TAAD Yıl 15 . Sayı 57 . Ocak 2024
ISSN 1309-6826
Araştırma Makalesi/Research Article
DOI: 10.54049/ taad.1418236

GENEL VERİ KORUMA İLKELERİNİN YAPAY ZEKÂ KARŞISINDA UYGULANABİLİRLİĞİ SORUNU

The Dilemma of Implementing General Data Protection Principles in the Realm of Artificial Intelligence

Ezgi TURGUT BİLGİÇ*

Özet

Yapay zekâ günümüzün en merak uyandırıcı ve üzerinde en dikkatli düşünülmesi gereken konularından biri haline gelmiştir. Bunun sebebi yapay zekânın etki alanının genişliği, hukuktan psikolojiye, felsefeden matematiğe ve ekonomiye çok çeşitli disiplinler ile ilişkilerinin olmasıdır. Yapay zekâ bugün sağlık, bilişim, ticaret, lojistik, çevre gibi pek çok alanda fayda sağlamakta rekabetçi ekonominin bir unsuru olmaktadır. Büyük veri kümelerini işleyen, veri ile beslenen bir çatı kavram olarak yapay zekâ, makine öğrenmesi ve derin öğrenme yöntemleri ile birlikte kişisel verilerin korunması konusunda bazı endişelere yol açmaktadır. Zira yapay zekânın kullanımının yaygınlaşması, kişisel veriler açısından yenilikleri de beraberinde getirmektedir. Yapay zekânın ön yargılı veya yanlış sonuçlar doğurduğu örnekler, bir taraftan çeşitli kaygılara sebep olurken diğer taraftan veri korumaya ilişkin demirbaş kabul edilen temel kuralları yerinden sarsmaktadır. Çalışmada yapay zekânın veri koruma hukukundaki şeffaflık, doğruluk, veri minimizasyonu gibi genel ilkelere olan etkisi, Avrupa Birliği Genel Veri Koruma Tüzüğü odağa alınarak incelenmiş, genel ilkelerin dönüşümünün ve olası çözümlerin gerekliliği vurgulanmıştır. Bunu yaparken yapay zekânın, makine öğrenmesinin ve derin öğrenmenin kapsamı, genel ilkelerin yapay zekâ karşısında sebep olduğu güncel çelişkiler ile uygulamadaki bazı çözüm önerileri ele alınmıştır.

Anahtar Kelimeler: Yapay zekâ, makine öğrenmesi, genel veri koruma ilkeleri, GDPR, AB Yapay Zekâ Tüzüğü, kara kutu problemi.

Abstract

Artificial intelligence has become one of the most intriguing and thought-provoking topics of our time. This is because of its breadth of influence, its diverse disciplines and contexts, from law to psychology, philosophy to mathematics, and economics. Today, artificial intelligence provides benefits in many fields such as health, informatics, trade, logistics and environment, and becomes an element of competitive economy. As a data-fed roof concept that processes large data sets, artificial intelligence, together with machine learning and deep learning methods, raises some concerns about the protection of personal data. Because the widespread use of artificial intelligence brings with it innovations in terms of personal data. Examples where artificial intelligence produces biased or wrong results, on the one hand, cause various concerns, on the other hand, it shakes the fundamental rules regarding data protection, which are accepted as fixtures. In the study, the effect of artificial intelligence on general principles such as

➢ *Bu makale Etik Kurul iznine tabi değildir/This article is not subject to Ethics Committee permission.*

➢ *Makale Geliş Tarihi/Article Received Date: 09.06.2023*

➢ *Yayın Kurulu Kabul Tarihi/Editorial Board Acceptance Date: 27.12.2023*

* Kişisel Verileri Koruma Kurumu-Uzman Yardımcısı, Hacettepe Üniversitesi Kamu Hukuku Doktroa Öğrencisi, ezgiturgut.int@gmail.com, https://orcid.org/0000-0001-9667-3637.

transparency, accuracy and data minimization in data protection law was examined by focusing on the GDPR, and the necessity of the transformation of general principles and possible solutions was emphasized. While doing this, the scope of artificial intelligence, machine learning and deep learning, current contradictions caused by general principles against artificial intelligence and some solution suggestions in practice are discussed.

Keywords: Artificial intelligence, machine learning, general data protection principles, GDPR, EU Artificial Intelligence Act, black box problem.

GİRİŞ

Yapay zekâ, modern çağın dikkate değer yeniliklerinden biridir. İnsan benzeri özelliklere sahip makinelerin soruları anında yanıtlayabilme ve problemleri hızla çözebilme kapasiteleri, önemli etkiler doğurmuştur. Yapay zekânın tarihsel yolculuğu günümüze ulaşmış ve hala sürmektedir. Bugün yapay zekâ bazı kanser türlerinin tespitinde hekimlerden daha başarılı olabilmekte[1], teknik çevresel önlemler alınmasında tespit ve tahmin çalışmaları yapmakta, eğitim aracı olarak kullanılmak suretiyle hem zamandan hem de ekonomik açıdan tasarruf sağlamakta, bilişim sektörüne hız getirmekte, kamusal makamlarca güvenliğin sağlanmasında ve suçlu takibinde etkili olabilmektedir. Bu denli işlevli bir aracın büyük bir ticari hacmi olduğu, kendi ekonomisini oluşturduğu, sermaye/güç biriktirme amaçlarına yeniden katkıda bulunduğu belirtilmelidir. Yapay zekânın piyasalara yansımasına dair 2021 ila 2030 yıllarını ele alan bir projeksiyona göre 2022'de 119,78 milyar ABD doları olan yapay zekâ pazarın büyüklüğü 2030'a kadar %38 civarında bir büyüme ile 1.591,03 milyar seviyelerine ulaşacaktır[2].

Belirtilen tablo karşısında, genişleyen bir veri koruma mevzuatının da konumlandığı belirtilmelidir. Özel hayatın gizliliğinin, mahremiyetin ve kişisel verilerin korunmasını amaçlayan bu mevzuat 1970'lerden itibaren gelişmiş, pek çok sektörü etkilemiştir. Özellikle Avrupa Birliği ("AB") tarafından düzenlenen bağlayıcı Genel Veri Koruma Tüzüğü ("GDPR"), kapsamlı ve yenilikçi olması ile öngördüğü para cezalarının caydırıcılığı açısından önemlidir. Kişisel verilerin korunmasına ilişkin getirilen kurallar, kuralların ruhunu taşıyan, uygulanmalarını kolaylaştıran birtakım temel prensipler barındırır. Genel veri koruma ilkeleri olarak ifade edilen "amaca odaklı, veri koruma ile amaçlanan bireysel çıkarları önceleyen" kurallar, OECD'nin "Özel Yaşamın Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkeleri"nde de 108 sayılı Sözleşme olarak bilinen Avrupa Konseyi düzenlemesinde de yaklaşık olarak -GDPR ile getirilen bazı yenilikler hariç- aynıdır. Bunun yanında 108 sayılı Sözleşme'nin yeni teknolojiler ve gelişmeler karşısında revize edilmiş hali olan ve 108+ olarak bilinen 2018 yılında kabul edilen "Kişisel

[1] The New York Times, "Using A.I. to Detect Breast Cancer That Doctors Miss" <https://www.nytimes.com/2023/03/05/technology/artificial-intelligence-breast-cancer-detection.html> (Erişim Tarihi: 31.07.2023)

[2] Precendence Research, "ICT Artificial Intelligence (AI) Market" <https://www.precedenceresearch.com/artificial-intelligence-market> (Erişim Tarihi: 31.07.2023)

Verilerin İşlenmesi Karşısında Bireylerin Korunması için Modernize Edilmiş Sözleşme"[3] kabul edilmiştir. Bu yeni ve yürürlüğe girmesi beklenen düzenlemede de genel ilkelere yer verilmiştir. Bahis konusu genel veri koruma ilkeleri GDPR'da yer alan haliyle "hukuka uygunluk, adillik ve şeffaflık", "amacın sınırlandırılması", "verilerin en az seviyeye indirilmesi ya da veri minimizasyonu", "doğruluk", "saklama süresinin sınırlandırılması", "verilerin bütünlük ve gizliliğinin sağlanması" ve "hesap verilebilirlik" tir.

Çalışma ile amaçlanan, kişisel veriler ile yapay zekâ arasındaki ilişkiyi, genel veri koruma ilkelerini temel alarak ifade etmek, bu ilkelerin yapay zekâ karşısında nasıl bir sınav verdiğini sorgulamak ve mevcut çelişkileri incelemektir. Bu sebeple kişisel veri ile yapay zekâ arasındaki bağlamı oluşturmak için çalışmanın ilk bölümünde yapay zekânın bir kavram olarak ele alınmasından başlayarak makine öğrenmesine ve derin öğrenmeye yer verilmiş, yapay zekânın kişisel verileri elde etme biçimi açıklığa kavuşturulmaya çalışılmıştır. Nitekim yapay zekânın genel ilkeler ve hatta tüm kişisel verileri koruma mevzuatı açısından yaratığı ikilemleri anlamak için sistem ile verilerin ayrılmaz bağının, verilere olan gereksinimin veya yapay zekânın kendisinin veriler üzerine kurulu olduğunun anlaşılması gerekir.

Çalışmanın ikinci bölümünde genel veri koruma ilkelerinin hangi yapay zekâ gerçekleri ile karşı karşıya olduğuna yer verilmiş, GDPR çerçevesinde genel ilkelerin kara kutu ("black box") sorunu, şeffaflık ve rıza ile ilgili zorluklar, amaç sınırlamasında potansiyel kaymalar, ön yargılı veya yanlış sonuç elde etme riski, silme taleplerinin anlamı ve etkisi, veri minimizasyonu ile meşru amaçlar arasındaki potansiyel çelişkiler gibi hususlara değinilmiştir. Son bölümde ise açıklanabilirlik, güvenilir yapay zekâ gibi yöntemler, yakın tarihte yürürlüğe girmesi planlanan taslak AB Yapay Zekâ Tüzüğü'nün ("EU Artificial Intelligence Act") genel işlevi ile bazı çözüm önerileri ele alınmıştır. Yapay zekâya ilişkin hukuki düzenlemeler, teknik gelişmeleri zorunlu kılması açısından oldukça önemlidir. Bunun yanında veri koruma alanındaki kurum/kuruluşların yapay zekâya ilişkin bağlayıcı olmayan düzenlemeler tercih ettikleri, ekonomik/ticari, toplumsal ve bireysel etkilerin dengelenmesi konusunun öne çıktığı, bu süreçte kişisel verilerin işlenmesinde genel ilkelerin uygulanmasının risk altında olabileceği fikri de çalışma kapsamında ele alınmıştır.

A. YAPAY ZEKÂ SİSTEMLERİ ve YAPAY ZEKÂ TARAFINDAN KİŞİSEL VERİ ELDE EDİLMESİ

1. Zekâ-Yapay Zekâ Ayrımı

Türk Dil Kurumu'nun zekâ tanımı *"İnsanın düşünme, akıl yürütme, objektif gerçekleri algılama, yargılama ve sonuç çıkarma yeteneklerinin tamamı, ahlak,*

[3] Council of Europe, "Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, Convention 108 and Protocols" <https://www.coe.int/en/web/data-protection/convention108-and-protocol> (Erişim Tarihi: 31.07.2023)

dirayet, zeyreklik, feraset"[4] şeklindedir. Bir diğer sözlükte ise kavram benzer olarak *"öğrenme, anlama ve yargıda bulunma veya akla dayalı görüşlere sahip olma yeteneği"*[5] olarak tanımlanmıştır. Ayrıca zekâ, geleneksel olarak, farklı entelektüel becerileri değerlendirmek için tasarlanmış bir dizi alt teste tabi tutulan aynı yaştaki bir grup bireyin performansını karşılaştıran ve bir indeksi temsil eden tek bir sayı -bir IQ- ile tanımlanır[6]. Zekâ bir dereceye kadar kişilerin karşılaştığı sosyal olaylardan da etkilenen, sosyal önemi haiz (sosyal rollerde başarılı olma yeteneği anlamında), bir kişinin karşılaşması muhtemel çevresel etkenlere tepki verme şeklini de etkileyen kalıtsal bir bileşendir[7]. Bu bilgiler ışığında zekânın, dış etkenler ile kısmen dönüşebilecek şekilde olgulardan anlam üretme kapasitesi olarak tanımlanması mümkündür.

Yapay zekâ ("Artificial Intelligence-AI") ise sözlük tanımında *"bilgisayarların veya diğer makinelerin akıllı davranışı sergileme veya simüle etme kapasitesi, bununla ilgili çalışma alanı"*[8] şeklinde ifade edilir. McCarty yapay zekâyı, akıllı makinelerin, özellikle akıllı bilgisayar programları yapma bilimi ve mühendisliği ile ilişkilendirerek tanımlar[9]. Makinelerin zekâsı insan zekâsından farklı olarak, sadece insan ve hayvanların yöntemlerini "gözlemleyerek" değil, dünyanın insan zekâsını sınadığı sorunları inceleyerek, daha fazla bilgi-işlem içeren yöntemleri kullanarak gelişir[10]. Böylece yapay zekâ, insan kullanımı ve programlaması gerektiren zor görevleri kendi kendine gerçekleştiren uygulamalar için kullanılan genel bir terim olarak karşımıza çıkmaktadır. Ayrıca genellikle makine öğrenmesi (Machine Learning/ML) ve derin öğrenmeyi ("Deep Learning-DL") içeren alt alanları da kapsayan şekilde tüm bu kavramlar birbirinin yerine kullanılabilmektedir[11].

IBM yapay zekâyı "*makineleri daha zeki yapabilecek olan her şey"* olarak tanımlar ve onun uzman insanların yerini almayıp insan kabiliyetlerini artıran ve insanlar ile makinelerin tek başına yapamayacakları görevleri gerçekleştiren bir araç olduğunu vurgular[12]. Kendisine yeni bilgi verilmesiyle çeşitli algoritmik işlemlerle öğrenen ve verinin içerisindeki yapıyı anlayan, tanımlayabilen ve bu sü-

---

4 Türk Dil Kurumu, "zekâ" <https://sozluk.gov.tr/> (Erişim Tarihi: 31.07.2023)

5 Cambridge Dictionary, "intelligence" <https://dictionary.cambridge.org/dictionary/english/intelligence> (Erişim Tarihi: 31.07.2023)

6 Nathan Brody, "What is Intelligence?" (1999) 11(1) International Review of Psychiatry 19.

7 Ibid 25.

8 Oxford English Dictionary, "artificial intelligence" <https://www.oed.com/viewdictionaryentry/Entry/271625> (Erişim Tarihi: 31.07.2023)

9 John McCarthy, "What is Artificial Intelligence?" (Computer Science Department, Stanford University, 2007) <http://www-formal.stanford.edu/jmc/>, 2 (Erişim Tarihi: 31.07.2023)

10 Ibid.

11 Andrew Glassner, Deep Learning: A Visual Approach (No Starch Press 2021) 3.

12 IBM, "What is artificial intelligence (AI)?" <https://www.ibm.com/topics/artificial-intelligence> (Erişim Tarihi: 31.07.2023)

reçlerin sonunda bir çıktı/sonuç üretebilen yapay zekâ, insan zekâsını simüle eden bir şey değildir. Onun yerine insan zekâsına benzer bir işleyiş kullanarak yüksek hız ve kapasitede veri işleme faaliyeti yürütür. Algoritmalar veya olasılık hesapları ile işleyen yapay zekâ, güç, genişlik ve uygulamaya dayalı olarak farklı şekillerde tasnif edilir. Aynı zamanda, insan zekâsına benzer çalışma prensibine göre modellendiği için pek çok farklı alan ile iç içedir.

2. Kısa Tarihsel Gelişim

Yapay zekânın tarihi, antik dönemlere kadar geçmişe giden bir izlekten ifade edilir[13]. Bu tarihsel yolculukta, otonom varlıklar konseptinin ilk kez ortaya çıktığı Homeros destanları, Aristoteles'in kıyas ("silojistik-syllogistic") mantığı, İskenderiyeli Heron'un otomataları, 1642'de Pascal'ın mekanik hesap makinesi, 1664'te Descartes'in bazı zihin problemlerine dair kodlamaları, 1890'da bilgiyi delikli kartlara kodlayan makineler kullanarak ABD nüfus sayımının gerçekleştirilmesi, 1923'te robot kelimesinin Capek'in "Rossum's Universal Robots" adlı oyunu ile İngilizce'ye girmesi, 1937'de Turing'in soyut bir evrensel hesaplama makinesi önerisi gibi pek çok gelişme vardır[14].

1957'de Rosenblatt tarafından geliştirilen perceptron[15] da ("tek katmandan oluşan sinir ağı modellemesi-algılayıcı") makine öğrenmesi için önemli bir eşik kabul edilir. İlk endüstriyel robot şirketi olan Unimation'un 1962'de kurulması, ilk kez Stanford Üniversitesi'nde yapay zekâ konferansı düzenlenmesi, 1997 yılına gelindiğinde ise IBM'in Deep Blue adını verdiği yapay zekâ programının oynadıkları satranç maçında Dünya satranç şampiyonu Kasparov'u yenmesiyle yapay zekânın gelişimi gözler önüne serilmiştir[16]. 2000'li yılların başından itibaren yapay zekânın birden çok alanda uygulanmasına yol açan "büyük veri çağı" ortaya çıkmış, Amazon ve Netflix gibi şirketler, müşterilere ürün veya film önermek için yapay zekâ algoritmalarıyla önerilerde bulunmaya başlamış, yapay zekâ artan şekilde sağlık hizmetlerine de girmiştir. COVID-19 salgınıyla mücadelede sağlık hizmetlerinin uzaktan sağlanması için dijital sağlık platformlarında da yapay zekâya başvurulmuştur.

AB istatistiklerine göre 2021 yılında büyük AB işletmelerinin %28'inin yapay zekâ teknolojilerini kullandığı, yapay zekânın en çok "bilgi ve iletişim sektörü"ndeki işletmeler tarafından kullanıldığı, AB işletmelerinin %53'ünün kulla-

---

13 Pamela McCorduck, "Machines Who Think: A Personal Inquiry into the History and Prospects of Artificial Intelligence" (2nd edn, A K Peters 2004) xxii.

14 Ibid xxiv, xxv. Ayrıca bkz. Alan M Turing, "Computing Machinery and Intelligence" (1950) 59(236) Mind, New Series, 433-460.

15 Frank Rosenblatt, "The Perceptron: A Probabilistic Model for Information Storage and Organization in the Brain" (1958) 65(6) Psychological Review 386.

16 TR AI, "Yapay Zekâ Zaman Çizelgesi" <https://turkiye.ai/kaynaklar/yapay-zekâ-zaman-cizelgesi/> (Erişim Tarihi: 31.07.2023)

nıma hazır ticari yapay zekâ yazılımlarını satın aldığı belirtilir[17]. OpenAI isimli derin öğrenme yöntemiyle işleyen üretken yapay zekâ ("generative AI") modelleri oluşturan şirket, 2020'de tanıttığı GPT-3 adlı API ile ("Application Programming Interface-Uygulama Programlama Arayüzü") metin girişi ve metin çıkışı şekilde işleyen modelini piyasaya sürmüştür. 2023 yılında gelişmiş modeli olan GPT-4 piyasaya arz edilmiş, böylece sadece metin değil aynı zamanda görüntü girişlerini de kabul eden, profesyonel ve akademik ölçütlerde daha yüksek düzeyde performans sergileyen bir model oluşturulmuştur[18].

Hızlı bir şekilde gelişen ve hemen her sektöre etki eden yapay zekâ teknolojisi, güvenli ve temiz ulaşım, daha verimli üretim, daha ucuz ve sürdürülebilir enerji gibi modern yaşam için elzem olan alanlardan, görüntü tanıma yazılımı, sanal asistanlar, konuşma ve yüz tanıma sistemleri veya cihazlara gömülü şekilde otonom robotlar, sürücüsüz araçlar, dronlar, sağlık, iklim modelleme/simülasyon, karbon azaltma stratejileri üretme gibi alanlarda anlamlı sonuçlar doğurmaktadır. Bugün yapay zekânın üçüncü aşaması olarak bilinen Süper Yapay Zekâ ("Artificial Super Intelligence-ASI") çalışmaları yapılmakta, modellerin yüksek hızda verdikleri çıktıların sonuçlarını gerekçeli şekilde açıklayabildiği bir düzey yakalanmaya çalışılmaktadır[19].

3. Yapay Zekâ'nın Sınıflandırılması

Yapay zekâ yapı, davranış, yetenek, işlev ve ilke özelliklerine göre değerlendirilen beş kategoriye ayrılır[20]. Yapısına göre ayrıma tabi tutulan yapay zekâyı ("Structure-AI") öne çıkaran husus, nöron benzeri işlem birimlerinden oluşan ve insan beynini andıran bir yapı oluşturarak sonuçlar elde etmeye çalışmasıdır. Bu tür yapay zekâ makine öğrenmesi ve yapay sinir ağları gibi teknikler kullanır. Davranışa göre ayrılan yapay zekânın ("Behavior-AI") odağında ise sistem davranışları vardır. Bu durum Turing testleri veya Chatbot'lar gibi yapay zekânın insan benzeri bir şekilde nasıl davranabileceği gösteren uygulamalarda görülebilir. Yeteneğe/kapasitesine göre yapay zekâ ("Capability-AI") sistemin zekâsını ve zor problemleri çözme kabiliyetini ölçer. İşleve göre yapay zekâ ise ("Function-AI") araştırmacılara belirli bir girdiyi belirli bir çıktıya nasıl eşleyeceğini göstererek bir çeşit aracı olarak yapay zekânın ne şekilde işlev gördüğünü anlamamızı sağlar. Son olarak ilkeye göre yapay zekâ ("Principle based-AI") çeşitli durumlarda bilgi

---

17 Eurostat, "Use of artificial intelligence in enterprises" <https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Use_of_artificial_intelligence_in_enterprises> (Erişim Tarihi: 31.07.2023)

18 OpenAI, gpt-4 <https://openai.com/research/gpt-4> (Erişim Tarihi: 31.07.2023)

19 Yapay zekânın gelişim evrelerini göstermesi ve Süper Yapay Zekâ hakkında daha detaylı bilgi için: Bing Zhang, Jing Zhu and Huimin Su, "Toward the Third Generation Artificial Intelligence" (2023) 66(2) Sci China Inf Sci 1-19.

20 Pei Wang, "What Do You Mean by AI?" (2008) 171 Frontiers in Artificial Intelligence and Applications 365-366-367.

işlemeyi inceler, farklı varsayımları ve onların sonuçlarını öngörmeyi sağlar[21].

Yapay zekânın kapasitesine göre dar ("Artificial Narrow Intelligence-ANI"), genel ("Artificial General Intelligence-AGI") ve süper/güçlü ("Artificial Super/ Strong Intelligence-ASI") şeklinde teorik bir ayrımı da söz konusudur. Dar yapay zekâ sınırlı belleğe ve belirli hedeflere yönelik, tek bir rolde hareket edebilen, soyutlama kapasitesi düşük, kendi kendine öğrenebildiği bir veri tabanından yoksun ve karar verme, optimizasyon veya arama sorunları nedeniyle her zaman uzman bilgisine dayalı bir türdür[22]. Örnek olarak Alexa veya Siri gibi sanal asistanlar, otonom araç sistemleri, e-posta spam filtreleri veya kişisel internet aramalarına dayanarak oluşturulan reklam önerileri verilebilir. Genel yapay zekâ ise insana benzer biçimde farklı senaryolarda otonom karar verme, insan beyni süreçlerini makinede simüle etme, farklı ihtiyaçları, süreçleri ve hatta duyguları tespit etme gibi yeteneklere sahip olduğundan, yapay sinir ağları-derin öğrenme yöntemlerini kullanır[23].

4. Makine Öğrenmesi ile Kişisel Veri Elde Edilmesi

a. Makine Öğrenmesi

Makine öğrenmesi, insanlar tarafından açıkça programlanmadan otomatik olarak, kendi kendine öğrenme ve deneyim geliştirerek gelişme yeteneği elde ederek yapay zekânın kapsamı içinde yer alan bir yöntemdir. Verilere erişebilen ve bunları kendi çalışması için kullanabilen bilgisayar programlarının geliştirilmesinde kullanılan makine öğrenmesi, "sezgisel analiz", deneme-yanılma gibi yöntemler kullanır[24]. Öğrenme süreci ise kendisine sunulan verilerdeki belirli kalıpları/olguları aramak, bir veri kümesini en iyi şekilde temsil eden algoritmalar geliştirmek diğer deyişle yeni veya farklı özellik ve ağırlık kombinasyonları kullanabilen bir algoritma oluşturmak için veri alt kümelerini kullanmak şeklindedir.

Algoritma basit bir şekilde, bilgisayardan veriler üzerinde çalışması sonucu bir çıktı almak için verilen kurallar bütünü, verilerin nasıl işleneceğini gösteren yöntemdir. Dolayısıyla makine öğrenmesiyle, klasik programlamada olan insanın çeşitli kurallar ve sınıflandırmalar kullanarak elle kodlama yapması, bilgisayara bir veri seti ve algoritma sunması durumu yoktur. Sisteme bir veri seti yani "girdi" verilir ve alınmak istenen "çıktı" belirtilir. Algoritma çeşitli analizler/hesaplamalar yaparak bu çıktıyı kendisi üretir. İşte bu noktada girdi şekilde sunulan verilerin içinde pek tabii kişisel veri bulunabileceği gibi algoritma işleyişiyle çıktı olarak verilen sonuçlarda da kişiler ile ilişkilendirilebilen veriler de bulunmaktadır.

---

21 Ibid.

22 Zhang, Zhu and Su (n 19) 1-3.

23 Ibid 3-4-5.

24 Mustafa Serdar Çekin, Yapay Zekâ Teknolojilerinin Hukuki İşlem Teorisine Etkileri (1. Baskı) (İstanbul: onikilevha, 2021) 13.

Makine öğrenmesinde algoritmanın işleyişini ifade edecek şekilde denetimli, denetimsiz, yarı denetimli ve takviyeli öğrenme yöntemleri vardır. Genellikle regresyon ve sınıflandırma problemlerine uygulanan denetimli ("supervised") öğrenmede, örnek girdi-çıktı çiftlerine dayalı olarak bir girdiyi çıktıya eşleyen bir işlev öğrenilir, veri setine bir fonksiyonun belirli bir tahminde hatayı hesaplayabilmesi için istenen çıktılar veya etiketler girilir (verinin karşılığı biliniyor)[25]. Verilecek çıktının bilinmesi yani veri kümelerinin etiketlenmesi, işlevi değiştirmek ve eşlemeyi öğrenmek için bir tahmin yapıldığında ve bir hata üretildiğinde işe yaramış olur[26]. Denetimsiz ("unsupervised") öğrenmede bundan farklı olarak etiketli girdi-çıktı bilgileri olmadan girdi verilerinden çıkarımlar yapılır. Sistem kendisine sunulan veriler arasındaki örüntüyü kendisi keşfederek tahminine dayalı bir sonuca varır.

Pekiştirmeli öğrenme ise bir yapay zekâ algoritmasının belirli bir hedefe ulaşmak için hangi eylemleri gerçekleştirmesi gerektiğini öğrenmeye çalıştığı bir tekniktir. Ancak denetimli öğrenmede olduğu gibi her aşamada geri bildirim almak yerine, pekiştirmeli öğrenme algoritması genellikle hedefe ulaştığında bir "pekiştirme sinyali" alır. Bu yöntem işleyişi itibarıyla bir ödül-ceza sistemine benzer. Algoritma, hedefe ulaşmak için doğru eylemleri gerçekleştirdiğinde ödül alır. Yanlış bir eylem gerçekleştirdiğinde-yani hata yaptığında- olumsuz bir geri bildirim alır. Bu süreç, algoritmanın doğru eylemleri tekrar etme ve hatalardan kaçınma eğilimini artırır, böylece zamanla daha iyi performans elde edilir[27].

b. Derin Öğrenme ve Yapay Sinir Ağları

Derin Öğrenme, makine öğrenmesi ve yapay zekânın kapsamı altında Dördüncü Sanayi Devrimi'nin ("4IR veya Endüstri 4.0") temel teknolojisi olarak kabul edilmektedir[28]. Verilerden öğrenme yetenekleri ve kapasiteleri nedeniyle yapay sinir ağlarından ("Deep Neural Networks") yararlanan derin öğrenme yöntemi bugün sağlık, siber güvenlik, yüz tanıma, model geliştirme ve sair pek çok alanda uygulamalı olarak kullanılmaktadır. Derin öğrenme, insan beyninin sinir ağı hücrelerinden ilham alan algoritmalara dayalı bir tür makine öğrenmesi biçimidir. Doğru tahminler üretmek için büyük hacimdeki verileri kümelere ayırarak insan beynini deyim yerindeyse taklit ederek işler.

Yapay sinir ağlarında biyolojik sinir ağlarındaki akson, dendrit ve hücre gövdelerine benzeyen şekilde düğümler bulunur ve iletişim de bu düğümler üzerinden

---

[25] Robert Y Choi, Aaron S Coyner, Jayashree Kalpathy-Cramer, Michael F Chiang and J Peter Campbell, "Introduction to Machine Learning, Neural Networks, and Deep Learning" (2020) 9(2) Trans Vis Sci Tech 14 2.

[26] Ibid.

[27] Ibid 4.

[28] Imran H Sarker, "Deep Learning: A Comprehensive Overview on Techniques, Taxonomy, Applications and Research Directions" (2021) 2 SN Comput Sci 420 1.

sağlanır[29]. Derin öğrenme, tipik olarak makine öğrenimiyle ilgili olan bazı veri ön işleme işlemlerini ortadan kaldırır, kullanılan algoritmalar metin ve resimler gibi yapılandırılmamış verileri alıp işleyebilir ve özellik çıkarma işlemini otomatikleştirerek insan uzmanlara olan bağımlılığın bir kısmını ortadan kaldırır[30]. Derin öğrenmede bir bilginin diğerinden ayırt edilmesi için hangi özelliğinin ayırt edici olduğu belirlenir. Makine öğreniminde, bu tip bir özellik hiyerarşisi bir uzman tarafından manuel olarak oluşturulur[31]. Dolayısıyla birkaç katman sinir ağına sahip olan klasik makine öğrenmesi karşısında çok daha fazla katmanı bulunan derin öğrenme, daha fazla veri kümesine ihtiyaç duyacaktır. Derin öğrenme, çok büyük miktarda veriyle eğitildiğinde yüksek oranda doğruluğa ulaşmakta olmakla birlikte tıbbi kişisel veriler gibi hassas veriler üzerinde bazı gizlilik endişelerine neden olmaktadır[32]. Konu hakkındaki önerilere sair alternatifler başlığında yer verilmiştir.

B. GENEL VERİ KORUMA İLKELERİ VE BUNLARIN YAPAY ZEKÂ KARŞISINDAKİ DURUMU

Kişisel verilerin hukuk tarafından korunması 1953'te imzalanan "İnsan Hakları ve Özgürlüklerinin Korumasına İlişkin Avrupa Sözleşmesi" ile başlayarak düzenleme altına alınmıştır. OECD tarafından 1980 yılında oluşturulan "Özel Yaşamın Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkeler" ile deyim yerindeyse sıçrama yaşanmış, Avrupa Konseyi'nin 1981'de imzalanmak üzere Konseyde yer alan ülkelere sunulan "108 No'lu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi[33] ve sonrasında 1995 yılında kabul edilen "95/46/EC Sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Direktifi"[34] ile bir uyumlaştırma arayışına girilmiştir. Burada AB ile ABD'nin kişisel veriye yaklaşımlarının farklılığını da ifade etmek gerekir. Zira Kıta Avrupası'nda kişilere mündemiç verilerin ekonomik değerinin kabulüyle birlikte ekonomik kazanç ile bireyin özgürlüğü ve onuru arasında bir denge kurulmaya çalışıldığı göze çarpar[35]. ABD'de ise verilerin birer meta olarak değerlendi-

---

29 Choi, Coyner and others (n 25) 7.

30 IBM, "What is deep learning?" <https://www.ibm.com/topics/deep-learning> (Erişim Tarihi: 31.07.2023)

31 Ibid.

32 P. C. Mahawaga Arachchige vd, "Local Differential Privacy for Deep Learning" (2020) 7(7) IEEE Internet of Things Journal 5827.

33 108 sayılı Sözleşme.

34 95/46/EC Sayılı Direktif.

35 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>, L 119/2 para. 4 ve 5 (Erişim Tarihi: 31.07.2023)

rilmesi, fikri mülkiyete veya mülkiyet hakkına konu edilmesi bahis konusudur[36].

Avrupa Konseyi ve Komisyonu tarafından hazırlanan ve 2016'da kabul edilen 2016/679 sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü ("GDPR"), 95/46/EC Sayılı Direktifi yürürlükten kaldırmış alanda oldukça geniş sayılan kapsamıyla veri öznelerine ("data subjects") geniş kapsamlı haklar sunmuştur. Bununla birlikte daha önce genel ilkeler kapsamında yer alan unutulma hakkı, GDPR ile genel ilkelerin bir parçası olmaktan çıkarılıp özel bir hüküm altında düzenlenmiştir[37]. İfade edilmelidir ki kişisel verilerin korunması, özel hayatın gizliliğinin korunması şemsiyesi altında 1953'ten önce de hukuk bilincinde olan bir mefhumdur. Henüz 1890 yılında mahremiyetin anlamı ve korunmasının tartışıldığı Warren ve Brandais'in "Right to Privacy" isimli çalışmalarında yalnız bırakılma hakkı, Prens Albert ve Strange davası gibi örnekler ile mahkemelerce mahremiyetin sağlanması ve sair hususlara yer verilmiştir[38].

1. GDPR Odağında Genel İlkeler

Başlık altında genel ilkeler izah edilirken genel nitelikli, bağlayıcı ve güncel veri koruma düzenlemesi olan GDPR ele alınmıştır. Ancak 108 sayılı Sözleşmede de genel ilkelere, kişisel verilerin adil, yasal, belirli ve meşru amaçlar için elde edilmesi, sınırlı ve belirli şekilde işlenmesi, doğru ve güncel olması, belirlenen süreyi aşmayacak şekilde muhafaza edilmesi gereği üzerinden yer verildiğini belirtmek gerekir. Genel ilkeler esasen kontrolörler ("data controllers") tarafından yürütülen veri işleme faaliyetlerinin kalbidir. Öyle ki henüz GDPR'ın başında belirtilen bu ilkeler, mevzuat boyunca bulunan diğer kural ve yükümlülükleri hem doğrudan hem de dolaylı olarak etkileyerek veri korumanın bu temel ilkelerine uyum, kontrolörlerin GDPR kapsamındaki yükümlülüklerini yerine getirmelerini sağlamada

---

[36] Konu hakkında detaylı bir karşılaştırma için bkz. Paul M., Schwartz ve Daniel J. Solove, "Reconciling Personal Information in the United States and European Union" (2014) 102 California Law Review 877-916.

[37] Unutulma hakkının GDPR çerçevesinde ifadesi ve hakkın GDPR'ın 17. maddesinde yer alan silme hakkı kapsamında düzenlenmesine yönelik bir değerlendirme için bkz. Tamer Soysal, "Unutulma Hakkının Avrupa Birliği'nin Genel Veri Koruma Tüzüğü Çerçevesinde İncelenmesi", 0 (2019) Uyuşmazlık Mahkemesi Dergisi 365.

[38] Samuel D Warren & Louis D Brandeis, "The Right to Privacy" (1890) 4 Harvard Law Review 193. Kişisel veriler Avrupa İnsan Hakları Sözleşmesi bakımından "Özel hayata ve aile hayatına, konuta ve haberleşmeye saygı hakkı" başlıklı 8. madde kapsamında korunmaktadır (ECHR, "Guide on Article 8 of the European Convention on Human Rights", <https://www.echr.coe.int/documents/d/echr/guide_art_8_eng>)(Erişim Tarihi: 31.07.2023).Ancak kişisel verilerin korunmasını isteme hakkı günümüzde özel hayatın gizliliğinden ayrıştırılması gereken bağımsız bir hak olarak karşımıza çıkmakta, müstakil şekilde hukuki düzenlemelerde vücut bulmaktadır. Örneğin; 2010 yılında kabul edilen Avrupa Birliği Temel Hakları Şartı'nın (Charter Of Fundamental Rights Of The European Union) 8. maddesinde, Avrupa Birliği'nin İşleyişine Dair Anlaşma'nın (Treaty on the Functioning of the European Union) 16. maddesinde ve Anayasamızın 20. maddesinin 3. fıkrasında kişisel verilerin korunması ayrıca hüküm altına alınmıştır. Hakkın AB'de bağımsız olarak ortaya çıkması hakkında bkz. Gloria Gonzalez Fuster, "The Emergence of Personal Data Protection as a Fundamental Right of the EU" (Springer 2014), 111-156

ilk adım kabul edilir[39]. Genel ilkeler mevzuat ve GDPR'da yer alan daha ayrıntılı hükümler için başlangıç noktası niteliğindedir ve Avrupa Konseyi ile Avrupa Birliği düzeyinde daha sonraki tüm veri koruma mevzuatı bu ilkelere uygun olmalıdır [40]. AB hukuku kapsamında, temel işleme ilkelerine yönelik kısıtlamalara yalnızca GDPR'ın 12 ila 22. maddelerinde belirtilen hak ve yükümlülüklere karşılık geldiği ve temel hak ve özgürlüklerin özüne saygı gösterilmesi gerektiği sürece kanunla, meşru bir amaç güdülerek ve demokratik bir toplumda gerekli ve orantılı olduğu sürece izin verilir[41]. Genel ilkelerin uygulanması, bunlar dışında herhangi bir sebeple bertaraf edilemeyecek, veri işlemenin tüm aşamalarında bunlara uyulması beklenecektir.

Bu ilkeler düzenlemenin "Kişisel Verilerin İşlenmesine İlişkin İlkeler" başlıklı 5. maddesinde;

> *"1. Kişisel veriler: (a) veri sahibi ile ilgili olarak hukuka uygun, adil ve şeffaf bir biçimde işlenir ('hukuka uygunluk, adillik ve şeffaflık'); (b) belirtilen, açık ve meşru amaçlara yönelik olarak toplanır ve bu amaçlara uygun olmayan bir şekilde işlenmez; kamu yararına arşivleme amaçları, bilimsel veya tarihi araştırma amaçlarıyla veya istatistiki amaçlarla işleme faaliyeti, 89(1) maddesi uyarınca, baştaki amaçlara aykırı şekilde değerlendirilmez ('amacın sınırlandırılması'); (c) işlendikleri amaçlarla ilgili olarak yeterli, yerinde ve gerekli olanla sınırlıdır ('verilerin en az seviyeye indirilmesi'); (d) doğrudur ve gereken şekilde, güncel tutulur; işlendikleri amaçlar göz önünde tutularak, doğru olmayan kişisel verilerin gecikmeye mahal verilmeksizin silinmesi veya düzeltilmesinin sağlanmasıyla ilgili makul tüm adımlar atılmalıdır ('doğruluk'); (e) veri sahiplerinin yalnızca kişisel verilerin işlenme amaçlarının gerektirdiği sürece teşhis edilmesini sağlayan bir şekilde tutulur; 89(1) maddesi uyarınca yalnızca kamu yararına arşivleme amaçlarıyla, bilimsel veya tarihi araştırma amaçlarıyla ya da istatistiki amaçlarla işlendikleri sürece ve veri sahibinin hakları ve özgürlüklerinin güvence altına alınmasına için bu Tüzük uyarınca gereken uygun teknik ve düzenlemeye ilişkin tedbirlerin uygulanmasına tabi olarak, kişisel veriler daha uzun süreler boyunca saklanabilir ('saklama süresinin sınırlandırılması'); (f) yetkisiz veya yasa dışı işlemeye karşı ve kazara kayba, imhaya veya tahribe karşı koruma da dahil olmak üzere teknik veya düzenlemeye*

---

[39] The Data Protection Commission (DPC), Principles of Data Protection <https://www.dataprotection.ie/en/individuals/data-protection-basics/principles-data-protection> (Erişim Tarihi: 31.07.2023)

[40] Handbook on European Data Protection Law (2018 edt.) (Luxembourg: Publications Office of the EU, 2018) 116.

[41] Ibid.

ilişkin uygun tedbirlerin kullanılması suretiyle kişisel verilerin güvenliğini sağlayan bir şekilde işlenir ('bütünlük ve gizlilik'). 2. Kontrolör 1. paragrafa uygun davranmaktan sorumludur ve buna uygun davrandığını gösterebilmelidir ('hesap verebilirlik').[42] *"*

şeklinde yer alır.

Öncelikle Hukuka Uygunluk, Adillik ve Şeffaflık ilkesini ele almak gerekir ("Lawfuness, fairness and transparency- 5(1)(a)"). GDPR'ın 6. maddesine göre veri işleme faaliyeti ancak maddede yer alan hususlardan en az biri geçerli olduğu ölçüde hukuka uygun kabul edilmiştir. Bu faaliyetler, veri öznesinin rızası, bir sözleşmenin uygulanmasında veya uygulanmasından önceki gereklilik, kontrolörün yasal sorumluluğu açısından gereklilik, kamu yararına icra edilen bir görev için veya resmi yetkinin kullanılması için gereklilik, meşru bir menfaatin varlığı şeklinde özetlenecek koşulları kapsamına almalıdır. Dolayısıyla veri işlemenin hukuka uygun kabul edilmesi için ya veri öznesinin açık rızası olacak ya da bu maddede belirtilen koşullardan birine dayalı veri işlenecektir. Aynı şekilde madde 8 bu alanda işlemenin hukuka uygun olması için gerekli şartları düzenlemektedir. Kişisel verilerin hukuka uygun işlenmiş sayılabilmesi için bu işlemenin hukuka uygun olması, meşru bir amaç için yapılmış olması ve bu amaca ulaşmak için demokratik bir toplumda gerekli ve ölçülü olması gerekir.

Adil işleme, verilerin aldatılarak veya veri sahibinin bilgisi dışında haksız yollarla elde edilmediğini veya başka bir şekilde işlenmediğini ifade eder. Yasal işlemeye ek olarak kontrolör ile veri öznesi arasındaki ilişkiyi yönettiği kabul edilen adil işleme ilkesi, kontrolörlerin yasal ve şeffaf bir şekilde veri kullanacaklarını ve işleme faaliyetlerinin GDPR ile uyumlu olduğunu gösterebilmelerini gerektirir[43]. Bu da veri işleme işlemlerinin gizli yapılmaması, veri öznelerinin olası risklerin farkında olması anlamını taşıyacaktır.

GDPR Resitali'nin 39. maddesi şeffaflık ilkesinin hem kişisel verilerin işlenmesine ilişkin her türlü bilgi ve iletişimin kolay erişilebilir ve kolay anlaşılır olmasını, açık ve sade bir dil kullanılmasını zorunlu kılar hem de özellikle veri öznelerine kontrolörün kimliği ve işlemenin amaçları hakkında bilgi alma, kişisel verilerinin adil ve şeffaf şekilde işlenmesi ve kişisel verilerine ilişkin haklarını kullanma konusunda bilgilendirilme hakkı sağlar[44]. İşlenmekte olan veriler kontrolörlerin bilgi sağlama ve kişisel verilere erişim sağlama yükümlülüğünü şart koşan GDPR madde 12-15'te yer alan hükümlere de uygun olmalıdır. Şeffaflık, kişisel verilerin toplanması, kullanılması veya başka bir şekilde işlenmesi süreçlerinin tamamında sağlanmalı, verileri işlenen kişiler bu verilere ne olacağını bilmelidir.

---

42 General Data Protection Regulation, AB Bakanlığı (Türkçe çevirisi).

43 Handbook on European Data Protection Law (n 40) 118.

44 General Data Protection Regulation (GDPR), "Recitals" <https://gdpr-info.eu/recitals/> (Erişim Tarihi: 31.07.2023)

Anlaşılacağı üzere bu "bilme" durumu genel ilkelerden hem adilliğin hem de şeffaflığın bir gereğidir.

Amaç sınırlaması ilkesi ("Purpose limitation- 5(1)(b)"), uzun süredir veri korumanın temel taşı ve birçok temel gereklilik için ön koşul olarak kabul edilmektedir. Bu ilke verilerin belirli, açık ve meşru amaçlar için toplanmasını ve bu amaçlarla bağdaşmayan bir şekilde daha fazla işlenmemesini gerektirir. Kişisel verilerin işlenmesi hem amaç hem de kapsam sınırlılığı gözetilerek, verilerin elde edildiği andan itibaren belirlenmelidir. Ayrıca veri işleme amaçları da açık olmalı ve gizli tutulmak yerine açıkça ifade edilmelidir. Son olarak amaçlar meşru olmalı yani söz konusu haklara, özgürlüklere ve çıkarlara orantısız bir müdahaleyi haklı göstermemelidir. Amaç sınırlılığı ilkesine ilişkin tartışma, kontrolörlerin bir kez belirledikleri amaca uygun/uyumlu olan tüm işlemleri yapıp yapamayacakları konusundadır. Her ne kadar 6. maddede kişisel verilerin toplanma amacı dışında bir amaçla işlemenin bu ilk amaçla uyumlu olup olmadığını belirlemek için bir dizi kriter sunulmuş olsa da (bağlantı, güvencelerin varlığı gibi) bu kriterlerin oldukça soyut ve geniş kapsamlı olduğu ifade edilmelidir.

Veri Sınırlaması ("Data minimization- 5(1)(c)") ilkesi kapsamında, işlenen kişisel veriler işlendikleri amaçlar çerçevesinde yeterli, ilgili ve gerekli olanla sınırlı olmalıdır. Resital'in 39. maddesinde kişisel verilerin yalnızca amaçların başka yollarla makul bir şekilde yerine getirilememesi durumunda işlenmesi gerektiği belirtilir. Bu gereklilik şartı, kişisel verilerin sadece niceliğini değil, aynı zamanda niteliğini de ifade etmektedir. Buna göre gerekli olmaması halinde aşırı büyük miktarda kişisel veri işlenmemeli, veri öznelerinin çıkarlarına orantısız müdahaleler yapılmamalıdır. Verilerin doğru olması ve gerektiğinde güncel tutulması gerekliliği, tüm yanlış verilerin düzeltilmesi veya silinmesi anlamına gelir. Kontrolör doğruluk ilkesine uyulmasını sağlamak için gecikmeden makul olan her adımı doğruluk ("Accuracy- 5(1)(d)") ilkesinin gereği olarak atmalıdır. Kişisel veriler, işleme amaçlarına ulaşmak için gerekli olan sürenin ötesinde veri konularının tanımlanmasına izin verecek biçimde saklanmamalı, saklama süresi sınırlı olmalıdır ("Storage limitation- 5(1)(e)"). Ek olarak kontrolörlerin silme veya periyodik inceleme şekildeki ek yükümlülükleri, kişisel verilerin gereğinden fazla tutulmamasını sağlayacaktır.

Kişisel verilerin güvenliğini ve gizliliğini temin etmeye yönelen bütünlük ve gizlilik ("Integrity and confidentiality- 5(1)(f)") ilkesi, kişisel verilerin ifşa edilmesinin engellenmesi, imhaya veya hasara karşı korunması için gerekli teknik/organizasyonel önlemlerin alınması, takma ad kullanma ("pseudonymisation") gibi alternatif yöntemlerin vaka bazında belirlenmesi gibi yükümlülükleri içerir[45]. Kontrolör gelişmiş teknolojiyi, uygulama maliyetlerini ve işlemenin niteliğini, kapsamını, bağlamını, amacını ve ayrıca değişim riskini dikkate almalı, önlemleri

[45] Handbook on European Data Protection Law (n 40) 131.

uygularken gerçek kişilerin hak ve özgürlüklerini korumayı öncelemeli, önlemlerin etkinliğini de değerlendirmelidir[46]. Veri korumanın temel ilkelerinin yer aldığı 5. madde kontrolörün önceki tüm ilkelere uyumdan sorumlu olacağı ifadesiyle sona ermektedir. Kontrolör işlemenin bu yasal kurallara uygun olduğunu gösterebilmeli ve uyum konusunda hesap verebilmelidir ("Accountability- 5(2)").

2. Genel İlkelerin Yapay Zekâ Karşısındaki Durumu

a. Rekabetçi Veri Ekonomisi: Amaç veya Menfaat Çatışması

Genel ilkeler bazında spesifik bir değerlendirme yapmadan önce kişisel verileri koruma yasalarıyla korunan özel hayatın gizliliğinin veya mahremiyetin korunması menfaatinin, uygulamadaki rekabetçi veri ekonomisi ile bağdaşmazlık içinde olduğunu belirtmek gerekir. Özellikle yapay zekâ ve büyük veri konularında dile getirilen *"büyük veri, sınırlı mahremiyet (big data, small privacy)*[47]*"* söylemi esasen bu yapısal çelişkiyi yansıtmaktadır. Büyük veri karmaşık yapısı olan (algoritmik) depolama, analiz etme ve daha fazla süreçten geçen devasa veri kümeleri için kullanılan bir terimdir[48]. Büyük veri analitiği ile elde edilen bilgiler -ki bunların içinde elbette kişisel veriler de vardır- şirketlerin birbiriyle rekabet etmesine ve rakipler üzerinde avantaj elde etmesine sebep olur[49]. Öyle ki kişisel veriler büyük verinin "ham madde kaynağı" olarak sosyal medya platformlarından sağlık hizmetlerine kadar pek çok alanda anlık olarak işlenmektedir[50]. Yapay zekâ ise büyük verinin analizinde faydalı bir araç olarak ondan elde edilen sonuçları güçlendirmektedir.

Bugün pek çok ülke yapay zekâ teknolojilerinin benimsenmesini artırmak için politikalar uygulamakta, veri değer zincirini güçlendirmek ve veriye dayalı ekonomiyi geliştirmek için endüstriler pek çok iş birliği ve stratejik ortaklıklar geliştirmekte, sektörler dönüşmeye başlamaktadır[51]. Yapay zekâ özellikle üretim ve lojistik, finans, pazarlama ve müşteri hizmetleri, sağlık, ilaç geliştirme gibi alanlarda etkili olmakta, kendi ekonomisini yaratmaktadır. Yapay zekâ uygulamaları, makine öğrenimi, bilgisayarlı görü, robotik ve doğal dil işleme üzerine onlarca yıllık araştırmalarla desteklenmekte, yapay zekânın küresel ekonomik etkisinin

---

46 Ibid.

47 The Internet, Policy & Politics Conferences Oxford Internet Institute, University of Oxford, "Markus Schroeder: Big Data, Small Privacy?", <http://blogs.oii.ox.ac.uk/ipp-conference/2012/programme-2012/track-b-policy/panel-5b-privacy/markus-schroeder-big-data-small-privacy.html> (Erişim Tarihi: 31.07.2023)

48 Seref Sagiroglu and Duygu Sinanc, "Big Data: A Review" in Proceedings of International Conference on Collaboration Technologies and Systems (CTS, 2013) 42.

49 Ibid.

50 Duygu Hatipoğlu Aydın, "Kişisel Verilerin Korunmasına Hukukun Sınırları" (2023) 88(2) İzmir Barosu Dergisi, 143.

51 Mark Johnson, Raj Jain and Peggy V Brennan-Tonetta, "Impact of Big Data and Artificial Intelligence on Industry: Developing a Workforce Roadmap for a Data Driven Economy" (2021) 22 Glob J Flex Syst Manag 197.

2030 yılına kadar 15,7 trilyon dolara ulaşması beklenmektedir[52]. Bunun yanında yapay zekâ teknolojilerinin ve kapasitesinin geliştirilmesinin yavaş yavaş devletlerin ulusal bir önceliği olarak kabul edilmesi[53], ondan elde edilen her faydanın (ekonomik ve sair) maksimize edilmeye çalışıldığı bir konjonktürde, kişisel verilerle ilgili daha fazla sorgulamaya sebep olmaktadır.

Günümüzde yapay zekâya ilişkin doğrudan hüküm içeren bağlayıcı yasalar henüz oluşturulmamıştır. Özellikle 2000'lerin başından beri hızla ilerlemeye devam eden yapay zekâ ve büyük veri konularının bağlayıcı hukuki düzenlemeler ile ele alınması gerekmektedir. Bu doğrultuda "Collingridge ikilemi[54]"nde olan durum apaçık karşımıza çıkmakta teknolojinin ezip geçtiği yalnızca hali hazırdaki iş modelleri değil aynı zamanda hukukun kendisi olabilmektedir[55]. Aynı ikilem yapay zekâ gibi hızlı gelişen teknoloji alanında belirgindir. Teknolojinin gelişmesiyle beraber, özellikle dijital pazarlamada ve sosyal medya platformlarında hali hazırdaki iş modelleri hızla değişirken, hukuk bu hızlı değişime ayak uydurmakta zorlanmaktadır. Karar verme mekanizmalarında kullanıldığı durumlarda, yapay zekâ objektif olmayan, önyargılı veya ayrımcılık yapan sonuçlar verebilmektedir. Bu sonuçlar, kişisel verilerin doğru olmayan kişilerle eşleştirilmesi gibi bir dizi problemi beraberinde getirir.

Hukukun bu problemlere ayak uydurmasından söz ederken belirli durumlardaki olası etkileri düşünmek faydalı olabilir. Örneğin bir yapay zekâ uygulaması, yasaların belirgin olmayan durumları düşünmeye yetişememesi nedeniyle hatalı veya ayrımcı kararlar verebilir. Yasa yapıcılar ve düzenleyicilerin, yapay zekânın neden olduğu bu ve benzeri problemleri çözmek için proaktif bir şekilde hareket etmeleri gerekir. Yapay zekâda yaşanan gelişmelerin bağlayıcı tekno-hukuki çözümlerle sınanması, önümüzdeki olumsuz senaryoların önüne geçmek için kaçınılmazdır. Bu olumsuz senaryolar, kişisel verilerin yanlış kullanılmasından önyargılı algoritmaların toplumda eşitsizliklere yol açmasına kadar geniş bir yelpazede olabilir. Bu nedenle yapay zekâ, teknoloji, etik ve hukuk arasındaki hassas dengenin korunması, bu alandaki olası çözümlerin teşvik edilmesi gerekmektedir.

---

52 Ibid 198.

53 The White House, "Select Committee on Artificial Intelligence" <https://www.whitehouse.gov/ostp/ostps-teams/nstc/select-committee-on-artificial-intelligence/> (Erişim Tarihi: 31.07.2023)

54 Collingridge ikilemi, teknolojinin gelişmesi sonucunda onu kullanarak ortaya konulan yeni araçların kullanımının sebep olduğu bir tür kontrol-fayda açmazıdır. Yani bu "yeni teknolojilerin" sebep olacağı sosyal-hukuki ve ekonomik etkilerin etraflıca anlaşılabilmesi için, kullanılmaları gerekir (tahmin edilmezlik sorunu). Ancak kullanılmaları neticesinde doğan olumsuz sonuçlar ortaya çıktığında, bu sonuçların bertaraf edilmesi için yapılacak müdahaleler geç kalmış olabilecektir (hız veya güç sorunu). Diğer taraftan teknolojiye önceden yapılan sınırlamalar (önleyici kontrol mekanizmaları) ise onun yavaşlamasına, ondan gelebilecek faydaların gözden kaçırılmasına sebep olabilir. İkilem, David Collingridge tarafından "The Social Control of Technology" isimli kitapta ifade edilmiştir. Kaynak için bkz. David Collingridge, The Social Control of Technology (New York: St. Martin's Press, 1980) 19-20-21.

55 Mesut Serdar Çekin, Yapay Zekâ Teknolojilerinin Hukuki İşlem Teorisine Etkileri (1. Baskı) (İstanbul: onikilevha, 2021) 29.

b. Kara Kutu Problemi

Bir model olarak yapay zekânın bir dizi veriyi alıp bunları işleyerek bir tanımlama veya çıktı ürettiği hususu ilk başlık altında ifade edilmişti. Yapay zekâ ve makine öğrenmesi modellerinin nasıl karar verdiğinin veya iç işleyişinin anlaşılamaması ve gözlemlenememesi sorunsalına yönelik yapılan kara kutu ("black box") adlandırması, girdilerin algoritmik hesaplama içine girmesi ve üretilen çıktının neye göre verildiğinin bilinmemesi durumunu yansıtır. Bir diğer deyişle yapay zekâ sistemlerince verilen çıktıların tam olarak nasıl bir programlama sonucu verildiğinin bilinmemesi opak durum olarak kabul edilir ve kara kutu problemini oluşturan da esasen bu opaklıktır. Derin öğrenme algoritmaları açısından geçerli olan bu durum, çeşitli nedenlerden ötürü büyük problemler meydana çıkarmaya gebedir.

Özellikle yorumlanması zor karmaşık hesaplamaları içeren sinir ağları ve derin öğrenme modelleri için geçerli olan kara kutu sorunsalı, ilk olarak istenmeyen sonuçlar ürettiklerinde derin öğrenme sistemlerini düzeltmeyi zorlaştırır. Diğer taraftan derin öğrenme ile ortaya çıkan ön yargılı sonuçlar, bu sonuçların değiştirilmesi ve ortadan kaldırılması gereğini doğurur. Örneğin siyahilerle ilgili ön yargılı bir sonuç üreten yapay zekâ sisteminin bu sonucu adil, tarafsız veya açıklanabilir kılmak için nasıl bir sürecin sonunda bu kararı verdiğinin bilinmesi gerekir. Önyargı, genellikle modelin eğitildiği veri setlerinin içerisine işlenmiş durumdadır ve bu veri setleri çoğunlukla önyargılı insan veya toplum davranışlarını yansıtır[56]. Dolayısıyla önyargının giderilmesi sadece algoritmanın düzeltilmesi ile mümkün olmayabilir; eğitim veri setlerinin de gözden geçirilmesi, bu tür sistemlerin geliştiricilerinin sosyal bilimler ve beşerî bilimlerden (örneğin antropoloji) çok sayıda profil içermesi tavsiye edilmektedir[57].

c. Şeffaflık ve Rıza Problemi

Şeffaflık prensibine ilişkin özellikle GDPR'ın 12. maddesinde yer alan, veri öznelerini şeffaf şekilde bilgilendirme yükümlülüğünü sağlamak, kontrolörler açısından yapay zekâ söz konusu olduğunda güç olabilecektir. Zira yapay zekânın, kişisel veri üzerindeki etkileri bilinmeyen hatta açıklanamayan değişkenlerle çalışan bir veri analizi yaparken amaçları önceden belirtmek, doğrulamak veya şeffaf bilgi sağlama girişiminde bulunmasının yerinde bir beklenti olmadığı belirtilmektedir[58]. Nitekim kara kutu problemi nedeniyle "işleyişi anlaşılamayan" katmanlar üzerinde yer alan sinir ağları böyle bir şeffaf işleyişi engellemekte, yazılım süreçlerinin izlenebilirliğini kısıtlamaktadır[59].

---

56 Alicia de Manuel vd, "Ethical Assessments and Mitigation Strategies for Biases in AI-systems Used During the COVID-19 Pandemic" (2023) 10(1) Big Data & Society 9.

57 Ibid.

58 Boris Paal, "Artificial Intelligence as a Challenge for Data Protection Law: And Vice Versa" in Silja Voeneky, Philipp Kellmeyer, Oliver Mueller, Wolfram Burgard (eds), The Cambridge Handbook of Responsible Artificial Intelligence: Interdisciplinary Perspectives (Cambridge Law Handbooks, 2022) 292-293.

59 Ibid.

Diğer taraftan veri koruma ilkelerinin desteklenmesi için GDPR'ın 35. maddesinde belirtilen veri koruma etki değerlendirmelerinin ("data protection impact assessment") yürütülmesi ve tasarım gereği gizlilik ("privacy by design") gibi uygun teknik ve organizasyonel önlemlerin uygulanması gibi yapay zekâ sistemlerinin geliştirme aşamasında güvenceler oluşturmak bakımından ele alınmalıdır. Ancak burada da üç problem belirtilir: Birincisi kişisel verilerin kategorize edilememesinden kaynaklı genişlik, ikincisi veri öznesinin bilgi alma ve kişisel verilere erişim hakları, üçüncüsü ise teknik ve organizasyonel önlemleri uygulama görevinin (veri işlemenin planlamasında ve gerçekleştirilmesinde) kontrolörleri önceden etik düşünmeye mecbur bırakmasıdır[60]. Son durumda genel ilkenin uygulanıp uygulanmaması kontrolörün takdirine bırakılmış olmaktadır.

Veri koruma etki değerlendirmesi ve tasarım gereği gizlilik ilkelerinin yapay zekâ sistemlerinin geliştirilmesi sürecine dahil edilmesi, kişisel verilerin korunmasına önemli katkı sağlayabilir. Örneğin bir yapay zekâ uygulaması geliştirilirken, kullanıcıların kişisel verilerini işlemek yerine anonimleştirilmiş veya takma isim verilmiş verileri işleyecek şekilde tasarlanabilir. Bir sistem, sadece işleme amacının gerektirdiği minimum miktarda kişisel veriyi işlemek üzere programlanabilir. Ancak bu ilkelerin uygulanmasının etkinliği ve yapay zekâ sistemlerinin veri koruma kuralları ile uyumu sürekli gözden geçirilmeli ve konu hakkındaki teknik hususlar mümkün olduğu ölçüde hukuki düzenlemeye tabi olmalıdır[61].

Kişisel verilerin birer bilgi parçası olarak geniş kapsamlı olması, veri işleme amaçları için de yapay zekâ kullanımının sınırlarını belirlemeyi zorlaştırabilir. Girdi olarak bağımsız şekilde bir taraftan da yapay zekâ kullanımının sınırları geliştirmek için kullanılan veriler -kişisel verileri de kapsayan biçimde- teknolojik gerçeklik karşısında korunaksız kalmaktadır. Ayrıca yapay zekâ tarafından kişisel verilerden elde edilen çıkarımların kişisel veri oluşturup oluşturmadığı ve kişisel veri kategorisine dahil edilmesinin gerekip gerekmediği de belirsizdir. Veri öznelerinin bilgi alma ve kişisel verilere erişim hakları konusunda, yapay zekânın işleyişinin karmaşıklığı nedeniyle kontrolörlerin bu karmaşıklığı ve yapay zekânın özerkliğini erişim yükümlülüklerini atlatmak için bir sebep olarak kullanma riski her zaman vardır[62]. Neticede GDPR uyumlu yapay zekâ kullanımını garanti etmek için kişisel verilerin yapay zekâ sistemleri tarafından işlenmesine ilişkin bilgi edinme hakkının kapsamının daha net belirtilmesi beklenir.

Kendi kendine öğrenen, otonom yapay zekâ teknolojilerinin doğasında şeffaflık, açıklık gibi bir özellik yoktur. Şeffaflık ilkesi GDPR çerçevesinde bilhassa veri işlemenin temelinde veri öznesinin onayının bulunduğu durumlar için kritik

---

60 Frederike Ufert, "AI Regulation Through the Lens of Fundamental Rights: How Well Does the GDPR Address the Challenges Posed by AI?" (2020) 5(2) European Papers 1094.

61 Oğuz Gökhan Yılmaz, "Yargı Uygulamasında Yapay Zekâ Kullanımı- Yapay Zekâ Hâkim Cübbesini Giyebilecek mi?" (2021) 66 Adalet Dergisi 408.

62 Ibid 1095.

bir önem taşır. Verilerin işlenme sebepleri dikkate alındığında, veri sahibinin rızası ile gerçekleştirilen işlemlerde GDPR'ın getirdiği şeffaflık kısıtlamaları geçerli hale gelir[63]. Kontrolörün öznenin onayını bilgilendirilmiş şekilde alması gerekliliği, aynı zamanda bir rıza problemini doğurur. Rıza GDPR'ın 4. maddesinde, *"veri öznesinin bir beyan yoluyla ya da açık bir onay eylemiyle kendisine ait kişisel verilerin işlenmesine onay verdiğini gösteren özgür bir şekilde verilmiş spesifik, bilinçli ve açık gösterge"* şeklinde tanımlanmaktadır. GDPR ilkelerine göre yapay zekâ sistemlerini kullanan dolayısıyla farklı kökenlerden gelen çok büyük miktarda verinin kapsamlı analizlerini gerçekleştiren kontrolörler, verileri kendilerine izin verilecek şekilde işleme olanağına sahip olmalıdır[64]. Bu da veri öznelerini, işlenen verilerin niteliği ve kaynağı hakkında açıkça ve yeterince bilgilendirmeyi gerektirir. Yani hukuka uygun bir rızanın kişisel verilerin korunması açısından verilmiş sayılması, genel hükümlerde yer alan rızadan farklı olarak özel koşulları da içermesine bağlı kılınmıştır[65]. Buna karşılık kişisel verilerin algoritmalarca yapılan analizler sırasında veya orijinal olarak kişisel olmayan verilerin kombinasyonları sonucunda üretildiği durumlarda ne olacağının, verilerin ilk kaynağının tam olarak nasıl belirleneceğini bilmenin oldukça güç olduğu belirtilmektedir[66]. Bu bağlamda GDPR'ın 14. maddesinde yer verilen bilgilendirme yükümlülüğü, bu tür bilgilerin veri öznelerine sağlanmasının orantısız şekilde külfetli olması durumu ile çelişki içindedir.

Yapay zekâ sistemleri yapılandırılmamış verileri ve algoritmik analizleri kullanarak, özgün bilgiler oluşturabilir. Bu durum, kişisel verilerin ilk kaynağını belirlemeyi zorlaştırabilir ve bu nedenle veri öznelerine yeterli bilgi sağlama görevini de yerine getirilmesi güç hale getirebilir. Örneğin bir makine öğrenme modeli, kişisel olmayan verilerden kişisel veriler oluşturabilir veya mevcut kişisel verileri yeni ve beklenmedik şekillerde analiz edebilir. Ayrıca makine öğrenmesinde karşımıza çıkan kara kutu sorunu, veri öznelerinin verilerinin nasıl kullanılacağına dair tam ve bilinçli bir onay vermesini de zorlaştırabilir. Son olarak kişisel verilerin işlenmesine izin veren yasal bir dayanak bulunması bakımından veri öznesinin taraf olduğu bir sözleşmenin uygulanması veya bir sözleşme yapılmadan önce veri sahibinin talebiyle adımlar atılması için işleme faaliyetinin "gerekli" olması gerekir. Ancak yapay zekâyı kapsamına alan sözleşmelerde, bu tür sözleşme öncesi durumların düzenli olarak ortaya çıkıp çıkmayacağı her zaman belirli olmayabilir.

d. Amaç Sınırlaması ve Değişikliği Olasılığı

GDPR'ın 5(1)(b) bendinde belirtilen amaç sınırlaması ilkesi uyarınca, (kişisel) verilerin işlenme ve elde edilme amaçları, öz ve anlaşılır bir şekilde veri öznesine

63 Paal (n 58) 293.

64 Ibid.

65 Sinan Akkurt, "Açık Rıza" P Çağlayan Aksoy, H C Aksoy (ed.), Kişisel Verilerin Korunmasına Akademik Bakış KVKK Akademi Derleme Çalışması (KVKK Yayınları No 42, Ankara)160.

66 Paal (n 58) 293.

sunulmalıdır. Bu ilke, kişisel verilerin işlenmesinde önceden belirlenen bir amaç kısıtlamasının gerekliliğini vurgular. Ancak yapay zekânın bağımsız gelişmesi, belki de önceden belirlenmemiş amaçlar için kullanılabilmesi durumları, ilkenin uygulanması bakımından bir uyumsuzluk doğurmaktadır. Algoritmanın ne öğreneceğini tahmin etmek neredeyse imkânsız olduğundan ve yapay zekânın öngörülemeyen sonuçlara yol açabileceği durumlarda, amaç sınırlaması ilkesi ile yapay zekâ teknolojilerinin yeniliği arasında bir denge bulmak güç olabilecektir.

Amaç sınırlamasının özellikle tahmine dayalı olarak yürütülen güvenlik birimleri faaliyetlerinde kullanılan yapay zekâ teknolojileri bağlamında etkili bir koruma gibi görünmediği ifade edilmektedir[67]. Bu uygulamaların giderek daha geniş amaçlar için uygulanmasından ve güvenlik birimlerinin erişebildiği veri kümelerinin ilgili tüm analitik süreçler için kullanılmasından ötürü bu ilke işlevini yerine getirememesi söz konusu olabilecektir[68]. Verilerin işlenmesinde amaç değişikliğini kapsamına alan GDPR'ın 6. maddesinin dördüncü fıkrasında yer alan "bağlantılı bir gerekçe bulunması"nın, verilerin farklı bağlamlarda üretildiği ve sonradan birleştirildiği ya da yeni amaçlar için kullanıldığı durumlar açısından nasıl uygulanacağı da diğer soru işaretidir.

e. Ön Yargılı veya Yanlış Sonuçlar: Silme Taleplerinin Anlamı

Yapay zekâ araçları tarafından üretilen sonuçların serbestçe çarpıtılması veya yanlış/ön yargılı şekilde ortaya çıkması riski ile bireyin çıkarları ve kamu refahı arasında dikkate değer bir çatışma riski söz konusudur. Doğruluk-bütünlük-gizlilik ilkesi, kişisel verilerin işlenmesinden etkilenen veri öznelerinin, kendileri hakkında yanlış veri kullanımından kaynaklanan herhangi bir dezavantaja maruz kalmaması için toplanan bu verilerin gerçeği doğru bir şekilde yansıtmasını sağlamayı amaçlamaktadır. Ancak verilerin doğruluğuna ilişkin durumlar, veri girişi ve çıkışı arasında bir ayrım yapılmasını gerektirirken yapay zekânın işleyişinde veri işleme analizlerinin ve süreçlerinin sonuçları verildiği için yapay zekâ tarafından verilen bilgiler sadece bir tahmin oluşturacaktır. Bu doğrultuda, üretilen yanlış bilgilerin tespit edilmesi ve doğru bilgilerin geri yüklenmesi ya da veri öznelerine tanınan silme hakkının kullandırılması beklenir. Ayrıca yanlış sonuçlar şeklinde ortaya çıkan kişisel verilerin yapay zekâ algoritmalarından silinip silinmeyeceği tartışmalı bir konudur. Tartışmaların çoğunda yapay zekâ/makine öğrenmesi bağlamında silme/değiştirme taleplerinin teknik sorunlara takılacağı sonucuna varılmaktadır[69].

---

67 Stefania Fantin and Panagiota Vogiatzoglou, "Purpose Limitation By Design As A Counter To Function Creep And System Insecurity In Police Artificial Intelligence" (2020) United Nations Interregional Crime and Justice Research Institute (UNICRI) 26.

68 Ibid. Kamu Denetçiliği Kurumu'nun (Ombudsman) Ulusal Yargı Ağı Bilişim Sistemi'ne (UYAP) entegre olan Emniyet Genel Müdürlüğü kayıtlarına ilişkin Adalet Bakanlığı'na tavsiyesi hk. bkz. Adalet gen.tr, "Ombudsmandan UYAP'a tavsiye" <https://www.adalet.gen.tr/ombudsmandan-uyapa-tavsiye.html> (Erişim Tarihi: 31.07.2023)

69 Eduard Fosch Villaronga, Peter Kieseberg and Tianying Li, "Humans Forget, Machines

Diğer taraftan yapay zekâ tabanlı karar verme, önceden var olan ön yargıları büyütebilir ve yeni ön yargı türleri için büyük potansiyele sahip yeni sınıflandırmalar ve kriterler geliştirebilir[70]. Sürekli artan bu endişeler, yapay zekâ tabanlı sistemlerin, kararlarının adilliğini de ele alan yeni yaklaşımlar ile etik ölçekte yeniden değerlendirilmesine yol açmaktadır. Ancak yapılan bir araştırma artan teorik etik çalışmalar ile uygulamadaki durumun örtüşmediğini, şirketlerin etik kaygıları gerektiği kadar dikkate almadığını gözler önüne sermektedir[71]. Bahsi geçen araştırma, etik konulu teorik çalışmalarda ilerleme sağlanmasına rağmen bu ilerlemelerin ticari kuruluşlar tarafından yeterli derecede dikkate alınmadığını ortaya koymaktadır. Şirketlerin kullanıcı verilerini gerektiğinden fazla toplaması ve bu verileri izinsiz veya şeffaf olmayan şekillerde kullanması durumlarına etik standartlara uygun olmayan bir şekilde yapay zekâ sistemlerinin kullanılmasının eklenmesi endişe vericidir. Bu sebeple toplumlara derinden yerleşmiş olan ön yargıların yalnızca teknik çözümlerle kaldırılmayacağı, sosyal ve yasal dayanağı olmayan teknik çözümlerin sorunu çözme noktasında yeterli olmayacağı açıktır[72].

Yapay zekâ destekli yüz tanıma teknolojileri tarafından yapılan tespitler üzerine yanlışlıkla tutuklanan kişilerin genellikle siyahi olması, yanlış tespit edilen kişilerin sabıka kaydı, ekonomik durum, etnisite gibi ortak özelliklere dayandığının sonradan anlaşılması, Amazon, Microsoft gibi şirketlerin bilhassa ABD'de kolluk kuvvetlerine sattığı yapay zekâ destekli programların hesaplamalarını gerekçe göstererek özgürlüğü bağlayıcı cezaya hükmedilmemesi gerektiğini gösterir[73]. Henüz oldukça yeni sayılabilecek OpenAI'ın ChatGPT sohbet robotunun kendisinden cinsel tacizde bulunan hukukçuların bir listesini oluşturmasının istenmesi üzerine bir kurgu oluşturması (tacizci olmakla suçlanan profesörün Alaska'ya yaptığı bir sınıf gezisinde müstehcen yorumlarda bulunduğu, bir öğrenciye dokunmaya çalıştığı, bilginin kaynağı olarak Washington Post'ta Mart 2018'de yayınlanan yazının bulunduğu), kurguda adı geçen hukuk profesörünün hiçbir zaman Alaska'ya bir sınıf gezisi yapmaması[74] ile karşımıza çıkan durum apaçık bu sorunsala işaret eder.

Remember: Artificial Intelligence and the Right to Be Forgotten" (2018) 34(2) Computer Law & Security Review 304-305.

70 Eirini Ntoutsi, Pavlos Fafalios and Ujwal Gadiraju, "Bias in Data-driven Artificial Intelligence Systems: An Introductory Survey" (2020) 10 WIREs Data Mining Knowl Discovery, e1356 2.

71 Stanford University, "State of AI in 10 Charts: Ethics Infiltates Research" <https://hai.stanford.edu/news/state-ai-10-charts> (Erişim Tarihi: 31.07.2023)

72 Ntoutsi, Fafalios and Gadiraju (n 70) 14.

73 Nytimes, "Wrongfully Accused by an Algorithm <https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html> (Erişim Tarihi: 31.07.2023)" Wired, "How Wrongful Arrests Based on AI Derailed 3 Men's Lives <https://www.wired.com/story/wrongful-arrests-ai-derailed-3-mens-lives/> (Erişim Tarihi: 31.07.2023)"

74 The Washington Post, "ChatGPT invented a sexual harassment scandal and named a real law prof as the accused" <https://www.washingtonpost.com/technology/2023/04/05/chatgpt-lies/ > (Erişim Tarihi: 31.07.2023)

Burada ön yargı probleminin ("bias problem") ötesinde kurgulama durumu karşımıza çıkmaktadır. Nitekim yapay zekâ modelleri, iddialarını desteklemek için birincil kaynaklar uydurarak ve önemli gerçekleri kurgulayarak yanlış/çarpıtılmış sonuçlar sunabilir. Chatbot adı verilen sohbet robotları, kendilerine sorulan sorulara fazlasıyla özgüvenli şekilde cevap ürettiklerinden, neyin gerçek neyin kurgu olduğunun anlaşılması için geçen zamanda çarpıtılmış gerçeklere maruz kalan bireylerin durumunun hukuk kurallarına dayanılarak düzeltilmesi beklenir. Özellikle bir üretken ("generative") yapay zekâ türü olan sistemlerin web entregrasyonlarının artmasıyla bu sorunların büyüyebileceğini de belirtmek gerekir.

Kişisel verilerle beslenen yapay zekâ dil modellerinin güçlü kimlik avı veya dolandırıcılık araçları olarak kötüye kullanılmalarının oldukça kolay olduğu (herhangi bir programlama bilgisine gerek olmadığı için), bu dil modellerinin hızlı bir şekilde günlük faaliyetlerin yapılmasını kolaylaştıran dijital asistanlara entegre edildiği ancak bu durumun yarattığı çok temel problemler olduğu belirtilmektedir[75]. Özellikle Jailbreak ("yazılımsal sınırlamaların ortadan kaldırılması") durumlarında hırsızlık veya patlayıcı yapımı gibi amaçlarla bu robotların kullanılması, ChatGPT gibi modellerin internette gezinen ve etkileşim kuran ürünlere entegre edilmesinin yaratacağı güvenlik zafiyetleri, bu yapay zekâ modellerinin veri setlerinin eğitim aşamasında kasıtlı şekilde bozulabilme ("poisoning the data sets") durumları bunlara örnektir[76]. Bu gibi ihtimallerde acil ve etkili müdahalelerin yapılması gerekmektedir.

f. Veri Sınırlaması/Minimizasyonu ve Meşru Amaç Çelişkisi

Kişisel verilerin işlendikleri amaçlarla bağlantılı olarak yalnızca yeterli, ilgili ve gerekli olanlarla sınırlı bir şekilde işlenmesi, veri minimizasyonu ilkesinin bir gereğidir. Bu ilkeyi uygulamaya geçiren ise özellikle GDPR'ın 25. maddesinde belirtilen "tasarım gereği ve varsayılan olarak" mahremiyet şeklinde tanımlanan yöntemlerdir ("privacy by design ve privacy by default"). Ancak bu ilke büyük miktarda veri elde etmeye dayanan ve bunu gerektiren yapay zekâ teknolojilerinin genel konseptiyle, yüksek veri talebiyle doğrudan bir çelişki içindedir. Zira kişisel verilerin amacına ulaştıktan sonra silinmesi veya kısıtlanması, yapay zekâ teknolojilerinin hem gelişimini hem de kullanımını önemli ölçüde engelleyebilmektedir[77].

Avrupa Parlamentosu tarafından oluşturulan "GDPR'ın Yapay Zekâ Üzerindeki Etkileri" isimli dokümanda öncelikle geleneksel veri koruma ilkeleri ile yapay zekâ arasındaki gerilim kabul edilir[78]. Yapay zekâ ve büyük veri kullanımında bu

---

75 Heikkila M, "Artificial Intelligence: Three Ways AI Chatbots Are a Security Disaster" (MIT Technology Review, 2023) <https://www.technologyreview.com/2023/04/03/1070893/three-ways-ai-chatbots-are-a-security-disaster/> (Erişim Tarihi: 31.07.2023)

76 Ibid.

77 Paal (n 58) 295-296.

78 European Parliament, "The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence" (2020) European Parliamentary Research Service: PE 641.530, II.

ilkelerin geliştirilmesi gereğinin altı çizilmektedir[79]. Sadece kişisel değil veri öznelerinin yeniden tanımlanmasına yol açan tüm verilerin yeni birer yaratım olduğunun kabulüyle, veri minimizasyonunda orantılılığın kontrolörler açısından "işleme amaçlarına göre ek amaçlardan daha ağır basan bir fayda" sağlanmasının verilerin saklanmasını haklı gösterebileceği vurgusu yapılmaktadır[80].

AB'nin veri koruma mevzuatını sıkı bir biçimde uygulamasının ABD ve Çin gibi enformasyona dayalı ekonomilere karşı yarışı kaybettireceği anlayışına karşılık önerilen, yapay zekânın ile bireylerin sosyal ilişkilerini dengelemenin gerekliliği, anonim veri üretme, profil oluşturma da dahil olmak üzere kişisel verilere dayalı işlemelere ancak belirli koşullar altında izin verilmesi anlayışıdır[81]. AB'nin bu etki dokümanının genel ilkeler ile yapay zekânın bağdaşmaz doğasını açıkça ifade etmesi önemli olmakla birlikte, "meşru menfaat" gibi belirsiz amaçlar doğrultusunda dengeleme yapması, bizi bulunduğumuz noktadan farklı bir yere götürmemektedir. Zira meşru menfaatin anlamı ticari faaliyetlerle ilgili görevleri yerine getirmek, müşteri ilişkileri veya doğrudan pazarlama amaçları gibi unsurlara gömülü olarak yorumlanmaktadır[82].

g. Konunun Kişisel Verilerin Korunması Kanunu Açısından Değerlendirilmesi

Hukukumuzda kişisel verilerin korunması, Anayasa'nın özel hayatın gizliliği başlıklı 20. maddesinin üçüncü fıkrası, 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK), 4721 sayılı Türk Medeni Kanunu'nun ilgili hükümleri, diğer Kanunlarda yer alan hükümler, 108 Sayılı Sözleşme ile ek protokolleri ve sair düzenlemelerle sağlanmaktadır. KVKK'da yapay zekâya veya onu kullanan sistemlere ilişkin ayrı bir hüküm bulunmamakla birlikte genel veri koruma ilkeleri, ikincil nitelikli düzenlemeler ve Kişisel Verileri Koruma Kurulu kararları, yapay zekâ aracılığı ile kişisel verilerin işlenmesine de uygulanmaktadır. Başlık altında yapay zekâ tarafından işlenen kişisel verilere ilişkin belirleyici ve GDPR'dan farklı olan hususlar ele alınmıştır.

KVKK'nın 4. maddesi kapsamında yer alan genel veri koruma ilkeleri 108 Sayılı Sözleşme ve 95/46/EC Sayılı Direktif ile uyumlu şekilde *"hukuka ve dürüstlük kurallarına uygun olma, doğru ve gerektiğinde güncel olma, belirli, açık ve meşru amaçlarla işlenme, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma; ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar mu-*

79 Ibid.

80 Ibid 47.

81 Ibid 76-77.

82 European Commission, "What does grounds of legitimate interest mean?" <https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/what-does-grounds-legitimate-interest-mean_en> (Erişim Tarihi: 31.07.2023)

hafaza edilme" şeklinde ifade edilmiştir. Bu ilkelere kişisel verilerin işlenmesinin her safhasında riayet edilmelidir[83].

KVKK kapsamında yapay zekâ ile verilerin işlenmesinde belirli ve açık bir amaç doğrultusunda işleme ilkesi gereği, genel geçer amaçlar kullanılmamalı, kullanılacak modelin kişisel verileri işleme sebebi ve amacı açıkça ifade edilmelidir[84]. Bu anlamda yapay zekâ çalışmaları yürütülmesi veya geliştirilmesi şeklindeki genel amaçlar yerine bir eğitim modeli geliştirilerek öğrencilerin başarı sıralamalarının yapılması gibi daha açık ve belirli amaçlar seçilmelidir. Amaç konusunda önemli olan, olay bazında ve seçilen algoritmaya özel bir değerlendirme yapılmasıdır[85]. Ayrıca muhtemel bir veri işleme gerekçesiyle kişisel verilerin gerekli olma ihtimaline binaen depolanması da belirli ve açık amaç ilkesine aykırılık teşkil eder[86].

GDPR'ın 6. maddesinin dördüncü fıkrası çerçevesinde kişisel verilerin işlenmesi için bir kez belirtilen sebebe bağlı veya onun gereği olan diğer amaçlar için de hukuka uygun bir işleme yapılabilecekken KVKK'nın uygulanması açısından aynı durum söz konusu olmayacaktır[87]. Dolayısıyla KVKK anlamında yapay zekâ kullanan sistem ve araçların kişisel veri elde etme amaçlarının, her bir veri işleme faaliyeti için ayrı ayrı belirtilmesi beklenir. KVKK gereği sonraki veri işleme amacının ilk işleme amacı ile uyumlu sayılamayacağı hallerde veri işlemeye devam edilmesi hukuka uygun olmayacaktır[88]. Aksi halde kişinin, kendi verileri üzerindeki hakimiyetini kaybetmesi söz konusu olabilir[89]. Yeni geliştirilmeye çalışılan yapay zekâ modellerinde henüz karşılaşılmayan veri işleme amaçlarının ortaya çıkması ise[90] hali hazırda genel ilkelere ilişkin karşılaşılan zorluklardandır.

Yukarıda yer alan başlıkta ifade edildiği üzere veri minimizasyonu GDPR kapsamında ayrıca belirtilmişken KVKK'nın lafzında bu ilke bulunmaz. Fakat uygulamadaki düzenlemelerde ve temel ilkelerin çerçevesinde veri minimizasyonunun, amaçla bağlantılı, sınırlı, müdahaleci olmayan biçimde veri işleme an-

---

83 Kişisel Verileri Koruma Kurumu, Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi (KVKK Yayınları No 1, Ankara, Aralık 2019).

84 E. Eylem Aksoy Retornaz ve Osman Gazi Güçlütürk, "Yapay Zekâda Kişisel Verilerin Korunması Kanununun Uygulanmasındaki Sorunlara İlişkin Değerlendirmeler" P Çağlayan Aksoy, H C Aksoy (ed.), Kişisel Verilerin Korunmasına Akademik Bakış KVKK Akademi Derleme Çalışması (KVKK Yayınları No 42, Ankara) 421.

85 Ibid.

86 Elif Küzeci, "Kişisel Verilerin Korunması" (4. baskı, On İki Levha Yayıncılık 2020) 231.

87 Aksoy Retornaz ve Güçlütürk (n.84) 422-423.

88 Nafiye Yücedağ, "Kişisel verilerin korunması kanunu kapsamında genel ilkeler" (2019) 1(1) Kişisel Verileri Koruma Dergisi 59.

89 Küzeci (n. 86) 235. Uyumlu olmayan amaç ve sonraki amaçların durumuna ilişkin değerlendirmeler de aynı kaynakta yer almaktadır.

90 Osman Gazi Güçlütürk, "Yapay Zekâ ve Verinin Kullanımı" (On İki Levha Yayıncılık 2022) 308.

lamlarında yer bulduğu görülmektedir[91]. Bununla birlikte Kişisel Verileri Koruma Kurumu'nun Yapay Zekâ Alanında Kişisel Verilerin Korunmasına Dair Tavsiyeler başlıklı dokümanında da geliştirici, üretici, karar alıcı ve servis sağlayıcı aktörler yönünden tavsiyeler bulunmakta, uygulamada yaşanması olası zorluklara yönelik kişisel verilerin korunmasını sağlayan yöntemlere işaret edilmektedir[92].

C. ULUSLARARASI DÜZENLEMELER ÇERÇEVESİNDE BAZI ÇÖZÜM ÖNERİLERİ

Avrupa Birliği'nin 2018 yılından itibaren yapay zekâya ilişkin pek çok ikincil nitelikli düzenlemeleri olmuş, insan merkezli yapay zekâ çalışmaları ile güvenilir yapay zekâ ("trustworthy AI") için etik yönergeler ile politika ve yatırım önerileri oluşturulmuş, Avrupa Komisyonu'nun Yapay Zekâ Üzerine Beyaz Kitap düzenlemesi yapılmış ve son olarak Yapay Zekâ Sorumluluk Direktifi Taslağı ile Yapay Zekâ Tüzüğü Taslağı oluşturulmuştur[93]. Yapay Zekâ Tüzüğü Taslağı Genel Kurul tarafından onaylanmış, yürürlüğe girmesi bakımından yapılacak müzakerelere hazır hale gelmiştir.

1. AB Yapay Zekâ Tüzüğü

14 Haziran'da AB Genel Kurulu'na sunulan ve onaylanan Yapay Zekâ Tüzüğü[94], ilk bağlayıcı/hukuki düzenleme olması ve sektörde faaliyette bulunan tüm aktörleri etkilemesi bakımından oldukça önemlidir. Düzenlemenin kapsamında yapay zekâ kullanımlarına ilişkin dört adet risk grubu belirlenmiş ("kabul edilemez, yüksek, sınırlı, minimum risk grupları şeklinde"), bu gruplara yönelik ayrı değerlendirmeler yapılmıştır. Öncelikle tüzüğün kapsamı;

> *" (a) Birlik içinde yapay zekâ sistemlerinin (YZ sistemleri) piyasaya arz edilmesi, hizmete sunulması ve kullanılması için uyumlaştırılmış kuralları;*

---

91 Bkz. Kişisel Verileri Koruma Kurumu, "İşlenme Amacının Gerektirdiğinden Fazla Kişisel Veri İşlenmesi/Aktarılması (Veri Minimizasyonu İlkesine Aykırılık)" <https://www.kvkk.gov.tr/Icerik/5413/Islenme-Amacinin-Gerektirdiginden-Fazla-Kisisel-Veri-Islenmesi-Aktarilmasi-Veri-Minimizasyonu-Ilkesine-Aykirilik-> (Erişim Tarihi: 31.07.2023) "Covid-19 ile Mücadele Sürecinde Kişisel Verilerin Korunması Kanunu Kapsamında Bilinmesi Gerekenler" başlıklı kamuoyu duyurusu <https://www.kvkk.gov.tr/Icerik/6721/KAMUOYU-DUYURUSU-Covid-19-ile-Mucadele-Surecinde-Kisisel-Verilerin-Korunmasi-Kanunu-Kapsaminda-Bilinmesi-Gerekenler-> (Erişim Tarihi: 31.07.2023)

92 Kişisel Verileri Koruma Kurumu, "Yapay Zekâ Alanında Kişisel Verilerin Korunmasına Dair Tavsiyeler" <https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/25a1162f-0e61-4a43-98d0-3e7d057ac31a.pdf> (Erişim Tarihi: 31.07.2023)

93 European Commission, "Important milestones" <https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence> (Erişim Tarihi: 31.07.2023)

94 EU Document 52021PC0206, "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/?uri=celex%3A52021PC0206> (Erişim Tarihi: 31.07.2023)

(b) bazı yapay zekâ uygulamalarının yasaklanmasını;

(c) yüksek riskli YZ sistemlerine dair özel gereklilikleri ve bu tarz sistemlerin operatörlerinin yükümlülüklerini;

(d) gerçek kişilerle etkileşime geçmeyi amaçlayan YZ sistemleri, duygu tanıma sistemleri ve biyometrik sınıflandırma sistemleri ile görüntü, ses ya da video içeriği üretmek veya bu içerikleri manipüle etmek için kullanılan YZ sistemleri için uyumlulaştırılmış şeffaflık kurallarını;

(e) piyasa izlemesi ve gözetimini düzenlemek[95]*"*

olarak belirtilmiştir.

Düzenlemenin 5. maddesinde, kabul edilemez risk ("prohibited risk") içerdiği belirlenen birtakım yapay zekâ sistemlerinin kullanımı yasaklanmıştır. Bunlar kişilerde fiziksel veya psikolojik zararlar yaratabilecek subliminal teknikler uygulayan, Çin'de olduğu gibi kamu otoritelerince bireylerin çeşitli kıstaslar ile sınırlandırılıp sosyal puanlamaya tabi tutulduğu sistemler, "gerçek zamanlı uzaktan biyometrik tanımlama sistemleri/real-time remote biometric identification systems"dir. Diğer taraftan yüksek risk grubu olarak belirlenen yapay zekâ sistemleri için sıkı bir uygulama rejimi öngörülmüştür. Bu gruba dahil olan yüksek risk durumları genel olarak sağlık, güvenlik ve temel haklara dair "olumsuz etki riski" oluşturabilecek kullanımlardır. Burada üretilen sonuç, riskin boyutları ve potansiyel etkileri, sosyo-ekonomik ve yaş gibi kriterler ışığında değerlendirilecektir.

52. maddede yer alan belirli yapay zekâ sistemleri için şeffaflık yükümlülüğü olarak, istisnai durumlar hariç gerçek kişilerin bilgilendirilmesi ve yapay zekâ sistemlerinin buna göre tasarlanması mecburiyeti getirilmiştir. Ayrıca tıpkı Avrupa Veri Koruma Denetçisi ("EU Data Protection Board") gibi bir AB Yapay Zekâ Denetçisi ("European AI Board"), konu hakkında ulusal otoritelerin görevlendirildiği bir denetim sistemi ve tıpkı GDPR'da olduğu gibi kademeli para cezaları sistemi tasarlanmıştır. Düzenlemenin etkileri salt AB sınırlarında değil çok daha geniş ölçekte her aktör için etkili olacaktır. Ancak kişilere başvuru yolunun öngörülmemesi, farklı mevzuatları kapsamına alması sebebiyle işlevini kaybetme ihtimalinin olması, şeffaflık konusunda "yeni" bir önlem getirmemesi düzenlemeye getirilen eleştirilerden birkaçıdır[96].

---

[95] İstanbul Barosu, Bilişim Hukuku Komisyonu, Yapay Zekâ Çalışma Grubu'nun Türkçe tercümesi <https://www.istanbulbarosu.org.tr/files/docs/AvrupaBirligiYapayZekâya%C4%B0liskinTuzukTeklifiTurkceTercumesi.pdf> (Erişim Tarihi: 31.07.2023)

[96] Armağan Ebru Bozkurt Yüksel, "Avrupa Komisyonu'nun Yapay Zekâ Tüzük Teklifi'ne Genel Bir Bakış" (2022) 0(51) Türkiye Adalet Akademisi Dergisi 41.

2. Sair Alternatifler

Yapay zekânın ön yargılı sonuçlar doğuran veya yanlış bilgi üreten sonuçlarını bertaraf etmek için "güvenilir" hale getirilmesi kapsamındaki "güvenilirlik", içinde farklı çözüm önerilerini barındıran bir çatı kavramdır. Burada amaç bireysel hakların korunduğu düzenlemeler açısından kullanılamaz hale gelen prensiplere işlerlik kazandırmaktır. Konsept yalnızca AB çerçevesinde değil veri korumaya dair düzenleme ortaya koyan hemen her kuruluş/ülke bünyesinde yankı bulmuştur. Örneğin OECD'nin güvenilir yapay zekâ sistemleri için uygulama araçlarını belirttiği dokümanında, şeffaflık ve açıklanabilirliğin geliştirilmesi ihtiyacı özellikle vurgulanmış, kapsayıcı büyüme, sürdürülebilir kalkınma ve esenlik, insan merkezli değerler ve adalet, şeffaflık ve açıklanabilirlik ile hesap verebilirlik şeklinde beş ilke belirlenmiştir[97]. Gereken durumlarda yapay zekânın yaşam döngüsüne insan müdahalesinin mümkün hale getirilmesi, yapay zekânın ürettiği bilgilerin çıktılarının insanlarca anlaşılmasının önemi ve kararlara itiraz hakkı sağlanması, uluslararası iş birliğinin önemi gibi çözüm önerileri de belgede yer alır.

Avrupa Konseyi'nin "Güvenilir Yapay Zekâ için Etik Yönergeler" belgesine göre de yasallığın, etik ilkelere uygunluğun ve sağlamlığın (teknik ve sosyal uyum) önemi vurgulanmış, yapay zekâ sistemlerinin güvenilir kabul edilmesi için karşılaması gereken yedi temel gereksinim kümesi belirlenmiştir. Bunlar insan temsili ve gözetimi, teknik sağlamlık ve güvenlik, mahremiyet ve veri yönetişimi, şeffaflık, çeşitlilik, ayrımcılık yapmama ve adalettir[98]. Bağlayıcı olmayan bu düzenlemelerden okunan ise yapay zekânın yarattığı ve yaratabileceği sorunların açıkça görüldüğü, bunun için "şimdilik" bazı teknik, hukuki ve etik çözümlerin, ekonomik unsurların da hesaba katıldığı çok etkenli bir denge mekanizması gözetilerek dikkate alınabileceğidir.

Doktrinde hali hazırda geliştirilen güvenilir ve etik yapay zekâ yaklaşımları için yapay zekâ tabanlı teknolojilerin arka planında gizlenen yapay zekâ dışı sorunların yeterince dikkate alınmaması, AI ve diğer yüksek teknoloji çözümlerinin yardımıyla her türlü sorunu (teknoloji ve teknoloji dışı) ele almaya meyilli tekno-çözümcü bir zihniyetin ısrarı, belirli (örneğin ticari, politik) çıkarların genel AI-etik tartışması üzerindeki güçlü ve çarpıtıcı etkisi ile bağımsız ve eleştirel felsefi ve etik uzmanlığın yetersiz entegrasyonu konularının önemine ve yarattığı derin çelişkilere değinilir[99].

---

97 OECD, "Tools for trustworthy AI (A framework to compare implementation tools for trustworthy AI systems)" <https://www.oecd.org/science/tools-for-trustworthy-ai-008232ec-en.htm> (Erişim Tarihi: 31.07.2023)

98 EC, "Ethics guidelines for trustworthy AI" <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai (Erişim Tarihi: 31.07.2023)

99 Jan-Christoph Heilinger, "The Ethics of AI Ethics. A Constructive Critique" (2022) 35(61) Philos. Technol 1-20.

Özellikle Google-Amazon gibi dağıtılmış, bulut tabanlı makine öğrenimi ortamları, kötü niyetli algoritmaları kolayca uygulayabilecek, bunları eğitim sürecinin bir parçası olarak sunabilecek ve bu şekilde hassas kullanıcı bilgilerini ezberleyebilecektir[100]. Buna örnek olarak bir yüz tanıma sisteminden görüntüleri kurtaran model ters çevirme saldırıları verilir[101]. Bu durumda kişisel verilerin bütünlük ve güveliğinin temini için sunulan hizmetlerde kullanılan derin öğrenme ve makine öğrenmesi yöntemlerinde aynı zamanda gizliliği koruyan teknik mekanizmaların devreye sokulması gerekecektir. Bu konuda gizlilik sızıntılarının önüne geçmek için diferansiyel gizliliği kullanarak dağıtılmış bir gizlilik koruma mekanizması ("differential privacy-DP") önerilmektedir[102].

Derin öğrenme ve genel olarak makine öğrenmesi için gizlilik koruyucu mekanizmaları inceleyen bir anket çalışmasında, makine öğrenmesinin kullanımındaki artışın veri ve hesaplama kapasitesinin büyümesinden kaynaklandığı, verilerin çoğunun bireylerden elde edildiği ve çok sayıda hassas bilgi içerdiği, veri toplama, eğitim ve çıkarım aşamaları arasındaki belirgin bir dengesizlik bulunduğu belirtilir[103]. Çalışmada gizlilik koruyucu yöntemlerin yanı sıra, gizliliği artıran belirli yürütme modellerine de yer verilmiştir. Bunlar verinin merkezi bir sunucuda toplanmadığı, bunun yerine tüm hesaplamaların yerel olarak (genellikle bir kullanıcının cihazında) gerçekleştiği bir makine öğrenme yöntemi olan federe öğrenme ("Federated Learning"), uygulanan modelin eğitimini birden çok cihaz veya makine arasında bölen bir teknik olan bölünmüş öğrenme ("Split Learning") ve verilerin izinsiz erişime veya değiştirilmesine karşı korunmasına yardımcı bir sistem olan güvenilir yürütme ortamları (Trusted Execution Environments) olarak yer almıştır[104].

Tersine mühendislik genel bir ifadeyle, bir nesnenin nasıl yeniden üretilebileceğini ortaya çıkaran tüm ipuçlarını aramak, bu maksatla yüzeyde görünenin ötesine bakmak ve gizli bir yapı bulmayı amaçlamaktır[105]. Girdiler ve çıktılar arasındaki bağlantının veya işlemin tamamen tespit edilmesinin, sınıflandırılmasının veya nasıl bir belirleyicilik ilişkisi içinde olduğunun anlaşılamadığı durumlarda kuvvetli

---

100 Arachchige vd (n.32) 5828

101 Ibid.

102 Ibid 5828-5829.
DP'nin esasen güçlü gizlilik düzeylerini garanti eden sağlam bir çerçeve oluşturduğu, kişisel verilerin ortaya çıkarılması ihtimalini en aza indirerek maksimum gizlilik sağladığı ifade edilir. Bu yöntem ile belirli bir veri tabanında bulunan bir kişinin verileri hakkında üçüncü bir tarafa ne kadar bilginin ifşa edilebileceğinin sınırları tanımlanmaktadır.

103 Fatemehsadat Mireshghallah vd, "Privacy in Deep Learning: A Survey" (2020) <https://arxiv.org/abs/2004.12254 16. (Erişim Tarihi: 31.07.2023)

104 Ibid 14-15.

105 Harvard Business Review, "You Can Learn Anything Through Reverse Engineering" <https://hbr.org/2021/11/you-can-learn-anything-through-reverse-engineering> (Erişim Tarihi: 31.07.2023)

kara kutu sorunu, bu bağlantının daha sonra tersine mühendislik başta olan bazı çözümlerle anlaşılabildiği hallerde ise zayıf kara kutu sorunu olduğu belirtilir[106].

Uygulamada yapay zekâ modellerinin yorumlanabilirliğini ve açıklanabilirliğini geliştirmek için yöntemler ve teknikler geliştirilmeye ve bu sorun "Açıklanabilir AI" (XAI) veya "Yorumlanabilir AI" şeklindeki çözümlerle aşılmaya çalışılmaktadır. Açıklanabilir yapay zekâ, beklenen etkisi tanımlanabilen bir yapay zekâ modelini tasvir etmek için kullanılır. Savunma İleri Araştırma Projeleri Ajansı DARPA ("Defense Advanced Research Projects Agency"), açıklanabilir yapay zekâyı makinelerin içinde çalıştıkları bağlamı ve çevreyi anladıkları ve zaman içinde gerçek dünya fenomenini karakterize etmelerini sağlayan açıklayıcı modeller inşa ettikleri üçüncü dalga yapay zekâ sistemlerini etkinleştirmesi beklenen bir konsept olarak ele alır[107].

Açıklanabilir yapay zekâ ve açıklanabilir makine öğrenimi, yeni ortaya çıkan/çıkacak yapay zekâlı makineleri anlamak, onlara güvenmek ve onları etkin bir şekilde yönetmek için önem atfedilen bir "eşik" olup çeşitli özellikteki makine öğrenimi tekniklerinin geliştirilmesini gerekli kılar. Modelleri son kullanıcı için anlaşılır ve yararlı açıklama diyaloglarına çevirebilen en gelişmiş insan-bilgisayar ara yüzü teknikleri, ticaret alanını kapsayan bir dizi tasarım seçeneği sağlayacak bir yöntem portföyü ile çoklu sistemler geliştirilmesi vurgusu yapılmıştır[108]. DARPA'nın çoklu sistemlerin geliştirilmesi stratejisi iki temel alandaki sorunlara odaklanır: ilgili olayları heterojen şekilde sınıflandırmak için aşılması gereken makine öğrenimi problemleri ve otonom bir sistemin çeşitli simüle edilmiş görevleri gerçekleştirmesi için karar politikaları oluşturmasına yönelik makine öğrenimi problemleri[109].

Bunun yanında açıklanabilirliğe yönelik de eleştirilerin bulunduğunu belirtmek gerekir. Bunlar genel olarak, farklı kullanıcıların farklı bağlamlarda farklı açıklama biçimleri gerektirmesinden dolayı hâlihazırdaki yöntem ve tekniklerin yine yetersiz kalacağı, sistem tasarımının genellikle rekabet eden talepleri dengelemesi gerekeceği fakat bunun oldukça zor olduğu, açıklanabilirliğin tek başına hesap verebilirlik ile ilgili soruları cevaplayamayacağı, açıklanabilirliğin her zaman öncelik olmayabileceği, açıklamaların da yanlış geliştirilip güven ve anlayış duygusunu yanlış şekilde yönlendirebileceğidir[110].

---

106 Ibid 22-23.

107 Matt Turek, "Explainable Artificial Intelligence (XAI) (Archived)" (DARPA) <https://www.darpa.mil/program/explainable-artificial-intelligence> (Erişim Tarihi: 31.07.2023)

108 Ibid.

109 Ibid.

110 The Royal Society, "Explainable AI: The Basics" (2019) <https://royalsociety.org/ai-interpretability> (Erişim Tarihi: 31.07.2023)

SONUÇ

Yapay zekâ, her geçen gün dijitalleşmenin daha fazla sırrına vakıf olunan küresel ağ toplumunda hem sektörel ölçekte hem de bireylerin hayatında ciddi etkiler doğurmaya başlamıştır. Konunun ekonomik yönünün oldukça belirgin olduğu, şirketlerin ve devletlerin bu ekonomik dönüşümden olabilecek en yüksek faydayı elde etmeyi amaçladığı açıktır. Zira büyük miktarda toplanan verilerin miktarı arttıkça doğal olarak işlenen ve üretilen kişisel veriler de artmakta, bu suretle yapay zekâ beslenmekte, aynı zamanda ondan edinilen ekonomik ve sair faydalar artmaktadır. Bu yinelenen çarkın içinde kişisel verilerin kullanılması sonucunda kişiselleştirilen hizmetler sağlanabilmekte, yüksek olasılık hesapları yapılabilmekte ve en önemlisi kamusal faydaları da olan neticeler alınabilmektedir.

Öncelikle genel veri koruma ilkeleriyle yapay zekâ arasında, henüz yapay zekâya verilerin girdi olarak sunulması aşamasında beliren bir potansiyel çelişki bulunur. Bunlardan belki de en önemlisi yapay zekâdan elde edilen ekonomik/ticari faydanın, ağ toplumu ve rekabetçi ağ ekonomisi ile kişisel verilerin korunmasının bireylere sağladığı faydanın uzlaşması güç iki farklı zeminde oluşudur. Örneğin yapay zekâ erişimi olan yüz tanıma cihazlarının güvenlik sağlamadaki etkisi, güvenlik güçlerine sağlayabileceği manevra kabiliyeti ya da tıbbi ve çevresel kamusal çıkarlar ile kişisel verilerin korunmasını isteme hakkıyla korunan bireysel çıkar başlı başına bir ikilik içindedir. Güvenlik gibi toplumsal menfaatler karşısında ölçülülük yaklaşımı ışığında bireysel çıkarların ve özgürlüklerin de sağlanması hukukun gereğidir. Bilhassa derin öğrenme modellemelerinin gelişmesi ile yapay zekâ tarafından üretilebilen yanlış sonuçların bireysel etkilerinin geri dönülemez bir noktaya gelebilme riskinin bertaraf edilmesi gerekir.

Diğer yandan kara kutu sorunu şeffaflık ve adillik ilkelerinin uygulanmasında problemlere sebep olmaktadır. Nitekim bireylerin kişisel verilerinin işlenmesi süreciyle ilgili ilkenin gerektirdiği açıklıkta aydınlatılması neredeyse olanaksızdır. Bir an için sisteme hem girdi hem çıktı bilgileri verilse dahi elde edilen sonuca nasıl erişildiği anlaşılamamakta, hangi algoritmik işleyişin sonucu o çıktının alındığı sorusu cevapsız kalmaktadır. Bu noktada aynı zamanda rıza sorunu karşımıza çıkar. Yapay zekâ bireylerin bilgilendirilmiş bir rıza verebilmesini bu sebeple güç kılar. Yine bu belirsizlik, yapay zekânın bireyler hakkında yanlış kanaat oluşmasına sebep olabilen, gerçek olmayan veya tam olmayan sonuçlar verdiği hallerde de güçlü biçimde ortaya çıkar. Burada da doğruluk, bütünlük ve hesap verilebilirlik ilkeleri işlerlik sahası bulamayacaktır. Veri minimizasyonu açısından da benzer bir durum söz konusudur. Yapay zekâ büyük veri kümeleri ile geliştiğinden ve işleyiş mantığının çekirdeği "daha fazla veri" olduğundan, "yeterli ve gerekli" miktarda kişisel veri işlenmesi gibi bir sınırlama getirilmesi, yapay zekânın ilerlemesini engelleme riskini barındırır.

Kişisel verilerin işlenmesinde amaç sınırlaması, "belirli ve açık amaç"ın elde edilmesini gerektirir ancak yapay zekâ teknolojilerinin yaygın ve geniş etki alanı bu amaçların belirlenmesini güçleştirmektedir. Örneğin, abonelik tabanlı yayın platformlarının seçim analizlerine dayanan algoritmalarının topladığı kişisel verilerin kapsamı, çok geniş bir potansiyele sahiptir. Bununla birlikte, bu tür bir veri işleme faaliyeti, şirketin ticari hedeflerine ve meşru çıkarlarına hizmet ettiği ve rıza alınarak gerçekleştirildiği için hukuken geçerli kabul edilebilir. Yeni yapay zekâ düzenlemeleri, bu meşruiyet sıkıntısına etkin çözümler bulmayı amaçlamalıdır. Bu durum, yapay zekâ ilgili veri işleme faaliyetlerinin mevcut yasal çerçevelere ne kadar uygun olduğu ve bu uyumun ne ölçüde sürdürülebilir olduğu sorgulamasını ortaya çıkarır.

Üçüncü nesil açıklanabilir, sonuçları gerekçelendirilebilen ve daha güvenilir sonuçlar üreten yapay zekânın elde edilmesi için yapılan çalışmalar konunun belirleyicisi olmaktadır. Diğer taraftan veri koruma alanındaki esnek ve ikincil nitelikte düzenlemeler ortaya konulmaktadır. Ancak belirli olmayan/uygulanışı takdiri olan önlemler uygulamada yapay zekâ ile elde edilen kişisel veriler açısından büyük etkiler doğuruyor gibi gözükmemektedir. Bu açıdan yürürlüğe girmesi beklenen AB Yapay Zekâ Tüzüğü bağlayıcılık, caydırıcılık ve belirlilik (risk grupları ve etki alanları) gibi yenilikleri barındırması sebebiyle -eleştirilere rağmen- umut vadetmektedir.

Sonuç itibarıyla çalışmada, genel veri koruma ilkeleri ve yapay zekâ arasındaki potansiyel çelişkiler ve genel ilkelere ilişkin uygulanabilirlik sorunları üzerinde durulmuştur. İlkeler ve yapay zekâ arasındaki bu çelişkilerin çözümlenmesi, hem bireylerin kişisel verilerini yani hak ve özgürlüklerini korumak hem de yapay zekânın hukuka uygun şekilde ilerlemesini sağlamak adına önemlidir. Çalışmada kapsamında yer verilen çözüm önerileri;

1. Yasa yapıcılar tarafından proaktif bir yaklaşım benimsenmesi; teknoloji, etik ve hukuk arasındaki bu hassas denge korunarak yeni gelişmelerin bağlayıcı tekno-hukuki çözümlerle sınanması, uluslararası iş birliğinin sağlanması,
2. Algoritmaların eğitim veri setlerinin gözden geçirilmesi, sistem geliştiricilerin profil düzeyinin çeşitlendirilmesi,
3. Veri koruma etki değerlendirmesi ve tasarım gereği gizlilik gibi mahremiyet koruyucu ilkelerin yapay zekâ sistemlerinin geliştirilmesi sürecine dahil edilmesi, bu ilkelerin uygulanmasının etkinliğin sağlanması,
4. Kişisel verilerin yapay zekâ sistemleri tarafından işlenmesine ilişkin silme hakkı, bilgi edinme hakkı gibi imkanların aktif bir şekilde kullandırılması,
5. Özgürlüğü bağlayıcı cezaya hükmedilmesi, tıbbi işlemlerin uygulanması gibi kritik faaliyetlerde yapay zekâ destekli programların ön yargılı veya yanlış sonuçlar vermesi risklerinin ayrıca ele alınması,

6. Gerekli durumlarda yapay zekânın yaşam döngüsüne insan müdahalesinin mümkün kılınması, gizlilik sızıntılarının önüne geçmek için diferansiyel gizlilik, federe öğrenme, bölünmüş öğrenme gibi yöntemlerden faydalanılması,

şeklindedir. Çözüm önerilerinde yer alan yöntemler, kişisel veri koruma ilkeleriyle yapay zekânın potansiyel çatışmalarını hem teknolojinin ilerlemesine hem de bireysel hakların korunmasına hizmet eden bir denge gözeterek aşmaya hizmet edebilecektir.

KAYNAKLAR

Arachchige PC M vd, "Local Differential Privacy for Deep Learning" (2020) 7(7) IEEE Internet of Things Journal, 5827-5842.

Bozkurt Yüksel AE, "Avrupa Komisyonu'nun Yapay Zekâ Tüzük Teklifi'ne Genel Bir Bakış" (2022) 0(51) Türkiye Adalet Akademisi Dergisi, 19-46.

Brody N, "What is Intelligence?" (1999) 11(1) International Review of Psychiatry, 19-25.

Çağlayan Aksoy P ve Aksoy H C (ed), Kişisel Verilerin Korunmasına Akademik Bakış KVKK Akademi Derleme Çalışması (KVKK Yayınları No 42, Ankara).

Çekin MS, Yapay Zekâ Teknolojilerinin Hukuki İşlem Teorisine Etkileri (1. Baskı) (İstanbul: onikilevha, 2021).

Choi RY, Coyner AS, Kalpathy-Cramer J, Chiang MF, Campbell JP, "Introduction to Machine Learning, Neural Networks, and Deep Learning" (2020) 9(2) Trans Vis Sci Tech, 1-14.

de Manuel A vd, "Ethical Assessments and Mitigation Strategies for Biases in AI-systems Used During the COVID-19 Pandemic" (2023) 10(1) Big Data & Society,1- 11.

European Parliament, "The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence" (2020) European Parliamentary Research Service: PE 641.530.

Fantin S, Vogiatzoglou P, "Purpose Limitation By Design As A Counter To Function Creep And System Insecurity In Police Artificial Intelligence" (2020) United Nations Interregional Crime and Justice Research Institute (UNICRI).

Fuster G G, "The Emergence of Personal Data Protection as a Fundamental Right of the EU" (Springer 2014).

Glassner A, "Deep Learning: A Visual Approach" (No Starch Press 2021).

Güçlütürk O G, "Yapay Zekâ ve Verinin Kullanımı" (On İki Levha Yayıncılık 2022).

Handbook on European Data Protection Law (2018 edt.) (Luxembourg: Publications Office of the EU, 2018).

Hatipoğlu Aydın D, "Kişisel Verilerin Korunmasına Hukukun Sınırları" (2023) 88(2) İzmir Barosu Dergisi, 141-189.

Heilinger JC, "The Ethics of AI Ethics. A Constructive Critique" (2022) 35(61) Philos. Technol, 1-20.

Johnson M, Jain R, Brennan-Tonetta PV, "Impact of Big Data and Artificial Intelligence on Industry: Developing a Workforce Roadmap for a Data Driven Economy" (2021) 22 Glob J Flex Syst Manag.

Kişisel Verileri Koruma Kurumu, Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi (KVKK Yayınları No 1, Ankara, Aralık 2019).

Küzeci E, "Kişisel Verilerin Korunması" (4. baskı, On İki Levha Yayıncılık 2020).

McCorduck P, "Machines Who Think: A Personal Inquiry into the History and Prospects of Artificial Intelligence" (2nd ed., A.K. Peters, Ltd., 2004).

Mireshghallah F, vd, "Privacy in Deep Learning: A Survey" (2020) <https://arxiv.org/abs/2004.12254>1-24.

Ntoutsi E, Fafalios P, Gadiraju U, "Bias in Data-driven Artificial Intelligence Systems: An Introductory Survey" (2020) 10 WIREs Data Mining Knowl Discovery, e1356.

Paal B, "Artificial Intelligence as a Challenge for Data Protection Law: And Vice Versa" in Voeneky S, Kellmeyer P, Mueller O, Burgard W (eds), The Cambridge Handbook of Responsible Artificial Intelligence: Interdisciplinary Perspectives (Cambridge Law Handbooks, 2022), 290-308.

Rosenblatt F, "The Perceptron: A Probabilistic Model for Information Storage and Organization in the Brain" (1958) 65(6) Psychological Review.

Sagiroglu S ve Sinanc D, "Big Data: A Review in Proceedings of International Conference on Collaboration Technologies and Systems" (CTS, 2013).

Sarker IH, "Deep Learning: A Comprehensive Overview on Techniques, Taxonomy, Applications and Research Directions" (2021) 2 SN Comput Sci, 420.

Schwartz PM ve Solove DJ, "Reconciling Personal Information in the United States and European Union" (2014) 102 California Law Review, 877-916.

Soysal T, "Unutulma Hakkının Avrupa Birliği'nin Genel Veri Koruma Tüzüğü Çerçevesinde İncelenmesi", 0 (2019) Uyuşmazlık Mahkemesi Dergisi, 339-422.

Turing AM, "Computing Machinery and Intelligence" (1950) 59(236) Mind, New Series, 433-460.

Ufert F, "AI Regulation Through the Lens of Fundamental Rights: How Well Does the GDPR Address the Challenges Posed by AI?" (2020) 5(2) European Papers, 1094.

Villaronga EF, Kieseberg P ve Li T, "Humans Forget, Machines Remember: Artificial Intelligence and the Right to Be Forgotten" (2018) 34(2) Computer Law & Security Review, 1-19.

Wang P, "What Do You Mean by AI?" (2008) 171 Frontiers in Artificial Intelligence and Applications.

Yılmaz OG, "Yargı Uygulamasında Yapay Zekâ Kullanımı- Yapay Zekâ Hâkim Cübbesini Giyebilecek mi?" (2021) 66 Adalet Dergisi, 379-415.

Yücedağ N, "Kişisel verilerin korunması kanunu kapsamında genel ilkeler" (2019) 1(1) Kişisel Verileri Koruma Dergisi, 47-63.

Zhang B, Zhu J, Su H, "Toward the Third Generation Artificial Intelligence" (2023) 66(2) Sci China Inf Sci., 1-19.

Elektronik Kaynaklar

Cambridge Dictionary,"intelligence"<https://dictionary.cambridge.org/dictionary/english/intelligence> (Erişim Tarihi: 31.07.2023)

DARPA, Explainable Artificial Intelligence (XAI) (Archived), Dr. Matt Turek. <https://www.darpa.mil/program/explainable-artificial-intelligence> (Erişim Tarihi: 31.07.2023)

EC, "Ethics guidelines for trustworthy AI" <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai> (Erişim Tarihi: 31.07.2023)

Eurostat, "Use of artificial intelligence in enterprises" <https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Use_of_artificial_intelligence_in_enterprises> (Erişim Tarihi: 31.07.2023)

European Commission, "Important milestones" <https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence> (Erişim Tarihi: 31.07.2023)

European Commission, "What does grounds of legitimate interest mean?" <https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/what-does-grounds-legitimate-interest-mean_en> (Erişim Tarihi: 31.07.2023)

EU Document 52021PC0206, "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/?uri=celex%3A52021PC0206> (Erişim Tarihi: 31.07.2023)

General Data Protection Regulation (GDPR), "Recitals" <https://gdpr-info.eu/recitals/> (Erişim Tarihi: 31.07.2023) Harvard Business Review, "You Can Learn Anything Through Reverse Engineering" <https://hbr.org/2021/11/you-can-learn-anything-through-reverse-engineering> (Erişim Tarihi: 31.07.2023)

Heikkila M, "Three ways AI chatbots are a security disaster", (MIT Technology Review, 03.04.2023), <https://www.technologyreview.com/2023/04/03/1070893/three-ways-ai-chatbots-are-a-security-disaster/> (Erişim Tarihi: 31.07.2023)

Kişisel Verileri Koruma Kurumu, "İşlenme Amacının Gerektirdiğinden Fazla Kişisel Veri İşlenmesi/Aktarılması (Veri Minimizasyonu İlkesine Aykırılık)" <https://www.kvkk.gov.tr/Icerik/5413/Islenme-Amacinin-Gerektirdiginden-Fazla-Kisisel-Veri-Islenmesi-Aktarilmasi-Veri-Minimizasyonu-Ilkesine-Aykirilik-> (Erişim Tarihi: 31.07.2023)

Kişisel Verileri Koruma Kurumu, "Covid-19 ile Mücadele Sürecinde Kişisel Verilerin Korunması Kanunu Kapsamında Bilinmesi Gerekenler" başlıklı kamuoyu duyurusu <https://www.kvkk.gov.tr/Icerik/6721/KAMUOYU-DUYURUSU-Covid-19-ile-Mucadele-Surecinde-Kisisel-Verilerin-Korunmasi-Kanunu-Kapsaminda-Bilinmesi-Gerekenler-> (Erişim Tarihi: 31.07.2023)

Kişisel Verileri Koruma Kurumu, "Yapay Zekâ Alanında Kişisel Verilerin Korunmasına Dair Tavsiyeler" <https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/25a1162f-0e61-4a43-98d0-3e7d057ac31a.pdf> (Erişim Tarihi: 31.07.2023)

IBM, "What is artificial intelligence (AI)?" <https://www.ibm.com/topics/artificial-intelligence> (Erişim Tarihi: 31.07.2023) IBM, "What is deep learning?" <https://www.ibm.com/topics/deep-learning> (Erişim Tarihi: 31.07.2023)

İstanbul Barosu, Bilişim Hukuku Komisyonu, Yapay Zekâ Çalışma Grubu'nun Türkçe tercümesi <https://www.istanbulbarosu.org.tr/files/docs/AvrupaBirligi-YapayZekâya%C4%B0liskinTuzukTeklifiTurkceTercumesi.pdf> (Erişim Tarihi: 31.07.2023)

McCarthy J, "What is Artificial Intelligence?" (Computer Science Department, Stanford University, 2007) <http://www-formal.stanford.edu/jmc/>, s.2 (Erişim Tarihi: 31.07.2023)

Nytimes, "Wrongfully Accused by an Algorithm" <https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html> (Erişim Tarihi: 31.07.2023)

OECD, "Tools for trustworthy AI (A framework to compare implementation tools for trustworthy AI systems)" <https://www.oecd.org/science/tools-for-trustworthy-ai-008232ec-en.htm> (Erişim Tarihi: 31.07.2023)

OpenAI, gpt-4 <https://openai.com/research/gpt-4> (Erişim Tarihi: 31.07.2023) Oxford English Dictionary, "artificial intelligence" <https://www.oed.com/view-dictionaryentry/Entry/271625> (Erişim Tarihi: 31.07.2023)

Precendence Research, "ICT Artificial Intelligence (AI) Market" <https://www.precedenceresearch.com/artificial-intelligence-market> (Erişim Tarihi: 31.07.2023)

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> (Erişim Tarihi: 31.07.2023)

Stanford University, "State of AI in 10 Charts: Ethics Infiltates Research" <https://hai.stanford.edu/news/state-ai-10-charts> (Erişim Tarihi: 31.07.2023)

The Data Protection Commission (DPC), Principles of Data Protection <https://www.dataprotection.ie/en/individuals/data-protection-basics/principles-data-protection> (Erişim Tarihi: 31.07.2023)

The New York Times, "Using AI to Detect Breast Cancer That Doctors Miss" <https://www.nytimes.com/2023/03/05/technology/artificial-intelligence-breast-cancer-detection.html> (Erişim Tarihi: 31.07.2023)

The Royal Society, "Explainable AI: The Basics" (2019) <https://royalsociety.org/ai-interpretability> (Erişim Tarihi: 31.07.2023)

The Washington Post, "ChatGPT invented a sexual harassment scandal and named a real law prof as the accused" <https://www.washingtonpost.com/technology/2023/04/05/chatgpt-lies/> (Erişim Tarihi: 31.07.2023)

The White House, "Select Committee on Artificial Intelligence" <https://www.whitehouse.gov/ostp/ostps-teams/nstc/select-committee-on-artificial-intelligence/> (Erişim Tarihi: 31.07.2023)

TR AI, "Yapay Zekâ Zaman Çizelgesi" <https://turkiye.ai/kaynaklar/yapay-zekâ-zaman-cizelgesi/> (Erişim Tarihi: 31.07.2023) Türk Dil Kurumu, "zekâ" <https://sozluk.gov.tr/> (Erişim Tarihi: 31.07.2023)

Wired, "How Wrongful Arrests Based on AI Derailed 3 Men's Lives" <https://www.wired.com/story/wrongful-arrests-ai-derailed-3-mens-lives/> (Erişim Tarihi: 31.07.2023)