Geliş Tarihi:
18.01.2021
Kabul Tarihi:
21.01.2021
Yayımlanma Tarihi:
30.09.2021

Kaynakça Gösterimi: Abudureyimu, Y., & Oğurlu, Y. (2021). Yapay zekâ uygulamalarının kişisel verilerin korumasına dair doğurabileceği sorunlar ve çözüm önerileri. *İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi*, 20(41), 765-782. doi:10.46928/iticusbe.863505

YAPAY ZEKÂ UYGULAMALARININ KİŞİSEL VERİLERİN KORUMASINA DAİR DOĞURABİLECEĞİ SORUNLAR VE ÇÖZÜM ÖNERİLERİ*

Araştırma

Yiliyaer Abudureyimu
Sorumlu Yazar (Correspondence)
İstanbul Ticaret Üniversitesi
aliyarlaw@gmail.com
Yücel Oğurlu
İstanbul Ticaret Üniversitesi
yogurlu@ticaret.edu.tr

Dr. Yiliyaer Abudureyimu, Uluslararası Ticaret ve Avrupa Birliği Hukuku doktora derecesine sahiptir. Başlıca araştırma alanları arasında; uluslararası ticaret hukuku, Avrupa Birliği hukuku, kişisel verilerin korunması hukuku, robot hukuku, yapay zekâ ve hukuk ilişkileri bulunmaktadır.

Prof. Dr. Yücel Oğurlu, İstanbul Ticaret Üniversitesi Hukuk Fakültesi İdare Hukuku Anabilim Dalı profesörüdür ve İstanbul Ticaret Üniversitesi'nde Rektörlük görevini yürütmektedir. Uzmanlık alanları olan İdare Hukuku, İdari Ceza Hukuku, İmar Hukuku, İnsan Hakları Hukuku ve Avrupa Birliği Hukuku alanlarında akademik yayınları yanında, belirtilen sahalarda Lisans ve lisansüstü öğrencilerine dersler vermektedir.

* Makale Yazarın İstanbul Ticaret Üniversitesi Dış Ticaret Enstitüsü Uluslararası Ticaret ve AB Hukuku Doktora Programı, "Karşılaştırmalı Örnekler Üzerinden Yapay Zekâ ve Kişisel Verilerin Korunması" isimli doktora tez çalışmasından uyarlanmıştır.

YAPAY ZEKÂ UYGULAMALARININ KİŞİSEL VERİLERİN KORUMASINA DAİR DOĞURABİLECEĞİ SORUNLAR VE ÇÖZÜM ÖNERİLERİ

Yiliyaer Abudureyimu
aliyarlaw@gmail.com
Yücel Oğurlu
yogurlu@ticaret.edu.tr

ÖZET

Günümüzde hayatımızın ayrılmaz bir parçası haline gelen yapay zekâ teknolojileri, bireylerin davranışları, tercihleri ve özel hayatları hakkında farklı yöntemler ile veri toplayıp, doğrulanamayan çıkarımlar ve tahminler yapabilmektedir. Bu verilerin toplanması, işlenmesi, değiştirilmesi, aktarılması ve çıkarım yapılması süreçleri, muhtelif hukuki sorunlara sebep olabilmektedir. Özellikle kişisel verilerin korunması kapsamında yapay zekâ teknolojileri büyük risk ve sorunlar oluşturmaktadır. Yapay zekâ çeşitli ve zengin kişisel verilerden yararlanarak ayrımcı, önyargılı ve "istilacı" kararlar verebilmektedir. Fakat günümüzde kişisel veri koruma kanunları, insanların yalnız kalma hakkı başta olmak üzere insanların mahremiyetini, kimliğini ve özerkliğini korumak için tasarlanmasına rağmen yapay zekâ teknolojilerinin getirdiği risklerinden ilgili kişileri korumada eksik kalınmaktadır.

Amaç: Çalışmada yapay zekâ uygulamalarının kişisel verilerin korumasına dair doğurabileceği sorunları bulmak ve genel anlamda çözüm önerileri ortaya çıkarmak amaçlanmıştır.

Yöntem: Çalışma betimleme yöntemine dayalı niteliksel bir çalışmadır.

Bulgular: Yapay zekâ döneminde, kişisel verilere yönelik ihlallerin niteliği ve ağırlığında da esaslı farklılıklar olmuştur. Kişisel verilerin korunması, kişilik haklarını, özel hayatın gizliliğini, kişilerin manevi bütünlüğünün, şeref ve onurlarının korunması gibi diğer temel haklarla yakın ilgisi olan bir konudur. Yapay zekâ çağında hassas veriler ile hassas olmayan veriler arasındaki nitelik farklılığının azalması; aynı şekilde, anonimleştirilmiş veri ile kişisel veri arasındaki farklılığın da azalması söz konusudur. Bunlara ek olarak, çıkarımların niteliği sorunu ve çıkarımların sebep olduğu önyargı ve ayrımcı kararlar da diğer ciddi bir problemdir. Yapay zekâ algoritmaların kara kutu ve şeffaflık sorunları, teknik açıdan çözülmeyi bekleyen sıradaki problemler arasındadır. İhlal failinin belirlenmesinin güçlüğü ve ihlalin delillerinin elde edilmesinin teknik olarak kolay olmaması ve yüksek maliyetli olması, yapay zekâ döneminde kişisel verilerin koruma kapsamında ortaya çıkan temel problemler arasında yer almaktadır. Bu sorunlar karşısında yapılması gerekenler ise verinin sadece toplanma aşamasında düzenlemelere tabi tutulmayıp, verilerden türetilen çıkarımların da kişisel verilerin korunması kapsamında değerlendirilmesidir. Kişisel veya kişisel olmayan ve hassas veya hassas olmayan verilerin güncel olmayan, etkisiz ve akışkan sınıflandırmalarından vazgeçilmelidir.

Özgünlük: Türkiye'de yapılan ilgili çalışmalara bakıldığında, kişisel verilerin korunması sorunu, yapay zekâ uygulamalarının doğurabileceği sorunlar ve çözüm önerilerini hukuk perspektifinden inceleyen çalışma özgün niteliktedir.

Anahtar Kelimeler: Yapay Zekâ, Kişisel Veri Koruma, Mahremiyet

JEL Sınıflandırması: K22

PROBLEMS AND SOLUTIONS ABOUT ARTIFICIAL INTELLIGENCE AFFECTING THE PROTECTION OF PERSONAL DATA

ABSTRACT

Artificial intelligence technologies, which have become an integral part of our daily lives today, can collect data about the behaviors, preferences and private lives of individuals with different methods and make non-intuitive and unverifiable inferences and predictions. These data collection, processing, modification, transfer and inference processes can cause various legal problems. Artificial intelligence technologies pose great risks and problems, especially in the scope of protecting personal data. Artificial intelligence is able to make discriminatory, prejudiced and invasive decisions by making use of diverse and rich personal data that have unforeseen great value. However, although the personal data protection laws are designed to protect the privacy, identity and autonomy of the people, especially the right to be alone, they fall short in protecting the relevant people from the risks brought by Artificial Intelligence technologies.

Objective: In the study, it is aimed to find the problems that artificial intelligence applications may cause regarding the protection of personal data and to reveal solutions in general terms.

Method: Method: The study is a qualitative study based on the descriptive method.

Findings: In the era of artificial intelligence, there have also been fundamental differences in the nature and severity of violations of personal data. Protection of personal data is an issue closely related to other fundamental rights such as personal rights, privacy, moral integrity, honor and dignity of individuals. Decreasing the quality difference between sensitive data and non-sensitive data in the age of artificial intelligence; likewise, the difference between anonymized data and personal data is reduced. In addition to these, the problem of the quality of the inferences and the bias and discriminatory decisions caused by the inferences are another serious problem. Black box and transparency problems of artificial intelligence algorithms are among the next problems waiting to be solved from a technical point of view. The difficulty of identifying the perpetrator of the violation and the technical difficulty and high cost of obtaining the evidence of the violation are among the main problems that arise within the scope of protection of personal data in the era of artificial intelligence. What needs to be done in the face of these problems is that the data is not only regulated during the collection stage, but also the inferences derived from the data are evaluated within the scope of the protection of personal data. Outdated, ineffective and fluid classifications of personal or non-personal and sensitive or non-sensitive data should be abandoned.

Originality: Looking at the related studies conducted in Turkey, the study examining the problem of protection of personal data, the problems that may arise from artificial intelligence applications and solution proposals from the perspective of law is original.

Keywords: Artificial Intelligence, Personal Data Protection, Privacy

JEL Classification: K22

GİRİŞ

Günümüzde teknolojilerin gelişmesi insana temas eden her sektörde belirli düzeyde etki oluşturmaktadır. Bilişim ve İletişim Teknolojileri (BİT)'ın yaygın kullanılmasıyla beraber, verilerin otomatize edilmiş sistemler vasıtasıyla hızlı, verimli bir şekilde işlenmesi ve uzun süreli saklanması mümkün hale gelmiştir. Yeni bilgisayar teknolojileri, hayatın birçok alanında dijitalleşme süreçlerini başlatmıştır. (Okur, 2010, s. 2) Hukukun her alanı bu yeniliklerden payını almaya başlamıştır.

Şimdi de yeni bilgisayar teknolojilerinin ulaştığı yepyeni bir aşama olan yapay zekâ sayesinde gerçekleşen verilerin otomatik işlenmesiyle beraber, veriler arası korelasyon ile dağınık verilerin ilişkilendirilip anlamlandırılması da kolay hale gelmiştir. Biz hukukçulara ilk bakışta yabancı gibi duran bu yeni aşama da hukukun birçok alanında değişiklikleri doğurmaya başlamıştır.

Yapay zekâ, genel anlamda kendi deneyimlerinden öğrenebilecek ve muhtelif durumlarda karmaşık problemleri çözebilecek veri sayar sistemlerini tanımlamak için kullanılan bir kavramdır. (Norvig & Russell, 2016, s. 3) Bir diğer ifadeyle, yapay zekâ, daha önce sadece insana özgü olduğunu düşündüğümüz belirli yetenekleri gerçekleştirmeyi hedeflemektedir. Her geçen gün yaşanan şaşırtıcı gelişmelerle bu uzak hedefe adım adım yaklaşılmaya çalışılmaktadır.

Yapay zekâ döneminin en önemli dayanağı, hatta bu motorun yakıtı niteliğinde olan "veri", sahip olanlar bakımından gücü de üretmektedir. Bu güç gerek devletler gerekse özel sektör açısından diğerleriyle rekabet için oldukça önemlidir. Bunun farkına varan kurumlar ve özel teşebbüsler, bir şekilde toplanan kişisel verileri kullanarak muhatap veya hedef kitleye daha kolay ulaşmak isterler. Kurumlar veya özel teşebbüsler, muhatap kitleyi kolaylıkla tespit etmeyi, onlara sundukları hizmetin kalitesini artırmayı ve bazen de bu verileri satarak ticarî kazanç elde etmeyi hedeflemişlerdir. Bu durum, bazılarına göre insanların sadece mahremiyetlerinin ihlali değil, belki de hayati sorunları da içeren başka alanları ilgilendirmektedir. (Varkonyi, 2018, s. 3)

Yapay zekâ döneminde, kişisel verilere yönelik ihlallerin niteliği ve ağırlığında da esaslı farklılıklar olmuştur. Kişisel verilerin korunması, kişilik haklarını, özel hayatın gizliliğini, kişilerin manevi bütünlüğünün, şeref ve onurlarının korunması gibi diğer temel haklarla yakın ilgisi olan bir konudur.

I. KİŞİSEL VERİ KORUMASINDA YAPAY ZEKÂ DÖNEMİNİN OLUŞTURDUĞU SORUNLAR

Yapay zekâ teknolojilerinin risk getirdiği alanlardan birisi, veri sahipleri/ilgili kişilerin bilgi mahremiyeti, yani gizlilik hakkıdır. Bu hakkın ihlali, kişisel verilerin kullanılması ile gerçekleşmektedir. Sanal dünyanın kişilik kavramı üzerindeki olumsuz etkileriyle mücadelede klasik hukuki araçlar etkili olamamıştır. (Civelek, 2011, s. 3) Özellikle kişiyi tanımlayan ve belirleyen kişisel verilerin aktarılması, saklanması, değiştirilmesi, sınıflandırılması ve aranmasına ilişkin alternatiflerin artışı temel hak ve özgürlüklere zarar vermeksizin korunmalarının nasıl sağlanacağı sorusunu gündeme taşımıştır. (Civelek, 2011, s. 6) Çünkü bu kapsamda, kişisel verilerin korunması

sorunu yaşanırken, verilerin sadece miktarının değil, aynı zamanda niteliğinin de değişime uğradığı görülüyor. (Cukier, 2014) Klasik anlayışın bu değişimi yakalayabilmesi için, temel yaklayış ve değerleri koruyarak ancak yeni araçlara uyum sağlayacak bir esneklik kazanması gerekir.

Avrupa Birliği (AB) *"Genel Veri Koruma Tüzüğü"* madde 4'te belirtilen kişisel veri tanımında, bu kavramın *bilgi*, *kişiye ilişkin olma* ve *kimliği belirli veya belirlenebilir bir kişi* olmak üzere üç temel unsurdan oluştuğu söylenebilir. Bu üç unsur, Madde 29 Çalışma Grubu tarafından yayımlanmış olan kişisel veri kavramına ilişkin belirsizlik ve yaklaşım farklılığını bertaraf etmek amacı taşıyan görüş metnini ile de örtüşmektedir. (European Commission, 2007, s. 6)

Yapay zekâ döneminde kişisel verilerin korunması konusunda muhtelif düzenlemeler yapılmış ve yapılmaya devam etmektedir. Genel olarak bakıldığında, bu tür düzenlemelerin iki gruba ayrıldığını görebilmekteyiz. Bunlardan ilk grup olan Kara Avrupası Hukuk Sisteminde kişisel verileri sosyal ve hümanist bir yaklaşımla temel insan hakları ve/veya kişilik hakkı kapsamında değerlendiriliyor. Bu yaklaşımda kişisel veri kavramı, anayasal anlamda bir temel hak (insan hakkı) olarak nitelendirildiğinde dahi, korunma altında olan değerin özel hayatın gizliliği (mahremiyet) olduğu görülmektedir. Özel hayatın gizliliği ise medeni hukuk terminolojisinde de var olan "kişilik hakkı" kapsamındaki kişisel değerler çerçevesinde bir terimdir. (Hatemi, 2018, s. 66) AB'nin kişisel veri koruma modeli, birleşik bir kişisel veri koruma kanununun çıkarılması ile karakterize edilebilir. Bu sebeple de birleşik model olarak da adlandırılır. AB çerçevesinde Almanya başta olmak üzere, üye ülkelerde yeknesak veri koruma kanunları yayımlanmıştır. (Hanhua, 2018, s. 79-80) Bu durum, Birliğe üye devletlerin hukuk siztemlerini uyumlaştırmak zorunda olmalarının sonucudur.

İkinci grup olan Anglo-Sakson Hukuk Sistemlerinde kişisel verilerin korunması düzenlemelerinin diğer bir boyutunun ön plana çıktığı görülmektedir. Bu yaklaşıma göre, kişisel verilerin korunması konusu, ekonomik ve iktisadi bir yaklaşım ile mülkiyet ve/veya fikri haklar kapsamında değerlendirilmektedir. (Aksoy, 2008, s. 215) Nitekim, bu yaklaşımda kişisel veri, yalnızca sahibinin kişiliğinin bir uzantısı olmayıp aynı zamanda ilgili kişiliğin bir ürünü olarak da kabul edilmektedir. (Akkurt, 2020, s. 21) Diğer bir ifadeyle, Anglo-Sakson modelinin kişisel verilerin korunması yaklaşımında bir yandan kişilik hakkı kapsamında korunma amaçlanırken diğer yandan da kişiliğin dışında olan ve ona bağlı olarak ortaya çıkan bir ürün olarak düşünülmektedir.

Bu iki grubun yaklaşımlarını karşılaştırdığımızda, AB müktesebatı çerçevesinde gelişen kapsamlı yasama modeli, kişisel verilerin yeknesak kanuni düzenlemelerle korunmasına odaklanmakta ve kişisel verilerin korunması için oldukça açık standartlar ortaya koymaktadır. Fakat bu yaklaşım, kişisel veri haklarının özel nitelik ve içeriğini özel haklar açısından doğrulayamamıştır. Bu yaklaşımın, devletin kamu iktidarının rolünü vurguladığı için soyut kurallar, katı denetim ve yönetim vb. sorunlar ortaya çıkardığı düşünülmektedir. (Lingjie, 2019, s. 167-168)

Amerika Birleşik Devletleri (ABD) düzenlemelerinin piyasa odaklı olduğu, konuya ticaret ve sanayinin ihtiyaçlarına göre pragmatik yaklaştığını, bunun da kişi güvenliği ve kişisel verilen

korunmasının felsefi ve hukuki dayanakları bakımından rahatlıkla eleştirilebilir olduğunu ifade etmek gerekir.

İster AB'deki gibi tek bir yasa ile kişisel verilerin korunmasını amaçlayan düzenlemeler olsun isterse ABD'deki gibi sektörel bazda kişiyi tanımlayan bilgilerin korunmasını ön planda tutan rejimler olsun, yapay zekâ döneminde beklenmedik hukuki ve fiili sorunlar ile karşılaşılmaktadır. Bu sorunların bazıları hukuk sisteminin ilkelerinden kaynaklanmaktaysa da bazılarının teknik ilerlemelerden ve uluslararası rekabetten kaynaklandığı görülmektedir.

A. Kişinin Paylaşım İradesi Her Zaman Gerçek mi?

1950'li yıllarda henüz sınırlı sayıda verinin olduğunu ve internet ortamı gibi verilerin hızlı dolaşımı imkânlarının olmadığı dönemlerde kişilerin veri güvenliği konusu günümüzdeki kadar yaygın bir problem alanı oluşturmuyordu. Ancak günümüzde verilerin yeni bilgisayar teknolojileri kanalıyla Büyük Veri kapsamında yaygınlaşması, insanların gönüllü veya gönülsüz olarak bilgilerini paylaşmak zorunda kalmaları, büyük muammalara yol açmıştır.

Cep telefonları ya da kişisel bilgisayarlar üzerinden kullanmak istenilen herhangi bir programın kullanıcıdan bir dizi sıralı erişim onayı olmaksızın kullanıma izin verilmemesi, bu programları kullanmak zorunda olan belirli kullanıcıların gönülsüzce ve zorunlu olarak verilerini paylaşmaya mecbur kılınmaları gerçeği ortaya çıkmaktadır. İşte tam da bu noktada, kişilerin verilerinin kullanıma açılmasında, onların özgür iradelerini ne kadar kullanılabildikleri hususu temel bir problemdir. İnsanın iradesi üzerinde, ister hileli yollarla isterse onun kullanmak zorunda olduğu bir programa erişmek için ilgili-ilgisiz birçok kişisel verisini kullanmaya mecbur bırakmak bazen hukuki, bazen de ahlaki bir sorun olarak önümüzde durmaktadır.

Bir bilgisayar programını mutlaka kullanmak zorunda olan kişilerin verdikleri bu gönülsüz rıza en azından onların iradelerinin sakatlanması boyutunda olmasa bile mecazi anlamda iradelerinin gölgelenmesi olarak düşünülebilir. Yapay zekâ döneminde tartışılması gereken bu problem gün geçtikçe daha ileri aşamalarda yaşanacaktır.

B. Hassas Veri Sorunu

Yapay zekâ döneminde ihdas edilen kişisel veri düzenlemelerine bakıldığında, hassas veriler ile hassas olmayan veriler arasındaki farkın azalmasından kaynaklanan risklerin ortaya çıktığı görülmektedir. Günümüzde en katı kişisel veri koruma kanunu niteliğinde olan *"Genel Veri Koruma Tüzüğü (Tüzük)"* sağlık, etnik köken veya siyasi inançlar gibi özellikleri tanımlayan "özel kategoriler" için daha fazla koruma sağlamıştır. Örneğin, söz konusu verilerin kullanılması izni için daha yüksek standartlar ve sınırlı izin verilen kullanımlara imkân tanımıştır. Avrupa Birliği Adalet Divanı (ABAD) da bir genel mahkeme kararında Tüzük'ün 9'uncu maddesinin uygulanmasını, veri sorumlusunun hassas verilere ulaşma niyetinin olması ve toplanan verilerin ilgili kişi hakkındaki çıkarımları ortaya çıkarmak için göreceli olması ile sınırlamıştır. (Kathleen Egan, Margaret Hackett ve Avrupa

Parlamentosu, 2012) Her iki şart da yapay zekâ döneminde kişisel verilerin korunması için birer risk oluşturmaktadır.

Bu konuda, ABAD ile Madde 29 Çalışma Grubu farklı yorum sergilemektedir. Madde 29 Çalışma Grubunun yorumuna göre hassas veriler, yalnızca doğası gereği hassas bilgiler içeren verileri değil, aynı zamanda kişiye ilişkin hassas bilgilerin çıkarılabileceği verileri de kapsamaktadır. (Kathleen Egan, Margaret Hackett ve Avrupa Parlamentosu, 2012) Bir diğer ifade ile, belli hassas olmayan verileri işleyerek ilgili kişi ile ilgili hassas veriler çıkarılabiliyorsa, giriş yapılan veriler artık hassas veri niteliği kazanacaktır. Zarsky'nın görüşünde her şey potansiyel olarak hassas veri olabilmekte, sadece bizim onu henüz hassas veri olarak bilmiyor olmamız bu korumaya engel olabilmektedir. (Zarsky, 2017, s. 47) Nitekim, günümüz yapay zekâ teknolojisinde hassas olmayan verilerin işlenmesi sonucunda kişiye özel hassas verilerin üretilebilmesi kolayca gerçekleştirilebilen bir işlemdir. Kısacası yapay zekâ teknikleri, hassas olmayan verilerin, kolaylıkla hassas verilerin ihlali sonucunda oluşacak riskleri oluşturabilmesini mümkün hale getirmiştir. Facebook, Wechat ya da herhangi biri gibi sosyal medyadaki iletişim/eğlence aracının size ait bütün veriler üzerinden sanal kimlikler oluşturması, alışkanlık, ilgi ve beklentilerinizi izlemesi ve bundan ticari ya da başka amaçlarla yararlanması ihtimali her zaman vardır.

Örnekleri biraz daha artırırsak işin daha farklı boyutları da ortaya çıkar. Nesnelerin İnterneti, akıllı şehirler aracılığıyla gerçekleştirilen veri işlemleri, bağlantılı verilerin öncülüne dayanmaktadır. Akıllı şehirlerde, sensör verileri, WiFi verileri ve konum verileri insanların yavaş faaliyetleri hakkında dahi veri topluyor. Ağ bağlantılı sensörlere sahip otomobillerin sürücüleri, yolculuk verilerine göre davranışsal profillemeye tabi tutuluyor. (Wachter, The GDPR and the Internet of Things: A Three-Step Transparency Model, 2018, s. 10) Bu tür teknolojiler tarafından üretilen veriler, bireylerin davranışları, tercihleri ve özel yaşamları hakkında sezgisel olmayan ve doğrulanamayan çıkarımlar ve tahminler yapmak için kullanılabiliyor. Bu çıkarımlar, öngörülemeyen değere sahip oldukça, çeşitli ve zengin özelliklere sahip verilere dayanır ve genellikle bireylerin özel hayatlarının hassas özelliklerine dayanan ayrımcı, önyargılı ve saldırgan kararların ortaya çıkmasına zemin hazırlayan bir risk ortamı oluşturabiliyor. (Wachter, Normative Challenges of Identification in the Internet of Things: Privacy, Profiling, Discrimination, and the GDPR, 2017, s. 34)

Öte yandan ilgili kişilerin özel hayatlarını tanımlayan hassas veriler, kullanıcıların davranışlarını ve karşılanmamış ihtiyaçlarını ortaya çıkarmak için giderek daha fazla yaygın şekilde toplanabilir, paylaşılabilir ve analiz edilebilir veriler olarak görülmektedir. (Wachter, Data Protection in the Age of Big Data, 2019, s. 6)

Özetle, yapay zekâ döneminde bir yandan ilgili kişinin haberi olmaksızın daha fazla sayıda hassas veri toplanabilirken, diğer yandan da hassas olmayan veriler aracılığıyla türetilen yeni veriler, hassas veri niteliği taşıyabilmektedir.

Halbuki yukarıda bahsi geçen Tüzük, sadece sınırlı kapsamdaki verilerin hassas veri olduğunu belirlemiş, çıkarımların hassas veri niteliğinde olduğu durumları ihmal etmiştir. Halbuki bu çıkarımların, yapay zekâ teknikleri kullanılarak gerçekle ilişkisi olmayan sanal üretimlerinin en az hassas veriler kadar korunmaya layık olduğunu, hatta gerçeği yansıtmayacak içerik üretimlerinin ortaya çıkabileceği de dikkate alınırsa daha büyük bir kişilik hakkı ihlaline sebep olabileceği unutulmamalıdır.

C. Çıkarımların Niteliği Meselesi

Yapay zekâ döneminde önemli sorunlarından bir diğeri de çıkarımların kullanılmasının yaygınlaşmasıdır. Gün içinde kullandığımız sosyal medya platformlarından medikal cihazlara kadar farklı araçlarla kolaylıkla toplanan veriler, çıkarımlar elde etmede "ekonomi klas veri" olarak değerlendirilmektedir. Çıkarımların kullanımı konusunda örnek vermek gerekirse, Netflix'ın kullanıcıların ırklarına göre çıkarımlarda bulunup onlara "ırksal hedefleme" yolu ile film afişlerini tasarlaması ve tavsiyelerde bulunması (Arnold, 2018); Facebook'un LGBT kullanıcılarının verilerinden yaptığı "çıkarım"larla "eşcinsel tedavisi" reklamlarını önermesi (Cook H. H., 2018); Amazon'un sadece öksürük sesine dayanarak ne zaman hasta olacağını tahmin edebilen ve ilaç tavsiye edebilen yeni Alexa sürümünü geliştirmesi (Cook J. , 2018) ilginç güncel örnekler olarak verilebilir.

Çıkarımların temel sorunu, çıkarım işleminden ötürü, çıkarım sebep olabilecek olan ayrımcılıktan kaynaklanmaktadır. Çıkarımlar, kişilerin işsiz kalmasına, ırkî, dinî, felsefî düşüncesini dolaylı olarak aşağılayan davranışlara maruz kalmasına neden olabilir. Bu tür sorunların çözülmesi, çıkarım mekanizmasının nasıl işleyeceği ile ilgilidir. Bir başka deyişle, bu konu, çıkarım probleminin teknik açıdan çözülmesi gereken kısmıdır. Konunun kullanılan algoritmaların önyargıya sebep olacak yollarının öngörülerek engellenmesiyle ilgili olduğunu söylemeliyiz. Çıkarımlardan kaynaklanan ayrımcılık, önyargılı kararlar sorun oluştururken, çıkarımların niteliği konusunda da bir muğlaklık göze çarpmaktadır.

Nitekim ABAD, çıkarımların, kişisel veri tanımı kapsamına girip girmediği konusunda açık bir karara varmamıştır. 2014 yılındaki verilen bir kararında (YS ve Diğerleri, 2014), çıkarımları kişisel veri kapsamı dışında tutarken, 2017'deki bir kararda (Peter Nowak v Data Protection Commissioner, 2018) çıkarımları kişisel veri olarak tanımlamıştır. Fakat sonraki bir davada ABAD, kişisel veri ile ilgili tüm hakları ilgili kişiye tanımamış ve veri koruma kanununun bireylerin nasıl değerlendirileceği konusunda bir hak içermediğini açıkça belirtmiştir. Sonuçta Tüzük'ün, sadece girdi verilerinin yasal olarak elde edilmesini sağlamak, tanımlamak ve korumak için tasarlandığı anlaşılıyor. Daha önceki örneklere baktığımızda, çıkarımların kişisel veri sayılıp sayılmayacağı ve nasıl korunacağı hakkında ABAD ve Madde 29 Çalışma Grubunun farklı yorumlarının olduğu görülmektedir. Bu farklı görüşleri burada Tablo 1'de görebiliriz:

Tablo 1. Çıkarımların Niteliği Hakkında Görüşler

Madde 29 Çalışma Grubu'nun Görüşü	*ABAD'nın Görüşü*
Kişisel verilerdir	Kişisel verilerin olup olmadığı belirsizdir
Tüzük haklarının çoğu için geçerlidir	Haklar yalnızca amaca göre geçerli olabilir.
Karar verme aşamasını (Decision- Making) daha şeffaf ve hesap verebilir kılmak için veri korumasından yararlanabilir.	Veri korumanın amacı içeriğe bağlı karar verme sürecini düzenlemek değildir. (CPDP, 2019)

Kaynak: Yazar Tarafından Oluşturulmuştur.

Madde 29 Çalışma Grubu'nun görüşüne göre kişisel veriler üç basamaklı model ile belirlenebilir: Bir kişi hakkındaki veriler (içerik); bir kişiye erişmek için kullanılan veriler (amaç); bir kişiyi etkileyen veriler (sonuç). Çalışma gurubu, sübjektif bilgileri, görüşleri ve değerlendirmeleri de kişisel veri olarak değerlendirdiği için çıkarımlar açık şekilde kişisel veri niteliğini kazanmış olacaktır. (Article 29 Data Protection Working Party, 2018) ABAD'nın konu hakkında verdiği kararlar değerlendirildiğinde, kişilerle ilgili yapılan hukuki analizleri, kişisel veri kapsamında değerlendirmediği görülmektedir. ABAD, Nowak kararında da Madde 29 Çalışma Grubunca buna benzer bir yorumlama yapmış olsa da bu hukuki analizin kişisel veri niteliği kazanması, onunla ilgili bütün haklardan yararlanılabileceği anlamına gelmeyeceği vurgulanmıştır. (Peter Nowak v Data Protection Commissioner, 2018) Kanımızca, bu durumda, hukuki savunmalar ve hukuk süreçlerinde ortaya çıkan hukuki değerlendirmeler içeren veriler, ilk bakışta kişisel veri koruması içinde görülmeyebilir. Fakat bu verilerin kişilerin özel hayatlarına dair mahrem bilgiler olması halinde, rızaları dışında paylaşılamamaları gerekir.

Çıkarım ile ilgili bir diğer mesele de, yapay zekâ tarafından yapılan çıkarımlar ile ticari sır arasındaki ilişkiden kaynaklanmaktadır. Yapay zekâ teknoloji şirketleri, ilgili kişilerin verilerinden türetilen çıkarımların ticari sır kapsamındaki verilerin gizli tutulması gerektiği savunulmuştur. (Protalinski, 2011) Örneğin Facebook, bu konuda ticari sır kapsamında ilgili kişi ile alakalı olan çıkarımların ilgili kişiye verilme talebini reddetmiştir. Halbuki, şirketlere ait olan verilerin onların rızası olmadan bu şekilde paylaşılması, aleyhinde sonuçlar ve algı doğurabileceğinden bu izinsiz paylaşımlar veri güvenliğinin ihlali anlamına gelmektedir.

Özetle, yapay zekânın hızlı ilerlemesi ile beraber, sadece hassas veriler değil, kişisel veriler ya da henüz kişisel veri niteliği kazanmayan verilerden, yapay zekâ tarafından çıkarılan çıkarımlar da kişisel veriler gibi korunma kapsamındaki hukuki değerleri ihlal edebilmektedir.

D. Anonimleştirilmiş Veri Sorunu

Yapay zekâ döneminde hassas veri ile hassas olmayan verilerin ayrımı zor olduğu gibi kişisel veri ile kişisel olmayan veri arasındaki ayrımın uygulanabilir olup olmadığı da diğer bir problem

oluşturmaktadır. Yapay zekânın geldiği ileri seviye göz önüne alındığında, teknik bakımından anonimleştirilmiş verilere (kişisel veri niteliği olmadığı varsayılan verilere) dayanarak işlenen ve doğrudan veri sahiplerini belirlenebilir kılan tahmini çıkarımlar karşısında ilgili kişinin nasıl korunacağı belirsizlik teşkil etmektedir. (Özdaş, Akıncı, & Türkkan, 2020, s. 230) Anonimleştirilmiş veri tekniği Yapay zekâ döneminde etkisiz durumda kalmıştır. Nitekim, teorik açıdan bütün anonimleştirilmiş veriler içeriklerinin tersi yönünde kullanılabilir ve bir kişiyle ilgili hale getirilebilmektedir. (Ohm, 2009, s. 1758)

Diğer yandan, Tüzük'teki ilgili kişilerin haklarının hiçbirisi anonim veriler için geçerli olmadığından yapay zekâ döneminde diğer bir sorun daha ortaya çıkmaktadır. Çünkü anonimleştirilmiş olan veriler bile kullanıcı profilleri oluşturmak için kullanılabilir ve bu nedenle, belirli bir kişiyi tanımlamaya gerek kalmadan gizlilik ihlali ve ayrımcılık riskleri meydana çıkabilir. (Hildebrandt, 2018, s. 320) Bu noktada Tüzük'ün, verilerin nasıl kullanıldığına; ilgili birey ve gruplar üzerinde veri toplama aşamasının etkisine odaklandığını söyleyebiliriz. (Mittelstadt, 2017, s. 482) Yani Tüzük'ün en büyük eksikliklerinden birisinin de bütün düzenlemeleri veri toplama aşamasına yönelik kurgulaması olduğunu söyleyebiliriz.

E. Algoritmik Önyargı, Kara Kutu ve Şeffaflık Sorunu

Şeffaflık konusu yalnızca özel sektörde şirketler için değil, çok daha fazlasıyla devletler ve İdare için de geçerlidir. Ticari sırlar ve devlet sırları hariç tutulursa, şeffaf yönetim, başarı ve güvenlik için aranan bir ön şarttır.

İdarenin şeffaf olması, kamu yönetimi ve idare hukuku açısından önemli bir araçtır ve "6 Sigma" kuralları arasında yer alır. Şeffaflık, idareye güven bakımından önemli olduğu kadar, kişilerin toplanan kişisel verilerinin İdare tarafından nerede ve ne amaçla kullanılacağının bilinmesini de gerektirir. Bu yönüyle, kamu kurumlarıyla paylaşılan kişisel verilerin mutlaka ilgililerin rızası alarak paylaşılması, onlardan habersizce başkalarının eline geçmesine izin verilmemesi gerekir.

Yapay zekâ denildiğinde en temel araç olarak akla algoritma gelir. Nasıl ki veriler yapay zekânın temelini oluşturuyorsa, algoritmalar da yapay zekânın özüdür. Geçmişte geleneksel algoritmalar, izlenecek kurallar ve belirli veri noktalarına eklenecek parametreler, "elle" programlanıyordu. Yapay zekâ döneminde ise algoritmalar, modellerin veri kümelerinden çıkarılma şeklini ve öngörülerin yapılma yöntemlerini büyük ölçüde değiştirmiştir. (Otterlo, 2013, s. 46) Nitekim artık sadece "elle" değil, algoritma bizzat bunu yapabilmektedir. Fakat açıkça söylemek gerekir ki, insan denetiminden yoksun kalan yapay zekâ algoritmalarının önyargı veya ayrımcılıkla hareket edebildikleri gözlemlenmektedir. Yapay zekâ, otomatik karar çıkarmak istiyorsa verilerin beslenmesine ihtiyaç duyar. Verilerin kendisinde önyargı veya ayrımcılık varsa, yapay zekâ otomatik karar verme doğal olarak önyargı veya ayrımcılıkla dolu olacaktır. Bunun dışında, verilerin bazen sosyal gerekçelerle zayıf kesimler lehine pozitif ayrımcılıkla değerlendirilmesi gereken konularda nötr karar vermesi de istenilen sonuçları doğurmayacaktır.

Örneğin, 2016 yılında yapılan ilk "Yapay Zekâ Uluslararası Güzellik Yarışması"nda yapay zekâyı eğitmek için kullanılan fotoğraflar içeresinde belli oranda siyahi yüzler yer almadığı için, yarışı kazananların büyük çoğunluğu beyazlar olmuştur. (Bates & Blackmore, 2017) Beyaz ya da siyah tercihinde, belli bir algoritmanın bu tür önyargı oluşturabilecek veriler ile beslenerek eğitilmesi, toplum düzeyinde düşünüldüğünde daha ciddi seviyede önyargı ve ayrımcılığa yol açabilmektedir. Bir diğer ayrımcılık örneği Google'ın fotoğraf uygulamasında ortaya çıkmıştır. Dijital fotoğraf albümlerindeki resimleri etiketleyen yapay zekâ otomatik etiketleme sistemi, siyahların görüntülerini "goriller" olarak sınıflandırmıştır. (The Economist, 2016, s. 18) Bu da farkında olunsun veya olunmasın açık ve ciddi bir saldırıdır. Kısacası, insanların deri renkleri geleneksel anlamda kişisel veri kategorisine girmese de başka veriler ile birleştirildiğinde, biyometrik veri sınıfına bile dâhil edilebilecek kadar büyük ayrımcılık riskleri taşıyabilmektedir.

ABD'de, IBM, Amazon ve Microsoft gibi şirketler polislere farklı düzeylerde yapay zekâ yüz tanıma yazılımları sağlamaktaydı. Bu tür araçlar sayesinde polisler, sokaklarda devriye gezerken cep telefonu kameralarındaki resimleri hızlı bir şekilde karşılaştırabilir ve bunları polis veri tabanındaki yüz binlerce fotoğrafla eşleştirebiliyordu. Bu yapay zekâ yüz tanıma yazılımları polisin yeteneğini güçlendirmekle birlikte algoritmik önyargıya sebep olabilmektedir. Bu sebeple, Haziran 2020 de, IBM, Amazon ve Microsoft art arda polislere yüz tanıma teknolojisi sağlamayacakları konusunda açıklamalar yapmıştır. Bunların arasında Amazon, yüz tanıma yazılımlarının polislere satışını bir yıl boyunca askıya alacağını söylemişken, Microsoft, durdurma süresini yüz tanıma teknolojisini düzenleyen federal yasanın yürürlüğe girmesinden sonraya uzatmıştır. IBM yapay zekâ yüz tanıma yazılımı sağlamayı kalıcı olarak durdurduğunu açıklamıştır. (Oktay, 2020)

Algoritmik Adalet Birliği'nin kurucusu Joy Buolamwini 2017 senesinde IBM, Microsoft ve Despise adlı üç şirketin yapay zekâ yüz tanıma algoritmaları üzerinde bir önyargı testi yapmıştır. Üç Afrika ülkesinden ve üç Avrupa ülkesinden yüz fotoğrafları toplamış. Araştırmada kadınların doğru tanınma oranının erkeklere göre daha düşük, siyahi ırkların tanınma oranının beyazlardan daha düşük olduğu ortaya çıkmıştır. Bunların arasında IBM'in algoritmasının en büyük hata oranına sahip olduğu ortaya çıkmış; beyaz tenli erkekler ve siyahi tenli kadınlar için hata oranı %34,4 olmuştur. (Yangyang, 2020) Bu problemin önleyici kolluk önlemleri kapsamında yaygınlaştırılmasının, bütün diğer ülkelerde de benzer problemler doğurması kaçınılmazdır. Çünkü, eldeki fotoğrafların benzerliği üzerine kurulu bir algoritmanın, aynı ırk veya milletten farklı ancak benzeyen kişileri kategorik olarak suçlu olarak teşhis etmesi riskli ve onur kırıcıdır.

Algoritmik önyargı aslında yapay zekânın bir diğer sorunu olan kara kutudan kaynaklanmaktadır. Yapay zekâ birçok katmanda karmaşık karar verebilse de geliştiricilerin kararlarının arkasındaki mantıksal ilkeleri tanımlamaları veya açıklamaları kolay değildir. Yapay zekâ algoritmasının giriş katmanı ve çıktı katmanı arasında "kara kutu" oluşmaktadır. (Nott, 2017) Bu sebeple, belli bir veri kümesinden işlenip ortaya çıkan ve sonucu beslenen veriler ile açıklamak zor oluyor. Algoritmanın

neden bu tür sakıncalı çıkarımlar yaptığı sorusu yapay zekâyı geliştiren uzmanlar tarafından bile cevaplanamamaktadır. Ayrıca, saldırıların ortaya çıkardığı derin sinir ağlarının kırılganlığı, bu yöntemlerin temelindeki öğrenilmiş karar verme süreçlerine şüphe uyandırmaktadır. (Kızrak, 2020) Sonuçta, yapay zekânın otomatik karar vermede ayrımcılık ve kara-kutu sorunları kişisel verilerin korunması için daha karmaşık zorluklar oluşturmaktadır.

Özetle, yapay zekâ döneminde önyargı ve ayrımcılık problemleri, kişisel verilerin korunması konusunda engeller oluşturmaktadır. Nitekim, kişisel veriler ile eğitilip önyargılı olmayan ve ayrımcılık yapmayan yapay zekâ oluşturmak teknik açısından hiç de kolay değildir. Çünkü kişisel verilerin veri kümelerine göre, kendinden kaynaklanan potansiyel önyargı ve ayrımcılık olabilmektedir. Hukuki açıdan yapay zekâ ile işlenen kişisel verilerin nasıl bir düzenleme altında önyargıya ve ayrımcılığa yol açmayacağı da kolay çözülecek bir problem değildir. Algoritmaların neden önyargılı kararları ele alacağını anlamak, algoritmik kara kutu üzerinde iyi çözümü belirlemek ve algoritmaların zararının sorumluluğunu paylaştırmak da aynı şekilde kolayca çözülebilecek bir iş değildir. (Ishii, 2019, s. 516) Yapay zekâ döneminde bu konuların çok boyutlu ve geniş bir bakış açısıyla ele alınması gerekmektedir.

Bazı veri bilimcileri, ilgili kişilerin kullanılan modeli veya kuralları tanımasına ve algoritmaları incelemesine izin vermek için algoritmaların şeffaf olması gerektiğini, böylece bir yapay zekâ sistemi tarafından verilen yanlış kararın araştırılabilir ve ilgileri sorumlu tutulabilir hale getireceğini savunmaktadır. (House of Commons, Science and Technology Committee, 2016, s. 17-18) Ancak, günümüzde çoğu yapay zekâ sistemleri, belirli bir karara varmak için bir neden sağlamak üzere kurulmamaktadır. Örneğin, Google DeepMind'in AlphaGo'su son derece sıra dışı bir hamle yaparak insan rakibini yendiğinde, AlphaGo ekibi bu hareketi neden yaptığını açıklayamamıştır ve şu anda insanlar yapay zekânın mantığını tam olarak anlayamamış veya çözememiştir. (House of Commons, Science and Technology Committee, 2016, s. 17) Viktor Mayer ve Kenneth Cukier'e göre günümüzde yapay zekâ teknolojileri, insanları "nedensel" olarak düşünmekten "korelasyon" şeklinde düşünmeye zorlamaktadır. (Schönberger & Cukier, 2013, s. 57) Bu görüşe göre artık, bütün bilgi edinme yöntemleri nitelik açısından değişime uğrayacaktır. Klasik yöntemlerden tamamen uzaklaşarak, yani nedensellikten uzaklaşarak, korelasyon aracılığıyla karar vermeye zorlayacağı belirtilmiştir. Sonuçta, alınan kararların bir nedeni olmayacak bu kararın sadece bir korelasyon sonucu olduğu açıklaması ile yetinilecektir. Google AlphaGo örneğinde, yapay zekânın yaptığı hamle, nedensel bir açıklama ile cevaplanmadığından o hamlenin rakibi yenme ile olan korelasyon ilişkisi ile cevaplamak daha mantıklı olacaktır. Bu tip sistemler, karar verilirken veri kümelerindeki korelasyonlardan faydalanmaktadır. (Kızrak, 2020) Sonuçta büyük şeffaflık problemlerine yol açabilmektedir.

Şeffaflık sorunundan dolayı ilgili kişi, verilerindeki hataları bulamaz ve bu hatalar üzerinden ayrımcı sonuçlara maruz kalırsa "algoritmik kara kutu" sorunu çözülemediği sürece -profil oluşturma da dahil- veri işleme sürecine karşı çıkamayacaktır. Bu şekilde kişisel verilerinin nasıl kullanıldığı ve

daha da önemlisi, ilgili kişi hakkındaki kararların nasıl alındığına dair bilgilere erişemeyecektir. (Buttarelli, 2016) Bu sebeple, ilgili kişilerin verilerinin kullanımına uygun bir şekilde izin vermesi/rıza göstermesi imkânsız hale gelmesi yapay zekâ döneminde kişisel verilerin korunması konusundaki önemli engellerdendir.

F. İhlal Failini Belirleme, Delil Elde Etme Sorunu

Gelişmiş ülkelerin hemen hepsinde hukuk kişisel verilerin ihlaline karşı kişiler korur ve bu verilerin kişilerin rızası olmaksızın paylaşılması yasaklanır. Günümüzden yaklaşık 20-30 yıl kadar öncesine kadar bu genel ve klasik koruyucu yaklaşım, kanuni düzenlemeler ve sıkı bir uygulama ile ihtiyaçları karşılayabiliyor iken "Büyük Veri" aşamasına geçilmesiyle artık işin boyutları ve ölçekleri de değişmiştir. Yine aynı durum, kişisel verilerin korunması ile ilgili "mahremiyet" kavramının nasıl algılanması gerektiği ile ilgili bir meseleye dönüşmektedir.

Geleneksel yöntemlerde kişisel verilerin toplanması çoğu zaman yüz yüze gerçekleştirilir ve bu sebeple veri işleyenin bulunması daha kolaydır. Sonuçta, veri ihlali gerçekleştiğinde ihlal öznesinin belirlenmesi hiç de zor değildir. Fakat, yapay zekâ döneminde veri ihlalini yapan öznenin bulunması artık eskisi kadar kolay olmamaktadır. Yapay zekâ üretici ve operatörlerinin belirlenebilmesi durumunda, haksız fiil sorumluluğu kuramına göre, yapay zekâ üreticisi ve operatörü, haksız fiil sorumluluğundan sorumlu tutulabiliyor. Sorumluluk konusunda yapay zekânın hayali kişilik (Legal Fiction Said) olarak değerlendirilebileceği ve kendisinin haksız fiil sorumluluğunu taşıyabileceğine dair bir görüş vardır. Fakat, yapay zekânın kendisinin hayali kişilik olarak kabul edilip edilemeyeceği de tartışmalı konudur. (Weigang, 2020, s. 169) Doğal olarak bu durumda ihlal eden özneyi belirlemenin hukuki kişilik bağlamında olduğu kadar sorumluluk konusu bakımından da zor olduğunu söyleyebiliriz.

Fakat, günümüzde yapay zekâ üreticileri ve operatörlerinin bulunması, pratikte ayrı bir güçlük oluşturabiliyor. Mesela, internette çevrimiçi olduğunuz sürece, kullanıcıya yönelik çeşitli bağlantı noktaları bulunabiliyor. Ne zaman, nerede ve hangi verileri topladıklarını, kimin topladığını belirlemek kişiler bakımından hiç de kolay değildir. Hayatımızın her köşesinde yer almaya başlayan kamera ve mikrofonların kişilerin verilerini toplayıp nerelere ilettiği, bu verilerin nasıl ve hangi amaçlarla işlendiği sorunlarının cevabını bulmak, devletler ve büyük şirketler için kolay olabilse de kişiler açısından neredeyse imkansızdır.

Kişisel verilerin işlenme amacı yapay zekâ döneminde takibi ve kaynaklarını bulma bakımından tamamen belirsizleşti. Veri ihlali konusunda delil elde etmek de diğer bir problemi oluşturmaktadır. Çünkü ihlal öznesi gerçek veya tüzel kişi değil, çeşitli elektronik bağlantı noktaları ve teçhizatlar ile gerçekleştirilmektedir. Elektronik bağlantı noktaları, kişisel verileri gözetlemek için yapay zekâ teknolojisini kullanabilir. Bu durum, doğal bir şekilde delil elde etmeyi zorlaştırıyor ve ihlalin delili elde edilse bile maliyeti oldukça yüksek oluyor. Gerçekleşen veri ihlali ortada olsa bile, hangi bağlantı noktasından toplandığı, saklandığı, işlendiği ve aktarıldığı belli olmayan verilerle gerçekleştiğini

araştırıp bulmak yüksek maliyetli olabilir. Ellerinde veri toplamak için kullanılan bağlantı noktaları hariç hiçbir teknoloji desteğe sahip olmayan mağdurlar, delil elde etme bakımından oldukça pasif bir durumda kalabilecektir.

Yukarıda belirtilen zorluklar yapay zekâ döneminde kişisel verilerin korunması düzenlemelerinin önünde engel teşkil edebilmektedir. Bu engelleri teknik açıdan çözmeye çalışırken, hukuki boyutlarıyla değerlendirme çalışmaları da ihmal edilmemelidir. Günümüzde başta AB olmak üzere, yapay zekâ etiği, yapay zekâ düzenlemeleri konusunda çalışmalar sürdürülmektedir. Fakat bütün bu çalışmaların disiplinler arası, diğer bir ifadeyle bilişimciler ile hukukçuların ortak çalışmalarıyla yapılması gerekir.

SONUÇ

Teknolojinin hızlı ilerlemesi ile beraber, yapay zekâ gibi teknolojiler hayatımızda kolaylıklar sağlamıştır. Bu kolaylıklar karşısında, hukuki alanda ortaya çıkan birçok teknik problem kadar hukuki ihtilafla da karşılaşmaktayız. Yapay zekâ döneminde en sıkı karşılaşılan problemlerden biri, kişisel verilerin korunması sorunudur. Günümüzde mukayeseli hukuktaki kişisel verilerin korunması düzenlemelerine bakıldığında yapay zekâ döneminde bazı eksikliklerin ortaya çıktığı görülür.

Hassas veriler ile hassas olmayan veriler arasındaki nitelik farklılığının yapay zekâ tekniği aracılığıyla azalması; aynı şekilde, anonimleştirilmiş veri ile kişisel veri arasındaki farklılığın da azalması söz konusudur. Bunlara ek olarak, çıkarımların niteliği sorunu ve çıkarımların sebep olduğu önyargı ve ayrımcı kararlar da diğer ciddi bir problemdir. Yapay zekâ algoritmaların kara kutu ve şeffaflık sorunları, teknik açıdan çözülmeyi bekleyen sıradaki problemler arasındadır. İhlal failinin belirlenmesinin güçlüğü ve ihlalin delillerinin elde edilmesinin teknik olarak kolay olmaması ve yüksek maliyetli olması, yapay zekâ döneminde kişisel verilerin koruma kapsamında ortaya çıkan temel problemler arasındadır.

Bu sorunlar karşısında yapılması gerekenler, verinin sadece toplanma aşamasında düzenlemelere tabi tutulmayıp, verilerden türetilen çıkarımların da kişisel verilerin korunması kapsamında değerlendirilmesidir. Nitekim yapay zekâ teknolojileri, verileri direk kullanmaktan ötürü, ileride farklı amaçlarla tekrar kullanabilme ve yaptığı çıkarımlardan yine çıkarımlar yapabilme riskini oluşturmaktadır.

Kişisel veya kişisel olmayan ve hassas veya hassas olmayan verilerin güncel olmayan, etkisiz ve akışkan sınıflandırmalarından vazgeçilmelidir. Bu kategoriler, yalnızca toplandıkları andaki verilerin niteliğini yansıtır. Fakat, daha sonraki kullanımını ve olası dönüşümlerini (örneğin, cinsel yönelim, sağlık durumu veya cinsiyet çıkarımı) göz ardı etmektedir. Anonim hale geldiğini zannettiğimiz veriler yapay zekâ teknolojileri yardımıyla, paylaşılması halinde kişilerde rahatsızlık uyandıracak verilere dönüşmesi halinde hassas veriler kategorisine bile girebilecektir. Sonuç olarak, kişisel veri koruma düzenlemelerinin anonimleştirilmiş veri tuzağına düşmemesi ve türetilen çıkarımlar ve

onların yeniden kullanılmasıyla çıkarılabilecek yeni aktif verilerin kullanılmasının kişisel veri kapsamında korunması kadar, kişi haklarının ve mahremiyetinin de korunması kapsamında yeni baştan dikkate alınması gerekir.

KAYNAKÇA

Akkurt, S. S. (2020). Kişisel Veri Kavramının Hukuki Niteliğine İlişkin Yaklaşımlara Mukayeseli Bir Bakış. *Kişisel Verileri Koruma Dergisi, 2*(5).

Aksoy, H. C. (2008). The Right to Personality and It's Different Manifestations as the Core of Personal Data. *Ankara Law Review, 5*(2).

Arnold, B. (2018, 10 22). *Netflix User Anger over 'racial Targeting' of Movie Posters*. 01 05, 2021 tarihinde Yahoo: https://www.yahoo.com/entertainment/netflix-users-anger-racial-targeting-movie-posters 104325948.html adresinden alındı

Article 29 Data Protection Working Party. (2018). *Guidelines on Personal data breach notification under Regulation 2016/679.* Brussels: European Commission.

Bates, R., & Blackmore, N. (2017). The Privacy Challenges of Big Data and Artificial Intelligence. *KennedysLaw*.

Buttarelli, G. (2016). *A Smart Approach: Counteract The Bias in Artificial Intelligence*. 12 05, 2020 tarihinde Europa: https://edps.europa.eu/press-publications/press-news/blog/smart-approach-counteract-bias-artificial-intelligence_en adresinden alındı

Civelek, D. Y. (2011). *Kişisel Verilerin Korunması ve Bir Kurumsal Yapılanma Önerisi.* Ankara: Bilgi Toplumu Dairesi̇ Başkanlığı.

Cook, H. H. (2018, 08 25). *Facebook Accused of Targeting Young LGBT Users with 'gay Cure' Adverts*. 01 05, 2021 tarihinde telegraph: https://www.telegraph.co.uk/news/2018/08/25/facebook-accused-targeting-young-lgbt-users-gay-cure-adverts/ adresinden alındı

Cook, J. (2018, 10 09). *Amazon Patents New Alexa Feature That Knows When You're Ill and Offers You Medicine*. 12 08, 2020 tarihinde telegraph: https://www.telegraph.co.uk/technology/2018/10/09/amazon-patents-new-alexa-feature-knows-offers-medicine/ adresinden alındı

CPDP. (2019, 02 11). *Profiling, Microtargeting and A Right to Reasonable Algorithmic Inferences*. youtube: https://www.youtube.com/watch?v=nN_sGuNhaOM adresinden alındı

Cukier, K. (2014, 6). *Big Data is Better Data*. 01 08, 2021 tarihinde TED: www.ted.com/talks/kenneth_cukier_big_data_is_better_data adresinden alındı

European Commission. (2007). *Article 29 Working Party Opinion 4/2007 on the Concept of Personal Data.* Brussels: European Commission.

Hanhua, Z. (2018). *Kişisel Bilgilerin Korunması Kanunu (Uzman Öneri Taslağı) ve Mevzuat Araştırma Raporu (个人信息保护法(专家建议稿)及立法研究报告).* Pekin: Kanun Yayınları.

Hatemi, H. (2018). *Kişiler Hukuku.* İstanbul: On İki Levha.

Hildebrandt, M. (2018). Profiling and the Identity of the European Citizen. İn profiling the european citizen. *Springer Dordrecht*, 303–343.

House of Commons, Science and Technology Committee. (2016). *Robotics And Artificial Intelligence: Fifth Report of Session.* https://www.publications.parliament.uk/pa/cm201617/cmselect/cmsctech/145/145.pdf adresinden alındı

Ishii, K. (2019). Comparative Legal Study on Privacy and Personal Data Protection for Robots Equipped with Artificial Intelligence: Looking at Functional and Technological Aspects. *AI & Soc*(34), s. 509 – 533.

Kathleen Egan, Margaret Hackett ve Avrupa Parlamentosu, T-190/10 (Genel Mahkeme'nin (Beşinci Daire) 5 28, 2012).

Kızrak, A. (2020, 12 05). *Açıklanabilir, Sorumlu ve Güvenilir Yapay Zekâ*. Medium: https://ayyucekizrak.medium.com/a%C3%A7%C4%B1klanabilir-sorumlu-ve-g%C3%BCvenilir-yapay-zeka-bece897c5ea9 adresinden alındı

Lingjie, K. (2019). *Kişisel Veri Gizliliğinin Korunması (个人资料隐私的法律保护).* Wuhan: Wuhan Üniversitesi Yayınları.

Mittelstadt, B. (2017). From Individusal to Group Privacy in Big Data Analytics. *Philosophy & Technology*, 475–494.

Norvig, P., & Russell, S. J. (2016). *Artificial Intelligence: A Moderin Approach.* New Jersey: Prentice Hall.

Nott, G. (2017). Explainable Artificial Intelligence': Cracking Open the Black Box of AI. *Computer World*.

Ohm, P. (2009). Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. *UCLA Law Review*, 1701–1777.

Oktay, M. (2020, 06 11). *Amazon'dan Yüz Tanıma Teknolojisinin Polis Tarafından Kullanımına Erteleme Kararı*. AA: https://www.aa.com.tr/tr/dunya/amazondan-yuz-tanima-teknolojisinin-polis-tarafindan-kullanimina-erteleme-karari/1872922 adresinden alındı

Okur, N. (2010). Anayasa Hukuku Açısından Özel Hayatın Gizliliği ve Korunması. *Gazi Üniversitesi Sosyal Bilimler Enstitüsü Yayınlanmamış Doktora Tezi*.

Otterlo, V. (2013). A machine learning view on profiling. *Privacy, Due Process and The Computational Turn: Philosophers of Law Meet Philosophers of Technology* (s. 41–64). London: Routledge.

Özdaş, M., Akıncı, A., & Türkkan, A. (2020). Yapay Zeka ve Hukuk 4.0: Yapay Zekanın Hukuk Uygulamalarına Etkisi. M. K. İyigün içinde, *Oyun Değiştiren Yapay Zeka.* İstanbul: Beta Yayıncılık.

Peter Nowak v Data Protection Commissioner, C-434/16 (ABAD 02 26, 2018).

Protalinski, E. (2011, 10 12). *Facebook: Releasing Your Personal Data Reveals Our Trade Secrets*. zdnet: https://www.zdnet.com/article/facebook-releasing-your-personal-data-reveals-our-trade-secrets/#:~:text=ZDNet%20Academy-,Facebook%3A%20Releasing%20your%20personal%20data%20reveals%20our%20trade%20secrets,trade%20secrets%20and%20intellectual%20property adresinden alındı

Schönberger, V. M., & Cukier, K. (2013). *Büyük Veri: Yaşama, Çalışma ve Düşünme Şeklimizi Dönüştürecek Bir Devrim.* İstanbul: Paloma Yayınları.

The Economist. (2016). Artificial Intelligence: Ethics, Frankenstein's Paperclips.

Varkonyi, G. G. (2018). Robots with AI: Privacy Considerations in the Era of Robotics. *Law 4.0* (s. 1-12). Györ: Széchenyi István University.

Wachter, S. (2017). Normative Challenges of Identification in the Internet of Things: Privacy, Profiling, Discrimination, and the GDPR. *Computer Law Security Review*, 436–449.

Wachter, S. (2018). The GDPR and the Internet of Things: A Three-Step Transparency Model. *Law Innovasion Technol*, 266-294.

Wachter, S. (2019). Data Protection in the Age of Big Data. *Nature Electronics*, 6-7.

Weigang, L. (2020). 人工智能时代对个人数据法律保护的挑战 (Yapay Zeka Çağında Kişisel Verilerin Yasal Olarak Korunmasının Önündeki Zorluklar). *法制博览*, 168 – 171.

Yangyang, W. (2020, 06 19). *IBM 宣布退出人脸识别，是道德楷模还是商业投机？*. Sina: https://tech.sina.com.cn/i/2020-06-19/doc-iircuyvi9289158.shtml?cref=cj adresinden alındı

YS ve Diğerleri, C-141/12 (ABAD 07 17, 2014).

Zarsky, T. (2017). Incompatible: The GDPR in the Age of Big Data. *Seton Hall Law Review, 47*(4(2)).