyaç olacaktır. Ancak şu anda akademi ve endüstrinin, dikkatlerini telekom endüstrisinde bir sonraki büyük oyun değiştirici olması beklenen 6G ağına odaklandığı ifade edilmektedir. Bilindiği üzere COVİD'19'un ortaya çıkması, tüm dünyada, birçok sektörde gerçek toplantı veya eğitim yerine sanal toplantının ve canlı video etkileşimin tercih edilmesine neden oldu. Bu kapsamda deneyimler elde edilmesi ile hücresel ağların etkinliğinin birçok alanda sorgulandığı ifade edilmektedir. Pandemi sonrası önümüzdeki yıllarda sanal ve gerçek zamanlı iletişimin öneminin daha çok artacağı ve teknolojinin performans gereksinimlerine ihtiyaç olacağı değerlendirilmektedir. Bunun sonucunda endüstriyel otomasyon, robotik ve otonom sürüş gibi çeşitli sektörlerin yükselişini de doğrudan etkileyeceği öngörülmektedir. Dijital, fiziksel ve biyolojik alanlardan oluşan 6G'yi mümkün kılan teknolojiler; YZ,

[179] ABD (National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems)

[180] Scholten vd.

THz haberleşme spektrumu[181], her yerde 3D iletişim[182], görünür ışık iletişimi (Visible Light Communication - VLC)[183], blockchain güvenliği, kuantum iletişimi, dijital ikizler. Söz konusu teknolojilerin yanı sıra, bilgiyi yerelleştirilerek tüm alanlara yaygınlaştırılması amaçlanmaktadır. Bu çerçevede robotik cerrahi, salgın sırasında temas takibi, XR tabanlı oyunlar, sosyal ağ uygulamaları, yemek dağıtımı, bağlama duyarlı pazarlama, otonom sürüş, kişisel navigasyon ve hayvan takibi dahil olmak üzere birçok uygulamanın önem kazanacağı vurgulanmaktadır[184].

5G ağları sayesinde dijitalleşme artarak eğitim, çevrenin korunması ve açlık gibi birçok sosyal meselede çözümlerin bağlantı noktası haline gelmiştir. Bununla birlikte, kapsamlı kentleşme ve bağlantı gerektiren çeşitli sorunları da beraberinde getirmiştir. 6G ağları kullanıcı deneyimine dayalı hiper veri bağlantısı sağlayacağından, özellikle Birleşmiş Milletler'in Sür-

---

181 THz frekanslarında daha geniş bant genişliğinin bulunması, yüksek veri hızını mümkün kılmaktadır. Bu durum da yüksek frekanslı iletişim devrenin (cihazın) minyatürleştirilmesini sağlamaktadır. Sonuç olarak, kullanıcı cihazlarına bir dizi anten yerleştirilebilir. Bu, iletişim kalitesini artırmak için etkili çok antenli MIMO şemalarının, hüzme oluşturmanın ve parazit bastırmanın kullanımını kolaylaştıracaktır. Ayrıca, bu yüksek frekanslı sinyaller görüş hattını (LoS) takip edecek ve oldukça yönlü olacak, bu da parazite karşı daha az duyarlı olmalarını sağlayacak ve güvenli iletişimi sağlayacaktır (Bhat Jagadeesha R. / Alqahtani Salman A.: 6G Ecosystem: *Current Status and Future Perspective*, IEEE Access, Vol. 9, Y. 2021, s. 43134-43167 (https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9335927, E.T. 18.04.2024).

182 6G ağlarının önemli gereksinimlerinden biri, önceki nesillerden farklı olarak, geniş bir dikey aralıkta arttırılmış uyumu sağlamak için yüksek irtifa, su altı ve kara bağlantısı gibi çok yönlü küresel bağlantıya sahip olacaktır. Bu kapsamda 6G ağları, insanlar ile akıllı nesneler, su altı araçları, İHA'lar veya uzay araçları gibi makine-makineler ve robotlar arasında genişletilmiş ve sürekli iletişim sağlamayı amaçlamaktadır. 2030 yılında karasal, uçak ve uydular ile gemiler arasındaki iletişim daha üst düzey hale gelecektir (Bhat / Alqahtani, s. 43134-43167).

183 Yoğun 6G ağlarında, büyük miktarda veri üretimi nedeniyle ana taşıyıcıda verileri yönetmek için çok yüksek bant genişliği teknolojisi zorunlu olacaktır. Daha önceki telekomünikasyon ağlarında, baz istasyonu ile mobil anahtarlama merkezleri arasındaki bağlantı ya mikrodalga (RF) ya da fiber optik bağlantılardı (RF olmayan). Ancak 4G'den bu yana, basitliği, lisanssız çalışması, yüksek veri hızları ve güvenliği nedeniyle ana taşıyıcıyı bağlamak için serbest alan optik (FSO) bağlantıları önem kazanmaya başladı. Serbest alan optik iletişimi (FSO), telekomünikasyon veya bilgisayar ağları için verileri kablosuz olarak iletmek üzere boş alanda yayılan ışığı kullanan bir optik iletişim teknolojisidir. Bu bağlamda VLC ve THz iletişimleri, fiziksel katmanda 6G hücresel iletişim için iki ana aday olacaktır (Bhat / Alqahtani, s. 43134-43167).

184 Bhat / Alqahtani, s. 43134-43167

dürülebilir Kalkınma Hedefleri[185] ile ilgili birçok küresel sorunu hafifletilmesinde katkı sağlayacağı değerlendirilmektedir. 6G ağı, çok yönlü iletişim yeteneği (uzun ve kısa menzilli, 3D bağlantı) ve kesintisiz bağlantı ve çok sayıda hizmet desteği sayesinde küresel sürdürülebilirliği teşvik etme potansiyeline sahiptir. Sürdürülebilir kalkınma hedeflerinin desteklenmesiyle ilgili olarak 6G ağlarının gelecekteki kapsamlarından bazıları ise şunlardır; *çevrim içi bankacılık,* herkesin finansal hizmetlere kolaylıkla erişmesini sağlayacak ve bu da yoksulluğun ortadan kaldırılmasına yardımcı olacaktır. *Çevrim içi sağlık hizmetleri* de seyahat süresini azaltacak ve daha iyi sağlık hizmeti sunumunu teşvik etmek için gerektiğinde ihtiyaç sahiplerine kolayca ulaşabilecek. *Kırsal bölgelerdeki çiftçiler*, çok yönlü ağ bağlantısına sahip olarak tarım ve ev aletleri için dijital işlemlerden yararlanabileceklerdir.

Verimi artırmak ve açlığı ortadan kaldırmak için gıda üretiminde IoT sistemleri uygulanabilecektir. Veri bağlantısı, güçlü bir ekonomi, akıllı sağlık hizmetlerini kolaylaştırma ve enerji verimliliğini de içeren 17 farklı Sürdürülebilir Kalkınma Hedefi'nden sadece bazılarıdır. 6G ile birlikte Sürdürülebilir Kalkınma Hedefleri ekosisteminde, insanların ve toplumun sorunlarını, onları güçlendirecek uygun dijital altyapıyı sağlayarak ele almak, son derece hassas yerelleştirme ve algılama yeteneklerini sağlamak, kaynakların çevrimiçi izlenmesi vb. ile mümkün olan çevre farkındalığını geliştirmek hedefleri yer almaktadır. Bu gereksinimlerin yanı sıra hedefe ulaşmak için temel gereksinim, çok yönlü bağlantı ve internete erişimin sağlanmasıdır. 6G ağlarının yardımıyla tüm bu sorunların küresel ölçekte büyük kısmının çözülmesine yardımcı olabileceği değerlendirilmektedir[186].

Sonuç olarak 6G, bu gereksinimler arasında en iyi dengeyi sağlamayı amaçlamaktadır. 6G ağlarının bu devasa hizmet sınıfları, her yerde mobil ultra geniş bant, düşük gecikmeli ultra yüksek hızlı iletişim ve ultra yüksek veri yoğunluğunu sağlayacaktır. Ortaya çıkan bu hizmetler neticesinde, 5G ağlarında çoğunlukla bulunmayan iletişim, kontrol, algılama ve bilgi işlem özelliklerinin yeni ortak tasarımını gerektirecektir. Bu haliyle 6G, gelecekteki bu gereksinimleri tam olarak desteklemeyi amaçlamaktadır. 6G ağlarının, her yerde muazzam bağlantıya izin verecek şekilde gelişmesi, farklı teknolojilerin ve uygulamaların entegrasyonu, YZ'nin etkinleştirilmesi ile büyük merkezi olmayan hesaplama işlemlerinin gerçekleştirilmesi bek-

[185] Birleşmiş Milletler: Sürdürülebilir Kalkınma Araçları (https://turkiye.un.org/tr/sdgs/1, E.T. 14.04.2024)

[186] Bhat / Alqahtani, s. 43134-43167

lenmektedir. 6G ağları ayrıca, holografik ışınlanma iletişimleri ve dokunsal internet ve artırılmış gerçeklik (AR) içeren dokunsal, çok duyusal genişletilmiş gerçeklik (XR) gibi gerçek zamanlı etkileşimli uygulamalarla makineden makineye ve insandan makineye bağlanmaya olanak sağlamayı amaçlamaktadır. Karma gerçeklik (MR) ve sanal gerçekliğin (VR) yanı sıra akıllı nesnelerin interneti (IoST) uygulamalarını da desteklemesi beklenmektedir. Bahsi geçen her şeyin interneti (IoE) uygulamaları, ultra yüksek veri yoğunluğu oluşturacağı ve bunlardan bazıları, ultra güvenilir ve düşük gecikmeli iletişim hizmetleriyle ultra yüksek hızlı bağlantı için temel gereksinimleri oluşturacağı değerlendirilmektedir. Bu nedenle gelecekteki 6G ağlarının bu uygulamaları son derece yüksek veri hızları ve çeşitli hizmet kalitesi gereksinimleriyle desteklemesi gerekmektedir. Ultra düşük iletim gecikmesi gereksinimleri uçtan uca gecikme süresi bir ila birkaç milisaniye arasında değişebilirken, ultra güvenilir iletişim yüzde yüze yaklaşacaktır. YZ ve makine öğrenimi (örn. derin sinir ağları) tekniklerinin, gelecekteki 6G ağları ile çeşitli gereksinim ve hizmetleri karşılamasını sağlayan temel faktör olması beklenmektedir[187]. Bu kapsamda; holografik ışınlanma (telepresence)[188], dokunsal internet[189], akıllı nesnelerin interne-

[187] Alsabah Muntadher / Naser Marwah Abdulrazzaq / Mahmmod Basheera M. / Abdulhussain Sadiq H. / Eissa Mohammad R. / Baidhani Ahmed Al / Noordin Nor K. / Sait Sadiq M. / Utaibi Khaled A. Al / Hashim Fazirul: 6G Wireless Communications Networks: A Comprehensive Survey, IEEE Access, Vol. 9, Y. 2021, s. 148191-148243 (https://ieeexplore.ieee.org/document/9598915, E.T. 18.04.2024).

[188] 6G ağlarının, gerçek zamanlı uzaktan fiziksel iletişim sağlamak için işitme, görme, tatma, koklama ve dokunma dahil olmak üzere tüm insan duyularını kullanan yeni bir insan uzaktan etkileşimi biçimini desteklemesi beklenmektedir. Holografik ışınlanma, karma gerçeklik teknolojisine sahip üç boyutlu bir videoya dayalı olarak gerçekleştirilebilen, gerçek zamanlı sanal ışınlanma olarak kabul edilmektedir. Holografik ışınlama, gerçek zamanlı uzaktan etkileşimi mümkün kılmak ve kişisel hologramın yeniden inşasını oluşturmak için birçok çoklu görüş kamerasından ve çoklu sensörden yararlanır. Bu, geleneksel video konferanstan sanal, gerçek zamanlı yüz yüze toplantıya doğru bir değişim olarak görülebilir; böylece iletişim deneyimi iyileşir, sanal konserlere izin verilir, sanal sporlar mümkün kılınır ve daha gösterge niteliğinde uzaktan eğitim sağlanır. Holografik ışınlanma, saniyede terabit (Tb/s) mertebesinde bir veri hızına ihtiyacı vardır. Bu sebeple ultra güvenilir ve düşük gecikmeli iletişim gerektirir (Alsabah vd. s. 148191-148243).

[189] Dokunsal İnternet, "İnsanlar veya makineler tarafından algılanan gerçek zamanlı olarak gerçek veya sanal nesnelere veya süreçlere uzaktan erişmek, bunları algılamak, manipüle etmek veya kontrol etmek için kullanılan bir ağ (veya ağlar ağı)." (Holland Oliver / Steinbach Eckehard / Prasad R. Venkatesha / Liu Qian / Dawy Zaher / Aijaz Adnan / Pappas Nikolaos / Chandra Kishor / Rao Vijay S. / Oteafy Sharief / Eid Mohamad / Luden Mark / Bhardwaj Amit / Liu Xun / Sachs Joachim / Araújo José: The IEEE 1918.1

ti uygulamaları[190], akıllı şehir[191] (akıllı ev, akıllı tarım, akıllı fabrikalar, akıllı ulaşım, akıllı şebeke, akıllı sağlık hizmetleri, akıllı radyo ortamları)[192] gibi daha birçok teknolojinin hayata entegre edileceği düşünülmektedir.

Bu kapsamda her ne kadar sadece bir şebeke ağının değişeceği ifade edilse de, birçok değişimin baş rolünde internetin olduğu düşünüldüğünde internet hızının teknolojik sistemleri etkilediği görülmektedir. Hızın artması

"Tactile Internet" Standards Working Group and its Standards IEEE, Vol. 107, Y. 2019, s. 256-279 (https://ieeexplore.ieee.org/abstract/document/8605315, E.T. 23.03.2024)). Uluslararası Telekomünikasyon Birliği (ITU) tarafından son derece yüksek güvenilirliğe sahip ultra düşük gecikme süresine sahip bir internet ağı olarak tanımlanmaktadır. Bu nedenle Dokunsal İnternet, bir ultra güvenilir ve düşük gecikmeli iletişim hizmeti gerektirir. Dokunsal İnternet, kablosuz bir ağ üzerinden insandan makineye ve makineden makineye gerçek zamanlı etkileşime izin verir. Dokunsal İnternet için eğitim, iş, sağlık hizmetleri (telecerrahi), endüstriyel (tele-bakım), akıllı şebeke ve toplumsal gibi çeşitli uygulamalar vardır. Dokunsal İnternet hizmeti, IoE uygulamalarının gerçek zamanlı olarak kontrol edilmesini sağlayacak bir sonraki gelişmedir. XR, gerçek ve sanal ortamları birleştirme potansiyeline sahiptir (Alsabah vd. s. 148191-148243).

190 IoT ağlarında, fiziksel cihazlara veya nesnelere birkaç farklı sensör ve çip yerleştirilmiştir ve bu da onları kablosuz olarak birbirine bağlamaktadır. Bu fiziksel sensörler ve nesneler, herhangi bir insan müdahalesi olmadan birbirleriyle ve diğer dijital bileşenlerle büyük miktarda veri alışverişi yapma yeteneğine sahiptir. Gelecekteki 6G iletişim sistemlerinde IoT bağlantılarının ve uygulamalarının önemli ölçüde artması beklenmektedir. 6G ağlarının, akıllı nesnelerin interneti bağlantılarını desteklemesi beklenmektedir (Alsabah vd. s. 148191-148243).

191 Akıllı bir şehir oluşturmak için, şehrin yönetimi, şirketleri ve bireyleri için çok çeşitli hizmetleri desteklemek üzere binalara, araçlara, yollara, fabrikalara ve evlere yerleştirilebilecek çok sayıda sensörden yararlanmayı amaçlamaktadır. Akıllı şehrin hedeflerinden biri vatandaşlar tarafından sunulan hizmetin kalitesini artırmak, kamu kaynaklarını daha iyi kullanmak ve işletme maliyetlerini azaltmaktır. Akıllı şehrin hayata geçirilmesi, geleneksel hizmetlerin kontrol edilmesi açısından önemli bir avantaj sağlayacaktır. Buna toplu taşıma ağları, güvenlik gözetimi, çöp toplama/atık yönetimi ve ortak alanların bakımı da dahildir. Akıllı şehirler, vatandaşların şehrin durumu hakkındaki farkındalığını artıracaktır. Örneğin, akıllı binaların etkinleştirilmesi, sera gazı emisyonlarının azaltılmasına yardımcı olabilecek hava kalitesini izlemek için sensörlerin yerleştirilmesi, trafik sıkışıklığının ve trafik yönetiminin izlenmesi, bahçeler için otomatik su sistemine izin verilmesi, enerji tüketiminin izlenmesi, elektrik ve suyun akıllı kullanımının sağlanması akıllı park ve akıllı aydınlatmanın kullanılmasına olanak sağlayacaktır. Dolayısıyla 6G ağlarında birleşik bir ağ mimarisi kurulması düşünülmektedir. Ancak akıllı şehir ekosisteminin 6G ağlarında daha fazla araştırılması gerekmektedir. Bu nedenle akıllı şehirlerde güvenli iletim, otomatik bakım, akıllı gerçek zamanlı izleme sistemi ve kesintisiz ağ oluşturma için uç bilişim, yazılım tanımlı ağlar ve YZ algoritmalarının kullanılması beklenmektedir (Alsabah vd. s. 148191-148243).

192 Alsabah vd. s. 148191-148243

yukarıda bahsedilen birçok teknolojinin hayatımıza girmesini sağlayacaktır. YZ temelli teknolojilerin birbirleri ile haberleşmesi önce '*nesnelerin interneti*'ni getirecek sonra da '*herşeyin interneti*'ni getirecektir. Tabi ki tüm teknolojilerin enerjiyle çalıştığını düşündüğümüzde enerjiye olan ihtiyacın da artacağı kuşkusuzdur.

Tüm bunların yönetişim çerçevesinde devlet tarafından kontrollerin sağlanması ve standartların getirilmesi gerekmektedir. Özellikle bu teknolojilerin artması neticesinde büyük verinin oluşması ve büyük verinin kontrolünün ve güvenliğinin sağlanması en büyük amaçlardan birisi olacaktır. Bu durum da teknoloji ile sağlanacaktır. Kuantum bilgisayar sistemleri ile hem kontrolün hem de güvenliğin üst seviyede sağlanabileceği düşünülmektedir.

IV. TÜRKİYE'DE YAPAY ZEKÂ YÖNETİŞİMİ VE METODOLOJİSİ

Türkiye' de Yapay Zekâ Yönetişimi ve Metodolojisi başlığında, yönetişim kapasiteleri irdelenerek mevcut durumların tespiti, geliştirilmesi gerekenler ile uygulamadaki sorunların çözülmesine yönelik öneriler dile getirilmektedir.

YZ, uluslararası, ulusal, kamu ve özel bağlamlardan oluşan bir hiyerarşi boyunca tüm vatandaşların haklarını, çıkarlarını ve yükümlülüklerini etkilemektedir. Uluslararası düzenlemelerin yapılması veya gelecekte yapılacak olması, ulusal mevzuatı da etkileyecektir. Bu sebeple ülkemiz gibi birçok ülke henüz ulusal düzenlemeleri gerçekleştirmemiştir. Bunun diğer sebebi de YZ'nin hızının öngörülemez şekilde artmış olmasıdır.

Hukuk evrensel normlar bütünüdür. Bir diğer anlatımla, hukukun ilgili özel alanında hem ilkeleri hem de geleceği kapsayan müeyyideleri bulunur. Sağlam bir hukuk mekanizması olması için geleceğin öngörülebilir, tekniğin de anlaşılabilir olması şarttır. Zira teknik bir alanda norm düzenlenecek ise o tekniği bilenlerin ve hukuku bilenlerin bir arada kanun taslak çalışması yapması önemlidir. Bunun sonucunda ilgili kurumların, sivil toplumun, tüzel kişilerin ve vatandaşların önerilerinin dikkate alınması metodolojik anlamda doğru sistemlerden birisidir. Bu çerçevede *Yapay Zekânın Sorumlu Bir Şekilde Geliştirilmesine İlişkin Montreal Bildirgesi* önemli bir ulusal bildirgedir. Montreal Bildirgesi'nin yazılması sürecinde birçok insanın farklı katkıları vardır. Vatandaşlara danışıldığı, birçok disiplinden araştırmacıların görüşünün alındığı çok disiplinli ve üniversiteler arası bir bi-

limsel ekibin çalışması sonucu hazırlanmıştır[193]. Önemli metodolojik örneklerden olan bu çalışmanın sonucunda Kanada ülkesinin YZ yönetişimi belirlenmiş, önce *Dijital Şart Uygulama Yasası*[194] taslağı ardından *Yapay Zekâ ve Veri Yasası*[195] taslağı kamuoyu ile paylaşılmıştır.

Ülkemizde ise çalışmalarda devletimiz aktif pozisyondadır. Özellikle CBDDO'nun ve Sanayi ve Teknoloji Bakanlığı'nın öncülüğünde yayımlanan Ulusal Yapay Zekâ Stratejisi[196], Ülkemizin YZ alanında metodolojisini yansıtmaktadır. 2021 ila 2025 yıllarını kapsayan strateji belgesinin vizyonu "*müreffeh bir Türkiye için çevik ve sürdürülebilir yapay zekâ ekosistemiyle küresel ölçekte değer üretmek*" tir. Strateji, 6 stratejik öncelik etrafında tasarlanmıştır: YZ uzmanlarını yetiştirmek ve alanda istihdamı artırmak, araştırma, girişimcilik ve yenilikçiliği desteklemek, kaliteli veriye ve teknik altyapıya erişim imkânlarını genişletmek, sosyoekonomik uyumu hızlandıracak düzenlemeleri yapmak, uluslararası iş birliklerini güçlendirmek, yapısal ve iş gücü dönüşümünü hızlandırmak.

Ulusal Strateji Belgesinin Amaç 4.1.'de yer alan "*Etik ve hukuki senaryoların test edilmesi ve tartışılabilmesi için çevik ve kapsayıcı bir yasal uyumlanma süreci işletilecektir.*" hedefi ve alt hedeflerinde referans model ve rehberlerin hazırlığından bahsedilmektedir[197]. YZ ilkeleri de Strateji belgesinde açıklanmış ve bu kapsamda önemli bir adım atılmıştır. Ancak somut olarak norm niteliğine haiz yasal bir çalışma henüz başlatılmamıştır. Adalet Bakanlığının 2024-2028 Stratejik Planı 2.5 maddesinin (h) bendinde ise "*Kurulacak bir merkez aracılığıyla yapay zekâ uygulamalarının etik ve hukuki çerçevesi oluşturulacaktır*" şeklinde hedef konulduğu görülmüştür[198].

---

193 Montréal Üniversitesi (2018), Sorumlu Yapay Zekâ Hakkında Montreal Bildirgesi (https://montrealdeclaration-responsibleai.com/the-declaration/, E.T. 22.03.2024).

194 Kanada (2022), Dijital Şart Uygulama Yasası (https://ised-isde.canada.ca/site/innovation-better- canada/en/canadas-digital-charter/bill-summary-digital-charter-implementation-act-2020, E.T. 24.03.2024).

195 Kanada, Yapay Zeka ve Veri Yasası Taslağı (https://ised-isde.canada.ca/site/innovation- better-canada/en/artificial-intelligence-and-data-act-aida-companion-document, E.T. 24.03.2024).

196 Sanayi ve Teknoloji Bakanlığı ve CBDDO(2021), Ulusal Yapay Zeka Stratejisi, (https://cbddo.gov.tr/SharedFolderServer/Genel/File/TR-UlusalYZStratejisi2021-2025.pdf, E.T. 25.03.2024).

197 Sanayi ve Teknoloji Bakanlığı ve CBDDO (2021), Ulusal Yapay Zeka Stratejisi, s.72

198 Adalet Bakanlığı, 2024-2028 Stratejik Planı (https://rayp.adalet.gov.tr/resimler/1/dosya/adalet-bakanligi-stratejik-plan-2024-2028-29-04-20244-20-pm.pdf, E.T.24.05.2024)

YZ'nin manipüle edilme veya kötüye kullanılma potansiyeli göz ardı edilemez[199]. Kamu hizmetlerinde otomatikleştirilmiş karar vermenin adaletli bir şekilde herhangi bir ön yargı bulunmadan gerçekleştirilmesi için bu konuda müeyyidelere ihtiyaç vardır. Kamu kuruluşlarında bu tür ön yargıların ortaya çıkma riskinin kontrol etmeye yardımcı olan karar verme algoritmalarının da bulunması gerekmektedir[200]. Tüm bu algoritmaların kurallara tabi olması ancak yasal düzenlemeler ile mümkün olabilecektir. Kamu yönünden ayrıca YZ ekosistemi aracılığı ile bir akreditasyon oluşturularak, akredite edilen kamu YZ projelerinin uygulanması sağlanabilecektir. Bu çerçevede ISO tarafından yayımlanan birçok uluslararası standart, *Yapay Zekâ Algoritmalarının Standardizasyonu* başlığında incelenmiştir. Söz konusu standartların kamu kurumları tarafından uygulanmasının sağlanması ileride oluşabilecek risklerin önüne geçebilecektir.

Hollanda'da yer alan üç ayrı kamu kurumuna yönelik yapılan araştırmalarda YZ alanında yaygın engellerin; etik ve yasal çerçevelere uyum, sağlamlık eksikliği, bilgi teknolojilerinin alt yapısı ve teknik uzmanlık eksikliği, YZ yeniliklerinin tek departmanla sınırlı oluşu, operasyonel bilgi ve teknik uzmanlığa sahip yöneticilerin olmayışı (uzman yönetim eksikliği) tespit edilmiştir. Yasal, etik, teknik ve organizasyonel engellerin ise YZ'nin benimsenmesini zorlaştırdığı belirtilmektedir. Yazarın önerisi ise, kamu kurumlarının nesnelerin interneti, dijital platformlar ve bulut bilişim gibi gelişen teknolojilerinin benimsenmesi ile departmanlar ve uzman arasındaki bağın kuvvetlendirilmesi ve yanıt verme ve taleplerin uyarlanmasına odaklanılmasıdır[201]. Kamu kurumlarına algoritmaların uygulanış şekli, makine öğrenimi ve derin öğrenme gibi YZ alt kümelerinin anlamları, yazılım projelerindeki yeri ve hangi hususların YZ olabileceği konusunda eğitim verilmelidir. Yazılım çalışmalarında talep eden birim ile teknik birim arasındaki uyumların önemli olduğu, yeterince uyumun olmadığı durumlarda, YZ projelerinde ise birçok hataya neden olabileceği öngörülmektedir. Bu sebeple ilgili kamu kurumunun kendi içerisinde YZ birimi kurması

---

199 Brewer vd.

200 Neumann Oliver / Guirguis Katharina / Steiner Reto: Exploring artificial intelligence adoption in public organizations: a comparative case study, Public Management Review, Vol. 26, Y. 2024, s. 114-141 (https://doi.org/10.1080/14719037.2022.2048685, E.T. 24.03.2024).

201 Selten Friso, Klievink Bram: Organizing public sector AI adoption: Navigating between separation and integration, Government Information Quarterly, Vol. 41,Y. 2024 (https://doi.org/10.1016/j.giq.2023.101885, E.T. 24.03.2024).

ve iletilecek proje taleplerinin belirli bir standartlar çerçevesinde oluşturulacak form aracılığı ile teknik birime iletmesi yerinde olacaktır. Bu kapsamda *Yapay Zekâ Algoritmalarının Standardizasyonu* başlığında incelenen uluslararası standartların benimsenmesi durumunda profesyonel bir yaklaşımın olabileceği değerlendirilmektedir.

Kamu YZ ekosisteminin oluşturulması Ulusal Strateji Belgesinin önemli hedeflerinden birisidir. TUBİTAK Yapay Zekâ Enstitüsü aracılığıyla proje çağrılarının teknik alanlarda yoğunlaştığı görülmektedir. Kamunun hizmetine yararlı olacak projelerin geliştirilmesi amacıyla proje çağrı tematik alanların genişletilmesi, kamu YZ ekosisteminin oluşturulması açısından önem arz etmektedir. Özellikle adalet alanında desteklenen ilk YZ projesi "*Türkiye Adalet Akademisi Eğitim Programlarının Yapay Zekâ Destekli Dijital Dönüşümü Projesi*"dir[202]. Türkiye Adalet Akademisi tarafından hazırlanan proje, akıllı eğitim sistemlerine yönelik olup hâkim ve Cumhuriyet savcı yardımcılarının eğitiminde aktif olarak kullanılacak YZ sistemlerinin mimarisini planlamaktadır.

Blok zincir (*blokchain*), dağıtık ağ teknolojisi veya dağıtık defter teknolojisi isimleriyle de anılan *blokchain teknolojisi*, güvenli veri saklama düşüncesi olup internet hızları ilerledikçe veri depolama konusunda bu düşünce daha uygulanabilir hale gelmiştir. Devlet Arşivleri Başkanlığı koordinesinde ülkenin farklı noktalarında ilgili depolama sistemlerinin yapılması ile verilerin daha güvenli bir şekilde saklanabileceği değerlendirilmektedir.

Bir başka konu ise YZ ile İHA sistemlerinin görüntülerinin analiz edilerek kullanılmasıdır. Mahkeme veya Cumhuriyet savcılıklarının öncelikle engebeli arazi yapısı olan *Doğu Anadolu, Karadeniz ve Güney Doğu Anadolu* bölgelerinde yapılacak arazi keşiflerinde İHA keşiflerin icra edilmesi sağlanabilecektir. RTK/PPK İHA sistemleri ile herhangi bir Yer Kontrol Noktası'na (YKN) gereksinim duyulmadan hukuki süreçte kullanılan fotogrametrik ürünler 10 santimetrenin altında bir doğruluk ile gerçekleştirilebilmektedir[203]. İHA fotogrametrisi ile keşif uygulamalarının yapılmasıyla birlikte elde edilen fotogrametrik ürünlerin derin öğrenme gibi yapay zekâ destek-

[202] TUBİTAK (2023), 1007 Programı Yapay Zekâ Alanında Kamu Yapay Zekâ Ekosistem, (https://tubitak.gov.tr/tr/duyuru/1007-programi-yapay-zeka-alaninda-kamu-yapay-zeka-ekosistem-2023-cagrisi-sonuclari-aciklandi, E.T. 25.03.2024)

[203] Türk Tarık / Öcalan Taylan: *PPK GNSS Sistemine Sahip İnsansız Hava Araçları İle Elde Edilen Fotogrametrik Ürünlerin Doğruluğunun Farklı Yaklaşımlarla İrdelenmesi*, Türkiye Fotogrametri Dergisi, S. 2(1), Y. 2020, s. 22-28.

li uygulamalarla bütünleştirilmesi, yapılan keşiflerin daha etkin hale getirilmesini ve yargı denetiminin arttırılmasını sağlayabilecektir. Bu çerçevede arazide kullanılacak her İHA'nın bu keşifler için yeterli doğruluk ve imkân sağlayamayacağına ve Ulusal İnsansız Hava Aracı Keşif Standartları'na yönelik akreditasyon oluşturulmasına yönelik önerilerde bulunulabilecektir.

Devletin kuantum bilgi teknolojilerini (KBT) kullanması YZ kadar stratejik öneme sahiptir. KBT, potansiyel olarak geniş kapsamlı ekonomik, jeopolitik ve hatta sosyal etkileri olan dinamik ve gelişmekte olan bir alandır. KBT düzenlemesi için bir dizi mevcut yönetişim prosedürü, çerçeve, kurum ve uygulamalar mevcuttur. KBT yönetişimi, KBT'nin genel olarak teknoloji yönetişiminin daha geniş bağlantı noktası ve hiyerarşisi içerisine yerleştirilmesi gerekmektedir. Bunu yapmak, mevcut yönetişim araçlarının KBT ile nasıl ilişkili olabileceğinin ve politika hedeflerini karşılamak için hangi yeni yönetişim yanıtlarının gerekli olduğunun bir analizini zorunlu kılmaktadır[204].

Kuantumun klasik hesaplamanın aksine ana ayırt edici özellikleri, süperpozisyon durumlarının ve dolanıklığın kullanılabilirliğidir. Bu iki temel kuantum olgusu, kuantum hesaplamanın klasik hesaplamaya göre etkili avantajlarındandır. Bu durum, eğer ölçeklenebilir, hatasız kuantum hesaplamaya ilişkin belirli teknik varsayımlar karşılanırsa, kuantum hesaplamanın hesaplama kaynaklarında ciddi bir genişleme olacaktır. Bunun sonucunda, bu tür bir genişleme klasik olarak çözümü mümkün olmayan (yani boyutu ne olursa olsun herhangi bir klasik bilgisayarda gerçekleştirilemeyen) bazı sorunların çözülebilir hale gelmesini sağlayacaktır[205]. Bu kapsamda yer alan bir teknolojinin; tek bir kuantum sistemi ile tüm devletin dijital alt yapısının yönetiminin YZ ile kontrol edilebileceği, kırılması imkânsız olan şifreler üreterek kriptografik siber güvenlik bariyerinin inşa edilebileceği, vatandaşlara ve devlete ait verilerin saklanması ve korunmasında tek kontrol merkezi oluşturulabileceği öngörülmektedir. Devletin tüm savunma mekanizmasının yönetişimi de KBT ile yapılabilecektir. Bunun yanı sıra özellikle sağlık ve biyoteknoloji olmak üzere birçok alanda deneylerin sistem alt yapısı olarak kullanılabileceği değerlendirilmektedir. Enerji platformlarındaki verilerin kontrol edilerek, daha az enerji sarfiyatı ile büyük organizasyonların nasıl yönetilebileceği hususun-

---

204 Perrier E.: The Quantum Governance Stack: Models of Governance for Quantum Information Technologies, Digital Society, Vol. 1, Y. 2022, s. 2 (https://doi.org/10.1007/s44206-022-00019-x, E.T. 17.04.2024)

205 Perrier, s. 6.

da KBT destek sağlayabilecektir. Tüm bu organizasyon yapısı oluşturulması için öncelikle CBDDO tarafından kamu kurumlarının bilgi teknolojilerinin alt yapısının ve kullandığı sistemleri belirleyerek siber güvenlik sistemlerini incelemesi gerekmektedir. İdeal kuantum yönetişiminde aktörlerin ve araç modelinin ana hatlarını sunarak öncelikle KBT sistemine dönüşümün yapılması amacıyla stratejiler belirlenmeli ardından ise KBT'nin YZ'ye yönelik yönetişim çerçevesi oluşturulmalıdır. Bu çerçevede kuantum stratejisinde, Amerika Birleşik Devletleri tarafından Mayıs 2022'de yayımlanan "National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems" önemli bir örnektir[206].

Devletin buradaki odağı, uluslararası, ulusal, kamusal ve özel bağlamlardan oluşan bir hiyerarşi boyunca tüm vatandaşların haklarını, çıkarlarını ve yükümlülüklerini etkilediğinden KBT'nin yararları ve risklerinin ortaya konularak yönetişim araçları oluşturulmalıdır. Yönetişimin hiyerarşik doğası ve bilgi teknolojileriyle doğrudan ilişkisi göz önüne alındığında, bu hiyerarşi, *kuantum yönetişim yığını* olarak adlandırılmaktadır[207].

YZ yönetişimi, birçok alanı kapsamakta ve bu yönüyle de karmaşık olması muhtemeldir. Kuantum yönetişim ise YZ'de yönetişim karmaşıklığını çözme yöntemidir. Bu model, toplum için olumlu sonuçlar elde etmek amacıyla KBT'nin sorumlu bir şekilde tasarlanması ve benimsenmesine yönelik stratejiler oluşturulmasını ifade etmektedir[208]. Öncelikle kamunun YZ tek-

---

206 Savunmasız Kriptografik Sistemlere Yönelik Riskleri Azaltırken Kuantum Hesaplamada Amerika Birleşik Devletleri Liderliğini Teşvik Etmeye İlişkin Ulusal Güvenlik Memorandumunun amacı; kuantum bilgisayarlarının ülkenin siber, ekonomik ve ulusal güvenliğine yönelik risklerini azaltırken, ülkenin kuantum bilgi bilimindeki rekabet avantajını korumak için gereken temel adımları belirlemektedir. Amerika Birleşik Devletleri'nin savunmasız bilgisayar sistemlerini kuantum dirençli kriptografiye geçirmeye yönelik dönüşümünde birçok yılı kapsayan eylemlere yönelik stratejidir. Ayrıca stateji, içerisinde hassas ulusal güvenlik konularını ele alan gizli eki de barındırmaktadır (ABD (2022), National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems (https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/, E.T. 14.02.2024)).

207 Perrier, s. 2

208 World Economic Forum (2022), Quantum Computing Governance Principles, (https://www.weforum.org/publications/quantum-computing-governance-principles/ E.T. 25.12.2023).

nolojilerindeki amacı; risklerin azaltılması, güvenlik, savunma, ileri teknolojilerden faydalanma, tek merkezden yönetişimin sağlanması, enerji tasarrufu ve kontrolü, veri merkezlerinin yönetimidir. Kamudaki tüm bu sistemlerin kuantum yönetişim yığını ile kontrol edilerek olası saldırıların önüne geçilmesi ve tek merkezden kontrolün sağlanması en güvenilir yollardan birisidir. Bu sayede tüm kamunun bilgi teknolojileri Kuantum Yapay Zekâ Ekosistemi ile sağlanabilecektir.

Ülkemizde, Ulusal Siber Olaylara Müdahale Merkezi (USOM)[209] kurulmuştur. USOM'un temel amaçları, ülkemizin siber güvenliğine karşı siber ortamda ortaya çıkan tehditlerin belirlenmesi, muhtemel siber saldırı ve olayların etkilerini azaltılması veya ortadan kaldırılmasına yönelik önlemlerin geliştirilmesi ve belirlenen aktörlerle paylaşılmasıdır[210]. Bu çerçevede YZ yönetişiminde önemli başlıklardan olan siber güvenlik, YZ'den yararlanılarak gerçekleştirilecek uygulamalar ile tüm kamu kurumları ve özel şirketlerin güvenliğinin üst seviyede sağlanabileceği görülmektedir. USOM tarafından siber güvenlik mimarisinin nasıl oluşturulması gerektiği, risklerin azaltılması, ortaya çıkan tehditlere proaktif olarak yanıt verebilme imkânının sağlanması ve bilgi iletişim teknolojileri alt yapısının güncellenmesi gibi hem yazılım hem de donanım seçeneklerini de ortaya koyarak her yıl (veya tehdit zamanlarında) kılavuz yayımlaması ve tüm paydaşlara iletilmesi gerekmektedir. Ayrıca USOM alt yapısında kamu kurumlarının ve özel şirketlerin bilgi iletişim teknolojileri alt yapısına koruyucu katman mekanizmasının yerleştirilmesi ve bu imkânın sağlanması güvenlik açıklarına anlık müdahale edilmesini de sağlayacaktır. Bu sayede bu stratejileri ve kılavuzları uygulamakla mükellef kamu kurumları ve özel şirketlerin, siber savunmaları güçlenerek ulusal güvenlik zafiyetlerinin önüne geçilmesi sağlanabilecektir.

---

209 20/10/2012 tarih ve 28447 sayılı Resmî Gazete'de yayımlanan "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Bakanlar Kurulu Kararı" ve 5809 sayılı Elektronik Haberleşme Kanunu gereğince 20/06/2013 tarih ve 28683 sayılı Resmî Gazate'de yayımlanan 2013/4890 sayılı Bakanlar Kurulu Kararı ile "2013-2014 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı" kapsamında Bilgi Teknolojileri ve İletişim Kurumu bünyesinde 27/05/2013 tarihinde Ulusal Siber Olaylara Müdahale Merkezi (USOM) kurulmuştur (USOM, https://www.usom.gov.tr/hakkimizda, E. T. 22.05.2024).

210 Siber Güvenliğin Etkisi başlığında detaylı olarak açıklanan kurumsal siber güvenlik mimarisinin Ülkemizde gerçekleştirecek kamu kurumu USOM olabilecektir.

Ülkemizde ayrıca Siber Güvenlik Başkanlığı kurulmuştur[211]. Söz konusu Cumhurbaşkanlığı Kararnamesi, Başkanlığın, teşkilat, görev, yetki ve sorumluluklarına ilişkin usul ve esasları düzenlemek amacıyla yayımlanmıştır. Başkanlık, Cumhurbaşkanlığına bağlı, kamu tüzel kişiliğini haiz, özel bütçeli bir kuruluş olarak kurulmuştur. Başkanlığın birçok görev ve yetkileri mevcuttur. Bunlardan en önemlileri ise siber güvenliğin sağlanması amacıyla politika, strateji ve hedefleri belirlemek, eylem planları hazırlamak, mevzuat çalışmalarını yürütmek, eğitim ve farkındalığı arttırmak, destekleyici projeler yürütmek, kamu, özel sektör ve üniversiteler arasındaki iş birliğinin arttırılmasına yönelik çalışmalar yapmak, siber güvenlik ekosistemin inşası ve yerli ve milli ürün ve teknolojilerin geliştirilmesi ve yerli girişimcilerin dünya pazarında rekabetçi konuma gelmesine yönelik çalışmalar yapmak, Ar-Ge ve teknoloji transferi gerçekleştirmek, güvenlik zafiyetlerini tespit etmek, kritik alanlara güvenlik kapasitesini yönlendirmek, acil durum ve kriz yönetim planları oluşturmak, ortak operasyon merkezleri kurmak gibi birçok önemli görev ve sorumluluk yüklenmiştir. Bu kapsamda yapılan değişiklikler ile CBDDO'nin ve BTK'nın siber güvenlik alanına ilişkin görevleri Siber Güvenlik Başkanlığına devredilecektir.

Siber Güvenlik Kanunu teklifi de TBMM' ye sunulmuştur[212]. Henüz Komisyon aşamasında olan Teklif ile, "*Türkiye Cumhuriyeti'nin siber uzaydaki milli gücünü meydana getiren bütün unsurlarına karşı içten ve dıştan yöneltilen mevcut ve muhtemel tehditlerin tespit ve bertaraf edilmesi, siber olayların muhtemel etkilerini azaltmaya yönelik esasların belirlenmesi, kamu kurum ve kuruluşları, kamu kurumu niteliğinde meslek kuruluşları, gerçek ve tüzel kişiler ile tüzel kişiliği bulunmayan kuruluşların siber saldırılara karşı korunmasına yönelik gerekli düzenlemelerin yapılması, ülkenin siber güvenliğini güçlendirmek için strateji ve politikaların belirlenmesi ile Siber Güvenlik Kurulunun kurulmasına dair esasların düzenlenmesi amaçlanmaktadır*"[213].

Teklifle;

Ülkemizin siber güvenlikle ilgili politika ve stratejisini belirlemek üzere Siber Güvenlik Kurulunun kurulması,

---

211 08/01/2025 tarih ve 32776 sayılı Resmî Gazete'de yayımlanan 177 Nolu "Siber Güvenlik Başkanlığı Hakkında Cumhurbaşkanlığı Kararnamesi" ile Siber Güvenlik Başkanlığı kurulmuştur.

212 28. Dönem, 3. Yasama yılı, 10.01.2025 Tarih ve 2/2860 Esas numaralı Siber Güvenlik Kanunu Teklifi

213 Siber Güvenlik Kanunu Teklif Özeti

Siber güvenlik alanında geliştirilen politikaların ulusal satıhta etkin bir şekilde uygulanması,

Kamu kurumları ile kritik altyapı kuruluşlarının siber mukavemetinin ve siber olgunluk seviyesinin artırılması,

Güncel teknolojik gelişmelerin takip edilmesi ve siber güvenlik süreçlerine entegre edilmesi,

Kamu kurumları ve kritik altyapı kuruluşlarının bilişim sistemlerinde oluşabilecek siber güvenlik olaylarının merkezi bir bakış açısıyla izlenmesi, tespiti ve bertaraf edilmesi,

Eylem planlarının ve ikincil mevzuatların hayata geçirilmesi,

Denetim ve özellikle caydırıcı yaptırım süreçlerinin işletilmesi,

Siber güvenlik ekosisteminin güçlendirilmesi,

Standardizasyon, sertifikasyon ve yetkilendirme süreçlerinin düzenlenmesi,

Siber suçlara yönelik cezaların artırılması suretiyle caydırıcılığın sağlanması amaçlanmaktadır.

Teklifin genel gerekçesinde ise; "*Yapay zekâ, blok zincir, büyük veri, kuantum ve bulut bilişim gibi teknolojilerin yaygınlaşması, siber tehditlerin karmaşıklığını artırırken, aynı zamanda savunma mekanizmalarının gelişimini de tetiklemiştir. Kritik altyapıların korunması ve kamu kurumlarının dijital süreç ve varlıklarının güvence altına alınması, modern siber güvenlik stratejilerinin merkezinde yer almaktadır. Bununla beraber, Milli Teknoloji Hamlesi kapsamında ülkemizin yaşadığı teknolojik dönüşüm ve gelişim sürecinde siber güvenlik en temel gerekliliklerinden biri haline gelmiştir.*". Bu çerçevede Kanunun kurulması amacındaki en önemli gerekçeleri belirtilmekle birlikte diğer birçok gerekçeyi de içerisinde barındırmaktadır.

Teklifin 6 ncı maddesinin 1 inci fıkrasının (h) bendinde; "*Kamu kurum ve kuruluşları ile kritik altyapıların bilişim sistemlerinde kullanılacak ve siber güvenliğe etkisi olan yazılım, donanım, ürün ve hizmetlere kullanım öncesinde uygunluk verir*".

Aynı fıkranın (i) bendinde; "*Siber güvenlik yazılım, donanım, ürün ve hizmetlerinin asgari güvenlik kriterlerini belirler. Bunları sağlayacak veya tedarik edecek gerçek ve tüzel kişilere yönelik sertifikasyon, yetkilendirme ve*

belgelendirme süreçlerini yönetir. Siber güvenlik yazılım, donanım, ürün ve hizmetlerinin belirlenecek standartlara uygun hale getirilmesini talep edebilir, bu talebe uyum sağlamayanların kullanılmasını önleyici tedbirler alabilir".

Kamu kurum ve kuruluşları yönünden hizmetlerin kullanım öncesi uyumluluğu, asgari güvenlik kriterlerinin belirlenmesi, sertifikasyon ve belgelendirme süreçleri gibi standardizasyon sağlanması Ülkemiz siber güvenliğinin kalite düzeyini arttıracağı düşünülmektedir.

Yapay zekâ, blok zincir, büyük veri, kuantum ve bulut bilişimin genel gerekçede yer alması, siber güvenlik açısından büyük gelişim sağlandığının bir göstergesidir. Siber Güvenlik Başkanlığının kurulması akabinde Siber Güvenlik Kanunun yürürlüğe girmesi de bu alanda yeterli olmayacaktır. Özellikle bahsi geçen bu teknolojilerin siber güvenlik alanında aktif olarak kullanılması ile ekosistemin gerçekleşebileceği değerlendirilmektedir.

SONUÇ

Yeni bir hukuk çağı açılmaktadır. İnsanlığın var oluşuyla ortaya çıkan insan - insan arasında olan hukuk, insan - makine (algoritma) ve makine (algoritma) – makine (algoritma) arasındaki uyuşmazlıkları çözümleyen hukuk sistemine evrilecektir. Etik şartlar, bu uyuşmazlıkları karşılamaya yetmeyecektir. Bu sebeple somut normların yer aldığı regülasyonların var olması gereklidir. Yapay genel zekâ, yapay zekâ ve yapay süper zekânın geliştirileceği ve yapay süper zekâ ile insan üstü zekâya sahip sistemlerin geleceği bilinmektedir. İnsan - insan uyuşmazlıkları çerçevesinde ele alınan klasik hukuk anlayışı, bu çağda ihtiyaçları karşılamayacaktır. Bu nedenle hukuk dünyasının makinelerin uyuşmazlıklarına da çözüm üretmesi gerekecektir. Bunun sonucunda hem insanı hem de makineyi ele alan yeni bir regülasyon beklenmektedir. *Vingean Yansıması*'nın yaşanmaması için yapay süper zekâ ve türevleri olan insan üstü sistemlerinin kontrollü şekilde ilerlemesi sağlanmalıdır. Zira insan üstü sistemleri insanların kontrol etmesi imkânsız olacaktır. Süper hizalama *(super alingment)* yine algoritmalar tarafından yapılacaktır. Bir diğer anlatımla hem kural koyma hem de kuralın uygulanması makinelerin gözetiminde olacaktır. Her yeni teknolojik gelişmede makineler tarafından yeni regülasyonlar koyularak denetim sağlanacaktır. YZ yönetişimi, makinelere devredilecektir. Ancak her zaman olduğu gibi insanların etik anlayışı, makinelere de öğretilmek zorundadır. Zira insanların uyması gerekli etik şartları, insanların korunması için öngörülmüştür. Korunması gereken sadece insanlar değil makineler de bu-

lunmaktadır. Bu nedenle hem insanlığın var oluşuna hem de evrensel hukuk kurallarına uygun olarak etik şartlar belirlenmeli ve sürekli olarak tartışılarak güncellenmelidir. Kuralı insan koymuyorsa etiğini insan belirlemelidir. Bu nedenle temel amaç, nihayetinde, insanın ve insana ait değerlerin korunması olduğundan etik şartların yeniden regülasyonu şarttır.

Ulusal Kuantum ve Yapay Zekâ Ekosistemi oluşturulmalıdır. Türkiye' de Yapay Zekâ Yönetişimi ve Metodolojisi bölümünde ayrıntılı olarak açıklandığı üzere Ülkemizin kamu kurumlarında her biri ayrı bilgi teknolojilerine yönelik sistemler vardır. Sistemlerin güvenlik açıklarının varlığında ise olası saldırıların odağı haline gelmesine neden olabilecektir. Bu nedenle tüm kamu kurumlarının kuantum bilgisayar alt yapısına dönüşümü için stratejiler belirlenmelidir. Kuantum bilgisayarlarının alt yapısının pahalı olması karşısında süper iletken malzemelere yönelik yeni keşifler için Ülkemiz Ar-Ge çalışmalarına yatırım yapmalıdır. Örneğin, Güney Kore gibi kuantum alt yapısına ve süper iletken malzemelere yönelik bilimsel çalışma yapan ülkeler ile ortak çalışmalar yapılması ve ikili protokollerin imzalanması kayda değer bir adım olacaktır[214]. Bu çerçevede hem ulusal hem de uluslararası çalışmaları yürütecek Türkiye Kuantum Bilim Merkezi kurulmalıdır.

Ülkemizde gerçekleştirilecek YZ projelerinin Yapay Zekâ Algoritmalarının Standardizasyonu başlığında belirtilen uluslararası standartlara tabi olması ve bu standartların da ülkemiz tarafından önem verilmesi gereklidir. Bu çerçevede Ülkemizce de YZ algoritma standartları belirleyerek bu kurallara uyulması akabinde güvenli bir ekosistem oluşturulabilecektir. Pilot olarak kamuda akabinde özel şirketlere uygulanması hedeflenebilecektir.

---

214 Swayne Matt: How Would Room-Temperature Superconductors Change Quantum Computing?, The Quantum Insider, Y. 2023 (https://thequantuminsider.com/2023/08/03/ how-would-room-temperature-superconductors-change-quantum-computing/, E.T. 09.04.2024); Kuantum bilgisayarlar genellikle kübitlerinin hassas kuantum durumlarını korumak için mutlak sıfıra yakın (yaklaşık -459F) son derece düşük sıcaklıklarda çalışması gerekmektedir. Ve bu çok fazla enerji gerektirmektedir. Güney Koreli bir araştırma ekibinin, oda sıcaklığında ve ortam basıncında çalıştığı bildirilen süper iletken bir malzeme (LK-99) keşfetmiştir. Bu keşif ise kuantum bilgisayarları daha erişilebilir hale getirebilecektir. Amerika Birleşik Devletleri ile Güney Kore Cumhuriyeti arasında iş birliği anlaşması imzalanmıştır: ABD (2023), Amerika Birleşik Devletleri ve Kore Cumhuriyeti'nin Kuantum Bilgi Bilimi ve Teknolojilerinde İşbirliğine İlişkin Ortak Açıklaması (https://www.state.gov/joint-statement-of-the-united-states-of-america-and-republic-of-korea-on-cooperation-in-quantum-information-science-and-technologies/, E.T. 09.04.2024).

Bilgi iletişim teknolojileri sistemlerinin her kamu kurumunda ve özel şirketlerde kurulması şarta bağlanmalıdır. Ayrıca iş sürekliliği için işletme ve bakım verilerinden YZ ile arıza tespit ve tahmin sistemlerinin kurulması da kamu kurumlarında sağlanmalı, özel şirketlerde ise teşvik edilmelidir. Yukarıda yer alan *Bilgi ve İletişim Teknolojileri Altyapısı* başlığı altında açıklandığı üzere bir kuruluşun, iş sürekliliği ve bilgi iletişim teknolojisi hazırlığına ulaşması için Planla – Uygula - Kontrol Et - Önlem Al döngüsel adımlarını uygulaması gerektiğine yönelik kılavuz yayımlanmalıdır.

Vatandaşların internet üzerinden kullanılan tüm uygulamalarda haklarına riayet etmek ve güven vermek için, ortaya çıkan ihtiyaçlara ayak uyduracak ulusal gizlilik ve veri yönetimi standartlarının oluşturulması gerekmektedir.

Ülkemizin Sandbox sistemini kurarak hızlı bir şekilde uygulaması gerekmektedir. Avrupa Birliği Yapay Zekâ Tüzüğü risk temelli yaklaşım çerçevesinde oluşturulmuş olup yüksek riskli alanları da sıralamıştır. Tüzükte, birçok yeni kurum ve düzenlemenin yanı sıra yazılım sistemlerinin de kurumların gözetiminden geçeceği bir yönetişim modeli öngörülmektedir. Hem Ülkemize hazırlanacak Yapay Zekâ ve Algoritma Yasası'na eklenmesi hem de henüz regülasyon yapılmadan kılavuz yayımlanarak kamunun ve özel şirketlerin sandbox'a hazırlanması sağlanabilecektir. Regülasyon öncesi YZ uygulamalarında şimdiden uyum sağlanması ileride doğabilecek olumsuz sonuçları da bertaraf edebilecektir.

Hem ulaşımda hem de tarımda YZ uygulamalarının oluşturulması amacıyla Ülkemiz tarafından teşviklerin verilmesi gerekmektedir. Ulaşımda, YZ destekli sistemler, rotaları optimize eder, emisyonları azaltır ve verimliliği artırarak daha temiz ve daha sürdürülebilir kentsel ortamlara katkıda bulunur. Tarımda ise, mahsul verimini artırarak, kaynak kullanımını optimize eder ve sürdürülebilir tarım uygulamalarını teşvik ederek tarımda devrim yapılabilir[215]. Özellikle son yıllarda İHA sistemleri ile ilaçlama gibi faaliyetler yapılmaktadır. Otonom tarım aletleri ile de tarım sektöründe verimlilik arttırılabilecektir.

IoT ve IoB sistemlerinin standartlaştırılmış veri formatları oluşturmaya teşvik edilmesi gerekmektedir. Standartlaştırılmış formatlarda veri alışverişi kullanımına dikkat edilmemektedir[216]. Bu sebeple çeşitli standartları

---

215 Camocha, s. 149

216 Turner Sarah / Tanczer Leonie Maria: In principle vs in practice: User, expert and policymaker attitudes towards the right to data portability in the internet of things, Computer Law & Security Review, Volume 52, 2024 (https://doi.org/10.1016/j.clsr.2023.105912, E.T. 18.04.2024).

da dikkate alarak, regülasyon kurumlarının, sağlıkta ve IoT kapsamında değişim gösterecek sektörlerin bu ve benzeri konuları tartışması ve buna yönelik yasal düzenlemeleri hayata geçirmesi önem arz etmektedir.

İnsanların doğrudan süper zeki sistemler belirlemek yerine, aşamalı zeki sistemler belirleyerek her aşamanın bir sonraki aşamayı denetleyebileceği şekilde yazılım mimarisi inşa etmelidir. Bu durumda, ortaya çıkan süper zeki sistemin güvenilirliği, onu oluşturan ilk sistemin muhakemesine bağlı olup sürekli bu konuda kendisini geliştirmesi sağlanmalıdır. Örneğin, otomobile entegre edilen otopilot yazılımında olduğu gibi son derece yüksek sorumluluk verildiği için *Vingean Yansıma* prensibi kullanılarak kritik karar anlarında yüksek güvene sahip akıl yürütme için bir başka YZ tarafından denetleyici rolü verilebilir[217].

Kurumsal siber güvenlik mimarisi, devletin ya da özel şirketlerin hedefli siber saldırılara ve sürekli gelişen tehdit ortamına karşı savunmalarını güçlendirmeleri için kapsamlı bir plan olarak hizmet etmektedir. Kurumsal siber güvenlik mimarisinin stratejilerini gerçekleştiren devlet ve özel şirketlerin, siber savunmaları güçlenir, ortak hareket etme mekanizması oluşur, risk azalır ve ortaya çıkan tehditlere proaktif olarak yanıt verebilme imkânı gelişir. Her büyüklükteki kuruluşun kritik varlıkları koruyan ve genel iş hedeflerini destekleyen sağlam bir siber güvenlik programı oluşturmasını sağlar. Bu çerçeve, kurumsal bir siber güvenlik programının tüm yönlerini yönetmek, bilgi ve rehberlik sağlamak, bilgi işlem teknolojileri politikası, teknoloji, bilgi işlem teknolojileri yaşam döngüsü ve değerlendirme protokolleriyle sorunsuz bir şekilde uyumlu bir siber güvenlik stratejisi tasarlamalarını, uygulamalarını ve işletmelerini sağlayarak katmanlı korumalar oluşturmaktadır. Bu sebeple dijital çağdaki tehditleri etkili bir şekilde azaltmak için YZ'yi siber güvenlik çerçevelerine entegre edilmesi gerekmektedir.

Siber Güvenlik Kanun Teklifi ile getirilecek mevzuatın ardından, siber güvenlik ekosistemi oluşturulması için, Ülkemizde yer alan tüm yazılım çalışmalarının katmanlı olarak siber güvenlik standardizasyonundan geçmesi için bir süreç oluşturulmalıdır. Standartlara uyulup uyulmadığı sürekli olarak denetleyecek bir ekosistem getirilmelidir. Bu çerçevede çok hızlı ve etkin denetim için kuantum bilgisayar sistemlerinden yararlanılması gereklidir. Bunun yanında Ar-Ge çalışmaları ile standartların belirlenmesi,

[217] Soares / Fallenstein (Technical report 2014-8).

sandbox'ın kurulması, YZ algoritmaları ile siber güvenlik stratejilerinin oluşturulması ve aktif olarak kullanılması, siber saldırıların bertaraf edilmesi, diğer ülkelerde geliştirilen güvenlik algoritmalarının tespiti gibi birçok konuda projeler desteklenmelidir. Siber güvenlik sadece insan eliyle değil aynı zamanda yazılımlar vasıtasıyla da yapılabilecektir. Siber güvenliğe yönelik YZ algoritmalarının oluşturulması ile sürekli olarak denetim yapılabilecektir. Bu durumda dış ülkelerden gelecek saldırıların önceden tespit edilerek siber güvenlik stratejilerinin belirlenmesi ile YZ algoritmalarının güncellenmesi ve yeni standartların ortaya çıkartılarak saldırıların bertaraf edilmesi sağlanabilecektir.

KAYNAKÇA

ABD (2022), *National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems* (https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/, E.T. 14.02.2024).

ABD (2023), *Amerika Birleşik Devletleri ve Kore Cumhuriyeti'nin Kuantum Bilgi Bilimi ve Teknolojilerinde İşbirliğine İlişkin Ortak Açıklaması* (https://www.state.gov/joint-statement-of-the-united-states-of-america-and-republic-of-korea-on-cooperation-in-quantum-information-science-and-technologies/, E.T. 09.04.2024).

ABD (2023), *Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence* (https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/, E.T. 19.03.2024).

ABD (2023), *The National Artificial Intelligence Research Resource (NAIRR)* (https://nairrpilot.org/about, E.T. 19.03.2024).

ABD, *the National AI Talent Surge* (https://ai.gov/, E.T. 19.03.2024).

ABD (2024) National Institute Of Standards And Technology: Post-Quantum Cryptography, (https://csrc.nist.gov/projects/post-quantum-cryptography, E.T. 01.12.2024)

AKTER Shahriar / MCCARTHY Grace / SAJİB Shahriar / MİCHAEL Katina / DWİVEDİ Yogesh K. / D'AMBRA John, SHEN Kathy Ning: *Algorithmic bias in data-driven innovation in the age of AI,* International Journal of Information Management, Vol. 60, Y. 2021 (https://doi.org/10.1016/j.ijinfomgt.2021.102387, 18.04.2024).

ALLEN Hilary J.: *Sandbox boundaries,* Vanderbilt Journal of Entertainment and Technology Law, Vol. 22, Y. 2020 (https://scholarship.law.vanderbilt.edu/cgi/viewcontent.cgi?article=1017&context=jetlaw, E.T. 18.04.2024).

ALSABAH Muntadher / NASER Marwah Abdulrazzaq / MAHMMOD Basheera M. / ABDULHUSSAİN Sadiq H. / EİSSA Mohammad R. / BAİDHANİ Ahmed Al / NOORDİN Nor K. / SAİT Sadiq M. / UTAİBİ Khaled A. Al / HASHİM Fazirul: *6G Wireless Communications Networks: A Comprehensive Survey*, IEEE Access, Vol. 9, Y. 2021 (https://ieeexplore.ieee.org/document/9598915, E.T. 18.04.2024).

Avrupa Komisyonu (2022), First regulatory sandbox on Artificial Intelligence presented (https://digital-strategy.ec.europa.eu/en/news/first-regulatory-sandbox-artificial-intelligence-presented, E.T. 14.04.2024)

Avrupa Konseyi: Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680afb11f, E.T. 21.05.2024)

AWAN Abid Ali: *What is Superalignment & Why It is Important?*, Kdnuggets, (https://www.kdnuggets.com/2023/07/superalignment-important.html, E.T. 14.03.2024).

BABİKİAN John: *Beyond Borders: International Law and Global Governance in the Digital Age*, Law Research Journal, Vol. 1, Y. 2024 (https://jabarreview.com/index.php/Journal/article/view/16/17, E.T. 18.04.2024).

BARNETT Peter / GİLLEN Jeremy: *Without Fundamental Advances, Misalignment and Catastrophe are the Default Outcomes Of Training Powerful AI*, Machine Intelligence Research Institute, Y. 2024 (https://intelligence.org/wp-content/uploads/2024/02/Misalignment_and_Catastrophe.pdf, E.T. 18.04.2024).

BEBESHKO B. / KHOROLSKA K. / KOTENKO N. / DESIATKO A. / SAUANOVA K. / SAGYNDYKOVA S. / TYSHCHENKO D.: *3d Modelling By Means Of Artificial Intelligence*, Journal of Theoretical and Applied Information Technology, Vol. 99, No. 6, Y. 2021 (https://www.jatit.org/volumes/Vol99No6/5Vol99No6.pdf, E.T. 17.04.2024).

BHAT Jagadeesha R. / ALQAHTANİ Salman A.: *6G Ecosystem: Current Status and Future Perspective*, *IEEE Access*, Vol. 9, Y. 2021 (https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9335927, E.T. 18.04.2024).

Birleşmiş Milletler: Sürdürülebilir Kalkınma Araçları (https://turkiye.un.org/tr/sdgs/1, E.T. 14.04.2024)

BODİMANİ Meghasai: *Assessing The Impact of Transparent Ai Systems in Enhancing User Trust and Privacy*, Journal of Science & Technology, Vol. 5, Y. 2024 (https://www.thesciencebrigade.com/jst/article/view/68/116, E.T. 18.04.2024).

BREWER Jordan / PATEL Dhru / KİM Dennie / MURRAY Alex: *Navigating The Challenges Of Generative Technologies: Proposing The Integration Of Artificial Intelligence And Blockchain*, Business Horizons, Y. 2024 (, E.T. 18.04.2024).

BUİTEN Miriam C: *Towards Intelligent Regulation of Artificial Intelligence*, European Journal of Risk Regulation, Vol. 10, Y. 2019 (doi:10.1017/err.2019.8, E.T. 17.04.2024)

CAMACHO Nicolas Guzman, The Role of AI in Cybersecurity: Addressing Threats in the Digital Age, Journal of Artificial Intelligence General Science (JAIGS), ISSN: 3006-4023 (Online), Vol. 3, Y. 2024, s. 148, 149 (https://ojs.boulibrary.com/index.php/JAIGS/article/view/75/46, E. T. 22.05.2024)

CARRİLLO Margarita Roble: *Artificial Intelligence: From ethics to law*, Telecommunications Policy, Vol. 44, Y. 2020 (https://doi.org/10.1016/j.telpol.2020.101937, E.T. 16.03.2024)

CHAMBERLAİN Johanna: *The Risk-Based Approach of the European Union's Proposed Artificial Intelligence Regulation: Some Comments from a Tort Law Perspective*, European Journal of Risk Regulation, S. 14, Y. 2023 (doi:10.1017/err.2022.38, E.T. 17.04.2024)

CHHETRİ Parbat: *Internet of Things in Libraries: A SWOT Analysis*, Library and Information Science Links Newsletter, Vol. 6, Y. 2020 (http://file.lislinks.com/newsletter/lislinks-newsletter-vol-6-no-1-p-10-17.pdf, E.T. 18.04.2024).

CRUZ Bruno Ramos / PEREZ Javier Andreu / MARTÍNEZ Luis: *The cybersecurity mesh: A comprehensive survey of involved artificial intelligence methods, cryptographic protocols and challenges for future research*, Neurocomputing, Vol. 581, Y. 2024 (https://www.sciencedirect.com/science/article/pii/S092523122400198X, E.T. 11.03.2024).

DELLERMANN Dominik / EBEL Philipp / SÖLLNER Matthias / LEİMEİSTER Jan Marco: *Hybrid Intelligence*, Business & Information Systems Engineering, Vol. 61, Y. 2019 (https://doi.org/10.1007/s12599-019-00595-2, E.T. 13.03.2024)

DİLBAZ Berna / KAPLANOĞLU Mustafa / KAYA KAPLANOĞLU Dilek: *Teletıp ve Telesağlık: Geçmiş, Bugün ve Gelecek*, Eurasian Journal of Health Technology Assessment, S. 4 (1), Y. 2020.

FEUERRİEGEL Stefan / HARTMANN, Jochen / JANİESCH Christian / ZSCHECH Patrick: "Generative AI", Business & Information Systems Engineering, Vol. 66, Y. 2024 (https://doi.org/10.1007/s12599-023-00834-7, E.T. 17.04.2024)

FULİ Zhou / KANGZHEN Yu / WEİ Xie / JİEYİN Lyu / ZHONG Zheng / SHOUQIN Zhou: *Digital Twin-Enabled Smart Maritime Logistics Management in the Context of Industry 5.0*, IEEE Access, Vol. 12, Y. 2024, (https://ieeexplore.ieee.org/ document/10401169, E.T. 12.02.2024).

GAUMOND Eve: *Artificial Intelligence Act: What Is The European Approach for AI?,* Lawfare, Y. 2021 (https://www.lawfareblog.com/artificial-intelligence-act-what-european-approach-ai, E.T. 11.03.2024)

GİLLİS Alexander S.: *Internet of Things (IoT)* (https://www.techtarget.com/ iotagenda/definition/Internet-of-Things-IoT, E.T: 11.02.2024).

GİUDİCİ Paolo / CENTURELLİ Mattia / TURCHETTA Stefano: *Artificial Intelligence risk measurement*, Expert Systems with Applications, Vol. 235, Y. 2024 (https://doi.org/10.1016/j.eswa.2023.121220, E.T. 18.04.2024).

GÖLLNER Sabrina / TROPMANN-FRİCK Marina / BRUMEN Bostjan: *Towards a Definition of a Responsible Artificial Intelligence*, Information Modelling and Knowledge Bases XXXV, Vol. 380, Y. 2024 (https://ebooks.iospress.nl/doi/10.3233/FAIA231146, E.T. 18.04.2024).

GREENSTEİN Stanley: *Preserving the rule of law in the era of artificial intelligence (AI)*, Artifcial Intelligence and Law, Vol. 30, Y. 2022 (https://doi.org/10.1007/s10506-021-09294-4, 18.04.2024)

GUENDUEZ Ali A. / METTLER Tobias: *Strategically constructed narratives on artificial intelligence: What stories are told in governmental artificial intelligence policies?*, Vol. 40, Y. 2023 (https://doi.org/10.1016/j.giq.2022.101719, E.T. 21.05.2024).

HEAVEN Will Douglas, Now we know what OpenAI's superalignment team has been up to, MIT Technology Review, Y. 2023 (https://www.technologyreview. com/2023/12/14/1085344/openai-super-alignment-rogue-agi-gpt-4/, E.T. 15.03.2024).

HOLLAND Oliver / STEİNBACH Eckehard / PRASAD R. Venkatesha / LİU Qian / DAWY Zaher / AİJAZ Adnan / PAPPAS Nikolaos / CHANDRA Kishor / RAO Vijay S. / OTEAFY Sharief / EİD Mohamad / LUDEN Mark / BHARDWAJ Amit / LİU Xun / SACHS Joachim / ARAÚJO José: *The IEEE 1918.1 "Tactile Internet" Standards Working Group and its Standards IEEE*, Vol. 107, Y. 2019 (https://ieeexplore.ieee.org/abstract/document/8605315, E.T. 23.03.2024).

International Organization for Standardization: *Cyber-vulnerability* (https://www.iso.org/foresight/tech-risks.html, E.T. 21.05.2024)

International Organization for Standardization: *Data privacy* (https://www.iso.org/foresight/tech-risks.html, E.T. 21.05.2024)

International Organization for Standardization: Ethics of technology (https://www.iso.org/foresight/tech-risks.html, E.T. 21.05.2024)

International Organization for Standardization: *ISO 12100:2010(en) Safety of machinery - General principles for design - Risk assessment and risk reduction* (https://www.iso.org/obp/ui/en/#iso:std:iso:12100:ed-1:v1:en, E.T. 15.03.2024).

International Organization for Standardization: *ISO/IEC 22989:2022(en) Information technology - Artificial intelligence - Artificial intelligence concepts and terminology* (https://www.iso.org/obp/ui/en/#iso:std:iso-iec:22989:ed-1:v1:en, E.T. 09.03.2024).

International Organization for Standardization: *ISO/IEC 23053:2022(en) Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML)* (https://www.iso.org/obp/ui/en/#iso:std:iso-iec:23053:ed-1:v1:en, E.T. 07.03.2024).

International Organization for Standardization: *ISO/IEC 23894:2023(en) Information technology - Artificial intelligence - Guidance on risk management* (https://www.iso.org/obp/ui/en/#iso:std:iso-iec:23894:ed-1:v1:en, E.T. 07.03.2024).

International Organization for Standardization: *ISO/IEC 24029-2:2023(en) Artificial intelligence (AI) - Assessment of the robustness of neural networks - Part 2: Methodology for the use of formal methods* (https://www.iso.org/obp/ui/en/#iso:std:iso-iec:24029:-2:ed-1:v1:en, E.T. 08.03.2024).

International Organization for Standardization: *ISO/IEC 24668:2022(en) Information technology - Artificial intelligence - Process management framework for big data analytics* (https://www.iso.org/obp/ui/en/#iso:std:iso-iec:24668:ed-1:v1:en, E.T. 07.03.2024).

International Organization for Standardization: *ISO/IEC 25010:2023(en) Systems and software engineering - Systems and software Quality Requirements and Evaluation (SQuaRE) - Product quality model* (https://www.iso.org/obp/ui/en/#iso:std:iso-iec:25010:ed-2:v1:en, E.T. 16.03.2024).

International Organization for Standardization: *ISO/IEC 27031:2011(en) Information technology - Security techniques - Guidelines for information and communication technology readiness for business continuity* (https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27031:ed-1:v1:en, E.T. 16.03.2024).

International Organization for Standardization: *ISO/IEC 38505-1:2017(en) Information technology - Governance of IT - Governance of data - Part 1: Application of ISO/IEC 38500 to the governance of data* (https://www.iso.org/obp/ui/#iso:std:iso-iec:38505:-1:ed-1:v1:en, E.T. 09.04.2024).

International Organization for Standardization: *ISO/IEC 38507:2022(en) Information technology - Governance of IT - Governance implications of the use of artificial intelligence by organizations* (https://www.iso.org/obp/ui/en/#iso:std:iso-iec:38507:ed-1:v1:en, E.T. 09.03.2024).

International Organization for Standardization: *ISO/IEC 42001:2023(en) Information technology - Artificial intelligence - Management system* (https://www.iso.org/obp/ui/en/#iso:std:iso-iec:42001:ed-1:v1:en, E.T. 07.03.2024).

International Organization for Standardization: *ISO/IEC 5338:2023(en) Information technology - Artificial intelligence - AI system life cycle processes* (https://www.iso.org/obp/ui/en/#iso:std:iso-iec:5338:ed-1:v1:en, E.T. 09.03.2024).

International Organization for Standardization: *ISO/IEC 5339:2024(en) Information technology - Artificial intelligence - Guidance for AI applications* (https://www.iso.org/obp/ui/en/#iso:std:iso-iec:5339:ed-1:v1:en, E.T. 09.03.2024).

International Organization for Standardization: *ISO/IEC 8183:2023(en) Information technology - Artificial intelligence - Data life cycle framework* (https://www.iso.org/obp/ui/en/#iso:std:iso-iec:8183:ed-1:v1:en, E.T. 09.03.2024).

International Organization for Standardization: *ISO/IEC TR 24027:2021(en) Information technology - Artificial intelligence (AI) - Bias in AI systems and AI aided decision making* (https://www.iso.org/obp/ui/en/#iso:std:iso-iec:tr:24027:ed-1:v1:en, E.T. 09.03.2024).

International Organization for Standardization: *ISO/IEC TR 24028:2020(en) Information technology - Artificial intelligence - Overview of trustworthiness in artificial intelligence* (https://www.iso.org/obp/ui/en/#iso:std:iso-iec:tr:24028:ed-1:v1:en, E.T. 09.03.2024).

International Organization for Standardization: *ISO/IEC TR 24029-1:2021(en)Artificial Intelligence (AI) - Assessment of the robustness of neural networks - Part 1: Overview* (https://www.iso.org/obp/ui/en/#iso:std:iso-iec:tr:24029: -1:ed-1:v1:en, E.T. 08.03.2024).

International Organization for Standardization: *ISO/IEC TR 24368:2022(en) Information technology - Artificial intelligence - Overview of ethical and societal concerns* https://www.iso.org/obp/ui/en/#iso:std:iso-iec:tr:24368:ed-1:v1:en, E.T. 09.03.2024

International Organization for Standardization: *ISO/IEC TR 24372:2021(en) Information technology - Artificial intelligence (AI)- Overview of computational approaches for AI systems* (https://www.iso.org/obp/ui/en/#iso:std:iso-iec:tr:24372:ed-1:v1:en, E.T. 09.03.2024).

International Organization for Standardization: *ISO/IEC TR 5469:2024(en) Artificial intelligence - Functional safety and AI systems* (https://www.iso.org/obp/ui/en/#iso:std:iso-iec:tr:5469:ed-1:v1:en, E.T. 08.03.2024).

International Organization for Standardization: *ISO/IEC TS 4213:2022(en) Information technology - Artificial intelligence - Assessment of machine learning classification performance* (https://www.iso.org/obp/ui/en/#iso:std:iso-iec:ts:4213:ed-1:v1:en, E.T. 09.03.20224)

International Organization for Standardization: *ISO/TR 22100-5:2021(en) Safety of machinery - Relationship with ISO 12100 - Part 5: Implications of artificial intelligence machine learning* (https://www.iso.org/obp/ui/en/#iso:std:iso:tr:22100:-5:ed-1:v1:en, E.T. 09.03.2024).

International Organization for Standardization: *ISO/TR 9241-810:2020(en) Ergonomics of human-system interaction - Part 810: Robotic, intelligent and autonomous systems* (https://www.iso.org/obp/ui/en/#iso:std:iso:tr:9241:-810:ed-1:v1:en, E.T. 09.03.2024).

International Organization for Standardization: *Tech risks* (https://www.iso.org/foresight/tech-risks.html, E.T. 21.05.2024)

International Organization for Standardization: *What is deep learning?* (https://www.iso.org/artificial-intelligence#toc3, E.T. 16.03.2024).

İspanya Krallığı (2022), *21 Aralık 2022 tarih ve 28/2022 sayılı Kanun* (https://www.boe.es/buscar/doc.php?id=BOE-A-2022-21739, E.T. 14.04.2024).

İspanya Krallığı (2023), *8 Kasım 2023 tarihli ve 817/2023 sayılı Kraliyet Kararnamesi* (https://www.boe.es/boe/dias/2023/11/09/pdfs/BOE-A-2023-22767.pdf, E.T. 14.04.2024).

JANSSEN Marijn / BROUS Paul / ESTEVEZ Elsa / BARBOSA Luis S. / JANOWSKİ Tomasz: *Data governance: Organizing data for trustworthy Artificial Intelligence*, Government Information Quarterly, Vol. 37, Y. 2020 (https://doi.org/10.1016/j.giq.2020.101493, E.T. 16.03.2024).

JOWARDER Rafiul Azim, SAWGAT Jahan: Quantum computing in cyber security: *Emerging threats, mitigation strategies, and future implications for data protection,* World Journal of Advanced Engineering Technology and Sciences, C. 13(01), Y. 2024

JUN Yao / CRAİG Alisa / SHAFİK Wasswa / SHARİF Lule: *Artificial Intelligence Application in Cybersecurity and Cyberdefense*, (ed. Lv Zhihan), Hindawi, Vol. 2021, Y. 2021 (https://doi.org/10.1155/2021/3329581, E.T. 18.04.2024).

Kanada (2022), *Dijital Şart Uygulama Yasası* (https://ised-isde.canada.ca/site/innovation-better-canada/en/canadas-digital-charter/bill-summary-digital-charter-implementation-act-2020, E.T. 24.03.2024).

Kanada, *Yapay Zeka ve Veri Yasası Taslağı* (https://ised-isde.canada.ca/ site/innovation-better-canada/en/artificial-intelligence-and-data-act-aida-companion-document, E.T. 24.03.2024).

KARAKAŞ Sirel: *Prof. Dr. Sirel Karakaş Psikoloji Sözlüğü*, Y. 2017, (www.psikolojisozlugu.com, E.T. 13.03.2024).

Montréal Üniversitesi (2018), *Sorumlu Yapay Zeka Hakkında Montreal Bildirgesi* (https://montrealdeclaration-responsibleai.com/the-declaration/, E.T. 22.03.2024).

REY Eduardo Mosqueira / PEREİRA Elena Hernández / RÍOS David Alonso / BASCARÁN José Bobes / LEAL Ángel Fernández: *Human-in-the-loop machine learning: a state of the art*, Artifcial Intelligence Review, Y. 2023 (https://doi.org/10.1007/s10462-022-10246-w, E.T. 18.04.2024).

MUTAİRİ Muna B. Al / ATEEKİ Maha A. Al / MESHAL Alanoud I. Al / MUTAİRİ Faten B. Al / GEORGE Rhea / ALMUSHARRAF Ahlam: *An Exploratory Review Of National Strategies In AI: A Systematıc Revıew*, DCU&PNU MSc Business Administration Research Digest Y. 2023 (https://doras.dcu.ie/28421/2/DCU%26PNU%20Research%20Digest%20-%202023.pdf#page=34, E.T. 18.04.2024).

NAJJAR Reabal: *Digital Frontiers in Healthcare: Integrating mHealth, AI, and Radiology for Future Medical Diagnostics*, IntechOpen, Y. 2024 (https://www.intechopen.com/online-first/88984, E.T. 18.04.2024).

NEUMANN Oliver / GUİRGUİS Katharina / STEİNER Reto: *Exploring artificial intelligence adoption in public organizations: a comparative case study*, Public Management Review, Vol. 26, Y. 2024 (https://doi.org/10.1080/14719037.2022.2048685, E.T. 24.03.2024).

Oxford Üniversitesi, Oxford English Dictionary (https://www.oed.com, E.T. 18.04.2024).

PANCHANATHAN Sethuraman: *Envisioning the future of the AI research ecosystem*, *PNAS Nexus*, Vol. 3, Y. 2024 (https://doi.org/10.1093/pnasnexus/pgae021, E.T. 18.04.2024).

PAPYSHEV Gleb / YARİME Masaru: *The state's role in governing artificial intelligence: development, control, and promotion through national strategies*, Policy Design and Practice, S. 6, Y. 2023 (https://doi.org/10.1080/25741292.2022.2162252, E.T. 17.04.2024).

PATEL Kaushikkumar: *Ethical Reflections On Data-Centric AI: Balancing Benefits And Risks*, International Journal of Artificial Intelligence Research and Development (IJAIRD) Vol. 2, Y. 2024 (https://iaeme.com/MasterAdmin/Journal_ uploads/IJAIRD/VOLUME_2_ISSUE_1/IJAIRD_02_01_001.pdf, E.T. 18.04.2024)

LESLİE David / BURR Christopher / AİTKEN Mhairi / COWLS Josh / KATELI Michael / BRİGGS Morgan: *Artificial intelligence, human rights, democracy, and the rule of law: a primer*, The Council of Europe, Y. 2021 (https://doi.org/10.48550/arXiv.2104.04147, E.T. 18.04.2024).

PERRİER Elija: *The Quantum Governance Stack: Models of Governance for Quantum Information Technologies*, Digital Society, Vol. 1, Y. 2022 (https://doi.org/10.1007/s44206-022-00019-x, E.T. 17.04.2024).

RİNGE Wolf Georg / RUOF Christopher: *Regulating FinTech in the EU: the Case for a Guided Sandbox*, European Journal of Risk Regulation, Vol. 11, Y. 2020 (doi:10.1017/err.2020.8, E.T. 18.04. 2024).

ROMEO Nzanzu Katasohire / MAHANGUE Edson Bernardo C. / COSSA Aderito Eduardo / KAUR Mandeep / GOYAL Mayank Kumar / CHHABRA Megha, "Transforming Data into Behavioral Insights: A Review of the Internet of Behavior (IoB)", 2024 11th International Conference on Computing for Sustainable Global Deve-

lopment (INDIACom), New Delhi, India, 2024, s. 70-75 (10.23919/ INDIACom61295.2024.10498875, E.T. 22.05.2024)

Sanayi ve Teknoloji Bakanlığı ve CCBDO (2021), Ulusal Yapay Zeka Stratejisi, (https://cbddo.gov.tr/SharedFolderServer/Genel/File/TR-UlusalYZStratejisi2021-2025.pdf, E.T. 25.03.2024).

SCHOLTEN Travis L. / WİLLİAMS Carl J. / MOODY Dustin / MOSCA Michele / HURLEY William "whurley" / ZENG William J. / TROYER Matthias / GAMBETTA Jay M.: *Assessing the Benefits and Risks of Quantum Computers*, Cornell University arXiv, Y. 2024, (https://arxiv.org/pdf/2401.16317.pdf, E.T. 14.02.2024).

SELTEN Friso, KLİEVİNK Bram: *Organizing public sector AI adoption: Navigating between separation and integration*, Government Information Quarterly, Vol. 41,Y. 2024 (https://doi.org/10.1016/j.giq.2023.101885, E.T. 24.03.2024).

SİNGH Bhupinder / KAUNERT Christian: *Integration of Cutting-Edge Technologies such as Internet of Things (IoT) and 5G in Health Monitoring Systems: A Comprehensive Legal Analysis and Futuristic Outcomes*, GLS Law Journal, Vol. 06, Y. 2024 (https://glslawjournal.in/index.php/glslawjournal/article/view/123/109, E.T. 17.04.2024).

SOARES Nate / FALLENSTEİN Benja, *Aligning Superintelligence with Human Interests: A Technical Research Agenda*, Machine Intelligence Research Institute, Technical report 2014-8.

Soares Nate / FALLENSTEİN Benja: *Vingean Reflection: Reliable Reasoning for Self-Improving Agents,* Machine Intelligence Research Institute, Technical report 2015-2.

STROBEL Gero / BANH Leonardo / MÖLLER Frederik / SCHOORMANN Thorsten: *Exploring Generative Artificial Intelligence: A Taxonomy and Types*, Proceedings of the 57th Hawaii International Conference on System Sciences, Y. 2024 (https://scholarspace.manoa.hawaii.edu/server/api/core/bitstreams/fa9a6175-9ff2-4ad4-868e-fec5127cd430/content, E.T. 17.04.2024).

SWAYNE Matt: *How Would Room-Temperature Superconductors Change Quantum Computing?*, The Quantum Insider, Y. 2023 (https://thequantuminsider.com/2023/08/03/how-would-room-temperature-superconductors-change-quantum-computing/, E.T. 09.04.2024).

TAGDE Priti / TAGDE Sandeep / BHATTACHARYA Tanima / TAGDE Pooja / Chopra Hitesh / Akter Rokeya / Kaushik Deepak / Rahman Md. Habibur: *Blockchain and artificial intelligence technology in e-Health*, Environmental Science and Pollu-

tion Research, Vol. 28, Y. 2021 (https://doi.org/10.1007/s11356-021-16223-0, E.T. 18.04.2024).

THOMAS John J.: *From principles to actions: building a holistic approach to AI governance* (https://www.ibm.com/blog/from-principles-to-actions-building-a-holistic-approach-to-ai-governance/, E.T. 13.12.2023).

TRUBY Jon / BROWN Rafael Dean / IBRAHİM Imad Antoine / PARELLADA Oriol Caudevilla: *A Sandbox Approach to Regulating High-Risk Artificial Intelligence Applications*, European Journal of Risk Regulation, Vol. 13 Y. 2022 (doi:10.1017/err.2021.52, E.T. 18.04.2024).

TUBİTAK (2023), 1007 Programı Yapay Zekâ Alanında Kamu Yapay Zekâ Ekosistem, (https://tubitak.gov.tr/tr/duyuru/1007-programi-yapay-zeka-alaninda-kamu-yapay-zeka-ekosistem-2023-cagrisi-sonuclari-aciklandi, E.T. 25.03.2024).

TUBİTAK (2023), Türkiye Bilimsel ve Teknolojik Araştırma Kurumu Kamu Kurumları Araştırma ve Geliştirme Projelerini Destekleme Programı (https://tubitak.gov.tr/sites/default/files/1776/1007-cbddo-2023-01_0.pdf, E.T. 25.03.2024).

TURNER Sarah / TANCZER Leonie Maria: *In principle vs in practice: User, expert and policymaker attitudes towards the right to data portability in the internet of things*, Computer Law & Security Review, Volume 52, 2024 (https://doi.org/10.1016/j.clsr.2023.105912, E.T. 18.04.2024).

TÜRK Tarık / ÖCALAN Taylan: *PPK GNSS Sistemine Sahip İnsansız Hava Araçları İle Elde Edilen Fotogrametrik Ürünlerin Doğruluğunun Farklı Yaklaşımlarla İrdelenmesi*, Türkiye Fotogrametri Dergisi, S. 2(1), Y. 2020.

TÜRK Tarık / TUNALIOĞLU Nursun / ERDOĞAN Bahattin / ÖCALAN Taylan / GÜRTÜRK Mert: *Accu-racy assessment of UAV-post-processing kinematic (PPK) and UAV-traditional (with ground control points) georeferencing methods*, Environmental Montoring And Assessment, C. 194(7), Y. 2022 (https://doi.org/10.1007/s10661-022-10170-0).

TÜRK Tarık / TUNALIOĞLU Nursun / ÖCALAN Taylan / GÜRTÜRK Mert: *Investigation of accuracy of PPP and PPP-AR methods for direct georeferencing in UAV photogrammetry*, Earth Science Informatics, C. 15(4), Y. 2022.

USOM, (https://www.usom.gov.tr/hakkimizda, E. T. 22.05.2024).

VİNGE Vernor: *The Coming Technological Singularity: How to Survive in the Post-Human Era*, In Vision 21, Interdisciplinary Science and Engineering in the Era of Cyberspace, 11–22. NASA Conference Publication 10129. NASA Lewis Research Center, Y. 1993 (https://ntrs.nasa.gov/api/citations/19940022856/downloads/19940022856.pdf, E.T. 18.04.2023).

VİNGE Vernor: True Names, Y. 1981.

WANG Zongyan, Digital Twin Technology, IntechOpen, Y. 2020 (https://www.intechopen.com/chapters/63861 E.T. 12.02.2024)

WİJAYA Eric / CHRİSTİAN Jonathan / VENNA Carla / ROWAN Jennie / SURACHMAN Ivan / Sellyna / OKTAVİA Tanty: *Examining The Efficacy Of The Internet Of Behaviour (IoB) In The Identification Of Client Needs On Electronic Commerce Platforms*, Journal of Theoretical and Applied Information Technology, Vol. 102, Y. 2024.

World Economic Forum (2022), Quantum Computing Governance Principles Insıght Report (https://www3.weforum.org/docs/WEF_Quantum_Computing_2022.pdf, E.T. 25.12.2023).

World Economic Forum (2022), Quantum Computing Governance Principles, (https://www.weforum.org/publications/quantum-computing-governance-principles/ E.T. 25.12.2023).

YUDKOWSKY Eliezer / HERRESHOFF Marcello, *Tiling Agents for Self-Modifying AI, and the Löbian Obstacle*, Early Draft MIRI, Y. 2013, (https://intelligence.org/files/TilingAgentsDraft.pdf, E.T. 18.04.2024).

ZİELKE Thomas: *Is Artificial Intelligence Ready for Standardization?*, (Ed: YILMAZ Murat / NİEMANN Jörg / CLARKE Paul / MESSNARZ Richard), Systems, Software and Services Process Improvement, 27th European Conference, EuroSPI, CCIS Vol. 1251, Y. 2020 (https://link.springer.com/chapter/10.1007/978-3-030-56441-4_19, E.T. 16.03.2024)

kvkkurumu

KVKK
KİŞİSEL VERİLERİ KORUMA KURUMU

Kişisel Verileri Koruma Kurumu

Nasuh Akar Mahallesi 1407. Sokak
No.4 06520 Çankaya | ANKARA

T. 0312 216 50 00

www.kvkk.gov.tr

9 786253 772123

adalet