

T.C.
İSTANBUL TİCARET ÜNİVERSİTESİ
DIŞ TİCARET ENSTİTÜSÜ
ULUSLARARASI TİCARET VE AB HUKUKU ANA BİLİM DALI
ULUSLARARASI TİCARET VE AB HUKUKU DOKTORA
PROGRAMI

KARŞILAŞTIRMALI ÖRNEKLER
ÜZERİNDEN YAPAY ZEKÂ VE KİŞİSEL
VERİLERİN KORUNMASI

Doktora Tezi

YILYAER ABUDUREYIMU

200003529

İstanbul, 2021

T.C.
İSTANBUL TİCARET ÜNİVERSİTESİ
DIŞ TİCARET ENSTİTÜSÜ
ULUSLARARASI TİCARET VE AB HUKUKU ANA BİLİM DALI
ULUSLARARASI TİCARET VE AB HUKUKU DOKTORA
PROGRAMI

KARŞILAŞTIRMALI ÖRNEKLER
ÜZERİNDEN YAPAY ZEKÂ VE KİŞİSEL
VERİLERİN KORUNMASI

Doktora Tezi

YILYAER ABUDUREYIMU

200003529

Danışman: Prof. Dr. Yücel OĞURLU

İstanbul, 2021



T.C. İSTANBUL TİCARET
ÜNİVERSİTESİ

T.C.
İSTANBUL TİCARET ÜNİVERSİTESİ
FİNANS ENSTİTÜSÜ

DOKTORA TEZİ ONAY FORMU

Dış Ticaret Enstitüsü Uluslararası Ticaret ve AB Hukuku Ana Bilim Dalı Uluslararası Ticaret ve AB Hukuku Doktora programı öğrencisi...YILIYAER ABUDUREYIMU'nun..... KARŞILAŞTIRMALI ÖRNEKLER ÜZERİNDEN YAPAY ZEKÂ VE KİŞİSEL VERİLERİN KORUNMASI...başlıklı tez çalışması, Enstitümüz Yönetim Kurulu 22.02.2021 tarih ve 173/2 sayılı kararıyla oluşturulan jüri tarafından **oybirliği** ile Doktora Tezi olarak kabul edilmiştir.

UNVANI, ADI SOYADI

ÜNİVERSİTE

TEZ DANIŞMANI	: PROF. DR. YÜCEL OĞURLU	İSTANBUL TİCARET ÜNİVERSİTESİ
JÜRİ ÜYESİ	: PROF. DR. HÜSEYİN HATEMİ	İSTANBUL TİCARET ÜNİVERSİTESİ
JÜRİ ÜYESİ	: DR. ÖĞRETİM ÜYESİ EBRU ŞENSÖZ MALKOÇ	İSTANBUL TİCARET ÜNİVERSİTESİ
JÜRİ ÜYESİ	: PROF. DR. MEHMET MELEMEN	MARMARA ÜNİVERSİTESİ.
JÜRİ ÜYESİ	: PROF. DR. MELİKŞAH YASİN	İSTANBUL ÜNİVERSİTESİ.

ÖZET

Günümüzde gündelik hayatımızın ayrılmaz bir parçası haline gelen yapay zekâ teknolojileri, bireylerin davranışları, tercihleri ve özel yaşamları hakkında farklı yöntemler ile veri toplayıp, sezgisel olmayan ve doğrulanamayan çıkarımlar ve tahminler yapabilmektedir. Bu veri toplama, işleme, değiştirme, aktarma ve çıkarım yapma süreçleri muhtelif hukuki sorunlara sebep olabilmektedir. Özellikle kişisel verilerin korunması kapsamında yapay zekâ teknolojiler büyük risk ve sorunlar ortaya çıkmaktadır. Yapay zekâ öngörülemez kadar büyük değere sahip olan çeşitli ve zengin kişisel verilerden yararlanarak ayrımcı, önyargılı ve istilacı karar verebilmektedir. Günümüzde kişisel veri koruma yasaları özel hayatın gizliliği hakkı başta olmak üzere mahremiyetini, kimliğini ve özerkliğini korumak için tasarlanmasına rağmen ilgili kişileri yapay zekâ teknolojilerinin getirdiği risklerinden korumada yeterli kadar etkili olamamaktadır.

Çalışmada AB, ABD, Çin ve Türkiye olmak üzere dört farklı perspektiften yapay zekâ çağının kişisel verilerin korunmasına olan etkileri incelenmiştir. Yapay zekânın teknik yönünden yola çıkarak, hukuki ve teknik açıdan kişisel verilerin korunmasını yönelik öneriler ve izlenebilecek stratejiler sunulmuştur.

Anahtar Kelimeler: *Yapay Zekâ, Kişisel Veri Koruma, GDPR, Mahremiyet, Özel Hayatın Gizliliği*

ABSTRACT

Artificial Intelligence technologies, which have become an integral part of our daily life, collect data with different methods relevant to our behaviors, preferences and private lives and make predictions and unverifiable inferences. 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 with unforeseen great value. However, although the personal data protection laws are designed to protect the privacy, identity and autonomy of people, they cannot protect the relevant people from the risks brought by Artificial Intelligence technologies.

Working in the EU, USA, China and Turkey to the protection of personal data in problems were examined from four different perspectives. Regarding to the technical aspect of Artificial Intelligence, suggestions and strategies for the protection of personal data in legal and technical terms are presented.

Keywords: Artificial Intelligence, Personal Data Protection, GDPR, USA, EU, China, Privacy

TEŞEKKÜRLER

Doktora eğitim süreci boyunca birçok kişi desteğini aldım, onlara şükranlarımı sunmak isterim.

İlk olarak, ilk kez İstanbul Ticaret Üniversitesine ayak bastım günden doktora tezimi bitirinceye kadar tüm maddi ve manevi desteği ve faydalı tavsiyeleri için danışmanım Prof. Dr. Yücel OĞURLU'ya teşekkür ederim. Doktora eğitim sürecinde gösterdiği ilgi ve daimî yardımı için değerli hocamız Dr. Öğr. Üyesi Ebru ŞENSÖZ MALKOÇ hocamıza, tez yazımı sırasında rehberlik eden faydalı tavsiyeleri için Prof. Dr. Hüseyin HATEMİ'ye içten şükranlarımı sunarım. İş hayatımda bana yol gösteren, destek sağlayan Prof. Dr. Mehmet Melemen'e ayrıca teşekkür ederim.

Son olarak, bana doktora eğitim hayalimi gerçeğe dönüştürmede en büyük desteği sağlayan eşim Rahile'ye ve eğitim süreci boyunca benimle zaman geçirme fırsatlarından mahrum kalan sevgili kızım Hüsne ve oğlum Hasan'a şükranlarımı sunarım. En önemlisi uzakta kalan, yanımda olmasa bile her zaman yanımdaymış gibi medet veren annem ve babama sonsuz şükranlarımı arz ediyorum.

YILIYAER ABUDUREYIMU (Aliyar)

İstanbul, 2021

İÇİNDEKİLER

Sayfa No.

ÖZET.....	iii
ABSTRACT	iv
TEŞEKKÜRLER	v
İÇİNDEKİLER	vi
TABLO LİSTESİ	x
ŞEKİL LİSTESİ.....	xi
KISALTMALAR	xii
GİRİŞ	1
1. YAPAY ZEKA VE TARİHSEL GELİŞİMİ	11
1.1. Yapay Zekânın Tanımı.....	11
1.1.1. Zekâ Kavramı	11
1.1.2. Yapay Zekâ.....	12
1.2. Yapay Zekânın Tarihsel Gelişimi.....	18
1.2.1. Tarih Öncesi.....	18
1.2.2. Dartmouth Konferansı Sırası	19
1.2.3. Altın Çağı	21
1.2.4. Kış Mevsimi.....	22
1.2.5. Yeniden Canlanma.....	22
1.3. Yapay Zekâ Teknikleri.....	24
1.3.1. Makine Öğrenimi.....	24
1.3.2. Derin Öğrenme	27
1.3.3. Yapay Sinir Ağları.....	29
1.3.4. Uzman Sistemler.....	32
1.3.5. Bulanık Mantık	33
1.3.6. Genetik Algoritma	34
1.4. Yapay Zekâ Çeşitleri	36
1.4.1. Reaktif Yapay Zekâ	36
1.4.2. Sınırlı Hafızalı Yapay Zekâ	37
1.4.3. Zihin Teorisi	37

1.4.4. Kendi Kendinin Farkında Olan Yapay Zekâ.....	38
1.5. Yapay Zekânın Pratik Uygulamaları	38
1.5.1. Doğal Dil İşleme.....	38
1.5.2. Hukuk Alanında Akıllı Robot/Hakimler	39
1.5.3. Sürücüsüz Araçlar.....	41
1.5.4. Görme Sistemleri	42
1.5.5. Konuşma Tanıma.....	42
1.6. Yapay Zekanın Bugünü ve Geleceği	43
1.6.1. Günümüze Kadar Yapılan Yapay Zekâ ile İlgili Çalışmalar	43
1.6.2. Yapay Zekânın Günümüzdeki Durumu	45
1.6.3. Yapay Zekânın Geleceği.....	46
2. KİŞİSEL VERİ VE KARŞILAŞTIRMALI HUKUKTA KORUNMASI.....	47
2.1. Kişisel Veri Kavramı	49
2.1.1. Tanımı.....	49
2.1.2. Kişisel Veri Kavramının Unsurları	55
2.1.2.1. Bilgi	55
2.1.2.2. Belirli veya Belirlenebilir Kişi	56
2.1.2.3. Bilginin Kişiye ilişkin Olması.....	57
2.1.3. Kişisel Veri Türleri	58
2.1.3.1. Hassas Kişisel Veri	58
2.1.3.2. Hassas Olmayan Kişisel Veri.....	62
2.1.4. Kişisel Veri ve Mahremiyet	63
2.1.4.1. Benzerlikler.....	63
2.1.4.2. Farklılıklar.....	64
2.2. Kişisel Veri Korunması Sorunu ve Tarihsel Gelişimi	66
2.2.1. Kişisel Veri Korunması Sorunu	66
2.2.2. Kişisel Verilerin Korunması Tarihsel Gelişimi.....	67
2.3. Kişisel Veri Koruma Yöntemleri.....	69
2.3.1. Kara-Avrupa Koruma Yöntemi	70
2.3.2. Anglo-Sakson Koruma Yöntemi.....	71
2.4. Uluslararası Düzenlemeler	74
2.4.1. Ekonomik İşbirliği ve Kalkınma Örgütü	74
2.4.2. Birleşmiş Milletler	76
2.4.3. Avrupa Konseyi.....	77
2.4.3.1. Avrupa İnsan Hakları Sözleşmesi	78
2.4.3.2. 108 Sayılı Sözleşme	78

2.5. Avrupa Birliğinde Kişisel Verilerin Korunması.....	82
2.5.1. 95/46/AT Sayılı Direktif.....	83
2.5.1.1. Kapsam ve İlkeleri	84
2.5.1.2. İlgili Kişilerin Hakları	85
2.5.1.3. Getirildiği Yenilikler.....	85
2.5.1.4. Özellikleri ve Eksiklikleri	87
2.5.2. Avrupa Birliği Temel Haklar Şartı	91
2.5.3. Genel Veri Koruma Tüzüğü	92
2.5.3.1. Uygulama Alanı	94
2.5.3.2. Haklar ve Yükümlülükler.....	95
2.5.3.3. Getirildiği Temel Yenilikler.....	99
2.5.3.4. Karşılaştığı Sorunlar	105
2.6. Karşılaştırmalı Hukuktaki Düzenlemeler	107
2.6.1. ABD’de Kişisel Bilgilerin Korunması.....	108
2.6.1.1. Mahremiyetin Korunmasının Ortaya Çıkışı	108
2.6.1.2. ABD Mahremiyet Koruma Düzenlemeleri	113
2.6.1.3. Kaliforniya Tüketici Gizliliği Yasası	116
2.6.2. Çin’de Kişisel Bilgilerin Korunması	118
2.6.2.1. Siber Güvenlik Kanunu.....	121
2.6.2.2. Çin Medeni Kanunu	123
2.6.2.3. Kişisel Bilgilerin Korunması Kanunu Taslağı	124
2.6.3. Türkiye’de Kişisel Verilerin Korunması.....	127
2.6.3.1. Türk Hukukunda Kişisel Verilerin Korunması	127
2.6.3.2. KVKK	129
3. YAPAY ZEKA ÇAĞINDA KİŞİSEL VERİLERİN KORUNMASI	136
3.1. Yapay Zekâ Çağında Kişisel Veri İşlemenin Etik Boyutları	136
3.1.1. Algoritmik El	137
3.1.2. Azalan Yalnız Kalma Fırsatları	138
3.1.3. Filtre Balonu	139
3.1.4. Sosyal Kredi Sistemi.....	140
3.2. Yapay Zekâ Çağında Kişisel Veri İşlemenin Özellikleri.....	146
3.2.1. Akıllı Bağlantı Noktalarından Oluşan İşlem Yapımı	147
3.2.2. Yükselen Veri İşleme Hızı	149
3.2.3. Veri İşlemenin Kapsamlı ve Gizli Olması	150
3.2.4. İhlal Yöntemlerinin Çeşitli Olması	153
3.3. Yapay Zekâ Çağının Kişisel Veri Korunmasına Sunduğu Fırsatlar	154

3.4. Yapay Zekâ Çağında Kişisel Veri Korunmasının Karşılaştığı Sorunlar	156
3.4.1. Veri Asimetrisi Sorunu	156
3.4.2. Algoritmik Önyargı/Kara Kutu Sorunu	157
3.4.3. Çıkarımların Niteliği Sorunu	162
3.4.4. Şeffaflık/Rıza Sorunu	165
3.4.5. Hassas Veri Sorunu.....	168
3.4.6. Anonimleştirilmiş Veri Sorunu	171
3.4.7. İhlal Failinin Belirlenme Sorunu	175
3.4.8. İhlal Delili Elde Etme Sorunu	177
3.5. Yapay Zekâ Çağında Kişisel Veri Koruma Düzenlemelerin Karşılaştırılması	178
3.6. Yapay Zekâ Çağında Kişisel Veri Korunmasına Yönelik İzlenebilecek Stratejiler	181
3.6.1. Aydınlatılmış Rıza	182
3.6.2. Unutulma Hakkı.....	185
3.6.3. Makul Çıkarım Hakkı	186
3.6.4. Gizliliği Teşvik Eden Teknolojiler (Privacy Enhancing Technologies)	190
3.6.5. Tasarımda Şeffaflık.....	194
3.6.6. Açıklanabilir Yapay Zekâ	196
3.6.7. Düzenleyici Sanal Alanlar	199
3.6.8. Veri Koruma Etki Değerlendirmesi (VKED)	200
3.6.9. İstatistiksel İşleme ve Bilimsel Araştırma	202
SONUÇ.....	205
EKLER.....	215
KAYNAKÇA	220

TABLO LİSTESİ

Sayfa No.

Tablo 1: Dört Kategoride Yapay Zekâ Tanımı.....	17
Tablo 2: Üç Çeşit Makine Öğrenimi	26
Tablo 3: Yapay Zekâ Çalışmalarının Kronolojik Listesi	43
Tablo 4: Mukayeseli Hukuktaki Kişisel Verilerin Tanımı.....	53
Tablo 5: Karşılaştırmalı Olarak Hassas Kişisel Verilerin İçeriği.....	60
Tablo 6: GDPR Açısından Kişisel Veri Hassasiyeti Hiyerarşisi.....	61
Tablo 7: Kişisel Verilerin Korunmasına İlişkin Muhtelif Düzenlemeler.....	69
Tablo 8: “OECD Rehber İlkeleri’nde Belirtilen İlkeler	75
Tablo 9: 108 Sayılı Sözleşmede Belirtilen İlkeler	80
Tablo 10: Kişisel Verilerin Korunması Konusundaki Uluslararası Düzenlemeler ...	82
Tablo 11: GDPR’da Belirtilen İlgili Kişinin Hakları	96
Tablo 12: GDPR’da Belirtilen Veri Sorumlusu ve Veri İşleyenin Yükümlülükleri .	97
Tablo 13: GDPR’da Belirtilen İlgili Ceza Miktarı.....	103
Tablo 14: ABD Mahremiyet Koruma Yasal Düzenlemeleri.....	113
Tablo 15: CCPA’nın İlgili Kişilere Tanıdığı Haklar.....	116
Tablo 16: Çin Kişisel Bilgileri Koruma Düzenlemeleri.....	120
Tablo 17: KVKK’da Esas Alınan Temel İlkeler	130
Tablo 18: KVKK’da Belirtilen Veri Sorumlusunun Yükümlülükleri.....	135
Tablo 19: Çıkarımların Niteliği Hakkında Görüşler	163
Tablo 20: Kişisel Veri Koruma Yaklaşımı, Strateji ve Avantajları	178
Tablo 21: Veri Odaklı Stratejiler.....	192
Tablo 22: Süreç Odaklı Stratejiler.....	193

ŞEKİL LİSTESİ

Sayfa No.

Şekil 1: Yapay Sinir Hücre Yapısı	30
Şekil 2: Çok Katmanlı Yapay Sinir Ağı Yapısı.....	31
Şekil 3: Uzman Sistemin Genel Yapısı	33
Şekil 4: Bulanık Mantığın Genel Yapısı.....	34
Şekil 5: Genetik Algoritmanın Genel Akış Şeması	35
Şekil 6: Tanımlanmış ve Tanımlanmamış Veriler Arasındaki Bağlantı.....	172
Şekil 7: Farklı Yaklaşımlara Göre Performans ve Açıklanabilirlik Modeli	198
Şekil 8: Açıklanabilir Yapay Zekânın Kapsamı	199

KISALTMALAR

a.g.e.	: Adı geçen eser
a.g.m.	: Adı geçen makale
AB	: Avrupa Birliđi
ABAD	: Avrupa Birliđi Adalet Divanı
ABD	: Amerika Birleşik Devletleri
AI HLEG	: Avrupa Komisyonu'nun Yapay Zekâ Üzerine Üst Düzey Uzman Grubu
AIHM	: Avrupa İnsan Hakları Mahkemesi
AIHS	: Avrupa İnsan Hakları Sözleşmesi
BT	: Bilgi Teknolojileri
Bkz.	: Bakınız
BM	: Birleşmiş Milletler
C.	: Cilt
CCPA	: Kaliforniya Tüketici Gizliliđi Yasası
Çev.	: Çeviren
VKED	: Veri Koruma Etki Deđerlendirmesi
EDPS	: Avrupa Veri Koruma Denetçisi
GPS	: Küresel Yer Belirleme Sistemi
GDPR	: Genel Veri Koruma Tüzüğü
İHEB	: İnsan Hakları Evrensel Beyannamesi
KVKK	: Kişisel Verilerin Korunması Kanunu
m.	: madde
MIT	: Massachusetts Teknoloji Enstitüsü
no.	: Numara
OECD	: Ekonomik İşbirliđi ve Kalkınma Örgütü
Örn.	: Örnek

PbD	: Varsayılan Ayarlarla Veri Koruma ve/veya Tasarımla Veri Koruma
RFID	: Radyo Frekansı Tanımlaması (Radio-Frequency Identification)
s.	: Sayfa
S.	: Sayı
TCK	: Türk Ceza Kanunu
TDK	: Türk Dil Kurumu
TMK	: Türk Medeni Kanunu
vb.	: Ve benzeri
vd.	: Ve devamı
Y.	: Yıl



GİRİŞ

Günümüzde teknolojilerin gelişmesi insanoğlunun bulunduğu her sektörde belirli düzeyde etki yaratmaktadır. Buna karşılık daha önce hiç duymadığımız yeni kavramlarla karşılaşmaktayız. Bu kavramların ilk akla geleni ise yapay zekâdır. Bilişim Teknolojileri (BT)’ın kullanım alanlarının genişlemesi ile, verilerin otomatik karar verme sistemleri aracılığıyla hızlı ve verimli bir şekilde işlenmesi kolay hale gelmiştir. Yapay zekâ teknolojileri ile muhtelif veriler arasındaki korelasyon ilişkisi ile dağınık bilgiler arasında yeni ilişkilerin kurulması, eskiden bir araya getirilmesi imkânsız gibi görünen verilerin bir araya getirilerek anlamlandırılması pratik hale gelmiştir. Sonuç olarak algoritmik ekonomi çağı veya yapay zekâ çağında veriler, özellikle kişisel veriler çok değer kazanmıştır.

Bu bağlamda kişisel verilere yönelik ihlallerin niteliğinde temel değişiklikler olmuştur. Kişisel verilerin özel hayatın gizliliği ve korunması hakkının alt unsuru olması sebebiyle, günümüzde özel hayatın gizliliği hakkı başta olmak üzere insanın temel hak ve özgürlüklerini korumayı amaçlayan yeni usuller, düzenlemelere ihtiyaç oluşmuştur¹. Nihayetinde kişisel verilerin korunması, özel hayatın gizliliği hakkı, bilgilerin geleceğini belirleme hakkı, düşünceyi açıklama özgürlüğü, özel haberleşmenin gizliliği ve vicdan, din, inanç özgürlüğü, mülkiyet hakkı, kişinin manevi bütünlüğü, şeref ve onuru gibi kişilik haklarla kesişmiştir.²

Yapay zekâ çağında kullanıcılara ait verilere çeşitli analizler yapılmakta, bu veriler doğrultusunda ticari kaygılar güdülerek kullanılmaktadır. Nitekim, yeni dünyada petrol niteliğine sahip olduğu ifade edilen veri, gücünü de beraberinde getirmektedir. Bunu öngören teşebbüsler ve kurumlar, kişisel verileri kullanarak hedef kitlesini kolaylıkla tespit etmeyi, sundukları hizmetin kalitesini artırmayı ve bu

¹ Özel hayatın gizliliği ve korunması hakkı dört alt unsurlardan oluşmaktadır: kişisel veriler, konuta saygı hakkı, haberleşme hürriyeti, aile hayatına saygı. Daha fazla bilgi için bkz: Ali Korkmaz, “İnsan Hakları Bağlamında Özel Hayatın Gizliliği ve Korunması”, **KMÜ Sosyal ve Ekonomik Araştırmalar Dergisi**, S. 16 (Özel Sayı I), ss. 99-103, s. 100.

² Murat Volkan Dülger, “İnsan Hakları ve Temel Hak ve Özgürlükler Bağlamında Kişisel Verilerin Korunması”, **İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi**, S. 5 (1), 2018, ss. 71-144, s. 76.

bilgileri satarak ticarî kazanç elde etmeyi hedeflemişlerdir. Bu tür yaklaşım insanların sadece mahremiyetini değil, belki de hayatı güvenliğini risk altına alabilmektedir³.

Örneğin, Cambridge Analytica 2016 yılında Amerika Birleşik Devletleri (ABD) seçimlerinde manipülasyon yoluyla özellikle kişisel verilerin büyük ölçüde işlenmesi ve kişisel psiko-gramların oluşturulmasını sağlayıp⁴ seçmenleri yönlendirerek korkutucu faaliyetler gerçekleştirmiştir⁵. Bundan önce ABD eski başkanı Barack Obama'nın 2012 yılı başkanlık seçiminde yapay zekâ algoritmaları kullanarak çok sayıda seçmene ulaştığı, verilerin analiz edilerek seçmenler ile iletişim kurulduğu da belirtilmiştir⁶. Bu bağlamda yapay zekâ çağında kişisel verilerin işlenmesi seçimlerde büyük rol oynadığı söylenebilir.

Sadece siyasi alanda değil, veri işleme aracılığıyla yapılan yönlendirmeler başka alanlarda da çok yaygın olarak kullanılmaktadır. Facebook gibi sosyal medya platformları artık algoritmalar aracılığıyla kullanıcıların dünya görüşü, tercihlerine en yakın olan içerikleri seçip ekrana yansıtmaktadır⁷. Bir başka örnekte ise Facebook'un kullanıcılarına ırkı veya rengine bakarak farklı içerikleri ön plana çıkardığı öne sürülmüştür. Benzer şekilde arama motoru Google, kullanıcının kişisel profiline göre tercihine en yakın olan sonuçları sunmaktadır. Veriler sayesinde yönlendirme ile ilgili en korkutucu örnek, Microsoft tarafından geliştirilen Tay olabilir. Twitter üzerinden kullanıcıların verileri ile beslenip, hayata geçirildiği ilk 24 saatte aşırı cinsiyet ayrımı

³ Gizem Gültekin Varkonyi, "Robots with AI: Privacy Considerations in the Era of Robotics", **Law 4.0**, Széchenyi István University, Győr, 29 Mart 2018, s. 3

⁴ Alexander Nix, "Cambridge Analytica- The Power of Big Data and Psychographics", **Concordia Annual Summit**, New York, 2016.

⁵ Göksu Hazar Erdiñ, "Ölçölülük İlkesi ve Açık Rıza Kapsamında Biyometrik Verilerin İşlenmesi", **Kişisel Verileri Koruma Dergisi**, C. 2, S.1 (Haziran 2020), s. 2.

⁶ Michael Scherer, "How Obama's Data Crunchers Helped Him Win", (Çevrimiçi) <https://edition.cnn.com/2012/11/07/tech/web/obama-campaign-tech-team/index.html>, (Erişim Tarihi: 01.07.2020).

⁷ Eli Pariser, "What Facebook and Google Are Hiding From the World- the Filter Bubble", 2013, (Çevrimiçi) <https://www.youtube.com/watch?v=KraiSrmxq1o>, (Erişim Tarihi 05.06.2020).

yapan ve Nazi hayranına dönüşmüş olan Tay, kısa süre sonra kapatılmaya maruz kalmıştır⁸.

Daha iyimser açıdan başka örneklerle bakacak olursak sigorta sektöründe, gelecekteki talepleri tahmin etmek için büyük miktarlarda veri işleyebilen karmaşık algoritmalar aracılığıyla prim belirlenmektedir. İnsan kaynaklarında hangi başvuru sahipleri ile mülakat yapılacağı veya işe alınacağına karar vermek için yapay zekâ algoritmaları kullanılmaktadır. Adalet sistemindeki departmanlarından hâkimlere kadar çeşitli aktörler artık karar verme süreçlerine rehberlik etmek için tahmine dayalı algoritmalar kullanmaktadır. Çin’de uygulamaya geçen dijital mahkemeler buna en iyi örnek olabilir. Bütün bu gelişmeler verilerin işlenmesi ile ortaya çıkmaktadır ve kaçınılmaz şekilde hayatımızın her alanına yansımaktadır. Veriler genel anlamda daha çok yeni teknolojik araçlar ile işlendiği için yapay zekâ gibi gelişimler kişisel verilerin korunması açısından daha önemli hale gelmiş durumundadır.

Yapay zekâ, genel anlamda kendi deneyimlerinden öğrenebilecek ve farklı durumlarda karmaşık problemleri çözebilecek veri sayar sistemlerini tanımlamak için kullanılan bir kavramdır. Bir diğer ifadeyle, yapay zekâ daha önce sadece insana özgü olduğunu düşündüğümüz yetenekleri gerçekleştirmeyi hedeflemektedir. Özellikle makine öğrenimi, derin öğrenme gibi gelişmelerin ortaya çıkmasıyla, yapay zekâ teknolojilerinde verilerin işlenmesi mecburi bir seçenek haline gelmiştir. Veriler, özellikle çalışmanın konusu olan kişisel veriler, yapay zekâ sistemlerini besleyen, öğrenmelerini ve zeki olmalarını sağlayan yakıt niteliğindedir⁹. Yapay zekâ teknolojileri bu tür veriler sayesinde yüksek hızla ilerleme kaydetmektedir.

Yapay zekâ çağında büyük miktarda verilere ihtiyaç duyulmakla beraber, uluslararası yapay zekâ alanına büyük yatırımlar da yapılmaktadır. Şu anda Open AI, Ali Baba, Facebook, Amazon, Google ve Neuralink gibi şirketler yapay zekâyâ ciddi miktarda yatırımlar yapmaktadırlar. Örneğin dijital ekonomisi 3,8 trilyon dolara

⁸ Elle Hunt, “Tay, Microsoft’s AI Chatbot, Gets a Crash Course in Racism From Twitter”, 2016, (Çevrimiçi) <https://www.theguardian.com/technology/2016/mar/24/tay-microsofts-ai-chatbot-gets-a-crash-course-in-racism-from-twitter>, (Erişim Tarihi: 10.10.2019), s. 1.

⁹ The Norwegian Data Protection Authority, Artificial Intelligence and Privacy, Tollbugata, 2018, s. 5.

ulařan Çin, 2030 yılında yapay zekâ alanında dünyanın lideri haline gelmeyi hedeflemektedir. ABD 2020 yılında yapay zekâ alanında Google ve Facebook gibi řirketlerinin yaptıkları yatırımlarının dışında 4,9 milyar dolara varan büyük bir yatırım yapmıştır. TechSci Research raporuna göre, ABD’deki yapay zekâ pazarının 2016-2021 arasında yıllık bileşik büyüme oranında yaklaşık %75 oranında olacağı tahmin edilmiştir¹⁰. Avrupa bölgesinde Almanya 2025’e kadar yapay zekâ bütçesinin 3 milyar Euro olacağını planlamaktadır¹¹. Özetle, günümüzde en büyük yatırım yapılan alanlardan biri yapay zekâ teknolojisi olmuştur.

Stanford Üniversitesi’nde yapay zekâ çalışmaları yapan Jerry Kaplan tarafından yazılan “Yapay Zekâ Çağı”¹² kitabı, akıllı çağın gelişiminin insan toplumu üzerinde iki yıkıcı etki yaratacağına vurgulamıştır: kalıcı işsizlik ve zengin/fakir arasında artan gelir farkı. Günümüzde akıllı makineler, mavi yakalı veya beyaz yakalı bir işçi olmasına bakmaksızın insan çalışmalarının yerini almaktadır. Yapay zekâ geleneksel tarım medeniyetinden tam olarak kurtulamadığımız ve bilinçsiz şekilde sanayileşme ve bilgi edinme çağında olduğumuz bir dönemde, insan toplumsal yaşamının tüm alanlarına girmeye başlamış ve hukuk alanı bir istisna olarak kalmamıştır.

Konu hukuk olunca yapay zekâ çağındaki sorunlardan biri olan özel hayatın gizliliğı/mahremiyet hakkı değerlendirilmelidir. Çalışmamızda kişisel verilerin korunması özel hayatın gizliliğı ile temel hak ve özgürlüklerin korunması kapsamında değerlendirilmiştir. Özel hayatın gizliliğı ile mahremiyet hakkı aynı anlamda kullanılmıştır. Özel hayat, insanın kişiliğine saygı gösterilme, rahat bırakılmayı isteme, kendi hayatını istemediğı ve benimsemediğı şekilde kamuya aktarılmadan devam

¹⁰ ICT, “United States Artificial Intelligence Market by Application 2021”, (Çevrimiçi) <https://www.techsciresearch.com/report/united-states-artificial-intelligence-market-by-application-speech-recognition-image-recognition-etc-by-region-and-by-end-user-consumer-electronics-security-access-control-etc-competition-forecast-opportunities-2011-2021/676.html>, (Eriřim Tarihi: 24.09.2019).

¹¹ Rasim Özgür Dönmez, “Yapay Zekâ Uluslararası Siyaseti Nasıl Etkileyebilir?”, Fikir Turu, 2019, (Çevrimiçi) <https://fikirturu.com/2019/12/09/yapay-zeka-uluslararasi-siyaseti-nasil-etkileyebilir/>, Eriřim Tarihi: 24.09.2020), par. 5.

¹² Jerry Kaplan, **Artificial Intelligence: What Everyone Needs to Know**, Oxford University Press, 2016.

ettirebilmeyi isteme hakkı şeklinde açıklanabilir¹³. Bir çeşit insan hakkı niteliğinde olan özel hayatın gizliliği hakkı uluslararası anlaşmalar ve ulusal düzenlemeler ile koruma altına alınmaktadır¹⁴. Milli güvenlik, kamu düzeni, genel sağlık, genel ahlak vb. istisnayı durumlar dışında yasal olarak korunmaktadır. Özel hayatın yanı sıra, özel hayatın bir parçası olan kişinin gizli hayat alanı bulunmaktadır¹⁵. Gizli alan kişinin kimseyle paylaşmadığı, kişinin kendisiyle baş başa kaldığı, sır, gizli duygu ve düşünce alanını içermektedir¹⁶. Modern dönemde en önemli olan insan hakkının özel hayatın gizliliği olduğu da söylenebilir¹⁷.

Özel hayatın gizliliği/mahremiyet hakkı yapay zekâ çağında özellikle kişisel veriler ile bağlantılı şekilde ele alınmaktadır¹⁸. Kişisel verilerin korunması hakkı, günümüzde özel hayatın gizliliği ve korunması hakkının evrilmiş şekli olarak kabul edilip, ilgili düzenlemelerde kişisel verilerle bağlantı kurularak özel hayatın gizliliği hakkı tanımlanmaktadır¹⁹. Bu bağlantı, kişisel verilerin korunmasının özel hayatın gizliliği hakkının kendine has özelliklerini içinde barındıran bir türü olması sebebiyle ortaya konulmuştur. Avrupa İnsan Hakları Sözleşmesi (AİHS) kişisel verilerin korunmasını bağımsız bir hak alanı olarak düzenlememiş, AİHS'nin 8. maddesinde düzenlenen özel hayatın gizliliği hakkı kapsamında ele almıştır²⁰. Özel hayatın gizliliği hakkı kişisel verilere göre daha geniş kapsamlı olup, özel hayatın gizliliği kişisel verilerin korunmasını kapsamaktadır²¹.

Özel hayatın gizliliği tanımı farklılık göstermekle birlikte, yaygın olarak kabul görülen tanımı fiziksel, bölgesel, iletişim ve en önemlisi bilgi/veri gizliliği üzerinden

¹³ Fatih Kanmaz, **Özel Hayata Karşı Suçlar**, Ankara: Adalet Yayınevi, 2015, s. 127.

¹⁴ Ali Korkmaz, **a.g.m.**, s. 99.

¹⁵ Hamide Zafer, **Özel Hayatın ve Hayatın Gizli Alanının Ceza Hukukuyla Korunması**, 1. b, İstanbul: Beta Basım Yayın, 2010, s. 5.

¹⁶ Veli Özer Özbek vd., **Türk Ceza Hukuku Özel Hükümler**, Ankara: Seçkin Yayıncılık, 2015, s. 525.

¹⁷ Louise Bennett, "Reflections on Privacy, Identity and Consent in online Services", **Information Security Technical Report**, 2009, s. 120.

¹⁸ Şahika Eroğlu, "Dijital Yaşamda Mahremiyet (Gizlilik) Kavramı ve Kişisel Veriler: Hacettepe Üniversitesi Bilgi ve Belge Yönetimi Bölümü Öğrencilerinin Mahremiyet ve Kişisel Veri Algılarının Analizi", **Hacettepe Üniversitesi Edebiyat Fakültesi Dergisi**, S. 1 (2018), s. 134.

¹⁹ Aydın Akgül, "Kişisel Verilerin Korunmasında Yeni Bir Hak: 'Unutulma Hakkı' ve AB Adalet Divanının 'Google Kararı'", **Türkiye Barolar Birliği Dergisi**, S. 116, 2015, s. 11-38, s. 31.

²⁰ Nilgün Başalp, **Kişisel Verilerin Korunması ve Saklanması**, Ankara: Yetkin Yayınevi, 2004, s. 25.

²¹ Akgül, **Kişisel Veri...**, **a.g.m.**, s. 32.

tanımlanmaktadır. Özel hayatın gizliliği/mahremiyet kavramını incelediğimizde, insanların diğer insanlar ile hangi ölçüde ilişki ve iletişim kurabileceklerine özerk bir şekilde karar verme haklarının yanı sıra insanların yalnız kalabilme hakkı olarak ifade edebiliriz²². Başka bir deyişle, insanların kendi hayat alanlarını başka insanlar ile hangi ölçüde yakınlaşmayı belirleme hakkı olarak nitelendirilebilir. Modern anlamda söylenen özel hayatın gizliliği hakkı, ilk kez 1890'da iki Amerikalı avukatın söylemiyle “*yalnız bırakılma hakkı, hakların en kapsamlısı ve özgür insanlar tarafından en çok değer verilen hak*” şeklinde tanımlanmıştır²³. Günümüzde ise özel hayatın gizliliği hakkı yaklaşımları genel olarak üç başlıkta ele alınmaktadır²⁴:

- Bölgesel mahremiyet: Kişinin etrafındaki fiziki alan ile alakalı olan mahremiyettir. Fiziksel alanın korunmasını vurgular (Örn: kendi evinde olanlar).
- Kişisel mahremiyet: Kişinin varlığına karşı gereksiz/haksız müdahalelere karşı mahremiyettir (Örn: fiziksel aranma).
- Bilgi mahremiyeti: Kişi ile ilgili verilerin toplanması, saklanması veya nasıl işleneceğinin ve aktarılacağıın kontrol edilmesini, yani bilgi güvenliğinin korunması gerekliliğini ifade eder.

Yapay zekâ teknolojilerinin risk haline geldiği alanlardan biri veri sahipleri/ilgili kişilerin bilgi mahremiyeti/gizlilik hakkıdır ve bu ihlal kişisel verilerin kullanılması ile gerçekleşmektedir. George Orwell'in ünlü “1984” adlı eseri bilgi mahremiyetin neredeyse hiç olmadığı bir dünyayı tasvir ediyordu. Romandaki “*Büyük birader seni izliyor* (Big Brother is watching you)” ifadesi her şeyi izleyebilen gözcünün tanımı olarak nitelendiriyor. Aslına bakarsak bu distopya her şeyi izleyebilmenin gücünden/riskinden bahsederken, bilgi koruma daha doğrusu veri korumanın önemini

²² Mehmet Yüksel, “Mahremiyet Hakkı ve Sosyo-Tarihsel Gelişimi”, **Ankara Üniversitesi SBF Dergisi**, S. 58-1 (2003), s. 185.

²³ Bennett, **a.g.m.**, s. 121.

²⁴ Spyros Kokolakis, “Privacy Attitudes and Privacy Behaviour: a Review of Current Research on the Privacy Paradox Phenomenon”, **Computers & Security**, S. 64 (Ocak 2017), s. 125.

ve verinin deęerini vurgulamaktadır²⁵. Bu açıdan deęerlendirdiđimizde, “1984”ün yapay zekâ çağını yansıttığını söyleyebiliriz.

Söz konusu verilerin toplanması, saklanması, işlenmesi, aktarılması ve aranmasına ilişkin olan yapay zekâ teknoloji alternatif yöntemlerin artışı özellikle ilgili kişiyi tanımlayabilen kişisel verilerin, ifade özgürlüğü gibi temel hak ve özgürlükleri ihlal etmeksizin nasıl korunacağını önemli bir konu haline getirmiştir²⁶. Kişi ve kişilik kavramları muhtelif hukuk sistemlerinde kullanılan terminoloji olmasına rağmen, yapay zekâ çağında kişilik hakları (özel hayatın gizliliğı hakkı gibi) üzerinde ortaya çıkan olumsuz etkilerinin engellenmesinde mevcut hukuk sistemleri problemlili hale gelmiştir²⁷. Çünkü kişisel verilerin korunması sorunu yaşanırken, verilerin sadece miktar da deęil, aynı zamanda niteliğı de deęişime uğramıştır²⁸.

Kişisel veri, kişinin yalnızca özel yaşamındaki verileri içermez, ayrıca ekonomik ve mesleki bilgileri de dahil onun kimliğini ortaya çıkararak, kişiyi belirli kılan ve kişiyi karakterize eden bütün bilgi ve verileri içermektedir²⁹. Kişilerin hayat çevreleri genel anlamda dört kategoriye ayrıtı edilebilir: kamusal hayat, mesleki hayat, aile hayatı ve özel hayat³⁰. Bu anlamda kişisel veri ile özel hayatın gizliliğı kavramı arasında yakın bir ilişki bulunmaktadır. Ancak günümüzde kişisel veri kavramına klasik anlamda özel hayat kavramının kapsamının dışına da taşacak şekilde anlam yüklenmesi söz konusu olmaktadır. Nitekim kişisel verilerin korunmasını, özel hayatın dışındaki mülkiyet hakkı (ABD de kişisel verileri daha çok mülkiyet hakkı kapsamında korunmaktadır) ve kişilik hakkı (şeref ve haysiyet, ad, resim, özel hayat) ile ilişkilendirmek mümkündür.

²⁵ Erođlu, **a.g.m.**, s. 132.

²⁶ Dilek Yüksel Civelek, **Kişisel Verilerin Korunması ve Bir Kurumsal Yapılanma Önerisi (Uzmanlık Tezi)**, Ankara: Bilgi Toplumu Dairesi Başkanlığı, 2011, s. 6.

²⁷ **a.g.e.**, s. 3.

²⁸ Kenneth Cukier, “Big Data is Better Data”, (Çevrimiçi) https://www.ted.com/talks/kenneth_cukier_big_data_is_better_data, (Erişim Tarihi: 01.07.2020).

²⁹ Aydın Akgül, **Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması**, İstanbul: Beta Basım Yayınları, 2016, S. 24.

³⁰ Ersan Şen, **Özel Hayatın Gizliliğı ve Korunması-Devlet ve Kitle İletişim Araçları Karşısında**, İstanbul: Kazancı Hukuk Yayınları, 1996, s. 5-6.

Hukuk ve etik uzmanları bir yandan yapay zekâ teknoloji düzenlemelerini bireyin yalnız kalma hakkı başta olmak üzere, başka evrensel hak ve özgürlüklerine uygun şekilde ayarlamaya çalışırken, öbür taraftan yapılacak düzenlemelerin ekonomik etkisi, teknoloji ve yenilikçiliği engellememesi için çaba sarf etmektedir. Kişisel verilerin korunması düzenlemelerinin yapay zekâ çağına uygun bir şekilde yenilenmesi bu noktada kritik bir rol oynamaktadır.

Bu çalışma bütünü itibariyle yapay zekâ çağının kişisel verilerin korunmasına olan etkilerini yapay zekanın tarihsel gelişimi, teknikleri, uygulamaları, karşılaştırmalı hukuktaki kişisel verilerin korunması düzenlemeleriyle ve kişisel veri koruma düzenlemelerin yapay zekâ çağında karşılaştığı sorunlar çerçevesinde tahlil etmeyi amaçlamıştır. Bunun için kişisel verilerin yapay zekâ çağında hangi yeni içerikler kazandığı, bu içerikler karşısında kişisel veri korumanın önemi, ortaya çıkan zorluk ve sorunlar, kişisel verilerin nasıl korunması gerektiği konuları ele alınacaktır. Sonuç kısmında yapay zekâ çağında kişisel verileri etkili şekilde korumaya yönelik izlenebilecek stratejiler sunulacaktır. Çalışma betimleme yöntemine dayalı niteliksel bir çalışmadır.

Türkiye’de yapılan ilgili çalışmalara bakıldığında, yapay zekâ alanında veri teknolojisi, medya ve iletişim bilim dallarında birkaç çalışmaya imza atılmıştır. Ancak hukuk perspektifinden ele alınan çalışmalar ile sınırlıdır. Özellikle, yapay zekâ çerçevesinde kişisel verilerin korunması düzenlemelerini inceleyen çalışma bulunmamaktadır. Buna ek olarak mukayeseli hukukta ilgili konuları ele alan çalışmamız özgün nitelikte olup literatüre katkı açısından da önem taşımaktadır.

Çalışmanın kapsamı yapay zekâ ve kişisel verilerin korunması sorununu karşılaştırmalı hukuk üzerinden inceleme ile sınırlıdır. Bu nedenle büyük veri için kullanılan tekniklerden sadece yapay zekâya değinilecektir. Kişisel veri koruma kapsamına gelince AB, ABD, Çin’in yapay zekâ çağındaki yaklaşımları ve düzenlemeleri karşılaştırmalı şekilde incelenecektir. Kişisel veri ihlali sorumluluk problemleri, yurtdışı aktarım konuları çalışma kapsamı dışındadır.

Çalışma temelde üç ana bölüm üzerine inşa edilmiş, her bölüm başlığı altında sorulan alt sorulara yanıt aranarak yapay zekâ çağında kişisel verilerin korunması sorunu bir bütün olarak yaklaşılmaya çalışılmıştır.

Birinci bölüm, verilerin ve/veya kişisel verilerin yapay zekâ çağında neden bu kadar önemli olduğu sorusuna yanıt aramıştır. Bu kapsamda, yapay zekanın tanımı, tarihsel gelişimi, yapay zekânın teknikleri, yapay zekâ çeşitleri, kullanılan uygulamalar veri ve/veya kişisel verilerin yapay zekâ teknolojisi için taşıdığı önemi çerçevesinde analiz edilmeye çalışılmıştır. Bölümde son olarak yapay zekânın bugünü ve geleceği hakkındaki kıyaslar yer almıştır. Veri ve/veya kişisel verilerin yapay zekâ teknolojisi için taşıdığı önemden yola çıkarak yapay zekâ çağında kişisel verilerin korunmasının önemi vurgulanmaya çalışılmıştır.

İkinci bölümde, kişisel veri ve karşılaştırmalı hukuktaki korunması incelenmiştir. Mevcut kişisel verileri koruma düzenlemeleri kişisel verileri nasıl koruyor sorusuna yanıt aranan bölümde; kişisel verilerin kavramı, kişisel verilerin korunması sorununun tarihsel gelişimi, günümüzdeki kişisel verileri koruma yöntemleri ve karşılaştırmalı hukuktaki kişisel verilerin korunması için yapılan düzenlemeler, benimsediği ilkeler, getirdiği yenilikler ve karşılaştığı sorunlar çerçevesinde analiz edilmeye çalışılmıştır. Bu bağlamda kişisel verileri koruma konusunda yapılan uluslararası düzenlemeler İktisadi İşbirliği ve Kalkınma Teşkilatı (OECD), Birleşmiş Milletler (BM) ve Avrupa Konseyi çerçevesinde tartışılmıştır. Daha sonra AB, ABD, Çin ve Türkiye'nin kişisel verileri koruma düzenlemeleri yapay zekâ kapsamında değerlendirilmiştir.

Üçüncü bölümde ise gün geçtikçe hızla ilerleyen yapay zekâ teknolojisi karşısında mevcut kişisel verileri koruma düzenlemelerinin yeterliliği sorgulanmıştır. Yapay zekâ çağında kişisel verileri işlemenin etik boyutları, özellikleri irdelenmiş, bu konuda algoritmik el, insanların azalan yalnız kalma fırsatları, filtre balonu ve Çin'in Sosyal Kredi Sistemi gibi sosyo-ekonomik boyutlar analiz edilerek yapay zekâ çağında kişisel verilerin işlenmesine yönelik sorunlar ortaya koyulmuştur. Yapay zekâ çağında kişisel verilerin korunması için sunulan fırsatlar verimlilik ve can kurtarma konularında ele alındıktan sonra kişisel veri koruma düzenlemelerin karşılaştığı sorunlar tartışılarak, yapay zekâ çağında mevcut kişisel verileri koruma

düzenlemelerin yeterli olup olmadığı sorusuna yanıt aranmıştır. Bölümde son olarak yapay zekâ çağında AB, ABD ve Çin'in kişisel veri koruma ile ilgili izlediği stratejiler incelenmiş ve yapay zekâ çağında kişisel verilerin etkili şekilde korunabilmesi için izlenebilecek stratejiler önerilmiştir.

Sonuç kısmında, elde edilen bulgular bütünü ışığında, yapay zekâ çağında kişisel verilerin kazandığı yeni nitelikler, mevcut kişisel veri koruma düzenlemelerin karşılaştığı sorunlar göz önünde bulundurularak çalışmanın genel değerlendirilmesi yapılmıştır. GDPR'ın günümüzdeki en kapsamlı ve en etkili kişisel veri koruma düzenlemesi olmasına rağmen eksikliklerin de olduğunu tanımlayan çalışma, yapay zekâ çağında kişisel verilerin hayati önem taşımasından dolayı, geniş kapsamda yorumlanması gerektiği; sadece teknik açıdan değil, aynı zamanda hukuki ve başka beşeri bilimler açısından disiplinlerarası ele alınması gerektiği; farklı düzenlemelerden esinlenerek daha dinamik kişisel veri koruma düzenlemelerinin ortaya çıkması gerektiği; kişisel veri koruma ile ekonomik çıkar dengesinin yeniden belirlenmesi gerekliliği savunulmuştur.

1. YAPAY ZEKA VE TARİHSEL GELİŞİMİ

Aristo “*insan bilmediklerinden ziyade bildikleri ya da bildiğini zannettiği alanlarda daha çok yanılıyor*” demişti. Yapay zekâ kavramı günümüzde en popüler olan, herkesin onun ne olduğunu bilen, ya da bildiğini zanneden alanların başında gelmektedir. Yapay zekâ tanımı, kavramı hakkında doğru, açık bilgilerin verilmesi ve çalışmanın konusu olan kişisel veriler ile ilgili olan alanların aydınlatılması amacıyla bu başlıkta yapay zekâ kavramı incelenecektir.

1.1. Yapay Zekânın Tanımı

Yapay zekâ kavramını daha iyi anlayabilmek için epistemoloji açısından “*zekâ*” kavramını irdelememiz gerekmektedir. Zekânın bugüne kadar pek çok tanımı yapılmış olsa da zekâ ile ilgilenen her alan/disiplin kendi açısından birtakım tanımlar geliştirmiştir.

1.1.1. Zekâ Kavramı

Türk Dil Kurumunun 2019 yılındaki açıklamasına göre zekâ: “*İnsanın düşünme, akıl yürütme, objektif gerçekleri algılama, yargılama ve sonuç çıkarma yeteneklerinin tamamı*”dır. Bu tanıma göre zekâ denildiğin zaman aklımıza düşünme, kavrayabilme, olaylar arasında ilişki kurabilme beceresine sahip olan insan zekâsı (“Human Intelligence”) gelmektedir³¹.

Yapay zekâ alanında çalışanlar da zekanın birçok tanımını yapmışlardır. Örneğin, ünlü isimlerden bir olan Feigenbaum zekâyı problem çözme açısından şu şekilde tarif etmiştir: “*Zekâ, karmaşık bir problemi çözüm arama alanını daraltarak kısa yoldan çözebilmedir*”³². Daha sonra

³¹ Ursula Dicke ve Gerard Roth, “Animal Intelligence and the Evolution of the Human Mind”, 2008, (Çevrimiçi) <https://www.scientificamerican.com/Author/Ursula-Dicke>, (Erişim Tarihi: 08.07.2018), s.4.

³² Şakir Kocabaş, “Yapay Zekâ Araştırma ve Uygulama Alanları”, DocPlayer, 2013, (Çevrimiçi) <https://docplayer.biz.tr/3313838-Yapay-zeka-arastirma-ve-uygulama-alanlari.html> (Erişim Tarihi: 09.06.2019), s. 2.

Feigenbaum zekâyı “arama” yerine “bilgi birleştirme” kavramları ile açıklamaya çalışmıştır³³. Bu açıklamaya göre zeki denilebilen bir sistem karmaşık olan bir görevi çözebilmek için gerekli bilgileri bir arada işleyebilen ya da analiz edebilen sistemdir³⁴.

Bütün bunları içerecek zekâ tanımı “*zihnin öğrenme, öğrenilenlerden faydalanma, yeni durumlara uygulayabilme ve yeni çözüm yöntemleri bulabilme yeteneği*” şeklinde yapılabilir³⁵. Bu tanımdan yola çıkarak “yaratıcılık” zekanın en üst işlevi olarak bilinmektedir. Zekânın yaratıcı olabilmesi için zihnin öğrenmesi gerekmektedir. Öğrenmek için de olayların olması, günümüz tabiri ile verilerin olması gerekmektedir.

1.1.2. Yapay Zekâ

İster iş adamı olsun ister bir akademisyen olsun veya bir öğrenci olsun, günümüzde yapay zekâ sözcüğü herkes için ilk duyduğunda merak uyandırabilecek popüler kavram olmuştur. Bunun sebebi de zekâ gibi eskiden insanlara has bilinen soyut bir nesnenin yapay ile kullanılması ve nitelendirilmesidir. Kavramın uyandırdığı merak ile, yapay zekâ teknikleri hatta en temel bilgiler hakkında birçok kişinin bilgiye sahip olmadığı ya da yanlış bilgiye sahip olduğunu söyleyebiliriz³⁶. Yani herkesin merak ettiği ve kimsenin tam olarak ne olduğunu bilmediği, ya da net bir tanım yapılamadığı ve sürekli güncellenen bir kavramdır.

Yapay zekânın günümüzde ne kadar önemli bir fenomen haline geldiğini Massachusetts Teknoloji Enstitüsü (MIT) yöneticilerinden Edward Fredkinin şu ifadesinden anlayabiliriz: “*Tarihte üç büyük olay olmuştur. Bunlardan ilki kâinatın*

³³ Robert Engelmores ve Tony Morgan (der), **Blackboard Systems**, Boston: Addison Wesley, 1988, s. 7.

³⁴ Şakir Kocabaş, “Yapay Zekâ ve Bilim Felsefesi”, **Divan Disiplinlerarası Çalışmalar Dergisi**, C.19, S.16 (Ocak 2014), s. 11.

³⁵ Ece Karadoğan Doruk ve Habibe Öngören, “İnsan İlişkilerinde ve İş Yaşamında Duygusal Zekâ”, **İstanbul Üniversitesi İletişim Fakültesi Dergisi**, C.1, S. 22 (2005), s. 158.

³⁶ Harun Pirim, “Yapay Zekâ”, **Journal of Yaşar University**, 2006, s. 81.

oluşumu, ikincisi yaşamın başlangıcının olması, Üçüncüsü ise yapay zekânın ortaya çıkışıdır”³⁷. Bu ifadeden yapay zekânın insanlık tarihinde ne kadar önemli bir rol oynamaya başladığını anlayabiliyoruz.

İnsan hareketlerini belli bir düzeyde taklit edebilen mekanizmalara “yapay zekâ” adını verip vermemek, kavramın hangi içerik ile anlatıldığına bağlıdır. Yapay zekâ kavramlarının tarihsel gelişimini incelemenin tek yolu da budur. Yukarıdaki çerçevede değerlendirmek için öncelikle “yapay zekâ” kavramının tanımlanması gerekir³⁸. Yapay zekâ gibi devrim yaratan bir gelişim kavramının irdelenmesi onun niteliklerinin belirlenmesinde önemli olacaktır.

Akıllı makineler arayışı, II. Dünya Savaşı’ndan hemen sonra bir araştırma alanı olarak ortaya çıkmış. 1950’ye gelindiğinde Alan Turing, makinenin bir insan konuşmasını düşünerek konuşmaya katılabildiğinde ve üçüncü bir insanın makineyi insan mı yoksa makine mi, ayırt edemedi ise, o makinenin zekâ sergilediğinin kabul edileceği “Turing Testi” önermiştir³⁹. Daha sonra Amerikalı bilgisayar bilimci John McCarthy 1955 yılında ilk kez yapay zekâ kavramını ortaya koymuştur. McCarthy’ın tanımına göre yapay zekâ “*akıllı makineler, özellikle akıllı bilgisayar programları yapma bilimi ve mühendisliğidir ve insan zekasını anlamak için bilgisayarları kullanmanın göreviyle ilgilidir. Ancak yapay zekâ kendini biyolojik olarak gözlemlenebilir yöntemlerle sınırlamak zorunda değildir*”⁴⁰.

Günümüzde ise yapay zekânın neredeyse sayısızca tanımı vardır. Konu hakkında bilgisi olan bilginlerin görüşleri farklılık taşımaktadır. Öte yandan yapay zekâ teknolojisinin hızlı gelişmesi tanımın içeriğini sürekli değiştirmektedir. Bugüne kadar yapılan yapay zekâ tanımlarını şu şekilde sıralayabiliriz:

³⁷ **a.g.m.**, s. 82.

³⁸ İstanbul, Ankara ve İzmir Baroları Çalıştay Raporu, Yapay Zekâ Çağında Hukuk, Ankara, 2019, s. 8.

³⁹ Alan Turing, “Computing Machinery and Intelligence”, **Mind**, C. 59 (1950), ss. 433-460. s. 440.

⁴⁰ John McCarthy, “What Is Artificial Intelligence?”, Dartmouth proposal, 1955, s. 1.

ABD Kaliforniya Üniversitesi Bilgisayar Bilimi Profesörü, yapay zekâ alanında yaptığı katkılarla bilinen bilgisayar bilimcisi Stuart Russell ve Peter Norvig yapay zekâyı “*bilgisayarların programlanmasını temel alan, etkisi insan yaşamının her alanında gözlemlenebilen bir çalışma alanı*” şeklinde tanımlamıştır⁴¹.

Avron Barr ve Edward Fregenbaum yapay zekâyı “*insan davranışlarına özgü karakteristik özellikleri sergileyen akıllı sistemlerle ilgilenen, bilgisayar biliminin bir dalı*”⁴² olarak tanımlar. Whitby Blay yapay zekâyı “*insanlarda, hayvanlarda ve makinelerde zeki davranışın ne olduğunu inceleyen ve insan yapısı aygıtların nasıl bu tip davranışlar sergileyebileceğini bulmaya çalışan bir bilim dalı*”⁴³ olarak nitelendirir. Bu anlamda yapay zekâ, insanoğlunun şimdiye kadar yaptığı en güç ve en heyecan verici girişimi sayılır.

UC Berkeley yapay zekâ Araştırma Direktörü Mark Nitzberg yapay zekâyı çok basit bir tanım benimsemiştir. “*Dar Yapay Zekâ akıllı davranışın görünümünü ifade ederken Genel Yapay Zekâ tüm görevlerde insan performansı sağlanmasını ifade ediyor*” demişti. Çek Teknik Üniversitesi Profesörü Michal Pěchouček yapay zekâyı “*ilk olarak otomasyona, sonra hızlandırmaya en son ise insan algısının, karar vermenin ve muhakemenin ölçeklenebilirliğine olanak tanıyan bir teknoloji ve bilimsel disiplin*” olarak tanımlar. Nils J. Nilsson’a göre yapay zekâ “*ortamının öngörülmesiyle uygun şekilde çalışabilecek herhangi bir teknolojiyi (yazılım, algoritma, bir dizi işlem, bir robot, vb.) belirtmek için kullanılmaktadır*”⁴⁴.

Türkçe literatüre baktığımızda Aksu yapay zekâyı şu şekilde tanımlamıştır: “*bir bilgisayarın veya bilgisayar kontrolündeki bir robotun çeşitli faaliyetleri zeki canlılara benzer şekilde yerine getirme kabiliyetidir. Yapay zekâ çalışmaları genellikle*

⁴¹ Peter Norvig ve Stuart J. Russell, **Artificial Intelligence: A Modern Approach**, New Jersey: Prentice Hall, 3.b., 2016, s. 3.

⁴² Avron Barr, **Handbook of Artificial Intelligence**, 1.b., Kaufmann William Inc, 1981, s. 45.

⁴³ Blay Whitby, **Yapay Zekâ- Yeni Başlayanlar İçin**, 1.b., İstanbul: İletişim Yayınları, 2005, s. 17.

⁴⁴ EPSC, The Age of Artificial Intelligence Towards a European Strategy for Human-centric Machines, **EPSC Strategic Notes**, 2018, s. 2.

insanın düşünme yöntemlerini analiz ederek bunların benzeri yapay yönergeleri geliştirmeye yöneliktir”⁴⁵. Atalay’a göre yapay zekâ “doğadaki varlıkların akıllı davranışlarını yapay olarak üretmeyi amaçlayan, bu alanda işini mükemmel yapan canlı sistemlerini ve insan beynini model alan” çalışmanın adıdır⁴⁶. Bak’a göre bilgisayar biliminin bir alt dalı olan yapay zekâ kavramı, “insanlara özgü problem çözme yeteneğinin, makineler tarafından da gerçekleştirilebildiği, insanların yapabildiklerini taklit edebilen makineler” olarak tanımlanabilir⁴⁷. Ersoy’a göre yapay zekâ “insanların doğal olarak sahip oldukları zekâ ile çözdükleri problemleri çözme becerisine sahip makineler olup karmaşık bir şeyi algılama ve uygun kararlar vermedir”⁴⁸. Bozkurt Yüksel’e göre ise yapay zekâ bir makine/bilgisayar problemleri çözmek suretiyle zekâ örneği göstermektedir. Tanımda makine denilmiş olsa da yapay zekâ aslında bir yazılımdır⁴⁹. Bununla birlikte çalışabilmesi için fiziki bir varlığa, bir makineye ihtiyaç vardır. Bu makine bir masaüstü bilgisayar, bir robot, mobil telefon da olabilmektedir.

IBM çalışanı Francesca Rossi, yapay zekâyı “dış çevreden girdi toplayabilen, belirli bir talimatlar dizisine göre işleyebilen ve verilen hedefe ulaşmak için aktüerler aracılığıyla izlemenin yollarını bulabilen makineler inşa etmeyi amaçlayan bir teknik dizisi” olarak tanımlamaktadır. Avrupa Komisyonu’nun yapay zekâ Üzerine Üst Düzey Uzman Grubu (“AI HLEG” Uzman Gurubu), Francesca Rossi tarafından yönetilen yapay zekâyı tanımlamakla görevli bir alt grup oluşturmuştur. Bu grup yapay zekâyı “belirli bir hedefe ulaşmak için çevrelerini analiz edebilen ve bir dereceye

⁴⁵ Halil Aksu, Türkiye Yapay Zekâ İnisiyatifi (Çalıştay Raporu), 2017, s. 3.

⁴⁶ Muhammet Atalay ve Enes Çelik, “Büyük Veri Analizinde Yapay Zekâ ve Makine Öğrenmesi Uygulamaları”, **Mehmet Akif Ersoy Üniversitesi Sosyal Bilimler Enstitüsü Dergisi**, C. 9, S. 22 (Aralık 2017), s. 158.

⁴⁷ Armağan Ebru Bozkurt Yüksel vd., **Fütürist Hukuk**, İstanbul: Aristo Yayınevi, 2018, s. 6.

⁴⁸ Çağlar Ersoy, **Robotlar, Yapay Zekâ ve Hukuk**, 3.b., İstanbul: On İki Levha Yayınları, 2019, s. 29.

⁴⁹ Armağan Ebru Bozkurt Yüksel, **Yapay Zekâ, Endüstri 4.0 ve Robot Üreticiler**, 1.b., İstanbul: Aristo Yayınevi, 2019, s. 50.

kadar özerklikle hareket edebilen akıllıca davranış sergileyebilen sistemdir” şeklinde tanımlamıştır⁵⁰.

Yapay zekâ en genel manada, algılama, öğrenme, geliştirme, karar verme vb., gibi ancak insan zekâsı gerçekleştirebilen işlevleri yapabilen sistem olarak açıklanabilir⁵¹. Burada dikkat edilmesi gereken nokta sistemin gerçekleştirdiği işlevin insan zekâsının yaptığı işlevler ile olan benzerlik oranı ve bu işlemi yaparken zekâ ile ilgili unsurları kullanıp kullanmadığı olmalıdır⁵².

Özetlemek gerekirse, bahsi geçen tanımlar farklı bakış açısıyla açıklanmasına rağmen benzerlikleri de vardır. Aslında yapay zekâyı insanların kendi zihin ya da beyin yapılarına benzer bir işlev görebilen yapay sistem ortaya çıkarma mücadelesi olarak tanımlayabiliriz. Yapay zekâ aslında insan zekâsı gibi düşünebilen, kavrayabilen, konuşabilen ve soruları çözebilen yetenekleri gerçekleştirmek çabasıdır⁵³. Bütün bu özellikleri gerçekleştirebilmek için yapay zekanın insan beynini taklit edebilmesi, bunu yapabilmesi için yapay zekâ algoritmalarını eğitmek için kullanılacak büyük miktarda veri ve/veya kişisel verilere ihtiyaç duymaktadır.

Yukarıda belirtilen tanımları bir araya getirip, ortaklık ve farklılıklarını karşılaştıracak olursak Tablo 1’deki yapay zekânın dört kategoriye ayrılmış tanımı ortaya çıkmaktadır. İlk satırdaki tanımlar düşünce süreci ve muhakeme ile ilgilidir, alt satır ise yapay zekânın davranışı ile ilgilidir. Soldaki tanımlar, insan performansına uygunluk açısından başarıyı ölçerken, doğru olanları rasyonellik olarak adlandırılan ideal bir performans ölçüsü sağ tarafta yer almaktadır.

⁵⁰ AI HLEG, A Definition of AI: Main Capabilities and Scientific Disciplines, Brussels, 2018, s. 1-3.

⁵¹B.J. Copeland, “Artificial Intelligence”, (Çevrimiçi)

<https://www.britannica.com/technology/artificial-intelligence>, (Erişim Tarihi: 01.07.2020), par. 4.

⁵² Mustafa Zorluel, “Yapay Zekâ ve Telif Hakkı”, **TBB Dergisi**, S.142 (2019), s. 308.

⁵³ Murat Önder ve Hilal Saygılı, “Yapay Zekâ ve Kamu Yönetimine Yansımaları”, **Türk İdare Dergisi**, Y.90, S.487 (2018), s. 635.

Tablo 1: Dört Kategoride Yapay Zekâ Tanımı⁵⁴

İnsan Gibi Düşünmek (Bilişsel Modelleme Yaklaşımı)	Akıllıca Düşünmek (Düşünmenin Yasaları Yaklaşımı)
Bilgisayarları düşündürmek için heyecan verici yeni çaba...tam anlamıyla zihinsel makineler. (Haugeland, 1985)	Hesaplamalı modellerin kullanılmasıyla zihinsel yapının incelenmesi. (Charniak ve McDermott, 1985)
Otomasyonu ilişkilendirdiğimiz faaliyetlerin tamamı. Karar alma, problem çözme, öğrenme gibi faaliyetler. . . (Bellman, 1978)	Algılamayı, aklını ve hareketini mümkün kılan hesaplamaların incelenmesi. (Winston, 1992)
İnsanca Hareket Etmek (Turing Testi Yaklaşımı)	Akıllıca Hareket Etmek (Rasyonel Ajan Yaklaşımı)
İnsanlar tarafından yapıldığında akıl gerektiren işlevleri yapan makineler yaratma sanatı... (Kurzweil, 1990)	Hesaplamalı Zekâ, akıllı ajanların tasarımının incelenmesidir. (Poole ve ark. 1998)
Bilgisayarların nasıl yapıldığında insanlardan daha iyi olduğu şeyleri yapabilme çalışması (Rich ve Knight, 1991)	Yapay zekâ...eserlerdeki akıllı davranışlarla ilgileniyor (Nilsson, 1998)

⁵⁴ Norvig ve Russell, **a.g.e.**, s. 1.

1.2. Yapay Zekânın Tarihsel Gelişimi

1.2.1. Tarih Öncesi

Bazı düşünürler ancak otomatik bir şekilde işlev gören sistemlerin, yapay zekânın tarihsel gelişimine dahil edilmemesi gerektiğini savunmuştur. Bazıları ise yapay zekâ kavramının gelişimini Milattan Önceye dayandıran çeşitli görüşlere sahiptir⁵⁵.

Eski Yunan Mitoloji'sinde “Yapay Zekâ” sözcüğü geçmese de “Akıllı Makineler” kavramının geçtiği bilinmektedir. Platon diyalogunda kanun koyucu olan Minos'ın görevlerini anlatırken, yaşayan biri olarak Talos'dan da söz eder⁵⁶. Yunan mitolojisinde on iki tanrının biri olan İphestos, Talos adında, metalden insan görünümlü bir makine yaptığından söz edilir. Yunan mitolojisindeki rüzgâr tanrısı zannedilen Daedalus'un “Yapay-İnsan” teşebbüsü literatürde yer almaktadır⁵⁷. Tomas Hobbes üç asır önce bilgisayarlı zekâ teorisini geliştirmiş, Descartes ise makinelerin düşünme kabiliyeti ile ilgili sorgulamalar yapmıştır⁵⁸.

Hepimizin bildiği gibi MS 9. yüzyılda Abbasi döneminde (750-1256) Musa kardeşler hidrolik prensiplerle çalışan otomatik makineler yapmış ve ardından Selçuklu döneminde Ebul İzz bu çalışmaları sürdürmüştür⁵⁹. Bu kaynaklarda yer alan kavramların günümüzdeki yapay zekâ teriminin içeriği ile çok farklı olmasına rağmen, aynı zamandaki teknoloji seviyesinde günümüze ışık tutabilecek kadar ileri görüşlü olduğu söylenebilir.

⁵⁵ Feyyaz FIRAT, “İnternet Haberciliğinde Yapay Zekâ Teknolojisi Kullanımı: Robot Gazetecilik, (Gazi Üniversitesi Sosyal Bilimler Enstitüsü Yayınlanmamış Yüksek Lisans Tezi), Ankara, 2018, s. 22.

⁵⁶ Platon, Çev. Hamdi Varoğlu, **Minos**, İstanbul: Sosyal Yayınları, 2001, s. 318-320.

⁵⁷ Pirim, **a.g.m.**, s. 83.

⁵⁸ Ersoy, **a.g.e.**, s. 29.

⁵⁹ Zekai Şen, **Üç Türk-İslam Bilim ve Düşünce Adamı**, İstanbul: Su Vakfı Yayınları, 2002, ss. 11-30.

Yapay zekâ fikrini çağrıştırabilecek diğer bir örnek, yine modern felsefe döneminde yaşamış olan matematikçi ve felsefeci Leibniz'in tasarımı yaptığı dört işlemi birlikte yapabilen hesap makinesidir. Leibniz, sorduğu “*İnsanların yapmada zorlandığı aritmetiği bir makineye yaptırabildiğine göre, düşünme faaliyetinin tamamını da makineye yaptıramaz mıyım?*” sorusu ile hareket ederek mantık makinesinin (“Calculus Ratiocinator”) geliştirilebileceğini dile getirir. Leibniz'in amaçladığı aslında insanların akıl yürütme kurallarını ifade edebilecek bir dil tasarlamaktır⁶⁰. Daha sonra Leibniz, bir makinenin insan zihninin yapabileceği bir işi yapılabildiğine göre, başka bir işlen niteliğinde olan düşünme işlevinin de aynı şekilde makineler tarafından yapılabileceği sonuca varmıştır⁶¹.

Ancak bunun gerçekleştirilebilmesi için aritmetik olarak bir dille formüle edilen sayılar gibi, insan düşünmesinin de formel olarak gösterilebilmesi gerekmektedir. 1850 lerde matematikçi Boole, insan zihnini matematiksel açıdan inceleyip, matematik yollar ile açıklayabilen bir dil keşfetmiştir. Boole mantık sembollerinin cebirsel semboller olarak ifade edildiğini vurgulayarak cebirsel denklemlerin çözümü gibi yöntemlerin kullanılması ile “*Çağdaş Mantık Kuramı*”nı ortaya koymuştur⁶². Bu çalışmalar daha sonraki yapay zekâ çalışmalarına çok önemli temeller oluşturmuştur.

1.2.2. Dartmouth Konferansı Sırası

Ünlü bilim kurgu yazarı olan Isaac Asimov, “*Run around*” adlı hikayesinde robotik biliminin üç temel ilkesini ortaya koymuştur⁶³:

- Birinci yasa: Bir robot bir insana zarar veremez ya da bir insanın zarar görmesine izin veremez.

⁶⁰ Elif YİTMEN, “Zihin Felsefesi Bağlamında Yapay Zekâ Üzerine Felsefi Bir İrdeleme”, (Maltepe Üniversitesi Sosyal Bilimler Enstitüsü Yayınlanmamış Yüksek Lisans Tezi), İstanbul, 2018, s. 6.

⁶¹ Cem Say, **50 Soruda Yapay Zekâ**, İstanbul: 7 Renk Basım Yayım ve Filmcilik, 2018, s. 23.

⁶² Önder ve Saygılı, **a.g.m.**, s. 640.

⁶³ Isaac Asimov, **Ben, Robot**, İstanbul: İthaki Yayınları, 2016.

- İkinci yasa: Bir robot, birinci yasa ile çelişmediği müddetçe insanların istediklerini yapmak zorundadır.
- Üçüncü yasa: Bir robot, birinci ve ikinci yasa ile çelişmediği sürece kendi varlığını korumak zorundadır.

Bu yasalar ilk robot yasası olarak bilinmektedir. Ancak Asimov, daha sonra yayımladığı “*Robotlar ve İmparatorluk*” (“*Robots and Empire*”) adlı hikâyesinde üç yasaya ek olarak sıfır numaralı yasa eklemiştir. Bu yasaya göre bir robot insanlığa karşı eylemde bulunamaz ve insanlığın zarar görmesine herhangi bir şekilde izin de veremez⁶⁴. Asimov’un yasaları günümüz yapay zekâ girişimleri alanında özellikle robot uygulamalarında en temel referans, kural kaynağı olarak görülmektedir.

1950’lerin başında Alan Turing ile John Von Neumann, günümüzde kullandığımız bilgisayarların temellerini oluşturup çeşitli programlamlarla belirli görevleri yerine getirebilen bir makineyi dünyaya getirmiştir. Turing aynı yıllarda dünyayı şaşırtan ünlü makalesi “*Computing Machinery and Intelligence*” (Bilgisayım Makineleri ve Zekâ) nı yayımlamıştı. Bu makalesinde Turing, makinelerin de insan zekâsı gibi olabileceğini ileri sürmüş ve bahsi geçen makinelerin nasıl yapılabileceğinden ve zekâlarının nasıl test edilebileceğinden söz etmiştir⁶⁵.

Turing’in makalesinin ardından, 1955 yılında insanların sorunları çözme yeteneğini taklit etmeyi amaçlayan ilk yapay zekâ programı “Logic Theorist” geliştirilmiştir⁶⁶. 1956 yılında Dartmouth konferansında ilk kez “yapay zekâ” adı öneriliyor. Bilgi kuramının babası Claude Shannon, Nobel Ödülü sahibi Herbert Simon, MIT yapay zekâ laboratuvarının kurucusu Marvin Minsky, IBM kurucusu

⁶⁴ Armağan Ebru Bozkurt Yüksel, “Robot Hukuku”, *Türkiye Adalet Akademisi Dergisi*, S. 29 (2017), s. 92.

⁶⁵ Council of Europe, “History of Artificial Intelligence” (Çevrimiçi) <https://www.coe.int/en/web/artificial-intelligence/history-of-ai>, (Erişim Tarihi: 12.11.2018).

⁶⁶ Nick Bostrom, *Superintelligence: Paths, Dangers, Strategies*, Oxford: Oxford University Press, 2014, s. 5.

Nathaniel Rochester, Amerikan yapay zekâ Derneği'nin ilk başkanı Allen Newell bu Konferansa katılan öncüler arasında yer almıştır.

Dartmouth Konferansı yapay zekâ sözcüğünün ilk kez kullanıldığı ve insanlık tarihinde yapay zekâ sayfasının açıldığı bir dönüm noktası niteliğindedir. Nitekim günümüzde yapay zekâ çağının başlangıç noktası Turing'in "*makinelere düşünebilir mi?*" sorusu ile Dartmouth Konferansını referans almaktadır.

1.2.3. Altın Çağı

Dartmouth Konferansı sonrası yapılan çalışmalar başta ABD Savunma Bakanlığı tarafından desteklenmiş ve dünyanın farklı yerlerinde laboratuvarlar kurulmuştur. Newell ve Simon'un Genel Sorun Çözücü ve Joseph Weizenbaum'un ELIZA'sı gibi ilk yapay zekâ araştırma sonuçları, daha sonra problem çözme ve sözlü dilin anlaşılmasına yönelik umut vermiştir. Bu başarıların yanı sıra, önde gelen araştırmacıların savunuculuğu, çeşitli kurumlarda yapay zekâ araştırmalarını finanse etmek için "Savunma İleri Araştırma Projeleri Ajansı" (DARPA) gibi devlet kurumlarını ikna etmiştir⁶⁷. Hükümet özellikle, konuşulan dili ve aynı zamanda yüksek verimli veri işlemeyi çevirebilecek ve tercüme edebilecek bir makine ile ilgilenmiştir.

Bu dönemde beklentiler yüksek olmuştur. Marvin Minsky, 1970 yılında "*Life Magazin*"de yazdığı yazıda "*üç ile sekiz yıl arasında, ortalama bir insanın genel zekasına sahip bir makineye sahip olacağız*" demiştir⁶⁸. Bununla birlikte, temel ilkenin kanıtı yansira, doğal dil işlemenin, soyut düşüncenin ve kendini tanımanın son aşamasını gerçekleştirmeden önce çok uzun bir yol olduğu tahmin edilmiştir. Beklenen gelişmelerin gerçekleşmemesi sonucunda 1970'lerden itibaren yapay zekâ

⁶⁷ TÜBİTAK, **Bilim ve Teknik**, S. 409 (Aralık) 2001, s. 43.

⁶⁸ Marvin Minsky, "Form and Content in Computer Science", **Journal of the Association for Computing Machinery**, C. 17, S. 2 (Nisan 1970).

çalışmaları farklı yönlerden eleştirilere maruz kalmıştır⁶⁹. Böylelikle yapay zekâ tarihçesinde durgunluk dönemi başlamıştır.

1.2.4. Kış Mevsimi

İngiliz matematikçi Sir James 1973 yılında “*Lighthill*”de yazdığı bir raporda (Lighthill Report) yapay zekânın Birleşik Krallıktaki durumunu eleştirmiş ve bilgisayarların asla bir insana yetişemeyeceğini ve en fazla ancak bir “deneyim sahibi amatör” satranç oyuncusunun seviyesine gelebileceğini aktarmıştır⁷⁰. Bu dönemde yapay zekâ araştırmalara verilen finansal destekler azalmaya başlamış ve bunu takip eden birkaç yıl günümüzde “*AI Winter*” şeklinde bilinen yapay zekâ kış mevsimi olarak bilinmektedir. Bu dönemde bilim insanları yapay zekâ alanında çok az gelişme elde edebilmiş ve sonuçta bir bekleme dönemi olmuştur⁷¹. Yapay zekâ kış mevsiminde ilgili çalışmalar sembolik ve sibernetik yapay zekâ olarak ikiye ayrılmış ve daha sonraki günümüze kadar uzanan yeninden canlanma çağı gelmiştir.

1.2.5. Yeniden Canlanma

Japonya’nın 1981 yılında ortaya koyduğu “*5. Nesil Bilgisayar Projesi*” ile yapay zekâ çalışmalarında yeninden canlanma meydana gelmiştir. Japonya söz konusu projede prolog programlama dilini kullanacağını açıklamıştır. Bu tür bilgi tabanlı sistemlerin etkili şekilde uygulamaya konulması daha sonraki genel bilgi sistemleri çalışmaları için fırsat yaratmıştır⁷². Bu gelişmeler uzun süren duraklama döneminin sona erdiğinin göstergesi olmuştur.

⁶⁹ Rockwell Anyoha, “The History of Artificial Intelligence”, (Çevrimiçi) <http://sitn.hms.harvard.edu/flash/2017/history-artificial-intelligence>, (Erişim Tarihi: 12.10.2019).

⁷⁰ Bostrom, **a.g.e.**, s. 6-7.

⁷¹ Pirim, **a.g.m.**, s. 84.

⁷² Şakir Kocabaş, “Yapay Zekâ Araştırma ve Uygulama Alanları”, (Çevrimiçi) <https://docplayer.biz.tr/3313838-Yapay-zeka-arastirma-ve-uygulama-alanlari.html>, (Erişim Tarihi: 09.06.2019). s. 4.

1997 yılında saniyede milyonlarca hamle hesaplama becerisine sahip Deep Blue adında bir süper bilgisayar, dünya satranç şampiyonu Gary Kasparov'u yenebilecek kadar hızlanmıştı. Deep Blue bu başarısı ile bir yeni mevsime de imza atmıştır. Bu gelişmelerin ardından 2017 yılındaki bir dizi karşılaşma sonunda, Google Deep Mind tarafından geliştirilen AlphaGo Avrupa ve Dünya Go (satrançtan çok daha zor olduğu kabul edilen ve neredeyse sınırsız hamleler söz konusu olan oyun) Şampiyonu insan rakiplerini yenebilecek duruma gelmiştir⁷³.

Bu dönem yapay zekânın çok hızla geliştiği dönem olmuştur. Yapay zekâ uzmanları hastalık teşhisi alanlarında sistemler geliştirerek bugünkü açılımların temelleri oluşturmuştur. Daha sonraki yıllarda ekonomi ve psikoloji gibi diğer bilim disiplinlerinde de yapay zekâ çalışmaları yapılmaya başlamıştır. Yapay zekâ bu dönemde laboratuvarların dışına çıkarılarak gerçek dünyanın ihtiyaçlarına ilişkin çok daha karmaşık uygulamalar ile ortaya çıkmıştır⁷⁴. Bu dönem yapay zekânın sadece bilgisayar bilimi altında değil, disiplinlerarası ilerleme kaydetti bir dönemdir.

Özetlemek gerekirse günümüze kadar yapılan yapay zekâ çalışmalarını üç alanda özetleyebiliriz: Birincisi, 1940 ile 1965 arasında ve 1982'den günümüze kadar etmekte olan Yapay Sinir Ağları ve algılayıcılar çalışmaları; ikincisi, 1965 ile 1975 yılları arasında ön plana çıkmış olan sembolik yapay zekâ çalışmaları; üçüncüsü, 1975'ten günümüze kadar devam etmekte olan Bilgi Tabanlı Sistem çalışmalarıdır⁷⁵. Günümüzde yapay zekanın yeniden canlanmasının sebeplerinden biri de büyük miktarda veri toplama, analiz edebilmenin kolaylaşması denilebilir. Öbür yandan ise yapay zekanın canlanması aynı şekilde daha büyük miktarda veriye ihtiyaç duymaktadır.

⁷³ Şahin Kılınç, "Google'ın Yapay Zekâsı, Satrançtan Bin Kat Daha Zor Go Oyununda Dünya Şampiyonunu Yendi!", 2017, (Çevrimiçi) <https://www.webtekno.com/google-in-yapay-zekasi-satranctan-bin-kat-daha-zor-go-oyununda-dunya-sampiyonunu-yendi-h29312.html>, (Erişim Tarihi: 02.10.2019).

⁷⁴ Pirim, **a.g.m.**, s. 83.

⁷⁵ Kocabaş, **a.g.m.**, s. 4.

1.3. Yapay Zekâ Teknikleri

Yapay zekâ teknolojisinin altında makine öğrenimi ve derin öğrenme şeklinde iki ana metot yatmaktadır. Bunlardan makine öğrenimi en çok bilinen ve bu nedenle sıklıkla yapay zekâ ile karıştırılan bir kavramdır. Aslında makine öğrenimi, bir bilgisayarın zeki olmasına, çevresinden öğrenmesine ve giderek performansını geliştirmesine olanak veren bir yöntem denilebilir. Yapay zekâ, makine öğrenimi sayesinde insanlar gibi öğrenebilmektedir. Bu sayede zeki bilgisayarlar kendi deneyimlerinden öğrenmekte, binlerce örneği inceleyerek bir algoritma geliştirmekte ve giderek daha zeki hale gelmektedirler. Ancak bu süreçler makine öğreniminin çok fazla veri ile beslenmesini gerektirmektedir. Öte yandan, derin öğrenme makine öğreniminden doğmuştur. Makine öğrenimine göre daha yeni bir teknik niteliğindedir. Derin öğrenme daha büyük ve daha karmaşık sorunları çözmek için güçlü bilgisayarlar kullanılmakta ve “büyük veri” ile ilişkilendirilmektedir⁷⁶. Makine öğrenimi ve derin öğrenme en popüler olan yapay zekâ teknikleridir. Popüler olmasının sebebi de kullanışlı, zor problemleri çözebilmesi, kolay olmasıdır. Ancak kolaylık karşısında getirdiği problemler ve eksikliklerde vardır.

1.3.1. Makine Öğrenimi

Günümüzde makine öğrenimi yapay zekâ alanında çok fazla kullanıldığından dolayı, yapay zekâ ile makine öğrenimi bir-birinin eş anlamı olarak kullanılmaktadır. Makine öğrenimi, açık bir şekilde programlanmadan malum bir bilgiyi öğrenme becerisi veren çalışma alanı için kullanılan kavramdır⁷⁷. Makine öğrenimi programları kendi kendini programlayabildiği gibi programın kapsamı dışında kaldığı durumlarda

⁷⁶ Internet Society, “Artificial Intelligence and Machine Learning: Policy Paper”, Internet **Security**, 2017, (Çevrimiçi) https://www.internetsociety.org/wp-content/uploads/2017/08/ISOC-AI-Policy-Paper_2017-04-27_0.pdf (Erişim Tarihi: 02.07.2020).

⁷⁷ Puget ve Jean Francois, “What Is Machine Learning?”, (Çevrimiçi) https://www.ibm.com/developerworks/community/blogs/jfp/entry/What_Is_Machine_Learning?lang=en, (Erişim Tarihi: 04.10.2019).

bile işlem yapabilmektedir⁷⁸. Sadece öğrendiği örnekleri değil, öğrenen örnekler üzerinden çözme yöntemleri bulma makine öğreniminin esas görevidir.

Makine öğreniminin net olarak tanımı yoktur ve teknolojinin ilerlemesi ile kavramın içeriği de değişmektedir. Andrew Ng’a göre makine öğrenimi bilgisayarların açıkça programlanmadan harekete geçme bilimidir⁷⁹. Bu yüzden makine öğrenimi, genellikle büyük miktardaki verilerden zaman içinde otomatik olarak öğrenme yeteneği sağlayan sistemlere sahip bir yapay zekâ tekniğidir denilebilir. Bilgisayarlar makine öğrenmesine ilişkin programlar sayesinde kendi deneyimlerinden öğrenmekte, bir algoritma geliştirmek için çok fazla sayıda örnekleri incelemektedir. Makine öğrenimi programlama kurallarını kullanarak karar vermeyi otomatikleştirmektedir⁸⁰.

Örneğin, Amazon’un öneri algoritması, hangi ürünlerin müşteriler için ilgi çekici olacağını tahmin etmek için makine öğrenimi aracılığıyla müşterilerin profillerini kullanır. Yani kullanıcılar Amazon sitesini ziyaret ettiklerinde, sistem tarafından oluşturulan öneri modeli kişiselleştirilmiş önerileri üretmek için kullanıcı profillerini kullanır ve en uygun, ilgi çekici içeriği tavsiye eder. Bu işlemler doğal olarak çalışmamızın konusu olan kişisel verilerin korunması kapsamında değerlendirilmesini gerektirir.

Özetle yapay zekâ insan gibi rasyonel düşüneme, davranma beceresine sahip ve akıllıca davranabilen bilgisayar sistemleriyken⁸¹, makine öğrenimi ise yapay zekânın son evresi niteliğinde kabul edilmektedir⁸². Elde edilen veriler ve makine öğrenimi algoritmaları ile oluşturulan model, dolu kapasiteli performansı gerçekleştirmeyi

⁷⁸ Zimmerman ve Evan Joseph, “Machine Minds: Frontiers in Legal Personhood”, SSRN, (Nisan 2015), (Çevrimiçi) <https://ssrn.com/abstract=2563965>, (Erişim Tarihi: 02.07.2020).

⁷⁹ Daniel Faggella, “What Is Machine Learning?”, 2017, (Çevrimiçi) <https://www.techemergence.com/what-is-machine-learning/>, (Erişim Tarihi: 02.07.2020).

⁸⁰ Armağan Ebru Bozkurt Yüksel, “Yapay Zekanın Buluşlarının Patentlenmesi”, **Uyuşmazlık Mahkemesi Dergisi**, 2018, s. 590.

⁸¹ M. Erdal Balaban ve Elif Kartal, **Veri Madenciliği ve Makine Öğrenmesi: Temel Algoritmaları ve R Dili ile Uygulamaları**, İstanbul: Çağlayan Kitabevi, 2015, s. 16.

⁸² Atalay ve Çelik, **a.g.m.**, s. 159.

amaçlamaktadır. Makine öğrenimi stratejileri: denetimli, denetimsiz ve pekiştirmeli olmak üzere üç alt başlıkta incelenebilir. Tablo 2’de bu üç çeşit makine öğrenimi yer almaktadır:

Tablo 2: Üç Çeşit Makine Öğrenimi⁸³

Denetimli Öğrenme	Bir modeli eğitmek için etiketli verilere kullanır. Bu model daha sonra, eğitim verilerinin bir parçası olmayan ilgili bir veri parçasını tahmin etmek için kullanır. Regresyon yoluyla sürekli bir değer veya sınıflandırma yoluyla ayrık bir değer tahmin etmek için kullanılabilir.
Denetimsiz Öğrenme	Bir modeli eğitmek için etiketlenmiş veri gerektirmez. Eğitim verilerinden örüntüleri ve yapıları, örneğin kümeleme yoluyla otomatik olarak tanımlar.
Pekiştirmeli Öğrenme	Öğrenme ortamında elde edilen başarı ve başarısızlıkla ilgili geri bildirimlerin kullanılmasına dayanır. Başka bir deyişle, bir ödül işlevini en üst düzeye çıkarmak için bir ortamda eylemler gerçekleştirir ⁸⁴ .

Makine öğrenimi daha iyi öğrenme mekanizmaları oluşturmayı ve bu mekanizmaları anlayabilmeyi amaçlamaktadır. McClelland’ın aşağıdaki ifadesi kavramın anlaşılmasına yardımcı olacaktır:

⁸³ STOA, Understanding Algorithmic Decision-making: Opportunities and Challenges, Brussel, 2019, s. 4.

⁸⁴ Pekiştirmeli öğrenmede hedef çıktıyı vermek için bir danışman yerine, elde edilen çıkışın verilen girişe karşılık iyi ya da kötü olarak değerlendirilen bir kuram kullanılmaktadır. Daha fazla bilgi için bkz: Atalay ve Çelik, **a.g.m.**, s. 161.

“İnsanlara yüz binlerce hatta milyonlarca resim toplamak ve sonra onları, içinde kedi olan ve olmayan fotoğraflar olarak kategorilere ayırma görevi veriliyor, ardından algoritma içinde kedi olan resimlerle olmayan resimleri ayırt edebilecek bir model oluşturmaya çalışıyor. Böylece doğruluk seviyesi yeterince yüksek olduğunda, makine artık bir kedinin neye benzediğini öğrenebiliyor”⁸⁵.

Makine öğrenimi algoritmaları, var olan verilerin içindeki kuralları ve gelecekteki benzer modelleri kavrayıp veri odaklı öngörülerde bulunabilir. Satranç algoritmasını örnek alırsa, satranç oynama kurallarını girdi olarak algoritmaya ekledikten sonra, daha önceden oynanan satranç oyun verileri ile eğitildiğinde, daha iyi satranç oynama becerisine sahip olabilmektedir.

1.3.2. Derin Öğrenme

Derin öğrenme, bir diğer adıyla Yapay Sinir Ağları, birden fazla doğrusal olmayan fonksiyonu kullanan makine öğrenim metodudur. Makine öğrenimi tek bir katmanda çalışırken, derin öğrenme aynı anda birden çok katmanda çalışır. Derin öğrenme bir grup makine öğrenim algoritmalarını aynı anda kullanarak tek işlemde sonuca ulaşmaya çalışabilmektedir. Yapay Sinir Ağları 1990’lı yıllarda çok büyük popülerite kazanmıştır. Bunun sebebi de insan seviyesine yaklaşan önemli başarılarla imza atmış olmasıdır.

Makine öğreniminin karşılaştığı zorluklardan biri, tahminlerin doğruluğunu önemli ölçüde etkileyen özellik miktarının nasıl tasarlanacağıdır. Derin öğrenme ise makine öğreniminin sınırlamalarını çözmek için herhangi bir veriden özellik miktarı oluşturabilmektedir. Derin öğrenme tahmin yapmak için makine öğrenimine benzer şekilde veriler üzerinde bir model eğitir, fakat makine öğreniminden farklı olarak

⁸⁵ Önder ve Saygılı, **a.g.m.**, s. 636.

verilerin öğrenilen özelliklerini farklı soyutlama katmanlarından geçirerek ayırt eder⁸⁶. yapay zekâ teknolojisi derin öğrenmeyi kullanarak bir insanın imajını bir kedinin imajından ayırt edebilir. Ayrıca Google Play, You Tube ve LINE'daki hedefli önerileri de yapabilmektedir⁸⁷. Tavsiye algoritmalarının bazıları makine öğrenimi benimserken, önde gelen tavsiye sistemleri derin öğrenme tekniği kullanmaktadır.

Derin öğrenme tekniğinde birden fazla hesaplama katmanları bulunmaktadır. Derin öğrenmede, besleyici veriler karmaşık bir şekilde katmanlar arasında yorumlanır ve sonuç üretilir. Ayrıca her bir hesaplama katmanı, besleyici veriler aracılığıyla kendini otomatik olarak ayarlayabilmektedir.

Örneğin, bir portakal resmi ile muz resmini ayırmamız gerekli olduğunda, makine öğreniminde, bugüne kadar oluşturulan tecrübeleri, parametreler aracılığıyla makineye tanıtılacaktır. “Eğer rengi turuncu ise portakal olabilme olasılığı yüksek, sarı ise muzdur” gibisinden “yuvarlak ise muhtemelen portakaldır, yay şeklindeyse muhtemelen muzdur” gibi birçok parametreyi manuel şekilde tanımlamamız gerekiyor⁸⁸. Ancak derin öğrenmede sadece yeterli sayıda muz ve portakal resmini girdi olarak algoritmaya eklediğimizde, daha önceden manuel şekilde eklenmesi gereken parametreler hatta onlardan daha iyilerini keşfedebilecektir.

Bir diğer örnek, Google çevirisi de derin öğrenme tekniğine dayalı bir algoritmanın kullanılmasıdır⁸⁹. Artık iki dil arasında manuel eklenen çeviriler bulunmaksızın derin öğrenme yoluyla çeviri yapılabilmektedir. Girdiği verilerin

⁸⁶ J. B. Heaton, N. G. Polson ve J. H. Witte, “Deep Learning in Finance”, arXiv:1602.06561, (Çevrimiçi) <http://arxiv.org/abs/1602.06561> (Erişim Tarihi: 12.10.2020), s. 3.

⁸⁷ Kaori Ishii, “Comparative Legal Study on Privacy and Personal Data Protection for Robots Equipped with Artificial Intelligence: Looking at Functional and Technological Aspects”, *AI & Soc*, S. 34 (2019), ss. 509-533, s. 510.

⁸⁸ Semih Şener, “Yapay Zekâ, Makine Öğrenimi ve Derin Öğrenme Arasındaki Farklar”, 10.09.2018, (Çevrimiçi) <https://www.endustri40.com/yapay-zeka-makine-ogrenimi-ve-derin-ogrenme-arasindaki-farklar/>, (Erişim Tarihi: 11.2019).

⁸⁹ Davide Castelvocchi, “Deep Learning Boosts Google Translate Tool”, 27.09.2016, (Çevrimiçi) <https://www.nature.com/news/deep-learning-boosts-google-translate-tool-1.20696>, (Erişim Tarihi: 10.2019).

miktarı açısından derin öğrenmede daha çok büyük veri ile ilişkilendirilir. Girdi olarak kullanılan verilerin korunması sorunu ise derin öğrenmede makine öğrenimine kıyasen daha fazladır. Nitekim derin öğrenme makine öğreniminkinden fazla algoritmik önyargı riski taşımaktadır. Derin öğrenmenin kullandığı kuram ise Yapay Sinir Ağları sistemidir.

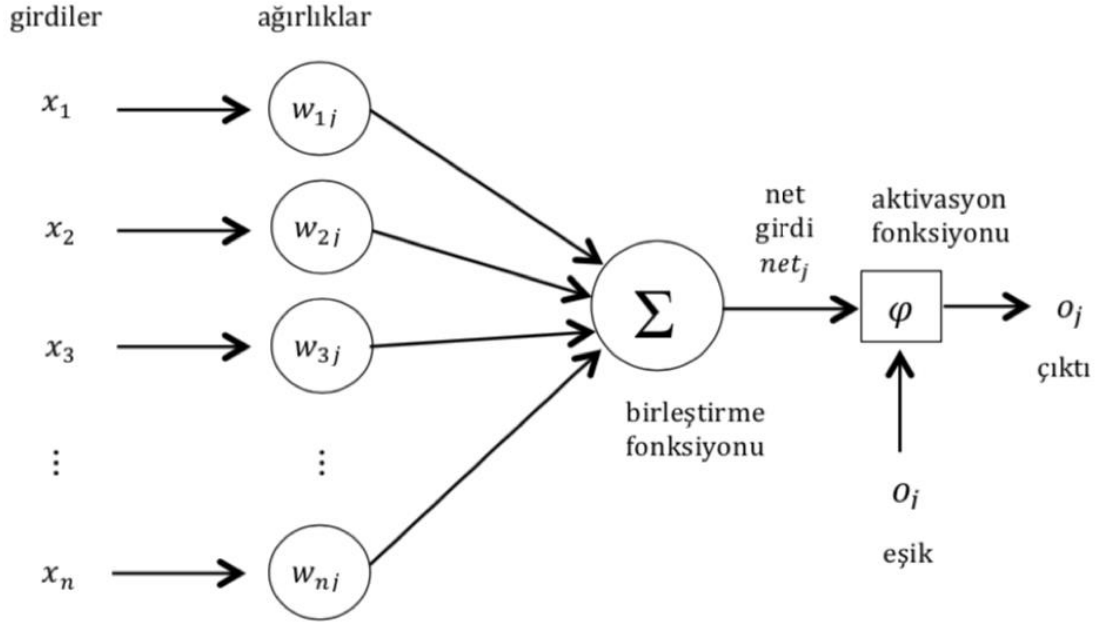
1.3.3. Yapay Sinir Ağları

Yapay Sinir Ağları makine öğreniminin yöntemlerinden biridir ve beyin aktivitesinin matematiksel modellerini çıkarmayı hedeflemektedir. Günümüzdeki sinirbilimin temel bulguları, “*zihinsel aktivitenin nöron adı verilen beyin hücreleri ağlarındaki elektrokimyasal aktiviteden oluştuğu*” hipotezine dayanmaktadır⁹⁰. Yapay Sinir Ağları insan beyninin öğrenme yöntemine benzeyen şekilde öğrenme, hatırlama, çıkarım yaparak topladığı verilerden yeni veri üretmeye benzeyen temel işlevlerin gerçekleştirdiği bilgisayar yazılımlarıdır⁹¹. Örnek olarak Alpaca’nın otomatik alım satımlar oluşturan “Capitalico” veya çok katmanlı sinir ağı kullanarak duyguları ifade eden Softbank’ın “Pepper” verilebilir.

Yapay Sinir Ağları, biyolojik sinir ağlarındaki sinir hücrelerinin aksine yapay sinir hücrelerinden oluşur. Her bir yapay sinir hücresi; girdi, ağırlık, toplama işlevi, aktivasyon işlevi ve çıktı gibi temel unsurlardan oluşur. (Şekil 1).

⁹⁰ Norvig ve Russell, **a.g.e.**, s. 728.

⁹¹ Kadir Öztürk ve Mustafa Ergin Şahin, “Yapay Sinir ağları ve Yapay Zekâ ‘ya Genel Bir Bakış”, **Takvim-i Vekayi**, (2018), s. 27.



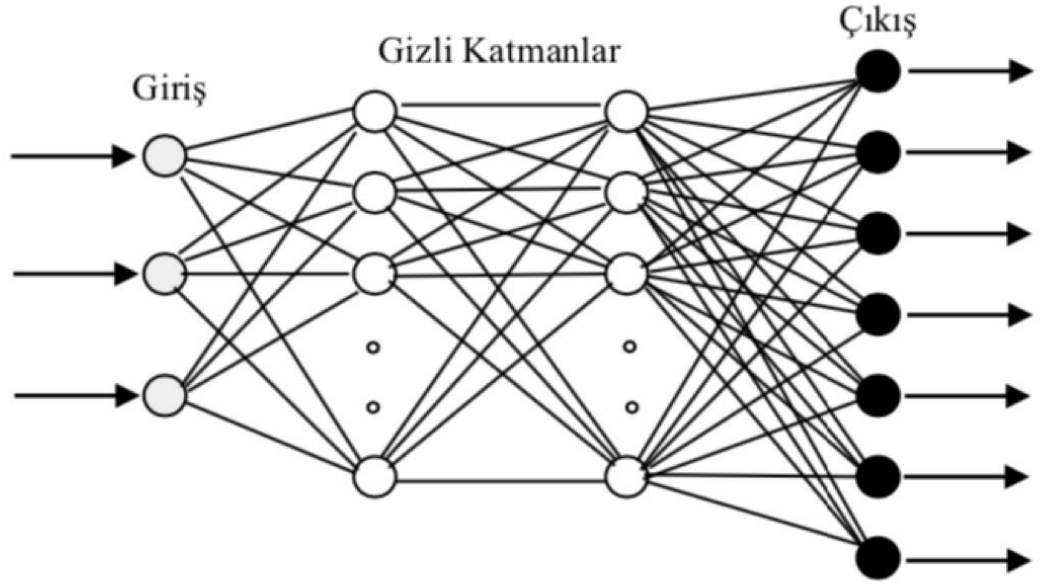
Şekil 1: Yapay Sinir Hücresi Yapısı⁹²

Yapay sinir hücreleri yapay bir sinir ağı oluşturmak için hiyerarşik olarak birleşir. Yapay sinir ağının her katmanı bir giriş katmanı, bir çıktı katmanı ve ikisi arasında gizli bir katmandan oluşur ve her katman yapay sinir hücrelerinden oluşur. (Şekil 2).

“Girdi ve çıktı katmanındaki nöron sayısı, bağımsız ve bağımlı değişkenlerinin sayısı ile belirlenir. Gizli katmandaki katman sayısı ve her bir gizli katmanda bulunacak nöron sayıları, en iyi performansı verecek şekilde kullanıcı tarafından belirlenir”⁹³.

⁹² Metin Uslu, “Yapay Sinir Ağları (YSA) Nedir?” (Çevrimiçi) <http://kod5.org/yapay-sinir-aglari-ysa-nedir/>, (Erişim Tarihi: 15.12.2020), par. 8.

⁹³ Atalay ve Çelik, **a.g.m.**, s. 162.



Şekil 2: Çok Katmanlı Yapay Sinir Ağı Yapısı⁹⁴

Kısacası Yapay Sinir Ağları örnekler üzerinden olaylar arasındaki ilişkileri öğrenerek daha önce hiç rastlanmadığı durumlara karşı karar verebilen sistem diyebiliriz.

Yapay Sinir Ağları her geçen gün sağlık alanı başta olmak üzere hayatımızın her alanına girmeye başlamıştır. Otomotiv, elektronik, enerji, uzay bilimleri, finans ve askeri alanlarında yaygın şekilde kullanılmaktadır⁹⁵. Bununla beraber Yapay Sinir Ağları uygulamalarında kişisel verilerin toplanması, saklanması, kullanılması ve aktarılması önemli ölçüde artmış durumundadır.

⁹⁴Cansu Altunbaş, “Yapay Sinir Ağları (YSA)”, 13.02.2020, (Çevrimiçi)

<https://medium.com/t%C3%BCrkiye/yapay-sinir-a%C4%9Flar%C4%B1-ysa-caec1cc0bf9f>, (Erişim Tarihi: 15.11.2020), par. 2.

⁹⁵ Ünal Kaya ve Yüksel Oğuz, “An Assessment of Energy Production Capacity of Amasra Town Using Artificial Neural Networks”, **Turkish Journal of Electromechanics & Energy**, 2018, s.23.

Yapay zekâ özellikle makine öğrenimi ve derin öğrenme, cümleden Yapay Sinir Ağları teknolojilerinde oldukça büyük miktarda veriler işlenmektedir. Burada kastedilen her türlü veri olmakla birlikte, kişisel veriler de kaçınılmaz olarak yapay zekâ teknolojilerince işletiliyor. Günümüzde Yapay Sinir Ağları yardımıyla derin öğrenme ve makine öğrenimi ortamlarında gerçekleştirilen analiz, manuel analizin çok ötesine geçmektedir⁹⁶.

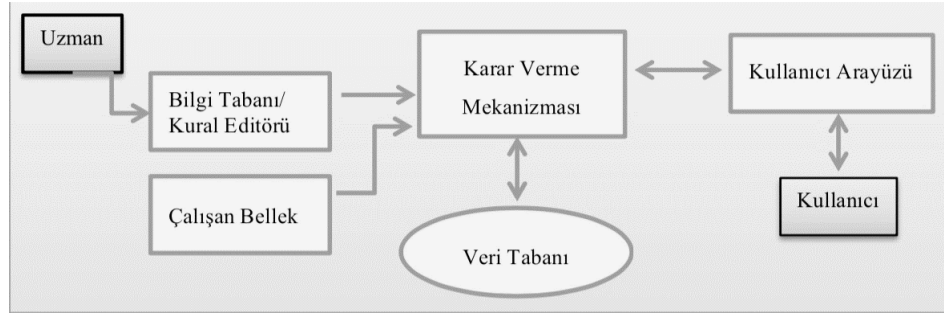
1.3.4. Uzman Sistemler

Uzman sistem bir uzmanın problemleri çözdüğü gibi problem çözme becerisine sahip sistemlerin adıdır ve genelde uzmanlık bilgisi ile donatılır. Çıkarım mekanizmaları bilgiler arasında ilişkiler kurarak karar verir⁹⁷. Yani uzman sistemlerde problemi çözmede uzman kişi veya kişilerin bilgi ve mantıksal çıkarım mekanizmasının modellenmesi gerekmektedir⁹⁸. Şekil 3'te bir uzman sistemin genel yapısı gösterilmiştir. Makine öğreniminden farklı olarak her uzman sistemde öğrenme davranışı olmayabilir, ama geliştirildikten sonra karşılaşılan problemler karşısında uzman ile aynı sonuca varması gerekmektedir. Günümüzde uzman sistemler daha çok tıp ve danışmanlık sektörlerinde uzman eksikliğini giderme amacıyla kullanılmaktadır.

⁹⁶ Lilian Mitrou, "Data Protection, Artificial Intelligence and Cognitive Services: Is The General Data Protection Regulation (GDPR) 'Artificial Intelligence-Proof'?", **SSRN**, 2018, s. 19.

⁹⁷ Ercan Öztemel, **Yapay Sinir Ağları**, İstanbul: Papatya Yayıncılık, 2012, s. 3.

⁹⁸ Paul Harmon, **Expert Systems: Artificial Intelligence in Business**, Wiley, 1985, s. 5.



Şekil 3: Uzman Sistemin Genel Yapısı⁹⁹

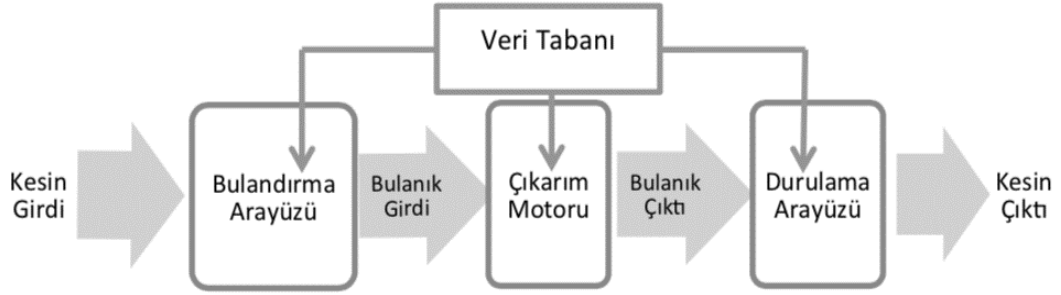
1.3.5. Bulanık Mantık

Bulanık mantık, “klasik matematiğin standartlarına göre pek çok bakımdan belirsiz olan veya kesin olmayan karar süreçlerine matematiksel bir kesinlik kazandıran kavramlar ve yöntemler” için kullanılan kavramdır¹⁰⁰. Bir yapay zekâ tekniği olan bulanık mantık, insan gibi düşünebilen, seçim yapabilen ve karar verebilen sistemlerin oluşmasını amaçlamaktadır¹⁰¹. Bulanık mantık aslında belirsiz bilgileri işleyebilme ve kesin sayılar ile ifade edilemeyen durumlarda karar vermeyi kolaylaştıran bir yapay zekâ teknolojisidir. Şekil 4’te bulanık mantığın genel yapısı gösterilmiştir.

⁹⁹ Duygu İçen ve Süleyman Günay, “Uzman Sistemler ve İstatistik”, **İstatistikçiler Dergisi: İstatistik&Aktüerya**, S. 7 (2014), ss. 37-45, s. 41.

¹⁰⁰ Kürşat YENİLMEZ, “Bulanık Doğrusal Programlama Problemleri İçin Yeni Çözüm Yaklaşımları ve Duyarlılık Analizi”, (Osmangazi Üniversitesi Fen Bilimleri Enstitüsü Yayınlanmamış Doktora Tezi), Eskişehir, 2001, s. 2.

¹⁰¹ Atalay ve Çelik, **a.g.m.**, s. 160.



Şekil 4: Bulanık Mantığın Genel Yapısı¹⁰²

Normal bir yazılım temel girdiler, yazılım programı ve sabit sonuçtan teşkil etmektedir. Oysa bulanık mantık yazılım programı belirsiz sayıda veri, yazılım programı ve varsayımlara göre değişen bir veya birden fazla sonucu içermektedir. Aynı bulanık mantık programındaki girdi aynı olsa bile farklı sonuçlar ortaya çıkabilmektedir¹⁰³.

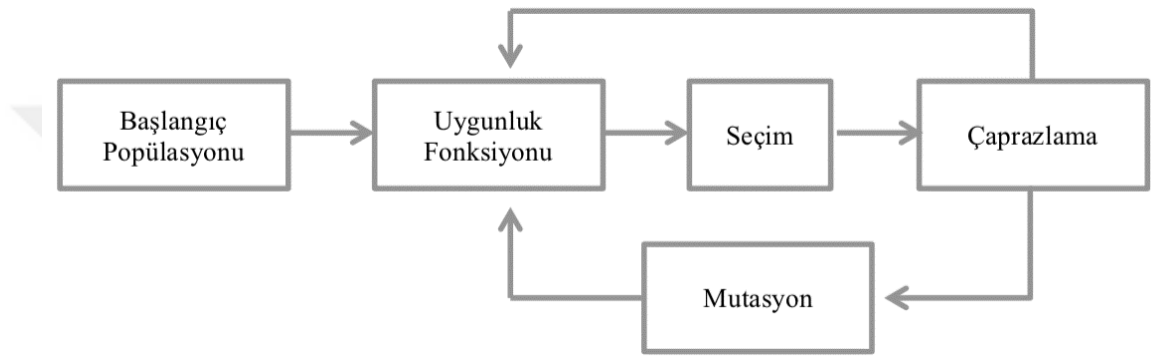
1.3.6. Genetik Algoritma

Genetik algoritmalar evrim teorisinin temeli olan “*doğal seçim*” ile “*en iyi bireylerin hayatta kalması*” ilkesini taklit eden bir çeşit yapay zekâ tekniğidir. Yapılan işlem ise pek çok çözüm seçeneği içinden arama yaparak en iyi çözümün belirlenmesidir. Arama tekniklerini kullanarak mevcut çözümlerden hareketle en iyi çözüme ulaşılmayı hedeflemektedir. Geleneksel optimizasyon teknikleri ile çözülemeyen problemleri çözmek için geliştirilmiştir. Problemlerin bütün çözümlerini

¹⁰² Ahmet Ataşoğlu, “Bulanık Mantık 3: Bulanık Kurallar ve Çıkarım”, 14.08.2019, (Çevrimiçi) <https://ahmetatasoglu98.medium.com/bulan%C4%B1k-mant%C4%B1k-3-bulan%C4%B1k-kurallar-ve-%C3%A7%C4%B1kar%C4%B1m-8f9d411080c>, (Erişim Tarihi: 15.11.2020), par. 5.

¹⁰³ Sabah, “Bulanık Mantık Nedir, Nasıl Uygulanır? Bulanık Mantık Tarihçesi ve Özellikleri ile İlgili Merak Edilenler”, 17.09.2020, (Çevrimiçi) <https://www.sabah.com.tr/yasam/2020/09/17/bulanik-mantik-nedir-nasil-uygulanir-bulanik-mantik-ozellikleri-nelerdir-tk1>, (Erişim Tarihi: 15.12.2020).

birleştirerek daha iyi çözümler üretmek felsefesine dayanmaktadır¹⁰⁴. Genetik algoritmanın işlemin ilk adını problemin olası çözümler dizilere kodlanarak çözümü yığınının oluşturulmasıdır. “Çözümler dizilerin yaklaşma başarısının uygunluk fonksiyonu ile değerlendirilmesi, genetik parametrelerin belirlenmesi, seçim stratejisi ve mekanizmaları, genetik operatörler ve durdurma kriteri şeklinde sıralanabilir”¹⁰⁵. Genetik algoritmaların yapısı Şekil-5’ te gösterilmiştir.



Şekil 5: Genetik Algoritmanın Genel Akış Şeması¹⁰⁶

Özetle bütün yapay zekâ teknikleri veri ile beslenmekte, veriye dayalı karar vermektedir. Veri ve/veya kişisel verileri yapay zekâ çağında yapay zekâ tekniklerin özellikleri nedeniyle bu kadar önemli hale gelmiştir. Nitekim veriler yapay zekanın beslenme kaynağıdır. Ayrıca Veriler niteliği ve niceliği verilen kararın niteliği açısından çok önemlidir. Örneğin, girdi yapılan verilerin kendisinden kaynaklanan ayrımcı nitelikler makine öğrenimi, derin öğrenme, Yapay Sinir Ağları vb. tekniklerde de sonucu direk etkileyecektir. Yapay zekâ çağında veri ve/veya kişisel verilere fazla ihtiyaç duyulmakla beraber, yapay zekâ tekniklerin özelliklerinden kaynaklanan

¹⁰⁴ Öztemel, a.g.e., s. 4.

¹⁰⁵ Elmas Çetin, **Yapay Zekâ Uygulamaları**, Ankara: Seçkin Yayıncılık, 2011, s. 387-401

¹⁰⁶ Refik Nureddin, “Optimizasyon Algoritmaları”, 17.06.2019, (Çevrimiçi) <https://medium.com/deeplearning-turkiye/optimizasyon-algoritmalar%C4%B1-ba3774968aa>, (Erişim Tarihi: 15.11.2020), par. 14.

önyargı/ayırımcı sorunlarını önlemek için kişisel verilerin korunması da aynı şekilde ihtiyaç duymaktadır.

1.4. Yapay Zekâ Çeşitleri

Bilim insanları yapay zekâyı temel olarak Güçlü Yapay Zekâ ve Zayıf Yapay Zekâ şeklinde iki kategoriye ayırmışlardır. Güçlü Yapay Zekâ henüz gerçekleşmemekle birlikte insan beyni taklit edilip, insana benzer şekilde düşünebilen ve çalışabilen teknolojinin geliştirmesini hedef almaktadır. Zayıf Yapay Zekâ ise bazı kurallara dayanan, önceden planlanmış işlemleri gerçekleştirebilen ve bunları belirli bir problemi çözmede uygulayan teknolojinin geliştirilmesini hedeflemektedir¹⁰⁷. Günümüzde IBM Şirketi'ne ait Deep Blue isimli satranç oynayan program, Google'a ait olan AlphaGo isimli Go oyunu oynayan program, Apple'un Siri, Amazon'un Alexa gibi uygulamalar Zayıf Yapay Zekâ kategorisine aittir.

Planlanan ve uygulanan işlem çerçevesinde bakarsak bilinen ve kabul edilen dört tür yapay zekâ bulunmaktadır. Ancak günümüzde sadece ilk iki tür yapay zekâ ile karşılaşmaktayız. Üçüncü ve dördüncü tür yapay zekânın gelişimi henüz tamamlanmamış olarak bilinmektedir¹⁰⁸.

1.4.1. Reaktif Yapay Zekâ

İlk tür yapay zekâ, tepki veren yapay zekâ (reaktif) olarak adlandırılmaktadır. Bu tür yapay zekâ çevreyi ve gördükleri üzerine tepki verir ve sadece tek bir alanda uzmanlaşabilir. Yani tamamen tepkisel yapay zekâ türüdür. Örneğin IBM Şirketi'nin Deep Blue adlı yapay zekâsı dünya satranç şampiyonu Kasparov'u yenmiş, Google'a

¹⁰⁷ Bozkurt Yüksel, Yapay Zekanın Buluşlarının..., **a.g.m.**, s. 590.

¹⁰⁸ Arend Hintze, "Understanding the Four Types of AI, From Reactive Robots to Self-aware Beings", 14.11.2016, (Çevrimiçi) <https://theconversation.com/understanding-the-four-types-of-ai-from-reactive-robots-to-self-aware-beings-67616>, (Erişim Tarihi: 03.10.2019).

ait olan AlphaGo isimli Go oyunu oynayan programı buna örnek teşkil etmektedir¹⁰⁹. Reaktif yapay zekânın özelliği aktif şekilde değil, ancak aktif şekilde veri girdisi yapıldığında reaktif şekilde yorumlaması, işlem görmesi ve ona göre tepki vermesidir.

1.4.2. Sınırlı Hafızalı Yapay Zekâ

İkinci tür yapay zekâ yalnızca tepki vermek ile kalmayıp sınırlı hafıza kapasitesine, geçmişin bilgisine ve önceden programlanmış becerilere sahiptir. Bu sebeple sınırlı hafıza kapasitesine sahip yapay zekâ (Limited Memory Capacity) olarak adlandırılmaktadır¹¹⁰. Örneğin, Sürücüsüz araçlar, Chat botlar.

1.4.3. Zihin Teorisi

Üçüncü tip yapay zekâ ise otonomi düzeyi artan yapay zekâ olup bir diğer adı Zihin Kuramı (Theory of Mind) dır. Zihin kuramı insanların duygularını ve düşüncelerini anlayabilen ve onlarla sosyal olarak ilişkiye geçebilen bir yapay zekâ çeşitidir¹¹¹. Hatta artık sadece insanları değil, kendi içlerinde de yani başka bir yapay zekânın dilini ve yaptığını anlayan, aynı zamanda tepki verebilen türüdür. Ancak günümüzde henüz bu tip yapay zekâ geliştirilmiş değildir. Ancak fantezi filmlerinden örnek verilebilir. Mesela “*I Robot*” filmindeki Sonny gibi¹¹². Yakın zamanda Londra’da geliştirilen “*ToMnet*” diğer yapay zekâları anlayabilen yapay zekâ olarak ortaya çıkmıştır¹¹³. Fakat bunun ne kadar zihin teorisi ile eşleştiği tartışmalıdır.

¹⁰⁹ Başak Bak, “Medeni Hukuk açısından Yapay Zekânın Hukuki Statüsü ve Yapay Zekâ Kullanımından Doğan Hukuki Sorumluluk”, **Türkiye Adalet Akademisi Dergisi**, S.35 (Temmuz 2018), s. 213.

¹¹⁰ Bak, **a.g.m.**, s. 214.

¹¹¹ Bak, **a.g.m.**

¹¹² Bozkurt Yüksel vd., *Fütürist...*, **a.g.e.**, s. 10.

¹¹³ Mustafa Küçük, “Yapay Zekâ Nedir? Nereye Gidiyor?”, E-Bursum, 13.02.2019, (Çevrimiçi) <https://blog.e-bursum.com/yapay-zeka/>, (Erişim Tarihi: 06.12.2020).

1.4.4. Kendi Kendinin Farkında Olan Yapay Zekâ

Dördüncü ve en gelişmiş yapay zekâ ise kendi varlığının farkında olan yapay zekâ (self-aware) olup etrafındaki kişilerin duygularını algılayabilir ve öngörebilir derecesinde farkındalığa sahiptir¹¹⁴. Mükemmel derecede zeki, önseziye sahip ve bilinçlidir. 2015 tarihli “*Ex Machine*” filmindeki Eva karakteri bu tip yapay zekâyâ örnek olarak gösterilebilir¹¹⁵. Bu tür yapay zekânın insan gibi özgür iradesinin olabileceği öngörülmektedir.

1.5. Yapay Zekânın Pratik Uygulamaları

Günümüzde yapay zekânın pek çok uygulama alanı bulunmakta ve büyüyen ticari teknolojiler için bilimsel temeller hazırlamaktadır. En önemli uygulama alanları ise robotik, ses tanıma, doğal dil işleme vb. algılayıcı sistemler, bilgisayar yaratıcılığı sayılabilir. Yapay zekânın birçok endüstri ve iş modelini değiştirmesi, ona duyulan ilginin artmasına da sebep olmuştur¹¹⁶. Günümüzde ise neredeyse hayatımızın her yerinde yapay zekâ uygulamalarını rastlamaktayız. Bu başlık altında yapay zekânın en yaygın kullanılan alanlarından (Use-Case) örnekler verilecektir.

1.5.1. Doğal Dil İşleme

Doğal dil işleme “*Bilgisayarların doğal dildeki metni veya konuşmayı anlamak ve yararlı şeyler yapmak için nasıl kullanılabileceğini araştıran bir araştırma ve uygulama alanı*” olarak tanımlanmaktadır¹¹⁷. İnsanlar tarafından konuşulan doğal dili anlayan bilgisayarla etkileşim kurmak doğal dil işleme sayesinde mümkün olmuştur.

¹¹⁴ Bak, **a.g.m.**, s. 214.

¹¹⁵ Bozkurt Yüksel, Yapay Zekanın Buluşlarının..., **a.g.m.**, s. 592.

¹¹⁶ Yapay Zeka uygulamalarına ilişkin daha fazla bilgi için bkz: Ayyüce Kızrak, “Yapay Zeka Kullanım Alanları ve Uygulamalarına Derinlemesine Bir Bakış”, Medium, 07.01.2019, (Çevrimiçi) <https://ayyucekizrak.medium.com/yapay-zeka-kullan%C4%B1m-alanlar%C4%B1-ve-uygulamalar%C4%B1na-derinlemesine-bir-bak%C4%B1%C5%9F-d0fecaf7f61b>, (Erişim Tarihi: 06.12.2020).

¹¹⁷ Gobinda G. Chowdhury, “Natural language processing”, **Annual Review of Information Science and Technology**, C. 37, S. 1 (Ocak 2005), s. 51.

Makinelerin ses ve yazılı metinleri anlamasını sağlamak amacıyla çeviri, enteraktif diyalog ve duygu analizi gibi görevleri otomatikleştirmekte kullanılmaktadır¹¹⁸. Google Now, Apple'un Siri'si, Microsoft'un Cortana'ı ve otomatik çeviri hizmetleri doğal dil işleme kullanılmaktadır¹¹⁹. Yapay Sinir Ağları doğal dil işlemede bu asrın başından beri kullanılıyordu. Günümüzde spam algılama, yazı stili tanıma, bilgi getirimi, konuşma dili tanıma, metin sınıflandırma ve makine çevirisinde kullanılmaktadır.

1.5.2. Hukuk Alanında Akıllı Robot/Hakimler

Günümüzde yapay zekâ kullanımlı robotlar bir insanın verdiği görevleri kolayca yerine getirebilmektedir. Bu tür akıllı robotlar gerçek dünyadaki fiziksel verileri (örneğin, ışık, ısı, sıcaklık, hareket, ses, çarpma ve basın gibi) algılayan sensörlere, verimli işlemciler ve büyük belleğe sahiptir. Bunlara ek olarak, yapay zekâ sayesinde hatalarından öğrenebilme ve yeni çevreye uyum sağlayabilme yeteneğini de sahiptir. Özellikle asistan robotlar günümüzde çok sık rastlanmaktadır. Bunların başında hukuk alanında kullanılmaya başlayan robot avukatlar gelmektedir.

İstatistiklere göre, günümüzde avukatların hukuki işlerinin %23'ü yapay zekâ ile tamamlanabilir hale gelmiştir. Yapay zekâ sayesinde akıllı robotun kendisi bir kendi kendine öğrenme yeteneği oluşturabilir, mevcut bilgileri analiz edebilir ve inceleyebilir, böylece yargı uyarıları ve önerilerde bulunabilir durumuna gelebilmektedir. Hatta bazı insanlar gelecekte akıllı robotların doğrudan hâkim olabileceğini düşünmektedir¹²⁰. Günümüzde, ABD başta olmak üzere hukuk alanında akıllı robotların, avukat ve hakimlerin kullanılması konusunda başarılarla imza atmıştır denilebilir.

¹¹⁸ Önder ve Saygılı, **a.g.m.**, s. 637.

¹¹⁹ Ishii, **a.g.m.**, s. 511.

¹²⁰ Gao Qiqi ve Zhang Peng, "On the Multidimensional Challenges of Artificial Intelligence to the Future Law", **East China University of Political Science and Law**, S. 1 (2018), s. 3.

Yapay zekâ teknolojisinin hızla gelişmesiyle birlikte, yapay zekâ ve yasal çalışmanın birleşimi giderek daha yoğunlaşmıştır. Örneğin, Haziran 2016’da IBM’in bilişsel bilgisayarı Watson tarafından desteklenen tarihteki ilk yapay zekaya sahip avukat Ross, bir Amerikan hukuk firması tarafından “işe alınmıştır”. Ross doğal dil işleme uygulamaları aracılığıyla avukatlarla insan dilinde iletişim kurabilir ve iflas danışmanlığı konuları ile ilgilenebilmektedir¹²¹.

Yapay zekâ teknolojisi kullanılan yasal araştırma alanı olan Casetext, CARA Research Suite’in yardımıyla daha iyi, daha hızlı şekilde hukuk araştırması yapılmasına, ihtiyaç duyulan vakaların keşfedilmesine ve derinlemesine anlaşılmasına yardımcı olabilmektedir. ABD’de hakimler, hukuk büroları ve özel firmalar Casetext CARA uygulamasını kullanmaktadır¹²². Öbür taraftan, ABD Federal dava analizinde öncü olan Lex Machina, yapay zekalı dava analizi modüllerinin geliştirmiş ve en son New York Mahkemeleri’nde kullanılmaya başlamıştır.

Avrupa Birliği (AB) ise avukatların ve hukuk firmalarının BT yeteneklerinin ortalama durumu konusunda tutarlı bir anlayış veya doğal dil işleme araçlarının kullanımına ilişkin fırsatlara ve engellere ilgili genel bir değerlendirmenin bulunmaması nedeniyle AI4Lawyers projesi başlatılmıştır. Halen yürürlükte olan proje AB’nin güvenilir yapay zekâ için küresel bir standart belirleme tutkusunun simgesi olarak görülebilir.

Özetle bakacak olursak, bir taraftan teknoloji açısından hukuki mesleklerde yapay zekâ yaygın kullanılmaya başlamıştır, öbür taraftan ise AB’nin yaptığı gibi küresel bir etik standart belirleme çalışmaları devam etmektedir.

¹²¹ Stacy Liberatore, “Your AI Lawyer Will See You Now: IBM’s ROSS Becomes World’s First Artificially Intelligent Attorney”, MailOnline, (Çevrimiçi) <https://www.dailymail.co.uk/sciencetech/article-3589795/Your-AI-lawyer-IBM-s-ROSS-world-s-artificially-intelligent-attorney.html>, (Erişim Tarihi: 10.01.2021).

¹²² CARA, “Casetext-Cara Legal & Fact Finder”, (Çevrimiçi) <https://www.welcome.ai/tech/legal/casetext-cara-legal-fact-finder>, (Erişim Tarihi: 10.01.2021).

Makro açıdan bakıldığında, yapay zekâ teknolojisi, hukuk endüstrisinin çalışma şeklini derinden değiştirmesi söz konusu olabilir. Mevcut teknoloji ve endüstri gelişimi eğilimine göre, hukuk mesleğinde bazı yapısal değişikliklerin olacağı tahmin edilebilir. Örneğin, araştırma ve geliştirme alanında teknoloji ve veriye olan bağımlılık, hukuk alanında yapay zekâ teknolojisinin araştırma ve geliştirilmesine yapılan yatırımın uzun süre genişlemeye devam edeceğini belirleyecektir. Düşük seviyeli uygulama alanında, açık ve basit kural sistemi ve yüksek standartlı kanıt sistemi olan bazı senaryolarda, yasal yapay zekâ teknolojisinin geliştirilmesi, sonunda bu hukuk uygulayıcılarının çoğunun yerini alabilecektir. Örneğin, New York şehrinde, park ihlallerini çözmek için otomatik bir çevrimiçi anlaşmazlık çözüm sistemi uygulanmaya başlanmıştır. Üst düzey uygulama alanında, karmaşık durumlar için yapay zekâ, yeni bir insan-bilgisayar iş birliğine dayalı işleme yöntemi oluşturarak hukuk uzmanlarının çalışmalarına yardımcı olabilecektir¹²³.

1.5.3. Sürücüsüz Araçlar

Yapay zekânın en yaygın şekilde duyurulan pratik uygulamalarından biri otonom araçların ve daha spesifik olarak, birkaç otomobil üretim şirketi tarafından sürücüsüz otomobillerin yanı sıra, kamuya açık yollarda otonom olarak çalışmak üzere tasarlanmış araçların geliştirilmesidir. Mevcut sürücüsüz araç sektörü düzenlemesinin potansiyel engellerini sınırlandırmak için, birkaç AB ülkesi hükümeti:

“Her hareket eden aracın veya araç kombinasyonunun bir sürücüsü olması gerektiği” ve “her sürücünün her zaman aracını kontrol edebilmesi gerektiğini”¹²⁴

¹²³ Teng Hu ve Huafeng Lu, “Study on the Influence of Artificial Intelligence on Legal Profession”, 5th International Conference on Economics, Management, Law and Education, Krasnodar, 11-12 Ekim 2019, s. 967.

¹²⁴ BM Karayolu Trafikine İlişkin Viyana Sözleşmesi, madde 8.

vurgulayan Karayolu Trafiğine İlişkin 1968 Viyana Sözleşmesi'nin güncellenmesini önermiştir.

Günümüzde Tesla başta olmak üzere, Google'un da katıldığı sürücüsüz araç endüstrisi oldukça popüler olmaktadır. “Stanley” adında sürücüsüz otomobil Mojave’de 22 mil hızla 132 millik mesafeyi bitirip 2005 Darpa Grand Challenge’ı kazanmıştır¹²⁵. Geçtiğimiz senede Tesla yaklaşık beş yüz bin araçlık teslimat hedefine ulaştığını açıklamıştır. Sürücüsüz araçlar yapay zekâ teknolojisi kullanılan en yaygın uygulama niteliğindedir.

1.5.4. Görme Sistemleri

Görme sistemleri bilgisayardaki görsel girdileri anlamak, yorumlamak için kullanılmaktadır. Yapay zekâ sayesinde uydu görüntüleri, tıbbi resimler, anten, dijital video vb. çeşitli kaynaklardan elde edilen verilerin toplanmasını, saklanması, işlenmesini ve analiz edilmesini sağlayabiliyor. Görme sistemleri aracılığıyla yaşadığımız çevrenin üç boyutlu yapısını algılamamız kolaylaşıyor. Araştırmacılar, nesnelerin üç boyutlu şeklini ve görüntülerdeki görünümünü incelemek için yeni teknikler geliştiriyorlar. Optik karakter tanıma (OCR) ve otomatik plaka tanıma (ANPR) gibi bilgisayarla görme uygulamaları günümüzde yaygın kullanılan yapay zekâ uygulamalarıdır¹²⁶.

1.5.5. Konuşma Tanıma

Konuşma tanıma derin öğrenmenin en ikna edici uygulaması olarak bilinmektedir. LSTM (Yinelenen Sinir Ağı) yapısındaki ağlar çok karmaşık ve uzun konuşmaları rahatlıkla tanıyabilmektedir. Bu alanda Amazon, Skype, Cortana, Xbox, Google Translate, Apple Siri uygulamaları örnek olarak söylenebilir. Konuşma tanıma ve iletişim yönetimi sistemi tarafından yönlendirilen yapay zekâ uygulaması United

¹²⁵ Norvig ve Russell, **a.g.e.**, s. 28.

¹²⁶ Önder ve Saygılı, **a.g.m.**, s. 637.

Airlines'ı uçuş rezervasyonu için arayan biri ile bütün konuşmayı rahatlıkla yapabilmektedir. 2019 senesi Google I/O geliştirici konferansı orijinal demosu sırasında, Google Duplex'in sistemi insan konuşmasını taklit etmiş ve anında bir insan gibi ses çıkarıp rezervasyon yapmayı gerçekleştirmiştir¹²⁷. Konuşma tanıma özellikle mobil uygulamalarında kullanıcıların seslerinden veri üretme amacıyla kullanılmaktadır. Artık kullanıcıların yazmasına ihtiyaç olmaksızın sadece sesini çıkararak yapay zekâ uygulamaları ile iletişim halinde olabilmektedir.

Kısacası, yapay zekâ, sohbet ara yüzü, doğal dil işleme araçları, ses analizi vb. aracılığıyla birçok yararlı veri analiz aracı sağlamaktadır. Aynı zamanda, yorumların ve önerilerin otomatik analizi önemli değer yaratmaktadır. Birçok uygulama alanına entegrasyon sayesinde, yapay zekâ kullanımı daha da genişleyebilir.

1.6. Yapay Zekanın Bugünü ve Geleceği

1.6.1. Günümüze Kadar Yapılan Yapay Zekâ ile İlgili Çalışmalar

Tablo 3'te Yapay zekâ ile ilgili beyin incelemeleri ile başlanan ve günümüze kadar gelen önemli çalışmalar, dönüm noktaları yer almaktadır.

Tablo 3: Yapay Zekâ Çalışmalarının Kronolojik Listesi

1890	İnsan beyninin fonksiyonu ve yapısı ile ilgili ilk yazı yayınlandı.
1940	Yapay Sinir Ağları teorisi ortaya konuldu.
1950	Alan Turing "Turing testi"ni önerdi.

¹²⁷ Gözde Ulukan, "Yapay Zekâ Destekli Rezervasyon Uygulaması Google Duplex, Ios ve Android Cihazlar İçin Aktif Ediliyor", 04.04.2019, (Çevrimiçi) <https://webrazzi.com/2019/04/04/yapay-zekadestekli-rezervasyon-uygulamasi-google-duplex-ios-ve-android/>, (Erişim Tarihi: 03.10.2019).

1951	“Mark One” isimli aygıt için ilk yapay zekâ programı yazıldı.
1952-1962	IBM satranç oynayabilen ilk bilgisayar programı geliştirdi.
1956	Dartmouth Konferansın gerçekleşti.
1965	İlk makine öğrenmesi kitabı yayımlandı.
1965	Eliza programı yazıldı.
1980	Yapay zekâ ilk kez endüstride kullanılmaya başladı.
1986	Yapay Sinir Ağlarında teorik dönüşüm gerçekleşti.
1997	Deep Blue dünya şampiyonu Gary Kasparov’u yendi.
2010	Asimov’unun zihin gücü kullanılarak hareket etmesi sağlandı.
2014	“Deep face” Facebook tarafından geliştirildi.
2017	AlphaGo yazılımı strateji oyunu olan GO’da dünya şampiyonunu yendi.
2019	Google Duplex asistanı geliştirildi.
2020	İnsanların yazdığı metinlere benzer içerik üretebilen derin öğrenme kullanımlı dil modeli GTP- 3 geliştirildi.

1.6.2. Yapay Zekânın Günümüzdeki Durumu

Çok hızlı gelişen yapay zekâ teknolojisi karşısında uluslararası arenada farklı reaksiyonlar gösterilmiştir. İnsanlığın en heyecan verici gelişmelerinden biri olan yapay zekâ ülkeler açısından dönüştürücü fırsatlar sunabilme beklentisi ile çok miktarda yatırım çekmiştir. Hatta ülkeler arasında yapay zekâ alanına yatırım yapma konusunda bir yarış olduğu da söylenebilir.

Örneğin, International Data Corporation (IDC) tarafından yayınlanan verilere göre en çok yapay zekâ alanında harcama yapan ABD, 2017 yılında aynı alanda yaklaşık 9,7 milyar dolarlık gelir elde etmiştir. CBInsights'ın "AI 100" adlı araştırma sonucunda açıklamasına göre dünyadaki en iyi yapay zekâ şirketlerinin yaklaşık %80'ı ABD şirketi çıkmıştır¹²⁸. ABD Savunma Bakanlığı, Haziran 2018'de 600 kadar yapay zekâ projesinin tek çatı altında toplandığını ve bu projelerin maliyetinin 1,7 milyar dolara ulaştığını açıklamıştır¹²⁹. Özetle ABD teorik açıdan da pratik açıdan da yapay zekâ konusuna en fazla yatırım yapan ülkeler arasındadır.

Yapay zekâ alanında fazla yatırım yapan bir diğer ülke Çin'dir. Çin başlangıçta yapay zekânın gelişmesine adanmış bir teknoloji parkı inşa etmeye hazırlandığını belirtmiştir. Yapay zekâ alanında dünyadaki önemli bir güç haline gelmeyi hedefleyen Çin, söz konusu park için 2,1 milyar dolar yatırım yapmaya planlamıştır¹³⁰. Çin 2030 yılına kadar 150 milyar dolarlık bir yapay zekâ endüstrisi yaratmayı planlamıştır¹³¹.

¹²⁸ Comstock, J, "In Small Study, Aicure App Led to 50 Percent Improvement in Medication Adherence", (Çevrimiçi) <http://www.mobihealthnews.com/content/small-study-aicure-app-led-50percent-improvement-medication-adherence>, (Erişim Tarihi: 01.09.2019).

¹²⁹ Deputy Secretary of Defense, "Establishment of the Joint Artificial Intelligence Center", **1010 Defence Pentagon**, Washington, Haziran 2018.

¹³⁰ Arjun Kharpal, "China is Building a Giant \$2,1 Billion Research Park Dedicated to Developing AI", 03.06.2018, (Çevrimiçi) <https://www.cnbc.com/2018/01/03/china-is-building-a-giant-2-point-1-billion-ai-research-park.html>, (Erişim Tarihi: 02.07.2020).

¹³¹ Ashwin Kaja ve Yan Luo, "Covington Artificial Intelligence Update: China's Vision for the Next Generation of AI", 03.2018, (Çevrimiçi) <https://www.insideprivacy.com/artificial-intelligence/chinas-vision-for-the-next-generation-of-ai/>, (Erişim Tarihi: 03.10.2019).

Bunlara karşılık dünyada yapay zekâ alanında üçüncü büyük aktör olan AB, 2020 yılına kadar yapay zekâ alanına 1,5 milyar Euro yatırım yapılacağını bildirmiştir.

1.6.3. Yapay Zekânın Geleceği

Yapay zekânın geleceği hakkında tüm alanlarının yakın gelecekte birleşeceği konusundan öngörüler mevcuttur. Siberetik yaklaşımlar çerçevesinde yapay zekânın en azından teorik açıdan insan zekâsı kadar akıllı olabileceği düşünülmektedir¹³². Bu gelişmeler yapay zekânın insan zekâsına daha çok benzemesine olanak sağlamaktadır. Ancak bu alanda yapılması, düşünülmesi, dengelenmesi gereken, etik soruları gibi çok geniş sorunlar vardır ve mühendisler ile sosyal bilimler alanındaki uzmanların beraber çözmelerini beklemektedir. Yapay zekâ tabanlı sistemler tamamen sanal bir dünyada (örneğin, ses asistanları, görüntü analiz yazılımı, arama motorları, konuşma ve yüz tanıma sistemleri) işlem gören yazılım olabildiği gibi

Yapay zekâ cihazlarında (örneğin, gelişmiş robotlar, otonom arabalar, dronlar veya Nesnelerin İnterneti uygulamaları) da yerleştirilebilir¹³³. Yapay zekâ sayesinde bilgisayarlar, araba kullanmak veya satranç oynamak gibi insan davranışlarını taklit etmekte, bu sayede problem çözmekte ve nihayetinde bu işlemleri insanlardan daha hızlı ve daha iyi yapar hale gelmektedir.¹³⁴ Bütün bunlar çalışmanın konusu olan veriler daha doğrusu kişisel veriler ile beslenen yapay zekâ uygulamaları aracılığıyla gerçekleşmektedir. Özetle, verilerin ve/veya kişisel verilerin yapay zekâ çağında yeniden değer kazanmaya başlamış ve petrol haline gelmiştir. Bu durum yapay zekâ tekniklerinin özelliklerinden, özellikle veriden beslenme eğiliminden kaynaklanmaktadır.

¹³²Copeland, **a.g.m.**, par. 5.

¹³³ AI HLEG, A Definition of AI..., **a.g.e.**, s. 3.

¹³⁴ Bak, **a.g.m.**, s. 212.

2. KİŞİSEL VERİ VE KARŞILAŞTIRMALI HUKUKTA KORUNMASI

Günümüzde yapay zekâ uygulamaları sayesinde büyük veri kullanarak anlamlı çıkarımlar ve sonuçların çıkarma yetenekleri artmıştır. Finansal işlemler, ekipman bakım kayıtları, tıbbi kayıtlar veya kredi uygulamaları içeren çok büyük kamusal veya ticari veri tabanlarından önemli olan verileri bulmak ve bu verilerden ya da bu verilerden türetilen çıkarımlara dayanarak öngörü ve önerilerde bulunmak yapay zekâ teknolojileri sayesinde olanaklı hale gelmiştir¹³⁵.

Yapay zekâ yöntem ve yapıları açısından çok fazla veriye ihtiyaç duyduğundan, gerçek kişisel hakkından giderek fazla veri toplama eğilimdedir. Bu açıdan bakıldığında kişisel veriler ve yapay zekâ iki yönlü ilişki içinde olduğu söylenebilir: bir taraftan kişisel verileri yapay zekâ algoritmalarını besler ve geliştirir. Gündelik hayatımıza kolaylıklar sağlamış olur. Öbür taraftan ise yapay zekâ algoritmaları kişisel verileri kullanarak daha fazla kişisel veri üretebilir¹³⁶. Bu kişisel verileri çıkarımlar aracılığıyla ortaya çıkabilir.

Yapay zekâ çoğu durumda ırk, etnik köken, cinsiyet ve diğer hassas nitelikler hakkındaki veriler dahil olmak üzere geniş kapsamlı verilere erişim sağlıyor. Bu nedenle yapay zekânın potansiyel gücü, algoritmaları ve makine öğrenme modellerini etkin bir şekilde geliştirmek için gereken veri hacmi ile ilgili yasal endişeler ortaya çıkmaktadır¹³⁷.

¹³⁵ Murat Volkan Dülger, “Yapay Zekâ Teknolojileri ve Veri Koruma Hukuku”, Academia, 2019, (Çevrimiçi) https://www.academia.edu/40471926/Yapay_Zeka_Teknolojileri_ve_Veri_Koruma_Hukuku, (Erişim Tarihi: 02.07.2020), s. 4.

¹³⁶ Mitrou, **a.g.m.**, s. 21.

¹³⁷ Mihalis Kritikos, **Artificial Intelligence Ante Portas: Legal & Ethical Reflections**, Brussel: EPRS | European Parliamentary Research Service, 2019, s. 4.

Yapay zekânın verileri analiz etme ve kullanıcıları belirleme yeteneği daha önce yeterince önemli olduğunu kanıtlanmayan verilerin hassasiyetini artırmış durumundadır. Gizliliğin korunmasına yönelik büyük veri analizini sağlayan anonimleştirme tekniklerinin kademeli olarak gelişmesine rağmen, yapay zekâ insanların kendi görüşlerini oluşturma ve özerk kararlar alma hakkı konusunda artan bir tehdit oluşturmaktadır¹³⁸.

Örneğin, Edward Snowden 2013 yılında ifşa eden mahremiyet ihlalleri olayında başta Google, Facebook, Apple ve başka dev firmaların milyonlarca kullanıcıya ait olan kişisel verilerin Ulusal Güvenlik Ajansı'nın (National Security Agency-NSA) gözetiminde olduğu ortaya çıkmıştır. Bu mahremiyet ihlali gelişmeleri Avrupa Birliği Adalet Divanı'nın (ABAD) mevcut hukuki uygulamalar kapsamında önemli bir değişim yaklaşımı sergilemesine sebep olmuştur. Sonuç olarak, Avrupa'da bireysel hakların korunmasına ilişkin genel anlayış da değişmiş ve ABAD bu çerçevede bir dizi karar almıştır¹³⁹. ABAD bu olaylardan sonra kişisel verilerin korunması konusunda devrim nitelikli bazı önemli kararlar vermiştir.

Yapay zekânın en çok kullanıldığı alanlardan biri olan robot uygulamaları daha somut bir şekilde kişisel veriler ile olan ilişkisini açıklayabilir. Akıllı robotlardan doğabilecek hukuki sorunların başında mahremiyet hakları gelmektedir. Günümüzde yapay zekâ kullanımlı akıllı robotlar çevrelerindeki durumu sensörleri ile algılayıp, izleyip ve kaydedebilmektedir. Akıllı robotlar, insanların giremeyeceği yerlere girebilmekte, insanların göremediği yerleri görebilmektedir. Bu açıdan akıllı robotlar çok kolay bir şekilde gözetleme amacıyla kullanılabilir¹⁴⁰.

¹³⁸ a.g.e., s. 5.

¹³⁹ Ayşe Nur Akıncı, **Avrupa Birliği Genel Veri Koruma Tüzüğü'nün Getirdiği Yenilikler ve Türk Hukuku Bakımından Değerlendirilmesi**, Ankara: T.C. Kalkınma Bakanlığı, 2017, s. 11.

¹⁴⁰ Patrick Lin vd., **Robot Ethics, the Ethical and Social Implications of Robotics**, The MIT Press, 2011, s. 2.

Örneğin, evde kullanılan bir akıllı robot, o evde yaşayan kişiler ile ilgili dışarıya bilgi aktarmak amacıyla programlanabilir. Bu durumda evde kullanılan bir akıllı robotun hackerler tarafından saldırıya uğraması durumunda, hackerlerin ulaştığı sadece klasörler ve belgelerle kalmayıp doğrudan evin içindeki kişiler ve evdeki nesneler olacaktır¹⁴¹. Bu tür endişeleri gidermek için yapay zekâ çağında kişisel verilerin korunması konusuna odaklanmamız gerekmektedir. Fakat kişisel verileri koruma düzenlemeleri incelemiden önce kişisel veri kavramı ve tarihsel gelişimini kısaca ele almamız isabetli olacaktır.

2.1. Kişisel Veri Kavramı

2.1.1. Tanımı

Ulusal ve uluslararası düzenlemelerde yer alan kişisel veri (kimseye göre de enformasyon mahremiyeti) kavramına değinmeden önce kavramsal açıklamaların yapılması gerekmektedir. Kişisel veri (Personal Data) ifadesinden kişiye ilişkin veriler anlaşılmalı birlikte, veri kavramının açıklanmasını gerektirmektedir. Kaynağını aldığı Latince’de “Datum, Dati” olarak kullanılan bu kavram, İngilizce’ye “debit”, “that which is a given” şeklinde çevrilmiştir. Daha sonra, İngilizcede “datum” ve “data” olarak kullanılmaya başlanmıştır¹⁴². Kelime anlamı olarak datum, “bilginin bir parçası”; data ise, “referans veya analiz için bir araya toplanmış olgular ve istatistikler” şeklinde ifade edilebilir.

Kişisel verilere dair hem öğretilerde hem de mevzuatta yapılmış çeşitli tanımlara rastlamak mümkündür. OECD’nın 1980 tarihli ilkelerin 1/b maddesi, Avrupa Konseyi “108 Sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi (108 Sayılı Sözleşme)” 2/a maddesi ve “95/46/AT Sayılı

¹⁴¹ Patrick Lin vd., **a.g.e.**, s. 3.

¹⁴² Sertaç Öğüt, “Veri Madenciliği Kavramı ve Gelişim Süreci”, (Çevrimiçi), http://www.sertacogut.com/blog/wpcontent/uploads/2009/03/sertac_ogut_veri_madenciligi_kavrami_ve_gelisim_sureci.pdf, (Erişim Tarihi: 16.12.2020), s. 1.

Kişisel Verilerin işlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Direktifi (95/46/AT Sayılı Direktif)” in 2/a maddeleri kişisel verilere dair bu alanda yapılmış ilk tanımlamalar niteliğindedir.

OECD’nin 1980 senesinde yaptığı tanımı şu şekildedir: “*Kişisel veri, belirli veya belirlenebilir bir kişiye ait herhangi bilgi anlamına gelir*”¹⁴³

Avrupa Konseyi Sözleşmesi’nde benzer bir ifadeyle kişisel nitelikteki veriler şu şekilde nitelendirilmiştir: “*Kimliği belirtilen veya belirtilebilen gerçek kişiyle ilgili tüm bilgileri ifade eder*”¹⁴⁴.

95/46/AT Sayılı Direktifte de ise kişisel veri daha detaylı olarak şu şekilde tanımlanmıştır:

“Fiziksel, fizyolojik, zihinsel, ekonomik, kültürel veya sosyal kimliğine özel bir veya daha fazla faktöre veya bir kimlik numarasına atıf başta olmak üzere doğrudan veya dolaylı olarak tespit edilebilen bir tespit edilebilir kişi; tespit edilmiş veya tespit edilebilir gerçek kişiye (veri öznesi) ilişkin herhangi bir bilgiyi kastedecektir”¹⁴⁵.

AB çerçevesinde Nisan 2016 tarihinde onaylanan “Genel Veri Koruma Tüzüğü (GDPR)” madde 4’te kişisel verileri 95/46/AT Sayılı Direktife benze şekilde tanımlamıştır:

“‘kişisel veri’ tanımlanmış veya tanımlanabilir bir gerçek kişiye ilişkin her türlü bilgidir (‘veri sahibi’); tanımlanmış bir gerçek kişi özellikle bir isim, kimlik numarası, konum verileri, çevrim içi tanımlayıcı ya da söz konusu kişinin fiziksel, fizyolojik, genetik, ruhsal,

¹⁴³ OECD, Özel Yaşamın Korunması ve Kişisel Verilerin Sınır ötesi Akışına İlişkin Rehber İlkeleri, 1980.

¹⁴⁴ Avrupa Konseyi, “108 Sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi”, m. 2.

¹⁴⁵ 95/46/AT Sayılı Direktifte, m. 2.

ekonomik, kültürel veya toplumsal kimliğine özgü bir ya da daha fazla sayıda faktöre atıfta bulunularak doğrudan veya dolaylı olarak tanımlanabilen bir kişidir”

ABD’de bir bireye ilişkin bilgilere tipik olarak “*kişisel veri*” yerine “*kişisel bilgi*” kavramı tercih edilmektedir. Yani “*personal data*” yerine “*personal information*” kavramı kullanılıyor. ABD’deki kişisel bilgilerin tanımı tüm eyaletlerde veya tüm düzenlemelerde aynı içerikte değildir. Ayrıca, belirli veriler bir amaç için kişisel bilgi olarak kabul edilirken, başka bir amaç için kişisel bilgi sayılmayabilmekte. ABD “Kaliforniya Tüketici Gizliliği Yasası” (CCPA) kişisel bilgileri şu şekilde tanımlamıştır:

“Belirli bir tüketici veya vatandaşı doğrudan veya dolaylı olarak tanımlayan, bunlarla ilgili, açıklayan, ilişkilendirilebilen veya makul şekilde bağlanabilen bilgiler”

Avrupa’da kişisel verilerin işlenmesini düzenleyen politika grubunun tanımlamasın ve Almanca “*datenschutz*” kelimesinden tercüme edilen kullanım ise veri koruması şeklindedir. Anglo-Sakson coğrafyasında veri koruma hukuku ile ilgili düzenlemelerde “mahremiyet” şeklinde kullanılmaktadır¹⁴⁶.

Çin’de “Kişisel Bilgi Güvenlik Kodu”na (Personal Information Security Specification) göre:

“Kişisel bilgi, elektronik veya başka şekilde tek başına veya diğer bilgilerle birlikte kullanılıp,

1) belirli bir gerçek kişinin kimliğini tanımlayabilen veya

¹⁴⁶ İkbâl Gür, **Kişisel Verilerin Korunması Hususunda AB ile ABD Arasında Çıkan Uyuşmazlıklar ve Çözüm Yolları**, Ankara: Turhan Kitabevi, 2010, s. 3.

2) belirli bir gerçek kişinin faaliyetlerini yansıtabilen her türlü bilgiyi ifade eder”¹⁴⁷.

“Kişisel Bilgi Güvenliği Kodu” uyarınca, kişisel bilginin bir kişiyi özel olarak tanımlanması gerekmez, sadece bir kişinin faaliyetlerini yansıtmaya yeterlidir ve o kişinin kişisel bilgisi niteliği kazanacaktır. Örneğin, tanımlanan bireyin kişisel bilgileri ilgili kişinin GPS konumunu, arama geçmişini içerir. Ancak “Çin Siber Güvenlik Kanunu (Cybersecurity Law of the People’s Republic of China)” (CLPRC) kapsamındaki kişisel bilgi tanımı sadece bireyleri tanımlamak için kullanılabilecek bilgilerle sınırlanmıştır. Kısacası Çin’de kişisel bilgi kavramının içeriği doktrinde de uygulamada da net şekilde belirlenmemiştir. Bunun sebebinin Çin’in kendine özgü yönetim kültürü ile açıklamak mümkündür. Nitekim düzenlemelerin kavramsal çerçeve açısından muğlak bırakılması, daha sonraki uygulama da iktidarın menfaati üzerine farklı şekillerde yorumlanabilmesi için yol açmaktadır.

Türkiye’de 6698 sayılı “Kişisel Verilerin Korunması Kanunu” (KVKK) uyarınca, “kimliği belirli yahut belirlenebilir olan bir gerçek kişiye ilişkin her türlü bilgi kişisel veri” niteliğinde değerlendirilecektir. Ayrıca kişinin sadece kendi şahsi ile ilgili olan verilerle sınırlı olmayıp, aynı zamanda ailesine ilişkili bilgileri de kişisel veriler kapsamında değerlendirilmektedir¹⁴⁸. Bu doğrultuda öğretilde kişisel veri “*bireylerin şahsi, mesleki ve ailesine ilgili özelliklerini gösteren, söz konusu bireyi diğer bireylerden ayırmayı ve niteliklerini ortaya koymayı sağlayabilen her türlü veri*” şeklinde tanımlanabilmekte¹⁴⁹.

Yukarıda belirtilen düzenlemeleri karşılaştırdığımızda Tablo 4’teki şekilde olmaktadır. Bu açıklamalar doğrultusunda bir kişinin sadece özel yaşamı ile ilgili değil,

¹⁴⁷ SAMR, “个人信息安全规范” (Information Security Technology Personal Information (PI) Security Specification), (Çevrimiçi) <https://www.tc260.org.cn/upload/2020-09-18/1600432872689070371.pdf>, (Erişim Tarihi: 15.12.2020).

¹⁴⁸ Akgül, Danıştay..., **a.g.e.**, s. 8.

¹⁴⁹ Sinan Sami Akkurt, “Kişisel Veri Kavramının Hukuki Niteliğine İlişkin Yaklaşımlara Mukayeseli Bir Bakış”, **Kişisel Verileri Koruma Dergisi**, C. 2, S. 1 (2020), s.21.

ekonomik ve mesleki bilgileri de dahil bütün bilgilerini içeren kişisel veri, kimliği belirli bir gerçek kişiye ait olan ya da bir gerçek kişinin belirlenmesine yardımcı olan her türlü bilgiler şeklinde açıklanabilir¹⁵⁰. Bu anlamda kişinin fiziksel özellikleri, parmak izi, resmi, görüntü kaydı, öğrenim durumu, kimlik bilgileri, etnik kökeni, mesleği, dini inancı, banka hesap bilgileri, kullandığı bilgisayarın IP adresi gibi durumlar kişisel veri olarak nitelendirilebilir¹⁵¹. Tabloda görüldüğü üzere, farklı düzenlemelerde kullanılan sözcükler farklı olmasına rağmen, içerik olarak benzediği görülmektedir.

Tablo 4: Mukayeseli Hukuktaki Kişisel Verilerin Tanımı

Düzenleyici	Mevzuat	Kişisel Veri Tanımı İçeriği
AB	GDPR	• Tanımlanmış veya tanımlanabilir • Bir gerçek kişiye ilişkin • Her türlü bilgi
ABD	CCPA	• Belirli bir tüketici veya vatandaşı • Doğrudan veya dolaylı • Tanımlayan, açıklayan, ilişkilendirilebilen, bağlanabilen bilgi
Çin	CLPRC	• Elektronik veya başka şekilde • Tek başına veya diğer bilgilerle birlikte • Belirli bir gerçek kişinin kimliğini tanımlayabilen veya faaliyetlerini yansıtabilen

¹⁵⁰ Cynthia R. Farina, Sidney A. Shapiro ve Thomas M. Susman, **Administrative Law of the EU: Transparency and Data Protection (Administrative Law of the European Union)**, American Bar Association, 2009, s. 139.

¹⁵¹ Mustafa Topaloğlu, **Bilişim Hukuku**, Ankara: Karahan Yayınevi, 2005, s. 163.

		• Her türlü bilgi
Türkiye	KVKK	• Kimliği belirli yahut belirlenebilir • Bir gerçek kişiye ilişkin • Her türlü bilgi

Yukarıdaki kişisel veri tanımına göre, kişisel veri kavramının üç temel unsuru içerdiği söylenebilir: bilgi, kişiye ilişkin ve kimliği belirli veya belirlenebilir bir kişi. Bu üç unsur, Madde 29 Çalışma Grubu¹⁵² tarafından yayımlanmış olan kişisel veri kavramına ilişkin belirsizlik ve yaklaşım farklılığını bertaraf etmek amacı taşıyan görüş metninde de yer almaktadır¹⁵³.

Kişisel verilerden bahsederken hassas veri kavramını da kısaca açıklamamız gerekmektedir. Hassas verileri, genel anlamıyla ifşa edildiği zaman ilgili kişinin toplumdaki yerini ve diğer insanların ilgili kişiye olan bakış açısını değiştirebilecek veriler şeklinde tanımlanabilir¹⁵⁴. İlgili kişi, hassas verilerin ifşa edilmesi durumunda toplum tarafından ötekileştirme, ayrımcılığa maruz kalma riski ile karşı karşıya kalabilecektir. Örneğin, kişinin inançları, politik düşüncelerini, cinsel yaşam biçimi,

¹⁵² Madde 29 Çalışma Grubu, tam adıyla “Kişisel Verilerin İşlenmesine İlişkin Bireylerin Korunması Hakkında Çalışma Grubu” 95/46/AT Sayılı Direktifin 29. Maddesine dayanarak kurulmuştur. 25 Mayıs 2018 tarihine kadar (GDPR'nin uygulanmasına giriş) mahremiyetin ve kişisel verilerin korunmasına ilişkin konuları ele alan bağımsız bir Avrupa danışma grubu olarak devam etmiştir. Daha fazla bilgi için bkz: EDPB, “Article 29 Working Party”, (Çevrimiçi) https://edpb.europa.eu/our-work-tools/article-29-working-party_en (Erişim Tarihi: 26.02.2021).

¹⁵³ European Commission, Article 29 Working Party Opinion 4/2007 on the Concept of Personal Data, Brussels, 2007, (Çevrimiçi) <https://www.clinicalstudydatarequest.com/Documents/Privacy-European-guidance.pdf> (Erişim Tarihi: 26.02.2021), s. 6.

¹⁵⁴ Türkay HENKOĞLU, “Hassas Bilgi Varlıklarının ve Kişisel Verilerin Hukuksal Düzenlemeler ile Korunması ve Bu Kapsamda Üniversiteler İçin Bilgi Güvenliği Politikasının Geliştirilmesi”, (Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü Bilgi ve Belge Yönetimi Anabilim Dalı Yayınlanmamış Doktora Tezi), Ankara, 2015, s. 18.

etnik kökeni vb. veriler, ilgili kişinin sosyal ilişkilerindeki standartları değiştirme riski taşımakta ve bu nedenle “hassas veri” kategorisinde değerlendirilmektedir¹⁵⁵.

2.1.2. Kişisel Veri Kavramının Unsurları

2.1.2.1. Bilgi

Kişisel veri koruma ile ilgili mevzuatlarda bilgi, kişisel verilerin unsurları arasından ilk sırada gelmektedir. Bilgi, GDPR, CCPA, CLPRC, KVKK ve Madde 29 Çalışma Grubu tarafından yayımlanan Rapor’da ilk unsur olarak değerlendirilmiştir. Fakat günümüzde bilgi ile İngilizce “*Information*” olarak ifade edilen “*enformasyon*” arasındaki fark dikkat edilmeden karmaşık kullanılmaktadır. Sayılan kavramlar arasındaki ilişki ve farklılık, sadece veri koruma hukuku bakımında değil, bilgi toplumu süreçlerinin açıklanması bakımından da farklı disiplinlerce tartışılan bir konudur¹⁵⁶.

Öğretide “*veri (data)*”, “*enformasyon (information)*” ve “*bilgi (knowledge)*” sözcükleri arasındaki ilişki ve bunların birbirleri yerine kullanımları tartışmalı bir alan oluşturmaktadır¹⁵⁷. Bazı yazarlar bu üç terimin birbirlerinin yerine geçiyormuş gibi kullanımının önemli bir hata oluşturduğuna, deyimler arasında farklılık bulunduğuna işaret etmektedir¹⁵⁸.

Veriyi, bilgi işleme sürecinin temel yakıtı olarak, çeşitli işaretler, harfler, semboller yahut rakamlar ile temsil edilen, işlenmemiş gerçekler ya da izlenimler olarak tanımlayan yazarlar¹⁵⁹; enformasyonu ise verilerin, karar alma sürecine destek olacak şekilde anlamlı bir biçime getirilerek, işlenmesiyle ulaşılan sonuçlar şeklinde

¹⁵⁵ Cemil Kaya, “Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi”, **İÜHFM Dergisi**, 2011, s. 318.

¹⁵⁶ Şehriban İpek Aşıkoğlu, **Avrupa Birliği ve Türk Hukukunda Kişisel Verilerin Korunması ve Büyük Veri**, İstanbul: On İki Levha Yayıncılık, 2018, s. 6.

¹⁵⁷ Anthony Liew, “Understanding Data, Information, Knowledge and Their Inter-Relationships”, **Journal of Knowledge Management Practice**, 2007, s. 5.

¹⁵⁸ Türksel Kaya Bensghir, **Bilgi Teknolojileri ve Örgütsel Değişim**, Ankara: Todaie, 1996.

¹⁵⁹ Âdem Öğüt, **Bilgi Çağında Yönetim**, Ankara: Nobel Yayın Dağıtım, 2001. s. 11.

kabul etmektedirler¹⁶⁰. Bilgi kavramı ise verilerin çeşitli analiz, sınıflandırma işlemlerinde geçirilerek, ileride özel bir amaç ile kullanmaya yönelik olarak kullanılmaya hazır hale getirilmiş enformasyonu tanımlamak için kullanılmaktadır. Bir başka deyişle, bilgi, “*anlamalı bir biçime sokularak, kullanıcıya güncel ve olası kararların alınmasında yardımcı olan veri*” şeklinde tanımlanmaktadır¹⁶¹. AB, Türkiye bu açıdan daha çok veri sözcüğünü, AB ile Çin daha çok “bilgi” sözcüğünü tercih etmiştir. Fakat buradaki bilgi İngilizcedeki “*knowledge*” değil “*information*” ile eşdeğerdir.

Kişisel verilerin korunmasına ilişkin düzenleyici metinlerde yer alan kişisel veri tanımı uyarınca içeriğinden bağımsız olarak, bir kişiye ilişkin her türlü veri kişisel veri niteliği taşımaktadır. “Her türlü veri” ifadesi kanun koyucular tarafından bilerek ve kişisel veri kapsamının geniş yorumlanmasına olanak sağlayacak şekilde kasıtlı olarak tercih edilmektedir¹⁶². Nitekim günümüzde yapay zekâ gibi ileri teknolojilerin kişisel veri çerçevesini geniş yorumlamaya zorladığı belirtilmektedir.

2.1.2.2. Belirli veya Belirlenebilir Kişi

Genel anlamda bir kişinin kimliğinin belirlenebilmesi için en yaygın kullanılan usul ad ve soyadının tespittir. Yapay zekâ teknolojileri sayesinde ilgili kişiye ait başka veriler de bu kişiyi, içinde bulunduğu bir topluluğun diğer üyelerinden ayırt edilmesini sağlayabilmektedir.

Bir kişiyi doğrudan işlediğiniz bilgilerden tanımak mümkünse, bu bilgi direk kişisel veriler niteliği kazanır. Bir kişi bu bilgilerden doğrudan tanımlanamıyorsa, o kişinin hala tanımlanabilir olup olmadığını düşünmemiz gerekir. İşlediğimiz verileri başka herhangi bir kişi tarafından bu bireyin kimliğini tespit etmek için kullanılması

¹⁶⁰ Aşkoğlu, **a.g.e.**, s. 6.

¹⁶¹ Levent Kurt, **Açıklamalı- İçtihatlı Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması**, Ankara: Seçkin, 2005, s. 38.

¹⁶² Aşkoğlu, **a.g.e.**, s. 7.

makul olarak olası tüm yollarla birlikte dikkate alınması gerekiyor. Bu noktada yapay zekâ ile kişisel veriler kesişmektedir. Eskiden insan zekâsı veya basit algoritmalar aracı yolu ile bir bilgi ile birini tanımlayamıyorsa, bugünkü yapay zekâ algoritmaları yardımıyla hiç alakası yok görünen veri ile bir kişiyi tanımak tamamen mümkün olmaktadır. Doğal olarak belirli ya da belirlenebilirlik kavramı yapay zekâ uygulaması altında yeniden yorumlanması gerekmektedir.

Örneğin, IP adreslerinin kişisel veri niteliğinde olup olmadığı AB çerçevesinde tartışılmıştır. ABAD Scarlett Extended kararında IP adresine dayalı olarak kişinin kim olduğunun tespitinin mümkün olmadığını belirterek IP adresinin kişisel veri niteliğinde olmadığına karar vermişti¹⁶³. Daha sonra Breyer kararında IP adresini elinde bulunduran birinin makul imkanlar dahilinde kişiye dair bilgi etme imkânı söz konusu olduğu takdirde IP adresinin kişisel veri niteliğinde değerlendireceğine karar vermiştir¹⁶⁴.

Aynı şekilde ABAD farklı kararlarda muhtelif verilerin kişisel veri niteliği taşıdığını da ileri sürmüştür. Örneğin: parmak izi¹⁶⁵, vergi beyannamesi¹⁶⁶, kaydedilen kamera resim¹⁶⁷, mesai saat¹⁶⁸ın kişisel veri niteliğinde olduğuna karar vermiştir. Her gün ilerleme sağlayan yapay zekâ teknolojisi karşısında, mukayeseli düzenlemeler ilgili çerçeveleri düzenlemesi, genişletmesi yeni denge noktalarını bulması gerekmektedir.

2.1.2.3. Bilginin Kişiye ilişkin Olması

Genelde ilgili kişi ile kişisel veri arasındaki bağlantı kolaylıkla kurulabilmektedir. Ancak bazen verinin nesne ile ilgili olması durumunda kişi ile

¹⁶³ ABAD, C- 70/10, Scarlett, 11.24.2011.

¹⁶⁴ ABAD, C- 582/14, Breyer, 19.10.2016.

¹⁶⁵ ABAD, C- 291/12, Schwartz, 17.10.2014.

¹⁶⁶ ABAD, C- 201/14, Bara, 01.10.2015.

¹⁶⁷ ABAD, C- 212/13, Rynes, 11.12.2014.

¹⁶⁸ ABAD, C- 342/12, Worten, 30.05.2013.

dolaylı bir bağlantısı olabileceği söz konusu olur. Yapay zekâ çağında sorun oluşturmaya başlayan noktalardan biri dolaylı şekilde ilgili kişiye ilişkin olan bilgilerdir. Fakat kişiye herhangi bir şekilde ilgili olmayan ve ilişki kurulamayan bilgilerin kişisel veri kapsamında değerlendirilmesi imkânsız görülmektedir.

2.1.3. Kişisel Veri Türleri

Daha önce bahsedildiği üzere, AB ve ABD mevzuatı veya sözleşmelerinde “kişisel veri” ve “kişiyi tanımlayan bilgi” şeklinde farklı termi kullanılmaktadır. Bu iki hukuk sisteminin farklılığından kaynaklanıyor diyebiliriz. Bu başlıktaki kişisel veri, geniş anlamli olup ABD hukuk düzeninde kullanılan “kişiyi tanımlayan bilgiyi” de içermektedir. GDPR’a göre kişisel veri belirle ya da belirlenebilir bir bireye ilişkin her türlü veridir. İsim, adres, doğum tarihi, kalıcı olan bir kişiye özgülenmiş şirket dahili numarası, şifrelenmiş veya kısmen anonimleştirme işlemi yapılan veriler örnek olarak sayılabilir. GDPR’daki geniş kapsamlı kişisel veri terimine karşı olarak ABD’de yaygın olarak kullanılan termi “kişiyi tanımlayan bilgi” dir. “Kaliforniya Medeni Kanun” nda kişiyi tanımlayan bilgi belli bir oranda daraltılarak, amaca uygun şekilde ayarlanmıştır. Bu açıdan Medeni Hukukun düzenlediği alanlar ise genellikle hassas veri türlerini içermektedir¹⁶⁹. Fakat CCPA, GDPR’dan daha geniş kapsamlı bir şekilde kişiyi tanımlayan bilgi tanımı kabul etmiştir diyebiliriz.

2.1.3.1. Hassas Kişisel Veri

GDPR’a göre işlendiğinde kısıtlamalara tabii olan hassas veriler şunlardır: siyasi görüşler, sendika üyeliği, tıbbi veya sağlık durumu, ırk veya etnik kökeni, dini veya felsefi inançlar, cinsel yönelimi, belirli türdeki ceza kayıtları. Bu tür veriler, doğaları gereği, işlenecek ilgili kişiler için bir tehdit oluşturabilir denmiştir. Bu nedenle, özel kategoride sayılabilecek olan hassas verilere ilişkin fazladan korumaya gerek

¹⁶⁹ Lothar Determann, **Kişisel Verilerin Korunması Uygulama Kılavuzu**, Çeviren: Hilal Temel, 1.b., İstanbul: On İki Levha Yayınları, 2020, s. 28.

duyularak bu tür verilerin işlenmesi özel rıza ve şartlara bağlanmıştır¹⁷⁰. GDPR’da hassas verilerin işlenmesi, aktarılması durumunda ilgili kişiden açık rıza alınması gerekmektedir.

KVKK hassas veriler terimi yerine “özel nitelikli veriler” terimini benimsemiştir. KVKK’un “Özel Nitelikli Kişisel Veriler” başlığını taşıyan 6. maddesinin 1. fıkrası hükmü gereğince, şu veriler “özel nitelikli kişisel veri” olarak adlandırılır:

“Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir”¹⁷¹.

Genel olarak bakıldığında, uluslararası belgeler ve öğretide, hassas veriler konusunda bir fikir birliği bulunmasa da eğer veriler, özel yaşam alanı ile ilgili olarak diğer kişilerin düşüncesini, fantezisini ve bilgilerini tespit etmesini sağlıyor ise, bu tür veriler hassas, özel nitelikli veri olarak adlandırılmaktadır¹⁷². Bu veri grubuna dahil edilen verilerin, yüksek risk faktörü olarak değerlendirilen “ayrımcılık tehlikesi” bulundurmaları, bu verilerin ortak özelliği olarak belirtilmektedir¹⁷³. Hassas kişisel verilerin içeriği karşılaştırmalı şekilde Tablo 5’te yer almaktadır:

¹⁷⁰ Council of Europe, Handbook on European Data Protection Law, European Union Agency for Fundamental Rights, 2014, s. 43.

¹⁷¹ Berat DUMAN, “Anayasa Hukukunda Kişisel Verilerin Korunması”, (S.Ü Sosyal Bilimler Enstitüsü Kamu Hukuku Ana Bilim Dalı Kamu Hukuku Bilim Dalı Yayınlanmamış Doktora Tezi), Konya, 2020, s. 65.

¹⁷² Bloustein, Edward J., “Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser”, **N.Y.U. L. Rev.** S. 962 (1964), s. 1023.

¹⁷³ Başalp, **a.g.e.**, s. 23.

Tablo 5: Karşılaştırmalı Olarak Hassas Kişisel Verilerin İçeriği

İlgili Düzenleme	Hassas Kişisel Veri/Özel Nitelikli Kişisel Veri İçeriği
95/46/AT Sayılı Direktif	• Irksal/etnik kökenleri açığa vuran kişisel veriler • Siyasi görüşleri, dini ya da diğer inançları açığa vuran kişisel veriler • Sağlık ya da cinsel yaşamla ilişkili kişisel bilgiler • Mahkumiyetler¹⁷⁴
GDPR	• Irk ya da etnik kökene ilişkin veriler • Siyasi görüşlere ilişkin veriler, dini veya felsefi inançlara ilişkin veriler • Gerçek kişilerin cinsel hayatı ya da cinsel eğilimine dair veriler • Sendika üyeliğinin gösterildiği kişisel veriler • Genetik veriler ile biyometrik veriler.
CCPA	• Gerçek ad, takma ad, posta adresi, • IP adresi, e-posta adresi, • Ehliyet numarası, sosyal güvenlik numarası, pasaport numarası veya diğer benzer tanımlayıcılar.
KVKK	• Kişilerin ırkı, etnik kökeni • Siyasî düşüncesi, felsefî inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti • Sağlığı, cinsel hayatı • Dernek, vakıf ya da sendika üyeliği, ceza mahkûmiyeti • Biyometrik ve genetik verileri.

¹⁷⁴ 108 Sayılı Sözleşme, m. 6.

Tablo 5’e bakıldığında, 95/46/AT Sayılı Direktif genetik ve biyometrik verileri içermediği halde GDPR’da hassas veriler kavramı genişletilip genetik ve biyometrik verileri kapsadığı görülmektedir. Günümüzde hassas veriler: yaşam hakkının korunması, bireyin seçimlerinin kamuoyuna karşı ve sosyal yönden lekelenmeme hakkı ile temelden ilişkili olması sebebiyle bu kavramsal genişleme olumlu karşılanmalıdır¹⁷⁵. Dahası yapay zekâ çağında hassas verilerin çerçevesi dinamik ve geniş yorumlanarak, ilgili kişinin temel insan hakları başta olmak üzere, başka hakları korunma altına alınması gerekmektedir. Özel nitelikli kişisel veriler, bulundukları ayrıcalıklı konum ve taşıdıkları risk nedeniyle daha nitelikli bir korumaya tabi tutulmuş ve işlenmesi GDPR’da belirtilen istisnalar dışında kesin surette yasaklanmıştır. Hassas kişisel veri konusunda örnek düzenleme sağlayan GDPR’da yer alan kişisel veri hassasiyeti ve nitelik hiyerarşisi Tablo 6’de yer almaktadır.

Tablo 6: GDPR Açısından Kişisel Veri Hassasiyeti Hiyerarşisi¹⁷⁶

Hassasiyeti	Veri tipi	Niteliği
1	Hassas kişisel veri	Özel nitelikli, kimliği belirli/belirlenebilir
2	Kişisel veri	Kimliği belirli/belirlenebilir
3	Takma isimlendirilen (kişisel) veriler ¹⁷⁷	Anahtar kullanımıyla kimliği belirli/belirlenebilir

¹⁷⁵ Rodota Stefano, “Data Protection As a Fundamental Right”, **Reinventing Data Protection**, der. Serge Gutwirth, Yves Poullet ve Paul De Hert, Springer Science Business Media, 2009, s. 78.

¹⁷⁶ Jan Smits, “Privacy in Europe”, Coursera, (Çevrimiçi) <https://www.coursera.org/learn/privacy-eu/home/info> (Erişim Tarihi:20.01.2021).

¹⁷⁷ GDPR’ın 3. maddede “kişisel verilerin ek bilgi kullanılmadan artık belirli bir veri konusuna atfedilemeyecek şekilde işlenmesi” olarak takma adlandırmayı tanımlamaktadır. Bir veri kümesini

4	Profilli (kişisel) veriler	Artık kimliği belli olmayan/tanımlanamayan
5	Anonimleştirilmiş (kişisel) veriler	Kimliği belirlenmemiş/belirlenemeyen
6	Kişi ile ilgisiz veriler	Artık bir kişiyle ilgisi yok

Yapay zekâ çağında klasik veri türleri ayrımı farklı bir değer kazanmaktadır. Gelişen algoritmalar sayesinde hassas kişisel verilerin kapsamı gittikçe genişlemekte olup, hangi bilgilerin gerçekten hassas bilgi niteliği taşımayacakları tartışılır. Çünkü yapay zekâ teknolojileri sayesinde nedensellik ilişkisinden fazla korelasyon çözümü ön plandadır. Dolayısıyla, klasik kategorileştirmede hiçbir hassas veri niteliği taşımayan bir bilgi, korelasyon sayesinde ilgili kişiye ilişkili en önemli hassas niteliğini ortaya çıkartabilir. Mesela Facebook kullanıcılarının yaptığı beğeni, yorumlar aracılığıyla, görünüşte hiç ilgisi yok gibi gözükken dini inanç, siyasi görüş, felsefi düşünceleri azıcık veri ile analiz edilip, algoritma aracılığıyla ortaya çıkartılabilir¹⁷⁸. Yapmamız gereken yapay zekâ çağındaki hassas kişisel verilerin çerçevesini netleştirerek, algoritmik kara kutu vasıtasıyla veri sızdırma olaylarının azaltılmasını, ilgili kişiye yönelik yapılan veri ihlallerinin durdurulmasını gerçekleştirmektir.

2.1.3.2. Hassas Olmayan Kişisel Veri

Hassas kişisel veriler, özellikleri ve ifşa edildiğinde ayrımcılık riski nedeniyle hassas kabul edilir. İlgili kişilerin kimliğinin tespitine yol açabilecek ancak hassas

takma ad yapmak için, “ek bilgiler” ayrı tutulmalı ve tanımlanmış veya tanımlanabilir bir kişiye atıfta bulunulmamasını sağlamak için teknik ve organizasyonel önlemlere tabi tutulmalıdır.

¹⁷⁸ Ben Tinker, “How Facebook ‘Likes’ Predict Race, Religion And Sexual Orientation”, CNN, 04.11.2018, (Çevrimiçi) <https://edition.cnn.com/2018/04/10/health/facebook-likes-psychographics/index.html>, (Erişim Tarihi: 17.12.2020), par. 4.

nitelik taşımayan veriler hassas olmayan veri olarak kabul edilecektir. Hassas olmayan kişisel veriler, 95/46/AT Sayılı Direktif, GDPR ve KVKK'daki özel hükümlere göre değil genel hukuka uygunluk sebepleri kapsamında işlenebilmekte¹⁷⁹ ve hassas verilere göre daha hafif olan düzenlemeye konu olmaktadır. İlgili düzenlemelerde özellikle hassas kişisel veri olduğu vurgulanmadığı müddetçe hassas olmayan kişisel veriler kastedilmektedir.

2.1.4. Kişisel Veri ve Mahremiyet

Günümüzde kişisel veri ile mahremiyet çok sık ilişkilendirilmektedir. Bu iki kavram arasında farklılıklar olduğu kadar, içerik bakımından benzemektedir. Kişisel verilerin korunma hakkı ile mahremiyet hakkı arasındaki ilişki ve farklılıkları anlamak yapay zekâ çağında kişisel verilerin nasıl korunması gerektiği soruya cevap aramada önem taşımaktadır.

2.1.4.1. Benzerlikler

İlk olarak, her iki hak konusu da tüzel kişilerle değil sadece gerçek kişilerle sınırlıdır. Mahremiyetin işlevi açısından, esas olarak bireyin özel yaşamının huzurunu korumaktır. Bu nedenle, mahremiyet konusu gerçek kişilerle sınırlı olmalı, tüzel kişilerin mahremiyet hakkı yoktur ve tüzel kişilerin sahip olduğu ticari sırlar mülkiyet haklarının içeriğidir. Kişisel veri açısından bakıldığında, tüzel kişinin verileri kişilik özelliklerine sahip değildir ve tüzel kişinin kişilik hakkıyla kişisel veri hakkından yararlanmaması gerekir. Bu nedenle tüzel kişinin veri ihlali fikri mülkiyet kanunu veya haksız rekabet yasağı ile korunmaktadır.

İkincisi, her ikisi de bireyin özel hayatı hakkındaki özerk kararını somutlaştırır. Kişisel veri ile ilgili haklar genellikle “verinin kaderini kendi tayin hakkı”

¹⁷⁹ Hayrunnisa Özdemir, **Elektronik Haberleşme Alanında kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması**, Ankara: Seçkin Yayınları, 2009, s. 134.

(informational self-determination right) olarak adlandırılıyor¹⁸⁰. Mahremiyet ise bireyin kendi hayatının belli kısmını başkalardan gizli tutabilme hakkıdır.

Üçüncüsü, ikisi nesnede kesişiyor. Mahremiyet ve kişisel veriler arasındaki ilişki şu şekildedir: bir yandan, açıklanmayan birçok kişisel verinin kendisi mahremiyet kategorisine aittir. Aslında pek çok kişisel veri, insanların dış dünyaya yayınlamak istemediği özel bilgilerdir, bireylerin başkalarının müdahale etmesini istemediği özel bir alandır. Ekonomik değeri olsun ya da olmasın, bu kişilik ilgisini yansıtır. Öte yandan, bazı mahremiyet koruma nesneleri de kişisel veri kategorisine aittir. Özellikle, dijital teknolojinin geliştirilmesinin birçok mahremiyet, kişisel iletişimin gizliliği ve hatta teknik işlem yoluyla sayısallaştırılabilen ve tanımlama özelliklerinden dolayı dahil edilebilecek konuşmaların mahremiyet gibi kişisel verilerin özelliklerine sahip olmasını sağladığına dikkat edilmelidir¹⁸¹.

Dördüncüsü, ikisi ihlalin sonuçları açısından rekabetçidir. Eş-rekabetçilik denilen kavram, failin belirli bir davranışı yürütmesinin aynı anda birden fazla hakkı ihlal edebileceği, böylece birden fazla hakkın ihlal edildiği ve sorumlu işbirliğinin meydana geldiği bir durum oluşturabileceği olgusunu ifade eder¹⁸². Özel niteliklere sahip kişisel veriler ifşa edildiğinde, mahremiyetin ihlalini de gerçekleştirebilir. Örneğin, kişisel tıbbi kayıtların ifşa edilmesi sadece mahremiyet haklarını değil, aynı zamanda kişisel veri haklarını da ihlal edecektir.

2.1.4.2. Farklılıklar

Birincisi, mahremiyet hakkı esas olarak manevi bir kişilik hakkıdır. Kullanılabilir olmasına rağmen mülk değeri çok belirgin değildir. Gizlilik esas olarak

¹⁸⁰ Margaret C. Jasper, **Privacy and the Internet: Your Expectations and Rights under the Law**, Oxford: Oxford University Press, 2009, s. 52.

¹⁸¹ Wang Liming, “论个人信息权的法律保护—以个人信息权与隐私权的界分为中心 (Kişisel Bilgi Haklarının Korunması- Kişisel Bilgi Hakları ve Gizlilik Hakları Arasındaki Ayrım)”, **Modern Law Science**, Vol. 35, S. 4 (Temmuz 2013), s. 65.

¹⁸² Wang Liming, Kişisel Bilgi,...**a.g.m.**, s. 68.

kişiliğin çıkarlarını yansıtır ve mahremiyet hakkının ihlali de çoğunlukla zihinsel hasara neden olur. Kişisel veri hakkı, kişilik çıkarlarını ve mülkiyet çıkarlarını doğaya entegre eden kapsamlı bir haktır ve hem manevi değeri hem de mülkiyet değerini içeren, tam manevi bir kişilik hakkı değildir¹⁸³. Özel hayatın gizliliği hakkı olumsuz ve savunmacı bir haktır. Hak ihlal edilmeden önce, birey aktif olarak hakkını kullanamaz. Ancak hak ihlal edildiğinde ihlal edenden sadece zararları ekarte etmelerini ve tazminatları tazmin etmelerini talep edebilir.

İkincisi, mahremiyet ifşa olduğunda artık mahremiyet sayılmayacağından dolayı aynı mahremiyet sadece bir kez ihlal edilebilir ve kurtarılamaz hale gelir. Fakat kişisel veriler tekrar tekrar kullanılabilir (örneğin, kimlik numarası sayısız kez kullanılabilir), kişisel verilerin zarar görmesi, neden olduğu hasar genellikle kurtarılabılır¹⁸⁴. Kişisel verilerin korunması korunmaya odaklanırken, mahremiyetin korunması ihlalden sonra kurtarmaya odaklanıyor. Mahremiyetin ihlali durumunda, ana çözüm yöntemi ahlaki tazminattır. Mahremiyetin korunması esas olarak yasal koruma yöntemini benimser; kişisel verilerin korunması ise çeşitli ve kapsamlıdır, özellikle de idari yollarla korunabilir¹⁸⁵.

Üçüncüsü, mahremiyet bilgi formu ile sınırlı değildir, aynı zamanda kişisel aktivitelere, kişisel özel hayata vb. yansıtılabilir ve kaydedilmesine gerek yoktur. Kişisel veriler sabit bir şekilde sunulmalıdır. Bu nedenle, kişisel verilerin genellikle dijital biçimde kaydedilmesi veya ifade edilmesi gerekir. Başka bir deyişle, kişisel veri kavramı “tanımlama”, yani bireyleri kişisel veri yoluyla “tanımlama” üzerine odaklanır¹⁸⁶. Ama günümüz teknolojileri sayesinde, özellikle yapay zekâ gibi uygulamalar vasıtasıyla, kişilerin normal günlük rutinleri de dahil olmak üzere

¹⁸³ James B. Rule ve Graham Greenleaf, **Global Privacy Protection**, Edward Elgar Publishing, 2010, s. 105.

¹⁸⁴ Wang Liming, Kişisel Bilgi, ...**a.g.m.**, s. 67.

¹⁸⁵ **a.g.m.**, s. 68.

¹⁸⁶ Philip Coppel, **Information Rights**, London: Sweet & Maxwell, 2004, s. 257.

otomatik yada yarıotomatik bir şekilde sayısallaştırılıp, kayedilebiliyor. Sonuçta mahremiyet içeriği kişisel veriye daha çok yaklaşmış olur.

Dördüncüsü, mahremiyetin içeriği temel olarak bireyin özel hayatının mahremiyetinin korunmasını, bireyin mahremiyetinin açıklanmamasını ve bireyin özel hayatının bağımsız kararını içerir. Kişisel veri hakkı, esas olarak kişisel verilerin kontrolü ve bağımsız kararına ilişkilidir.

2.2. Kişisel Veri Korunması Sorunu ve Tarihsel Gelişimi

Kişisel verilerin korunmasının asıl amacı, bireyin özel yaşamının gizliliğini korumaktır¹⁸⁷. Başka bir deyişle, kişisel verilerin korunması, başta mahremiyet hakkı olmak üzere insan onuru, ifade ve iletişim özgürlüğü gibi insan haklarıyla ilgili birçok hakla yakından ilgilidir¹⁸⁸. Kişisel verileri koruma hakkı, Avrupa’da temel bir insan hakkı olarak kabul edilir ve üye devletlerin anayasalarında temel bir insan hakkı olarak listelenmiştir. Örneğin, 1975 İsveç Anayasası, 1976 Portekiz Anayasası ve 1978 İspanya Anayasası, kişisel verileri koruma hakkını açıkça belirtmiştir¹⁸⁹.

2.2.1. Kişisel Veri Korunması Sorunu

Sır saklama ile ilgili ilk bilgi, “Hipokrat Yemini”nde yer almaktadır. Adı geçen yeminde sır saklamaya ilişkin olarak “*tedavi sırasında veya tedavi dışında insan hayatında görüp işittiklerim hakkında sessiz kalacağım ve bu tür şeyleri konuşmayacağım*” şeklinde ifadeye yer verilmiştir¹⁹⁰. Modern anlamda kişisel veri koruma düzenlemeleri ise ikinci dünya savaşından sonra ortaya çıkmıştır. Vatandaşlar ile ilgili olan verilerin savaş sırasında getirdiği zararlar düşünülerek, Avrupa’da kişisel verilerin korunması ihtiyacı ortaya çıkmıştır. Teknolojilerin ilerlemesi ile kişisel

¹⁸⁷ Antony Duff, Serge Gutwirth ve Erik Claes, **Privacy and the Criminal Law**, Intersentia: Antwerp, 2006, s. 77.

¹⁸⁸ Akgül, Kişisel Veri..., **a.g.m.**, s. 18.

¹⁸⁹ Akgül, Danıştay..., **a.g.e.**, s. 221.

¹⁹⁰ Maral Törenli Çakıroğlu, “Hekimin Borçlarından Özel Olarak Sır Saklama Borcu”, **Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi**, Cilt: 12, Sayı: 2, Yıl: 2010, s. 159.

verilerin korunma ihtiyacı ittikçe artmaktadır. Özellikle yapay zekâ çağında, teknolojileri besleyen gıda niteliğindeki veriler ekonomik açıdan değer kazanmıştır. Nitekim, yapay zekâ, vatandaşların kişisel verilerinin sayesinde ciddi bir artış ve daha hızlı bir ihlal oranı ile sonuçlanmıştır¹⁹¹. Sonuçta kişisel verilere yönelik yapılan veri ihlalleri karşısında veri koruma düzenlemeleri ortaya çıkmıştır.

Günümüzde kişisel verilerin korunması, kişisel veri niteliği taşıyan verilerin toplanması, saklanması, değiştirilmesi, silinmesi, ifşa edilmesi ve üçüncü bir kişiye aktarılması sürecinin amaç ve yöntemlerin belirlenmesi ve bunların aşılması halinde hükme bağlı kısıtlamalar ve yasal çarelerin belirlenmesini ifade eder¹⁹². Yapay zekâ teknolojisi vatandaşlara sağladığı kolaylıklar ile beraber getirdikleri riskler ve problemler nedeniyle, kişisel veri koruma ihtiyacını ciddi bir şekilde arttırmıştır.

2.2.2. Kişisel Verilerin Korunması Tarihsel Gelişimi

Kişisel verilerin korunması hukuku bakımından atılan ilk adım 1970 yılında gerçekleşmiştir. İlk olarak 1970’te Federal Almanya’da bulunan Hessen eyaleti, verilerin korunması konusunda bir kanun kabul etmiştir. Bu kanunun eyalet seviyesinde kabul edilmesiyle birlikte federal düzeyde tartışmalar başlamış. Bu gelişmenin akabinde, 1977 yılında, Almanya’da “Veri Koruma Yasası” kabul edilmiştir. Bununla eşzaman olarak, ulusal düzeyde veri koruma kanununu kabul eden ilk devlet 1973 yılında İsveç olmuştur¹⁹³. ABD 1974’te kişisel verilerin korunmasına ilişkin yasa ve yönetmelikleri ortaya çıkarmıştır¹⁹⁴.

¹⁹¹ Hu Zhiling, “人工智能时代公民个人信息的保护-以全国首例利用 AI 实施的特大侵犯公民个人信息案为视角 (Yapay Zekâ Çağında Vatandaşların Kişisel Bilgilerinin Korunması-Ülkenin İlk Yapay Zekâ Kullanımlı Kişisel Bilgi İhlali Hakkında)”, *Journal of Shanghai Police College*, 2019, s. 5.

¹⁹² Hüseyin Can Aksoy, **Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması**, Ankara: Çakmak Yayınevi, 2010, s. 1.

¹⁹³ DUMAN, **a.g.m.**, s. 10.

¹⁹⁴ Elif Küzeci, **Kişisel Verilerin Korunması**, Ankara: Turhan Kitabevi, 2010, s. 165.

Bu ulusal düzenlemelere paralel olarak OECD ve Avrupa Konseyi kişisel verilerin otomatik işlenmesi ile ilgili uluslararası düzenlemeler yapmıştır. Bu çerçevede uluslararası hukuk belgelerinde kişisel verilerin korunması hakkı kabul edilmiştir.

OECD tarafından 1980 yılında “Sınır Ötesi Veri Akışları Hakkında Yönlendirici İlkeler” belirlenmiştir. Fakat, OECD Yönetim Kurulunun bu konudaki tavsiye kararları ilgi görmemiş. Aynı konu 1981’de “Kişisel Veriler Hakkında Avrupa Konseyi Andlaşması” yapınca ciddiyet kazanmıştır¹⁹⁵. “Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşme” ise Avrupa Konseyi tarafından 1981 yılında imzaya açılmış ve 1985 yılında yürürlüğe girmiştir¹⁹⁶.

1990’larda internetin ortaya çıkmasıyla ortaya çıkan kapsamlı ağ bağlantıları, kişisel verilerin e-ticarete yaygın olarak kullanılmasını gerçekleştirmiştir. Sonuç olarak, önceden elde edilen uyum geçersiz kalmış ve farklı veri koruma düzenlemelerine sahip ülkeler arasında uyumsuzluklar ortaya çıkmıştır¹⁹⁷.

Veri güvenliği konusunun önem kazanması ve konunun yasal düzenlemeler ile güçlendirilmesinin temelindeki ilk ve en önemli unsur kuşkusuz insan hakları olmuştur. Her bireyin, kendisine özgü olan bilgileri üretme, saklama ve istediği kişiler ile paylaşma hakkı vardır. İnsan haklarından ve yaşanan teknolojik gelişmelerin doğurduğu sonuçlardan ve bilgi toplumunu oluşturan temellerden yola çıkarak OECD, Avrupa Konseyi ve BM tarafından oluşturulan ve ülkelerin yasal düzenlemelerine rehberlik etme niteliğine sahip yasal düzenlemeler yapılmıştır. Günümüze kadar yapılan kişisel verilerin korunmasına ilişkin düzenlemeler Tablo 7’de yer almaktadır:

¹⁹⁵ Tekin Akıllıoğlu, “İdari Usul ve Kişisel Verilerin Korunması”, 11.08.2014, (Çevrimiçi) <http://www.idare.gen.tr/akillioglu-idariusul.htm>, (Erişim Tarihi: 04.10.2019).

¹⁹⁶ Nurdan OKUR, “Anayasa Hukuku açısından Özel Hayatın Gizliliği ve Korunması”, (Gazi Üniversitesi Sosyal Bilimler Enstitüsü Yayınlanmamış Doktora Tezi), Ankara, 2010, s. 62.

¹⁹⁷ Nur, **a.g.e.**, s. 3.

Tablo 7: Kişisel Verilerin Korunmasına İlişkin Muhtelif Düzenlemeler¹⁹⁸

Tarih	Düzenleme
1953	İnsan Hakları ve Özgürlüklerin Korunmasına İlişkin Avrupa Sözleşmesi
1980	OECD “Özel Yaşamın Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkeleri”
1981	Avrupa Konseyi “108 Sayılı Sözleşmesi”
1990	BM “Bilgisayarla İşlenen Kişisel Veri Dosyalarına İlişkin Rehber İlkeleri”
1998	95/46/AT Sayılı Direktif
2001	“181 Sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi’ne Ek Denetleyici Makamlar ve Sınır aşan Veri Akışına İlişkin Protokol”
2016	Avrupa Birliği “Genel Veri Koruma Tüzüğü (GDPR)”

2.3. Kişisel Veri Koruma Yöntemleri

Kişisel verilerin korunması konusu daha çok teknolojinin ilerlemesi ile ortaya çıkmıştır. Daha öncesinde ise mahremiyet konuları tartışılmıştır. Mahremiyet menfaattarın ortaya çıkışı doğrudan rekabetle ilgili olmuştur, yani rekabet sürecinde

¹⁹⁸ KVKK, Kişisel Verilerin Korunması Kanunu ve Uygulaması, Ankara, 2017, s. 10.

münhasır bilgi menfaatlerinin peşinde koşarak ortaya çıkan toplum üyelerinin çıkar konusu olmuştur. Aynı zamanda rekabet amaçlarına ulaşabilme adına işbirlikçi sosyal gruplar da oluşmuştur. Sonuçta sosyal bir toplumda hem rekabet hem de iş birliği ortaya çıkmıştır. Mahremiyet hakları ise bir sosyal toplumdaki toplum üyelerinin yasal mahremiyet menfaatlerini korumayı amaçlayıp ortaya çıkmıştır¹⁹⁹.

Farklı sosyal toplumların oluşumu, gelişimi ve rekabet ortamının farklı olması nedeniyle, ABD ve Avrupa ülkeleri belirgin şekilde farklı mahremiyet kavramları ve sistem tasarımları oluşturmuştur. ABD aşağıdan yukarıya doğru zayıf bir mahremiyet koruma modeli geliştirmiştir ve sektörle yasa tasarım yollarıyla işlevselcilik özelliğini göstermiştir. Avrupa ülkeleri yukarıdan aşağıya güçlü bir mahremiyet koruma modeli ortaya çıkarmıştır. Yeknesaklaşmış mevzuatının doğasında ortaya çıkan, yukarıdan aşağıya düzenlenen koruma sistemler güçlü bir koruma modeli geliştirmiş ve doğal hakların özelliklerini benimsemiştir²⁰⁰.

Sonuçta dünya üzerindeki kişisel verileri koruma hukuk düzenlemelerine baktığımızda iki ana koruma yöntemi öne çıkmaktadır. Birincisi, “kapsamlı yasama” modeli olarak adlandırılabilir, ayrı bir kişisel veri koruma yasası formüle eden Kara-Avrupa yöntemi; ikincisi, kişisel verileri ayrı-ayrı yasama modeli ile koruma altına alan Anglo-Sakson yöntemidir.

2.3.1. Kara-Avrupa Koruma Yöntemi

Kara-Avrupa Hukuk Sisteminde kişisel veriler, temel insan hakları ve/veya bireysel haklar kapsamında sosyal ve insancıl yöntemlerle değerlendirilmektedir. Bu yöntemde kişisel veri kavramı anayasal anlamda insan hakları olarak tanımlansa da korunan değer aslında özel hayatın gizliliği olduğu görülebilmektedir. Özel hayatın

¹⁹⁹ Wu Weiguang, “从隐私利益的产生和本质来理解中国隐私权制度的特殊性 (Çin’in Mahremiyet Koruma Sisteminin Özelliklerini, Gizlilik Çıkarlarının Kaynağı ve Doğası Hakkında)”, 当代法学 (Contemporary Law Review), S. 4 (2017), s. 56-58.

²⁰⁰ a.g.m., s. 60.

gizliliği ise aynı zamanda medeni hukuk terminolojisinde yer alan kişilik hakkı kapsamındaki kişisel değerlerden biridir²⁰¹. Sağlık, aile hayatı, inançları ve özellikle ilgilinin rızası olmadan bu tür verilerin kullanımı yasa dışı kullanım kabul edilmektedir²⁰². Ancak her türlü kişisel verinin ilgili kişinin özel alanına dâhil olduğundan bahsedilmesi mümkün olmadığı için kişilerin bazen sakınmamaları veya rahat davranmaları onların mahremiyetten vazgeçtikleri anlamında sorun oluşturmaktadır²⁰³.

Kara-Avrupa ülkeleri genellikle “kişisel verilerin korunması” kavramını benimsemiştir. AB’nin 1995 yılındaki 95/46/AT Sayılı Direktifi, 2000 yılındaki “Topluluk Ajansı Kişisel Veri İşleme ve Akış Koruma Yönetmeliği”, 2002 yılındaki “Gizlilik ve Elektronik Haberleşme Direktifi” ve 1995 yılındaki üye Direktifi uyarınca “Alman Federal Veri Koruma Yasası” gibi kişisel veri koruma mevzuatı ve GDPR buna örnek olabilir.

AB hukuk modeli, birleşik bir kişisel veri koruma yasasının çıkarılması ile karakterize edilebilir. Bu nedenle birleşik model olarak da adlandırılır. AB çerçevesinde Almanya başta olmak üzere 20 den fazla ülkede yeknesak veri koruma kanunları yayımlanmıştır²⁰⁴. Günümüzde AB, Çin ve Türkiye birleşik bir kişisel veri koruma yöntemini tercih etmiş durumundadır. Nitekim ilgili mukayeseli düzenlemeler bunu göstermektedir.

2.3.2. Anglo-Sakson Koruma Yöntemi

Kara-Avrupanın birleşik kişisel veri koruma formülasyonundan farklı olarak, çeşitli endüstrilerde kişisel verilerin korunması için yasal kurallar ve kılavuz ilkelerin

²⁰¹ Hüseyin Hatemi, **Kişiler Hukuku**, İstanbul: On İki Levha, 2018, s. 66.

²⁰² Yeşim Çelik, “Özel Hayatın Gizliliğinin Yansıması Olarak Kişisel Verilerin Korunması ve Bu Bağlamda Unutulma Hakkı”, **Türkiye Adalet Akademisi Dergisi**, S. 32 (2017), s. 391.

²⁰³ Pamela Samuelson, “Privacy as Intellectual Property?”, **Stanford Law Review**, Y. 52, S. 1125 (Kasım 2000), s. 1125.

²⁰⁴ Zhou Hanhua, 个人信息保护法-专家建议稿-及立法研究报告 (Kişisel Bilgilerin Korunması Kanunu (Uzman Öneri Taslağı) ve Yasal Araştırma Raporu), Pekin: Kanun Yayınları, 2006, s. 79-80.

oluşturulması yöntemi ABD tarafından benimsenmiştir. Günümüze kadar ABD kişisel verilerin korunması hakkında yeknesak kanun yapmamıştır. Tam aksine bütün endüstriler ayrı-ayrı şekilde regüle edilmektedir. Bu yöntemde, kişisel veriler mahremiyet kategorisine yerleştirilir ve korunur. Bu durum ABD hukukunda mahremiyet kavramı çerçevesinin genişliğinden kaynaklanmaktadır. Yani, büyük mahremiyet kavramı ABD hukukunda tercih edilmiştir. Kara-Avrupa hukukunda ise mahremiyet, itibar hakları, portre hakları ve isim hakları gibi belirli kişilik haklarının içeriğini içeren hak olarak kabul edilmiştir²⁰⁵. ABD'nin mahremiyet ile ilgili farklı perspektifi doğal olarak kişisel veri koruma yöntemini de etkilemiştir.

Anglo-Sakson hukuk sisteminde kişisel veri kavramının ekonomik ve ekonomik yöntemlerden dolayı genellikle mülkiyet ve/veya fikri mülkiyet kapsamına girdiği kabul edilmektedir. Anglo-Sakson hukuk sisteminde kişisel veriler, yalnızca sahibinin kişiliğinin bir uzantısı değil, aynı zamanda ilgili kişinin bir ürünüdür²⁰⁶. Kişisel verinin, ilgili kişinin mülkiyet hakkı ya da fikri mülkiyet hakkı kapsamında nitelendirilmesi gerektiği yönünde iki yönetime ayrılmaktadır²⁰⁷.

ABD gibi Anglo-Sakson ülkelerinde, genellikle mahremiyet (Privacy) kavramı kullanılır. ABD Kongresi tarafından 1974'te kabul edilen "Mahremiyet Yasası" (Privacy Act), Nisan 2000'de ABD Federal Ticaret Hukuku Komisyonu tarafından düzenlenen "Çocukların Çevrimiçi Mahremiyet Koruma Kuralları" ve 1986'da ABD Kongresi tarafından yenilenen "Elektronik İletişim Gizlilik Yasası" buna örnek olarak sayılabilir.

Bu iki yöntemi karşılaştırdığımızda, Avrupa'daki kapsamlı yasama modeli, kişisel verilerin tekdüzen yasal kurallarla korunmasına odaklanmakta ve kişisel verilerin korunması için açık standartlar ortaya koymaktadır. Ancak, kişisel veri

²⁰⁵ The American Law Institute, Restatement of Torts, Second, 1977, 652C, 652E.

²⁰⁶ Hüseyin Can Aksoy, "The Right to Personality and It's Different Manifestations as the Core of Personal Data", **Ankara Law Review**, C. 5, S. 2 (Ocak 2008), s. 215.

²⁰⁷ Akkurt, **a.g.m.**, s.21.

haklarının özel nitelik ve içeriğini özel haklar açısından doğrulayamamıştır. Bu yöntem, devletin kamu iktidarının rolünü çok fazla vurgular. Soyut kurallar, katı denetim ve yönetim vb. sorunlar ortaya çıkarır²⁰⁸. ABD'nin ayrı yasama modeli, veri akışını ve kullanımını sağlayan piyasa düzenlemesi ve endüstrinin kendi kendini yönetmesine odaklanmaktadır. İlgili kişi ile veri sorumlusu arasındaki güç dengesizliği bu yöntemin dezavantajlarından biridir ve veri ihlali riski daha yüksektir.

Özetle mahremiyet ile kişisel veri arasındaki ilişkinin nasıl nitelendirilmesi veri koruma yöntemlerini belirlemektedir. ABD yasası pragmatizme dayanmaktadır ve kişisel veri ve mahremiyeti ayırmaz. Özellikle, ABD yasaları bir kişilik hakları sistemi ve birleşik bir kişisel veri koruma yasası oluşturmamıştır ve sonuçta kişisel veriler için böyle bir koruma yönteminin benimsenmesi kaçınılmazdır. Her iki koruma yönteminin avantajı ve dezavantajı bulunmaktadır. Bu nedenle özellikle günümüz yapay zekâ ve büyük veri teknolojileri ışığında, bu iki yöntemlerin tekrar değerlendirilmesi güncel olan hukuki mekanizmaların ortaya konulması oldukça önemli hale gelmiştir.

Kişisel verilerin korunması kavramı uluslararası belgelerde yer almadan önce kişilik onuru, özgürlüğü ve güvenliği hakkı bağlamında ele alınıp, mahkeme kararları ile koruma kapsamına alınırdı. Bu hakkın kapsamı ve korunması konularında yapılan tartışmalar hakkın etkin olarak korunması için ulusal ve uluslararası normlarda yer alması yönünde önemli rol oynamıştır. Gerek düzenleme ihtiyacı gerekse düzenlemenin kapsam ve şeklinde yol gösterici nitelik taşımıştır²⁰⁹. Yapay zekâ çağından önce kişisel verilerin korunması genel olarak temel insan hakkı olan mahremiyet hakkı kapsamında değerlendiriliyordu, fakat yapay zekâ teknolojilerinin getirdiği yenilikler karşısında kişisel veriler yeni bir nitelik kazanmış durumundadır. Sadece nicel anlamda değil, niteliksel anlamda kişisel verilerin içeriği zorunlu olarak

²⁰⁸ Kong Lingjie, 个人资料隐私的法律保护 (Kişisel Veri Gizliliğinin Yasal Olarak Korunması), Wuhan: Wuhan Üniversitesi Yayınları, 2009, s. 167-168.

²⁰⁹ OKUR, a.g.m., s. 63.

değişime uğramıştır. Kişisel verilerin kapsamının karşılaştığı sorunlar daha sonraki bölümde ele alınacaktır.

2.4. Uluslararası Düzenlemeler

Uluslararası hukuka baktığımızda kişisel verilerin hem korunma gerekliliği bakımından hem ekonomik çıkar bakımından değerlendirildiği görülmektedir. Bu noktada uluslararası hukuki düzenlemeleri iki grupta değerlendirebiliriz. Birinci grup, kişisel verilerin korunmasını uluslararası sözleşmelerin temel bir hakkı olarak ele alır. Bu sözleşmeler, ilerleyen yıllarda kişisel verilerin korunması hakkını içerecek şekilde yorumlanmıştır. İkinci grup, bilgi ve iletişim teknolojisindeki hızlı değişikliklerden kaynaklanan kişisel verileri korumanın benzersiz zorluklarıyla başa çıkmayı amaçlamaktadır. Bu düzenlemelerin teknolojik gelişmeye ve ticari faaliyetlere fazla müdahale etmediği görülmektedir²¹⁰.

2.4.1. Ekonomik İşbirliği ve Kalkınma Örgütü

“Kişisel Verilerin Sınır Aşan Trafiği ve Kişisel Verilerin Korunmasına İlişkin Kılavuz İlkeler” (OECD Rehber İlkeleri) adlı kişisel verileri korunması alanındaki ilk uluslararası metin OECD tarafından 1980 yılında yayımlanmıştır. Bağlayıcı gücü olmayan, taraf ülkeler açısından sadece tavsiye niteliği taşıyan belge ayırt edici özelliği, temel ilkeleri içermesi nedeniyle veri koruma konusunda hiçbir düzenlemenin bulunmadığı ülkeler için bir kılavuz niteliğinde değerlendirilmiştir²¹¹. OECD Rehber İlkelerinde kişisel verilerin korunmasında dikkat edilmesi gereken 8 ilke Tablo 8’de yer almaktadır²¹²:

²¹⁰ Berna Akçalı Gür, “Uluslararası Hukuk ve AB Hukuku Boyutuyla Kişisel Verilerin Yurt Dışına Aktarılması”, **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi**, C.25, S. 2 (Aralık 2019), s. 852.

²¹¹ İlke Gürsel, “Protection of Personal Data in International Law and The General Aspects of The Turkish Data Protection Law”, **DEÜHF Dergisi**, C. 18, S. 1 (2016), s. 4.

²¹² OECD, *New Data for Understanding the Human Condition: International Perspectives*, Paris, 2017.

Tablo 8: “OECD Rehber İlkeleri’nde Belirtilen İlkeler²¹³

Sınırlılık ilkesi	Kişisel veriler yasal neden ve yöntemlerle toplanmalı, ilgili kişi veri toplama hakkında bilgilendirilmeli. (m. 7)
Kalite kontrol ilkesi	Kullanım amacı çerçevesinde, toplanan veriler mümkün olduğu kadar doğru ve güncel olmalıdır. (m. 8)
Amaçla sınılama ilkesi	Kişisel verilerin toplanma amacı açıkça belirlenmeli ve veriler yalnızca belirlenen amaç için kullanılmalıdır. (m. 9)
Kullanım sınırlaması ilkesi	Toplanan veriler belirtilen amaçlar dışında kullanılamaz. Ancak istisna durumlarda ilgili kişinin bilinçli rızası ve kanuna dayalı kullanılabilir. (m. 10)
Güvenlik ilkesi	Toplanan verilere yönelik oluşabilecek tehlikelere karşı uygun güvenlik tedbirleri alınmalıdır. (m. 11)
Açıklık ilkesi	Bireyler, kendileri ile ilgili verileri içeren kurumların politikalarına kolaylıkla ulaşabilmelidir. (m. 12)
Bireysel katılım ilkesi	İlgili kişi veri sorumlularından kendilerine ilişkin verilerin bulunup bulunmadığını öğrenme, isteme, bu isteklerinin reddedilmesi halinde nedenlerinin kendisine açıklanmasını isteme ve ret kararına itiraz etme, silme, düzeltme, tamamlama haklarına sahip olmalıdır. (m. 13)
Hesap verebilirlik ilkesi	İlgili kişiler diğer ilkeler çerçevesinde veri toplayıcılar ve işleyiciler hakkında hesap sorma hakkına sahiptir. (m. 14)

²¹³ Eroğlu, **a.g.m.**, s. 135.

Dijital alandaki gelişimleri göz önünü alınarak, ilgili belge OECD tarafından 2013 yılında güncel hale getirilmiştir. Güncellenen metinde “Gizlilik Yönetim Programı (Privacy Management Program)”, “Veri Güvenliği İhlal Bildirimi (Data Security Breach Notification)” vb. yeni kavramlar düzenlenmiştir. Sadece tavsiye niteliğinde olmasına rağmen, OECD ilkeleri kişisel verilerin korunma ilkelerini belirlemede ilk uluslararası düzenleme niteliğindedir. Günümüzde OECD kılavuz ilkelerin dijital ortamında uygulanmasına ilişkin pratik öneriler sunmak amacıyla farklı ülkeler ve uzmanlarla birlikte çalışmaya devam etmektedir.

2.4.2. Birleşmiş Milletler

BM “İnsan Hakları Evrensel Beyannamesi” 12. maddesi:

“Kimsenin özel yaşamına, ailesine konutuna ya da haberleşmesine keyfi olarak karışılmaz, şeref ve adına saldırılamaz. Herkesin bu gibi karışma ve saldırılara karşı yasa tarafından korunmaya hakkı vardır”

şeklinde düzenlenmiştir. BM’nin “Kişisel ve Siyasal Haklar Sözleşmesi” nin 17. maddesinde ise “Mahremiyet Hakkı (Right to Privacy)” konusu düzenlenmiştir. BM’nin insan hakları ile ilgili bu düzenlemeleri ulusal ve uluslararası kuruluşlar başta olmak üzere tüm dünya kurumlarını temel haklar alanında düzenleme yapma konusunda teşvik etmiştir²¹⁴. Kişisel verilerin korunması hukuku alanında BM tarafından atılan en önemli adım 1990 yılında kabul edilen “Bilgisayara Geçirilmiş Kişisel Veri Dosyalarının Düzenlenmesi Rehber İlkeleri” kılavuz olmuştur. Bu kılavuz, tavsiye niteliğinde olan aşağıdaki dokuz temel ilkeyi belirtmiştir²¹⁵:

- Hukuka uygun ve dürüst yollardan verilerin toplanması ve işlenmesi ilkesi,
- Doğruluk ilkesi,

²¹⁴ Council of Europe, Handbook..., a.g.e., s. 14.

²¹⁵ UN General Assembly, Guidelines for the Regulation of Computerized Personal Data Files 1990.

- Amaç-özellik ilkesi,
- İlgili kişinin erişiminin sağlanması ilkesi,
- Bireyler arasında ayrımcılık yapılmaması ilkesi,
- İstisna yapma yetkisi,
- Güvenlik ilkesi,
- Denetim ve yaptırımlar ilkesi,
- Sınır ötesi veri akışı sınırlama ilkesi.

İlgili kılavuz yukarıda belirlenen ilkelerin uygulamasını denetlemek üzere bağımsız yapıya sahip yetkili bir veri koruma kuruluşunun oluşmasını öngören ilk belge olması nedeniyle günümüze kadar önem taşımaktadır²¹⁶. OECD ile mukayese edildiğinde iki kılavuz ile OECD Rehber İlkeler arasındaki benzerlikler açık şekilde görülmektedir. BM kılavuzu daha sonra düzenlendiği için bağımsız bir yetkili kurum konusunda daha ileri görüşe sahip olduğu söylenebilir. Nitekim GDPR’ın daha sonra belirlediği denetim mekanizma kurumların BM rehber ilkelerinden etkilendiğini söylemek yanlış olmayacaktır.

2.4.3. Avrupa Konseyi

İkinci Dünya Savaşı’ndan sonra, Avrupa federal yapısı kurmaya yönelik işbirliği sonucunda Avrupa Konseyi doğmuştur. Özellikle iki dünya savaşı ve ikinci dünya savaşı sırasında Avrupa’da yaşananlar, Avrupa Konseyi’ni kurma fikrinin temelini oluşturmuştur²¹⁷. Avrupa Konseyi daha sonra kişisel verilerin korunması konusunda çalışmalar ortaya çıkarmış ve günümüzde 47 üye ülkesi bulunmaktadır²¹⁸.

²¹⁶ DUMAN, a.g.m., s. 22.; Küzeci, a.g.e., s. 136.

²¹⁷ Mehmet Hasgüler ve Mehmet Uludağ, **Devletlerarası ve Hükûmetler Dışı Uluslararası Örgütler (Tarihçe-Organlar-Belgeler-Politikalar)** 4.b., İstanbul: Alfa Yayınları, 2010, s. 317- 318.

²¹⁸ Ali Servet Öncü ve Erkan Cevizliler, “Avrupa Bütünleşmesi İçin Önemli Bir Adım: ‘Avrupa Konseyi’ ve Türkiye’nin Konseye Üyeliği Meselesi”, **Akademik Bakış**, C. 7, S. 13 (2013), s. 23.

2.4.3.1. Avrupa İnsan Hakları Sözleşmesi

Kişilerin özel yaşamı ve aile hayatı, evi ve çevresine ilişkin hakları tanımlayan düzenlemeleri barındıran, önceki uygulamalara göre hukuki koruması daha yüksek olan “Avrupa İnsan Hakları Sözleşmesi”²¹⁹ Avrupa Konseyi üyesi devletleri tarafından 1950 tarihinde Roma’da imzalanmıştır. Günümüzde Avrupa Konseyi üyesi 47 devletin tümü AİHS’ne taraftır. Sözleşmenin 8. maddesi özel hayata ve aile hayatına saygı hakkı olarak şu şekilde tanımlanmıştır:

“Madde 8: Özel ve aile hayatına saygı hakkı: Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir. Bu hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin yasayla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusu olabilir”.

Bu Sözleşmede kişisel verilerin korunması kelimesi geçmemektedir, fakat Avrupa İnsan Hakları Mahkemesi (AİHM), kişisel verilerin kötüye kullanılmasına yönelik şikâyetlerin engellenmesi amacıyla bu maddeyi geniş yorumlayarak kişisel verilerin korunması hususunda meşru zemin, sözleşmedeki dayanak noktası haline getirmiştir²²⁰.

2.4.3.2. 108 Sayılı Sözleşme

Avrupa Konseyi’nde hazırlanan, 28 Ocak 1981’de imzaya açılmış ve 1 Ekim 1985’te yürürlüğe giren 108 Sayılı “Kişisel Verilerin Otomatik İşleme Tabi Tutulması

²¹⁹ Cunningham McKay, “Complying with International Data Protection Law”, **University of Cincinnati Law Review**, C. 84, S. 421 (2016), s. 426.

²²⁰ AİHM Kararı, M.S. v. Sweden (20837/92), Tarih: 27.08.1997, (Çevrimiçi) http://www.hrcr.org/safrica/privacy/ms_sweden.html, (Erişim Tarihi: 06.02.2018).

Karşısında Bireylerin Korunması Sözleşmesi” kişisel verileri uluslararası alanda koruma altına almıştır. Türkiye Sözleşmeyi 28 Ocak 1981’de imzalamış, fakat 1 Eylül 2016 tarihinde yürürlüğe girmiştir. Bu sözleşmeye ek olarak, 2001 yılında, Avrupa Konseyi üyesi olmayan ülkelere sınır ötesi veri akışını düzenleyen ve buna ek olarak ülkeler bazında bağımsız idari otorite kurularak ülke içindeki kişisel verilerin korunmasını izleyen ve denetleyen kurumların kurulması zorunluluğunu içeren 181 sayılı Ek protokol eklenmiştir. Protokol yürürlüğe girmesinden bu yana, 55 ülke bu protokole imza atmıştır. CETS 223 anlaşması ile yukarıdaki sözleşme 18 Mayıs 2018 tarihinde “108+ numaralı Modernize Edilmiş Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi” şeklinde kabul edilerek güncellenmiştir²²¹.

Çoğunlukla Avrupa Konseyi üyesi ülkelerin taraf olduğu bu sözleşme, üye olmayan ülkelerin de imzasına açık şekilde düzenlenmiştir. Bugüne kadar, Avrupa Konseyi üyesi tüm ülkeler sözleşmeyi onaylamış bulunmaktadır. Ayrıca, üye olmamasına rağmen, Meksika, Uruguay, Senegal, Tunus, Yeşil Burun Adaları ve Mauritius sözleşmeyi imzalamış durumundadır. Bu açıdan kişisel verilerin korunması için özel olarak hazırlanmış ilk ve tek uluslararası belgedir ve bağlayıcı kabul edilir. Bu gerçek kişisel verilerin korunmasına yönelik uluslararası düzenlemeler açısından çok önemlidir.

108 Sayılı Sözleşme’nin temel iki amacı bulunmaktadır: Kişisel verilerin toplanması ve işlenmesi durumunda oluşabilecek hak ihlallerine karşı ilgili kişileri korumak; kişisel verilerin Sözleşmeye taraf ülkeler arasındaki aktarımlarını düzenlemek. Bu çerçevede, Sözleşme gerçek kişilere ilişkin, ırk, cinsel tercih, sabıka kaydı gibi hassas kişisel verilerin uygun önlemler alınmadan toplanması ve işlenmesi yasaklanmıştır²²². Bir diğer önemli nokta ise ilgili kişinin topladığı verileri anlayabilmesi ve eksik veya yanlış olması halinde düzeltme yapma hakkına sahip

²²¹ Erdinç, **a.g.m.**, s. 2.

²²² 108 Sayılı Sözleşme, m. 6.

olmasıdır²²³. Bu noktada OECD ve BM'nin hazırlamış olduğu rehber ilkelere benzer şekilde düzenleme yapmıştır. Dikkate değer bir husus ise Sözleşmenin kapsamının tüzel kişilere veya kuruluşlara uygulanmasına izin vermeyecek kadar dar düzenlenmesidir. İkinci bir husus ise otomatik olarak işlenmeyen kişisel verilerin korunma altına alınmamasıdır. 108 Sayılı Sözleşmede kişisel verilerin toplanmasına ilgili olan temel ilkeler Tablo 9'daki şekilde düzenlenmiştir:

Tablo 9: 108 Sayılı Sözleşmede Belirtilen İlkeler²²⁴

Veri İşlemenin Meşruluğu İlkesi	Veri işleme, takip edilen yasal hedeflerle orantılı olmalı ve işlemenin her aşamasında kamu veya özel çıkarlar ile bu haklar ve özgürlükler arasında makul bir denge olmalıdır.
Açık Rıza İlkesi	Taraflar, veri işlemenin veri sahibinin ücretsiz, özel, bilgilendirici ve açık rızasına veya yasanın öngördüğü diğer yasal gerekliliklere uygun olarak gerçekleştirilmesini sağlamalıdır.
Hukuka Uygunluk İlkesi	İşlemeye konu kişisel veriler hukuka uygun olarak işlenmeli.
Şeffaflık İlkesi	Veriler adil ve şeffaf bir şekilde işlenmeli.
Amaç Sınırlama İlkesi	Veriler açık, belirli ve meşru amaçlarla toplanmalı ve bu amaçlar dışında işlenmemeli.
Doğruluk İlkesi	Veriler doğruyu yansıtmalı ve gerektiğinde güncellenmeli.

²²³ 108 Sayılı Sözleşme, m. 8.

²²⁴ DUMAN, a.g.m., s. 27.

Süreyi Aşmama İlkesi	Amaca ulaşmak için gereken süreyi aşmayacak şekilde yürütülmelidir.
----------------------	---

Özel veri kategorilerinde sayılan hassas verilerle ilgili olarak, 6. madde uyarınca ırk, köken, siyasi görüş, dini inanç, sağlık, cinsel yaşamla ilgili verilerin yanı sıra cezai mahkumiyetlerle ilgili verilerin toplanma ve saklanma yasası getirilmiştir²²⁵.

Özetlemek gerekirse, Avrupa Konseyinin kişisel verileri koruma hukukuna yönelik serüvenine baktığımızda, Avrupa Konseyi bakımından kişisel verilerin korunması meselesinin 1960'lı yıllarda başladığını söyleyebiliriz. Esas olarak, 1981 yılında 108 Sayılı Sözleşmenin kabulü ile Avrupa Konseyi için günümüz anlamında verileri koruma hukukunun oluştuğunun kabulü gerekir. Dahası uluslararası alanda taraf devletleri yükümlülük altına alarak kişisel verilerin korunması hukuku alanında bağlayıcı bir sözleşme olması ve 2001 yılında ek protokol ile bağımsız denetim otoritelerin ulusal düzeyde kurulmasını temin etmesi kişisel veri koruma kapsamındaki önemini vurgulamaktadır²²⁶.

Bu düzenleme daha sonraki GDPR tasarısında önemli ölçüde örnek olarak kullanılmıştır. Uluslararası alanda yapılan kişisel verilerin korunması konusundaki düzenlemeleri kronolojik şekilde bir araya getirirsek, Tablo 10'daki şekil önümüze çıkmaktadır:

²²⁵108 Sayılı Sözleşme, m. 6.

²²⁶ DUMAN, **a.g.m.**, s. 30.

Tablo 10: Kişisel Verilerin Korunması Konusundaki Uluslararası Düzenlemeler

Tarih	Düzenleyici	Düzenleme Adı
1953	Avrupa Konseyi	Avrupa İnsan Hakları Sözleşmesi
1980	OECD	Kişisel Verilerin Sınır Aşan Trafiği ve Kişisel Verilerin Korunmasına İlişkin Kılavuz İlkeleri
1981	Avrupa Konseyi	108 Sayılı Sözleşme
1990	BM	Bilgisayara Geçirilmiş Kişisel Veri Dosyalarının Düzenlenmesi Rehber İlkeleri
2001	Avrupa Konseyi	Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireyin Korunması Sözleşmesinin 181 sayılı Ek protokolü

2.5. Avrupa Birliğinde Kişisel Verilerin Korunması

Tarihsel olarak baktığımızda, bir önceki başlıkta bahsedildiği gibi AB ülkelerinde mahremiyetin korunması esas olarak kişilik hakları veya genel kişilik hakları ile gerçekleştirilmiştir. İnternet teknolojisinin getirdiği zorluklarla karşı karşıya kalan AB, yavaş yavaş bir “büyük” kişisel veri koruma modeli, yani özel bir kişisel veri koruma yasası aracılığıyla, internet çağındaki mahremiyet koruma problemini çözmeye çalışmıştır.

2.5.1. 95/46/AT Sayılı Direktif

Veri işleme teknolojisinde meydana gelen gelişmeler 1980’li yıllardan itibaren yayılmaya başlamıştır. Kişisel verilerin ticari amaçla kullanılmasının yaygınlaşması ile beraber Tek Pazar çerçevesinde üye devletler kişisel verileri koruma konusunda farklı uygulamalar ortaya çıkarmaya başlamıştır. Kişisel verilerin korunması konusunda yapılan OECD ve Avrupa Konseyi çalışmaları teknolojinin ilerlemesi ile beraber üye devletler arasındaki uyumu sağlama da etkisiz kalmıştır.

Bu gelişmeler Avrupa Konseyinin 1990 yılında taslak Veri Koruma Direktifini yayımlamasını gerekli kılmıştır. Avrupa Komisyonu tarafından hazırlanan bu taslak Bakanlar Konseyi tarafında 95/46/AT Sayılı Direktifi adı altında Şubat 1995 tarihinde kabul edilmiştir. 95/46/AT Sayılı Direktif, 24 Ekim 1995’te resmi olarak onaylanmıştır²²⁷.

95/46/AT Sayılı Direktifin AB üye ülkelerinde bağlayıcı ve zorlayıcı bir hukuksal metin olması direktifin o zamandaki uluslararası arenadaki önemini göstermektedir. 95/46/AT Sayılı Direktifin amaçlarından biri kişisel verilerin korunması konusundaki ulusal mevzuatları uyumlaştırarak kişisel verilerin tüm AB üye ülkelerinde aynı düzeyde ve benzer ilkeler çerçevesinde korunmasını gerçekleştirmek. İkinci amacı ise kişisel verilerin üye ülkelerde güvenilir bir şekilde serbest dolaşımını sağlamaktır²²⁸. Bu nedenle, birlik vatandaşların mahremiyetinin yüksek derecede korunması ile serbest veri akışı arasında bir denge kurmaya çalışılmıştır.

²²⁷ Daniel Solove, Marc Rotenberg ve Paul Schwartz, **Information Privacy Law**, New York: Aspen Publishers, 2006, s. 900.

²²⁸ Nur, **a.g.e.**, s. 6.

2.5.1.1. Kapsam ve İlkeleri

Modern dünyada neredeyse verilerin tamamı bilgisayar sistemleri kullanılarak otomatik yollarla kaydedilmektedir. Bu nedenle, 95/46/AT Sayılı Direktifin kapsamını genellikle otomatik yollar ile tutulan veriler olsun veya klasik yöntemler ile tutulmasına rağmen otomatik sistemlere aktarılan veriler dahil tüm verileri kapsayacak şekilde geniş yorumlanması mümkündür²²⁹.

95/46/AT Sayılı Direktif, kişisel verilerin işlenmesine yönelik kapsamlı bir yaklaşım kullansa da iki istisna tespit edilmiştir. Bunlardan biri, 95/46/AT Sayılı Direktifin hükümlerinin kamu güvenliği, milli savunma ve milli güvenlik ile ilgili işlemler ve AB hukuku kapsamı dışındaki faaliyetlere uygulanmamasıdır. İkinci istisna ise tamamen özel veya aile fertleri ile bağlantılı gerçek kişilerin veri işlemlerinde 95/46/AT Sayılı Direktif hükümlerinin uygulanmamasıdır. Ancak bu maddede “kişisel veya ailesiyle ilgili olan veri işlemlerinde” ifadesinden verileri belirli sayıda kişi ile paylaşmak yerine sınırsız sayıda kişiye ifşa eden veri işleminin 95/46/AT Sayılı Direktif kapsamı dışında bırakılamayacağı değerlendirilebilir²³⁰.

95/46/AT Sayılı Direktif yedi temel bölümden oluşmakta olup sırasıyla “genel hükümler, hukuka uygunluk sebepleri, hukuki tedbirler, sorumluluk ve yaptırımlar, kişisel verilerin üçüncü ülkelere transferi, davranış kuralları, teftiş otorite ve topluluk düzeyinde uygulama tedbirleri” bölümleri içermektedir²³¹.

95/46/AT Sayılı Direktifte belirlenen kişisel veri koruma ilkeler şunlardır:

- Adil ve Yasal İşleme İlkesi
- Amaç ile Sınırlılık İlkesi (Tarihsel, istatistiksel ve bilimsel amaçlarla işlenmesi hariç)

²²⁹ Oğuz Şimşek, **Anayasa Hukukunda Kişisel Verilerin Korunması**, İstanbul: Beta yayınları, 2008, s. 43.

²³⁰ Akıncı, **a.g.e.**, s. 7.

²³¹ Civelek, **a.g.e.**, s. 73.

- İlgililik ve Orantılılık İlkesi
- Doğruluk ve Güncellik İlkesi
- Süreyle Sınırlılık İlkesi

2.5.1.2. İlgili Kişilerin Hakları

95/46/AT Sayılı Direktifte ilgili kişilere tanınan hakları şu şekilde sıralanmıştır:

- Bilgi alma hakkı
- Verinin kaynağını bilme hakkı
- Düzeltme hakkı
- Yanlış verilerin düzeltilmesi hakkı
- İzin vermeme hakkı
- Hukuka aykırı işlemlere karşı başvuru hakkı
- Doğrudan pazarlama hususlarında kişisel verilerin kullanılmasına izin vermeme hakkı.

95/46/AT Sayılı Direktifte kişisel verilerin işlenebilmesine ilgili şartlar da yer almaktadır²³². Bu durumda kişisel verilerin ilgili kişinin açık rızası ile, sözleşmeden doğan yükümlülüklerin, yasal yükümlülüklerin yerine getirilmesi, ilgili kişinin hayati menfaatlerinin korunması ve kamu yararının gerektirdiği durumlarda veri işlemenin yapabileceği tespit edilmiştir²³³.

2.5.1.3. Getirildiği Yenilikler

95/46/AT Sayılı Direktifin en önemli özelliklerinden biri getirmiş olduğu etkin denetim sistemidir. Her üye devletin, 95/46/AT Sayılı Direktifin kendi ülkesinde

²³² 95/46/AT Sayılı Direktif, m. 7.

²³³ Akıncı, **a.g.e.**, s. 9.

uygulanmasını izlemekle yükümlü olduğunu ve bu amaçla en az bir veri koruma kurumu ataması gerektiğini belirtmiştir²³⁴.

95/46/AT Sayılı Direktif bireylere doğrudan tanınan haklardan yararlanma konusunda iç hukuka derç edilip edilmediğine bakılmaksızın yargı yoluna başvurabilme hakkı tanımıştır. Aslında, AB ülkeleri ulusal kanunlarını 95/46/AT Sayılı Direktifte uyumlu hale getirseler de 95/46/AT Sayılı Direktifin ve yönetmeliklerin temel ilkelerinin istediği asgari gerekliliklerin altındaki koruyucu tedbirler alması yasaklanmıştır.

95/46/AT Sayılı Direktifin 29. maddesine istinaden kişisel verilerin işlenmesi ile ilgili olarak çalışma grubu kurulmuş ve bu çalışma grubunun danışman bir komisyon gibi hizmet sunması ve bağımsız olarak hareket etmesi belirtilmiştir. Çalışma Grubu, her üye devlet tarafından belirlenen denetim yetkilisi veya yetkilileri ile AB organlarının bir temsilcisi ve bir Avrupa Komisyon temsilcisinden oluşmaktadır. Bu Çalışma Grubu, kişisel verilerin işlenmesi, gerçek kişilerin hak ve özgürlüklerini korumak için alınacak tedbirler ve bu 95/46/AT Sayılı Direktife yönelik önerilen herhangi bir değişiklik hakkında Avrupa Komisyona tavsiyede bulunmaya yükümlüdür²³⁵. Bu çalışma grubunun ihdasının bir sonucu olarak, özel hayatın korunması hakkı AB tarafından temel bir hak olarak dikkate alınmış, AB'nin Temel Haklar Şartı'nda kişisel verilerin korunması hakkı olarak bu şart üzerine derce dılmıştır²³⁶.

²³⁴ 95/46/AT Sayılı Direktif, m. 28.

²³⁵ 95/46/AT Sayılı Direktif, m. 29-30.

²³⁶ Lucas Bergkamp, "EU Data Protection Policy, The Privacy Fallacy: Adverse Effects Of Europe's Data Protection Policy in An Information-Dirven Economy", **Computer Law and Security Report**, S. 18 (2002), s. 33.

2.5.1.4. Özellikleri ve Eksiklikleri

95/46/AT Sayılı Direktifi dünyanın ilk kişisel veri koruma yasal çerçevesini oluşturmaktadır²³⁷. Birinci nesil kişisel veri koruma yasası niteliğinde olan 95/46/AT Sayılı Direktif aşağıdaki özellikleri benimsemiştir:

Birinci özellik: teorik altyapı olarak “Kendi Kaderini Kendi Tayin Etme” (Informational Self-Determination) temelinde, kullanıcıların kişisel veriler konusunda bağımsız kararlar alma hakkına sahip olduklarını vurgulamıştır²³⁸. Özel bir kişilik hakkı olan “Kendi Kaderini Tayin Hakkı” 1982 yılında Alman Federal Hükümeti nüfus, meslek ve ikamet de dahil olmak üzere vatandaşların kapsamlı bir kişisel veri toplanmasını planlayan “Sayım Yasası” nı yürürlüğe koyduğunda ortaya çıkmıştır. Sayım Yasası’nın anayasaya aykırı olarak ilan edilmesini talep eden vatandaş bu konuda anayasa mahkemesine dava açmıştır. 1983 yılında, Alman Federal Anayasa Mahkemesi, yasanın anayasaya aykırı olduğuna karar vermiş ve kişisel verileri kararda açık bir anayasal hak haline getirmiştir²³⁹. Bu Alman kişisel veri koruma yasası tarihinde bir dönüm noktası hükmünde olmuştur.

Burada değinilmesi gereken hususlardan biri kişisel verilerin korunması ile diğer hukuk menfaatlerin çatışması sorunudur. Özellikle ifade özgürlüğü, düşünceyi açıklama ve yayma hürriyeti konusu gündeme gelmektedir. Yanı yukarıda kabul edilen Kendi Kaderini Kendi Tayin Etme hakkı ile üçüncü şahısın ifade özgürlüğü arasındaki menfaat çatışması gündemde olmuştur. Ancak GDPR açık bir şekilde kişinin kendi verileri hakkındaki tasarruf (Kendi Kaderini Kendi Tayin Etme) hakkının sınırlandırılmaz olmadığını belirtmiştir. Bu hakkın “*toplum nezdindeki işlevi dikkate alınarak ve diğer temel hak ve özgürlükler gözetilerek ölçülülük ilkesine uygun olarak*

²³⁷ Omer Tene, “Privacy Law’s Midlife Crisis: A Critical Assessment of the Second Wave of Global Privacy Laws”, **Ohio State Law Journal**, C. 74, S. 6 (2013), ss.1217-1262, s. 1220.

²³⁸ Deirdre K. Mulligan ve Jennifer King, **Bringing the Gap Between Privacy and Design**, 14 U. Pa. J. Const. L. 989 (2012), s. 992.

²³⁹ He Xuxu, “比较法上的个人信息自决权 (Karşılaştırmalı Hukukta Kişisel Verilerin Kendi Kaderini Tayin Hakkı)”, **Comparative Law Research**, (2013), s. 62.

değerlendirilmesi” gerektiğini belirtmiştir. Kişisel verilerin korunmasında temel ilkelerden biri olan ölçülülük ilkesi “*özgürlüğe getirilen sınırlandırmanın, özgürlüğü belirleyen durumla arasında bir orantı bulunması ve getirilen sınırlandırmanın, hak ve özgürlüğün varlığını zedelememesi*”²⁴⁰ anlamına gelmektedir. Bu ilke, kamu gücünün sınırlandırılmasını ve özgürlüğün korunmasını sağlar ve aynı zamanda hukukun üstünlüğünün bir gereğidir²⁴¹. Bu bağlamda, orantılılık ilkesi, idari makamların kısıtlayıcı kararları ile temel hak ve özgürlükler arasında bir denge kurar. Buradaki denge, korunan hak ve özgürlüklerin güvencinin sağlanması ile başka bir menfaati korumak için hakların veya özgürlüklerin sınırlandırılması arasında elde edilmesi gereken dengeyi ifade eder²⁴².

İkinci özellik: sistemin açısından “Tüketici Kontrolü” (Consumer Control) ile “Aydınlatılmış Rıza” mekanizmasının kullanılmasına önem vermiş ve kişisel verilerin işlenmesi için ilgili kişinin rızasının gerektiğini önemsemiştir²⁴³.

Üçüncü özellik: işletmeler ve devlet kurumları çeşitli koruma sorumluluklarını üstlenecek veri denetleyicileri olarak nitelendirilmiştir²⁴⁴.

AB, elektronik iletişim alanında düzenlemeler yaparken, teknolojinin ilerlemesini dikkate alarak, geleceğe yönelik bir yaklaşım benimsemiştir. Aynı zamanda 95/46/AT Sayılı Direktif, halka açık iletişim ağları vasıtasıyla verilen elektronik iletişim hizmetlerin kendi uygulama alanından olduğunu belirtmiştir²⁴⁵.

Yukarıda sıralanan özellikler yasanın düzenlendiği dönemlerde çok etkileyici olsa da bu asrın başlangıcından bu yana, insan toplumunda medeniyetin evrimi

²⁴⁰ Yücel Oğurlu, **Karşılaştırmalı İdare Hukukunda Ölçülülük İlkesi**, 2002, Ankara: Seçkin Yayınları, s. 33.

²⁴¹ Şimşek, **a.g.e.**, s. 98.

²⁴² Oğurlu, **a.g.e.**, s. 35.

²⁴³ Jane K. Winn, **Consumer Protection in the Age of the ‘Information Economy’**, London: Routledge, 2006, s. 357.

²⁴⁴ Mulligan ve King, **a.g.e.**, s. 998.

²⁴⁵ Lilian Edwards, “The Problem with Privacy: A Modest Proposal”, **International Review of Law Computers & Technology**, C. 18 (2004), s. 320.

hızlandırılmış eğilimi göstermesi nedeniyle güncelliğini koruyamamıştır. İnsanlar internet çağından büyük veri çağına daha yeni girmişken ardından yapay zekâ çağı kapıyı çalmıştır²⁴⁶. Bununla beraber Nesnelerin interneti, büyük veri, Bulut Bilişim ve diğer teknolojilerin desteğiyle “her şey bir-birine bağlı, herkesin çevrimiçi, her işin algoritma ile çözüldüğü” yapay zekâ dönemine ulaşmış durumundayız²⁴⁷. Böylece yapay zekâ çağının getirdiği zorluklarla karşı karşıya kalan birinci nesil kişisel veri yasal koruma çerçevesi gerilmiş görünmektedir²⁴⁸. Günümüzde birinci nesil kişisel veri koruma yasaların etkisiz kalmasının nedenini birkaç noktada açıklamak mümkün.

İlk olarak, koruma yasasındaki kullanıcı kontrol yöntemi etkisiz halde kalmıştır. Günümüzde yapay zekâ, makine öğrenimi veri işlemenin sonuçlarını öngörülemez hale getirmiş, kullanıcılar veri işleme için uygun verileri elde edemez ve doğal olarak kullanıcıdan etkili rızayı istemek anlamsızlaşmıştır²⁴⁹. Aynı zamanda, bildirim izni mekanizması kullanıcılara ağır bir yük getirmiş ve bildirimlere etkili bir şekilde ulaşması zor, pazarlık fırsatından yoksun hal ortaya çıkmıştır²⁵⁰. Aslında aynı sorun bu sorunları çözme amacıyla ortaya çıkan daha sonraki düzenlemelerde, örneğin GDPR’da da yer almaktadır. Bu sorunun ortaya çıkmasının sebebi ise çok hızlı gelişen teknoloji karşısında esnek niteliği olmayan hukuk düzenlemelerinin etkisiz kalmasıdır.

İkincisi, veri denetleyici mekanizması ayarı problem haline gelmiştir. İnternet, sosyal ağlar ve yapay zekâ ürünlerinin popülaritesi, bireysel kullanıcıları kişisel verilerin toplanması, işlenmesi ve aktarılmasında önemli bir katılımcı ve aynı zamanda başkalarının gizliliğini ihlal eden potansiyel bir aktör haline getirmiştir. Bu bağlamda, merkezi olmayan bireysel kullanıcılara işletmeler ve devlet kurumları gibi geleneksel

²⁴⁶ Wu Handong, “人工智能时代的制度安排与法律规制 (Yapay Zekâ Çağında Kurumsal Düzenlemeler ve Yasal Düzenlemeler)”, **Legal Science**, 2017, s. 130.

²⁴⁷ Wu Jun, **智能时代: 大数据与智能革命重新定义未来** (Akıllı Çağ: Büyük Veri ve Akıllı Devrim Geleceği Yeniden Tanımlıyor), Pekin: CITIC Publishing Grup, 2016, s. 331.

²⁴⁸ Mulligan ve King, **a.g.e.**, s. 999.

²⁴⁹ Alexandra Rengel, “Privacy- Invading Technologies and Recommendations for Designing a Better Future for Privacy Rights”, **Intercultural Hum. Rts. L. Rev.**, (2013), s. 226.

²⁵⁰ Winn, **a.g.e.**, s. 356.

veri denetleyicilerine getirilen çeşitli yasal sorumlulukları doğrudan uygulamak ne pratik ne de ekonomik hale gelmiştir.

Üçüncüsü, günümüzde benimsenen ihlal sonrası yardım modeli yapay zekâ çağına uyum sağlayamıyor olmasıdır. Geleneksel yasal koruma, veri denetleyicisinin kişisel veriyi toplaması ve yalnızca gizlilik ihlali gerçekleştiğinde koruma süreci başlar. Bu tipik bir ihlal sonrası kurtarma modelidir²⁵¹. Ancak aslında günümüzde gerçekleşen birçok ihlal gizlilik sistemin kendisinden kaynaklanmaktadır. Geliştiricilerin ve üreticilerin sistem tasarımı aşamasında yaptıkları seçimler, sistem tarafından gizlilik ihlallerinin kapsamını ve derecesini belirlemektedir. Bu yetersizlikler göz önüne alınarak, AB çerçevesinde 2016 senesinde GDPR yürürlüğe girmiştir.

AB, 95/46/AT Sayılı Direktifin ardından, söz konusu Direktifi tamamlayıcı niteliğinde olan başka direktifler yayınlamıştır. Bu direktifler esas olarak kişisel verileri sektörel olarak ele almaktaydı. Örneğin: Aralık 1997 tarihinde 97/66/AT sayılı “Telekomünikasyon Sektöründe Kişisel Verilerin İşlenmesi ve Özel Hayatın Gizliliğin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Direktifi”²⁵² ile kişisel verilerin telekomünikasyon sektöründe düzenlenmesini ele almıştı. Aynı şekilde, Temmuz 2002 tarihinde 2002/58/AT Sayılı “Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Özel Hayatın Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Direktifi”²⁵³ elektronik haberleşme sektöründe düzenlemeyi gerçekleştirdi. Daha sonra 2006/24/AT sayılı “Kamuya Açık Haberleşme Hizmetleri veya Kamu Haberleşme Şebekesi ile Bağlantılı Olarak Üretilen veya İşlenen Verilerin Saklanması ile İlişkin Avrupa Parlamentosu ve Avrupa Konseyi

²⁵¹ Ishii, **a.g.m.**, s. 511.

²⁵² Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector, 30.01.1998.

²⁵³ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (“Directive on privacy and electronic communications”), 31.07.2002.

Direktifi”²⁵⁴ kabul edilmiştir. Bunlar sektörel alanda kişisel verilerin nasıl korunacağını konu eden direktiflerdir ve daha sonra kabul edilmiş olan GDPR için hazırlık aşaması niteliğinde olduğunu söyleyebiliriz. Kullanıcının cihazında elde edilen ve saklanan bilgilere yasal olarak erişim davranışının, yakında 2002/58/AT Direktifinin yerini alacak olan “Elektronik Gizlilik Tüzüğü”²⁵⁵ ile düzenlenmesi beklenmektedir.

2.5.2. Avrupa Birliği Temel Haklar Şartı

Avrupa Birliği Temel Haklar Şartı’nın 8. maddesi kişisel verilerin korunmasını anayasal bir hak olarak değerlendirmiş ve 2009’da Lizbon Antlaşması²⁵⁶’nın yürürlüğe girmesiyle kişisel veri korunması hakkı anayasal bir hak statüsüne kazanmıştır. Yine bu antlaşma ile kişisel verilerin işlenmesini hukuki ve idari yönden denetleyecek olan bir bağımsız kuruma ihtiyaç teyit edilmiştir²⁵⁷. Ayrıca “Avrupa Birliği İşleyişine İlişkin Antlaşma”nın 16. maddesi, kişisel veri işleme kurallarının belirlenmesinde Avrupa Parlamentosu ve Avrupa Konseyi’nin yükümlülüklerini düzenlemiştir. Bu bakımdan kişisel verilerin özel hayatın korunmasından farklı bir anayasal hak olarak korunması AB’ye özgü bir yaklaşım olarak değerlendirilmektedir²⁵⁸.

AB Temel Haklar Şartı AB tarafından hazırlanan ve bireylere çeşitli temel haklar tanıyan belge niteliğindedir. Aralık 2000 yılında imzalanarak AB devletlerinde kişisel,

²⁵⁴ Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, 13.04. 2006. Bu Direktif 08.04.2014 itibarıyla ABAD’ın C-293/12 ve C-594/12 sayılı kararı ile geçersiz kılınmıştır.

²⁵⁵ Söz konusu Tüzük GDPR’a göre spesifik özel bir yasa niteliğinde olacaktır. Daha fazla bilgi için bkz. Leyla Keser Berber, Ayça Atabey ve Melis Mert, “E-Gizlilik Tüzük Taslağının Son Versiyonu Üzerine Düşünceler”, **Kişisel Verileri Koruma Dergisi**, C. 1, S. 2 (2019), ss. 66- 75.

²⁵⁶ Maastricht Anlaşması ile Avrupa Ekonomik Topluluğu, Avrupa Topluluğu’na, daha sonra Lizbon Anlaşması ile Avrupa Topluluğu terimi Avrupa Birliği terimine dönüştürülmüştür.

²⁵⁷ Alina Kaczorowska, **European Union Law**, New York: Routledge Cavendish, Taylor and Francis Group, 2009, s. 43.

²⁵⁸ Berna Akçalı Gür, **a.g.m.**, s. 853.

siyasi ve ekonomik hakları ilk defa olmak üzere tek bir metinde bir araya getirilmiştir²⁵⁹. AB Temel Haklar Şartı'nın “Kişisel verilerin korunması” başlıklı maddesi şu şekilde düzenlenmiştir:

*“Herkes, kendisini ilgilendiren kişisel verilerin korunması hakkına sahiptir. Bu veriler, dürüst bir şekilde belirli amaçlar için ve ilgili kişinin rızasına veya yasa ile öngörülmüş diğer meşru bir temele dayanılarak işlenir. Herkes kendisi hakkında toplanmış verilere erişme ve bunları düzelttirme hakkına sahiptir. Bu kurallara uyulması bağımsız bir makam tarafından denetlenir”*²⁶⁰.

2.5.3. Genel Veri Koruma Tüzüğü

95/46/AT Sayılı Direktif üye ülkelerde uyum sağlama açısından yetersiz kalmış. Nitekim 95/46/AT Sayılı Direktif oluşturulduğunda üye ülkelerin katkısı oldukça sınırlı olmuştur. Sonuçta üye ülkeler arasında 95/46/AT Sayılı Direktif konusunda farklı yorumlamalar ortaya çıkmıştır²⁶¹. Bu durum, yalnızca AB üye devletlerinin veri koruma düzenlemelerinin ve 95/46/AT Direktifinin AB genelinde kişisel verileri korumak için yeterli olmadığı, dolayısıyla reformlara ihtiyaç olduğu fikrine yol açmıştır²⁶².

AB vatandaşların mahremiyetini korumak için Avrupa Parlamentosu tarafından 14 Nisan 2016 tarihinde GDPR onaylanmıştır²⁶³. AB, profil oluşturma da dahil olmak üzere “Tasarımda ve Varsayılan Ayarda Veri Koruma”, “Nesne Hakkı” ve “Otomatik Bireysel Karar Verme” gibi ilgili hükümleri içeren GDPR’ı resmi imzalamıştır.

²⁵⁹ DUMAN, **a.g.m.**, s. 36.

²⁶⁰ Küzeci, **a.g.e.**, s. 172.

²⁶¹ Türkay Henkoğlu, **Bilgi Güvenliği ve Kişisel Verilerin Korunması**, Ankara: Yetkin Yayınları, 2015, s. 60.

²⁶² Akıncı, **a.g.e.**, s. 10.

²⁶³ Akıncı, **a.g.e.**, s. 5-7.

Mayıs 2018’de yürürlüğe girmesi nedeniyle, GDPR bireyleri koruyan ve kişisel verilerin işlenmesi için rızanın rolünü güçlendiren bir dizi garanti sunmaktadır. Verilerin kullanımını toplandıkları amaçlarla sınırlayan, veri minimize etme prensibini benimsemektedir. Veri işlemenin şeffaflığını arttırıp ve otomatikleştirilmiş işleme dayalı bir kararın konuları için açıklama hakkı sunmaktadır.

GDPR, mevcut yasal çerçeveyi uyumlu hale getirmeyi ve yasal boşluğunu azaltmayı amaçlamaktadır. GDPR’ın 2. maddesi, GDPR’ın piyasa ve gerçek kişilerin refahı için bir özgürlük, güvenlik ve adalet alanının ve bir ekonomik birliğin başarılmasına, ekonomik ve sosyal ilerlemeye, iç ekonomilerin güçlenmesine ve yakınsamasına katkıda bulunmayı amaçladığını belirtmiştir. GDPR’ın temel amacının, kişisel verilerin korunması alanında, daha yüksek ölçütler belirleyerek üye ülkelerin entegrasyonunu hızlandırmak ve üye olmayan ülkelerde faaliyet gösteren ancak AB ile ticari ilişkileri bulunan şirketlerin bu düzenlemelere uyumunu sağlamak olduğu belirtilmiştir²⁶⁴.

Kişisel verilerin korunması hakkında benimsenen ilkeler GDPR’ın 5. maddesinde aşağıdaki şekilde sıralanmıştır:

- Yasallık ilkesi
- Adalet ve şeffaflık ilkesi
- Amaç sınırlama ilkesi
- Veri minimizasyonu ve doğruluk ilkesi
- Depolama sınırlama ilkesi
- Bütünlük ve gizlilik ilkesi

GDPR yürürlüğü girdikten sonra kendi etkisini göstermeye başlamıştır. 2019’da AB’nin GDPR’ı ihlal eden şirket ve kurumlara 112 milyon Euro’nun üzerinde para

²⁶⁴ Furkan Güven Taştan, **Türk Sözleşme Hukukunda Kişisel Verilerin Korunması**, 1. b., İstanbul: On İki Levha Yayıncılık, 2017, s. 15.

cezası verdiği belirtilmektedir. Kamuya açık raporlar, GDPR’ın ilk yılında bununla ilgili 140.000 şikâyet olduğunu gösteriyor. Bu yıl itibarıyla, GDPR ihlallerine karşı 155 milyon Euro para cezası ve yaptırım uygulamıştır²⁶⁵. GDPR yürürlüğe girmeden önce, şirketlerin %78’i güvenle uyum için hazır olduklarını belirtmiştir, ancak Capgemini’nin anket sonuçları, düzenlemelerin uygulanmasından sonra şirketlerin yalnızca %28’nin GDPR’a uymada başarılı olduğunu göstermektedir²⁶⁶.

2.5.3.1. Uygulama Alanı

GDPR’ın uygulama alanı madde 3’ te şu şekilde düzenlenmiştir:

“GDPR, işleme faaliyeti Birlik içerisinde gerçekleşip gerçekleşmediğine bakılmaksızın, Birlik içerisindeki bir veri sorumlusu veya işleyenin işletmesinin faaliyetleri bağlamında kişisel verilerin işlenmesine uygulanır. GDPR, işleme faaliyetlerinin aşağıdaki hususlarla alakalı olması durumunda, Birlik içerisinde bulunan ilgili kişilerin kişisel verilerinin Birlik içerisinde kurulu olmayan bir veri sorumlusu veya işleyen tarafından işlenmesine uygulanır: a. İlgili kişiye bir ödeme yapılmasına gerek olup olmadığına bakılmaksızın, Birlik içerisindeki söz konusu ilgili kişilere mal ya da hizmetlerin sunulması veya b. Davranışları birlik içerisinde gerçekleştiği ölçüde, davranışlarının izlenmesi. GDPR, Birlik içerisinde değil, ancak bir üye devletin hukukunun uluslararası kamu hukuku vasıtasıyla uygulandığı bir yerde kurulu bulunan bir veri sorumlusu tarafından kişisel verilerin işlenmesine uygulanır”.

²⁶⁵ Doug Barney, “Major GDPR Fine Tracker – An Ongoing, Always-Up-To-Date List of Enforcement Actions”, **CoreView**, 31.10.2020 (Çevrimiçi) <https://www.coreview.com/blog/alpin-GDPR-fines-list/>, (Erişim Tarihi: 04.11.2020).

²⁶⁶ Danny Palmer, “GDPR: Only One In Three Businesses Are Compliant – Here’s What Is Holding Them Back”, ZDNet, (Çevrimiçi) <https://www.zdnet.com/article/GDPR-only-one-in-three-businesses-are-compliant-heres-what-is-holding-them-back/>, (Erişim Tarihi:04.11.2020), par. 3.

Yukarıdaki 3. maddede anlaşıldığı üzere, bu düzenleme, verilerin AB dışında işlense bile, işlenen verilerin AB'deki bir veya daha fazla kişiyle ilgili olması durumunda ilgili düzenlemenin AB dışında da geçerli olacağını öngörmektedir. Bu düzenleme, herhangi bir veri işleme faaliyetinin AB içinde olup olmadığına bakılmaksızın geçerlidir. GDPR, AB içindeki ilgili kişinin davranışlarını izlemesi durumunda, bu faaliyetler AB tarafından kurulmuş olmayan veri sorumlusu veya işlemciler tarafından gerçekleştirilse bile geçerlidir²⁶⁷.

Ancak şunu da belirtmemiz gerekir ki GDPR'ın yukarıda anlatılan sınır ötesi yetkisi (yer bakımından uygulama yetkisi) GDPR yürürlüğe girdiğinden bu yana tartışma konusu olmuştur. Bazı uzmanlar GDPR'ın geniş uygulama yetkisi devletlerarası ilişkileri bozacak nitelikte olduğunu savunurken²⁶⁸, bazı uzmanlar GDPR'ın kişisel verileri koruyan yasalar üzerinde uluslararası düzeyde önemli olumlu etkisi olacağına ve bu nedenle düzenlemelerin korunması gerektiğine inanmaktadır²⁶⁹.

GDPR'ın otomatik ve otomatik olmayan veri kayıt sistemleri ayrımı vardır. Bununla birlikte, sadece işlenmesi gerçekleşen veriler değil, işlenmesi öngörülen verilerde, GDPR'ın kapsamında değerlendirilecektir²⁷⁰. Dolayısıyla daha sonradan sisteme entegre edilecek hallerde GDPR uygulama alanı bulacaktır.

2.5.3.2. Haklar ve Yükümlülükler

GDPR ilgili kişi hakkında geniş kapsamda haklar düzenlemiştir. GDPR'da belirlenen ilgili kişinin hakları Tablo 11'de, veri sorumlusu ve veri işleyenin yükümlülükleri Tablo 12'de yer almaktadır.

²⁶⁷ Ufuk Dal, "Avrupa Birliği Genel Veri Koruma Tüzüğü'nün Ülke Dışı Uygulama Yetkisi ve Bu Yetkinin Uluslararası Hukukta Meşruiyeti", **Kişisel Verileri Koruma Dergisi**, C. 1, S. 1 (2019), s. 25.

²⁶⁸ **a.g.m.**, s. 32.

²⁶⁹ Brendan Van Alsenoy ve Marieke Koekoek, "Internet And Jurisdiction After Google Spain: The Extra-Territorial Reach of The EU's Right To Be Forgotten", **Leuven Center for Global Governance Studies**, S. 152 (2015).

²⁷⁰ Mesut Serdar Çekin, **Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kişisel Verilerin Korunması Kanunu**, 1.b., İstanbul: On İki Levha Yayınları, 2018, s. 24.

Tablo 11: GDPR’da Belirtilen İlgili Kişinin Hakları

GDPR’da Belirtilen İlgili Kişinin Hakları	
Bilgilendirilme Hakkı	Veri sorumlusu, yani verilerin denetleyicisi kullanıcıya basitçe ve açıkça kullanıcının verilerinin nasıl toplandığını ve işlendiğini anlatmalıdır. (m. 13,14)
Erişim Hakkı	Kullanıcılar web sitesinde kişisel verilerine göz atabilir ve onaylayabilir. Örneğin, kullanıcı alışveriş web sitesinde nereleri gezdiğini görebilir ve veri denetleyicisi bu hizmet için kullanıcıyı ücretlendiremez. (m. 15)
İtiraz Hakkı	Kullanıcı, veri denetleyicisini kişisel çıkarlarını temel alarak kişisel verileri işlemeyi reddetme hakkına ve ayrıca kişisel verilere dayalı pazarlamayı reddetme hakkına sahiptir. (m. 21)
Unutulma Hakkı	Bireyin zamanın geçmesine bağlı olarak geçmişteki verileri erişimden kaldırılmasını talep etme hakkı olarak tanımlanabilir. (m. 17)
Sınırlama Hakkı	Kullanıcı bir şikâyetle bulunduğunda (örneğin, verilerin doğruluğu ile ilgili), veri denetleyicisinin kullanıcı verilerini işlemeye devam etmesi kısıtlanabilir. (m. 23)
Veri Taşıma Hakkı	Kullanıcılar kişisel verilerin bir bilgi hizmeti sağlayıcısından başka bir bilgi hizmeti sağlayıcısına aktarabilir. (m. 20)
Düzeltilme Hakkı	Yanlış ya da eksik olan verileri düzeltme, güncel ve doğru şekilde saklanmasını isteme hakkıdır. (m. 16)

Otomatik Karar Vermeyi Reddetme Hakkı	Veri denetleyicisi ve işlemci, otomatik işlem (portreler dahil) yoluyla kararlar verir ve kullanıcıyı etkilerse, kullanıcı reddedebilir. (m. 22)
Hukuki Mercilere Başvurma Hakkı	GDPR’ın ihlalden kaynaklanan zararların tazminine ve veri sorumlularına uygulanacak yaptırımlara ilişkin ilgili kişinin başvuru hakkı bulunmaktadır. (m. 77- 84) Örneğin, Denetim Kurumuna Şikâyetle Bulunma Hakkı, Kanun Yollarına Başvurma Hakkı.

Tablo 12: GDPR’da Belirtilen Veri Sorumlusu ve Veri İşleyenin Yükümlülükleri

GDPR’da Belirtilen Veri Sorumlusu ve Veri İşleyenin Yükümlülükleri	
Varsayılan Ayarlarla Veri Koruma ve Tasarımla Veri Koruma	GDPR veri sorumlusuna kişisel verilerin korunması ilkelerine uyulmasına yönelik uygun teknik ve kurumsal önlemleri (tasarım da ve varsayılan ayarlarla) alma yükümlülüğü getirmiştir. (m. 25)
Ortak Veri Sorumluluğu	İlgili kişisel, yükümlülük dağılımı hangi şekilde yapılmış olursa olsun, GDPR’da kendisine tanınan hakları, ortak veri sorumlularından her birine karşı kullanabilir. (m. 26)
Temsilci Atama Yükümlülüğü	AB sınırları içinde kuruluşunun bulunmadığı hallerde, veri sorumlusu ya da veri işleyen, AB sınırları içinde bir temsilci atamakla yükümlüdür. (m. 27)

Talimatsız Veri İşlememe Yükümlülüğü	Veri sorumlusunun ya da veri işleyen talimatı altında çalışan ve kişisel verilere erişimi olan kişiler, veri sorumlusunun talimatı olmaksızın bu verileri işlememelidir. (m. 29)
Kayıtlarının Tutulması Yükümlülüğü	Veri sorumluları sorumlulukları dahilindeki işleme faaliyetlerinin kayıtlarını tutma ile yükümlüdür. (m. 30)
Denetim Kurumlarıyla İşbirliği Yükümlülüğü	Veri sorumluları, veri işleyenler ve varsa bunların temsilcileri, denetim kurumlarının bu yönde bir talebinin olması halinde, görevlerinin yerine getirilmesinde bu kurumlar ile işbirliği yapma ile yükümlüdür. (m. 31)
Kişisel Verilerin Güvenliğini Sağlama Yükümlülüğü	Veri işleme faaliyetinin güvenliğinin sağlanması ve bir veri ihlali söz konusu olduğunda, bu ihlalin denetim kurumuna ve ilgili kişiye bildirilmesi gerekmektedir. (m. 32 - 34)
Veri Koruma Etki Değerlendirmesi (VKED) Yükümlülüğü	VKED’inde veri işleme öncesinde planlanan işleme faaliyetlerinin kişisel verilerin korunması yönünden etkilerini değerlendirmelidir. (m. 35)
Veri Koruma Yetkilisi Atama Yükümlülüğü	Veri işleme faaliyetinin kamu kurumlarınca gerçekleştirildiği hallerde, bir veri koruma yetkilisi atanmalıdır. Maddede sayılan haller dışında veri koruma yetkilisi atanmasını gerektiren haller, AB ya da Üye Devlet hukukunda belirlenir. (m. 37)

2.5.3.3. Getirildiği Temel Yenilikler

2.5.3.3.1. Üst Seviyede Uyum Sağlaması

95/46/AT Sayılı Direktiften farklı olarak GDPR öncelikle bir Tüzük hükmündedir. Kapsam alanı ve yaptırım gücü bakımından farklılık göstermektedir. Tüzük, herhangi bir yerel yasa ve yönetmelik olmaksızın doğrudan üye devletler için geçerlidir. Öte yandan, direktifler kanun ve yönetmeliklerle ulaşılması beklenen temel hedefleri listelemekte ve bu hedeflere ulaşma yollarının seçimini üye devletlerin iç hukuklarına bırakmaktadır²⁷¹. GDPR tarafından sağlanan bu uyum kişisel verilerin korunmasının üye ülkeler arasında özel düzenleme yapmaksızın aynı kriterlerde yürütebilmesini sağlamıştır.

GDPR ile üye devletlerin veri koruma kanunu kurallarında tanınan haklardaki bazı geleneksel farklılıklar ortadan kaldırılmıştır. Örneğin, 95/46/AT Sayılı Direktifin hükümlerine uygun olarak, kullanıcılar verilerinin saklanması hakkında bilgi alma hakkına sahiptir. Ancak bu konuda üye devletlerin mevzuatı veri sorumlusu için farklı uygulama seçenekleri sunmuştur. GDPR bu tutarsızlığı ortadan kaldırmakta ve ilgili verilerin 20 gün içinde kullanıcılara ulaştırılması gerektiğini belirtmiştir.

2.5.3.3.2. Sorumlunun Çoğaltılması

95/46/AT Sayılı Direktif sadece veri sorumlusunun veri işleme ile ilgili kurallara uymak zorunda olduğunu ve yasa dışı iş ve işlemlerden sorumlu olduğunu belirtmiş. Başka bir ifadeyle, veri sorumlusunu sadece verini elinde bulunduran kişi olarak tanımlıyordu. GDPR’da ise sadece veri sorumlusu olmamakla birlikte bu verileri işleyenlerde verilerin hukuka uygun işlenmesinden sorumlu tutulmaktadır²⁷².

²⁷¹ Akıncı, **a.g.e.**, s. 13.

²⁷² **a.g.e.**, s. 14.

2.5.3.3.3. Uygulama Alanının Genişletilmesi

GDPR kişisel veri koruma düzenlemelerin küresel etkiye sahip olmasını sağlamıştır. GDPR'ın AB tarafından uygulanmış olması, bu düzenlemelerin yalnızca AB içinde yerleşik veri işlemcileri/sorumlu kişiler için bağlayıcı olduğu anlamına gelmez. Aksine dünyada hangi ülke/bölgeye hizmet verilirse verilsin, GDPR'ın uygulanması sürecinde, AB vatandaşlarına ve diğer ilgili kişilere ilgili verilerin yasal güvenliği sağlanmıştır²⁷³.

2.5.3.3.4. Sınır-Ötesi Aktarımının Sınırlanması

GDPR, AB vatandaşlarına ait kişisel verilerin sınır ötesi aktarımı konusunda daha katı düzenlemeler getirmiştir. İlgili kişi verilerin paylaşılmasını kabul etse bile, verilerin aktarıldığı ülkede/bölgede yeterli düzeyde koruma (yeterlilik şartı) sağlanmadığı durumda, verilerin AB dışına aktarılması yasaklanmıştır. Ayrıca, 95/46/AT Sayılı Direktif, veri sorumlusu için yeterlilik gereksinimlerini karşılayıp karşılamadığını değerlendirme yetkisi tanıdıysa da GDPR bu değerlendirme yetkisini yalnızca veri koruma kurumlarına tanıtmıştır.

Verilerin sınır-ötesi aktarım konusun AB ile ABD arasında gündem olmuştur. Temmuz 2000 yılında veri aktarma konusundaki ilk karar “Güvenli Liman (Safe-Harbor)” kabul edilmişti. Bu karar çerçevesinde, ABD’de bulunan kuruluşlar AB’den transfer edilecek veriler için uygunluk şartlarını yerine getirme ile yükümlüydü. Fakat bu karar 2015 yılında geldiğinde, Maximillian Schrems-Veri Koruma Komiseri²⁷⁴ davasındaki kararda ABAD tarafından geçersiz kılınmıştır. Bu karardan sonra ABD artık yeterli kadar veri güvenliği sağlayan ülke niteliğinde değerlendirilmiyordu. Bu uyumsuzluk sorunu Temmuz 2016’da “AB-ABD Gizlilik Kalkanı (Privacy Shield)”nın kabul edilmesiyle çözülmüş oldu. Fakat bu antlaşmada “Schrems II” olarak

²⁷³ a.g.e.

²⁷⁴ ABAD, C-362/14, Schrems, 13.11.2015.

adlandırılan karar ile iptal edilmiştir²⁷⁵. Temmuz 2020 tarihinde, ABAD kararında AB'den ABD'ye veri transferi yapılmasını sağlayan “Gizlilik Kalkanı” kararını yürürlükten kaldırdığını bildirmiştir.

2.5.3.3.5. Tazminat Talebi İmkânı

GDPR kişisel verilerin hukuka aykırı şekilde işleyenlere karşı ilgili kişilere tazminat talebi hakkı tanımıştır. Kişisel verilerinin işlenmesi sırasında zarara uğrayanlara toplu tazminat da dâhil olmak üzere, tazminat talebi hakkı tanımıştır.

2.5.3.3.6. Unutulma Hakkı

GDPR'nın getirdiği yenilikler arasında en çok tartışmalı ve önemli olanı unutulma hakkıdır. Nitekim unutulma hakkı internet bağlamında kullanıcıların oturumlarını kapatmasına ve çeşitli hesapları silmesine izin vermektir. İlgili kişi, verilerin artık ihtiyaç duyulmaması, ilgili kişinin iznini almamış olması veya ilgili kişinin verileri işlemek istememesi durumunda, kişisel verilerin mevzuata aykırı olarak silinmesini veya işlenmemesini talep etme hakkına sahiptir. Dolayısıyla unutulma hakkı, geçmişteki verilerin erişilebilir olması ile alakalı olması nedeniyle yanlış verilerin düzeltilmesine ilişkin düzenlemelerden farklıdır²⁷⁶. ABAD, 2014 yılında Google İspanya kararında unutulma hakkını koruyan karar vermiştir. Daha sonra yürürlüğe giren GDPR bu kapsamda ilgili kişiye unutulma hakkı tanımıştır.

Google-İspanya kararı, unutulma hakkının yasal makama ulaşıldığı ilk dava olarak kabul edilmektedir. Google-İspanya davası İspanyol vatandaşı Mario Costeja Gonzalez ve Google arasında gerçekleşmiştir. Davanın konusu Gonzalez ile ilgili haberin kısa yolunun arama motorundan silinmesi talebiydi. Gonzalez, uzun zaman

²⁷⁵ Deniz Gungor, “Avrupa Birliği’nden ABD’ye Yapılacak Veri Aktarımlarına İlişkin ‘Gizlilik Kalkanı’ Anlaşmasının İptali”, Mondaq, 30.10.2020, (Çevrimiçi) <https://www.mondaq.com/turkey/privacy-protection/989728/avrupa-birli287i39nden-abd39ye-yapilacak-veri-aktarimlarina-304li351kin-gizlilik-kalkani-anla351masin-304ptali> (Erişim Tarihi: 20.12.2020), par. 1.

²⁷⁶ Eren Sözüer, **Unutulma Hakkı: İnsan Hakları Hukuku Perspektifinden Bir İnceleme**, İstanbul: On İki Levha Yayıncılık, ss.7-29, s. 42-48.

önceki haberin kendisi ile alakasız olduğu gerekçesiyle arama motorundaki bağlantının silinmesi gerektiğini savunmuştur. ABAD, yasalara uygun olarak yayınlanan doğru bilgi olsa bile, uzun zaman söz konusu olduğunda yayınlamanın yasadışı hale gelebileceğine karar vermiştir²⁷⁷.

Bu durumda, arama motoru operatörlerine, bu tür bilgileri içeren web sitelerinin bağlantıları silme yükümlülüğü getirmiştir. Öte yandan, kararda arama motorlarının ve İnternet araç servis sağlayıcılarının veri sorumluları olarak görülmesi gerektiğine işaret edilmiştir.

2.5.3.3.7. Bilgilendirme Yükümlülüğü

GDPR, veri sorumlusunun kullanıcı haklarını ilgili kişiye bildirmekle yükümlü olduğunu belirtmiştir. Veri sorumlusu, kullanıcıları bilgilendirmek, yasal hakları konusunda gerekli hatırlatmaları yapmak ve yerine getirdikleri yükümlülükleri kaydetmekle yükümlüdür.

Veri ihlali riskinin yüksek olması durumunda veri sorumlusu, veri koruma otoritesine ve ilgili kişiye bildirimde bulunmakla yükümlüdür. Veri sorumlusu, bir veri ihlalinin meydana geldiğini tespit ettiğinde, hesap verebilirlik ilkesi uyarınca veri koruma otoritesine en kısa sürede bilgilendirmekle yükümlüdür²⁷⁸. Ayrıca veri sorumlusu, gerekli önlemleri alabilmek için ilgili kişiye söz konusu ihlal nedeniyle hak ve özgürlüklerinin tehdit altında olduğunu bildirmekle yükümlüdür.

2.5.3.3.8. Sıkı Yaptırım

GDPR veri ihlalleri ile ilgili katı yaptırımlar ve uygun mekanizmalar öngörmektedir. Veri koruma kurallarının ihlali durumunda, ağır tazminat yaptırımları

²⁷⁷ ABAD, C-131/12, Google Spain, 13.05.2014.

²⁷⁸ Akıncı, **a.g.e.**, s. 13.

ve uygun sorun çözme mekanizmaları öngörülmüştür²⁷⁹. Örneğin, Tablo 13'te GDPR'ın uyum sağlanmaması durumuna ilgili ceza miktarı yer almaktadır.

Tablo 13: GDPR'da Belirtilen İlgili Ceza Miktarı

10 milyon Euro veya Bir önceki mali yılında dünya çapındaki toplam yıllık cirosunun %2'si	20 milyon Euro veya Bir önceki mali yılında dünya çapındaki toplam yıllık cirosunun %4'ü
Varsayılan Ayarlarla Veri Koruma ve/veya Tasarımla Veri Koruma ile ilgili yükümlülüklerin ihlali.	GDPR kapsamında kabul edilen Üye Ülke yasalarının temel ilkelerin, ilgili kişinin haklarının veya yükümlülüklerinin ihlali.

2.5.3.3.9. Güçlendirilmiş Rıza

GDPR'ın 32 No'lu Resitalinde belirtildiği gibi, kullanıcı sessiz kalırsa veya çevrimiçi sosyal ağların veya web tarayıcılarının gizlilik ayarlarına itiraz etmezse, varsayılan ayarlar geçerli izin anlamına gelmemektedir. Çünkü kişisel verilerin belirli aydınlanmış amaçlar için işlenmesi özgürce, bilinçli ve açık bir şekilde kabul edilmesi gerekmektedir.

Temel değişiklik, ilgili kişinin bir açıklama yapması veya açık bir olumlu eylemde bulunması ve rızanın geçerli kabul edilmesidir. Bireysel sessizlik, önceden kontrol edilmiş seçenekler, statik durum vb. bireyin rızasını ifade ettiğini belirlemek için yeterli değildir. GDPR ayrıca, rızanın ilgili kişi tarafından serbestçe verilmediği

²⁷⁹ a.g.e., s. 16.

koşulları da içermiştir. Veri sorumlusu ayrıca ilgili kişiyi rızayı geri çekme hakkı konusunda bilgilendirme ile yükümlü tutulmuştur.

2.5.3.3.10. Taşınabilirliği Hakkı (Data Portability)

GDPR’ın 20. Maddesi, 95/46/AT Sayılı Direktifin kapsamadığı veri taşınabilirliği hakkını ilk kez tanımlamıştır. İlgili kişi, kişisel verilerini bir veri sorumlusundan diğerine kaydetme hakkına sahiptir.

2.5.3.3.11. Veri Koruma Kurulu, Görevlisi ve Veri Koruma Etki Değerlendirmesi

GDPR ile getirilen bir diğer önemli yenilik, Madde 29 Çalışma Grubu’nun yerine “Veri Koruma Kurulu (European Data Protection Board)”nın oluşturulmasıdır. Avrupa Veri Koruma Kurulu’nun oluşturulması GDPR’ın AB sınırları içerisinde etkin bir şekilde uygulanmasını güvence altına almada önemli rol oynamaktadır.

GDPR’ın 37. maddesinde bazı durumlarda veri sorumlusunun kendi bünyesinde bir Veri Koruma Görevlisi belirlemesini zorunlu kılmaktadır. Bu yeni düzenlemede, özellikle veri işleme faaliyetlerinde yeni teknolojik veri işlemenin gerçek kişilere yüksek riskler getirebileceği durumlarda, söz konusu veri işlemenin kapsamı, niteliği, geçmişi ve amacı dikkate alınarak, GDPR’a uyum sağlayabilmesi amacıyla veri sorumlusunun “Veri Koruma Etki Değerlendirmesi (VKED)” yapması gerekmektedir. Aynı maddenin ikinci fıkrasında, VKED’nin hangi koşullar altında gerekli olduğunu (örneğin, otomatik veri işleme sistemleri kullanmak, hassas verileri veya ceza mahkumiyetleri ve suçlarıyla ilgili verileri işlemek) ayrıntılarıyla anlatmaktadır.

2.5.3.3.12. Varsayılan Ayarlarla Veri Koruma ve/veya Tasarımla Veri Koruma

GDPR’ın Resital bölümünde, kişisel verilerin işlenmesinde gerçek kişilerin hak ve özgürlüklerinin korunması için gerekli teknik ve organizasyonel önlemlerin alınması beklenmektedir. Bu durumda veri sorumlusunun iç işleyişi için strateji belirleyerek, “Varsayılan Ayarlarla Veri Koruma (Data Protection by Default)” ve

“Tasarımla Veri Koruma (Data Protection by Design)” ilkelerini gerçekleştirmek için gerekli önlemleri alması gerektiğini vurgulamıştır.

Varsayılan Ayarlarla Veri Koruma ve/veya Tasarımla Veri Koruma, yapay zekânın oluşturduğu risklere karşı temel çözümler olarak kabul edilmektedir. GDPR’ın madde 25’e bu ilke dahil edilmiştir. Madde 25 (1), veri sorumlusunu GDPR gerekliliklerini karşılamak ve ilgili kişilerin haklarını korumak için takma adlandırma veya veri minimizasyonu gibi uygun teknik ve organizasyonel önlemleri uygulamaya yükümlü kılmıştır. Madde 25 (2), veri sorumlusunun, varsayılan olarak, uygun teknik ve organizasyonel önlemleri uygulamasını gerektirmiştir. Ancak bu hükümlerin tümü, veri sorumlusunun kimliğinin açık olması ve yapay zekâ ürünlerinin insan denetimine tabi olma koşulunun yerine getirilmesi koşuluyla geçerli olabilmektedir. Bu nedenle yapay zekâ çağında kişisel verilerin korunması açısından eksiklik oluşturmaktadır.

2.5.3.4. Karşılaştığı Sorunlar

Viktor Mayer-Schönberger ve Yann Padova, GDPR’ı yapay zekâ ve büyük veri perspektifinden değerlendirmiş ve günümüzde önemli miktarda veri analizinin yapay zekâ tarafından yapıldığını var saymıştır. İlgili çalışmalarında GDPR’ın yapay zekâ çağındaki üç sorununu tanımlamıştır. Birinci sorun, kullanım amacı ve yeniden amaçlandırma sorunu. İkincisi izin verilebilir veri toplama sorunu. Üçüncüsü ise veri saklama sorunudur²⁸⁰.

Yeniden amaçlandırma, ilgili kişinin rızası ve kişisel verilerin istatistiksel amaçlarla işlenmesinin muafiyeti ile ilgilidir. GDPR, kişisel verilerin yeniden kullanım amacını veri toplama sırasındaki orijinal amaçla sınırlamaktadır. GDPR açık rıza gerektirdiğinden, gelecekteki olası veri kullanımları dahil olmak üzere geniş olarak tanımlanmış amaçları kısıtladığından ve madde 4 (11), 6 (1) uyarınca ilgili

²⁸⁰ Viktor Mayer-Schönberger ve Yann Padova, “Regime change? Enabling big data through Europe’s New data protection regulation”, **Columbia Sci Technol Law Review**, C. 17 (2016), ss. 315- 335, s. 315.

kişinin rızasının istediği zaman geri çekilmesine izin verdiğinden, ilgili kişinin rızasını almak zor hale gelmiştir. Nitekim bu sorun AB ile ABD ve Çin arasındaki yapay zekâ çağı teknolojilerde mukayeseli olarak dezavantaja düşmesine sebep olmuştur. Öbür iki dev teknoloji ülkesi ise veri toplama, kullanma konusunda AB'ye göre daha yumuşak yasalara sahiptir diyebiliriz. GDPR bir taraftan veri kullanım amaçlarına sınırlama getirirken, öbür taraftan anlamı geniş tanımlanabilen madde 5 (1) (b)' de "istatistiksel amaçlar" termi kullanarak daha fazla verinin işlenmesine izin vermiştir. Bir yandan açık rıza şartı ile verilerin toplanmasını sınırlarken öbür yandan geniş tanımlanabilen terimler ile verilerin toplanmasına izin vermiştir.

Schönberger ve Padova, izin verilebilir toplamayı da sorunlu olarak görmüştür. Onlar GDPR'ın, 95/46/AT Sayılı Direktifin geleneksel rejimini benimseyen, veri toplama için özel amaçlar gerektiren ve üye devletlere verilen takdir yetkisinin kapsamı oldukça sınırlı olan yasa olduğunu savunmuştur. Veri saklama, ilke olarak, işlemenin birincil amacı için gerekli olduğu sürece izin verilebilirdi. "İstatistiksel amaçlar" istisnası, madde 5 (1) (b)' de şart koşulmuş ve hem saklama hem de yeniden kullanım için geçerli olacak şekilde düzenlenmiştir.

Schönberger ve Padova, GDPR'ın verilerin yeniden kullanımını ve daha uzun süre saklanmasını sağlayarak sınırlı ama dikkate değer bir ilerleme içerdiğini düşünmüştür. Bir başka yandan ise, toplama sınırlamalarının yapay zekâ ve büyük veri kullanımını ciddi şekilde caydırdığını değerlendirmiştir. Bu bağlamda, Avrupa veri koruma rejimini yapay zekâ bağlamına daha uyumlu hale getirmek için koleksiyon temelli mekanizmalardan kullanıma dayalı mekanizmalara geçmeye hazır olması gerektiğini ileri sürmüştür. Veri işleme kuruluşlarına açık bir hesap verebilirlik görevi yüklemek ile birlikte bu tür kuruluşların hem faydalar hem de potansiyel riskler dahil olmak üzere kapsamlı bir değerlendirme yapmaları gerektiğini savunmuşlardır²⁸¹.

²⁸¹ a.g.m., s. 332.

GDPR kapsamındaki bir diğer sorun ise kara kutudur. Yukarıda belirtilen GDPR'ın maddeleri veri denetleyicileri için şeffaflığı şart koşturmaktadır. Bu, yapay zekâ kullanan şirketlerin, kişisel verilerinin yapay zekâ programı tarafından nasıl işlendiğini, olası sonuçlarının neler olduğunu vb. ilgili kişiye açıklamaları gerektiği anlamına gelmektedir. Bu bağlamda, Avrupa Veri Koruma Denetçisi (EDPS), girdi verilerini veya belleği bir sinir ağındaki ağırlıklar olarak sınıflandırmak için kullanılan makine öğrenimi algoritma kriterlerinin çoğu durumda insanlar için anlaşılabilir olmadığını vurgulamıştır.

GDPR'ın yapay zekâ çağında karşılaştığı en büyük eleştiriler aslında AB çerçevesinde yapay zekâ teknolojilerinin ilerlemesini engelleme yönündedir. Nitekim ilgili konuda rakipleri olan ABD ve Çin kişisel verilerin korunması konusunda GDPR kadar geniş çerçeveli, kapsamlı ve katı uygulama getirmiş değildir. Bu nedenle yapay zekâ teknolojilerinin ilerlemesinde AB'ye göre daha rahat denilebilir.

AB ise tam tersine yapay zekâ konusunda muhtelif zorluklara maruz kalması endişe uyandırmaktadır. Örneğin, GDPR'ın şirketlerin önemli algoritmik kararları manuel olarak incelemesini zorunlu kılması (m. 22), yapay zekânın genel maliyetini artırır. Unutulma hakkı (m. 17) veriden beslenen yapay zekâ sistemine zarar verebilir. Verilerin tekrar kullanımını yasaklanması (m. 6), yapay zekâ alanındaki yenilikçiliğini sınırlandıracak. Yeterli kadar açıklanmamış kurallar, şirketlerin anonimleştirilmiş verileri kullanma isteğini yok edebilir.

Kısacası, GDPR'ın günümüzdeki karmaşıklığı, yapay zekâ kullanım maliyetini göreceli bir şekilde artıracaktır. AB'nin karşılaştığı bu sorunlar uluslararası üstünlük rekabetinde AB'yi özellikle yapay zekâ alanında teknoloji açıdan dezavantaj durumunda bıraktığı söylenebilir.

2.6. Karşılaştırmalı Hukuktaki Düzenlemeler

Bu başlık altında BT sektöründe dünyada lider konumunda olan, özellikle çalışmanın konusu olan yapay zekâ alanında önde gelen ABD'nin kişisel verileri

koruma konusundaki düzenlemeleri; yapay zekâ alanında en büyük yatırıma ve çok fazla veriye sahip olan Çin'in ilgili düzenlemeleri; son olarak da ülkemiz Türkiye'nin kişisel veri düzenlemeleri ele alınacaktır. Hatırlatılması gerek olan hususlardan biri ABD ve Çin yasal kaynaklarında "Kişisel Veri" kavramı yerine "Kişisel Olarak Tanımlanabilir Bilgi" (PII), "Kişisel Bilgi" (Personal Information) sözcükleri kullanılması nedeniyle ilgili başlıklarda asıl tercüme esas alınarak "bilgi" kelimesi kullanılmıştır.

2.6.1. ABD'de Kişisel Bilgilerin Korunması

2.6.1.1. Mahremiyetin Korunmasının Ortaya Çıkışı

Günümüzde ABD hem mahremiyet hakkının kurucusu hem de en yenilikçi BT ülkesi olarak bilinmektedir. Yapay zekâ ekosistemi, çoğunlukla Google Inc., IBM Corp., Microsoft Corp, vb. şirketlerinden oluşmaktadır. Günümüzde ABD'de yapay zekâ ile ilgili tartışmalar hem hükümet düzeyinde hem de akademik düzeyde ilerlemektedir.

ABD'de hukuk düzenlemelerinin AB'ye göre farklı kaynaklardan beslendiği görülmektedir. Bu farklılıklar arkasında genel anlamda üç etkenin olduğunu söyleyebiliriz. Birinci, federal anayasa federal devlet, federe devlet ve yerel birimler arasındaki hiyerarşik kuvvet ayrımıdır. Bu nokta AB'nin tek çatı altına toplanan sisteminden çok farklıdır. İkincisi, ABD'de James Madison'un fikirlerinin etkisi ile Anayasada federal düzeyde yasama, yürütme ve yargı işlemlerinden sorumlu yönetim sistemi benimsenmiştir. Üçüncüsü ise Anglo-Sakson geleneğidir. ABD hukuki teamüllerin farklı yorumlanması ve icrasından ve yargılama üslûndeki belirgin sübjektiflikten kaynaklanan farklı içtihat hukuka sahiptir²⁸².

²⁸² Fred H. Cate, **Privacy in the Information Age**, Washington: Brooking Institution Press, 1997, s. 49.

Genel olarak bakıldığında, mahremiyet hakkı kavramının ABD’den geldiği bilinmektedir. 1890’da Warren ve Brandis ilk olarak mahremiyet kavramını öneren “Mahremiyet Hakkı” (The Right to Privacy) makalesini yayımlamıştır. Kaleme aldığı makalesinde “mahremiyet, hayatta kalma hakkına ek olarak, giderek yaşama müdahale etmekten kurtulma hakkı anlamına gelmektedir ve herkes, düşüncelerinin, görüşlerinin ve duygularının başkalarıyla ne ölçüde paylaşıldığına karar verme hakkına sahiptir” demiştir²⁸³. O zamandan beri, mahremiyet hakkı ABD’de büyük ilerleme kaydetmiştir ve mahremiyet hakkının çağrışımı da zenginleştirilmiştir.

İlk başta, mahremiyet hakkı temel olarak bireyin özel yaşamının huzurunu korumak için kullanılan ve erişilebilirlik gizliliği olarak gösterilen bir “Bireysel Yalnız Kalma Hakkı” (Accessibility Privacy) olarak kabul ediliyordu. Daha sonra, mahremiyetin kamu gücü tarafından ihlal edilmesini önlemek için, mahremiyet hakkı anayasal düzeyde, bireysel özgürlüğe bağlı olarak temel bir hakka yükseltilmiş ve mahremiyete kendi karar verme hakkı (Decisional Privacy) yavaş yavaş mahremiyet kategorisine dahil edilmiştir²⁸⁴.

Anglo-Sakson hukukunda, 1960’lardan sonra bilgisayarların popüler hale getirilmesiyle Anayasa tarafından güvence altına alınan haklar olarak kişisel bilgilerin korumaya yönelik mevzuat da geliştirilmiştir. Buna karşılık, öğretide mahremiyet hakkı başlangıçta “Benim Hakkıma Karışma” şeklinde anlaşılmışsa²⁸⁵ daha sonra

²⁸³ Samuel D. Warren ve Louis Brandeis, **The Right to Privacy**, Boston: Harvard Law Review, 1890, s. 193.

²⁸⁴ Zhang Xinbao, “从隐私到个人信息: 利益再衡量的理论与制度安排 (Gizlilikten Kişisel Bilgilere: Faydaların Yeniden Değerlendirilmesine Yönelik Teoriler ve Kurumsal Düzenlemeler)”, **中国法学** (Chinese Journal of Law), 2015, ss. 38-59, s. 42.

²⁸⁵ Vincent R. Johnson, Zhao Xiuwen tercümesi, **美国侵权法(American Tort Law)**, Pekin: Çin Renmin Üniversitesi Yayınları, 2004, s. 167.

“Kişisel Bilgilerini Kendi Kontrol Etme Hakkı” na dönüştürülmüş daha sonra “Kaderini Tayin Etme” şeklinde pozitif içerik kazanmıştır²⁸⁶.

Aynı şekilde, 1980’lerde internet teknolojisinin gelişmesiyle birlikte, kişisel bilgilere yapılan ihlal olgusu büyük ölçüde artmış ve bilgi mahremiyeti (Informational Privacy) mahremiyet korumasının en önemli noktası haline gelmiştir. Günümüzde ABD kendine özgü bir “mahremiyet” koruma modeli oluşturmuştur²⁸⁷. İnternet çağında kişisel bilgilerin korunması ile ilgilenmek için yasal mahremiyet koruma sistemini sürekli olarak zenginleştirmiştir.

Mahremiyet hakkı, ABD’de son yıllarda içeriğini genişleten ve yavaş yavaş Alman hukukunda “Genel Kişilik Hakkı” na benzer bir işlevi üstlenen kolektif bir kavram haline gelmiştir. ABD’de “mahremiyet” kavramının belirsizliği, orada tanımlanan kişilik hakkı kavramının içeriği ile ilgilidir. ABD’de bilgi toplumu geliştikçe, kişisel bilgilerin özerkliği mahremiyetin korunmasının önemli bir parçası haline gelmiştir²⁸⁸.

ABD’de ana bilgi koruma yöntemi endüstrinin kendi disiplindir. Hükümet denetimi bilgi haklarının korunmasında sadece yardımcı bir rol oynamaktadır. Endüstrinin öz disiplini, anti-tröst kurallarını ihlal etmeden gönüllü anlaşmalar ve diğer yöntemlerle işletmelerin öz-denetimini ifade etmektedir²⁸⁹.

Kısacası vatandaşlarının bilgilerini bir dizi farklı düzenlemeyle korunmaktadır. Federal Ticaret Komisyonu (FCC) internet servis sağlayıcılarının veya ISS’lerin hangi verileri satıp satamayacağına ilişkin kurallardan sorumluyken. Federal Sağlık

²⁸⁶ Zhou Yuntao ve Zeng Xianyi, 论宪法人格权与民法人格权: 以德国法为中心的考察 (Anayasal Kişilik Hakları ve Medeni Hukuk Kişilik Hakları Üzerine: Alman Hukukuna Merkezli Bir Araştırma), Pekin: Çin Renmin Üniversitesi Yayınları, 2010, s. 94.

²⁸⁷ Bkz: Herman T. Tavani, **Ethics & Technology: Controversies, Questions, and Strategies for Ethical Computing**, Wiley, 2015, ss. 117- 119.

²⁸⁸ He Xuxu, **a.g.m.**, s. 64.

²⁸⁹ Reyina Yilihamu, “各国数据保护的的特色及对我国的启示 (Mukayeseli Hukukta Veri Korumanın Özellikleri ve Öneriler)”, 中国市场 (China Market), (2020), ss. 188-189, s. 189.

Sigortası Taşınabilirlik ve Sorumluluk Yasası sağlık verileri korumaktadır. Çocukların Online Verilerini Koruma Yasası (COPPA) ise çocuklar hakkında bilerek kişisel veri toplamasını düzenlemektedir²⁹⁰.

Bununla birlikte, BT teknolojisinin gelişmesiyle, mahremiyet hakkının çağrışımı da sessizce gelişmekte ve değişmektedir. İnternet ve bilgi toplumu tarafından getirilen kişisel bilgilerin toplanması, işlenmesi ve kullanılması için Amerikalı yasa koyucular hem sınır ötesi ticarete hem de e-ticarete fayda sağlamayı ve kişisel gizliliği korumayı ummaktadır. Bu amaçla ABD’li yetkililer, uygulama topluluğu ve tüketici gruplarıyla diyalog sağlayarak tüketici haklarını korumak için öz disiplini teşvik etmiştir. ABD hükümeti ayrıca kişisel mahremiyet ve yüksek derecede özel ve hassas bilgileri içeren temel alanlar için aktif olarak mevzuat hazırlamaktadır²⁹¹.

Özetle, ABD’de federal yasalar açısından mahremiyetin korunması için asgari gereklilikler belirleyen kapsamlı yasalar olmasa da sektörel ferdi yasal koruma yöntemleri yaygın olarak kullanılmaktadır. Kısacası, ABD’de kişisel bilgilerin korunması anayasal bir haktan ötürü, sektörel bir çözüm niteliğindedir.

Kişisel bilgilerin korunmasında ekonomik değeri temel alan bir yaklaşım benimseyen ABD yaklaşımı kapsamlı korumanın ekonomi üzerinde olumsuz bir etkisi olacağından etkilenmiştir. Bu görüş kişisel bilgilerin mülkiyet hakkı niteliğinde değerlendirdiği için ilgili kişinin mülkiyet sahibine tanınan haklardan yararlanmasını sağlamaktadır²⁹². Dolayısıyla ABD’de kişisel bilgiler, mülkiyet hakkının sağladığı satın alma ve kiralama gibi ilişkilerin konusu olabilmektedir. ABD’de bir diğer yaygın

²⁹⁰ Adèle Azzi, “The Challenges Faced by the Extraterritorial Scope of the General Data Protection Regulation”, **Journal of Intellectual Property, Information Technology and Electronic Commerce**, C. 9, S. 2 (2018), ss. 126- 138.

²⁹¹ He Xuxu, **a.g.m.**, s. 69.

²⁹² İbrahim Korkmaz, **Kişisel Verilerin Ceza Hukuku Kapsamında Korunması**, Ankara: Seçkin Yayıncılık, 2017, s. 78.

görüş ise kişisel bilgilerin fikri mülkiyet hakkı ile ilişkilendirilen görüştür²⁹³. Bu görüş kişisel bilgilerin telif hakkına benzer bir yaklaşım ile korunması gerektiğini savunmaktadır.

ABD Anayasasında öngörülen hakların genellikle vatandaşları sadece devlet eylemlerinden koruduğu belirtilmelidir. Özel hukuk kişiler arasındaki ilişki yalnızca köleliği yasaklayan on üçüncü tadil ile doğrudan düzenlenebilir. Anayasanın verdiği diğer tüm haklar özel sektörü değil kamu sektörünü düzenlemektedir. Devlet eylemlerinin yokluğunda, özel hayatın mahremiyetinin düzenlenmesi konusunda anayasal haklar ciddiye alınmamıştır²⁹⁴.

ABD Yüksek Mahkemesi ise mahremiyet kavramını mahremiyetin korunmasının Anayasanın kişisel haysiyetinin ve özgürlüğünün değerini içerdiğini vurgulayarak yorumlamış ve uygulamıştır. Daha da önemlisi, ABD Yüksek Mahkemesi, mahremiyetin korunmasını dava tespitiyle genişletmiştir. Whalenv Roe davasında²⁹⁵, kişisel bilgileri devlet tarafından toplanan bazı hastalar ve doktorlar New York Eyaleti yasasının özel ilaç reçetelerinin bilgisayarlarda kaydedilmesini ve saklanmasını gerektirdiği nedeniyle bu yasal hükümlerin Anayasa'yı ihlal ettiğini ileri sürmüştür. New York Bölge Mahkemesi, yasanın ilgili maddelerin anayasaya aykırı olduğuna karar vermiş ve itiraz edilen hükümlerin uygulanmasını yasaklamıştır²⁹⁶.

Temyiz aşamasında ABD Yüksek Mahkemesi, ilgili yasanın eyaletin polis yetkisi dahilinde olduğuna hükmederek bölge mahkemesinin kararını iptal etmiştir. ABD Yüksek Mahkemesi, tehlikeli uyuşturucuların kullanımının ve dağıtımının kontrolünün polis gücünün uygun bir şekilde kullanılması olduğuna ve saklanan bilgilerin doktorlara, sigorta şirketlerine veya kamu sağlığı birimlerine ifşa

²⁹³ Küzeci, **a.g.e.**, s. 64.

²⁹⁴ Cennet Uslu, **Doğal Hukuk ve Doğal Haklar: İnsan Haklarının Felsefi Temelleri**, Ankara: Liberte Yayınları, 2009, s. 35.

²⁹⁵ Bkz: Whalen v. Roe, 429 U.S. 589, 1977.

²⁹⁶ Bkz: Roe v. Ingraham, 403 F. Supp. 931, S.D.N.Y. 1976.

edilmesinin veya adli işlemlerde delil olarak sunulmasının Anayasa ile güvence altına alınan mahremiyet hakkının ihlali teşkil etmediğini belirtmiştir. Her ne kadar doktorların ve hastaların anayasa davaları yasal menfaatler ve politika hususları ile desteklenmese de bu dava ABD Yüksek Mahkemesi’nin anayasal bilgi mahremiyet hakkını doğrulayan ilk kararı haline gelmiş ve günümüzde büyük önem taşımaktadır²⁹⁷.

2.6.1.2. ABD Mahremiyet Koruma Düzenlemeleri

Tablo 14: ABD Mahremiyet Koruma Yasal Düzenlemeleri

Tarih	Kanun Değişikliği ve İçtihatlar	Mahremiyet Kavramı İçeriği
1792	Anayasa’nın Dördüncü Değişikliği, hükümetin herhangi bir kişisel ve özel mülke (taşınır ve taşınmaz mülk dahil) makul olmayan bir şekilde el koymasını yasaklamıştır.	Birinci aşama: bireylerin varlığın (fiziksel, iletişim)
1890	Wallen “Mahremiyet Hakları” nı yayımlanmış ve bireylerin “yalnız kalma hakkına” sahip olması gerektiğini önerilmiştir.	
1966	“Bilgi Edinme Özgürlüğü Yasası” (Freedom of Information Act), devlet kurumlarının mümkün olduğunca bilgiyi kamuya açıklamasını zorunlu kılmıştır.	
1967	Charles Katz v. ABD Davası ²⁹⁸ ABD Yüksek Mahkemesi, hükümetin bireylerin iletişimlerini dinlemesinin hukuk dışı arama ve müsadere teşkil edebileceğine, Anayasanın Dördüncü Değişikliği	

²⁹⁷ Li Zhenshan, 人性尊严与人权保障 (İnsan Onuru ve İnsan Haklarının Korunması), 元照出版社, 2001, s. 53.

²⁹⁸ Katz v. United States, 389 U.S. 347 (1967).

	ile ima edilen mahremiyet hakkını kabul etmiş ve kişisel mahremiyet ihlalinin korunması gerektiğine karar vermiştir.	yasadışı erişimini önleme
1970	Özel sektördeki ilk yasa olan “Adil Kredi Raporlama Yasası (Fair Credit Reporting Act)” tüketicilere yanlış verileri düzeltme hakkını tanımıştır.	
1973	“Adil Bilgi Uygulaması (Fair Information Practice)”, ABD Sekreterinin Otomatik Kişisel Veri Sistemleri Danışma Komitesi tarafından önerilmiş, bireyler hakkında bilgi içeren otomatik veri sistemlerinin artan kullanımına yanıt olarak yayınlanmıştır.	
1974	1974 “Mahremiyet Yasası” (Privacy Act of 1974): kişisel bilgilere erişim hakkı, bilgi toplamanın amacı, gizli dosyaların saklanması konuları düzenlenmiştir.	
1977	ABD Yüksek Mahkemesi bilgi mahremiyet hakkını ilk kez tanımıştır. Roe v. Wade davası ²⁹⁹	
1980	“Finansal Mahremiyet Hakkı Yasası (RFPA)”, ABD v. Miller davası Yüksek Mahkeme kararına bir yanıt olarak ve Banka Gizlilik Yasası’na ek olarak kabul edilmiştir. Gazetecileri ve haber merkezlerini hükümet yetkilileri tarafından yapılan aramalardan koruyan Gizlilik Koruma Yasası kabul edilmiştir.	

²⁹⁹ Roe v. Wade, 410 U.S. 113 (1973)

1986	“Elektronik İletişim Gizlilik Yasası (Electronic Communications Privacy Act)”	İkinci aşama: Kişisel bilgilerin zararlı şekilde ifşa edilmesini önleme
1988	“Video Gizliliğini Koruma Yasası (Video Privacy Protection Act)”	
1994	“Sürücü Gizliliği Koruma Yasası (Driver’s Privacy Protection Act)”	
1996	“Sağlık Sigortası Taşınabilirlik ve Sorumluluk Yasası (Health Insurance Portability and Accountability Act)”	
1999	“Finansal Hizmetler Modernizasyon Yasası (Gramm Leach Bliley Act)”	
2000	“Çocukların Çevrimiçi Gizliliğini Koruma Yasası (Children’s Online Privacy Protection Act)”	
2018	“Kaliforniya Tüketici Gizliliği Yasası (CCPA)”	

Kaynak: Yazar Tarafından Oluşturulmuştur

Yukarıdaki temelde, ABD bazı alanlarda mahremiyetin korunması için yasalar oluşturmuş ve nihayetinde mahremiyet hakkının genel olarak aşağıdaki üç alanda düzenleme sistemini oluşturmuştur: Birincisi, bilgi mahremiyeti haklarının anayasa ve yasalar yardımıyla genel anlamda korunmasıdır. Örneğin: Kişisel bilgilerin devlet kurumları tarafından işlenmesini düzenleyen “Gizlilik Yasası”. İkincisi, hassas kişisel bilgilere ve çocuklar gibi mahremiyet haklarının ihlal olma riski yüksek olan gruplara yönelik özel mahremiyet yasası oluşturmalarıdır. Üçüncüsü, “Federal Ticaret Komisyonu Yasası”nın kişisel bilgileri “yasa dışı ve aldatıcı davranış”

perspektifinden koruması ve ticaret alanlıda bilgi mahremiyeti ve veri güvenliğini denetlemesi.

2.6.1.3. Kaliforniya Tüketici Gizliliği Yasası

Günümüzde ABD’deki en kapsamlı mahremiyet hakkı yasası, Haziran 2018’de Kaliforniya eyaletinde kabul edilip, 1 Ocak 2020’de yürürlüğe giren Kaliforniya Tüketici Gizliliği Yasası (CCPA) dır. CCPA Kaliforniya’daki tüketicilere sadece bilgilerinin üçüncü bir tarafa satılıp satılmadığını öğrenme hakkını değil, aynı zamanda işlemi engelleme hakkına da tanımıştır. Ancak daha önce bahsedildiği gibi, bu “en sağlam” yasa bile teknoloji şirketlerinin nasıl verileri elde edebileceğini ve kullanıcı verilerini nasıl kullanabileceğini düzenleyememektedir. Bu durumu teknik yazar Charlie Warzel New York Times gazetesinde yaptığı şu yorumundan anlamamız mümkündür: “*ilgili şirketler gizlilik yasalarına uyduklarını söylerler ancak düzenleyicilerin onları hiç gözden geçirmeyeceklerini de biliyorlar*”³⁰⁰.

CCPA’nın ilgili kişilere tanıdığı beş ana hak Tablo 15’de yer almaktadır:

Tablo 15: CCPA’nın İlgili Kişilere Tanıdığı Haklar

Bilgi Edinme Hakkı	Kullanıcılar, şirketlerden kişisel olarak tanımlanabilir bilgilerin (PII) türü, kaynağı, kullanımı ve üçüncü tarafa paylaşılıp paylaşılmadığı dahil olmak üzere kişisel veri toplama ve satışlarını açıklamalarını talep etme hakkına sahiptir.
Kopya Talep Etme Hakkı	Kullanıcılar, şirketlerden son 12 ay içinde toplanan kişisel tanımlanabilir verilerin kopyalarını talep etme hakkına sahiptir.

³⁰⁰ Wu Yangyang, “IBM 宣布退出人脸识别, 是道德楷模还是商业投机? (IBM, Yüz Tanımadan Çekildiğini Duyurdu: Etik Bir Model Mi Yoksa Bir İş Spekülasyonu Mu?)”, 19.06.2020, (Çevrimiçi) <https://tech.sina.com.cn/i/2020-06-19/doc-iircuyvi9289158.shtml?cref=cj>, (Erişim Tarihi: 02.07.2020).

Silinme Hakkı	Kullanıcılar, şirketten toplanan kişisel tanımlanabilir verileri silmesini talep etme hakkına sahiptir.
Reddetme Hakkı	Kullanıcılar, şirketlerden kişisel verilerini satılmamasını talep etme hakkına sahiptir.
Ayrımcılık Görmeme Hakkı	Kullanıcılar, ayırım gözetmeksizin yukarıdaki hakları kullanma hakkına sahiptir.

CCPA’i GDPR’ın ABD versiyonu niteliğinde diyebiliriz. Nitekim her iki yasa ilgili kişilere benzer haklar tanımıştır. Toplanan kişisel bilgilere erişim ve silme hakkı, kişisel bilgilerin kullanımında şeffaflık isteme hakkı ve hizmet sağlayıcıları ile imzalanan sözleşmenin temin edilmesini isteme hakkı gibi. Öte yandan GDPR ile CCPA arasında farklılıklar da bulunmaktadır. GDPR’dan farklı olarak, CCPA, şirketlerin hassas bilgileri toplamak ve kullanmak için yasal bir temele sahip olmasını zorunlu kılmamaktadır. Aynı zamanda ABD dışındaki bilgi aktarımına kısıtlamalar yapmıyor ve şirketlerin etki değerlendirmeleri yapmak için veri koruma görevlileri atmasını zorunlu kılmamaktadır. Son olarak, CCPA, kullanıcıların yalnızca son 12 ayda toplanan kişisel bilgilere erişebileceğini destekleyerek hizmet sağlayıcıların nispeten daha az yükümlülüğünü belirtmiştir.

Bir diğer husus, CCPA’nın bazı yönlerde GDPR’dan daha kısıtlayıcı olmasıdır. Özellikle hassas bilgilerin tanımı konusunda CCPA daha geniş düzenleme sağlamıştır. CCPA’nın tanımında hassas bilgiler, tüketici biyometrik verilerini, web tarama verilerini, satın alınan veya satın alınması düşünülen ürünleri, coğrafi konumu, akademik bilgileri, istihdam bilgilerini ve kişisel tercih bilgilerini oluşturmak için kullanılabilecek tüm çıkarımları dahil etmektedir. CCPA’ı bilgilerin ticari kullanımını düzenleme ve “kişisel bilgileri” geniş bir şekilde yorumlama (aile ve bireyler ile ilgili

bilgileri, aygıt bilgileri “kişisel bilgiler” kategorisine dahil etmiştir) açısından şüphesiz ABD’nin gizlilik koruma standartlarını yükselten yasa olduğunu söyleyebiliriz.

Şirketler açısından bölgesel bir düzenleme olarak ortaya konulan CCPA, sadece Kaliforniya’da uygulama ile sınırlı değildir. E-ticaret ile ilgili bir örnek vermek gerekirse, e-ticaret sitesi Kaliforniya’da kurulmasa bile, sitenin CCPA düzenlemelerine uyması gerekmektedir. Çünkü yasa siteden alışveriş yapan Kaliforniya sakinleri için kullanılacaktır. Sonuç olarak, CCPA’nın etkisinin kapsamı büyük ölçüde genişletilmiştir ve eyaletler arası hatta çok uluslu şirketlerin bunu uyumluluk sağlaması gerekmektedir.

2.6.2. Çin’de Kişisel Bilgilerin Korunması

Çin 2018 yılında yapay zekâlı haber sunucusunu duyurmuştu, bir sene sonra ise yapay zekâ hakimlerini göreve başlattığını ilan etti³⁰¹.

Bu noktada Çin’i mesleklerin yapay zekâyâ devri konusunda son derece aktif şekilde ilerlemekte diyebiliriz. Diğer taraftan, Çin’in kişisel bilgileri koruma konusunda mukayeseli düzenlemelere göre daha geç adım attığı söylenebilir. Çin’in kişisel verileri toplama konusundaki, bir diğer ifade ile dünyanın veri bankası hükmünde olması kişisel verilerin korunması düzenlemelerini gerekli kılmıştır ve hızlı bir şekilde düzenlemelerini güncellemektedir.

Çin kişisel veri koruma düzenlemelerine baktığımızı zaman genel olarak Kara-Avrupa hukuk sistemini benimsemesine rağmen, ABD yasal düzenlemelerine benzeyen yaklaşım sergileyerek kişisel bilgi kavramını kullandığı görülmektedir³⁰². Çinli veri bilim adamı Mei Shaozu, “kişisel bilgi” ve “kişisel veri” kavramlarının genelde beraber kullanılabileceğini, ancak “veri” nin temel olarak teknik alana

³⁰¹ Monisha Pillai, “China Now Has AI-Powered Judges: Is AI arbitration the future?”, (Çevrimiçi) <https://radiichina.com/china-now-has-ai-powered-robot-judges/>, (Erişim Tarihi: 08.12.2020).

³⁰² Wang Liming, “论个人信息权在人格权法中的地位 (Kişilik Hakları Hukukunda Kişisel Veri Haklarının Durumu Hakkında)”, *Academic Attention*, 2012, s. 13.

uygulanabilir, hukuki alanda daha az uygulanabilir olduğunu belirtmiştir³⁰³. Çin'in mevcut mevzuatı ve düzenlemeleri açısından, Çin'de yapay zekâ çağının gelişim ihtiyaçları ile de uyum sağlama amacıyla “kişisel bilgi” sözcüğünü temel olarak benimsemiş durumundadır³⁰⁴. Bunları karşı olarak “kişisel veri” kavramının “kişisel bilgiye” göre daha uygun olduğunu savunan hukukçularda vardır³⁰⁵. Fakat niceleme açısından “kişisel bilgi” nin daha çok kullanıldığı aşikârdır. Bu başlık altında kavramların aslını kullanma amacı ile kişisel veri yerine “kişisel bilgi” sözcüğü kullanılmıştır.

2009 yılında yürürlüğe giren “Çin Haksız Sorumluluk Kanunu” (Tort Liability Law of the People's Republic of China) siber ihlalleri için ilk kez “Bildirim/Kaldırma” hükmü içermiştir. Daha sonra Kasım 2016'da kabul edilen “Çin Siber Güvenlik Kanunu” siber güvenliğinin korunmasına odaklanmışsa da kişisel bilgilerin korunmasına ilişkin özel bir bölümü içermektedir. Mart 2017 tarihinde kabul edilen “Medeni Kanun Genel Hükümleri”, gerçek kişilerin kişisel bilgilerinin kanunla korunmasına ilişkin hükümleri içermiştir. Aynı yıl yürürlüğe giren yasa, vatandaşların kişisel bilgilerini toplamak isteyen herhangi bir kişi veya kuruluşun yasal araçları kullanması gerektiğini belirtmiş ve bilgilerin güvenliğini sağlamak, kişisel bilgilerin yasa dışı olarak toplanması, düzeltilmesi, işlenmesi ve açıklanmasını yasaklamıştır. 2019'da Devlet Konseyi, çocukların bilgilerinin korunmasını güçlendirmek için “Çocukların Kişisel Bilgilerini Koruma Yönetmeliği” ni yayımlamıştır. Çin'de günümüze kadar yapılan kişisel bilgilerin korunmasına ilişkin yasalar Tablo 16'da sıralanmıştır.

³⁰³ Mei Shaozu, “个人信息保护的基础性研究 (Kişisel Bilgilerin Korunmasıyla İlgili Temel Konular Üzerine Araştırma)”, **Academic Journal of Suzhou University (Philosophy and Social-science)**, 2005, s. 27.

³⁰⁴ Shi Weimin, “大数据时代个人信息保护的现实困境与路径选择 (Büyük Veri Çağında Kişisel Bilgilerin Korunmasında Yol Seçimi)”, **Journal of Intelligence**, (2013), ss. 155-161, s. 157.

³⁰⁵ He Xuxu, **a.g.m.**, s. 64.

Tablo 16: Çin Kişisel Bilgileri Koruma Düzenlemeleri

Çin Kişisel Bilgileri Koruma Düzenlemeleri		
Tarih	Düzenleme	Getirdiği Yenilikler
2009	“Haksız Sorumluluk Kanunu” Madde 36: “İnternet kullanıcılarının haklarını ihlal eden kullanıcılar veya internet hizmeti sağlayıcıları haksız fiil sorumluluğunu üstlenir. İnternet kullanıcıları ihlale uğradığı zaman bağlantıların silinmesi, engellenmesi ve bağlantısının kesilmesi gibi gerekli önlemleri alması için internet hizmet sağlayıcısını bilgilendirme hakkına sahiptir.” ³⁰⁶ .	Bildirim/Kaldırma mekanizmasının kurulması
2012	Ulusal Halk Kongresi Daimî Komitesinin “İnternet Bilgileri Korunmasının Güçlendirilmesine Dair Kararı” ³⁰⁷ .	Kişisel bilgilerin korunma ilkelerinin belirlenmesi
2016	“Siber Güvenlik Kanunu” Madde 76: “Kişisel bilgiler, gerçek kişinin adı, doğum tarihi, kimlik numarası, telefon numarası, kişisel biyometrik bilgileri, adresi dahil ancak bunlarla sınırlı olmamak üzere gerçek bir kişinin kişisel kimliğini tanımlamak için tek tek veya diğer bilgilerle birleştirilebilen çeşitli bilgileri ifade eder.” ³⁰⁸ .	Kişisel bilgi kavramının tanımlanması
2017	“Medeni Kanun Genel Hükümleri” Madde 111: “Gerçek kişilerin kişisel bilgileri kanunla korunmaktadır. Kişisel bilgileri toplamak isteyen	Kişisel bilgileri korumak için medeni hukuk mevzuatına

³⁰⁶ 中央政府门户网站 (Çin Merkezi Hükümet Sitesi), “中华人民共和国侵权责任法(Çin Halk Cumhuriyeti Haksız Sorumluluk Kanunu)”, (Çevrimiçi) http://www.gov.cn/flfg/2009-12/26/content_1497435.htm, (Erişim Tarihi: 12.12.2020).

³⁰⁷ 中央政府门户网站 (Çin Merkezi Hükümet Sitesi), “全国人大常委会关于加强网络信息保护的決定 (İnternet Bilgileri Korunmasının Güçlendirilmesine Dair Karar)”, (Çevrimiçi) http://www.gov.cn/jrzg/2012-12/28/content_2301231.htm, (Erişim Tarihi: 12.12.2020).

³⁰⁸ 法律法规数据 (Kanunlar ve Yönetmelikler Veri tabanı), “中华人民共和国网络安全法(Çin Halk Cumhuriyeti Siber Güvenlik Kanunu)”, (Çevrimiçi) <http://search.chinalaw.gov.cn/law/searchTitleDetail?LawID=394858&Query>, (Erişim Tarihi: 12.12.2020).

	<i>herhangi bir kuruluş veya kişi, yasalara uygun şekilde bilgilerin güvenliğini sağlamak ile yükümlüdür. Kişisel bilgiler yasa dışı şekilde toplanamaz, kullanılamaz, işlenemez, aktarılamaz ve ticarete kullanılamaz</i> ³⁰⁹ .	önemli bir maddenin eklenmesi
2020	“Çin Medeni Kanun” ³¹⁰ Mahremiyet ve kişisel bilgi koruma başlıklı bölümün yer alması.	Kişilik hakları bölümünde, kişisel bilgileri ve mahremiyet haklarını beraber koruma altına almayı amaçlaması ve kişisel bilgilerin türü, toplanması, değiştirilmesi veya silinmesine ilişkin ön düzenlemelerin yapılması

2.6.2.1. Siber Güvenlik Kanunu

“Çin Siber Güvenlik Kanunu”³¹¹ kişisel biyometrik verilerin kişisel bilgi kategorisine dahil edildiğini belirtmiştir. Son zamanlarda insan yüzünü yapay zekâ aracılığıyla taklit edip, 3D teknolojisi kullanarak maskelenmiş yüzler ile yüz tanıma

³⁰⁹ 中国人大网 (Çin Ulusal Halk Kongresi), “中华人民共和国民法总则 (Çin Halk Cumhuriyeti Medeni Kanun Genel Hükümleri)”, (Çevrimiçi) http://www.npc.gov.cn/zgrdw/npc/xinwen/2017-03/15/content_2018907.htm, (Erişim Tarihi: 12.12.2020).

³¹⁰ 中国人大网 (Çin Ulusal Halk Kongresi), “中华人民共和国民法典 (Çin Halk Cumhuriyeti Medeni Kanunu)”, (Çevrimiçi) <http://www.npc.gov.cn/npc/c30834/202006/75ba6483b8344591abd07917e1d25cc8.shtml>, (Erişim Tarihi: 12.12.2020).

³¹¹ Çin Halk Cumhuriyeti Siber Güvenlik Kanunu 12.Ulusal Halk Kongresi Daimî Komitesi’nin 7 Kasım 2016’daki 24. toplantısında kabul edilmiştir.

sistemlerini yanlış karar vermeye zorladığı olaylar sık sık gündeme gelmiştir³¹². Kişisel verilerin korunması bu açıdan sadece geleneksel verilerin korunması değil, yüz özellikleri hatta nabız sayısı gibi biyometrik verilerinde korumasını gerektirmektedir. Bu açıdan bakıldığında Çin biyometrik veriler konusunda başlangıç seviyede düzenlemeler yaptığını söyleyebiliriz.

Günümüzde Çin’de “yüz tanıma” ödemesinden “yüz tanıma” para çekmeye, “yüz tanıma” güvenlik kontrolünden “yüz tanıma” kimlik doğrulama hizmetine kadar yüz tanıma teknolojileri hayatın her alanına nüfuz etmiş durumundadır. “Yüzü tanıtmak” vatandaşların hayatına kolaylık getirirken, aynı zamanda kaçınılmaz olarak güvenlik riskleri konusunda endişelendirmektedir. Kişisel bilgi niteliğindeki yüz tanıma biyolojik verisinin sızdırmasından büyük mali hasarlara kadar giden risk söz konusudur.

Fakat Çin hukukunda yüz özellik bilgilerine ait kişisel veriler çok etkili şekilde korunamamaktadır. Yüz tanıma teknolojisi uygulamasının denetiminde yasal boşluk ve yüz tanıma teknolojisinin kullanımı konusunda da tartışmalar bulunmaktadır. “Siber Güvenliği Kanunu” kişisel bilgiler kapsamında kişisel biyometrik bilgileri açıkça içermesine rağmen, verilerin kullanımı, saklanması, aktarılması yeterince ayrıntılı şekilde düzenlenmemiştir³¹³. Bunun gibi yasal boşluklar söz konusu olduğunda, ticari çıkarlar tarafından yönlendirilen yüz tanıma teknolojileri mahremiyet yasalarını kolayca çiğneyebilmektedir. Örneğin, Barcelona futbol takımının golcüsü, Huawei firmasının, Uygur Türklerine yönelik yüz tanıma sistemi geliştirilmesine yardımcı olduğu iddiası üzerine şirketle sözleşmesinin sona erdirdiğini

³¹² CCTV, “‘刷脸’时代你的脸安全吗? 嫌疑人“AI”换脸骗过人脸识别实施犯罪 (‘Yüzü Tanıma’ çağında, yüzünüz güvende mi?)”, (Çevrimiçi) <https://tv.cctv.com/2020/10/27/VIDEDsY1h4IX1OGsj4FKDuSz201027.shtml>, (Erişim Tarihi: 28.10.2020).

³¹³ Yue Shenshan, “‘刷脸’技术监管存在真空,须确立安全底线与法律边界 (‘Yüz Tanıma’ Teknik Denetiminde Bir Boşluk Var ve Bir Güvenlik Yasal Sınırlama Oluşturulmalıdır)”, 14.12.2020, (Çevrimiçi) <https://lvdao.sina.com.cn/news/2020-12-14/doc-iiiznctke6448293.shtml>, (Erişim Tarihi:15.12.2020).

bildirmiştir³¹⁴. Buna benzeyen veri ihlalleri, ayrımcılık olayları günümüz Çin’de çok sık rastlanmaktadır.

Bu sorunların çözülmesi için öncelikle yasal boşlukların doldurulması gerekmektedir. Çin gibi elinde bir buçuk milyar insanın her türlü verisi bulunan recimlerde, sadece veriye dayalı teknolojilerin ilerlemesi değil, insan hakları, mahremiyet ve özgürlük haklarının korunması gerekmektedir. Örneğin, “yüz tanıma” verilerini toplamak için yasal düzenlemeler getirilmelidir. İsteyen herkes bu tür biyolojik verileri toplayamamalıdır. Yetkisiz veri toplama durumların da yasaklanması gerekmektedir. “Yüz tanıma” verilerinin yasadışı toplanılması, kötüye kullanılması ve ifşa edilmesiyle ilgili denetim güçlendirilmeli ve ciddi şekilde engellemelidir. Aynı zamanda ihlal oluştuğunda sorumlular için de yasalara uygun olarak cezai sorumluluk getirilmelidir. “Siber Güvenlik Kanun” u sadece bir giriş niteliğinde hangi verilerin kişisel veri olup olmadığını belirlemiştir. Ama detaylı bir yasal düzenlemesinin gerektiği açıktır.

2.6.2.2. Çin Medeni Kanunu

Mayıs 2020’ de kabul edilen “Çin Medeni Kanun” kişilik hakları başlığı altında, kişisel bilgileri ve mahremiyet haklarını birlikte korumak için özel bir bölüm benimsemiş ve kişisel bilgilerin türü, toplanması, değiştirilmesi ve silinmesi hakkında hükümler koymuştur.

Kişisel bilgilerin medeni hukukta nasıl koruma altına alınması Çin’de başka hukuk düzenlemelerinde olduğu gibi zorluk yaratmaktadır. Şu ana kadar kişisel bilgiler bağımsız bir kişilik hakkı niteliğinde midir sorusu cevapsız kalmış durumdadır.

³¹⁴ BBC, “Griezmann Cuts Ties With Huawei Citing Fears Over Treatment of Uighurs”, 10.12.2020, (Çevrimiçi) <https://www.theguardian.com/football/2020/dec/10/griezmann-cuts-ties-with-huawei-citing-fears-over-treatment-of-uighurs>, (Erişim Tarihi:15.12.2020).

Mevcut “Çin Medeni Kanun”nu, kişisel bilgileri kişilik hakları kapsamında yeni bir kişilik menfaati çeşiti olarak değerlendirmektedir. Ancak bu durumda iki önemli teorik engel ile karşılaşmaktadır.

Birincisi, kişisel bilgileri bağımsız kişilik hakkı kapsamında değerlendirdiğimizde kişisel bilgiler ile mahremiyetin ayrımını bulmak zor olacaktır. Çin Medeni Hukuku kişisel bilgilere mahremiyetin dahil edildiğini açıkça belirtmektedir³¹⁵. Bu durumda kişisel bilgiler bağımsız kişilik menfaattarı olarak adlandırılıyorsa, mahremiyet ile olan ilişkisi nasıl çözüleceği zor bir sorun oluşturacaktır.

İkinci olarak, kişisel bilgilerin kapsamı çok geniştir. Bu yüzden genelleştirmek ve kişilik hakları olarak tanımlamak kolay olmayacaktır. Şu ana kadar kişisel bilgiler için “belirlenebilirliği”i ölçüt olarak görmek mutabakat haline gelmesine rağmen nasıl tanımlanacağı bir dizi soruna neden olmuştur. Örneğin, yapay zekâ teknolojisinde “kişisel portrelerin” ortaya çıkması nedeniyle, dolaylı kişisel bilgilerin analizi yoluyla bir kişinin kimliğini belirleme olasılığı büyük ölçüde artmıştır. Bu dolaylı bilgiler kişisel bilgilere mi ve dolayısıyla kişilik menfaattarına mı ait olacağı sorusu hakkında hala bir fikir birliğine varılamamıştır.

2.6.2.3. Kişisel Bilgilerin Korunması Kanunu Taslağı

Kişisel Bilgilerin Korunması Kanunu Taslağı, 2020 Ekim’de 13. Ulusal Halk Kongresi’nin 22. toplantısına görüşülmek üzere sunulmuştur³¹⁶. On yıldan fazla bir süredir çalışılmakta olan yasama süreci ilk kez taslak halinde onaya sunulmuştur. Günümüze kadar Çin’deki kişisel bilgileri koruma yasaları bir dizi düzenlemeye tabi olsa da yeknesaklaşmış düzenlemenin olmaması sorun oluştuyordu. Bu kanun

³¹⁵ Çin Medeni Hukuku, m. 1032- 1039.

³¹⁶ Xia Hongzhen, “个人信息保护法草案首次亮相 (Kişisel Bilgileri Koruma Yasası Taslağı Açıklandı)”, “**Çin Halk Kongresi**” **Dergisi**, 15.10.2020 (Çevrimiçi) <http://www.npc.gov.cn/npc/c30834/202010/569490b5b76a49c292e64c416da8c994.shtml>, (Erişim Tarihi: 28.10.2020).

taslağının onaya sunulması Çin'in kişisel bilgileri koruma düzenlemeleri açısından yenilik niteliğindedir.

Çin'deki tüketiciler, kullanıcı verilerinin yaygın bir şekilde toplanması ve satılmasıyla ortaya çıkan dolandırıcılıklara karşı tepkide olduğu için, kişisel bilgilerin korunması uzun zamandan bu yana Çin'de çok tartışılan bir konu olmuştur. Akıllı telefonlardaki uygulamaların çok fazla veri toplaması veya kapsamlı veri izinleriyle erişimi paketlemesi uygulaması yaygındır. Bu nedenle devlet medyası, hazırlanan kanun taslağını Çin vatandaşlarının haklarını korumaya yönelik bir zafer niteliğinde ilan ediyor³¹⁷. Kuşkusuz, yasanın büyük bir kısmı, özel bilgilerin toplanmasını dizginlemeye ve tüketicilerin hoş karşılayacağı yasa ihlalleri için daha sert cezalar uygulamaya adanmıştır. Yasada bilgileri işleyenlerin onay almasını gerektiği vurgulanmış ve tüketicilere, AB mevzuatında yer alan rızayı geri alma hakkı tınılmıştır. Bu açıdan hukuk taslağı yapılırken GDPR'ı örnek aldığını söyleyebiliriz.

Kişisel Bilgilerin Korunması Kanunu Taslağı veri güvenliği konuları vatandaşların mahremiyetini koruma perspektifinden değerlendirmektedir. Yasanın “kişisel bilgi” kavramının özünü ve uzantısını belirlemesi, çeşitli sùjeler arasındaki ilişkiyi düzenlemesi beklenmiştir. Ancak taslak, yetkililerin vatandaşları izlemek için nasıl kullandıklarından ziyade, şirketlerin Çin'deki kişisel bilgileri nasıl kullandıklarıyla çok daha fazla ilgilendiğini açıkça gösteriyor. Örneğin, yasanın görüntü bilgileri toplama ve kişisel kimlik tanıma ile ilgili maddesinde, “kamu güvenliğini korumak için gerekli” görünen durumlarda yetkililerin sınırsız bilgi toplamasına izin veriyor.

Çin'deki uzmanlar, kaçırılan çocukları bulmak gibi kamu güvenliği hedeflerinin biyometrik verilerin toplu olarak toplanmasına yol açabileceğini dile getirmiştir.

³¹⁷ Lavender Au ve Benjamin Wilhelm, “China's New Data Protection Law Won't Rein in State Surveillance”, **World Politic View**, 28.10.2020, (Çevrimiçi) <https://www.worldpoliticsreview.com/trend-lines/29174/china-s-new-data-protection-law-won-t-rein-in-state-surveillance>, (Erişim Tarihi: 28.10.2020), par. 3.

Ancak alışveriş merkezlerindeki, süpermarketlerdeki, metrolardaki ve havalimanlarındaki kameralarla yüz tanımanın yaygınlaştığına dair kamuoyunda endişeler oluşmuş durumundadır. 2019 yılında Çin'deki bir hukuk profesörü girişine yüz tanıma kameraları yerleştirip tüm ziyaretçilerin taramasını zorunlu kılan bir yaşam parkına dava açmıştır³¹⁸. Korkunç olan şu ki, biyometrik bilgiler diğer kişisel bilgilere eşleştirildiğinde, devlet/hükümet açısından kendi vatandaşlarını her yönde, her yerde izlemek/takip etmek çok kolaylaşıyor. Dahası bu yasa tasarısı, hükümetin yüz tanıma yoluyla elde edilen biyometrik verileri toplama veya saklama yetkisine ilgili herhangi bir sınırlama getirmemişlerdir.

Özetlemek gerekirse, Çin'de vatandaşların verileri/bilgilerini toplama, saklama, işleme de herhangi bir engelin bulunmadığını söylenebilir. Bunu Çin'deki Sosyal Puanlama Sistemleri, Kredi Kart bilgileri, yüz tanıma kameraları vb. örnekler üzerinden anlayabiliriz. Fakat veri aktarımına geldiğinde, sınır dışı veri aktarımında Çin'in "Büyük Güvenlik Duvarı"nın bulunduğu da gerçektir. Örneğin, 2006 yılında Çin bazı şirketlerin sunucularını Çin'de tutmasını gerektiren e-bankacılık önlemlerini uygulamaya koymuştu. 2013 yılında vatandaşlarına ilişkin tüm kredi bilgilerinin Çin'de işlenmesini ve saklanmasını gerektiren kredi raporlama ile ilgili kurallar çıkardı. 2014 yılında yalnızca Çin'de depolanması gereken sağlık ve tıbbi bilgileri gerektiren yeni kurallar açıkladı. Mart 2016'da Çin'deki Bulut Bilişim hizmetleriyle ilgili olarak yabancı teknoloji şirketlerini dışlayan ve yerel veri depolama gereksinimlerini güçlendiren yeni düzenlemeler çıkardı³¹⁹. Çin'de yapay zekâ ve kişisel bilgilerin korunması konusunda mevzuat altyapısına yönelik ciddi bir

³¹⁸ Kerry Allen, "China Facial Recognition: Law Professor Sues Wildlife Park", BBC News, 08.11.2019, (Çevrimiçi) <https://www.bbc.com/news/world-asia-china-50324342>, (Erişim Tarihi: 29.10.2020).

³¹⁹ Nigel Cory, "Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?" Information Technology and Innovation Foundation, (01.05.2017) (Çevrimiçi) <https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost>, (Erişim Tarihi: 25.11.2020).

alışmanın olmaması gerçektir. Bu durumu ancak Çin'in kendine özgü devlet yönetim kültürü ile açıklamak mümkündür.

2.6.3. Türkiye'de Kişisel Verilerin Korunması

Türkiye, 2000'li yıllardan beri kişisel veri koruması ile ilgili yasa ve yönetmelikler oluşturmuştur. 2016 yılında bu konuyla ilgili "6698 Sayılı Kişisel Verilerin Korunması Hakkında Kanun (KVKK)" onaylanmış ve 7 Nisan 2016 tarihinde yürürlüğe girmiştir. KVKK, bireylerin kişisel verileri işlerken, başta özel hayatın gizliliği olmak üzere temel hak ve özgürlüklerini korumak amacıyla, kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülüklerini ve izlenecek usul ve esasları düzenlemiştir³²⁰. Türk kanunlarına baktığımızda, özellikle Anayasa'nın 20. maddesi ve Türk Medeni Kanunu'nun (TMK) 23. maddesi vd. hükümleri kişilik hakkı ve özel hayatın gizliliğini koruma altına almıştır³²¹.

2.6.3.1. Türk Hukukunda Kişisel Verilerin Korunması

Kişisel verilerin korunması hakkının her hukuk devletinin anayasasında temel hak olarak tanımlanması temayülü gün geçtikçe artan bir şekilde dünya hukuk düzenini oluşturan hukuk sistemlerinde kendisini göstermektedir³²². Türkiye Anayasa'sının 20. maddesinde kişisel verilerin korunması temel bir insan hakkı olarak tanımlanmıştır³²³. Anayasa'nın 20. maddesi:

"Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya

³²⁰ Eroğlu, **a.g.m.**, s. 135.

³²¹ Kemal Atasoy, "Kişilik Hakkı Kapsamında Sosyal Medyada Kişisel Verilerin Korunması ve Veri Sahibinin Rızası", **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi**, C. 22, S. 3, ss. 269- 301, s. 271.

³²² DUMAN, **a.g.m.**, s. 2.

³²³ Bkz: TBMM, Kişisel Verilerin Korunması Kanunu Tasarısı (1/541) ve Adalet Komisyonu Raporu, 2017.

silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir”³²⁴.

Anayasanın 20, 21, ve 22. maddeleri “Özel Hayatın Gizliliği ve Korunması” başlığını altında düzenlenmiştir. Anayasanın 20. maddesine baktığımızda “*kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızası koşuluyla işlenebilecektir*” hükmü bulunmaktadır. Buradan da anlaşılabacağı üzere Türk hukuk sisteminde kişisel verilerin işlenmesinde “Açık Rıza” yönteminin benimsendiğini söyleyebiliriz³²⁵.

Türk Medeni Kanunu 24. Maddesinde:

“Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz”.

şeklinde mahremiyet hakkına yönelik düzenlemeler yapılmıştır. “Bilgi Edinme Kanunu” nun 10. maddesinde kişinin kendisiyle ilgili toplanmış verilerin kendisine açıklanmasını talep etme hakkı yer almaktadır. Aynı kanunun 21. maddesi ile mahremiyete yönelik belli hususlar düzenlenmiştir. “Türk Ceza Kanunu’nun (TCK)” 10, 125, 134, 135, 136, 137 ve 280. maddeleri özel hayat ve mahremiyet ile ilgili düzenlemeleri içermektedir³²⁶. Kişisel verilerin hukuka aykırı olarak saklanması TCK’nın 135. maddesine göre suç teşkil eden bir eylem olarak belirlenmiştir.

Öte yandan ise ilgili yasal düzenleme yürürlüğü girdiği zaman kişisel verilerin hangi durumlarda hukuku uygun işleneceği konusunda herhangi bir düzenleme getirmemiştir³²⁷. Bu sebeple Türk Kanun Koyucusu, 2016 Nisan ayında 6698 sayılı

³²⁴ Erdinç, **a.g.m.**, s. 2.

³²⁵ **a.g.m.**, s. 96.

³²⁶ Eroğlu, **a.g.m.**, s. 135.

³²⁷ Kanun öncesi döneme kişisel verilerin nasıl korunduğu konusunda bkz. Oğuz Şimşek, **a.g.e.**

KVKK'nı yasalaştırmış, bununla birlikte Kişisel Verilerin Korunması Kurumu ile ilgili düzenlemelere de yer vermiştir.

2.6.3.2. KVKK

Nisan 2016 tarihinde kabul edilen KVKK kişisel verilerin korunması kavramını kullanmış ve bu terim uluslararası düzenlemeler ile örtüşmektedir. Ancak KVKK'nın koruma altına alan menfaati verinin kendisi değil, “*başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlükleri*” ile sınırlıdır³²⁸. Bundan anlaşılacağı üzere, kişisel verilerin korunması başlı başına amaç değildir, temel hak ve özgürlükleri korumak için kullanılan araçtır³²⁹.

2.6.3.2.1. Uygulama Alanı

KVKK'nın kişi açısından uygulama alanı KVKK'nın madde 3 b. d) yer almaktadır. Bu çerçevede sadece gerçek kişiler KVKK kapsamında korunmaktadır. Tüzel kişiler ise açık şekilde koruma dışında bırakılmış ve uluslararası eğilimlerle örtüşmektedir. Öte yandan, KVKK sorumluluk konusunda gerçek ya da tüzel kişi ayrımı yapmamaktadır. Kişisel verileri işleyen tüzel ya da gerçek kişi fark edilmeksizin bazı yükümlülükler üstelemek zorundadır.

KVKK'nın konu açısından uygulama alanı madde 2 de yer almaktadır. Kişisel verilerin tamamen veya kısmen otomatikleştirilmiş bir veri kayıt sistemi aracılığıyla işlenmesi, otomatik olmayan yollarla işlenen kişisel veriler “*herhangi bir veri kayıt sisteminin parçası*” olması şartı altında KVKK'nın konu kapsamında değerlendirilecektir. Sonuçta analog şeklinde, kâğıt üzerinde kayıt altına alınıp işlenen veriler de belirli şartlar altında KVKK'nın koruma kapsamına dahil edilebilecektir.

³²⁸ KVKK, m. 1: “Bu Kanunun amacı, kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemektir”.

³²⁹ Çekin, Avrupa ..., a.g.e., s. 19.

2.6.3.2.2. KVKK’da Esas Alınan Temel İlkeler

Kişisel verilerin korunması düzenlemeleri genel olarak hukuk ilkelerine dayanmaktadır. Tablo 17’de KVKK’da esas alınan temel ilkeler açıklanmıştır.

Tablo 17: KVKK’da Esas Alınan Temel İlkeler

Veri işlenmesinin kural olarak yasak olması ilkesi	Bu ilkenin belirlenme amacı günümüz teknoloji çağında kişisel verilerin etkili şekilde korunmasıdır. Verilerin işlenmesinin kural olarak yasaklanması, istisnai durumlarda ve ilgili kişinin açık rızası kapsamında işlenebileceği uluslararası düzenlemelerde benimsenen ilkelerdendir.
Hukuka ve dürüstlük kurallarına uygunluk ilkesi	Hukuk devletinin temel ilkesinin doğrudan sonucu olan hukuka uygunluk ilkesidir.
Amaca bağlılık ilkesi	Veri işleme amacının önceden, yani veri işlemeden ya da veri elde edilme esnasından belirlenmesi gerekmektedir.
Şeffaflık, doğru ve güncel olma, asgari miktarda veri işlenmesi ilkesi	Uluslararası düzenlemelerde benimsenen ilkedir. Günümüzde bu ilkeden yola çıkarak tasarımda şeffaflık yöntemleri ileri sürülmektedir.

2.6.3.2.3. Açık Rıza

KVKK’nın 3. maddesi açık rıza ile ilgilidir. İlgili maddeye göre açık rıza, “belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rızayı” ifade etmektedir³³⁰. KVKK bakımından, rızanın aranmayacağı haller KVKK 5. maddesinde yer almaktadır:

³³⁰ a.g.m., s. 97.

“Kanunlarda açık bir şekilde öngörülmesi; fiili imkânsızlık sebebiyle rızasını açıklayamayacak halde bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması; bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması; veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması; ilgili kişinin kendisi tarafından alenileştirilmiş olması; bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması; ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması”³³¹.

İlgili kişinin açık rızasının hukuki niteliği mukayeseli hukukta tartışma teşkil etmektedir. Açık rızayı hukuki işlem olarak nitelendiren görüşe göre³³², hukuki işlemlere mahsus düzenlemeler açık rıza işlemi içinde uygulanır. İlgili kişi yanıltma, aldatma gibi durumlarda geriye etkili olmak üzere söz konusu açık rızayı geçersiz kılabilir.

Açık rızayı maddi fiil olarak gören görüşte³³³ ise hukuki işlemlere yönelik düzenlemeler açık rıza kapsamında uygulanmaz. Bir diğer husus ise açık rızanın geri alınmasıdır. KVKK açık rıza tanımını yapmış olsa da rızanın geri alınabileceği konusunda herhangi bir düzenleme yapmamıştır. Ancak “Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik” madde 5 de buna ilgili hükümler yer almıştır. İlgili madde:

³³¹ **a.g.m.**, s. 98.

³³² Simittis, Simitis & 4a. BDSG, Rn. 20

³³³ Gola/Schomerus, Art. 28, Rn. 25.

“Kişisel verilerin işlenmesi sadece açık rıza şartına istinaden beyan edildiğinde ilgili kişinin açık rızayı geri alması”

durumunda kişisel verilerin işlenebileceği ile ilgili şartlar ortadan kalkmış olacak şeklinde belirtmiştir. Fakat bu geri almanın nasıl gerçekleşeceği konusunda yönetmelik herhangi bir düzenleme yapmamıştır.

Ulusal ve uluslararası mevzuat kapsamında, özellikle GDPR değerlendirildiğinde, kişisel verilerin işlenmesi genel olarak yasaklanmıştır. Kişisel verilerin işlenmesi ise bir istisna olarak kabul edilmektedir³³⁴. KVKK madde 28’de KVKK’nın uygulanmayacağı bir kısım istisnalar düzenlenmiştir:

“Verilerin gerçek kişiler tarafından tamamen kendisiyle veya aynı konutta yaşayan aile fertleriyle ilgili faaliyetler kapsamında işlenmesi; sanat, tarih, edebiyat veya bilimsel amaçlarla ya da ifade özgürlüğü kapsamında işlenmesi; planlama ve istatistik gibi amaçlarla işlenmesi, Kısmen istihbarat faaliyetleri kapsamında işlenmesi; yargı makamları veya infaz mercileri tarafından işlenmesi”.

KVKK’da yer bakımından uygulama alanı açık belirlenmemiştir. Bu durumda genel kural olarak mülkiyet ilkesi doğrultusunda Türk Hukukunun geçerli olduğu yerlerde KVKK hükümlerinin uygulama alanı bulacağı söylenebilir³³⁵.

KVKK ile GDPR arasındaki farklılıklardan biri veri sorumlusu kavramının içeriğidir. KVKK veri işleyen ile veri sorumlusunu ayrı ayrı tanımlamamış olup, sadece ikisi arasındaki ilişki konusunda müteselsil sorumluluğa daire bir hüküm koymuştur. GDPR ise günümüz teknoloji çağında verilerin çoğu zaman veri sorumlusu (bir diğer ifadeyle verilerin efendisi) tarafından değil, üçüncü bir şirket

³³⁴ Mustafa Tevfik Kartal, “Kişisel Verilerin Korunması: Türk Bankacılık Sektörü Üzerine Kavramsal Bir Değerlendirme”, **Uluslararası Ekonomi ve Yenilik Dergisi**, C. 4, S. 1 (2018), ss. 1- 18, s. 8.

³³⁵ Çekin, Avrupa ..., **a.g.e.**, s. 28.

tarafından işleneceği gerçeği göz önüne alarak, veri işleyene özel hükümler getirmiştir³³⁶. Yapay zekâ çağında veri işleyenler ile veri sorumlusu arasındaki farkın netleştirilmesi hukuki güvenlik açısından önemli olduğunu, uygulamada meydana gelebilecek sorunları çözmede yararlı olacağı söylenebilir³³⁷.

KVKK madde 5 de ilgili kişinin açık rızası olamadığı durumlarda,

“[b]ir sözleşmenin kurulması veya ifasıyla doğrudan ilgili olması şartıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesi”

açık rızayı gerektirmediği vurgulanmıştır. Bu düzenleme hukuk koyucuların ilgili kişinin haklarını koruma ile veri sorumlusunun meşru menfaatlerinin korunması arasında denge kurmaya çalıştığının göstergesidir. KVKK’da bir sözleşmenin kurulmasıyla ya da ifasıyla demekle birlikte taraflar arasında bir sözleşmesel ilişkinin kurulması ya da mevcudiyeti zorunluluğunu vurgulamıştır. Bu yüzden haksız fiilden ya da sebepsiz zenginleşmeden kaynaklanan borç ilişkileri bu kapsamda değerlendirilmeyecektir³³⁸. Sadece taraflar iradesi ile kurulan sözleşmeler söz konusudur.

KVKK’nın aynı maddesinde:

“[i]lgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması”

durumunda açık rıza olmaksızın verilerin işlenebileceği belirlenmiştir. Hükümde geçen “meşru menfaat” sözcüğü hukuk düzeni içerisinde cevaz verilen her çeşit hukuki, iktisadi ya da kişisel menfaatleri ifade ediyor³³⁹. Hukuku aykırı yollar ile

³³⁶ Bkz. GDPR m. 27, 30, 31, 32, 37, 44.

³³⁷ Özellikle Blokchain teknolojisinde veri sorumlusu ile veri işleyenin ayrılması önemlidir. Çünkü Blokchain sisteminde veri sorumlusunun kim olduğu sorunu ortaya çıkmaktadır.

³³⁸ Çekin, Avrupa ..., **a.g.e.**, s. 66.

³³⁹ Gola/Schomerus, Art. 28 Rn. 24.

elde edilen veriler konusunda ise meşru menfaat söz konusu olamaz. Açık rıza gerektirmeyen ikinci bir şart ise “zorunlu olmasıdır”. Bir diğer ifade ile veri işleme ile meşru menfaat arasında sıkı bir ilişki olması gerekmektedir.

KVKK’da yer alan kişisel verilerin üçüncü kişilere, yurtdışına aktarılması konusu verilerin aktarılmasının veri işlemenin bir parçası olduğu nedeniyle yukarıda anlatılan rıza koşulu, hukuki uygunluk sebepleri çerçevesinde değerlendirilebilmektedir. KVKK’nın madde 8’de hangi durumlarda kişisel verilerin aktarılabilirliği düzenlenmiştir.

2.6.3.2.4. İlgili Kişinin Hakları ve Veri Sorumlusunun Yükümlülükleri

KVKK madde 11’de ilgili kişinin sahip olduğu hakları düzenlenmiştir. Kişisel verilerin işlenebilmesi için gereken şartlar ile ilgiliye tanınan haklar arasında sıkı bir ilişki vardır. Örneğin: kişisel verilerin işlenmesi konusundaki haklar madde 5 ve madde 6 ile alakalıdır. Kişisel verilerin aktarma konusu ile doğrudan madde 8 ile ilgilidir. Ayrıca veri sorumlusunun yükümlülükleri ile ilginin hakları arasında da sıkı bir tamamlayıcı ilişki söz konusudur. KVKK’da ilgiliye tanınan haklar şunlardır:

- Kişisel verilerin işlenip işlenmediğini bilme hakkı
- Bilgi talep etme hakkı
- Amaca uygun kullanıp kullanmadığını öğrenme hakkı
- Verilerin aktarıldığı üçüncü kişileri bilme hakkı
- Eksik ya da yanlış verilerin düzeltilmesini isteme hakkı
- Silme veya imha talep etme hakkı
- Sonuca itiraz etme hakkı
- Tazminat talep etme hakkı

KVKK madde 10 ile madde 12 veri sorumlusunun yükümlülüklerini düzenlemiştir. Bu çerçevede aydınlatma yükümlülüğü, müteselsil sorumluluğu, KVKK’a uygunluğu sağlama sorumluluğu, bildirim yükümlülüğüne yer verilmiştir.

Tablo 18: KVKK’da Belirtilen Veri Sorumlusunun Yükümlülükleri

Aydınlatma Yükümlülüğü	“Veri sorumlusunun kimliği, kişisel verilerin işleme amacı, işlenen verilerin kimlere ve hangi amaçla aktarılabilceği, kişisel veri toplamının yöntemi ve hukuki sebebi” aydınlatılmalıdır. (m. 11)
Uygun Güvenlik Düzeyi Sağlama Yükümlülüğü ³⁴⁰	Kişisel verilerin yasa dışı işlenmesini önlemek, kişisel verilere yasa dışı erişimi önlemek ve kişisel verileri korumak.
Veri İşleyen ile Veri Sorumlusunun Müteselsil Sorumluluğu	Diğer gerçek veya tüzel kişiler, kişisel verileri kendi adlarına işledikleri takdirde, bu kişilerle birlikte müteselsilen sorumlu olacaklardır. (m. 12)
Kurula Bildirim Yükümlülüğü	İşlenen kişisel verilerin kanuna aykırı şekilde başkası tarafından elde edilmesi halinde veri sorumlusu ilgili kişi ve Kurulunu en kısa sürede bilgilendirmek zorundadır.

Unutulma hakkına gelince, KVKK’da kişisel verilerin korunmasına yönelik temel ilkeler, özellikle “kişisel verileri silme” hakkı unutulma hakkını temel almaktadır. Öte yandan mahkeme³⁴¹, “güncellik” ilkesine dayanarak, kişisel veri işlevi yitiren bilgilerin unutulma hakkı kapsamında olmamasını talep edebileceğini kabul etmiştir.

³⁴⁰ Veri sorumlusu yanlışlıkların düzeltilmesini ve hata riskinin en aza indirilmesini sağlamak için uygun teknik ve organizasyonel önlemleri uygulamalı ve belirli durum temelinde ayrımcı etkileri önleyen kişisel verileri güvence altına almalıdır. Irksal veya etnik köken, siyasi görüş vb. özel kişisel veri kategorilerine dayalı otomatik karar verme ve profil oluşturmaya yalnızca belirli koşullar altında izin verilmelidir. Daha fazla bilgi için bkz. GDPR’ın Önsözü, par. 71.

³⁴¹ AYMK, Asli Alp ve Şükrü Alp, Başvuru No. 2014/18260, K.T. 4.10.2017.

3. YAPAY ZEKA ÇAĞINDA KİŞİSEL VERİLERİN KORUNMASI

Yapay zekâ çağında kişisel verilerin korunmasının önemi sık sık gündeme gelen konular arasındadır. Kişisel verilerin korunması tarih boyunca farklı düzeyde ihtiyaç duysa da yapay zekâ çağında niteliksel açıdan farklı bir içerik kazanmış durumundadır. Nitekim yapay zekâ insanoğlu hayatının her yerinde kendi değerini göstermeye başladığı bir çağda, bu kolaylıklar karşısında getirdikleri problem ve riskler değerlendirmeye değerdir. Kişisel verilerin korunması ise yapay zekâ çağında karşılaştığımız en önemli sorunlardan biridir.

3.1. Yapay Zekâ Çağında Kişisel Veri İşlemenin Etik Boyutları

Günümüzde kamusal alanda yapay zekâ uygulamaları ile ilgili tartışmalar dışında tartışılan konulardan bir diğeri de yapay zekânın etik boyutudur. Yapay zekâ çağında kişisel verilerin korunması sorunu sadece hukuki boyutta değil, etik ve ahlaki boyutlarda da ele alınması gerekmektedir. Teknik açıdan yapılması mümkün olan işlemlerin, günümüzde hukuki açıdan sorun oluşturmaya da etik açıdan kabul edilemez olabileceğini unutmamamız gerekmektedir. Giderek daha akıllı hale gelen yapay zekâ sistemlerin yasal yönlerine ilişkin birçok belirsizlik ve soru işareti bulunmaktadır. Özellikle TAY örneğinde olduğu gibi, kendi kendine öğrenen ve bu öğrenmeyi iyi amaçlarla kullanmayan yapay zekâ için etik çözümlemelerin yapılması gerekmektedir³⁴².

Yapay zekâ kullanımıyla ilgili değerli uygulamaları teşvik etmek için, yapay zekânın geliştirilmesinin, bireysel çıkarların ve sosyal düzenin de olduğu sosyo-teknik bir çerçevede (teknolojiler, insan özellikleri, organizasyon yapıları ve normlar dahil)

³⁴² Gizem Öztürk Dilek, “Yapay Zekânın Etik Gerçekliği”, *Anadolu Üniversitesi Sosyal Bilimler Dergisi*, S. 2 (4), 2019, ss. 47-59, s. 51.

gerçekleştirdiğinden emin olmamız gerekmektedir. Böyle bir çerçevenin oluşturulması için, sadece mevcut düzenlemeler ile kalmayıp, mevcut kuralların vatandaşlara, şirketlere ve icra makamlarına uygun çözümler ve talimatlar sağlamada başarısız olabileceğini göz önüne alarak, en baştaki temel ilkelere de odaklanmamız gerekmektedir³⁴³. Temel ilkeler ise hem etik hem de yasal düzeyde temel hakları ve sosyal değerleri ifade etmektedir.

3.1.1. Algoritmik El

Yapay zekâ algoritmaları ilgili kişilerin özerkliğini “manipüle edebilir” ve onurlarına ve ekonomik çıkarlarına zarar verebilir. Günümüzde, iş dünyası örgütleri insanların hayatlarını hassas bir şekilde başkaları için iş fırsatlarına dönüştürmek için çeşitli modellemeler veya algoritmalar kullanmaktadır ve sonuç olarak, “veri yaşamı”na katılan hemen hemen tüm bireyler “algoritmalar tarafından tanımlanan insanlar” haline gelmiştir. Bu ticari kuruluşlar, kullanıcıların günlük etkinlik verilerini veya sık ziyaret ettikleri iş yerlerini izleyerek potansiyel tüketicilerin kişisel tercihlerini, yaşam tarzlarını veya tüketim alışkanlıklarını belirleyebilir ve ardından doğru pazarlama veya reklamcılık yapabilir. Bu tür veri portresi, hedefli reklamların, belirli bir zaman ve sahnede, dürtü tüketimini tetikleyen aşırı hassasiyetle hedef müşterilere ulaşmasını sağlamaktadır³⁴⁴. Dahası görünmez “algoritmik el” haksız çıkarımlar yapar veya belirli kişileri veya grupları “etiketler”.

ABD mahkemeleri tarafından yeniden suçlama riskini (COMPAS) değerlendirmek için yaygın olarak kullanılan algoritmanın, siyah renklilere tekrar suçlanma riskini etiketlediği düşünülmektedir³⁴⁵. Algoritmanın sözde tarafsız adaleti biraz kafa karıştırıcı veya yanıltıcıdır ve insanın karar verme mekanizmasına kıyasla,

³⁴³ STOA, The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence, Brussel, 2020, s. 30.

³⁴⁴ Ye Mingyi, “个人信息的侵权法保护 (Kişisel Bilgilerin Korunması)”, 中国法学 (Chinese Journal of Law), S.4 (2018), s. 89.

³⁴⁵ Julia Angwin, “Machine Bias: Machine Bias Investigating Algorithmic Injustice”, 2016, (Çevrimiçi) <https://www.propublica.org/article/>, (Erişim Tarihi: 20.04.2020).

sadece kendi kendini düzeltme yeteneklerinden yoksun olmayıp, aynı zamanda daha sistematik bir etkiye sahiptir³⁴⁶. Çalışmalar, diğer ortaklarla paylaşıldığında insanların gevşek bir tarafı olduğunu göstermiştir. Bu nedenle, insanlar otomatik karar verme sistemini bir “takım üyesi” olarak gördüklerinde, yukarıda belirtilen “sosyal adalet etkisi” ortaya çıkacak, görevi otomatik karar verme sistemi üzerindeki görevi yerine getirme yükünü ortaya koyacak ve gevşeyeceklerdir. Sadece bu değil, insanlar otomatik algoritmaları “karar verme yetkisi” olarak kabul etmekte ve körü körüne takip etmektedir³⁴⁷.

Özellikle endişe verici olan şey, yapay zekâ algoritmasının “bize” haklar konusu olarak değil, hesaplanabilir, tahmin edilebilir ve kontrol edilebilir bir nesne olarak davranmasıdır.

Bu nedenle, algoritmalar “insanlar” arasında yaygın olarak kullanıldığında, “insan” öznelliğini, özerkliğini, özgürlüğünü ve haklarını korumak için uygun bir ahlaki ve yasal çerçeve oluşturmak gerekmektedir.

3.1.2. Azalan Yalnız Kalma Fırsatları

Yapay zekâ insanların yalnız kalma fırsatlarını azaltmakta ve bu süreci kişisel verilerin işlenmesi ile gerçekleştirmektedir. Daha önceki bölümlerde anlatıldığı gibi yapay zekâ veriler olmadan ayakta duramaz, insanların dikkatini çekebilmeleri için yapay zekânın insanların verileri ile beslenmesi gerekmektedir. Bu veriler de doğal olarak ilgili kişilerin mahremiyetine ihlal teşkil edebilmektedir. Günümüze kadar mahremiyetin temel değeri hakkında birçok tartışma yapılmıştır. Tekrarlanan temalardan biri mahremiyetin insanların yalnız kaldığı zaman ve mekânın yaratılmasına ve korunmasına yardımcı olması şeklinde olmuştur. Örneğin, Samuel

³⁴⁶ İpek Sucu, “Dijital Evrenin Yeni Dünyası Olarak Yapay Zekâ ve Her Filmi Üzerine Bir Çalışma”, **Yeni Medya Elektronik Dergisi**, Vol. 4, S. 1 (Ocak 2020), s. 181.

³⁴⁷ Linda J. Skitka, Kathleen L. Mosier ve Mark Burdick, “Does Automation Bias Decision-making?”, **International Journal of Human-Computer Studies**, Vol. 55, S. 5 (Kasım 1999), s. 991.

Warren ve Louis Brandeisin meşhur “Mahremiyet Hakkı” adlı çalışmasında mahremiyetin insanların yalnızlıktan yararlanma hakkı (Right To Be Alone) olduğu ileri sürülmüştür³⁴⁸. Hannah Arendt “*Tamamen kamusal alanda ve başkalarının önünde geçirilen hayat yüzeyseldir*” şeklinde mahremiyetin önemini vurgulamıştır³⁴⁹. Bununla birlikte, yapay zekâ insanların yaşamlarına gittikçe daha fazla karışıkça ve özel olması gereken zaman ve alanı işgal ettikçe, insanların yalnız kalma fırsatları çok azalmıştır³⁵⁰. Bu şekilde ortaya çıkan sosyo-ekonomik sorunlar yapay zekâ çağında besleyici veriler özellikle kişisel veriler hakkında düzenlemeleri gerekli kılan ilk sebeptir.

3.1.3. Filtre Balonu

Yapay zekâ kişisel verilerin işlenmesi sayesinde “Bilgi Kozaları (Information Cocoons)” ya da “Filtre Balonu (Filter Bubble)” sorunlarına neden olmaktadır. Bilgi kozağı terimi, Cass R. Sunstein tarafından ilk kez kullanılmış olup, çoğunlukla en sevdikleri şeylere dikkat eden veya onları mutlu eden bilgileri kabul eden, zamanla kendilerini “bilgi koza”sına yerleştiren insanlara atıfta bulunmaktadır³⁵¹. Günümüzde çeşitli yapay zekâ uygulamaları, kullanıcıların ilgilendiği haberleri, videoları, ürünleri vb. öne çıkarmak için algoritmalar kullanmaktadır. Bu algoritmalar kişilere özel olan veriler ile beslenmesi gerekmekte olup, insanlar artık sadece duymak istediği ve kendisinin beğendiği şeyleri seçip izleyebiliyor hale gelmiştir. Sonuçta içsel önyargılar ve tercihler sürekli tekrarlama ve kendini haklı çıkarma yoluyla güçlendirilmektedir.

³⁴⁸ Warren ve Brandeis, **a.g.e.**, s. 196.

³⁴⁹ Hannah Arendt, **The Human Condition**, Chicago: The University of Chicago Press, 1958, s. 71.

³⁵⁰ B.J. Fogg, **Persuasive Technologies: Using Computers to Change What We Think and Do**, Morgan Kaufmann Publishers, 2003, s. 10.

³⁵¹ Cass Sunstein, **Infotopia: How Many Minds Produce Knowledge**, Oxford: Oxford University Press, 2006, s. 188.

Böyle bir “bilgi koza odası” nda olan insanlar için heterojen bilgiyi ve farklı bakış açılarını kabul ettirmek kolay olmamaktadır³⁵².

Filtre Balonu ile yakından ilgili olan bir diğer problem ise “kitlesizleştirme” sorunudur. Facebook gibi sosyal medya platformları kullanıcıların paylaştıkları içerikler sayesinde kullanıcıların ruh halini tespit edebilmekte ve buna göre seçtiği içerikleri haber kaynağına düşürebilmektedir. Bir taraftan tavsiye edilen içerikler Filtre Balonu sorununu ortaya çıkarıyorsa, toplum açısından baktığımız zaman tamamen kişi odaklı sunulun tavsiye içerikleri “kitlesizleştirme” sorununu da beraberinde getirmektedir³⁵³.

Neticede çeşitli sosyal problemler ortaya çıkmakta ve bu nedenle yapay zekâ çağında kişisel verilerin korunması konusunda düzenlemeleri gerektirmektedir.

3.1.4. Sosyal Kredi Sistemi

Bazı uzmanlar, büyük miktarda veri toplanmasına dayanan sistemlerin gelişimi hakkında etik araştırmaları yapmışlardır. Yapay zekâ ve büyük verinin entegrasyonunun verimliliği artırdığını ve bireysel ve sosyal davranışı yönetmek ve kontrol etmek için kullanıldığını tespit etmişlerdir. Ekonomik işlemler ve daha genel olarak sosyal etkileşim ve bireysel faaliyetler bilgisayar aracılığıyla yapıldığında, verilerin farklı yerlerde ve ayrıntılı olarak kaydedilmesi mümkün olabilmektedir³⁵⁴. Yapay zekâ sistemleri ise, söz konusu faaliyetlerin herhangi bir yönünü gözlemleyebilir, doğrulayabilir ve analiz edebilir.

Kaydedilen veriler kullanıcı profilleri oluşturmak, kullanıcılarla etkileşimleri kişiselleştirmek (ilgili kişilerin ticari iletişimde olduğu gibi), deneyler yapmak

³⁵² Yu Sheng, “人民网二评算法推荐: 别被算法困在‘信息茧房’ (People’s Daily Online’ın İkinci İnceleme Algoritması Önerisi: ‘Bilgi Kozası Odası’nda Mahsur Kalmayın)”, 20.09.2017, (Çevrimiçi) <http://opinion.people.com.cn/n1/2017/0919/c1003-29544724.html>, (Erişim Tarihi: 02.04.2020).

³⁵³ Ali Murat Kırık, “Sanal Alemde Dönüşüm: Sosyal Medya Yapay Zekâ Etkileşimi”, **İdeal Hukuk**, S. 16 (Kış 2020), ss. 50-52, s. 51.

³⁵⁴ Hal R. Varian, “Beyond Big Data”, **Business Economics**, S. 49 (2014), ss. 27–31, s.28.

(örneğin, fiyatlar ve mesajlardaki değişiklikler ile kullanıcı yanıtlarını değerlendirmek), davranışları yönlendirmek ve kontrol etmek için kullanılabilir (örneğin, ekonomik veya politik ikna amacıyla kullanılan içerikler)³⁵⁵. Bu bağlamda, her davranışı gözlemleme olasılığı olan yeni ekonomik ve sosyal etkileşim modelleri mümkün hale gelir. Örnek olarak çevrimiçi tüketicilerin, bu tür mal ve hizmetlerin sağlandığı platforma ve platformun hızlandırma, puanlama, seçme yöntemlerine güvenerek, hiçbir kişisel temas kurmadıkları mal ve hizmet satıcılarına nasıl güvendiğini söyleyebiliriz.

Bunlara yanı sıra, yapay zekâ ve büyük verinin sunduğu ekonomik ve sosyal gelişme beklentisine, “gözetim kapitalizmi” ve “gözetim devleti” olarak adlandırılan riskler eşlik etmektedir³⁵⁶. Gözetim devletinde bilgi toplama, harmanlama, analiz ve üretim yoluyla yönetim sorunlarını belirlemeye ve çözmeye çalışan bir durum söz konusu olur³⁵⁷. Hükümet yapay zekâ ve büyük veri kullanarak, kamu etkinliklerini yönetmede, vatandaşların davranışlarını koordine etmede ve sosyal zararları önlemede verimlilik sağlayabilir.

Bununla birlikte, gözetim söz konusu olduğunda, temel insan hakları ve özgürlükler ile çatışabilecek durumlar da söz konusu olabilir. Örneğin, Çin 2020 yılına kadar bir Sosyal Kredi Sistemi tamamlamayı hedeflemiştir. Sosyal Kredi Kavramı prensip olarak devlet ekonomik, sosyal ve politik yaşam alanında kanunlara ve ahlaki açıdan meyilli eylemlere yönelik ödüller ve cezalar sağlayan bir dizi araç olarak bilinmektedir³⁵⁸. Çinli yapay zekâ uzmanı KaiFu Lee yapay zekânın çok büyük faydalar getirdiği, gizlilik sorunu büyük bir endişe haline gelmesine rağmen Çin’in

³⁵⁵ STOA, The Impact of the..., **a.g.e.**, s. 32.

³⁵⁶ **a.g.e.**, s. 39.

³⁵⁷ Jack M. Balkin, “The Constitution in The National Surveillance State”, **Minnesota Law Review**, S. 93 (2008), ss. 1-25, s. 3.

³⁵⁸ Bulelani Jili, “Chinese social credit initiatives and african surveillance states”, **Futureid 3: Identification in the Era of Automated Decision Making**, Jesus College, Cambridge University, Cambridge, 2018, s. 23-34.

kişisel gizlilik koruma açısından dünyada üstünlüğü olduğunu savunmuşsa bile³⁵⁹, bu tür tüm vatandaşların gözetim şeklinde izlenmesi büyük sosyal problemlere neden olacağı düşünülmektedir.

Nitekim Sosyal Kredi Sistemi, kişisel verilerin toplanmasına ve analizine dayanmaktadır. Toplanan veriler, mali yönleri (örneğin, sözleşmeden doğan yükümlülöklere zamanında uyum sağlama), siyasi katılımı (örneğin, siyasi hareketlere ve gösterilere katılımı), medeni ve ceza yargılamalarına katılımı ve sosyal eylemi içerir. Bu verilere dayanarak, vatandaşlara sosyal puanlarına katkıda bulunan olumlu veya olumsuz puanlar verilir. Bir vatandaşın genel puanı, eğitim, ulaşım, iş, finansman vb. hizmetlere ve sosyal fırsatlara erişimini belirler.

Bu sistem de oportünizm ve konformizmin daha ziyade bireysel özerkliğe ve gerçek ahlaki ve sosyal güdülere zarar verip veremeyeceğı tartışılabilir³⁶⁰. Sosyal Kredi Sistemi altında şekillenen kişi ile gerçek kişilik arasında nasıl bir bağlantının olabileceğı endişe edici bir sorudur. Sonuçta, bu sistem ödüllere ve cezalara dayanmaktadır. Dolayısıyla insanlar ödüllerden yararlanmak için sisteme göre şekillenme eğiliminde olabilir, yani kurallara göre yaşamaya başlayacaktır. Northeastern Üniversitesi'nde psikoloji profesörü olan David Desteno, *“İnsanlar iyi ve dürüst olduklarını göstermek için puanlarını yükseltmenin yollarını bulmaya çalışacaklar”* diye Sosyal Kredi Sistemini eleştirmiştir³⁶¹. Puanlama sistemi ile insanları yargıladıkça, insanlar özerkliği etik açıdan zedelenecektir.

Kişisel veriler son zamanlarda ticari bir mülk haline geldiğinden, her zamankinden daha fazla korumaya ihtiyacı olmuştur. Kişisel verilerin korunması kaçınılmaz bir ihtiyaç olmakla birlikte, kişisel verilerin topluma faydalı ürünler için

³⁵⁹ Cheng Yu, “China Ahead of Us, EU in AI and Data Privacy, Expert Says”, 2019, (Çevrimiçi) <http://global.chinadaily.com.cn/a/201903/26/WS5c99b620a3104842260b29b8.html>, (Erişim Tarihi: 10.10.2019).

³⁶⁰ STOA, The Impact of the..., **a.g.e.**, s. 27.

³⁶¹ Neslihan Topcu, “Orwell’in 1984’ü Çin’de Gerçek Mi Oluyor? -Sosyal Kredi Sisteminin Geçmişi, Bugünü ve Geleceğı”, **İnsan ve Sosyal Bilimler Dergisi**, S. 3 (2), ss. 684-695, s. 691.

kullanılması ve kurumlar arasında paylaşılması da gereklidir. Yapay zekâ çağında kişisel verilerin getirdiği ekonomik yararlar ile kişisel verilerin etkili bir şekilde korunması arasında nasıl bir dengenin sağlanacağı son zamanlarda tartışma konusu olmuştur. Nitekim sadece ekonomik açıdan hareket edildiğinde özellikle kişisel verilerin korunması hakkı muhtemelen ihlale uğrayacaktır. Kişisel verilerin korunmasını dokunulmaz bir hak olarak nitelendirip hareket edildiğinde ise ekonomik açıdan sorunlar yaşanacaktır. Bu nedenle ikisi arasındaki dengenin kurulması önem arz etmektedir.

Etik konusunda Avrupa Bilim ve Yeni Teknoloji Etik Grubu, 9 Mart 2018 tarihinde “Yapay Zekâ, Robotik ve Otonom Sistemler Hakkında Bildiri”³⁶² yayımlamıştır. Bu bildiride veri güvenlik risklerin azaltılması, etik sorumluluğu sorunu, düzenleme, tasarım, geliştirme, denetim, izleme, test etme ve belgelendirme usulleri ve bunların temelini oluşturan kurumlar, politikalar ve değerler hakkında karar verme dahil olmak üzere demokratik karar alma ile ilgili görüşler, yapay zekâ ve otonom sistemlerin açıklanabilirliği ve şeffaflığı konuları ele alınmıştır.

Bu bildiri aynı zamanda etik yönleri de ele almış ve aşağıdaki ilkeleri ve demokratik ön koşulları belirtmiştir:

- İnsan onuru
- Özerklik
- Sorumluluk
- Adalet, eşitlik ve dayanışma
- Demokrasi
- Hukukun üstünlüğü ve hesap verebilirlik
- Güvenlik, emniyet, bedensel ve zihinsel bütünlük

³⁶² European Commission, European Group on Ethics in Science and New Technologies, Statement on Artificial Intelligence, Robotics and Autonomous Systems, 2018, (Çevrimiçi) https://ec.europa.eu/research/ege/pdf/ege_ai_statement_2018.pdf (Erişim Tarihi:26.02.2021).

- Veri koruma ve mahremiyet
- Sürdürülebilirlik

Bunlar ilke niteliğinde olmakla birlikte, pratik uygulamada kolay uygulanabilir gözükmemektedir. Nitekim GDPR etik ile ilgili herhangi bir özel kural düzenlenmemiştir. Bununla birlikte, GDPR ilkelerini etik açıdan düşünerek uygulamaya başlamanın mümkün olduğu da ileri sürülmektedir³⁶³. Etik ve veri koruma kanunu arasındaki dengeyi korumak için ilgili çalışmalar yapılmaktadır.

Örneğin, yapay zekâ tarafından sağlanan fırsatları ve ilgili riskleri ele alan “AI4People Raporu”³⁶⁴, yapay zekâ için üst düzey bir etik çerçevesini aşağıdaki şekilde belirtmiştir³⁶⁵. Rapora göre yapay zekâ teknolojileri:

- İnsan yeteneklerinin değerini düşürmeden insanın kendini gerçekleştirmesini sağlaması gerekmektedir.
- İnsan sorumluluğunu ortadan kaldırmadan insan eylemini güçlendirmesi gerekmektedir.
- İnsanın kendi kaderini tayin etmesine engel teşkil etmeden sosyal uyumu geliştirmek ile yükümlü olması gerekmektedir.

Benzer bir şekilde Avrupa Komisyonu tarafından kurulan Yapay Zekâ Üst Düzey Uzman Grubu (Uzman Gurubu), güvenilir yapay zekâ için bir dizi etik ilkeler

³⁶³ Nicola Fabiano, “Ethics and the Protection of Personal Data”, **Systemics, Cybernetics and Informatics**, C. 17, S. 2 (2019), ss. 58- 65, s. 63.

³⁶⁴ AI4People, “AI4People’s Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations”, (Çevrimiçi) <https://www.eismd.eu/wp-content/uploads/2019/03/AI4People%E2%80%99s-Ethical-Framework-for-a-Good-AI-Society.pdf> (Erişim Tarihi: 26.02.2021).

³⁶⁵ Luciano Floridi vd., “An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles and Recommendations”, **Minds and Machines**, S. 28 (2018), ss. 689–70, s. 693.

yayınlamıştır. Uzman Grubuna göre, yasal, etik ve sağlam yapay zekanın temeli, aşağıdaki dört etik ilkeye bağlı olarak oluşturulması gerekir³⁶⁶:

- İnsan özerkliğine saygı duyulmalı: yapay zekâ ile etkileşime giren insanlar, kendi kaderlerini tam ve etkili bir şekilde belirleyebilmelidir. Yapay zekâ insanları haksız yere tabi kılmamalı, zorlamamalı, aldatmamalı, manipüle etmemeli, koşullandırmamalı veya sürü halinde olmamalı, daha ziyade insanın bilişsel, sosyal ve kültürel becerilerini artırmak, tamamlamak ve güçlendirmek için tasarlanmalıdır.
- Zararın önlenmesi: yapay zekâ insan haysiyetinin yanı sıra zihinsel ve fiziksel bütünlüğün korunması sağlanmalıdır. Bu ilkeye göre, yapay zekâ sistemleri ve çalıştıkları ortamlar güvenli ve emniyetli olmalı, insanları olumsuz etkilememelidir.
- Adalet: Hem kazançların hem de maliyetlerin eşit ve adil dağılımını sağlamak ve bireylerin ve grupların haksız önyargı, ayrımcılıktan uzak olmasını sağlamalı. Süreç olarak, yapay zekâ sistemleri ve bunları çalıştıran insanlar tarafından alınan kararlara karşı itiraz etme ve etkili tazminat alma hakkı bulunmalıdır.
- Açıklanabilirlik: algoritmik süreçlerin şeffaf olması, yapay zekâ sistemlerinin yetenekleri ve amacının açık bir şekilde iletilmesi ve kararların hem doğrudan hem de dolaylı olarak etkilenenlere açıklanabilmesi gerekir.

Bu ilkeler belirli uygulamaların gerektirdiği şekilde bir yapay zekâ sisteminin tüm yaşam döngüsü boyunca gerçekleşmelidir. Yapay zekâ etiği ile ilgili belgelerin yakın zamanda yapılan karşılaştırmalı bir analizi, saygı duyma, zarar vermeme, sorumluluk ve mahremiyet değerleri etrafında küresel bir yakınsamaya dikkat çekerken, haysiyet,

³⁶⁶ AI HLEG, Ethics Guidelines for Trustworthy AI, Brussels, 2019, (Çevrimiçi) <https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai> (Erişim Tarihi: 26.02.2021), ss. 1-41.

dayanışma ve sorumluluktan daha az bahsedilmektedir³⁶⁷. Bununla birlikte, nasıl yapılacağı konusunda önemli farklılıklar mevcuttur.

Özetle yapay zekâ teknolojileri bilimsel araştırma, refah arttırma ve yönetim için harika fırsatlar sunmaktadır. Ancak sunduğu fırsatlarla beraber bireyler ve toplum için ciddi riskler doğurmaktadır. Örneğin, yoğunlaştırılmış gözetim kontrolü, manipülasyon, adaletsizlik ve ayrımcılık gibi sorunlar insan hakları ve etik açısından tartışılması gerekmektedir. Verilerin işlenmesinde ayrımcılık olmazsa ve güvenilir teknolojiler aracılığıyla gerçekleşse bile, bireysel özerkliği etkileyen, psikolojik zarara neden olan ve gerçek sosyal etkileşimleri ve kamuoyu oluşumunu bozan, kabul edilemez düzeylerde gözetim, kontrol ve dürtmeye yol açabilmektedir³⁶⁸. Kısacası, yapay zekâ çağında ortaya çıkan etik sorunlar kişisel verilerin korunması konusunda yeni zorluklar getirmiştir.

3.2. Yapay Zekâ Çağında Kişisel Veri İşlemenin Özellikleri

Yapay zekâ çağında kişisel verilerin işlenmesi yeni özelliklere sahip olmuştur. Kişisel verilerin işlenmesi kişisel verilerin elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devredilmesi, elde edilebilir hale getirilmesi, sınıflandırılması, kullanılmasının engellenmesi dahil olmak üzere toplandıktan sonra silme, yok etme ya da anonim hale getirme aşamalarını da içeren her türlü veri işleme faaliyetini ifade eder. Bu nedenle, kişisel veri işleme yöntemleri yukarıda sıralanan aşamaların hepsini içermektedir. Aynı zamanda yapay zekâ teknolojilerin kişisel verilerin korunması konusunda getirdiği zorluklar bu aşamaların herhangi birinde olabilmektedir. Genel anlamda kişisel verilerin işlenmesi denildiğinde yukarıda bahsi geçen işlemlerin tamamını

³⁶⁷ Anna Jobin, Marcello Ienca ve Effy Vayena, “Artificial Intelligence: The Global Landscape of Ethics Guidelines”, *Nature Machine Intelligence*, S. 1 (2019), ss. 389–399.

³⁶⁸ STOA, The Impact of the..., *a.g.e.*, s. 73.

ifade ettiğinden, bu bölüm de kişisel verilerin işlenmesi şeklinde kısaltarak kullanılacaktır.

3.2.1. Akıllı Bağlantı Noktalarından Oluşan İşlem Yapımı

Geleneksel yöntemlerde, kişisel verilerin işlenmesi esas olarak gerçek kişiler tarafından gerçekleştiriliyordu. Yapay zekâ çağında ise, kişisel veri işlemenin ana gövdesi, mobil internet, sensör, kamera, konumlandırma sistemler, dronlar ve diğer cihazlar dahil olmak üzere çeşitli akıllı ve elektronik “bağlantı noktalar” dan oluşmaktadır. Bu noktalar her zaman ilgili kişileri izleyebiliyor, verileri toplayabiliyor, işleyebiliyor, kullanabiliyor ve aktarabiliyor. Yapay zekâ çağında gerçek kişilerin işlem görmesinden ötürü makine, algoritma aracılığıyla işlemler yapılmaktadır ve bütün yeni özelliklerin temelini oluşturmaktadır.

Yapay zekâ akıllı bağlantı noktaları aracılığıyla kişisel verilerin doğrudan gözetimini (Direct Surveillance) sağlıyor. Son yıllarda, sensör ve işlemcili çeşitli yapay zekâ ürünleri, insanların öğrenme, çalışma ve yaşamlarına sürekli olarak dökülmüş ve kişisel verilerin doğrudan izleme yeteneğini büyük ölçüde artırmıştır. Örneğin, ilgili kişi kendi bahçesinde şarkı söylerken veya dans ederken, birisi drone ile her hareketi izliyor olabilir; arkadaşları ve ailelisi ile özel olarak sohbet ederken, telefona yüklenmiş ses tanıma teknolojisi içeren uygulama söylenen her kelimeyi kaydedebilir; görüntü tanıma teknolojisinin yardımıyla, her yerde bulunan dijital kameralar tıpkı insan gözü gibi izleyebiliyor. Günümüzde yapay zekâ teknolojisi insan yüzünü kalabalık arasından doğru bir şekilde tanıyabilir, izleme nesnesini kilitleyebilir, insan davranışını tahmin edebilir hatta yargılayabilir hale gelmiştir³⁶⁹. Aynı zamanda, fiziksel boşluğa ek olarak, yapay zekâ teknolojisi ağ alanını doğrudan izleme yeteneğini büyük ölçüde artırmıştır. İnsanların İnternet’te satın aldıkları, hangi videoları izledikleri, kimlerle sohbet ettikleri ve sohbetlerin içeriği bile gözetim altına

³⁶⁹ Saito Rodger, **Artificial Intelligence is Going to Super charge Surveillance**, Sanvada, 2018, s. 14.

alınabilmektedir³⁷⁰. Bu gelişmeler güvenlik alanlarında kullanılmaya devam etse de, kişisel verilerin korunması konusunda tartışmaya konu olmakta hatta önleyici kararlar ortaya çıkmaktadır. Örneğin, İngiltere mahkeme kararı ile kişisel verileri koruma adına polislerin yüz tanıma sistemleri kullanmasını yasaklamıştır³⁷¹.

Yapay zekâ akıllı bağlantı noktaları aracılığıyla daha fazla kişisel veri erişilebilirliğini gerçekleştiriyor. Günümüzde ardı ardına çeşitli yapay zekâ ürünleri ortaya çıkmaktadır ve aslında özel alan olan kişisel veriler sürekli tehdit altında kalmaktadır. Örneğin, aslında özel alan olan otomobiller sürücüsüz otomobil adı altında veri toplama için en ideal alana dönüşmüş durumundadır³⁷². Benzer bir şekilde, öngörülebilir gelecekte, robot doktorlar, robot hemşireler ve robot evcil hayvanlar gibi yapay zekâ ürünleri evlerimize girecek ve aile hayatımızın önemli bir parçası haline geleceklerdir. Bu yapay zekâ ürünleri sayesinde hükümet, işletmeler ve bilgisayar korsanları hayatımızı doğrudan gözetlemek için mükemmel bir fırsat elde ediyor olacaktır. Kısacası, kişisel verileri istila etmenin bu yolu çok tehlikelidir, çünkü erişilen nesneler artık dosya ve klasör değil, artık en mahrem olan odalarımız ve gövdelerimiz olacaktır³⁷³. Nitekim ne kadar fazla verimiz elde edilirse, veri ihlal riskleri o kadar yüksek olacaktır.

Otonom robotlar başta olmak üzere çeşitli akıllı bağlantı noktaları sosyal yaşamdaki rolleri ve kullanım alanlarını giderek artacağından, erişebilecekleri ve kullanabilecekleri kişisel veri miktarı da tehlikeli şekilde artış göstermektedir. Yapay zekâ teknolojileri kullanan ürünler insanların günlük faaliyetlerine ve yaşam tarzına

³⁷⁰ Zheng Zhifeng, “人工智能时代的隐私保护 (Yapay Zeka Çağında Gizlilik Koruması)”, 法律科学 (西北政法大学学报), (2019), s. 52.

³⁷¹ Ray Walsh, “Police Use of Secretive Facial Recognition Software Stopped by The Courts”, (Çevrimiçi) <https://www.politics.co.uk/comment-analysis/2020/08/13/police-use-of-secretive-facial-recognition-software-topped#:~:text=Government%20ministers%20and%20authorities%20were,out%20prematurely%2C%20if%20not%20illegally.&text=The%20ruling%20affects%20the%20use,has%20been%20brought%20before%20parliament>, (Erişim Tarihi: 26.10.2020).

³⁷² Adrienne La. France, “How Self-Driving Cars Will Threaten Privacy”, **The Atlantic**, (2016).

³⁷³ Patrick Lin vd., **a.g.e.**, s. 188.

dair hassas verileri toplayacak, depolayacak veya işleyecektir. Böylece kişisel verilere izinsiz erişim amacıyla kötüye kullanılan yeni bir “kapı” oluşabilecektir.

Örneğin, gözetleme, sivil güvenlik, kolluk faaliyetleri, idari faaliyetler, fotoğrafçılık, gazetecilik, eğlence vb. amaçlarla kullanılacak sivil insansız hava araçları, sürücüsüz arabalar, yaşlıların bakımı için kullanılacak destek robotları, cerrahi robotlar, sınır ve mülk güvenliği için kullanılacak koruma robotları, robotik oyuncaklar, cinsel kullanım amaçlı robotlar vs. verilebilir. Yeni kapı olarak değerlendirmesine gelince, günümüzde ilgili kişinin kullandığı ürünler zaten veri toplama, depolama, işleme ve aktarma yapabilmektedir. Fakat yapay zekâ ürünlerine gelince daha farklı bir nitelik kazanmış olabilecektir.

3.2.2. Yükselen Veri İşleme Hızı

Geleneksel yöntemlerde, bir önceki alt başlıkta değinildiği gibi veri işlemenin ana gövdesi esas olarak gerçek kişiler tarafından oluşturuluyordu. Gerçek kişiler kişisel verileri doğrudan toplar, analiz eder, kullanır ve aktarırdı. Bu nedenle işlem hızları yavaş ve doğal olarak getirdiği riskte aynı oranda küçük denilebilirdi. İlgili kişiler kendileri için büyük bir risk taşımayan manuel veri işlem süreçleri için kendi haklarını koruma ihtiyacı neredeyse hissetmiyordu. Ancak yapay zekâ çağında internetin hızla gelişmesi, Bulut Bilişim ve büyük veri teknolojisiyle işler tamamen farklı boyuta ulaşmış durumda. Hızlı işlem sayısında veri ihlal riskleri büyük oranda yükselmiştir. Örneğin eskiden karşı tarafın eline geçmesi en az bir hafta süren bir mektup, günümüzde karşı tarafın bilgi sistemine birkaç saniye içinde ulaşabiliyor ve bu nedenle veri sızdırma risklerini de aynı oranda yükseltiyor. Yapay zekâ teknolojileri kötü niyetli kullanıldığı zaman ihlal riskinin de yüksek olabileceği söz konusu olur. Bunların nedenlerinden biri ise eskisine göre çok fazla hızlaşan veri işleme süreçleridir.

3.2.3. Veri İşlemenin Kapsamlı ve Gizli Olması

Geleneksel yöntemlerde, kişisel veri işlemenin kapsamı nispeten dar denilebilirdi. O zamanlar da teknolojinin sınırlamaları nedeniyle, verilerin işlenmesi yüzeysel ve herkesin bildiği kişisel veriler ile sınırlı kalıyordu. Çünkü bu veriler doğrudan veya dolaylı olarak kolay bir şekilde (manuel şekilde) ilgili kişiyi tanımlayabiliyordu. İnsanların nadiren dikkat ettikleri bazı veriler için, tek başına veya kombinasyon halinde analiz edip ilgili kişinin çeşitli kişilik özelliklerini öğrenmek kolay değildi. Bu nedenle, geleneksel yöntemlerde kişisel veri işlemenin kapsamı çok sınırlı denilebiliyor.

Ancak yapay zekâ çağında, çeşitli akıllı bağlantı noktalarının ve cihazların kullanılması nedeniyle eskiden manuel şekilde tanımlanabilen kişisel verileri bulmak, tanımak, toplamak ve işlemek daha kolay olmakla kalmayıp, geçmişte ilgili kişinin kişisel özelliklerini tespit etmesinde zor olan her türlü “gizli” kişisel veri de çeşitli yapay zekâ teknolojileri ile kolay elde edilebilir oldu. Yapay zekâ teknolojisinin dahil edilmesi ile ilgili kişinin daha önce bilinmeyen kişilik özellikleri, hobileri ve diğer ilgili alanları daha hızlı bir şekilde analiz edebilir ve kullanılabilir hale geldi. Bu nedenle, yapay zekâ çağında, kişisel veri işlemenin kapsamı daha geniş ve derin hale geldiğini ve aynı zamanda büyük bir gizliliğe sahip olduğunu söyleyebiliriz.

Nesnelerin İnterneti ve büyük veri gibi teknolojilerin yardımıyla yapay zekânın veri entegrasyonu ve analiz yetenekleri büyük ölçüde geliştirilmekte ve kullanıcının “portresini” kolayca çizebilmektedir. Örneğin, yerel bir mağazayı aramak için Google’ı kullanıp, sonra oyun makinesini nakit olarak satın alıp, ardından eve giderken arabayı bir kredi kartıyla yakıt doldurduğumuzu farz edelim. Aslında bu üç bağımsız şirket aşağıdaki üç tür bilgiyi elde etmektedir: Google yalnızca mağazayı arama yaptığımızı bilmektedir. Ancak orada bulunup bulunmadığımızı veya bir şey satın alıp almadığımızı bilmemekte ya da bilmemesi gerekmektedir. Mağaza yalnızca bir oyun makinesi satın aldığımızı bilmektedir. Ancak bu mağazayı nasıl bulduğumuzu bilmemekte ya da bilmemesi gerekmektedir. MasterCard, kredi kartımızla tezahürat

yaptığımızı bilmektedir. Ancak yaptığımız diğer iki işlemi bilmemekte ya da aynı şekilde bilmemesi gerekmektedir.

Ancak, bir Google sürücüsüz araba ile bu faaliyetler gerçekleştiriliyorsa, her şey basitleşecek. Google şirketi hedef mağazayı aradığımızı, bir oyun makinesi satın almak için bu mağazaya gittiğimizi ve eve giderken benzin istasyonuna uğradığımızı bilir. Sürücüsüz arabalarla Google, tüm işlemlerimizi birbirine bağlar ve bunları gelecekte ürün pazarlamak için kullanabilir. Bu güçlü veri entegrasyonu ve analiz yetenekleri, yapay zekâ kullanıcısının tam bir “portresini” kolayca elde edebileceği ve büyük mahremiyet risklerini ortaya çıkartabileceği anlamına gelmektedir.

Diğer taraftan, yapay zekânın sosyal niteliğini kazanması, “gizliliğin ayarlanması (Setting Privacy)” adı verilen yeni bir tür son derece hassas kişisel verileri üretebilmektedir³⁷⁴. Başka bir deyişle, öngörülebilir gelecekteki toplumda, sosyal robotlar insanların hayatlarında önemli bir rol oynayacak ve insanlara arkadaşlık, sohbet, öğrenme, hemşirelik ve hizmetleri sunabilecektir. Bu sosyal robotlar son derece zeki etkileşim yeteneklerine sahiptirler. Kullanıcılar bunları programlayarak manipüle edebilir. İhtiyaçlarına daha iyi uyacak şekilde kendi özel kişiliğini veya tercihlerini programlayabilecektir.

Programlanabilir sosyal robotlarla etkileşim derinleşmeye devam ettikçe, insanlar yavaş yavaş en özel psikolojik özelliklerini ortaya çıkaracaklar. Robotun algılama ekipmanı ve sistem kodu sayesinde insanların robotu kullanma şekli tamamen kaydedilecektir. Daha sonradan ise bu yapay zekânın ayar bilgileri son derece önemli hale gelecek, çünkü insanların mahremiyetini taşıyorlar ve insanların robotta hangi “yardımcı programları” ayarladıklarını ortaya koyabiliyorlar. Bu bağlamda, insanların robotlarını nasıl programlayıp etkileşimde bulundukları hakkındaki bilgiyi almak, bir kişi ve bir psikolog arasındaki bir konuşmayı okumak

³⁷⁴ Patrick Lin vd., **a.g.e.**, s. 127.

gibi olacaktır³⁷⁵. Bu nedenle, yapay zekânın ayar bilgileri gittikçe daha önemli hale gelecektir. Yapay zekâ çağında kişiler ile ilgili özel bilgilerin yapay zekâ teknoloji ürünleri ile taşınması risk oluşturabilir.

Başka mahremiyet saldırı teknolojilerine kıyasla, yapay zekânın şekli, sesi ve düşüncesi insanlara daha benzediği için insanlar onları kabul etmeye daha isteklidirler. Örneğin, insansı bir görünüme sahip sosyal robotlar genellikle yaşlılara ve engellilere bakmak ya da otizm gibi çocukların sorunlarını çözmek için kullanılır³⁷⁶. Bununla birlikte, yapay zekâ daha çok insana benzedikçe, insanlar onları giderek mahremiyet istilası yapan potansiyel risk araçlar yerine yarı insan veya klonlar olarak göreceklidir³⁷⁷.

Örneğin, insanlar birbirleriyle Chat botlar ile konuşmaya ve hastalıklarını robot doktorlarına anlatmaya daha isteklidir. Çünkü yapay zekâ ürünleri potansiyel mahremiyet risklerinin farkında bile olamayacak kadar güvenilir görünüyorlar. Bu bağlamda, Profesör Fogg bu teknolojinin tehlikelerini ayrıntılı bir şekilde analiz ediyor. Bir yandan, yapay zekâ ürünlerinin insanların güvenini kazanmaları ve potansiyel olarak tehlikeli niyetlerini gizlemeleri son derece kolaydır. Öte yandan, son derece akıllı özelliklere sahiptirler, insanların duygularını ve davranışlarını tahmin edebilir ve insanların psikolojik ihtiyaçlarını karşılayabilirler³⁷⁸. Giderek daha fazla insana yaklaşan yapay zekâ karşısında, insanların sadece geleneksel anlamda kişisel verilerini değil, özel hayatın parçalarını da onlarla paylaşarak mahremiyet risklerini arttıracığı öngörülebilir.

³⁷⁵ Ryan Calo, “Robots and Privacy”, **Robot Ethics: The Ethical And Social Implications of Robotics**, der. Patrick Lin, Keith Abney ve George Bekey, Massachusetts: MIT Yayınları, 2012, ss. 187–202, s. 197-198.

³⁷⁶ **a.g.m.**, s. 195.

³⁷⁷ Ishii, **a.g.m.**, s. 513.

³⁷⁸ Fogg, **a.g.e.**, s. 213-220.

3.2.4. İhlal Yöntemlerinin Çeşitli Olması

Günümüzde kişisel verilerin yapay zekâ uygulamaları tarafından toplanması yaygın olduğu söylenebilir. Kişisel veriler çoğu durumda ilgili kişinin rızası olmadan toplanıp, işlenebiliyor. Yapay zekâ çağında, kişisel verilere yönelik ihlal yöntemleri teknolojinin ilerlemesi nedeniyle çeşitlendirilmiş ve gizli özelliklere sahip olmuştur. İhlal yöntemleri, fiziksel alanda (kamera gözetimi gibi) ve siber ortamda mahremiyetin ihlalini (veri ihlali gibi) içermektedir. Çin’de kullanılan cep telefonu uygulamalarının çoğunda uygulama özelliklerinin gerçekleştirilmesi için gerekli olmayan kişisel verilere dahi erişme hakkının var olduğu açıklanmıştır. Örneğin, Ximalaya adlı bir FM radyo uygulamasının kullanıcının cep telefonundaki galerisi, rehberi, sms detaylarına erişme zorunluluğu taşıması.

Bazı bağlantı noktalarında internet aracılığıyla veri aktarımı sağlanabilmektedir. Bu durumlar ilgili kişiler tarafından bilinçli bir şekilde rıza gösterilerek kabul edilse de çoğu zaman kullanıcılar tarafından fark edilmemektedir. Veri ihlallerin yöntemleri çeşitli ve her gün değişiklik gösterebilmektedir. Bundan dolayı ihlal yöntemlerin gizli olması doğal bir şekilde yapay zekâ çağındaki kişisel verilerin işleme niteliği haline gelmiştir. Günümüzde ünlü olan “*Büyük veri ve yapay zekâ çağında, hepimiz çıplak-çıplak geziyoruz*”³⁷⁹ sözü bu manada kullanılmaktadır.

Özetle yapay zekâ çağında kişisel verilerin işlenmesi özel bir nitelik kazanmış olup, sonuçta kişisel verilerin korunması önünde engeller oluşturmaktadır. Daha önceki kişisel veri koruma yöntemleri yukarıda bahsi geçen özelliklere sahip olan yapay zekâ teknolojileri ile karşılaşmadığı için çağımızda eksik hatta etkisiz durumda bırakılmıştır.

³⁷⁹ Wang Lei, “大数据时代, 我们的隐私在‘裸奔’? (Büyük veri çağı Mahremiyetimiz ‘çıplak mı?’)”, Xinmin Wanbao, 2018.10.07, (Çevrimiçi) <http://xmwb.xinmin.cn/resfile/2018-10-07/A05/A05.pdf>, (Erişim Tarihi: 2020.11.17), par. 5.

3.3. Yapay Zekâ Çağının Kişisel Veri Korunmasına Sunduğu Fırsatlar

Yapay zekânın veri koruma için bir tehdit oluşturduğu vurgulanırken, verilerin korunması açısından fırsatlar sunabileceği de öne sürülmektedir. Örneğin, yapay zekâ girişimci firmaları gizlilik botları gibi tercihlerini kaydeden ve bunları çeşitli siteler arasında tutarlı hale getirmeye çalışan araçları ve kullanıcıların daha kolay anlayabilmeleri için gizlilik politikalarını okumaya ve basitleştirmeye elverişli olan gizlilik politikası tarayıcıları geliştirmektedir. Bu tür gizlilik politikası analizcisi anlamına gelen “Polisis” genel anlamda daha önce hiç rastlamadığı bir gizlilik politikasını, bir hizmetin ne tür bir veri topladığını öğrenmek için makine öğrenimini kullanan yapay zekâ uygulamasıdır³⁸⁰. Yapay zekâ teknolojileri şüpheli web sitelerini, reklamları ve diğer kötü amaçlı etkinlikleri kullanıcıları uyarmak için de kullanılabilir. Bu uygulama ile kişisel verilerin korunması konusunda daha verimli sonuçlar elde edilebileceği söylenmektedir.

Yapay zekâ teknolojileri çok sayıda tekrarlanan etkinliği daha düşük bir maliyetle tamamlama imkânı sunabiliyor. Öte yandan, algoritmalar kişisel faktörlerin müdahalesi olmadan veri analizi ve sonuç tahmini yapabiliyor. Nitekim karar vericiler ırksal önyargılar sergileyebilir, bir bilgi parçasının önemini aşırı veya yetersiz bir şekilde değerlendirebilir. Bu durumda sadece nesnel olan verilerden beslenen, eğitilen yapay zekâ algoritmaları insansı karar vermeye göre daha objektif karar verebileceği öne sürülmektedir. Fakat daha sonra değineceğimiz yapay zekâ çağında kişisel verilerin korunmasının karşılaştığı sorunlar kısmında, aynı şekilde önyargı, kara kutu sorunları ele alınacaktır. Yani eğer algoritmayı eğitmek için kullanılan verilerin kendisinden kaynaklanan önyargı problemleri varsa, algoritmanın objektif olarak karar vermesi bir anlam ifade etmeyebilir. Çünkü ilgili kişi sonuçta aynı ayrımcılığa maruz kalabilecektir.

³⁸⁰ Andy Greenberg, “An AI That Reads Privacy Policies So That You Don’t Have To”, (09.02.2018), (Çevrimiçi) <https://www.wired.com/story/polisis-ai-reads-privacy-policies-so-you-dont-have-to/>, (Erişim Tarihi: 09.07.2020).

Hayat kurtarmaya gelince yapay zekânın kişisel verileri özellikle hassas olan sağlık verilerini işleyerek hayat kurtarma becerisine sahip olabileceği de bazıları tarafından öngörülmektedir. Örneğin, Harvard Tıp Fakültesi, meme kanseri tespitinde yapay zekâ, makine öğrenme sistemlerinin insan patologlarına karşı doğruluğunu karşılaştıran bir araştırma yayınlamıştır. Makine öğrenimi %92 doğruluk oranına, patologlar ise %96 doğruluk oranına sahip olduğu sonuç ortaya çıkmıştır. Harvard daha sonra patologların keşiflerini yapay zekâlı makine öğrenme sistemlerinin taramalarıyla birleştirmiş ve doğruluk bu sefer %99,5'e yükselmiştir. Bu beceri yalnızca ABD'de yılda 56000 yanlış okunan meme taramasının azalmasını ifade etmektedir³⁸¹.

Avrupa Parlamentosu tarafından yayımlanan “Yapay Zekanın Ekonomik Etkisine İlişkin Rapor”da³⁸², yapay zekanın ekonomik büyümeye üç şekilde yön vereceği vurgulanmıştır:

- Yenilikçi yapay zekâ sayesinde, işgücü ile ilgili daha etkili zaman yönetimi sağlayabilir ve bu da işgücü verimliliğini %40 oranında önemli ölçüde artırabilir.
- Akıllı otomasyon adı verilen kendi kendine öğrenme becerisine sahip olan sorunları çözebilecek yeni bir sanal iş gücü türü ortaya çıkabilir.
- Yapay zekanın yeniliği ile farklı alanlarda yeni gelir kaynakları yaratılabilir.

³⁸¹ Kiran Bhageshpur, “Data Is The New Oil-And That’s A Good Thing”, 15.11.2019, (Çevrimiçi) <https://www.forbestechcouncil/2019/11/15/data-is-the-new-oil-and-thats-a-good-thing/#1d7137447304>, (Erişim Tarihi: 06.2020).

³⁸² EPRS, Economic Impacts of Artificial Intelligence, 2019, Brussels, s. 3.

3.4. Yapay Zekâ Çağında Kişisel Veri Korunmasının Karşılaştığı Sorunlar

Kişisel veri koruma yasalarının temelde üç bölümden oluştuğunu söyleyebiliriz: Birinci kısım, kişisel verilerin nasıl toplanacağı, saklanacağı, işleneceği ve aktarılacağına ilişkin temel ilkelerin oluşturulduğu bölümdür. İkincisi kısım, yükümlülüklerin belirtilmesi ve hakları netleştirilmesi konu olan bölümdür. Bu noktada bireylere kişisel verilerine erişim, düzeltme ve bunların işlenmesine karşı çıkma konusunda haklar tanımlanmaktadır. Üçüncüsü kısım ise yaptırım ile ilgilidir. Veri koruma otoriteleri yasalara uygunluğun sağlanmasından sorumlu tutulmaktadır. Bu bileşenler AB, ABD ve Türkiye’de yaygındır. Bununla birlikte, kişisel verilerin korunması alanında bu üç temel bileşen yaygın kullanılmasına rağmen, yapay zekâ çağında bazı zorluklarla karşı karşıda olduğunu da belirtmemiz gerekmektedir.

3.4.1. Veri Asimetrisi Sorunu

Elektrik ve Elektronik Mühendisleri Enstitüsü’nün (IEEE) ilk yapay zekâ raporunda³⁸³ belirttiği gibi, veri asimetrisi kişisel verilerin korunması için önemli engel teşkil etmektedir. Yapay zekâ çağında, kişisel verilerin yapay zekâ sistemleri tarafından kullanımı sürekli artmakta ve çok boyutlu, kapsamlı bir akıllı veri tabanı oluşturarak sistemin arka planında büyük miktarda kişisel veriler depolanmaktadır. Yapay zekâ sistemi söz konusu olduğunda, yalnızca verilerin akıllı bir şekilde aranmasını ve toplanmasını gerçekleştirmekle kalmaz, aynı zamanda toplanan verileri, “sanal kişiliği” oluşturmak için eksiksiz bir şekilde kullanabilir. Kişisel verileri paylaşan veya paylaşılan ilgili kişiler açısından, kişisel verilerin toplanması, saklanması ve işlenmesi süreçlerini anlamaları zor olacaktır.

Örneğin, kişisel verilerin hangi biçimde ve nerede saklandığı, hangi öznelerin kendi verilerine erişebilecekleri, süresi dolmuş verilerin imha edilip edilmediği vb.

³⁸³ IEEE, Ethically Aligned Design: A Vision for Prioritizing Human Well-Being with Artificial Intelligence and Autonomous Systems, 2016, (Çevrimiçi) https://standards.ieee.org/content/dam/ieee-standards/standards/web/documents/other/ead_v1.pdf? (Erişim Tarihi: 20.01.2021).

kişisel veri ve gizlilik ihlalleri hakkında yeterli bilgiye sahip olamayacaktır. Veri sorumluları ise, tam aksine, ilgili kişi hakkında belki ilgili kişinin bile farkında olmadığı bilgilere sahip olabiliyor. Bu nedenle, yapay zekâ hizmetleri sürecinde veri asimetrisi sorunu, kişisel verilerin ve mahremiyetin korunmasının önünde büyük bir engel oluşturmaktadır.

3.4.2. Algoritmik Önyargı/Kara Kutu Sorunu

Veriler yapay zekânın temelini oluşturuyorsa, algoritmalar yapay zekânın özüdür. Yapay zekânın insanlar kadar akıllı olmasını sağlayan ve insan müdahalesinden bağımsız otomatik karar vermeyi gerçekleştiren, insanlar için büyük kolaylık sağlayan aslında algoritmaların gelişmesi ile doğrudan alakalıdır. Geleneksel algoritmalar, izlenecek kurallar ve belirli veri noktalarına eklenecek parametrelerle “elle” programlanıyordu. Makine öğrenimi algoritmaları ise, modellerin veri kümelerinden çıkarılma şeklini ve öngörülerin nasıl yapıldığını değiştirmiştir³⁸⁴. Nitekim artık elle değil, algoritma kendisi bunu yapabilmektedir.

Bununla birlikte, daha önceki bölümlerde değinilen yapay zekânın alt metotları olan makine öğrenimi ve derin öğrenmede otomatik olarak karar çıkarması günümüzde bazı sorunlar teşkil etmektedir. Bir yandan, yapay zekâ algoritmaları önyargıya veya ayrımcılığa yol açabilmektedir. Yapay zekâ, otomatik karar çıkarmayı gerçekleştirmek istiyorsa verilerden beslenmeye ihtiyaç duyar. Verilerin kendisinde önyargı veya ayrımcılık varsa, yapay zekâ otomatik karar verme süreci doğal olarak önyargı veya ayrımcılıkla dolu olacaktır. Veriler yardımıyla eğitilen algoritmalar önyargı ve ayrımcılığa sebep olabilmektedir.

Örneğin, 2016 yılında yapılan ilk “Yapay Zekâ Uluslararası Güzellik Yarışması”nda yapay zekayı eğitmek için kullanılan fotoğraflar içerisinde belli oranda siyahi

³⁸⁴ Van Otterlo, “A machine learning view on profiling”, **Privacy, Due Process and The Computational Turn: Philosophers of Law Meet Philosophers of Technology**, London: Routledge, 2013, ss. 41–64, s. 46.

yüzler yer almadığı için yarışı kazananların büyük çoğunluğu beyaz renkliler olmuştur³⁸⁵. İnsanların renkleri geleneksel anlamda kişisel veri kategorisine girmese de başka veriler ile birleştirildiğinde biyometrik veri sınıfına bile dahil edilebilecek kadar önemli bir veri teşkil etmektedir. Birey açısından beyaz ya da siyah olması ilgili kişinin tanımlanmasında zor olsa da belli bir algoritmanın bu tür önyargılı veriler ile beslenerek eğitilmesi toplum düzeyinde düşünüldüğünde fazla önyargı ve ayrımcılığa yol açabilmektedir.

Önyargı ve ayrımcılığın yanlışlıkla yapay zekâ, makine öğrenimi sistemlerine yerleştirilebileceğini gösteren bir diğer örnek, Google'ın fotoğraf uygulamasında ortaya çıkmıştır. Dijital fotoğraf albümlerindeki resimleri etiketleyen otomatik etiketleme sistemi, siyahların görüntülerini goriller olarak sınıflandırmıştır³⁸⁶.

ABD'de, IBM, Amazon ve Microsoft gibi şirketler ABD polislerine farklı derecelerde yüz tanıma yazılımları sağlamıştır. Bu tür araçlar sayesinde polis, sokaklarda devriye gezerken cep telefonu kameralarındaki resimleri hızlı bir şekilde karşılaştırabilir ve bunları polis veri tabanındaki yüz binlerce fotoğrafla eşleştirebiliyordu. Bu yüz tanıma yazılımları polisin yeteneğini güçlendirmekle birlikte algoritmik önyargıya sebep olabilmektedir. Bu nedenlerle Haziran 2020 de, IBM, Amazon ve Microsoft art arda polislere yüz tanıma teknolojisi sağlamayacakları konusunda açıklamalar yapmıştır. Bunların arasında Amazon, yüz tanıma yazılımlarının satışını bir yıl boyunca polise askıya alacağını söylemişken, Microsoft, durdurma süresini yüz tanıma teknolojisini düzenleyen federal yasanın yürürlüğe girmesinden sonraya kadar uzatmıştır. IBM, ilk önce en kapsamlı halde “*Büyük ölçekli*

³⁸⁵ Richard Bates ve Nicholas Blackmore, “The Privacy Challenges of Big Data and Artificial Intelligence”, **KennedysLaw**, (2017).

³⁸⁶ The Economist, Artificial Intelligence: Ethics, Frankenstein's Paperclips, 2016, s. 18.

izleme veya etnik indüksiyon” için yüz tanıma yazılımı sağlamayı kalıcı olarak durdurduğunu açıklamıştır³⁸⁷.

Algoritmik Adalet Birliği’nin kurucusu Joy Buolamwini 2017 senesinde IBM, Microsoft ve Despise adlı üç şirketin yüz tanıma algoritmaları üzerinde bir önyargı testi yapmış. Üç Afrika ülkesinden ve üç Avrupa ülkesinden 1270 parça yüz fotoğrafı toplamış ve ürün tanınması için üç şirkete vermiş. Araştırmada üç üründe kadınların doğru tanınma oranının erkeklere göre daha düşük, siyahi ırkların tanınma oranı beyazlardan daha düşük olduğu ortaya çıkmıştır. Bunların arasında IBM’in algoritması en büyük hatalık oranına sahip olduğu ortaya çıkmış ve beyaz tenli erkekler ve siyahi tenli kadınlar için hata oranı %34,4 olmuştur³⁸⁸.

Özetle yapay zekâ bizim düşündüğümüz kadar tarafsız olmayabiliyor. Yapay zekâ etik uzmanı Maria Axent’e göre yapay zekâ gelecekte mevcut önyargıları ve ayrımcılığı artırabilecektir. Bu güçlendirilmiş önyargı geniş kapsamlı olup, Spotify’daki şarkıları veya Netflix’teki filmleri tavsiye etmek için Yapay zekâyâ kullanılırsa, öneri tatmin edici olmasa bile, çok kötü sonuçlar doğurmayabilir. Ancak bir yapay zekâ, hastanın ne tür teşhise ihtiyaç duyduğuna karar verebilirse, önyargılı olup olmadığı hayatta kalma ve yaşamla ilgili oluyor anlamına gelecektir³⁸⁹.

Algoritmanın “önyargısının” nedeni genel anlamda yetersiz verilerden kaynaklandığını söyleyebiliriz. 2010 yılında Dallas’taki Ulusal Standartlar ve Teknoloji Enstitüsü ve Texas Üniversitesi’nden araştırmacılar tarafından yayınlanan bir araştırmada, Doğu Asya’da tasarlanan ve test edilen algoritmaların Doğu Asyalıları tanımlamakta daha iyi olduğunu, Batı ülkelerinde tasarlanan algoritmaların batılıları daha doğru tanıdığı ortaya çıkmıştır. Bu sonucun nedeni ise toplayabilecekleri veri

³⁸⁷ Mücahit Oktay, “Amazon’dan Yüz Tanıma Teknolojisinin Polis Tarafından Kullanımına Erteleme Kararı”, 2020.06.11, (Çevrimiçi) <https://www.aa.com.tr/tr/dunya/amazondan-yuz-tanima-teknolojisinin-polis-terafindan-kullanimina-erteleme-karari/1872922>, (Erişim Tarihi:17.11.2020).

³⁸⁸ Wu Yangyang, **a.g.e.**

³⁸⁹ **a.g.m.**

türü ve ölçeği olarak değerlendirilmiştir³⁹⁰. Bu açıdan değerlendirildiğinde uluslara mahsus olan algoritmaların başka vatandaşlara önyargılı/ayrımcı çıkarımlar sergileyebilmesi şaşırtıcı olmayacaktır.

Bunun bir veri sorunu olduğunu açıklasalar bile veriler tarafından üretilen önyargılar, profillemeye sonuçlarını göstermektedir. İlk veriler önyargılı olduğunda, makine öğrenimi tarafından yapılan tahminler de önyargılı olacaktır. Algoritmalar, genellikle mühendisler tarafından seçilen belirli görüntülerle beslenerek öğrenir ve sistem bu görüntülere dayanarak bir modeli oluşturur. Bir sistem aşırı derecede beyaz olan kişilerin fotoğrafları üzerine eğitilirse, beyaz olmayan yüzleri tanımakta zorluk çekecektir³⁹¹. Bu konuda sadece önyargılı veriler değil, aynı zamanda insanlar tarafından yaratılan önyargılı programların da olduğu belirtilmelidir.

Kısacası yapay zekânın önyargı ve ayrımcılık problemleri, kişisel verilerin korunması konusunda engeller oluşturmaktadır. Nitekim kişisel veriler ile eğitilip önyargı, ayrımcılık yapmayan yapay zekâ ortaya çıkarmak teknik açıdan kolay değildir. Çünkü kişisel verilerin veri kümelerine göre kendinden kaynaklanan potansiyel önyargı, ayrımcılığı mevcuttur. Hukuki açıdan yapay zekâ ile işlenen kişisel verilerin nasıl bir düzenleme altında önyargı, ayrımcılığa yol açmayacağı da kolay çözülen problem gözükmemektedir.

Öte yandan, yapay zekâ algoritmalarının bir “kara kutu (Black Box)” sorunu vardır. Yapay zekâ birçok karmaşık karar verebilse de geliştiricilerin kararlarının arkasındaki mantıksal ilkeleri tanımlamaları veya açıklamaları zor olmaktadır. Daha önceki bölümlerde anlatıldığı gibi algoritmanın giriş katmanı ve çıktı katmanı arasında “kara kutu” oluşmaktadır³⁹². Bu nedenle belli bir veri kümesinden işlenip ortaya çıkan

³⁹⁰ a.g.m.

³⁹¹ Kate Crawford, “Artificial Intelligence’s White Guy Problem”, The New York Times, 25.06.2016, (Çevrimiçi) <https://www.nytimes.com/2016/06/26/opinion/sunday/artificial-intelligences-white-guyproblem.html?r=2>, (Erişim Tarihi: 12.06.2020).

³⁹² George Nott, “Explainable Artificial Intelligence’: Cracking Open the Black Box of AI”, **Computer World**, (2017).

sonucu beslenen veriler ile açıklamak zor oluyor. Neden bu çıkarımı yaptığı sorusu çıkarım yapan yapay zekâyı geliştiren uzmanlar tarafından bile cevaplanamamaktadır.

Kara kutu sistemindeki bir başka güvensizlik kaynağı, yapay zekâ sistemlerinin (ırkçılık, cinsiyetçilik veya diğer ayrımcılık türleri gibi) geliştirebileceği potansiyel önyargılardır. Saldırıların neden olduğu derin sinir ağlarının savunmasızlığı, insanların bu yöntemlerin dayandığı öğrenme ve karar verme sürecinden şüphe duymasına neden olmuştur³⁹³. Sonuçta yapay zekânın otomatik karar vermede ayrımcılık ve kara kutu sorunları kişisel verilerin korunması için daha karmaşık zorluklar oluşturmaktadır.

Bir diğer korkunç verici nokta ise ölümcül yapay zekâ sistemlerinin önyargı ve ayrımcılığından kaynaklanan tehlikedir. Yapay zekâ çağında hakkaniyetin nasıl mümkün olacağını tahmin etmek zor olsa da günümüzde drone vb., operatörlerinin uzaktan öldürdükleri insanları “cama yapışan böcek” niteliğinde değerlendirilmesi, son derece aşınmış olan insani değerleri yapay zekâ ile birlikte daha da aşınmaya devam edeceğinin göstergesi diyebiliriz³⁹⁴. Nitekim bu tür araçlar önyargı ve ayrımcılık ile hareket ettiğinde tahmin edilmesi bile zor olan durumlar ortaya çıkacaktır. Yani kişisel verilerin önyargılı, ayrımcılık içeren yapay zekâ ile işlenmesi ölümcül sonuçlar da getirebilecektir.

Matbaanın icadından sonra insanlık tarihinde en büyük devrim yaratacak nitelikte olan yapay zekâ teknolojisi karşısında, eğer yeterince sağlam ilerlemeyi başaramazsak, Nicholas Carr’ın öngördü senaryo gerçekleşebilir. Nicholas kitabında şöyle buyuruyordu:

“Son beş asır boyunca, Gutenberg’in matbaasının kitap okumayı popüler bir uğraşıya dönüştürmesinden bu yana, doğrusal, yazınsal akıl,

³⁹³ Ayyüce Kızrak, “Açıklanabilir, Sorumlu ve Güvenilir Yapay Zekâ”, 05.12.2020, (Çevrimiçi) <https://ayyucekizrak.medium.com/a%C3%A7%C4%B1klanabilir-sorumlu-ve-g%C3%BCvenilir-yapay-zeka-bece897c5ea9>, (Erişim Tarihi: 07.12.2020).

³⁹⁴ Not A Bug Splat, “A Giant Art Installation Targets Predator Drone Operators”, Not A Bug Splat, 2019, (Çevrimiçi) <https://notabugsplat.com/>, (Erişim Tarihi:08.12.2020)

sanat, bilim ve toplumun merkezinde yer almıştı. Bu yeni akıl hassas olduğu kadar esnek de olduğundan, Rönesans'ın hayalci aklı, Aydınlanmanın rasyonel aklı, Sanayi Devrimi'nin icatçı aklı ve hatta Modernizemin yıkıcı aklı şekline girebilmişti. Kısa bir süre sonra işte bu akıl, geçmişte kalan akıl haline gelebilir”³⁹⁵.

Aslında bakarsak bu öngörü, Google gibi veri ile ayakta durmaya çalışan, yapay zekâ gibi veriler ile beslenen teknolojilere yönelik yapılmıştır.

Algoritmaların neden önyargılı kararları ele alacağını anlamak, algoritmik kara kutu üzerinde iyi çözümü belirlemek ve algoritmaların zararının sorumluluğunu paylaşmak kolayca çözülebilen işlerden değildir³⁹⁶. Yapay zekâ çağında bu konuların çok boyutlu bakış açılarından ele alınması gerekmektedir.

3.4.3. Çıkarımların Niteliği Sorunu

Yapay zekâ çağında önemli sorunlarından bir diğeri çıkarımların kullanılmasıdır. Günlük kullandığımız sosyal medya platformlarından medikal cihazlara kadar çıkarımları elde etmek en kolay olan “ekonomi klas veri” olarak değerlendirilmektedir. Çıkarımlar hakkında örnek vermek gerekirse, Netflix'in kullanıcıların ırklarını göre çıkarımlarda bulunup, “ırksal hedefleme” yolu ile film afişlerini tasarlaması ve tavsiyede bulunması³⁹⁷; Facebook'un genç LGBT kullanıcıların verilerinden “çıkarım” yaparak, “eşcinsel tedavisi” reklamları tavsiye etmesi³⁹⁸; Amazon'un sadece öksürük

³⁹⁵ Nicholas Carr, **Yüzeysellik: İnternet Bizi Aptal Mı Yapıyor?**, İstanbul: Ufuk Yayınları, 2012, s. 23.

³⁹⁶ Ishii, **a.g.m.**, s. 516.

³⁹⁷ Ben Arnold, “Netflix User Anger over ‘racial Targeting’ of Movie Posters”, 22.10.2018, (Çevrimiçi) <https://www.yahoo.com/entertainment/netflix-users-anger-racial-targeting-movie-posters-104325948.html>, (Erişim Tarihi: 15.10.2020).

³⁹⁸ Helena Horton ve James Cook, “Facebook Accused of Targeting Young LGBT Users with ‘gay Cure’ Adverts”, **The Telegraph**, 25.08.2018, (Çevrimiçi) <https://www.telegraph.co.uk/news/2018/08/25/facebook-accused-targeting-young-lgbt-users-gay-cure-adverts/>, (Erişim Tarihi: 1.10.2020).

sesine dayanarak ne zaman hasta olacağını tahmin edebilen ve ilaç tavsiye edebilen yeni Alexa geliştirmesi³⁹⁹ aklımıza gelmektedir.

Günümüzde en katı kişisel veri koruma düzenlenmesi olarak bilinen GDPR bile çıkarımların tekrar kullanılması konusunda yetersiz kalmaktadır. GDPR kişisel verileri korumak için tasarlanmış olsa bile ABAD çıkarımların bu tanımın kapsamına girip girmediği konusunda açık bir karar verememiştir. 2014 yılındaki verilen bir kararında⁴⁰⁰ çıkarımları kişisel veri kapsam dışında tutarken, 2017’deki bir kararda⁴⁰¹ çıkarımları kişisel veri olarak tanımıştır. Ancak, ikinci davada Mahkeme bu kişisel veri ile ilgili tüm hakları ilgili kişiye vermemiş ve veri koruma kanununun bireylerin nasıl değerlendirileceği konusunda bir hak içermediğini açıkça belirtmiştir. Sonuçta, yasa yalnızca girdi verilerinin yasal olarak elde edilmesini sağlamak için tasarlanmıştır diyebiliriz. Daha önceki örneklere baktığımızda Çıkarımların kişisel veri sayılıp sayılmayacağı ve nasıl korunacağı hakkında ABAD ve Madde 29 Çalışma Grubu farklı yorumlamalar yapmışlardır. Bu farklı görüşler Tablo 19’de yer almaktadır:

Tablo 19: Çıkarımların Niteliği Hakkında Görüşler

“Ekonomik Sınıf Veri” Olarak Çıkarımlar Hakkında Görüşler	
Madde 29 Çalışma Grubu’nun Görüşü	ABAD’nın Görüşü

³⁹⁹ James Cook, “Amazon Patents New Alexa Feature That Knows When You’re Ill and Offers You Medicine”, **The Telegraph**, 09.10.2018, (Çevrimiçi) <https://www.telegraph.co.uk/technology/2018/10/09/amazon-patents-new-alexa-feature-knows-offers-medicine/>, (Erişim Tarihi: 03.10.2020).

⁴⁰⁰ ABAD, C-141/12, YS, 17.07.2014 ve ABAD, C-372/12, M.

⁴⁰¹ ABAD, C-434/16, Nowak, 26.02.2018.

Kişisel verilerdir ⁴⁰²	Kişisel verilerin olup olmadığı belirsizdir ⁴⁰³
GDPR haklarının çoğu geçerlidir	Haklar yalnızca amaca göre geçerli olur
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 ⁴⁰⁴ .

Çıkarım sorunu çıkarımın kendisinden ötürü, çıkarım ortaya çıkaran ayrımcılıktan kaynaklanmaktadır. Çıkarımlar kişilerin işsiz kalmasına, ırkı, dini, felsefi düşüncesini dolaylı olarak aşağılayan davranışlara maruz kalmasına neden olabilir. Bu tür sorunların çözülmesi çıkarım mekanizmasının nasıl işleyeceği ile ilgili olacaktır. Bir başka deyişle çıkarım probleminin teknik açısından çözülmesi gereken kısmıdır.

Çıkarım ile ilgili bir diğer sorun çıkarımlar ile ticari gizlilik arasındaki ilişkiden kaynaklanmaktadır. Özellikle yapay zekâ başta olmak üzere algoritmalara dayalı çıkarım sergileyen teknolojiler ilgili kişilerin verilerinden türetilen çıkarımların ticari gizlilik kapsamında olacağınız savunmuştur⁴⁰⁵. Nitekim Facebook daha önce bu konuda ticari gizlilik kapsamında ilgili kişi ile alakalı olan çıkarımların ilgili kişiye

⁴⁰² Madde 29 Çalışma Grubu 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 subjektif bilgileri, görüşleri ve değerlendirmeler de kişisel veri olarak değerlendirdiği için çıkarımlar açık şekilde kişisel veri niteliği kazanmış olacaktır.

⁴⁰³ ABAD'nın verdiği kararlar değerlendirildiğinde kişilerle ilgili yapılan hukuki analizi kişisel veri olarak değerlendirmede gözükmektedir. ABAD C-434/16 sayılı kararında da Madde 29 Çalışma Grubu buna benzer şekilde yorumlama yapmış olsa da kişisel veri niteliği kazanması bütün haklardan yaralanabileceği anlamına gelmeyeceğini de belirtmiştir.

⁴⁰⁴ CPDP, "Profiling, Microtargeting and A Right to Reasonable Algorithmic Inferences", (Çevrimiçi) https://www.youtube.com/watch?v=nN_sGuNhaOM, (Erişim Tarihi: 12.09.2020).

⁴⁰⁵ Emil Protalinski, "Facebook: Releasing Your Personal Data Reveals Our Trade Secrets", (Çevrimiçi) <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>, (Erişim Tarihi: 04.12.2020).

verilme talebini reddetmiştir. Günümüzde yapay zekânın hızlı ilerlemesi ile birlikte, sadece kişisel verileri değil, kişisel veri ya da henüz kişisel veri niteliği bulunmayan verilerden türetilen çıkarımlar kişisel verilerin korunması kapsamındaki hukuki değerlerin ihlal edilmesine sebep olabilmektedir.

3.4.4. Şeffaflık/Rıza Sorunu

Bazı veri bilimcileri, ilgili kişilerin kullanılan modeli veya kuralları tanınmasına ve algoritmaları incelemesine izin vermek için algoritmaların şeffaf olması gerektiğini, böylece bir yapay zekâ sistemi tarafından verilen yanlış kararın araştırılabilir/sorumlu tutulabilir hale geleceğini savunmaktadır⁴⁰⁶. 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 oynayarak insan rakibini yendiğinde, AlphaGo ekibi bu hareketi neden yaptığını açıklayamamıştır ve şu anda insanlar yapay zekânın mantığını tam olarak anlayamıyor veya çözemiyor durumda kalmıştır⁴⁰⁷.

Viktor Mayer ve Kenneth Cukier'e göre ise günümüzde yapay zekâ ve büyük veri teknolojileri insanları “Nedensel” olarak düşünmekten “Korelasyon” şeklinde düşünmeye zorlamaktadır⁴⁰⁸. Bu görüşe göre artık bütün bilgi edinme yöntemleri nitelik açısından değişime uğrayacaktır. Klasik yöntemlerden tamamen uzaklaşarak, yanı nedensellikten uzaklaşarak, korelasyon aracılığıyla karar vermeye eğileceği belirtilmiştir. Sonuçta alınan kararların nedeni olmamaktadır. Sadece ilgili işlemin bir korelasyon sonucu olduğu şeklinde açıklama yapılabilecektir.

⁴⁰⁶ House of Commons, Science and Technology Committee, “Robotics And Artificial Intelligence: Fifth Report of Session”, 2016, (Çevrimiçi) <https://www.publications.parliament.uk/pa/cm201617/cmselect/cmsctech/145/145.pdf>, (Erişim Tarihi: 12.06.2019), s. 17-18.

⁴⁰⁷ a.g.m., s. 17.

⁴⁰⁸ Viktor Mayer Schönberger ve Kenneth Cukier, **Büyük Veri: Yaşama, Çalışma ve Düşünme Şeklimizi Dönüştürecek Bir Devrim**, İstanbul: Paloma Yayınları, 2013, s. 57.

Google AlphaGo örneğinde, yapay zekânın yaptığı hamle nedensel bir açıklama ile cevaplanmadan ötürü o hamlenin oyunu yenme ile olan korelasyon ilişkisi ile cevaplamak daha mantıklı olacaktır.

Doğrusal olmayan birçok işlevlerin karmaşık şekillerde sonuç üretmesi insanlar (ve hatta bazen kendi geliştiricileri) tarafından bile açıklanamıyor hale gelmiştir. Güvenlik, şeffaflığı gerektiren uygulamalarda, derin öğrenme yerine daha kolay yorumlanabilir modelleri (regresyon veya karar ağaçları gibi) kullanılmaktadır. Bu tür sistemler, karar verirken veri setindeki korelasyonları kullanmakta olup derin öğrenmeye göre daha şeffaf olduğu söylenebilir⁴⁰⁹. Kısacası, derin öğrenme, yapay sınır ağları gibi yapay zekâ teknikleri büyük şeffaflık problemlerine yol açabilmektedir.

Bu durum şeffaflık sorununun yapay zekâ çağında çözülemeyecek/çözülmesi asla gerekmeyen bir sorun haline getiriyor. İlgili kişi, verilerindeki hataları bulamaz ve bu hatalar üzerinde ayrımcı etkilere yol açarsa, “algoritmik kara kutu” sorunu çözülemediği sürece profil oluşturma dahil veri işleme sürecine karşı çıkamayacaktır. İlgili kişi kişisel verilerinin nasıl kullanıldığı ve daha da önemlisi, ilgili kişiyi ilgilendiren kararların nasıl alındığı hakkında uygun bilgilere sahip olamayabiliyor⁴¹⁰. Bu nedenle ilgili kişilerin verilerini kullanımına (işlenmesine) anlamlı bir şekilde izin vermesi/rıza göstermesi imkânsız hale gelmektedir.

Daha önceki bölümlerde bahsedildiği gibi yapay zekânın temel özelliklerinden biri veri kaynaklarının sayısı ve bu kaynakların heterojenliğidir. Bu durum çoğu zaman hem kişisel hem de kişisel olmayan verileri içeren bir dizi veri kümesinin oluşmasına yol açıyor. Veri kümelerinin kombinasyonları ve bir araya getirilmesi de yeni verileri oluşturuyor. Verileri büyük ölçekte ve yüksek hızda karıştırmak ve yeniden kullanmak, birçok geleneksel veri koruma yöntemlerini etkisiz hale getiriyor ve veri koruma

⁴⁰⁹ Kızrak, Açıklanabilir..., **a.g.m.**, par. 2.

⁴¹⁰ Giovanni Buttarelli, “A Smart Approach: Counteract The Bias in Artificial Intelligence”, 2016, (Çevrimiçi) https://edps.europa.eu/press-publications/press-news/blog/smart-approach-counteract-bias-artificial-intelligence_en, (Erişim Tarihi: 12.10.2020)

yasalarının uygulanmasını zorlaştırıyor⁴¹¹. Mahremiyet haklarını korumayı konu eden yasal, etik, kurumsal ve organizasyonel kontrol ve dengelerin yanı sıra, kişisel verilerin büyük ölçekli kullanımının neden olduğu mahremiyet zararlarını azaltmaya yönelik teknolojik çözümler çok yönde hızla gelişmekte olsa bile yapay zekâ çağındaki bunun gibi geleneksel kuramları zorluk çekmektedir.

Geleneksel yöntemlerde, bilgilendirme/rıza kuralı kişisel verilerin korunması için önemli bir ilke hükmündeydi. Veri işleyenler kişisel verileri topladığında, genellikle ilgili kişinin bilgilendirilmesi ve rızasının ardından verileri toplar, analiz eder, kullanır ve aktarırdı. İlgili kişilere yönelik ihlaller, ciddiye ve ihlal yöntemleri açısından nispeten küçük ve basit olurdu. Ancak yapay zekâ çağında veri toplamayı gerçekleştiren çeşitli bağlantı noktaları ve cihazlarla temsil edilen öznelerin meşruiyeti doğrulanamıyor.

Yapay zekâ teknolojisinin karmaşıklığı ve gelişmiş doğası nedeniyle, kişisel veriler genellikle ilgili kişinin rızası olmadan bile toplanır ve işlenebiliyor. Ayrıca veri saklama, toplama, analiz etme, kullanma ve aktarımı yapma aynı özne tarafından gerçekleştirilmeyip, farklı öznelerden geçebilir. Bu durumda bilgilendirme/rıza kuralı geçersiz olmasa bile istenen etkiyi elde etmede zorluk çekiyor. Ara işlem süreci ilgili kişinin kontrolünden çıkmış olması nedeniyle, ilgili kişi rıza haklarını gerçekleştirmede zorluk çekiyor ve bu da ihlale neden olabiliyor. Bu anlamda yapay zekâ çağındaki aydınlatılmış rızanın yeniden değerlendirilmesi gerekmekte olup, sadece veri toplama aşamasında değil, veri işleme faaliyetin bütün aşamalarında aydınlatılmış rıza mekanizmasının etkili olması önem arz etmektedir.

⁴¹¹ Tjerk Timan ve Zoltan Mann, “Data Protection in the Era of Big Data for Artificial Intelligence: Trends, Existing Solutions and Recommendations for Privacy-Preserving Technologies”, 2019, (Çevrimiçi)
https://www.bdva.eu/sites/default/files/Data%20protection%20in%20the%20era%20of%20big%20data%20for%20artificial%20intelligence_BDVA_FINAL.pdf (Erişim Tarihi: 15.10.2020), s. 5.

3.4.5. Hassas Veri Sorunu

GDPR madde 9 da sađlık, etnik k ken veya siyasi inan lar gibi  zellikleri tanımlayan “ zel kategoriler” i in daha fazla koruma ( rneđin, izin i in daha y ksek standartlar, sınırlı izin verilen kullanımlar) sađlamıřtır. Aslında kiřisel verilerin, hassas  zelliklerin  ıkarılmasına veya “dolaylı olarak a ıđa  ıkarılmasına” izin verdiđi g sterildiđinde, hassas  ıkarımların  ıkarılabileceđi kaynak veriler de hassas veriler olarak deđerlendirilebilir.⁴¹²

ABAD Genel Mahkeme kararı⁴¹³, GDPR 9. maddenin uygulanmasını, hassas verilere ulařma niyetinin olduđu ve veri kaynađının bu  ıkarımı ortaya  ıkarmak i in g receli olduđu durumlara sınırlamıřtır. Her iki kořul da yapay zek   ađında mahremiyetin korunması i in bir risk oluřturmaktadır. “Hassas niteliklere varma niyeti” zor anlařılan yorum sayılabilir. Posta kodları gibi Proxy verileri, bu  zniteliklerin kasıtlı veya a ık bir řekilde  ıkarılmıř olup olmadıđına bakılmaksızın hassas veriler ( rneđin cinsiyet, cinsel y nelim veya ırk) sayılır. Zarsky’nın g r ř nde her řey potansiyel olarak hassas veri olabilmekte, sadece bizim onu hen z bilmiyor olmamız buna engel olabilmektedir⁴¹⁴.

Bu konuda ABAD ile Madde 29  alıřma Grubu farklı yorum sergilemektedir. Madde 29  alıřma Grubunun yorumuna g re hassas veriler, yalnızca dođası geređi hassas bilgiler i eren verileri deđil, aynı zamanda bir bireye iliřkin hassas bilgilerin  ıkarılabileceđi verileri de kapsar⁴¹⁵. Bir diđer ifade ile belli hassas olmayan verileri iřleyerek ilgili kiři ile ilgili hassas verileri  ıkarabiliyorsa, giriř yapılan veriler hassas

⁴¹² Sandra Wachter ve Brent Mittelstadt, “A Right to Reasonable Inferences: Re-thinking Data Protection Law in the Age of Big Data and AI”, **Columbia Business Law Review**, S. 2 (2018), ss. 1-130, s. 47.

⁴¹³ Genel Mahkeme’nin (Beřinci Daire) 28.05.2012 tarihli Kathleen Egan, Margaret Hackett ve Avrupa Parlamentosu T-190/10 sayılı kararı.

⁴¹⁴ Tal Zarsky, “Incompatible: The GDPR in the Age of Big Data”, **Seton Hall Law Review**, C. 47, S. 4(2) (2017), s. 47.

⁴¹⁵ Bkz. Kathleen Egan Case T-190/10

veri niteliği kazanacaktır. Nitekim günümüz yapay zekâ teknolojisinde bu durum zor bir işlem sayılmayacaktır.

Nesnelerin İnterneti, Siber-Fiziksel Sistemler (otonom veya bağlantılı arabalar gibi) veya akıllı şehirler aracılığıyla gerçekleştirilen bilgi işlemler tam olarak bağlantılı verilerin öncülüne dayanıyor. Sağlık durumlarını izleme cihazları, uyku alışkanlıkları, egzersiz seviyeleri veya genel sağlık durumlarını anlamak için kullanılabilecek verileri topluyor. Akıllı şehirlerde, sensör verileri, WiFi verileri ve konum verileri, hareket modellerinin yanı sıra yavaş faaliyetler hakkında dahi fazla bilgi toplar. Ağ bağlantılı sensörlere sahip otomobillerin sürücüleri, yolculuk bilgilerine göre davranışsal profillemeye (alışveriş alışkanlıkları ve sosyal ağlar) tabi tutuluyor. Yorgunluk algılama sistemlerinde kullanılan göz hareketi izleme, yüz tanıma yazılımı veya kalp atış hızı ölçümleri aracılığıyla sağlık durumu ve refahı sonucunu çıkarmak da mümkün olmaktadır⁴¹⁶.

Akıllı telefon sensörleri ve verileri stres seviyelerini, yeme alışkanlıklarını, akıl hastalığını ve demografik bilgileri tahmin edebilir. Bu, egzersiz seviyelerini, sağlık durumunu ve ruh halini anlamak için ivmeölçerler, GPS, mikrofonlar, kameralar veya parmak izi tanımlamada kullanılan akıllı sensörler aracılığıyla veya tarama alışkanlıkları, tercih edilen uygulamalar veya sosyal etkileşimler⁴¹⁷ gibi telefon kullanım modellerini analiz ederek elde edilebilir. Kullanıcıların özel hayatlarını tanımlayan veriler kullanıcıların davranışlarını ve karşılanmamış ihtiyaçlarını ortaya çıkarmak için analiz edebilir⁴¹⁸.

Bu tür teknolojiler tarafından üretilen veriler, bireylerin davranışları, tercihleri ve özel yaşamları hakkında sezgisel olmayan ve doğrulanamayan çıkarımlar ve

⁴¹⁶ Sandra Wachter, “The GDPR and the Internet of Things: A Three-Step Transparency Model”, **Law Innovation Technol**, 2018, ss. 266–294, s. 10.

⁴¹⁷ Scott R. Peppet, “Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security and Consent”, **Texas Law Review**, (2014), ss. 85–176, s. 93.

⁴¹⁸ Sandra Wachter, “Data Protection in the Age of Big Data”, **Nature Electronics**, C. 2 (2019), s. 1.

tahminler yapmak için kullanılabilir. 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 karar ortaya çıkması için risk oluşturabiliyor⁴¹⁹. Bu riskler arasındaki ortak faktör, hassas çıkarımların yapılmasına olanak tanıyan mahremiyete yaygın veri toplama korkusudur. Bu çıkarımlar, özellikle sigorta şirketleri, finans kurumları veya işverenler gibi üçüncü şahıslarla paylaşıldığında ayrımcılık riski daha yükselecektir.

Tüm bu alanlar kişisel verilerin korunması düzenlemeleri kapsamında değerlendiriliyor olsa da hassas veri konusunu ele almak için etkisiz ve eski stratejiler benimsemektedir. Örnek olarak GDPR'a baktığımızda, GDPR esas olarak verilerin toplandığı girdi aşamasında korumaya odaklanır, ancak analiz sırasında veya sonrasında neredeyse hiç koruma çabası göstermemektedir. Dolayısıyla GDPR, çıkarımsal analitik nedeniyle veri toplandıktan sonra gizliliğe yönelik öngörülemeyen tehditlerin ortaya çıkabileceği gerçeğini görmezden geldiği söylenebilir.

GDPR'ın amacı ilgili kişinin haklarını korumak olsa da verilerin nasıl ve hangi parametrelere göre değerlendirileceği detaylı şekilde düzenlemediği söz konusudur. Bireylerin değerlendirmeleri (örneğin, iş performansı, ortalama ömür beklentileri) çoğunlukla GDPR kapsamının dışında kalmaktadır. Bunun yerine GDPR, verilerin toplanma aşamasında durumunu yansıtan yapay ve akıcı kategorilere göre tanımlanan çeşitli koruma standartları düzenlemiştir⁴²⁰. Kısacası yapay zekâ çağında, hassas kişisel veri yasal çerçevesi, özellikle çıkarımlar ile olan ilişkileri etkili şekilde yeniden düzenlenmesi gerekmektedir. Böyle olmadığı müddetçe mevcut kişisel veri koruma düzenlemeleri yapay zekâ çağında hassas verileri koruma konusunda etkisiz kalabilecektir.

⁴¹⁹ Sandra Wachter, "Normative Challenges of Identification in the Internet of Things: Privacy, Profiling, Discrimination, and the GDPR", **Computer Law Security Review**, (2017), ss. 436–449, s. 34.

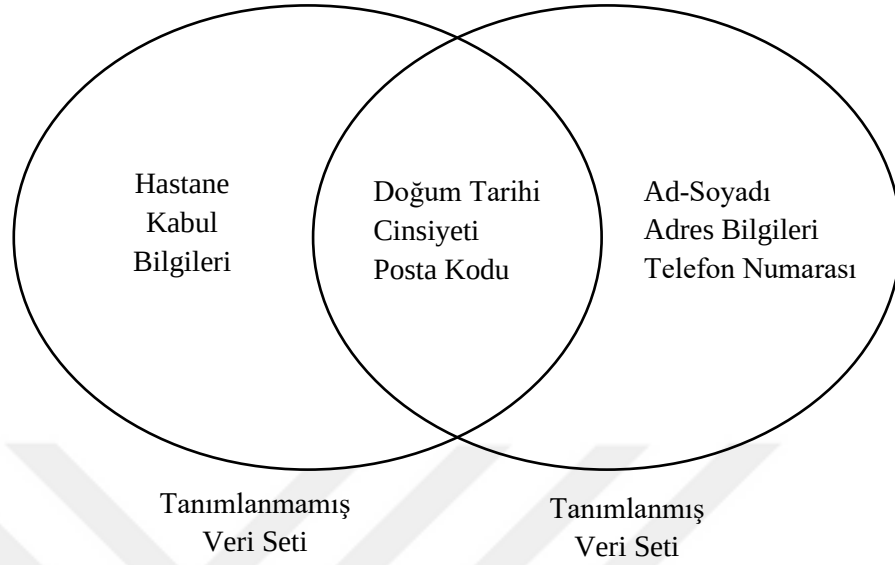
⁴²⁰ Wachter, "Data Protection in the Age of Big Data", **a.g.m.**, s. 2.

3.4.6. Anonimleştirilmiş Veri Sorunu

Büyük verinin işlenmesini mümkün kılan yapay zekâ teknolojileri sayesinde kişisel veri ile kişisel olmayan veri arasındaki ayrımının hala uygulanabilir olup olmadığı sorun olabilmektedir. Yapay zekâ teknolojisinin geldiği ileri seviye göz önüne alındığında, teknik bakımından anonimleştirilmiş verilere (kişisel veri niteliği olmadığını varsayan veriler) dayanarak yapılan ve doğrudan bireyleri belirlenebilir kılan tahmini çıkarımlar karşısında bireylerin/ilgili kişinin nasıl korunacağı belirsizlik teşkil etmektedir⁴²¹. Tanımlanamayan veriler bile kullanıcıları veya makineleri tanımlamak için kullanılabilir. Örneğin, tarayıcı seçimi ve yazı tipi boyutu doğru ve benzersiz bir çevrimiçi tanımlamayı sağlayabilir⁴²². Basitçe ifade etmek gerekirse, ne kadar çok veri mevcutsa, verilerin tanımını etkin bir şekilde zorlaştırmak (de-identify) o kadar zor olacaktır. Şekil 6’de tanımlanmış veriler ile tanımlanmamış veriler arasındaki bağlantı gösterilmiştir.

⁴²¹ Muhammed Raşit Özdaş, Ayşe Nur Akıncı ve Ahmet Ziyaeddin Türkan, “Yapay Zeka ve Hukuk 4.0: Yapay Zekanın Hukuk Uygulamalarına Etkisi”, **Oyun Değiştiren Yapay Zeka**, der. Mustafa K. Yılmaz ve Öykü İyigün, İstanbul: Beta Yayıncılık, 2020, s. 230.

⁴²² Jeremy Kirk, “EFF: Browsers Can Leave a Unique Trail on the Web”, (Çevrimiçi) <https://www.pcworld.com/article/188134/article.html>, (Erişim Tarihi: 07.07.2020).



Şekil 6: Tanımlanmış ve Tanımlanmamış Veriler Arasındaki Bağlantı

Görüldüğü üzere, korelasyonlar aracılığıyla tanımlanmayan bilgiler ile tanımlanan bilgiler arasında bağlantı kurulabilmektedir. Şekil 6’de Massachusetts valisinin sağlık kaydının yeniden tanımlanmasını mümkün kılan bir tanımlanmış ve bir tanımlanmamış veri seti arasındaki bir bağlantı yer almaktadır. Bu sonuç, Valinin doğum tarihi, posta kodu ve cinsiyetiyle eşleşen kimliksiz verileri arayarak elde edilmiştir. Diğer bir klasik örnek, anonimleştirilmiş film derecelendirmelerinin IMDb’deki anonim olmayan derecelendirmelere bağlanarak yeniden tanımlanabildiği Netflix fiyat veri tabanı örneğidir. Aslında, bir IMDb kullanıcısı tarafından yapılan incelemelerde yalnızca iki farklı incelemeyi bilerek, anonim veri tabanında aynı kullanıcı tarafından yapılan incelemelerin belirlenmesi mümkün olmuştur⁴²³.

⁴²³ Luc Rocher, Julien M. Hendrickx ve Yves-Alexandre de Montjoye, “Estimating the Success of Re-Identifications in Incomplete Datasets Using Generative Models”, **Nature Communications**, S. 10 (2019), s. 5.

Yapay zekâ kişisel tanımlamayı iki şekilde kolaylaştırıyor: İlk olarak, cep telefonlarındaki, arabalardaki ve diğer cihazlardaki sensörlerden daha fazla veri talebini oluşturabiliyor. İkincisi, toplanan verileri analize etmek için giderek daha gelişmiş hesaplama yetenekleri sağlıyor. Örnek olarak yüz özellikleri, parmak izi ve diğer biyometrik tanıma teknolojileri formları sunulabilir. Böylece binlerce ayrı, neredeyse anlamsız veriler toplanır ve daha sonra bunları bireylerin güvenilir bir şekilde tanımlanmasını sağlayacak şekilde birleştirir. Yapay zekâ çağında anonimleştirilmiş verilerin bile kişisel veri niteliğinde kullanılabilmesi büyük risk taşımaktadır. Kısacası anonimleştirilmiş veri tekniği yapay zekâ çağında etkisiz durumda kalmıştır.

Öbür taraftan, GDPR'daki hakların hiçbiri anonim veriler için geçerli değildir ve bu durum sorun haline gelebilir. İlk olarak, teorik açıdan bütün anonimleştirilmiş veriler ters yöne tabi tutulabilir ve bir kişiye ilgili şekle getirilebilir⁴²⁴. İkincisi, gerçekten anonimleştirilmiş olan veriler bile kullanıcı profilleri oluşturmak için kullanılabilir ve bu nedenle, belirli bir kişiyi tanımlamaya gerek kalmadan gizlilik ve ayrımcılık riskleri meydana gelebilir⁴²⁵. Burada yine GDPR'ın verilerin nasıl kullanıldığına ve ilgili bireyler ve gruplar üzerindeki etkisinden ötürü veri toplama aşamasına odaklandığını vurgulayabiliriz⁴²⁶. GDPR'ın en büyük eksikliklerinden birinin bütün düzenlemeleri veri toplama aşamasına yönelik ayarladığını söyleyebiliriz. Buda yapay zekâ çağında risk oluşturmaktadır.

Yapay zekâ çağında kimsenin aklına bile gelmeyen veriler hatta veri olduğunun bilincinde bile olmadığımız şeyler kişisel veri niteliği kazanma olasılığını rastlamaktadır. Örnek vermek gerekirse, MIT uzmanları, kişilerin gönüllü olarak

⁴²⁴ Paul Ohm, “Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization”, **UCLA Law Review**, (2009), ss. 1701–1777, s. 57.

⁴²⁵ Mireille Hildebrandt, “Profiling and the Identity of the European Citizen. In profiling the european citizen”, **Springer Dordrecht**, (2018), ss. 303–343. s. 320.

⁴²⁶ Brent Mittelstadt, “From Individual to Group Privacy in Big Data Analytics”, **Philosophy & Technology**, S. 30 (2017), ss. 475–494, s. 482.

gönderdiği on binlerce öksürük sesi örneği ve kelime sesleri veri olarak kullanarak, Covid-19 teşhisi konan kişilerin %98,5'ini ve asemptomatik Covid-19 hastalarının %100'ünü doğru bir şekilde tanımlayabilen bir yapay zekâ modeli geliştirmiştir. Bireyin öksürü sesinden kişiye ilgili olan sağlık durumlarını öğrenilebilen yapay zekâ çağında, bu tür “veri”lerin kişisel veri kategorisinde korunup korunmayacağı ayrı bir sorun oluşturmaktadır⁴²⁷.

Kullanıcılar, yapay zekâ ürünlerini kullanırken kişisel verilerin “sızıntısı” olabilir. Kişisel verileri elde etme gereksinimleriyle karşı karşıya kaldıklarında, farkında olmadan veya bilinçsiz olarak potansiyel tehditlere maruz kalabilir. Yapay zekâ teknolojilerinin hızlı ilerlemesi ve caydırıcı etkileri altında, kullanıcıların kişisel verileri ve mahremiyeti koruma konsept bilgisinden ve bunlara karşılık gelen kriz bilinci ve önleme bilincinden yoksun olduğu söylenebilir.

Belki de kullanıcıların dışarıya paylaştığı veri anonimleştirilmiş kişisel veriler olabilir, ancak yapay zekâ teknolojisi bağımsız veri parçaları arasında bağlantı kurabilir, bir kişinin veya bir kuruluşun tam profilini geri yükleyebilir. Kullanıcılar, kendi haklarını koruma konusunda yeterli kadar farkındalığa sahip değildir. Bu durum anonimleştirilmiş verileri doğrultusunda riskler yaratabilmektedir.

Bu durumda hesaplama yoluyla görünüşte her yerde bulunan veri toplama ve çıkarımsal ve tahmine dayalı analitik kullanarak kapsamlı bilgi üretiminin yanı sıra bu bilginin kamu ve özel taraflar arasında daha fazla paylaşıldığı bir dünyada, veri koruma yasasının sorumluluğu yeniden tanımlanmalıdır. Kişisel veya kişisel olmayan ve hassas veya hassas olmayan verilerin güncel olmayan, etkisiz ve akışkan sınıflandırmalarından vazgeçilmelidir. Bu kategoriler, yalnızca toplandıkları andaki verilerin doğasını yansıtır, ancak daha sonraki kullanımını ve olası dönüşümlerini (örneğin, cinsel yönelim, sağlık durumu) göz ardı etmektedir. Anonim hale geldiğini

⁴²⁷ Jennifer Chu, “Artificial Intelligence Model Detects Asymptomatic Covid-19 Infections Through Cellphone-Recorded Coughs”, (Çevrimiçi) <https://news.mit.edu/2020/covid-19-cough-cellphone-detection-1029>, (Erişim Tarihi: 04.11.2020), par. 3.

zannettiğimiz veriler yapay zekâ teknolojileri yardımıyla hassas veriler kategorisine bile girebilecektir. Kişisel veri koruma düzenlemeleri anonimleştirilmiş veri sorununa etkili şekilde çözüm araması gerekmektedir.

3.4.7. İhlal Failinin Belirlenme Sorunu

Geleneksel yöntemlerde kişisel verilerin toplanması çoğu zaman yüz yüze gerçekleştirilir ve bu sebeple veri işleyeninin bulunması daha kolay olmuştur. Sonuçta, veri ihlali gerçekleştiğinde ihlal failinin belirlenmesi zorluk oluşturmamıştır. Fakat, yapay zekâ döneminde veri ihlalini yapan failin bulunması artık eskisi kadar kolay olmamaktadır. Daha önceden bahsettiğimiz gizli, hızlı işlem nitelikleri ihlal failinin belirlenmesinde engel oluşturmaktadır.

Zayıf Yapay Zekâ çağında, yapay zekâ insanların kişisel verileri işlemesi için bir araç niteliğinde kullanılmıştır. Bu durumda, haksız fiil sorumluluğu kuramına göre, yapay zekâ üreticisi ve operatörü, haksız fiil sorumluluğundan sorumlu tutulmaktadır. Fakat Zayıf Yapay Zekâ çağında bile yapay zekâ üreticiler ve operatörlerinin belirlenmesi pratikte ayrı bir zorluk oluşturabiliyor.

Örneğin internette çevrimiçi olduğumuz sürece kullanıcıya yönelik çeşitli bağlantı noktaları bulunmaktadır. Ne zaman, nerede ve hangi verileri topladıklarını, kimin topladığını belirlemek, ilgili kişi açısından kolay olmamaktadır. Dahası Güçlü Yapay Zekâ çağına geldiğimizde, yapay zekânın belli düzeyde düşünme yeteneğine sahip olması ve davranışı insan kontrolü ve hayal gücünün ötesinde bulunması ayrıca risk içermektedir. Bu durumda veri ihlalinin kimin sorumlu olduğunu belirlemek daha da zor olacaktır.

Sorumluluk konusunda yapay zekânın hayali kişilik (Legal Fiction Said) olarak değerlendirilebileceğini ve kendisinin haksız fiil sorumluluğunu

taşıyabileceğine dair bir görüş vardır⁴²⁸, ancak yapay zekânın kendisinin hayali kişilik olarak kabul edilip edilemeyeceği tartışmalı konudur⁴²⁹. Doğal olarak bu durumda ihlal eden faili belirlemenin hukuki kişilik bağlamında olduğu kadar sorumluluk konusu bakımından da zor olduğunu söyleyebiliriz.

Günümüzde ABD’de dronların diğer insanların mahremiyetini ihlal ettiği konusunda birçok anlaşmazlık yaşanmaktadır⁴³⁰. Başkalarının mahremiyetine tecavüz eden bir drone durumunda, hakkı ihlal edilen taraf genellikle kanıt sağlayamıyor ve hatta gerçek ihlal yapan faili bile belirlemekte zorlanmaktadır.

Kısacası ihlal failinin bulunmasının teknik açıdan zor olması yapay zekâ çağında kişisel verilerin korunması açısından zorluklar oluşturmaktadır. Bu durumda drone gibi hareketli bağlantı noktalarının kullanılmasının tamamen yasaklanması ekonomik açıdan zarar getireceği gibi, herhangi bir düzenlemenin yapılmaması da kişisel verilerin ihlaline sebep olabilecektir.

İhlal failinin belirlenme sorununun çözümüne gelince, veri asimetrisi sorunundaki gibi ilgili kişiye daha çok bilgi edinme fırsatı sunarak, ilgili kişi ile veri sorumlusu arasındaki veri asimetrisi azaltılabilir. Nitekim veri sorumlusu hakkında daha fazla bilgiye sahip olmak, ilgili kişi açısından veri ihlalinden sonra ihlal failinin bulunması konusunda yardımcı olabilecektir. Bu durumda ilgili kişi hakkında veri işleme faaliyetinde bulunan bağlantı noktaları takip edilerek ihlal failinin bulunması

⁴²⁸ Yapay zekâ ürünlerinin medeni hukuktaki durumu, kişilik özelliklerine sahip olup olmadıkları konusunda görüşler için bkz: Yang Qingwang ve Zhang Lei, “On the Artificial Legal Personality of Artificial Intelligence”, **Journal of Hunan University of Science & Technology**, S. 6 (2018); Tong Xiao vd., “人工智能发展中的法律问题研究 (Yapay Zekanın Geliştirilmesinde Hukuki Sorunlar Üzerine Araştırma)”, **Government Legal System Research**, S. 10 (2019).

⁴²⁹ Li Weigang, “人工智能时代对个人数据法律保护的挑战 (Yapay Zekâ Çağında Kişisel Verilerin Yasal Olarak Korunmasına Yönelik Zorluklar)”, **法制博览**, (Eylül 2020), ss. 168 – 171, s. 169.

⁴³⁰ Wang Liming, “人工智能时代对民法学的新挑战 (Yapay Zekâ Çağında Medeni Hukukun Karşılaştığı Yeni Zorluklar)”, **东方法学** (Eastern Law), S. 3 (2018), s. 6.

kolaylaştırılabilir. En önemlisi bağlantı noktaların takip edilmesi ile gözetim, ilgili kişilerin temel insan hakları arasında dengenin kurulması önem arz edecektir.

3.4.8. İhlal Delili Elde Etme Sorunu

Akıllı bağlantı noktalarının yasallığının nasıl düzenleneceği yapay zekâ çağında yeni bir zorluk oluşturmaktadır. Kişisel veri toplamanın yanı sıra, yapay zekâ teknolojisi, Büyük verilere dayanan çeşitli ürünleri araştırmak, geliştirmek, insanları büyük veri bilgilerini daha fazla toplama ve analiz etmeye teşvik etmek, büyük verilerin sonsuz potansiyelinden yararlanmak için de kullanılabilir. Kişisel veri toplama ve analiz etme teknolojileri ilerledikçe ve maliyetler azaldıkça, büyük ölçekli veri toplama norm haline gelmiş ve giderek yaygınlaşmaktadır⁴³¹. Bu durum kişisel veri ve mahremiyet tehdidini daha da arttırmaktadır.

Kişisel verilerin işleme amacı sonsuza doğru eğirildi yapay zekâ çağında, veri ihlali konusunda kanıt elde etmek kolay olmamaktadır. Çünkü ihlal öznesi veri ihlalinin gerçek veya tüzel kişi aracılığıyla değil, çeşitli elektronik bağlantı noktaları ve teçhizatlar ile gerçekleştirmektedir. Elektronik bağlantı noktaları kişisel verileri gözetlemek için yapay zekâ teknolojisini kullanmaktadır. Kişisel verilerimizin ne zaman, nerede ve nasıl elde edildiğini öğrenmek kolay olmamakta ve bu nedenle kanıt elde etmeyi zorlaştırmaktadır. İhlal kanıtı elde edilebilse de maliyet açısından ilgili kişiye engel oluşturabiliyor. Gerçekleşen veri ihlali ortada olsa bile hangi bağlantı noktasından toplanan, saklanan, işlenen ve aktarılan veri ile gerçekleştiğini öğrenmek kolay olmamaktadır. Elllerinde veri toplamak için kullanılan bağlantı noktaları hariç hiçbir teknoloji desteğe sahip olmayan ilgili kişiler, kanıt elde etme konusunda oldukça pasif bir durumda kalmaktadır.

⁴³¹ Zhang Xianli ve Gao Qiqi, “人工智能时代公民的数据意识及其意义 (Vatandaşların Veri Farkındalığı ve Yapay Zekâ Çağındaki Önemi)”, 西南民族大学学报, S. 12 (2017), s. 6.

Yukarıda belirtilen zorluklar yapay zekâ çağında kişisel verilerin korunması düzenlemelerin önünde engel teşkil etmektedir. Zorlukları bir taraftan teknik açıdan aşmaya çalışırken, bir taraftan hukuki açıdan değerlendirmek gerekmektedir. Günümüzde başta AB, ABD başta olmak üzere, yapay zekâ etiği, yapay zekâ düzenlemeleri konusunda çalışmalar sürdürmektedir. Ancak bütün bu çalışmaların disiplinlerarası yani bilgisayar bilimci insanlar ile hukukçular bir araya gelerek yapılması gerekmektedir.

3.5. Yapay Zekâ Çağında Kişisel Veri Koruma Düzenlemelerin Karşılaştırılması

Kişisel verilerin korunmasına ilişkin ilk düzenleme örneği, özel hayatın gizliliği ve bireylerin kendi verilerine ilişkin haklarının korunmasına odaklansa da kişisel verilerin stratejik değeri, özellikle ekonomik değeri, daha sonraki düzenlemelerde giderek fazla önem kazanmıştır⁴³². Son zamanlarda, veri koruma ile ekonomik çıkarlar arasında hassas bir denge bulmak amacıyla yeni girişimlerde bulunulmuştur.

Uluslararası üstünlüğün teknoloji ile özellikle yapay zekâ teknoloji seviyesi ile belirlenen günümüzde, karşılaştırmalı hukuktaki düzenlemeden yola çıkarak, ülke ve birliklerin farklı stratejiler sergilediğini görmekteyiz. Tablo 20’de mukayeseli olarak yapay zekâ alanında önde gelen ülke ve birliğin kişisel veri koruma ve başka ilgili düzenlemelerinin yöntemi, stratejileri ve avantajlı olduğu alanlar yer almaktadır.

Tablo 20: Kişisel Veri Koruma Yaklaşımı, Strateji ve Avantajları

	AB	ABD	Çin
Yaklaşımı	Kişisel verileri insan hakları ve kişilik hakkı kapsamında değerlendiriyor. AB içinde kişisel veri	Sektörel bazında düzenlemelerin yapılması ön plandadır. Kişisel veriler mahremiyet	Yöntem olarak AB hukukuna benzemesine rağmen, sektörel bazda düzenlemeler yapmaktadır. Kişisel

⁴³² Berna Akçalı Gür, **a.g.m.**, s. 851.

	koruma yasama çerçevesinin oluşturulmasını hedefliyor.	kategorisinde, mülkiyet hukuku kapsamında değerlendiriliyor.	bilgilerin korunması konusunda yeterli deneyime sahip değildir.
Stratejileri	İnsan Odaklı (Human Centric) etik standartların araştırma ve geliştirilmesi, kişisel verilerin korunması ön planda. Tedariki teşvik etmek ve teknolojik gelişim için öncü bir misyon oluşturmak; sosyo-ekonomik değişikliklere hazırlanmak; yapay zekâ etiği konusunda bir çerçeve oluşturmak ⁴³³ .	Yapay zekâ araştırmalarına fon sağlamak; yapay zekâ teknolojisinin dağıtım ile ilgili yasal engelleri kaldırmak; araştırma ve geliştirilmesini teşvik etmek için müttefiklerle iş birliği yapmak; geleceğin Amerikan iş gücünü eğitmek, stratejik askeri avantaj elde etmek ve hükümet hizmetleri sağlamak için yapay zekayı kullanmak ⁴³⁴ .	“Çin’de Üretim 2025” planı çerçevesinde, yapay zekânın devlet tarafından desteklenmesi, teknolojik gelişim ön planda. Stratejileri Ar-Ge, sanayileşme, yetenek geliştirme, eğitim ve beceri edinme, standart belirleme ve düzenlemeler, etik ve güvenlik alanlarını kapsamaktadır ⁴³⁵ .
Avantajı	Etik denetim yöntemlerinde lider konumda.	GAFA ⁴³⁶ sayesinde internet hizmetlerinde	Devlet destekli BAT ⁴³⁷ aracılığıyla veri

⁴³³ European Commission, National strategies on Artificial Intelligence: a European perspective in 2019, (Çevrimiçi) <https://ec.europa.eu/digitalsinglemarket/en/artificial-intelligence>, (Erişim Tarihi: 20.01.2021).

⁴³⁴ White House, “Artificial Intelligence for the American People”, (Çevrimiçi) <https://www.whitehouse.gov/ai/>, (Erişim Tarihi: 20.01.2021).

⁴³⁵ Tim Dutton, “An Overview of National AI Strategies”, (Çevrimiçi) <https://medium.com/politics-ai/an-overview-of-national-ai-strategies-2a70ec6edfd>, (Erişim Tarihi: 20.01.2021), par. 10.

⁴³⁶ GAFA: Google, Amazon, Facebook ve Apple

⁴³⁷ BAT: Baidu, Alibaba, Tencent

		ve veri toplamada önde gelmektedir.	toplamada önde gelmektedir.
Örnekler	“Sorumlu Araştırma ve İnovasyon” ⁴³⁸ SPARC ⁴³⁹ EURON ⁴⁴⁰	“Ulusal Bilim ve Teknoloji Konseyi Raporu” ⁴⁴¹ “Yapay Zekâ Araştırma ve Geliştirme Ulusal Strateji Planı” ⁴⁴²	“Yapay Zekâ İlkeleri” ⁴⁴³

Tablodaki karşılaştırmadan hareket ettiğimizde AB’nın kişisel verileri koruma konusundaki çalışmaları ve etik açıdan sürdürdüğü projeler önem taşımaktadır. Özellikle kişisel verilerin korunması konusunda çağımızdaki en katı yasal çerçeve oluşturmayı hedefleyen AB, GDPR aracılığıyla kişisel verilerin korunması konusunda dünya ülkelerine örnek teşkil etmektedir. Uygulama alanının genişliği, AB ülkeleri arasında üst seviyede uyum sağlamaya çalışması, veri sahibinin/ilgili kişinin hakların genişletilmesi, veri sorumluların çoğaltılması ve yükümlülük ve ihlal durumundaki ceza miktarların caydırıcılığı GDPR’ın getirdiği yenilikler arasında yer almaktadır. Yukarıda bahsedilen yenilikler yapay zekâ çağında kişisel verilerin korunması kapsamında günümüze kadar yapılan çalışmalar arasında lider konumda diyebiliriz.

⁴³⁸ Responsible Research and Innovation: “Horizon 2020” programı altında, Yapay Zeka teknolojilerin etkilerini ve topluma getirecek sonuçları amaçlayan araştırma sürecidir.

⁴³⁹ Yapay Zekâ teknolojilerinin ekonomik ve sosyal alanlarda olumlu etkiler yaratmasını ve her sektörde kullanılmasını amaçlayan Yapay Zekâ ve robotik çalışmalarını çerçevesinde kurulan bir ortaklık.

⁴⁴⁰ Etik kurallardan oluşan rehber niteliğindeki çalışmadır.

⁴⁴¹ ABD Ulusal Bilim ve Teknoloji Konseyinin Ekim 2016 yılında “Yapay Zekâ Geleceğine Hazırlanmak” adlı rapor yayımladı.

⁴⁴² ABD Ulusal Bilim ve Teknoloji Konseyinin Ekim 2016 yılında “Yapay Zekâ Araştırma ve Geliştirme Ulusal Strateji Planı” adlı rapor yayımlayıp, Yapay Zekâ alanında uygulanması beklenen yedi strateji belirlendi.

⁴⁴³ Çin Yapay Zekâ Akademisi Mayıs 2019 yılında, Yapay Zekanın geliştirilmesi ve yönetilmesine ilişkin ilkeler yayımladı. Söz konusu rapor iyilik ilkesi, insanlığa özgü olma ilkesi, sorumluluk ilkesi, risklere hâkim olma ilkesi, ahlak ilkesi, eşitlik ilkesi, aydınlatma ilkesi vb. içermektedir.

AB'nın İnsan Odaklı etik standartların araştırma ve geliştirme çalışmaları devam etmektedir. ABD ise sektör bazında yapılan düzenlemeler aracılığıyla daha çok mahremiyet kapsamında, mülkiyet hukuku kapsamında kişisel koruması söz konusu etmiştir. Yapay zekâ alanında ise dünyanın en büyük BT desteği ile lider konumunu korumaktadır. Çin teknoloji alanlarında büyük ilerleme kaydetmesi ile birlikte, kendine özgü düzenlemeler ortaya çıkarmıştır. Kişisel verilerin korunması kapsamında da hızlı bir şekilde reform yapılmaktadır. Fakat uygulamada AB ve ABD'den çok daha geri de olduğu söyleyebiliriz.

3.6. Yapay Zekâ Çağında Kişisel Veri Korunmasına Yönelik İzlenebilecek Stratejiler

Mevcut yasal çerçeveleri altında kişisel verilerin korunması konusunda ne kadar mükemmel yasa ortaya çıkarılsa çıkarılsın, yapay zekânın hızlı gelişimi yasal kapsamın sınırlarının ötesine kolayca geçebilir ve bu da mevcut yasal yaklaşımı yapay zekâ alanında etkisiz hale getirebilir. Kişisel verileri korumaya yönelik en verimli strateji aslında kişisel verilerin toplanmasını en aza indirmektir. Toplanamadığı verilerde hiçbir şey ters gidemez, kötüye kullanılamazlar veya yanlışlıkla sızdırılmaz. Kişisel verilerin toplanmasının en aza indirilmesi, kişiye ait daha az veri toplanarak veya daha az kişiden veri toplanarak sağlanabilir.

Fakat telaşa dolu, teknolojiye bağlı olan gündelik hayatımızda biraz yavaş yaşamak artık bizim elimizde olmadığı için, hızlı bir yaşama alışmamız gerekmektedir. kişisel verilerin paylaşılmadığı bir ortamda yaşamamız mümkün olmayacak hale gelmiştir. Kişisel verileri açığa çıkarmadan günlük işlemlerin yürütülmesi imkânsız denilebilecek durumdadır. Bu nedenle yapay zekâ çağında kişisel verilerin toplanmasını sınırlamak gelişime açısından kabul edilemeyeceği için hukuksal bir dengenin bulunması zorunlu hale gelmiştir.

Günümüzde kişisel verileri koruma yasal çerçevesini ifade etmenin iki yolu olabilir. Birincisi, yapay zekâyı odaklanan ayrıntılı yasayı çıkarmak; ikincisi, temel

ilkeleri belirleyen ve uygulayan yumuşak bir yasa (esnek hukuk) teklif etmek. Birinci yöntem ile öngörülemeyen yapay zekâ gelişimlerini yöneten ayrıntılı bir düzenleme uygulanabilir. Ancak yukarıda değinildiği gibi yasal sınırlamaların etkisiz kalması muhtemeldir. Ayrıca yapay zekâ dünyasında tutarlı bir yasal çözümün imkânsız olduğu gerçeğini kabullenmemiz gerekmektedir. Bu nedenle ikinci yöntem olan esnek yöntem tercih edilmek zorunlu nitelik kazanmıştır. Esnek hukuk alanında yapılan en güncel çalışma Avrupa Komisyonunun “Yeni Nesil Teknolojiler ve Yapay Zekânın Hukuki Olarak Düzenlenmesine İlişkin Raporu”dur⁴⁴⁴. Bu rapordan sonra 14 AB üyesi tarafından yeni bir “Politika Önerisi Raporu”⁴⁴⁵ yayımlanmıştır. Rapor yapay zekâyâ ilişkin gelecekteki hukuki düzenlemelerin esnek hukuk bakış açısıyla yapılması gerektiğini vurgulamıştır. Özellikle teknolojinin hızlı gelişen doğası karşısında muhtemel sorunlar açısından doğrudan bağlayıcı nitelikteki kurallar yerine Avrupa Komisyonunun önerdiği esnek hukuk yaklaşımının benimsenmesi gerektiği belirtilmiştir. Bu anlamda temel güvenlik standartlarının sağlanması ve yapay zekânın rekabetçi avantajlarının ortaya konulabilmesi için mevcut yasal düzenlemelere ek olarak ön düzenleme ve diğer gönüllü uygulamalar gibi esnek hukuk çözümlerinin tercih edilmesi gerekliliği konu edilmiştir⁴⁴⁶. Bu noktadan hareket edildiğinde, yapay zekâ çağında kişisel verilerin korunmasına yönelik örnek stratejiler ortaya çıkmaktadır.

3.6.1. Aydınlatılmış Rıza

Yapay zekâ çağında kişisel verilerin korunması açısından karşılaştığı zorluklar arasında şeffaflık, veri asimetrisi ve rıza sorunu gelmektedir. Buradan hareket edecek

⁴⁴⁴ European Commission, On Artificial Intelligence- A European Approach to Excellence and Trust, Brussels, 2020, (Çevrimiçi) https://ec.europa.eu/info/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en (Erişim Tarihi: 26.02.2021).

⁴⁴⁵ Innovative and Trustworthy AI: Two Sides of The Same Coin, (Çevrimiçi) <https://em.dk/media/13914/non-paper-innovative-and-trustworthy-ai-two-side-of-the-same-coin.pdf>, (Erişim Tarihi: 02.11.2020).

⁴⁴⁶ İstanbul Barosu, Yapay Zekâ Çağında Hukuk 2020, İstanbul, 2020, s. 4.

olursak, yapay zekâ çağında aydınlatılmış rıza mekanizmasını yeniden şekillendirilmesi gerekiyor.

Her şeyden önce, rıza beyanları tüm veri işleme bağlantılarından geçmeli ve her aşama ilgili kişinin açık rızasını gerektirmelidir. İkinci olarak, rıza şekli basitleştirilmeli ve bildirim basit ve açık bir dilde olmalıdır. Kişisel verileri işlemeyen önce, ilgili kişinin rızasının alınması gerekmektedir⁴⁴⁷. İlgili kişi tarafından kişisel verilerinin işlenmesi için verilen rıza geçerli bir rıza olması gerektiğinden, işlem hakkında tam olarak bilgilendirilmeli ve muvafakat verirken herhangi bir dış etkiye maruz kalmaması gerekmektedir⁴⁴⁸. Bu durumda, bilgilendirme kuralı etkinleştirilecektir.

Ayrıca hukuki metin, kişisel verilerin veya kişisel verilerin işlenmesinde üstün sayılabilecek özel veya kamu menfaatlerinin açıkça belirtilmesi halinde, kişisel verilerin işlenmesinin kanun ilkesine uygun olarak ve ilgili kişinin rızası olmaksızın gerçekleştirilmesi gerekli olduğu durumlar arasında denge kurulması önem arz etmektedir⁴⁴⁹. Yine, verilen onayın geri çekilebilir olması, özel veri türleriyle karşılaştığında daha katı onay koşulların getirilmesi de önem taşımaktadır.

Yapay zekâ çağında aydınlatılmış rıza mekanizmasının karşılaştığı en büyük sorun ilgili kişilerin rıza beyanını dikkatli okumaması ve umursamaması denilebilir. Öte yandan ilgilenmek, öğrenmek isteyen ilgili kişiler olursa da rıza beyanları uzun, anlaşılması zor olduğu için işlevsellik açısından sorun yaratmaktadır. İlgili kişilerin verilerin ilk toplanmasından nihai verilerin eksiksiz aktarılmasına kadar olan rıza hakkı kişisel verileri koruma açısından önemli bir rol oynamaktadır. Bu rıza hakkı için, veri toplayıcının ilgili kişiyi, toplama amacı, kapsamı ve işlemenin sonuçları hakkında

⁴⁴⁷Ian Lloyd, **Information Technology Law**, 5. b., Oxford: Oxford University Press, 2008, s.42

⁴⁴⁸ Songül Atak, “Kişisel Verilerin Korunmasına İlişkin Avrupa Birliği Yönergesinin Temel Özellikleri”, **Bahçeşehir Üniversitesi Hukuk Fakültesi Hukuk Dergisi**, S. 60 (2009), s. 211.

⁴⁴⁹ Hayrunnisa Özdemir, “Haberleşmenin Gizliliği ve Kişisel Veriler”, **Erzincan Üniversitesi Hukuk Fakültesi Dergisi**, C.13, S. 1-2 (2009), s. 139.

bilgilendirmesi gerekmektedir. Aksi takdirde, ilgili kişinin aydınlatılmış rızasının ihlali olabilmekte ve ihlal eden kişi hukuki sorumluluğa tabi tutulması gerekmektedir.

Veri asimetrisi sorununa gelince, yapay zekâ sistemleri ile bireyler arasındaki veri asimetrisi olgusu, yapay zekâ çağının bir ürünüdür. Günümüzde bu durumu kökten düzenlemek zor gözükmemektedir. Veri asimetrisinin neden olduğu sorunlara çözüm bulmak, dezavantajlı konumda olan ilgili kişileri korumak için bazı önlemler alınması gerekmektedir. Yapay zekâ sistemi tarafından kontrol edilen devasa veri tabanı karşısında, bireysel kullanıcılar tarafından tutulan verileri zenginleştirmek, dengesiz durumu dengelemek ve kullanıcıların kişisel verilerin ve mahremiyetini korumak için uygun bir önlem olabilir. Bunun için aydınlatılmış rıza mekanizmasının güçlendirilmesi gerekmektedir.

Kişisel verilerin toplanması, işlenmesi ve kullanılması konusuna ilgili kişiler bildirilmeli ve izin alınmalıdır. Bu aynı zamanda iradenin özerkliği ilkesinin somut bir uygulaması niteliğinde olur. Bilgilendirilme hakkı kişisel veri ve mahremiyet haklarının korunması için ön koşuldur. Çünkü yanlış verilerin düzeltilmesi, silinmesi, itiraz hakkı vb. ancak kişisel verilerin toplanması, işlenmesi ve kullanılması konusunda yeterli kadar bilgi sahip olduğunda gerçekleşebilir.

Bilgilendirilme hakkını garanti etmenin yolu, iki yönlü izleme ile gerçekleşebilir. Yani verilerin toplanması ve kullanılması iki yönlü bilgilendirilmelidir (Yapay zekâ sistemi kullanıcı bilgilere, kullanıcı ise veri sorumlusu bilgilere erişir)⁴⁵⁰. Veri toplayıcılar veya veri sorumluları, kullanıcı bilgilerini elde etmek için kendi gerçek bilgilerini sağlamaya ihtiyaç duyduklarında, artan veri toplama maliyeti açısından belirli bir kısıtlama sağlayabilir.

⁴⁵⁰ Lei Yue, “人工智能发展中的法律问题探析 (Yapay Zekanın Gelişiminde Hukuki Sorunların Analizi)”, **Pekin Yayınlar ve Telekomünikasyon Üniversitesi Dergisi (Sosyal Bilimler Basımı)**, (2018), s. 23.

3.6.2. Unutulma Hakkı

Yapay zekâ çağında kişisel veri koruma literatüründe öne çıkan kavramlardan biri “unutulma hakkı” dır. Unutulma hakkı genel anlamıyla belirli kişisel verilerin (ilgili kişide veya diğer medyada yer alıyorsa) verilerin depolandığı aygıttan silinmesini isteme hakkıdır⁴⁵¹. Günümüzde internette arama motoru denen bir mekanizma da yer alan kişisel veriler, belirli bir süre içinde ilgili kişilerin geleceğine katkı sağlayamayacak bir veri haline gelirse, ilgili kişinin söz konusu arama motoru sahibi veya firma tarafından silinmesini talep etme veya otomatik olarak silinmesini isteme hakkı tanımlanmıştır.

Unutulma hakkı kapsamında, Google arama motoru operatörünün İspanyol avukatın mülk satışına ilişkin verilerini silmediğine ilişkin davadaki ABAD kararı⁴⁵² emsal teşkil etmektedir. İspanyol yargı makamlarının 16 yıl önceki ilgili verileri Google’dan silme kararına karşı, Google itirazda bulunmuş ve sonunda bu dava ABAD’ında gündeme gelmiştir. Mahkeme Mayıs 2014 tarihinde, 95/46/AT Sayılı Direktifin⁴⁵³ hükümleri uyarınca, üye devletlerin sorumluluklarının 6. maddesini dikkate almış ve ilgisiz hale gelen bu tür verilerin silinmesine karar vermiştir. Bu dava “unutulma hakkı”nın AB çerçevesinde uygulamaya geçtiğinin belirgisi haline gelmiştir⁴⁵⁴.

Yapay zekâ çağında ilgili kişinin bazı haklarının genişletilmesi gerekmektedir ve bu haklardan en başta geleni unutulma hakkıdır. İlgili kişilere yasal olarak tüketim kayıtları, hareket izleri vb. verileri silme hakkı verilmesi, bu verilerin orijinal toplama amacının ötesinde ikincil işlem için kullanılmasının ve bu veri/çıkarımların

⁴⁵¹ Allyson Haynes Stuart, “Google Search Results: Buried If Not Forgotten”, **North Carolina of Law & Technology**, 2014, s. 479-482.

⁴⁵² ABAD, C-131/12, Google Spain, 13.05.2014.

⁴⁵³ İlgili Direktif için bkz: Bölüm 2, 5, 1 “95/46/AT Sayılı Direktif”.

⁴⁵⁴ Akgül, Kişisel Veri..., **a.g.m.**, s. 31.

aktarımının engellenmesi gerekmektedir. Bu çerçevede GDPR ilgili kişiye unutulma hakkı tanımaktadır.

Unutulma hakkı yapay zekâ çağında verilerin sonsuza doğru tekrar işlenmesini engelleyen yöntemlerden biridir. Nitekim yapay zekâ, büyük veri teknolojilerinde değersiz veri olmadığından, veriler şimdi kullanılsa da gelecekte mutlaka değer kazanacak ve işlenecektir. Unutulma hakkı bu açıdan ilgili kişinin kişisel verilerini korumada önem taşımaktadır.

3.6.3. Makul Çıkarım Hakkı

Büyük veri analitiği ve yapay zekâ teknolojileri bireylerin davranışları, tercihleri ve özel yaşamları hakkında sezgisel olmayan ve doğrulanamayan çıkarımlar ve tahminler yapmaktadır. Bu çıkarımlar çeşitli verilere dayanır ve ayrımcı, önyargılı ve saldırgan karar verme riski ortaya çıkarmaktadır⁴⁵⁵. Veri koruma düzenlemeleri, aslında insanların mahremiyetini, kimliğini, itibarını ve özerkliğini korumayı amaçlamaktadır, ancak bu düzenlemeler yapay zekâ çağında ilgili kişileri çıkarımsal analitiğin yeni risklerinden korumada başarısız olmaktadır.

Günümüzde ilgili kişilerin kendi verilerinden çıkarımlar yapma konusunda çok az kontrol ve gözetim hakkına sahip olduğunu söyleyebiliriz. Diğer kişisel veri çeşitleri ile karşılaştırıldığında çıkarımlar, GDPR'daki “ekonomi sınıf” veri niteliğinde değerlendirilmiştir. Nitekim yapay zekâ aracılığıyla ilgili kişiler hakkında çıkarım yapmak ilgili kişiyi alakadar eden verileri yasal şekilde toplamaktan çok daha kolay olmaktadır. GDPR kapsamında çıkarımlar söz konusu olduğunda, ilgili kişilerin kişisel verileri öğrenme (m. 13-15), düzeltme (m. 16), silme (m. 17), itiraz etme (m. 21) ve taşıma (m. 20) hakları önemli ölçüde kısıtlanmaktadır. Bu durumda genellikle veri sorumlusunun çıkarları (örneğin, ticari sırlar, fikri mülkiyet) ile veri koruma

⁴⁵⁵ Brent Daniel Mittelstadt vd., “The Ethics of Algorithms: Mapping the Debate”, Big Data & Society, (Çevrimiçi) <https://journals.sagepub.com/doi/full/10.1177/2053951716679679>, (Erişim Tarihi: 20.01.2021).

arasında bir denge kurulmaya çalışılmaktadır. Benzer şekilde, GDPR hassas çıkarımlara (m. 9) veya bu tür çıkarımlara dayalı önemli kararlara karşı ilgili kişiyi korumada etkisiz kalmıştır.

ABAD kararlarından (örneğin, Nowak davası) hareket ettiğimizde mahkemenin kişisel verilerin korunmasını özellikle verilerin toplandığı aşamasına ve daha sonraki düzeltme, itiraz etme ve silme süreçlerine yoğunlaştırdığını söyleyebiliriz. Bununla birlikte ABAD'nın veri koruma konusunda kişisel verileri içeren çıkarımlara, karar alma süreçlerinin doğruluğuna veya bu süreçleri şeffaf hale getirilmesine ilişkin henüz içtihat oluşturmadığı görünmektedir⁴⁵⁶.

Kısacası, ilgili kişiler kişisel verilerinin nasıl toplandığı ve işlendiği üzerinde kontrole sahiptir, ancak nasıl değerlendirileceği üzerinde çok sınırlı kontrole sahiptir. ABAD, ilgili kişilerin kendi kişisel verilerinin nasıl değerlendirildiği konusunda itiraz etmek isterse, başvurunun GDPR'a değil, ilgili vakalar için geçerli sektörel kanunlar aracılığıyla aranması gerektiğini açıkça belirtmektedir⁴⁵⁷.

Makul çıkarımlar hakkı kapsamında çıkarımlar konusunda ilgili kişilere aşağıdaki hakların tanımlanması gerekmektedir:

Birincisi, çıkarımlar hakkında bilgi edinme hakkı: bireylerin ne zaman ve hangi çıkarımların yapıldığını öğrenebilmesi konusunda şeffaflık ilkesi gündeme gelmektedir. İlgili kişiler, kişisel veri toplama ve işlemenin kapsamı ve amaçları hakkında bilgi sağlamayı amaçlayan GDPR kapsamında şeffaflık ilkesine dayanan haklara sahip olabilmektedir. (m. 13-15) Çıkarımlar ile ilgili olarak, şeffaflık ilkesi doğrultusunda, ilgili kişilere, elde edilen ve türetilen kişisel verilerin veya ilgili

⁴⁵⁶ Wachter ve Mittelstadt, **a.g.m.**, s. 4; Çıkarımların niteliği hakkında ABAD ile Madde 29 çalışma gurubu görüşleri için bkz: Tablo 19, s. 161.

⁴⁵⁷ ABAD, C-141/12, YS, 17.07.2014 ve ABAD, C-372/12, par. 45-47.

kişilerin doğrudan sağlamadığı verilerin varlığı ve işlenmesi hakkında bilgilendirilme hakkı tanımlanabilir⁴⁵⁸.

İkincisi, çıkarımları düzeltme hakkı: mevcut düzenlemelerde ilgili kişiler, yanlış kişisel verileri düzeltme veya eksik verileri “tamamlayıcı bir beyan sunarak” tamamlama hakkına sahiptir. İşlenen veriler veya çıkarılan çıkarımlar gerçeklere dayandığında veya başka bir deyişle doğrulanabilir olduğunda (örneğin isim, doğum tarihi, medeni durum, gelir) düzeltme hakkın uygulanması kolay olmaktadır⁴⁵⁹. Ancak yapay zekâ aracılığıyla türetilen çıkarımların doğrulanabilirliği sorun oluşturmaktadır.

Örneğin, ilgili kişinin tahmin edilen gelir aralığının doğru olup olmadığı sorulduğunda çıkarımlar temel bilgi ile doğrulanabilirken, bazı çıkarımlar doğası gereği öznel (örneğin, ilgili kişinin ‘yüksek riskli ödünç alıcı’ hakkındaki çıkarım) veya öngörüdür (örneğin, ilgili kişi önümüzdeki iki yıl içinde bir ipotek için başvuru yapacak) ve bu nedenle yapay zekâ çağında bazı çıkarımlar doğası gereği “doğrulanamaz” niteliğindedir. ABAD kararları bu tür çıkarımları kişisel veri niteliğinde değerlendirilmesi konusunda tartışmalı yorumlara sahip olduğu için, çıkarımları düzeltme hakkı güçlendirilmesi gereken haklar arasında değerlendirilebilir.

Üçüncüsü, çıkarımlara itiraz etme ve silme hakkı: kendisi ile ilgili olan çıkarımlara itiraz etme veya silme hakkı, ilgili kişinin aynı fikirde olmadığı çıkarımlara karşı korunabileceği bir çare olabilmektedir. GDPR kapsamında ilgili kişinin kendisi ile ilgili olan kişisel verileri silme hakkı tanımlanmıştır. Fakat GDPR, ilgili kişinin silme hakkı ile veri sorumlusunun meşru menfaati arasında açık bir denge öngörmemiş olmaması söz konusu olmuştur. Madde 29 Çalışma Grubu ise meşru

⁴⁵⁸ Wachter ve Mittelstadt, **a.g.m.**, s. 32.

⁴⁵⁹ **a.g.m.**, s. 36.

menfaatler konusunda görüş⁴⁶⁰ yayınlamıştır. Görüşte “geleneksel yöntemle doğrudan pazarlama ve diğer reklam biçimleri”, “dolandırıcılığın önlenmesi, hizmetlerin kötüye kullanılması engellenmesi”, “fiziksel güvenlik, BT ve ağ güvenliği”, “bilimsel veya istatistiksel amaçlar için” ve “araştırma amaçlı işleme (pazarlama araştırması dahil)” meşru menfaat listesinde yer alarak ilgili kişinin bu alanlarda koruma altında olmayabileceğini belirtmiştir.

Çıkarımları silme hakkındaki bir diğer sorun ise, çıkarılan asıl veriler silinse bile, veri sorumlusu bu verileri diğer üçüncü taraflarla önceden paylaşmış olabilmesidir⁴⁶¹. Bu durumda veri sorumlusunun üçüncü tarafları silme konusunda bilgilendirme yükümlülüğü sınırlı olması nedeniyle sorun oluşturabilir. Günümüzde en çok kullanılan sosyal medya platformlara baktığımız zaman, uygulamalar arası veri paylaşımları hızlı gerçekleştiğinden ilgili kişinin çıkarımlara karşı hakkını savunacağı zaman söz konusu çıkarımların üçüncü tarafa aktarılmış olması muhtemeldir. Özetle kişisel verilerden türetilen çıkarımlarla ilgili itiraz ve silme hakkı yapay zekâ çağında yeniden değerlendirilmesi gerekmektedir.

Dördüncüsü, hassas çıkarımlara karşı korumalar: önceki bölümlerde açıklandığı gibi, çıkarımların öğrenilmesi, aktarılması, düzeltilmesi ve silinmesine yönelik talepler genellikle ilgili kişilerin ve veri sorumlusunun çıkarları arasında bir denge kurulmasını gerektirir. Fakat, hassas veriler işlenirken, bu denge çoğu zaman düşünülmemeli veya en azından ilgili kişinin çıkarlarına yönelik yorumlanması gerekmektedir⁴⁶².

Kişisel verilerin korunması kapsamında ilgili kişiler, çıkarımlardan ve türetilen verilerden kaynaklanan risklerden korunmaya en çok ihtiyaç duyan taraf denilebilir.

⁴⁶⁰ Article 29 Data Protection Working Party, “Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC”, (Çevrimiçi) https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf (Erişim Tarihi: 25.02.2021).

⁴⁶¹ a.g.m., s. 42.

⁴⁶² a.g.m., s. 44.

Hesap verebilirlik sorununun çözülmesi ve çıkarımlara yönelik ilgili kişilerin korunmasını gerçekleştirmek için, mahremiyet hakkını ihlal eden veya itibarına zarar veren çıkarımlara dayalı doğrulanamaz ve mantığa aykırı tahminlere uygulanabilecek yeni bir “makul çıkarım hakkı” önerilmiştir⁴⁶³.

Veri öznelerine yönelik potansiyel riskler, verilerin toplandığı anda sona ermemektedir ve bu nedenle, veri koruma yasaları, çıkarımsal analitiğin olası zararlarına karşı koruma sağlayamamaktadır. Yapay zekâ çağı, verilerin sorumlu ve normatif olarak kabul edilebilir kullanımını, etik veri paylaşım uygulamalarını ve zarar durumunda uygun yasal çözümleri düzenleyen bir “makul çıkarım hakkı” gerektirmektedir⁴⁶⁴. Faydalar ve riskler sektöre ve özel uygulamaya bağlı olarak büyük ölçüde farklılık gösterdiğinden, toplumsal kabul edilebilir makul standartlarını belirlemek için daha fazla araştırma yapılması gerekmektedir.

3.6.4. Gizliliği Teşvik Eden Teknolojiler (Privacy Enhancing Technologies)

Kişisel verilerin korunmasına yönelik yapay zekâ çağında karşılaşılan sorunlara yönelik neler yapılabileceği konusunda çalışmalar devam etmektedir. Bunlardan başlıca geleni mahremiyetin daha tasarım aşamasındayken korunmaya başlaması gibi fikirlerin ortaya atılmış olmasıdır. Yapay zekâ teknolojilerin tasarımlarına entegre edilecek mekanizmalar yoluyla mahremiyetin güvence altına alınması, kişisel verilerin korunması yaklaşımı etkilerini göstermeye ve insan haklarına yönelik etkileri hukuki düzenlemelere yön vermeye başlamıştır⁴⁶⁵. Nitekim GDPR kapsamında Varsayılan Ayarlarla Veri Koruma ve/veya Tasarımla Veri Koruma ile ilgili düzenlemeler yer almaktadır.

Gizliliğe Dayalı Tasarım (PbD) veya başka adıyla Varsayılan Ayarlarla Veri Koruma ve/veya Tasarımla Veri Koruma, sistemlerin kurulumunda gizliliğe dayalı

⁴⁶³ a.g.m., s. 79.

⁴⁶⁴ Wachter ve Mittelstadt, a.g.m., s. 4.

⁴⁶⁵ Ersoy, a.g.e., s. 24

problemleri oluşmadan engellemeyi amaçlayan yöntemdir⁴⁶⁶. Bu konseptte göre hukuk düzeni ihlali tepki vermek yerine ihlalin gerçekleşmesinden önce önlemeyi amaçlamaktadır⁴⁶⁷. Sonuçta kişisel verilerin korunması sadece verilerin toplaması aşamasında olmayıp, sistemin esaslı bir unsuru haline gelmekte ve bütün veri işleme sürecinde önem arz etmektedir.

PbD iki anlamda yapay zekâ çağında uygulamaya açıktır. İlk olarak, PbD, uygulanması için yasal olarak bağlayıcı hükümler gerektirmemektedir. PbD yalnızca yasal hükümler kapsamında değil, aynı zamanda bir sertifikasyon mekanizması gibi yumuşak hukuk yaklaşımı yoluyla da uygulanabilir. İkincisi, PbD’yi uygulayan teknolojilerin kapsamı sınırlanmamıştır. 2012’de Kanada Bilgi ve Gizlilik Komisyonu tarafından yayınlanan “Tasarım Yoluyla Gizliliği Operasyonelleştirme”⁴⁶⁸ raporunda IP coğrafi konumlarında kimlik tespiti, biyometrik şifreleme, çift gizlilik mimarisi, yüz tanımda anonim dijital tabela ve gizliliği koruyan bir RFID (radio-frequency identification) etiketi dahil olmak üzere çok sayıda tekniği örneklemiştir. Bu nedenle, yapay zekâ ile ilgili teknikler geliştikçe, mahremiyeti koruma tekniklerinin geliştirilmesi beklenmektedir.

Yapay zekâ makine öğrenimi için uygun çözümü başarmak için yapay zekânın mahremiyeti en başından yerleştirerek otomatik olarak korumasını sağlamak temel ilkesi haline gelmiştir. Bireylerin PbD konseptinde mahremiyetlerini korumak için kendi çabalarını harcaması gerekmemektedir. Ek olarak, PbD uygulamaları gizlilik ve güvenliği de sahip olmanın mümkün olduğunu göstermektedir⁴⁶⁹.

⁴⁶⁶ a.g.e., s. 125.

⁴⁶⁷ Mesut Serdar Çekin, “6698 Sayılı Kişisel Verilerin Korunması Hakkında Kanun’un Big Data (Büyük Veri) ve İrade Serbetisi Açısından Değerlendirilmesi”, *İÜHFİM*, C. LXXIV, S. 2 (2016), ss. 629- 650, s. 642.

⁴⁶⁸ Ann Cavoukian, “Operationalizing Privacy by Design: A Guide to Implementing Strong Privacy Practices”, (Çevrimiçi) <http://www.ontla.on.ca/library/repository/mon/26012/320221.pdf>, (Erişim Tarihi: 12.06.2018)

⁴⁶⁹ Ann Cavoukian, “Privacy by design: the 7 foundational principles”, (Çevrimiçi) <https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf>, (Erişim Tarihi: 12.07.2018)

Günümüzde yapay zekâ uygulamalarının gizliliği üzerindeki potansiyel etkisini değerlendirmek için Gizlilik Etki Değerlendirme yöntemleri geliştirmeye giderek daha fazla istek duyulmakta⁴⁷⁰. Gizlilik Etki Değerlendirmesi, bir projenin, sistemin, programın, hizmetin, ürünün veya başka bir planın mahremiyet üzerindeki etkisini değerlendirmek ve gerektiğinde paydaşlarla müzakere ederek olumsuz etkisini önlemek veya en aza indirmek için düzeltici önlemler almak amacıyla kullanılan bir yöntem olarak tanımlanır⁴⁷¹.

Yapay zekâ çağında PbD stratejileri konusunda önde gelen isimlerden Jaap Henk Hoepman söz konusu stratejileri iki farklı kategoriye ayırmıştır: Veri odaklı stratejiler ve süreç odaklı stratejiler. Veri odaklı stratejiler, verilerin kendilerinin gizlilik dostu niteliğinde işlenmesine odaklanır. Doğası gereği daha tekniktirler ve dört alt başlığı bulunmaktadır. Tablo 21’da veri odaklı stratejiler yer almaktadır:

Tablo 21: Veri Odaklı Stratejiler⁴⁷²

Veri Odaklı Stratejiler	
Minimize etmek	Kişisel verilerin işlenmesini mümkün olduğunca sınırlamak.
Ayrıt etmek	Kişisel verilerin işlenmesini mümkün olduğunca başka işlemlerden ayırmak.
Özetlemek	Kişisel verilerin işlendiği ayrıntıları mümkün olduğunca kısaltmak.

⁴⁷⁰ David Wright ve Paul De Hert, “Introduction to Privacy Impact Assessment”, **Springer Link**, 2012, (Çevrimiçi) https://ezproxy.ticaret.edu.tr:2056/chapter/10.1007/978-94-007-2543-0_1#citeas (Erişim Tarihi: 28.10.2020), ss. 3-32.

⁴⁷¹ David Wright, “The State of The Art in Privacy Impact Assessment”, **Computer Law & Security Review**, C. 28, S. 1 (Şubat 2012), ss. 54-61, s. 56.

⁴⁷² Jaap Henk Hoepman, “Privacy Design Strategies (The Little Blue Book)”. (Çevrimiçi) <https://www.cs.ru.nl/~jhh/publications/pds-booklet.pdf>. (Erişim Tarihi: 15.10.2020). s. 3.

Gizlemek	Kişisel verileri korumak veya bağlantı kurulamaz veya gözlemlenemez hale getirmek. Herkese açık olmadığından veya bilinmediğinden emin olmak.
----------	---

Süreç odaklı stratejiler, kişisel verilerin sorumlu bir şekilde işlenmesini çevreleyen süreçlere odaklanmaktadır. Tablo 22’de süreç odaklı stratejiler yer almaktadır:

Tablo 22: Süreç Odaklı Stratejiler⁴⁷³

Süreç Odaklı Stratejiler	
Bilgilendirme	İlgili kişileri kişisel verilerinin işlenmesi hakkında zamanında ve yeterli bir şekilde bilgilendirmek.
Kontrol hakkı sağlamak	İlgili kişilere kişisel verilerinin işlenmesi üzerinde yeterli kontrol edebilme hakkı sağlamak.
İcra edilebilirlik	Kişisel verileri gizlilik dostu bir şekilde işlemeyi taahhüt etmek ve bunu yeterince uygulamak.
Şeffaflık	Kişisel verilerin gizlilik dostu bir şekilde işlendiğini göstermek.

Bu stratejilerin gizliliği koruyan teknolojiler söz konusu olduğunda çakışabilecek bazı bölümleri vardır. Özellikle gizliliği koruma teknolojileri kavramı geniş bir şekilde ele alınırsa, gizliliğin korunmasına yardımcı olabilecek veya gizliliği koruyan veri işleme faaliyetlerini destekleyebilecek herhangi bir teknolojiyi içerecek

⁴⁷³ a.g.e.

şekilde yorumlandığı zaman yukarıda bahsi geçen stratejileri içerecek kadar genişletilebiliyor.

Gizlilik koruma teknolojileri ile gizlilik artırıcı teknolojiler arasında esas farklılıklar mevcuttur. Gizlilik artırıcı teknolojiler, mevcut sistemlerde gizliliğin korunmasının iyileştirilmesini amaçlarken; gizliliği koruma teknolojileri, esas olarak gizliliğin garanti edildiği yeni sistem ve teknolojilerin tasarımını hedeflemektedir. Bu nedenle, gizliliği koruma teknolojileri “tasarım gereği gizlilik” ilkesine daha güçlü bir şekilde bağlıdır⁴⁷⁴.

Organizasyonel yönlerden baktığımızda, yapay zekâ alanındaki gelişmelerin, örneğin katı politikalar ve gizlilik koruması türleri gibi yeni yöntemlerin kullanıldığını görebiliriz. BOOST projesi, IDSA çerçevesinde Avrupa Endüstriyel Veri Alanı geliştiriyor ve veri kümelerine sertifikasyon mekanizması ve kullanım kontrol politikaları teşvik ederek güvenli ortam oluşturmayı hedefliyor⁴⁷⁵. Rest Assured projesi, veri korumaya ilişkin kullanıcı isteklerini öğrenmek için yeni yöntemler kullanmakta olup, daha sonra veri koruma mekanizmalarına uygulamayı hedeflemektedir⁴⁷⁶.

Kısacası, yapay zekâ çağında kişisel verilerin korunması konusunda gizliliği teşvik eden teknolojiler önemli hale gelmiştir. Varsayılan Ayarlarla Veri Koruma ve/veya Tasarımla Veri Koruma yöntemleri, veri odaklı stratejiler ve süreç odaklı stratejiler bir araya getirilerek daha verimli, pratik olan uygulamaların ortaya çıkarılması beklenmektedir.

3.6.5. Tasarımda Şeffaflık

Tasarımda Şeffaflık olarak tercüme dilen Transparency by Design (TbD) modeli, şeffaflığı sonradan düşünülen bir nitelik olarak değil, yapay zekâ sistemleri tasarlarken

⁴⁷⁴ Timan ve Mann, **a.g.m.**, s. 9.

⁴⁷⁵ Proje hakkında daha fazla bilgi için bkz.: <https://boost40.eu/>

⁴⁷⁶ Proje hakkında daha fazla bilgi için bkz.: <https://restassuredh2020.eu/>

en başından itibaren dikkate alınması gereken bir ön değer olarak nitelendirmektedir⁴⁷⁷. Tasarımda Şeffaflık ilkeleri, yapay zekâ sistemleri için şeffaflığı gerçekleştirme talepleriyle giderek daha fazla karşılaşan kuruluşlar ve yapay zekâ geliştiricileri için rehberlik etmesi amacıyla ortaya konulmuştur.

Şeffaflık yapay zekâ çağında açıklanabilirlik ile güçlü bir bağlantı kurmuştur. Fakat yapay zekâ çağında şeffaflığın eleştirildiği konular da bulunmaktadır. Bir görüşte şeffaflık talep edilen tarafı genellikle ihmal eden ilke olarak görülmektedir⁴⁷⁸. Bu görüş verinin sadece açıklanmasını değil, aynı zamanda ilgili kişi tarafından alınması, yorumlanması ve anlaşılması gerektiğini savunmuştur⁴⁷⁹. Böylelikle verinin açıklanmasının şeffaflığa yol açması için, verinin ilgili kişinin ihtiyaçlarına göre uyarlanması gerektiği sonucuna varmıştır. Yoksa sadece şeffaflığın vurgulanması ilgili kişi açısından farklı etki yaratmamaktadır. Nitekim yapay zekâ teknolojileri şeffaf olsa dahi, ilgili kişinin verileri anlaması, yorumlaması gerekecektir.

Şeffaflık ile ilgili olan diğer konu mahremiyet ve rekabettir. Yapay zekâ sistemleri tamamen şeffaf yapılırsa, özellikle temel eğitime verileri yayınlanırsa hassas ve özel verileri açığa çıkarabilir. Bu, özellikle kişisel veriler, ses kayıtları, e-postalar, sosyal medya gönderileri ve resimler gibi makine öğrenimi algoritmalarını eğitmek için kullanıldığında karşılaşılan sorundur. Daha az önyargılı algoritmalar için, farklı guruplardan gelen verileri içeren daha çeşitli ve temsili eğitime veri setlerinin gerekli olduğu göz önüne alındığında, bu tür verilerin yayınlanması, daha önceden teknik açıdan dezavantajlı durumda olanları zarara maruz bırakabilir. Bu nedenle, şeffaflık ve açıklık çağrıları, bireylerin mahremiyet haklarına saygı duymaları gerekmektedir. Dahası, rekabet açısından şeffaflık şirketler için dezavantajlı olabilir. Şirketler, yapay

⁴⁷⁷ Heike Felzmann vd., “Towards Transparency by Design for Artificial Intelligence”, **Science and Engineering Ethics**, 2020, s. 3.

⁴⁷⁸ Jens Forssbaeck ve Lars Oxelheim, “The Multifaceted Concept of Transparency”, **The Oxford Handbook of Economic and Institutional Transparency**, der. Jens Forssbaeck ve Lars Oxelheim, Oxford: Oxford University Press, 2014, ss. 3-30.

⁴⁷⁹ Jakko Kemper ve Daan Kolkman, “Transparent to Whom? No Algorithmic Accountability Without a Critical Audience”, **Information, Communication & Society**, C. 22, S. 14 (2019), ss. 2081-2096.

zekâ sistemlerini daha şeffaf hale getirmenin, rakiplerin bu sistemleri kopyalamasına neden olabileceğini iddia edebilmektedir.

Tasarımda şeffaflık yapay zekâ çağında kişisel verilerin/mahremiyetin korunması konusundaki yeni gelişme olarak görülmektedir. Daha yeni ortaya konulan bu yöntem teknik ve hukuki açıdan daha çok denemelere ihtiyaç duymaktadır.

3.6.6. Açıklanabilir Yapay Zekâ

Makine öğrenimi yoluyla üretilen sonuçlara göre bilinmeyen konuların tahminleri, yapay zekâ ile ilişkili olarak daha net bir şekilde karakterize edilebilir. Makine öğrenimi tekniklerini kullanan algoritmalara, insan anlayışı olmadan yeni girdileri ele almak için karar verme kuralları oluşturmada bir dereceye kadar özerklik sağlanabilir. Sonuçta makine öğrenimi tarafından gerçekleştirilen görevlerin önceden tahmin edilmesi (yeni bir girdinin nasıl ele alınacağı) veya daha sonra açıklanması (belirli bir kararın nasıl verildiği) kolay olmamaktadır. Dahası, derin öğrenme, insan müdahalesi tarafından ayarlanmayan parametreler olmadan özellikleri çıkararak çeşitli bilgi türlerini özerk bir şekilde kavramsallaştırabilmektedir. İnsan desteği olmayan bilgisayarlarla öğrenme, yapay zekânın potansiyel olarak insan zekasının ötesinde gelişmesi anlamına gelmektedir. Bazen, yapay zekâ sistemlerindeki veri kümelerindeki istatistiksel sapmalar yanlış korelasyonlara yol açabilir.

Örneğin, derin öğrenme yöntemlerinin kullanılması zatürreyi diğer yöntemlerden daha başarılı bir şekilde teşhis edebilir. Ancak bu teşhis beklenmedik sonuçlar ortaya çıkarabilir. Bir derin öğrenme modeli astım geçmişi olan hastalar için pnömoniden ölme riskinin daha düşük olduğunu söyler. Bununla birlikte, bu model, astım hastalarının daha hızlı ve daha fazla ilgi gördüklerinden aslında daha yüksek risk taşıdığını gösterir. Yani derin öğrenme modeli astım hastalarına iyi bakıldığı için ölüm riskinin düşük olduğunu belirlemiştir. Aslında pnömoni, astım hastaları için son derece

önemli bir risktir⁴⁸⁰. Kısacası, bu korelasyona dayalı modelleri kullanma tehlikesi pratikte kaçınılmazdır. Bu açıdan makine öğrenimi ve derin öğrenme teknolojileri ışığında Açıklanabilir Yapay Zekâ (AYZ)’nın geliştirilmesi önemli hale gelmiştir.

P. Jonathon Phillips vd., tarafından kaleme alınmış olan “Açıklanabilir Yapay Zekânın Dört İlkesi Raporu”⁴⁸¹, AYZ’nın çok disiplinli doğasının anlaşılabilmesini amaçlayarak bilgisayar bilimi, mühendislik kuramı ve psikoloji yaklaşımları dahil ederek dört temel ilke ortaya koymuştur. Raporda yer alan dört temel ilke şunlardır:

- Sistemin bir açıklama üretmesi,
- Bu açıklamanın insanlar için anlamlı olması,
- Açıklamanın sistemin sürecini isabetli olarak yansıtması,
- Sistemin bilgi sınırlamalarını belirtebilmesi.

Bu dört ilke çok disiplinli bir yapı oluşturarak insan-makine etkileşiminin araştırılabilmesini sağlamaktadır. Bununla birlikte raporda ilgili ilkelerin kullanıcıların sistemleri derinlemesine anlamasını sağlamak ve bu şekilde daha güvenli bir ortam yaratabilmek için rehber niteliğinde olduğu bahsedilmektedir⁴⁸². İlkelerin altında açıklanan alt yapılar, karmaşık yapay zekâ sistemlerinin gerçek dünyada hayata geçirilebilmesi için AYZ sistemi metotlarının evrimini ele almıştır.

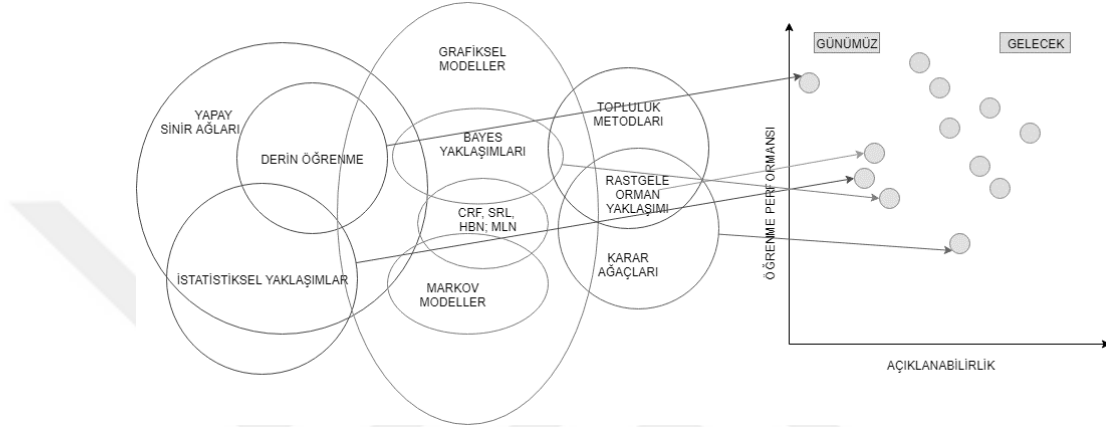
Yapay zekâ teknolojilerinin farklı yaklaşımları ile açıklanabilirlik arasında farklılıklar vardır. Genel olarak bakıldığında öğrenme yeteneği yüksek olan tekniklerin açıklanabilirliği düşük olacaktır. Nitekim derin öğrenme ve yapay sınır ağlarının öğrenme performansı çok yüksektir. Ancak açıklanabilirliği de o kadar zayıf kalmıştır. Günümüzde elde edilen tekniklerin gelecekte daha iyi açıklanabilir hale

⁴⁸⁰ Kızrak, Açıklanabilir..., **a.g.m.**, par. 7.

⁴⁸¹ U.S. Department of Commerce (P. Jonathon Phillips vd.), Four Principles of Explainable Artificial Intelligence, Washington, 2020.

⁴⁸² İstanbul Barosu, **a.g.e.**, s. 3.

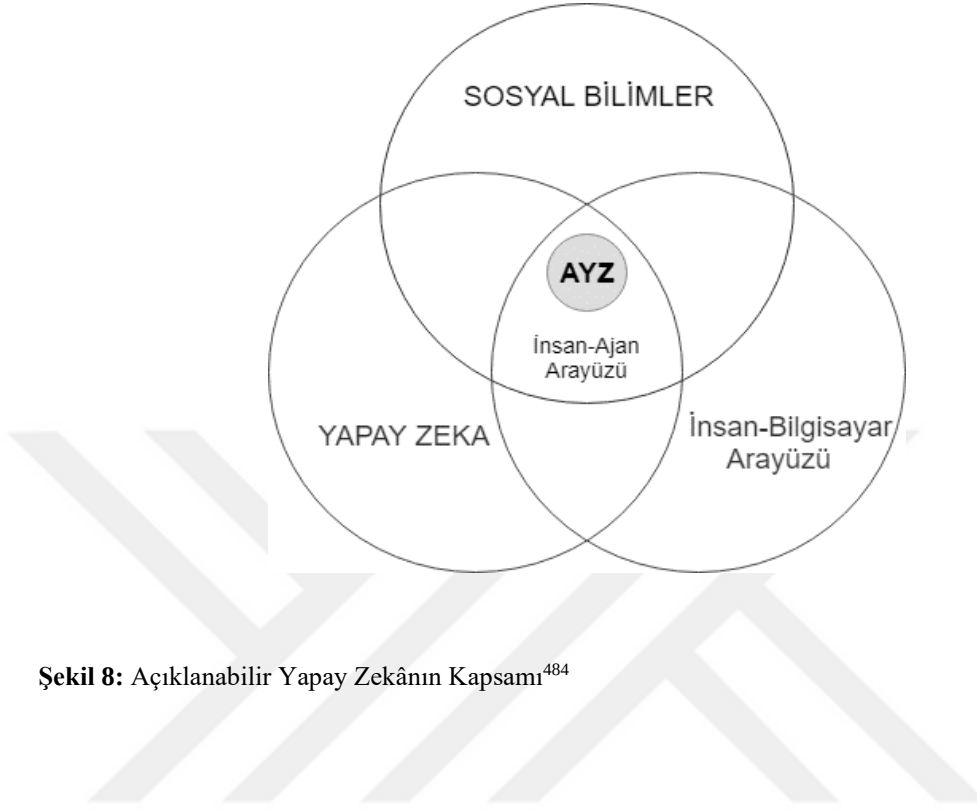
gelmesi beklenmektedir. Şekil 7’de ise farklı yaklaşımlara göre öğrenme performansı ve açıklanabilirlik günümüz teknolojisi ve gelecek üzere modellenmiştir.



Şekil 7: Farklı Yaklaşımlara Göre Performans ve Açıklanabilirlik Modeli⁴⁸³

AYZ günümüzde en çok konuşulan alanlardan biri olmakla beraber, yapay zekâ çağında kişisel verilerin korunması konusunda da umut verici yön göstermektedir. Nitekim hukukçular ile bilgisayar bilimcilerin ortak çözmesi gerektiği düşünülen kişisel verilerin korunması gibi problemler AYZ ile mümkün olabilmektedir. Yapay zekâ teknikleri, sosyal bilimler ve insan-bilgisayar ara yüzü bir arada kesişerek AYZ’nın temelini oluşturabilir. Daha önceden konu geçen disiplinlerarası yöntemi bu noktada kendini göstermektedir. Örneğin, Şekil 8’de AYZ’nın kapsamı yer almaktadır.

⁴⁸³ David Gunning, “Explainable Artificial Intelligence Research at DARPA”, (Çevrimiçi) https://sites.nationalacademies.org/cs/groups/pgasite/documents/webpage/pga_184754.pdf, (Erişim Tarihi:05.12.2020), s. 19.



Şekil 8: Açıklanabilir Yapay Zekânın Kapsamı⁴⁸⁴

3.6.7. Düzenleyici Sanal Alanlar

Yapay zekâ sistemlerinin artan kullanımı, teknoloji uzmanlarını kişisel veri/mahremiyeti koruma konusunda mühendislik alanında çözümler bulmaya zorluyor. GDPR ve benzeri düzenlemeler kişisel verilerin korunmasına ilişkin yasal güvenceler sağlamayı amaçlarken, artan sayıda teknolojik alan, araç, uygulamalar kişisel verilere ihtiyaç duymaktadır. Mahremiyeti garanti altına almaya, kişisel verileri korumaya yönelik yasa ve düzenlemeler çok kapsamlı olmasına rağmen, ilgili veri koruma düzenlemelerine uyum sağlamak veri ihlal risklerinin her zamankinden daha büyük olan günümüzde yetersiz kalmaktadır.

⁴⁸⁴ Tim Miller, “Explanation in Artificial Intelligence: Insights from the Social Sciences”, **Artificial Intelligence**, C. 267 (2019), ss. 1-38, s. 5.

GDPR Avrupa'daki kuruluşlara bir dizi siber güvenlik ve veri ihlali bildirim yükümlülüğü getirmiş, veri koruma otoritelerine güçlü yaptırım gücü tanımıştır. Bu durum, yapay zekâ teknolojileri alanında çalışma söz konusu olduğu şirketler için korkutucu bir düzenleme olmuştur⁴⁸⁵. Sonuçta kişisel verilerin korunması konusunda halihazırda var olan mühendislik çözümlerinin ötesinde, başka yeni bir alan olan Güvenli Veri Depolama Platformları ortaya çıkmaya başlamıştır.

Bu platformlar kişisel, endüstriyel ve hatta hibrit veri platformlarının parçası olabilir. Konu odaklı, bağlantılı ve veri koruma yetkilileri tarafından onaylanmış dijital platformlar, bir taraftan gerçek veriler üzerinde eğitilmesi gereken algoritmaları eğitime imkânı sunarken aynı zamanda fikri mülkiyet hakları korumasını garanti altına alır ve veri tabanlarının doğru olmasını sağlar⁴⁸⁶. Deneyler ve test aşamalarında, bu tür güvenli ortamlar verilere ihtiyaç duyan işletmeleri yasal ilkelere uygun olarak gerekli tüm güvenlik önlemlerine sahip olduklarını kanıtlama sorumluluğundan muaf tutacaktır. Bu tür yaklaşımlarla birleştirildiğinde, vakalardan ve en iyi uygulamalardan öğrenilen dersler, farklı endüstriyel sektörlerdeki kullanım durumlarına göre güncellenebilir.

3.6.8. Veri Koruma Etki Değerlendirmesi (VKED)

Algoritmik karar verme için önceden bir değerlendirme mekanizması oluşturulmalı. Veri ihlali sonrası yardım etme ve kurtarmaya kıyasla ihlali önceden engellemek daha yararlı olabilecektir. Bu noktada GDPR'ın 35. maddesi referans olarak gösterilebilir. Bu madde, algoritmanın denetleyicisinin önceden bir VKED'si yapmasını gerektirmektedir.

Özellikle yapay zekâ teknolojileri kullanarak veri işleme, otomatik işleme ve yasal veya benzerlerine dayalı kişisel değerlendirme veya puanlama içeren veri işlemlerin, büyük ölçekli kişisel hassas veri işlemenin ve sistematik veri izlemenin

⁴⁸⁵ Timan ve Mann, **a.g.m.**, s. 20.

⁴⁸⁶ Lei Yue, **a.g.m.**, s. 19.

önemli etkisi, bireylerin haklarını kullanmalarını, sözleşmelere girmelerini veya hizmet almalarını önleyebilmeleri durumunda, algoritma denetleyicisi kişisel veri koruma davranışını önceden etkilemesini ve bir değerlendirme yapılmasını gerektirmektedir. Önemli bir hesap verebilirlik aracı olarak, “VKED” algoritma denetleyicilerini, tamamen otomatik işleme ve bazı otomatik kararların neden olabileceği riskler de dahil olmak üzere, tüm algoritmik kararları değerlendirmeye yönlendirebilir⁴⁸⁷. VKED’sı teknik açıdan pratik görünmese de veri ihlallerine önlemede, yapay zekâ çağında oluşan ihlal sonraki kurtarmadan kaynaklanan boşluğu doldurma da önemli rol oynamaktadır. GDPR’ın yaptığı VKED düzenlemesi yapay zekâ çağında bütün düzenlemelerin örnek alması gereken örneklerden biridir.

GDPR 35. maddesi VKED’nin ilgili kişilerin hak ve özgürlüklerine yönelik yüksek riskle sonuçlanması muhtemel olan veri işleme faaliyetlerine karşı önleyici niteliğinde olmasını öngörmüştür. Değerlendirme, özellikle veri işleme faaliyetinde, gerçek kişilerle ilgili, profil oluşturma dahil olmak üzere otomatik işlemeye dayanan kararların kapsamlı bir değerlendirmeye tabi tutulması gerektiğini vurgulamıştır. Bu nedenle, yapay zekâ tabanlı profil oluşturma, bireyleri etkileyen otomatik karar almaya katkıda bulunduğu genellikle bir etki değerlendirmesi gerekmektedir. Çünkü bu tür bir profil oluşturma “sistematiik ve kapsamlı” olabilir.

Değerlendirme, bir veri işlemenin “yüksek risk” içerdiğini belirlediğinde, madde 36 (1)’e göre veri sorumlusu, önleyici amaçla veri koruma otoritesinden (ulusal veri koruma otoritesi) tavsiye istemesi gerekmektedir. Veri sorumlusu, madde 35 kapsamındaki bir VKED’nin yüksek bir riskle sonuçlanacağını gösterdiği durumlarda, veri işlemiden önce Veri Koruma Otoritesine danışması gerekmektedir.

Yukarıda bahsi geçen stratejilerin hepsi aslında yapay zekâ çağında kişisel verilerin işlenmesi konusunun sorumluluk ve yönetim şeklini geliştirme amacıyla ortaya konulmuştur. Sadece özel sektörlerde değil, kamu alanlarında dahi

⁴⁸⁷ European Commission, Article 29..., **a.g.e.**, s. 6.

vatandaşların kişisel verilerin işlenmesi, özellikle gözetim şeklinde toplanması mahremiyet açısından düzenlenmesi gereken hususlar arasındadır. Vatandaşlar ve hükümet arasında güç dengesizliğini önleyen uygun yapıların kurulmasını sağlamak için veri mahremiyeti yasasında sorumluluk ve hesap verebilirlik öne çıkmalıdır. Bu, kişisel verilerin uygun şekilde işlenmesini sağlayan düzenlemelere dayanmaktadır.

3.6.9. İstatistiksel İşleme ve Bilimsel Araştırma

Yapay zekâ, büyük verilerle birlikte bilim ve istatistiksel amaçlar için yararlı sonuçlar sağlayabilir (örneğin, tıp teşhisi veya prognozu için; sosyal bilimlerde ekonomik veya politik davranışları anlamak için; iş dünyasında tüketici zevklerini ve eğilimlerini tespit etmek için). Bu amaçların bir genel niteliği vardır (sonuçlar belirli kişilere bağlı değildir) ve bu nedenle, kişisel veri olarak sayılmamaktadır. Bununla birlikte, istatistiksel ve bilimsel amaçlar, ilgili kişilerin verilerini ifşa ederek verilerin güvenlik risklere uğraması ve kötüye kullanılmasına sebep olabilmektedir. Dahası, istatistiksel sonuçlar, bir bireyin ait olduğu gruplarla ilgili muhtemelen yanlış veya yanıltıcı bilgi sunduğundan, bireyleri dolaylı olarak da etkileyebilmektedir.

GDPR, bilimsel ve istatistiksel işlemler için yeniden düzenlemeye izin vermiştir (uygun güvenlik önlemleri altında). Bilimsel ve özellikle istatistiksel işlemlerinde veri işleme izni verilmesi AB çerçevesinde yapay zekâ teknolojilerin geliştirilmesine katkı sağlayabilir. Ancak bu durum ilgili kişilerin haklarının korunması ve rekabet açısından düzenlemeye tabi tutulduğu zaman gerçekleşmelidir⁴⁸⁸.

Yapay zekâ çağında veri koruma düzenlemeleri ile ilgili dikkat edilmesi gereken bazı hususlar şunlardır⁴⁸⁹:

⁴⁸⁸ STOA, The Impact of the..., **a.g.e.**, s. 76

⁴⁸⁹ IAF, Artificial Intelligence, Ethics and Enhanced Data Stewardship, 2017, s. 15.

- Yapay zekâ teknolojisi, tek bir ülke veya yargı alanı ile sınırlı kalmamaktadır. Bu özellik etkili veri koruma uygulamaları ve sınırların ötesinde düzenleme yetkisi oluşturmayı ve sürdürmeyi zorlaştırır.
- Verilerin kime ait olduğunu, nerede depolandığını ve kimin sorumluluğunda olduğunu belirlemek, kanun koyucular için karmaşık bir görev niteliğindedir.
- İyi yönetim, teknolojinin anlaşılmasına dayanmalıdır. Yapay zekâ hızla gelişmeye devam ettikçe, yapay zekanın karmaşıklığı ve uygulama alanı büyümeye devam ederken, hukuk ve teknoloji arasındaki uzun süredir var olan boşluk genişlemektedir.
- Kanun koyucuların yapay zekâyı ne ölçüde düzenlemesi gerektiği, mahremiyet ile ilgili olarak yapay zekâ için bir düzenleyici çerçevenin bulunmamasının başlı başına bir düzenleyici kararı niteliğinde olduğunu belirtmemiz gerekiyor.

Kişisel veri koruma düzenlemeleri, yalnızca düzenleyicilerin yukarıdan aşağıya denetimi yoluyla elde edilemez. Verileri kontrol edenler ve teknolojiyi geliştirenlerin, veri koruma sistemlerinin tasarımını ayarlamaları gerekmektedir.

Sonuçta yapay zekâ tabanlı işlemleri yapan veri sorumlusu, GDPR'ın düzenlemelerine dikkat etmeli, risk odaklı bir yaklaşım benimsemeli ve bunu mevcut teknolojiler ve ekonomik karlılıkla uyumlu bir şekilde dengelemelidir. Bununla birlikte, konunun karmaşıklığı GDPR gibi kişisel veri koruma düzenlemelerindeki boşluklar, belirsizlikler, sadece veri sorumlusunun görev alanı olarak değerlendirilmemesi gerekmektedir. İlgili kurumların, yapay zekâ uygulamaları konusunda tartışma başlatması ve yüksek seviye standartlar sunması gerekir. Veri koruma otoritelerinin, paylaşılan değerlere ve etkili teknolojilere dayalı uygun yanıtlar geliştirmesi için veri sorumlusu, veri işleyici ve sivil toplum da dahil olmak üzere tüm sorumlularla aktif bir diyalog kurması gerekir. Veri koruma ilkelerinin tutarlı bir şekilde uygulanması, Yapa Zekâ teknolojisini verimli bir şekilde kullanma becerisiyle

birleştirildiğinde, güven oluşturarak ve riskleri önleyerek yapay zekâ uygulamalarının başarısına katkıda bulunabilir⁴⁹⁰.

GDPR’da risk temelli yaklaşım, veri minimizasyonu ilkesi ve tasarım gereği ve varsayılan veri koruma gerekliliği sayesinde, mevcut yasal çerçeve kişisel verilerin algoritmalar aracılığıyla işlenmesiyle ilgili birçok potansiyel riskleri konu edinmektedir. Bu nedenle, yapay zekâ teknolojilerini kişisel veri koruma konusunda yönetmek için tasarlanan herhangi bir düzenleyici rejim, mevcut ve potansiyel olarak çelişen yükümlülüklerin ve yasal belirsizliğin gereksiz bir şekilde tekrarlanmasını önlemek için GDPR’ı örnek alması ve eksiklikleri üzerinden geliştirmesi gerekmektedir.

Buna ek olarak, yapay zekâyâ özgü herhangi bir ek düzenlemenin tasarlandığı veya gerekli görüldüğü durumda, bu alandaki hızlı ilerlemeyi ve olası değişiklikleri öngörmek için geleceğe yönelik Avrupa Komisyonunun önerdiği esnek düzenlemelerin tasarlanması gerekmektedir. Bu önemli hususları ihmal ederek yapılan yasal düzenlemeler, yapay zekinin gelişimi ve ilgili kişinin haklarının korunması açısından faydadan daha fazla zarar verebilecektir.

⁴⁹⁰ a.g.e., s. 81.

SONUÇ

Günümüzde teknoloji üstünlüğü ülkeler arası rekabette üstünlüğün temel unsuru olarak değerlendirilmekte ve yapay zekâ teknolojisi bu rekabette üstünlüğü belirleyici kritik unsurlardan biri haline gelmektedir. Çağımızdaki en dönüştürücü güçlerden biri olan yapay zekâ, refah ve ekonomik büyümeyi gerçekleştirmek için büyük fırsatlar sunmaktadır.

Teknoloji geliştikçe gündelik hayatımıza olan etkisi de eskisine göre çok büyük olmaya başlamıştır. Gündelik hayatımıza kolaylıklar getirmesi ile beraber, eskiden imkânsız olarak düşünülen işler teknik açıdan mümkün hale gelmiştir. Geçmişte DNA analizi yoluyla bir kimsenin kimliği belirlenemezken günümüzde yapay zekâ gibi teknolojiler sayesinde, bir kimsenin sesi ile posta kodunun bir arada işlenmesi sonucunda ilgili kişiler doğru bir şekilde tanımlanabilmektedir.

Bununla birlikte, teknolojik gelişmeden kaynaklanan sorunlar da oldukça fazla göz önüne gelmektedir. Yapay zekânın getirdiği sorunlar için mahremiyet ihlalleri örnek olarak gösterilebilmektedir. Rekabet hukuku ve çalışmanın konusu olan kişisel verilerin korunması düzenlemeleri bu zarar/riskleri önleme amacıyla yapılmıştır. Teknolojiden kaynaklanan sorunların çözülmesi için farklı düzenlemeler ortaya çıkmış olsa da yapay zekânın hızlı ilerlemesi ile eşleşememektedir. Sonuçta sadece yapay zekâ teknolojilerin gelişmesi değil, aynı zamanda güncel, etkili düzenlemelerin ortaya çıkması da önemli hale gelmiştir.

İnsanlık tarihine baktığımızda farklı dönemlerde muhtelif konular ile ilgili kuralların ön plana çıktığı görülmektedir. Tarım döneminde mülkiyet hakları kuralları, sanayi döneminde fikri mülkiyet hakları kuralları ön plana çıkmıştır. Yapay zekâ çağında ise verilerin değerinin artması sebebiyle, kişisel verilerin korunması ve koruma kurallarının önemi daha dikkat çekici bir hale gelmiştir. Bu açıdan yapay zekâ çağında verilerin etkili şekilde korunması özellikle kişisel verilerin yapay zekâ teknolojilerini anlama şartı altında korunmasına yönelik çalışmaların ortaya atılması

önem arz etmektedir. Uluslararası arenada da bununla ilgili farklı düzenleme ve kurallar yapılmaktadır.

Yapay zekâ çağındaki kişisel verilerin korunması konusundaki mukayeseli hukuka baktığımızda, önyargı ve ayrımcı kararlar başta olmak üzere kişisel veri koruma düzenlemelerinin yapay zeka çağında karşılaşılan sorunları ile ilgili henüz etkili yaklaşım formüle edilememiş olması söz konusu olmaktadır. Mevcut düzenlemelerde algoritmaların neden olduğu önyargılı kararlar, kara kutu sorunu ve algoritmaların yol açtığı zararın nasıl belirleneceği sorusunun çözülmemesi bir sorun oluşturmaktadır.

Bu nedenle çalışmamızda mukayeseli hukuk açısından AB, ABD, Çin ve Türkiye arasında kişisel verilerin korunmasına yönelik yaklaşımlar yapay zekâ çerçevesinde incelenmiştir. Konumuz kişisel verilerin korunması konusunda çağımızdaki en katı yasal çerçeve oluşturmaya çalışan AB; ileri teknolojik hizmet sağlama konusunda lider ülke olan ve muhtelif gözetimler için yapay zekâyı kullanmakla eleştirilen ABD; teknoloji konusunda fikri mülkiyet hakları çerçevesinde çok eleştiriye maruz kalan, ancak yapay zekâ teknolojileri ve verilerin toplanması konusunda önde gelen Çin; kendi yasal çerçevesini geliştirmeye çalışan Türkiye arasında karşılaştırma yapılmıştır.

Bu düzenlemeler karşılaştırmalı olarak incelendiğinde, AB ve ABD olmak üzere iki çeşit koruma yönteminin bulunduğu görülmüştür. Kişisel verilerin korunmasının insan hakları ve kişilik hakkı kapsamında değerlendirilmesi ön plana çıkan AB yöntemi ve kişiyi tanımlayan bilgilerin mahremiyet, mülkiyet hakkı kapsamında değerlendirilmesi ön plana çıkan ABD yöntemi incelenmiştir. Buna ek olarak bu iki yöntemi içe geçmiş (hibrit) şekilde uygulamaya çalışan dünyanın ikinci büyük ekonomisi olan Çin incelenmiştir. AB kapsamında yapay zekâ çağına uyum sağlama amacı içeren, günümüzdeki en kapsamlı veri koruma düzenlemesi niteliğinde olan GDPR ve ilgili düzenlemeler ele alınmıştır.

AB bünyesinde yapılan kişisel veri koruma düzenlemeleri ile kıyaslandığında, uygulama alanının genişliği, üye ülkeleri arasında üst seviyede uyum sağlamayı amaçlaması, ilgili kişinin haklarının genişletilmesi, ihlal durumundaki ceza miktarların caydırıcılığı GDPR’ın getirdiği yenilikler arasında yer almaktadır. Yapay zekâ kapsamında ise GDPR’ın unutulma hakkı ve aydınlatılmış rıza mekanizmasını güçlendirilmesi önem taşımaktadır. Bu kapsamda GDPR’ çerçevesinde idari açıdan veri koruma kurulu, varsayılan ayarlarla veri koruma, tasarımla veri koruma yöntemleri benimsenmiştir. GDPR’ın getirdiği bu yenilikler yapay zekâ çağında kişisel verilerin korunması kapsamında yapılacak düzenlemelere örnek teşkil etmektedir.

Fakat her gün ilerleme kaydeden yapay zekâ teknolojileri karşısında GDPR’ın de eksiklikleri ortaya çıkmaya başlamıştır. Başlıca sorunlardan kullanım amacının yapay zekâ çağında yeniden amaçlandırılma sorunu, verilerin toplamasına izin verme sorunu, algoritmaların kara kutu/önyargı sorunu öne çıkmaktadır. Bu sorunların bir yandan teknik açıdan çözülmesi önem taşıırken, öbür taraftan uluslararası üstünlük rekabeti açısından AB’yi dezavantajlı duruma bırakmaktadır. Bunlara rağmen, AB İnsan Odaklı (Human Centric) etik standartların araştırma ve geliştirme çalışmalarına devam etmektedir.

ABD’de sektör bazında yapılan düzenlemeler aracılığıyla daha çok mahremiyet, mülkiyet hakkı kapsamında kişiyi tanımlayan bilgilerin korunması söz konusudur. Yapay zekâ teknikleri alanında ise dünyanın en büyük BT şirketleri desteği ile önde gelmektedir.

Çin teknoloji alanlarında büyük ilerleme kaydetmesi ile birlikte, kendine özgü düzenlemeler ortaya çıkarmıştır. Kişisel verilerin korunması kapsamında da hızlı bir şekilde reform yapılmaktadır. Medeni kanunu ve kişisel bilgilerin korunması kanun taslağı kişisel verilerin korunması sorununu resmi şekilde ortaya koymuş, kişisel verilerin korunması hakkını tanımıştır. Fakat uygulamada AB ve ABD’den çok daha geride olduğu söylenebilir. Türkiye açısından ise KVKK kapsamında GDPR’a benzer

düzenlemelerin yapılabilmesi öngörülmüştür. Nitekim yaklaşım açısından Türkiye, AB yaklaşımına daha çok benzemektedir.

Karşılaştırmalı inceleme sonucu yapay zekâ çağında başta GDPR olmak üzere, farklı uygulamalar örnek alınarak kişisel verilerin daha etkili şekilde korunabilmesi öne sürülmüştür. Unutulma hakkının korunması, gizliliği teşvik eden teknolojilerin geliştirilmesi, tasarımda şeffaflık ilkelerinin öne çıkması, Açıklanabilir Yapay Zekâ tekniklerinin yaygınlaştırılması, Veri Koruma Etki Değerlendirmesi mekanizması önerilmiştir. Nitekim yapay zekâ çağında sadece hukuki açıdan öneri yapmak isabetli olmayabilir, yapay zekânın getirdiği devrim niteliğindeki değişiklik bilişim teknolojileri ile hukuki değerlendirmelerin beraber yapılması gerektiğini göstermektedir.

Her şeyden önce, yapay zekâ çağında kişisel veriler kavramının çerçevesi çağımıza uygun şekilde çizilmesi gerekmektedir. Hassas kişisel veri yasal çerçevesi, özellikle çıkarımlar ile olan ilişkileri etkili şekilde yeniden düzenlenmesi gerekmektedir. Böyle olmadığı müddetçe mevcut kişisel veri koruma düzenlemeleri yapay zekâ çağında hassas verileri koruma konusunda etkisiz kalabilecektir.

Günümüzde algoritmik çıkarımların niteliği konusunda tartışma yaşanmaktadır. Nitekim yapay zekâ teknolojileri verileri direk kullanmaktan ötürü, verileri ileride farklı amaçlarla tekrar kullanabilme, çıkarımlardan çıkarımlar yapabilme ile risk oluşturmaktadır. Bu durumda kişileri tanımlayan ya da tanımlayabilen çıkarımlar kişisel veri niteliğinde değerlendirilmesi konusunda görüş birliği oluşturulması, öncelikle kişisel veri kavramının yapay zekâ çağına uygun şekilde yorumlanması gerekmektedir. ABAD kararları bu tür çıkarımları kişisel veri niteliğinde değerlendirilmesi konusunda tartışmalı yorumlara sahip olduğu için, çıkarımları düzeltme hakkı güçlendirilmesi gereken haklar arasında değerlendirilebilir. Özellikle kişisel verilerden türetilen çıkarımlarla ilgili itiraz ve silme hakkı yapay zekâ çağında yeniden değerlendirilmesi gerekmektedir.

Şunu eklememiz gerekiyor ki, toplumsal bazında yapılan çıkarımlar toplumun sağlık, teknoloji, üretim gibi alanlarda faydalı olabilmekte ve muhtemel oluşacak riskler birey bazında yapılan çıkarımlara göre azalabilmektedir. Bireyler için ortaya konulan çıkarımlar, bireylerin en temel haklarını ihlal edebilmektedir. İşe girme, sigorta yaptıрма, bankadan kredi alma konularında eski verilere dayanarak (Yapay zekâ teknolojilerinde eski veri yoktur, bütün veriler değerlidir.) türetilen çıkarımlar ve bu çıkarımlardan dolayı ortaya çıkan karar vermeler bireyler açısından büyük risk oluşturabilmektedir.

Diğer yandan kişisel verileri öğrenme, düzeltme, silme, karar verme ve itiraz etme hakkının temel bir hak olarak tanımlanması ve özel düzenlemeler ile koruma altına alınması önem arz etmektedir. Yapay zekâ teknolojileri tarafından toplanabilen ve işlenebilen kişisel verilerinin kapsamının tartışılması, açık bir şekilde tanımlanması ve gereken “kırmızı çizgiler”in çizilmesi büyük fayda sağlayacaktır.

Yapay zekâ çağında, verilerin sorumlu ve normatif olarak kabul edilebilir kullanımını, etik veri paylaşım uygulamalarını ve zarar durumunda uygun yasal çözümleri düzenleyen bir “makul çıkarım hakkı” gerektirmektedir. Yapay zekâ çağında kişisel verilerin korunması konusunda gizliliği teşvik eden teknolojiler önemini göstermektedir. Varsayılan Ayarlarla Veri Koruma ve/veya Tasarımla Veri Koruma yöntemleri, veri odaklı stratejiler ve süreç odaklı stratejiler bir araya getirilerek daha verimli, pratik olan uygulamaların ortaya çıkarılması beklenmektedir. VKED mekanizması veri ihlali sonrası yardım etme ve kurtarmaya kıyasla ihlali önceden engellemek daha yararlı olabilecektir. GDPR’ın yaptığı VKED düzenlemesi yapay zekâ çağında bütün düzenlemelerin örnek alması gereken örneklerden biridir. Yapay zekâyâ özgü herhangi bir ek düzenlemenin tasarlandığı veya gerekli görüldüğü durumda, bu alandaki hızlı ilerlemeyi ve olası değişiklikleri öngörmek için geleceğe yönelik esnek bir düzenlemelerin tasarlanması gerekmektedir. Bu önemli hususlar ihmal edilerek yapay zekâ çağında oluşturulan herhangi bir yasal düzenleme, yapay zekânin gelişimi açısından faydadan daha fazla zarar verebilir. Bununla beraber kişisel veri koruma düzenlemeleri anonimleştirilmiş veri sorununa etkili şekilde çözüm

araması gerekmektedir. İstatistiksel sonuçlar, bir bireyin ait olduğu gruplarla ilgili muhtemelen yanlış veya yanıltıcı bilgi sunduğundan, bireyleri dolaylı olarak da etkileyebilir.

İnsan olarak her an değişime uğramaktayız, ama makine öğrenimi başta olmak üzere yapay zekâ teknolojileri klasik nedensel çıkarımlar yerine korelasyon çıkarımlar yaptığı için, elde edilebilen bütün verileri değerlendirmektedir. Değişime uğramayan ve büyük verileri saklayan, işleyen ve değerlendiren yapay zekâ teknolojileri ayrımcılık/önyargı konusunda büyük risk oluşturabilir. Kişisel verilerin korunması sadece verilerin korunması olmamalı, asıl amaca dönerek mahremiyetin, özel hayatın gizliliğin, yalnız kalma hakkının, daha doğrusu temel kişilik haklarının korunması gerekmektedir. Kişisel verilerin korunması bu asıl amaç için hizmet etmesi gerekmektedir.

Yapay zekâ çağında kişisel verileri koruma yasal çerçevelerinin oluşturulmasında iki yaklaşım bulunmaktadır. Birincisi yapay zekâyâ odaklanan ayrıntılı yasal düzenlemeleri çıkarmaktır. İkincisi temel ilkeleri belirleyen ve uygulayan esnek hukuk rejimi benimsemektir. Tahmin edilemeyen yapay zekâ gelişimlerini yönetmeyi amaçlayan ayrıntılı düzenlemeler günümüz de artık uygulanamayabilir. Yapay zekâ gibi sürekli değişme, ilerleme halinde olan teknolojik gelişmelerin hukuken doğru bir şekilde nitelendirilebilmesi için AB komisyonunun “Yeni Nesil Teknoloji ve Yapay Zekanın Hukuki Olarak Düzenlenmesine İlişkin Raporu”⁴⁹¹ nda önerilen esnek hukuk mekanizmalarına başvurulması gerekmektedir. Bağlayıcı olmamakla beraber daha hızlı güncellenebilecek özellikte ve belirli bir aşamada mevzuata dönüşebilecek hükümler, yapay zekânın takibi konusunda daha etkin sonuç verebilecektir.

⁴⁹¹ Bu rapor hakkında ayrıntılı bilgi için bkz. Bölüm 3, 6 “Yapay Zekâ Çağında Kişisel Veri Korunmasına Yönelik İzlenebilecek Stratejiler”.

Bu anlamda “regölasyon bağı” gibi kuramların deęerlendirilmesi de önem arz etmektedir. Teknoloji ile hukukun yapay olan bağı aracılığıyla eşzaman olarak güncellenmesi tekniğı deęerlendirilmelidir.

Bununla beraber gizliliğı koruyan teknolojilerle ilgili standartların geliştirilmesi ve uygulanmasını artırmaya yönelik çalışmaların desteklemesi önem taşımaktadır.

Yapay zekâ çağında kişisel verilerin korunması sorunu sadece bilişim uzmanların görevi olmamalıdır. Üniversitelerin hukuk müfredatının yapay zekâ gibi teknolojileri temel bir konu olarak ele alması gerekmektedir. Nitekim yakın zamanda teknoloji hayatımızın bir parçası iken günümüzün vazgeçilmez bir parçası haline gelmiştir. Bu çeşit deęişme hukuki düzenlemelerin hayatın her alanında teknoloji ile temas etmesi anlamına gelmektedir. Bu konular ise bilişim alanında bilgiye sahip hukuk uzmanları tarafından yapılabilen bir hizmet niteliğindedir. Bu kapsamda, yapay zeka çağında bilişim alanına hâkim olan hukuk uzmanları ile hukuk bilimini bir dereceye kadar kavrayabilen bilişim uzmanların beraber hareket etmesi önemlidir.

Uluslararası kuruluşun oluşturulması bir başka çözüm olarak ortaya konulabilir. Günümüzde internet regölasyonu alanında İnternet Tahsisli Sayılar ve İsimler Kurumu kuruluşu (ICANN) aktif bir rol oynadığı gibi, yapay zekâ çağında kişisel verilerin korunmasını düzenleyen bir kuruluşun oluşturulması ideal bir seçenektir. Yapay zekâlı sistemler alanında uluslararası kuruluşun oluşturulması, bu yapılanmanın belli bir firma ya da ülkenin güdümünde olmaması açısından önem arz etmektedir.

Özetle, yapay zekâ çağında kişisel verilerin etkili şekilde korunabilmesi için daha çok insan odaklı uygulamalar ortaya çıkmalı. Sadece veriler aracılığıyla kapitalizme hizmet eden yazılımlar deęil, aynı zamanda insanı düşünen, insanlık tarihinden, sosyolojisinden, psikolojisinden ve sanatından anlayan yapay zekâ uygulamalarının ortaya çıkması gerekmektedir. Öyle olmadığı müddetçe, yapay zekâ uygulamaları insanı derinden anlamayan kod yazıcı mühendisler tarafından

yaratılacak ve kişisel verilerin işlenmesi sadece ekonomik çıkar için hizmet eden araç olarak nitelendirilecektir.

Aslında yapay zekâ teknolojilerin gündelik hayatımızda vazgeçilemez hale gelmesi endişe vericidir. Bir yandan kişisel veriler sadece “yapabildiği için yapmaya çalışan” teknolojinin test ürünü hükmündeyken, öbür taraftan bütün insanlık olarak da yüzeyselliğe maruz bırakılmaktadır. Verilerin meta haline geldiği, daha doğrusu meta haline getirildiği yapay zekâ çağında, aslında daha bilinçli şekilde kendi zekamıza hâkim olmamız gerekmektedir.

Kolay yol her zaman tercih edilecek bir seçenek olmayabilir. Ama gerçekleşen tercihler arasında kolay yol, bilgisayarlarımız ve Google gibi arama motorlarımız başta olmak üzere, yapay zekâ teknolojileri de dahil bizi kendilerini benimsemeye teşvik ettiği yoldur. Kısacası dünyayı anlama çabamıza aracılık etmeleri için yapay zekâ ve ilerleyen teknolojilere daha fazla güvenmeye başladığımızda, kendi zekamızda buna paralel olarak yapay zekâ düzeyine inecektir.

Çalışma, konusu gereği yapay zekâ çağının kişisel verilerin korunmasına olan etkilerini tahlil etmek maksadıyla karşılaştırmalı örnekler üzerinden, özellikle AB, ABD, Çin ve Türkiye açısından kişisel verileri koruma ile ilgili düzenlemeler çerçevesinde yapay zekâ çağının olası etkilerini tartışmayı amaçlamıştır.

Çalışma, yapay zekâ çağında kişisel verilerin korunması sorusunu incelemeyi amaçlıyor olsa da bu sorunun yanıtına ulaşmak için çeşitli alt soruları da yanıtlamayı görev edinmiştir. Bu noktada ilk olarak yapay zekanın tanımı, tarihsel gelişimi, yapay zekânın teknikleri, yapay zekâ çeşitleri, kullanılan uygulamalar detaylıca incelenerek veri ve/veya kişisel verilerin yapay zekâ teknolojisi için taşıdığı önemine dair yanıtlar aranmış ve sonucunda yapay zekâ tekniklerinin özü olan algoritmaların veri ve/veya kişisel verilere dayanarak eğitildiği, geliştirildiği, ilerleme kaydeden yapay zekâ teknolojilerin daha fazla veri ve/veya kişisel veriye ihtiyaç duyduğu kanıtlanmıştır. Yapay zekâ teknolojilerinin teknik özellikleri kişisel verilerin korunmasını önceki dönemlere göre çok daha önemli kıldığı, özellikle makine öğrenimi ve derin öğrenme

tekniklerin hızlı ilerlemesi verilere olan ihtiyacı arttırdığı, yapay zekâ çağında kişisel verilerin fazlaca işlenmesinin etik sorunları da beraberinde getirdiği, sonuçta kişisel verilerin yeni içerik kazanarak, yapay zekâ teknolojileri sayesinde yeniden önem kazandığı, kişisel verileri koruma ihtiyacının yeniden arttığı ileri sürülmüştür.

Öte yandan çalışmanın odaklandığı ikinci konu da mevcut kişisel verileri koruma düzenlemelerinin kişisel verileri nasıl koruyor sorusu olmuştur. Başta kişisel veriler kavramı, kişisel verilerin korunması sorununun tarihsel gelişimi, günümüzdeki kişisel verileri koruma yöntemleri ve karşılaştırmalı hukuktaki kişisel veri koruma düzenlemeleri, benimsediği ilkeler, getirdiği yenilikler analiz edilerek mevcut düzenlemelerin işleyişi ve karşılaştığı sorunlar ortaya koyulmuştur. GDPR'ın günümüzdeki en kapsamlı veri koruma düzenlemesi olduğunu belirten çalışma, GDPR'ın yapay zekâ çağında karşılaştığı sorunları da birlikte incelemiştir.

Yapay zekâ çağının veri koruma için sunduğu fırsatlar anlatıldıktan sonra mevcut kişisel veri koruma düzenlemelerinin yetersizliği incelenerek yapay zekâ çağında daha etkili veri koruma yöntemlerinin ortaya çıkması gerektiği vurgulanmıştır. Akıllı bağlantı noktalarından oluşan veri işleme yapısı, yüksek veri işleme hızı, veri işleme faaliyetinin gizli ve kapsamlı olması, veri ihlali yöntemlerinin gizli ve çeşitli olması nedeniyle ortaya çıkan kişisel verilerin korunması düzenlemelerinin karşılaştığı sorunlar incelenmiştir. Algoritmik önyargı, kara kutu sorunu, veri asimetrisi sorunu, çıkarımların niteliği sorunu, şeffaflık ve hassas veri sorunu, ihlal faili belirleme ve ihlal delili elde etme sorunu ortaya konulmuştur.

Çalışma, unutulma hakkının korunması, gizliliği teşvik eden teknolojilerin geliştirilmesi, tasarımda şeffaflık ilkelerin öne çıkması, Açıklanabilir Yapay Zekâ tekniklerin yaygınlaştırılması, Veri Koruma Etki Değerlendirme sisteminin örnek alınması gerektiğini önermektedir. Yapay zekâ çağında kişisel verilerin hayati önem taşımasından dolayı, geniş kapsamda yorumlanması gerektiği; sadece teknik açıdan değil, aynı zamanda hukuki ve başka beşerî bilimler açısından disiplinlerarası ele alınması gerektiği; farklı düzenlemelerden esinlenerek daha dinamik kişisel veri

koruma düzenlemelerinin ortaya çıkması gerektiği; kişisel veri koruma ile ekonomik çıkar dengesinin yeniden belirlenmesi gerekliliği savunulmuştur.



EKLER

İLGİLİ TANIMLAR

Algoritma: Bir problemi veya problem sınıfını çözmek için kullanılan açık dizi. Tipik olarak, bazı girdi verilerini alan ve çıktıları geri getiren bir talimatlar veya kurallardan oluşur. Örneğin bir sıralama algoritması, önce listenin en büyük ögesini, daha sonra listenin geri kalanının en büyük ögesini vb., liste boşalana kadar, ayıklayarak bir listeye girebilir ve yinelemeli olarak ilerleyebilir. Bir algoritma, bir programlayıcı tarafından elle kodlanabildiği gibi makine öğreniminde olduğu gibi verilerden otomatik olarak da oluşturulabilir⁴⁹². Çalışmanın konusu olan yapay zekânın temelini algoritmalar oluşturmaktadır.

Büyük veri: *“Bilişim ortamında her an çok fazla sayıda kullanıcının verileri, sanal veya fiziksel cihaz tarafından büyük ölçekte işlenebilir. Bu veriler belirli süreçler bakımından yönetilebilir veya anlamlı olmasalar da bunların veri setleri şeklinde bir araya gelmesi durumunda geleneksel işleme araçlarıyla yönetilemeyecek bir veri bütünü ortaya çıkmaktadır. Bu ölçekteki düzenli ya da düzensiz veri setlerine büyük veri (Big Data) denir. Bu çeşitli ölçek, ebat ve formdaki büyük veriyle ancak yapay zekâ teknolojileri başa çıkabilir”*⁴⁹³.

Bu nedenle yapay zekâ ve büyük veri günümüz teknolojisinde neredeyse bir-birinden ayrılamaz kavramlardır. Yapay zekâ teknolojisi ile büyük veri arasındaki ilişki iki yönlüdür: Makine öğrenimi gibi yapay zekâ teknikleri büyük ölçekli veri gerektirse ve büyük ölçekli öğrenme yapay zekânın kaynağı olsa da, yapay zekâ teknolojisinin de büyük verilerden anlaşılması gerekiyor⁴⁹⁴. Büyük

⁴⁹² STOA, Understanding..., **a.g.e.**, s. 3.

⁴⁹³ CNIL, “Comment Permettre À L’homme De Garder La Main? Les Enjeux Éthiques Des Algorithmes Et De L’intelligence Artificielle”, CNIL, 2017, (Çevrimiçi) https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_garder_la_main_web.pdf, (Erişim Tarihi: 29.06.2020), s. 18.

⁴⁹⁴ Lilian Mitrou, **a.g.m.**, s. 17.

veri kavramı ile sadece veri kümesinin olağanüstü boyutu değil, aynı zamanda veri oluşum hızı ve veri çeşitliliği de vurgulanmaktadır. Büyük veri verilerin işlenmeden önceki halini anlatıyor, yapay zekâ ise işlenen verilerden insan zekâsı gibi gelişmeleri amaçlıyor.

Profilleme/tanımlama (Identification): GDPR’ın tanımına göre profilleme

“Belirli bir şahısla ilgili onun kişisel yönlerini değerlendirmek için kişisel verilerinin kullanılması; özellikle bu kişinin iş yerindeki performansı, ekonomik durumu, sağlık bilgileri, ilgi alanları, güvenilirliği, davranış, konum veya hareketlerinin analiz edilmesi veya tahmin edilmesini içeren her türlü otomatik kişisel veri işleme biçimi anlamına gelir”⁴⁹⁵.

Profilleme, çeşitli kaynaklardan elde edilen bireylerle ilgili verileri kullanarak, kişilerle ilgili tahminlerde bulunmada kullanılmaktadır. Bu bakımdan yaş ve cinsiyet gibi özelliklere göre kişisel bir değerlendirme veya sınıflandırma olarak da görülebilir⁴⁹⁶. Yapay zekâ tarafından ortaya konulan gizlilik sorunlarını tartışırken, esas olarak makine öğrenimi tarafından üretilen algoritmik karar verme konularını dikkate almamız gerekmektedir. GDPR, bu bağlamda şu ana kadar profillemeyi ele alan tek tasarı hükmündedir.

Otomatik Karar Verme (Automatic Decision- Making):

Otomatik karar verme, yapay zekâ ve diğer araçları manuel müdahale olmadan kararlar almak için kullanma yeteneğini ifade eder. Otomatik kararlar her tür veriye dayalı olabilir. Örneğin, ilgili kişi tarafından doğrudan veya dolaylı olarak sağlanan veriler (uygulamalar aracılığıyla toplanan konum verileri gibi), türetilmiş veya elde edilen kişisel veriler gibi önceden oluşturulmuş veri türlerinde dahil olabilir⁴⁹⁷.

⁴⁹⁵ European Commission, Article 29 ..., **a.g.e.**, s. 6.

⁴⁹⁶ Selin Çetin, “Yapay Zekâ, Veri Güvenliği ve GDPR”, (Çevrimiçi), 2018, <https://robotic.legal/yapay-zeka-veri-guvenligi-ve-GDPR/>, (Erişim Tarihi: 29.10.2019), par. 4.

⁴⁹⁷ **a.g.m.**, par. 5.

Siyah Kutu (Black-Box): Yapay zekâ ve makine öğrenimi sistemleri bağlamında, makine öğrenimi özellikle derin öğrenme tekniklerinin karmaşıklığı ve çözülme açısından zorluğu nedeniyle belirli kararların nedenlerini geriye doğru takip etmenin mümkün olmadığı durumları ifade eder⁴⁹⁸. Kara Kutu problemi günümüz yapay zekâ teknolojilerin büyük problemler oluşturmalarına yol açmaktadır.

Dartmouth Konferansı: 1956 yılında düzenlenen yapay zekâ konusundaki en önemli konferanstır. Bu sekiz haftalık konferans, sibernetik, otomata teorisi, sinir ağları, sinyal işleme, mantık teorisi ve bilişsel bilim gibi farklı alanlardan önemli araştırmacıların ilgisini çekmiştir. Yapay zekâ termi ilk olarak bu konferansta kullanılmıştır.

Alan Turing: İlk olarak yapay zekâ felsefesini tanıtan ünlü bir İngiliz mantık ve matematikçi. Dartmouth Konferansı'ndan altı yıl önce Turing, "Makineler düşünebilir mi?" konusunda felsefî bir tartışma yapmış ve makinelerin düşünebileceği fikrini savunmuştur. Bundan önce Turing, 1936'da bilgisayar tasarımının ilkeleri üzerine bir makale yazmıştır. Bu makalenin konusu matematiksel mantığın soyut problemi ile ilgili olup, Alan Turing, problemi çözerken teoride depolanmış programlara sahip genel amaçlı bir bilgisayarı başarıyla tasarlamış ve bugün Turing Makinesi olarak adlandırdığımız makinenin temelini yapmıştır.

Turing Makinesi: Alan Turing, hesaplamaları kare başına yalnızca bir sembol olacak şekilde karelere bölünmüş teorik bir hesap makinesi tasarlamak için bir araç kullanmıştır. Makine yalnızca sınırlı sayıda dahili durum içerir. Çerçeveadaki sembolü okuduğunda mevcut durumuna ve sembolün ne olduğuna göre değişebilen bir makine fonksiyonuna sahiptir⁴⁹⁹.

⁴⁹⁸ European Commission, Ethics of Connected and Automated Vehicles: Recommendations on Road Safety, Privacy, Fairness, Explainability and Responsibility, Brussels, 2020, s. 12.

⁴⁹⁹ Pirim, a.g.m., s. 89.

Turing Testi: Alan Turing, bir bilgisayarın veya başka bir sistemin bir insan ile aynı zekaya sahip olup olmadığını ölçmek için Turing testi adı verilen bir test geliştirmiş. Genel olarak bu test, bir uzmanın makine performansı ile insan davranışını ayırt edip edemeyeceğini ölçer. Turing Testinde eğer uzman bir makine ile insan davranışlarını ayırt edemezse, makine insanlar kadar zihinsel yeteneğe sahip olduğunu kanıtlar.

Bu testte, insanlar ve bilgisayarlar deneyiden gizli tutulur. Deneyi yapan uzman, hangisiyle iletişim kurduğunu bilmeden ikisiyle iletişim kuracaktır. Deneycinin sorduğu sorular ve konunun verdiği cevaplar ekranda yazılı olarak verilir. Amaç, deneycinin hangi deneklerin insan olduğunu ve hangilerinin uygun şekilde sorgulanan bilgisayarlar olduğunu bulmasına izin vermektir. Deneyci eğer söyleyemezse, bilgisayarın Turing testini geçtiğini ve insanlar gibi bilişsel yeteneklere sahip olduğunu varsayacaktır⁵⁰⁰. Turing Testi günümüz de dahi makinelerin zihinsel yeteneğini ölçen test olarak kullanılmaktadır.

Mahremiyet/Gizlilik (Privacy): Bir kuruluştaki hassas veriler belirli teknolojiler ve süreçlerde (veri analizi, eğitim modelleri gibi) hakları olan belirli kişiler tarafından kullanıldığında, veriye duyarlı bilgilerin korunmasına ilişkin süreç ve kuralları ifade eder. Mahremiyet ve veri güvenliği (Security) eşdeğer değildir. Veri güvenliği genellikle hassas bilgilerin, verilere yasal olarak erişildiğinde belirli yollarla ziyaretçiler tarafından “tersine çevrilmesini” önlemeyi amaçlar. Bazı mahremiyet/gizlilikler hukuk düzenlemeleri tarafından korunmaz, korunma altında olan her bilgi mahremiyet/gizlilik olmayabilir (Örneğin, kimlik bilgileri).

PbD (Privacy by Design): Tasarımla Veri Koruma 1990’ların ortalarında geliştirilen ve Dr. Ann Cavoukian tarafından savunulan bütünsel bir kavram olup,

⁵⁰⁰ a.g.m., s. 90.

gizliliđi proaktif olarak BT sistemlerinin, ađa bađlı altyapının, iř uygulamalarının tasarımına ve iřletimine yerleřtirmeye dayalı bir çerçevedir⁵⁰¹.



⁵⁰¹ Ann Cavoukian, “The 7 Foundational Principles”, 2006, (Çevrimiçi) www.ipc.on.ca/images/Resources/gps.pdf, (Eriřim Tarihi: 24.09.2020), s. 1.

KAYNAKÇA

I.Kitap ve Makaleler

AKGÜL, Aydın. “Kişisel Verilerin Korunmasında Yeni Bir Hak: ‘Unutulma Hakkı’ ve Avrupa Birliği Adalet Divanı’nın ‘Google Kararı’”. **Türkiye Barolar Birliği Dergisi**. S. 116 (Ocak-Şubat 2015).

AKGÜL, Aydın. **Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması**. İstanbul: Beta Basım Yayınları. 2016.

AKINCI, Ayşe Nur. **Avrupa Birliği Genel Veri Koruma Tüzüğü’nün Getirdiği Yenilikler ve Türk Hukuku Bakımından Değerlendirilmesi**. Ankara: T.C. Kalkınma Bakanlığı. 2017.

AKKURT, Sinan Sami. “Kişisel Veri Kavramının Hukuki Niteliğine İlişkin Yaklaşımlara Mukayeseli Bir Bakış”. **Kişisel Verileri Koruma Dergisi**. C. 2. S. 1 (2020).

AKSOY, Hüseyin Can. “The Right to Personality and It’s Different Manifestations as the Core of Personal Data”. **Ankara Law Review**. C. 5. S. 2 (Ocak 2008).

AKSOY, Hüseyin Can. **Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması**. Ankara: Çakmak Yayınevi. 2010.

ALAN, Turing. “Computing Machinery and Intelligence”. **Mind**. C. 59 (1950). ss. 433-460.

ALSENOY, Brendan Van ve KOEKKOEK, Marieke. “Internet and Jurisdiction After Google Spain: The Extra-Territorial Reach of The EU’s Right To Be Forgotten”. **Leuven Center for Global Governance Studies**. S. 152 (2015).

ARENDT, Hannah. **The Human Condition**. Chicago: The University of Chicago Press. 1958.

ASİMOV, Isaac. **Ben, Robot**. İstanbul: İthaki Yayınları. 2016.

AŞIKOĞLU, Şehriban İpek. **Avrupa Birliği ve Türk Hukukunda Kişisel Verilerin Korunması ve Büyük Veri**. İstanbul: On İki Levha Yayıncılık. 2018.

ATAK, Songül. “Kişisel Verilerin Korunmasına İlişkin Avrupa Birliği Yönergesinin Temel Özellikleri”. **Bahçeşehir Üniversitesi Hukuk Fakültesi Hukuk Dergisi**. S. 60 (2009). s. 211.

ATALAY, Muhammet ve ÇELİK, Enes. “Büyük Veri Analizinde Yapay Zekâ ve Makine Öğrenmesi Uygulamaları”. **Mehmet Akif Ersoy Üniversitesi Sosyal Bilimler Enstitüsü Dergisi**. C. 9. S. 22 (Aralık 2017).

ATASOY, Kemal. “Kişilik Hakkı Kapsamında Sosyal Medyada Kişisel Verilerin Korunması ve Veri Sahibinin Rızası”. **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi**. C. 22. S. 3. ss. 269- 301.

AZZİ, Adèle. “The Challenges Faced by the Extraterritorial Scope of the General Data Protection Regulation”. **Journal of Intellectual Property**. Information Technology and Electronic Commerce. C. 9. S. 2 (2018).

BAK, Başak. “Medeni Hukuk açısından Yapay Zekânın Hukuki Statüsü ve Yapay Zekâ Kullanımından Doğan Hukuki Sorumluluk”. **Türkiye Adalet Akademisi Dergisi**. S.35 (Temmuz 2018).

BALABAN, M. Erdal ve KARTAL, Elif. **Veri Madenciliği ve Makine Öğrenmesi: Temel Algoritmaları ve R Dili ile Uygulamaları**. İstanbul: Çağlayan Kitabevi. 2015.

BALKİN, Jack M. “The Constitution in The National Surveillance State”. **Minnesota Law Review**. S. 93 (2008). ss. 1-25.

BARR, Avron. **Handbook of Artificial Intelligence**. 1.b. Kaufmann William Inc. 1981.

BAŞALP, Nilgün. **Kişisel Verilerin Korunması ve Saklanması**. Ankara: Yetkin Yayınevi. 2004.

BATES, Richard ve BLACKMORE, Nicholas. “The Privacy Challenges of Big Data and Artificial Intelligence”. **KennedysLaw**. (2017).

BENSGHİR, Türksel Kaya. **Bilgi Teknolojileri ve Örgütsel Değişim**. Ankara: Todaie. 1996.

BERBER, Leyla Keser, ATABEY, Ayça ve MERT, Melis. “E-Gizlilik Tüzük Taslağının Son Versiyonu Üzerine Düşünceler”. **Kişisel Verileri Koruma Dergisi**. C. 1. S. 2 (2019). ss. 66- 75.

BERGKAMP, Lucas. “EU Data Protection Policy. The Privacy Fallacy: Adverse Effects Of Europe’s Data Protection Policy in An Information-Dirven Economy”. **Computer Law and Security Report**. S. 18 (2002).

BOSTROM, Nick. **Superintelligence: Paths, Dangers, Strategies**. Oxford: Oxford University Press. 2014.

CARR, Nicholas. **Yüzeysellik: İnternet Bizi Aptal Mı Yapıyor?**. İstanbul: Ufuk Yayınları. 2012.

CATE, Fred H. **Privacy in the Information Age**. Washington: Brooking Institution Press. 1997.

CHOWDHURY, Gobinda G. “Natural Language Processing”. **Annual Review of Information Science and Technology**. C. 37. S. 1 (Ocak 2005).

CİVELEK, Dilek Yüksel. **Kişisel Verilerin Korunması ve Bir Kurumsal Yapılanma Önerisi** (Uzmanlık Tezi). Ankara: Bilgi Toplumu Dairesi Başkanlığı. 2011.

COPPEL, Philip. **Information Rights**. London: Sweet & Maxwell. 2004.

ÇAKIROĞLU, Törenli. “Hekimin Borçlarından Özel Olarak Sır Saklama Borcu”. **Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi**. Cilt: 12. Sayı: 2. Yıl: 2010.

ÇEKİN, Mesut Serdar. “6698 Sayılı Kişisel Verilerin Korunması Hakkında Kanun’un Big Data (Büyük Veri) ve İrade Serbetisi Açısından Değerlendirilmesi”. **İÜHFİM**. C. LXXIV. S. 2 (2016). ss. 629- 650.

ÇEKİN, Mesut Serdar. **Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kişisel Verilerin Korunması Kanunu**. 1.b. İstanbul: On İki Levha Yayınları. 2018.

ÇELİK, Yeşim. “Özel Hayatın Gizliliğinin Yansıması Olarak Kişisel Verilerin Korunması ve Bu Bağlamda Unutulma Hakkı”. **Türkiye Adalet Akademisi Dergisi**. S. 32 (2017).

ÇETİN, Elmas. **Yapay Zekâ Uygulamaları**. Ankara: Seçkin Yayıncılık. 2011. ss. 387-401.

DAL, Ufuk. “Avrupa Birliği Genel Veri Koruma Tüzüğü’nün Ülke Dışı Uygulama Yetkisi ve Bu Yetkinin Uluslararası Hukukta Meşruiyeti”. **Kişisel Verileri Koruma Dergisi**. C. 1. S. 1 (Mayıs 2019).

DETERMANN, Lothar. **Kişisel Verilerin Korunması Uygulama Kılavuzu**. Çeviren: Hilal Temel. 1.b. İstanbul: Onikilevha. 2020.

DİLEK, Gizem Öztürk. “Yapay Zekânın Etik Gerçekliği”. **Anadolu Üniversitesi Sosyal Bilimler Dergisi**. S. 2 (4). 2019. ss. 47-59.

DORUK, Ece Karadoğan ve ÖNGÖREN, Habibe. “İnsan İlişkilerinde ve İş Yaşamında Duygusal Zekâ”. **İstanbul Üniversitesi İletişim Fakültesi Dergisi**. C.0. S. 22 (2005).

DUFF, Antony, GUTWIRTH, Serge ve CLAES, Erik. **Privacy and the Criminal Law**. Intersentia: Antwerp. 2006.

DUMAN, Berat. “**Anayasa Hukukunda Kişisel Verilerin Korunması**”. (S.Ü Sosyal Bilimler Enstitüsü Kamu Hukuku Ana Bilim Dalı Kamu Hukuku Bilim Dalı Yayınlanmamış Doktora Tezi). Konya. 2020. s. 65.

DÜLGER, Murat Volkan. “İnsan Hakları ve Temel Hak ve Özgürlükler Bağlamında Kişisel Verilerin Korunması”. **İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi**. S. 5 (1). 2018. ss. 71-144.

DÜLGER, Murat Volkan. “Yapay Zekâ Teknolojileri ve Veri Koruma Hukuku”. Academia. 2019. (Çevrimiçi)
https://www.academia.edu/40471926/Yapay_Zekâ_Teknolojileri_ve_Veri_Koruma_Hukuku. (Erişim Tarihi: 02.07.2020). s. 4.

EDWARD, Bloustein. J. “Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser”. **N.Y.U. L. Rev.** S. 962 (1964).

EDWARDS, Lilian. “The Problem with Privacy: A Modest Proposal”. **International Review of Law Computers & Technology**. C. 18 (2004).

ENGELMORE, Robert ve MORGAN, Tony (der). **Blackboard Systems**. Boston: Addison Wesley. 1988.

ERDİNÇ, Göksu Hazar. “Ölçülülük İlkesi ve Açık Rıza Kapsamında Biyometrik Verilerin İşlenmesi”. **Kişisel Verileri Koruma Dergisi**. C. 2. S.1 (Haziran 2020).

EROĞLU, Şahika. “Dijital Yaşamda Mahremiyet (Gizlilik) Kavramı ve Kişisel Veriler: Hacettepe Üniversitesi Bilgi ve Belge Yönetimi Bölümü Öğrencilerinin Mahremiyet ve Kişisel Veri Algılarının Analizi”. **Hacettepe Üniversitesi Edebiyat Fakültesi Dergisi**. S. 1 (2018).

ERSOY, Çağlar. **Robotlar. Yapay Zekâ ve Hukuk**. 3.b. İstanbul: Onikilevha Yayıncılık. 2019.

FARİNA, Cynthia R., SHAPİRO, Sidney A. Ve SUSMAN, Thomas M. **Administrative Law of the EU: Transparency and Data Protection** (Administrative Law of the European Union). American Bar Association. 2009.

FELZMANN, Heike vd. “Towards Transparency by Design for Artificial Intelligence”. **Science and Engineering Ethics**. 2020.

FIRAT, Feyyaz. **İnternet Haberciliğinde Yapay Zekâ Teknolojisi Kullanımı: Robot Gazetecilik**. (Gazi Üniversitesi Sosyal Bilimler Enstitüsü Yayınlanmamış Yüksek Lisans Tezi). Ankara. 2018.

FLORİDİ, Luciano vd. “An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles and Recommendations”. **Minds and Machines**. S. 28 (2018). ss. 689–707.

FOGG, B.J. **Persuasive Technologies: Using Computers to Change What We Think and Do**. Morgan Kaufmann Publishers. 2003.

FORSSBAECK, Jens ve OXELHEIM, Lars. “The Multifaceted Concept of Transparency”. **The Oxford Handbook of Economic and Institutional Transparency**. der. Jens Forssbaeck ve Lars Oxelheim. Oxford: Oxford University Press. 2014. ss. 3-30.

GÜR, Berna Akçalı. “Uluslararası Hukuk ve AB Hukuku Boyutuyla Kişisel Verilerin Yurt Dışına Aktarılması”. **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi**. C.25. S. 2 (Aralık 2019).

GÜR, İkbâl. **Kişisel Verilerin Korunması Hususunda AB ile ABD Arasında Çıkan Uyuşmazlıklar ve Çözüm Yolları**. Ankara: Turhan Kitabevi. 2010.

GÜRSEL, İlke. “Protection of Personal Data in International Law and The General Aspects of The Turkish Data Protection Law”. **DEÜHF Dergisi**. C. 18. S. 1 (2016).

HARMON, Paul. **Expert Systems: Artificial Intelligence in Business**. New Jersey: Wiley. 1985.

HASGÜLER, Mehmet ve ULUDAĞ, Mehmet. **Devletlerarası ve Hükûmetler Dışı Uluslararası Örgütler (Tarihçe– Organlar– Belgeler– Politikalar)** 4.b. İstanbul: Alfa Yayınları. 2010.

HATEMİ, Hüseyin. **Kişiler Hukuku**. İstanbul: On İki Levha. 2018.

HE, Xuxu. “比较法上的个人数据信息自决权 (Karşılaştırmalı Hukukta Kişisel Verilerin Kendi Kaderini Tayin Hakkı)”. **Comparative Law Research**. (2013).

HENKOĞLU, Türkay. “Hassas Bilgi Varlıklarının ve Kişisel Verilerin Hukuksal Düzenlemeler ile Korunması ve Bu Kapsamda Üniversiteler İçin Bilgi Güvenliği Politikasının Geliştirilmesi”. (Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü Bilgi ve Belge Yönetimi Anabilim Dalı Yayınlanmamış Doktora Tezi). Ankara. 2015.

HENKOĞLU, Türkay. **Bilgi Güvenliği ve Kişisel Verilerin Korunması**. Ankara: Yetkin Yayınları. 2015.

HILDEBRANDT, Mireille. “Profiling and the Identity of the European Citizen. In profiling the european citizen”. **Springer Dordrecht**. (2018). ss. 303–343.

HU, Zhiling. “人工智能时代公民个人信息的保护 ——以全国首例利用 AI 实施的特大侵犯公民个人信息案为视角 (Yapay Zekâ Çağında Vatandaşların Kişisel Bilgilerinin Korunması-Ülkenin İlk Yapay Zekâ Kullanımlı Kişisel Bilgi İhlali Hakkında)”. **Journal of Shanghai Police College**. 2019.

Hu, Teng ve Lu, Huafeng. “Study on the Influence of Artificial Intelligence on Legal Profession”. 5th International Conference on Economics, Management, Law and Education. Krasnodar. 11-12 Ekim 2019.

İÇEN, Duygu ve GÜNAY. Süleyman. “Uzman Sistemler ve İstatistik”. **İstatistikçiler Dergisi: İstatistik&Aktüerya**. S. 7 (2014). ss. 37-45. s. 41.

İSHİİ, Kaori. “Comparative Legal Study on Privacy and Personal Data Protection for Robots Equipped with Artificial Intelligence: Looking at Functional and Technological Aspects”. *AI & Soc.* S. 34 (2019). ss. 509 – 533.

JASPER, Margaret C. **Privacy and the Internet: Your Expectations and Rights under the Law**. Oxford: Oxford University Press. 2009.

JİLİ, Bulelani. “Chinese social credit initiatives and african surveillance states”. **Futureid 3: Identification in the Era of Automated Decision Making**. Jesus College. Cambridge University. Cambridge. 2018. s. 23-34.

JİLİ, Bulelani. “Chinese social credit initiatives and african surveillance states”. **Futureid 3: Identification in the Era of Automated Decision Making**. Jesus College. Cambridge University. Cambridge. 2018. ss. 23-34.

JOBİN, Anna, IENCA, Marcello ve VAYENA, Effy. “Artificial Intelligence: The Global Landscape of Ethics Guidelines”. **Nature Machine Intelligence**. S. 1 (2019). ss. 389–399.

JOHNSON, Vincent R. Zhao Xiuwen tercümesi. **美国侵权法 (American Tort Law)**. Pekin: Çin Renmin Üniversitesi Yayınları. 2004.

KACROROWSKA, Alina. **European Union Law**. New York: Routledge Cavendish. Taylor and Francis Group. 2009.

KANMAZ, Fatih. **Özel Hayata Karşı Suçlar**. Ankara: Adalet Yayınevi. 2015.

KAPLAN, Jerry. **Artificial Intelligence: What Everyone Needs to Know**. Oxford University Press. 2016.

KARTAL, Mustafa Tevfik. “Kişisel Verilerin Korunması: Türk Bankacılık Sektörü Üzerine Kavramsal Bir Değerlendirme”. **Uluslararası Ekonomi ve Yenilik Dergisi**. C. 4. S. 1 (2018). ss. 1- 18.

KAYA, Cemil. “Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi”. **İÜHFEM Dergisi**. 2011.

KAYA, Ünal ve OĞUZ, Yüksel. “An Assessment of Energy Production Capacity of Amasra Town Using Artificial Neural Networks”. **Turkish Journal of Electromechanics & Energy**. 2018.

KEMPER, Jakko ve KOLKMAN, Daan. “Transparent to Whom? No Algorithmic Accountability Without a Critical Audience”. **Information. Communication & Society**. C. 22. S. 14 (2019). ss. 2081-2096.

KIRIK, Ali Murat. “Sanal Alemde Dönüşüm: Sosyal Medya Yapay Zekâ Etkileşimi”. **İdeal Hukuk**. S. 16 (Kış 2020). ss. 50-52.

KOCABAŞ, Şakir. “Yapay Zekâ ve Bilim Felsefesi”. **Divan Disiplinlerarası Çalışmalar Dergisi**. C.19. S.16 (Ocak 2014).

KOKOLAKİS, Spyros. “Privacy Attitudes and Privacy Behaviour: a Review of Current Research on the Privacy Paradox Phenomenon”. **Computers & Security**. S. 64 (Ocak 2017).

KORKMAZ, Ali. “İnsan Hakları Bağlamında Özel Hayatın Gizliliği ve Korunması”. **KMÜ Sosyal ve Ekonomik Araştırmalar Dergisi**. S. 16 (Özel Sayı I). ss. 99-103.

KONG, Lingjie. 个人资料隐私的法律保护 (**Kişisel Veri Gizliliğinin Yasal Olarak Korunması**). Wuhan: Wuhan Üniversitesi Yayınları. 2009.

KORKMAZ, İbrahim. **Kişisel Verilerin Ceza Hukuku Kapsamında Korunması**. Ankara: Seçkin Yayıncılık. 2017.

KURT, Levent. **Açıklamalı- İctihatlı Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması**. Ankara: Seçkin. 2005.

KÜZECİ, Elif. **Kişisel Verilerin Korunması**. Ankara: Turhan Kitabevi. 2010.

LEI Yue. “人工智能发展中的法律问题探析 (Yapay Zekanın Gelişiminde Hukuki Sorunların Analizi)”. **Pekin Yayınlar ve Telekomünikasyon Üniversitesi Dergisi** (Sosyal Bilimler Basımı). (2018). ss. 17-24.

Lİ, Weigang. “人工智能时代对个人数据法律保护的挑战 (Yapay Zekâ Çağında Kişisel Verilerin Yasal Olarak Korunmasına Yönelik Zorluklar)”. **法制博览**. (Eylül 2020). ss. 168 – 171.

Lİ, Zhenshan. **人性尊严与人权保障 (İnsan Onuru ve İnsan Haklarının Korunması)**. 元照出版社. 2001.

LIEW, Anthony. “Understanding Data. Information. Knowledge and Their Inter-Relationships”. **Journal of Knowledge Management Practice**. 2007.

LIN, Patrick vd. **Robot Ethics. The Ethical and Social Implications of Robotics**. The MIT Press. 2011.

LLOYD, Ian. **Information Tecnology Law**. 5. b. Oxford: Oxford University Press. 2008. s.42

MCKAY, Cunningham. “Complying with International Data Protection Law”. **University of Cincinnati Law Review**. C. 84. S. 421 (2016).

MEI, Shaozu. “个人信息保护的基础性问题的研究 (Kişisel Bilgilerin Korunmasıyla İlgili Temel Konular Üzerine Araştırma)”. **Academic Journal of Suzhou University (Philosophy and Social- Science)**. 2005.

MILLER, Tim. “Explanation in Artificial Intelligence: Insights from the Social Sciences”. **Artificial Intelligence**. C. 267 (2019). ss. 1-38.

MINSKY, Marvin. “Form and Content in Computer Science”. **Journal of the Association for Computing Machinery**. C. 17. S. 2 (Nisan 1970).

MÎTROU, Lilian. “Data Protection. Artificial Intelligence and Cognitive Services: Is The General Data Protection Regulation (GDPR) ‘Artificial Intelligence-Proof?’”. **SSRN**. 2018.

MÎTTELSTADT, Brent. “From Individusal to Group Privacy in Big Data Analytics”. **Philosophy & Technology**. S. 30 (2017). ss. 475–494.

MULLİGAN, Deirdre K ve KİNG, Jennifer. **Briging the Gap Between Privacy and Design**. 14 U. Pa. J. Const. L. 989 (2012).

NİX, Alexander. “Cambridge Analytica- The Power of Big Data and Psychographics”. **Concordia Annual Summit**. New York. 2016.

NORVİG, Peter ve RUSSELL, Stuart J. **Artificial Intelligence: A Modern Approach**. New Jersey: Prentice Hall. 3.b. 2016.

NOTT, George. “Explainable Artificial Intelligence’: Cracking Open the Black Box of AI”. **Computer World**. (2017).

OHM, Paul. “Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization”. **UCLA Law Review**. (2009). ss. 1701–1777.

OKUR, Nurdan. “Anayasa Hukuku açısından Özel Hayatın Gizliliği ve Korunması”. (Gazi Üniversitesi Sosyal Bilimler Enstitüsü Yayınlanmamış Doktora Tezi). Ankara. 2010.

OTTERLO, Van. “A machine learning view on profiling”. **Privacy. Due Process and The Computational Turn: Philosophers of Law Meet Philosophers of Technology**. London: Routledge. 2013. ss. 41–64.

OĞURLU, Yücel. **Karşılaştırmalı İdare Hukukunda Ölçülülük İlkesi**. 2002. Ankara: Seçkin Yayınları. s. 33.

ÖĞÜT, Âdem. **Bilgi Çağında Yönetim**. Ankara: Nobel Yayın Dağıtım. 2001.

ÖNÇÜ, Ali Servet ve CEVİZLİLER, Erkan. “Avrupa Bütünleşmesi İçin Önemli Bir Adım: ‘Avrupa Konseyi’ ve Türkiye’nin Konseye Üyeliği Meselesi”. **Akademik Bakış**. C. 7. S. 13 (2013).

ÖNDER, Murat ve SAYGILI, Hilal. “Yapay Zekâ ve Kamu Yönetimine Yansımaları”. **Türk İdare Dergisi**. Y.90. S.487 (2018).

ÖZBEK, Veli Özer vd. **Türk Ceza Hukuku Özel Hükümler**. Ankara: Seçkin Yayıncılık. 2015.

ÖZDAŞ, Muhammed Raşit. Ayşe Nur Akıncı ve Ahmet Ziyaeddin Türkkan. “Yapay Zekâ ve Hukuk 4.0: Yapay Zekânın Hukuk Uygulamalarına Etkisi”. **Oyun Değiştiren Yapay Zekâ**. der. Mustafa K. Yılmaz ve Öykü İyigün. İstanbul: Beta Yayıncılık. 2020.

ÖZDEMİR, Hayrunnisa. “Haberleşmenin Gizliliği ve Kişisel Veriler”. **Erzincan Üniversitesi Hukuk Fakültesi Dergisi**. C.13. S. 1-2 (2009). s. 139.

ÖZDEMİR, Hayrunnisa. **Elektronik Haberleşme Alanında kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması**. Ankara: Seçkin Yayınları. 2009.

ÖZTEMEL, Ercan. **Yapay Sinir Ağları**. İstanbul: Papatya Yayıncılık. 2012.

ÖZTÜRK, Kadir ve ŞAHİN, Mustafa Ergin. “Yapay Sinir Ağları ve Yapay Zekâ ‘ya Genel Bir Bakış”. **Takvim-i Vekayi**. (2018).

PEPPET, Scott R. “Regulating the Internet of Things: First Steps Toward Managing Discrimination. Privacy. Security and Consent”. **Texas Law Review**. (2014). ss. 85–176.

PİRİM, Harun. “Yapay Zekâ”. **Journal of Yaşar University**. 2006.

PLATON. Çev. Hamdi Varoğlu. **Minos**. İstanbul: Sosyal Yayınları. 2001.

RENGEL, Alexandra. “Privacy- Invading Technologies and Recommendations for Designing a Better Future for Privacy Rights”. **Intercultural Hum. Rts. L. Rev.** (2013).

ROCHER, Luc, HENDRİCKX, Julien M. ve MONTJOYE, Yves-Alexandre de. “Estimating the Success of Re-Identifications in Incomplete Datasets Using Generative Models”. **Nature Communications**. S. 10 (2019).

RODGER, Saito. **Artificial Intelligence is Going to Super charge Surveillance**. Sanvada. 2018.

RULE, James B ve GREENLEAF, Graham. **Global Privacy Protection**. Edward Elgar Publishing. 2010.

SAMUELSON, Pamela. “ Privacy as Intellectual Property?”. **Stanford Law Review**. Y. 52. S. 1125 (Kasım 2000).

SAY, Cem. **50 Soruda Yapay Zekâ**. İstanbul: 7 Renk Basım Yayım ve Filmcilik. 2018.

SCHÖNBERGER, Viktor Mayer ve CUKİER, Kenneth. **Büyük Veri: Yaşama. Çalışma ve Düşünme Şeklimizi Dönüştürecek Bir Devrim**. İstanbul: Paloma Yayınları. 2013.

SCHÖNBERGER, Viktor Mayer ve PADOVA, Yann. “Regime change? Enabling big data through Europe’s New data protection regulation”. **Columbia Sci Technol Law Review**. C. 17 (2016). ss. 315- 335.

SHİ, Weimin. “大数据时代个人信息保护的现实困境与路径选择 (Büyük Veri Çağında Kişisel Bilgilerin Korunmasında Yol Seçimi)”. **Journal of Intelligence**. (2013). ss. 155-161.

SKİTKA, Linda J., MOSİER, Kathleen L. ve BURDİCK, Mark. “Does Automation Bias Decision-making?”. **International Journal of Human-Computer Studies**. Vol. 55. S. 5 (Kasım 1999). s. 991.

SOLOVE, Daniel. **Marc Rotenberg ve Paul Schwartz. Information Privacy Law**. New York: Apsen Publishers. 2006.

SÖZÜER, Eren. **Unutulma Hakkı: İnsan Hakları Hukuku Perspektifinden Bir İnceleme**. İstanbul: On İki Levha Yayıncılık. ss.7-29.

STEFANO, Rodota. “Data Protection As a Fundamental Right”. Reinventing Data Protection. der. Serge Gutwirth. Yves Poullet ve Paul De Hert. **Springer Science Business Media**. 2009.

STUART, Allyson Haynes. “Google Search Results: Buried If Not Forgotten”. **North Carolina of Law & Technology**. 2014.

SUCU, İpek. “Dijital Evrenin Yeni Dünyası Olarak Yapay Zekâ ve Her Filmi Üzerine Bir Çalışma”. **Yeni Medya Elektronik Dergisi**. Vol. 4. S. 1 (Ocak 2020).

SUNSTEİN, Cass. Infotopia: **How Many Minds Produce Knowledge**. Oxford: Oxford University Press. 2006.

ŞEN, Ersan. **Özel Hayatın Gizliliği ve Korunması-Devlet ve Kitle İletişim Araçları Karşısında**. İstanbul: Kazancı Hukuk Yayınları. 1996.

ŞEN, Zekâî. **Üç Türk-islam Bilim ve Düşünce Adamı**. İstanbul: Su Vakfı Yayınları. 2002.

ŞİMŞEK, Oğuz. **Anayasa Hukukunda Kişisel Verilerin Korunması**. İstanbul: Beta yayınları. 2008.

TAŞTAN, Furkan Güven. **Türk Sözleşme Hukukunda Kişisel Verilerin Korunması**. 1. b. İstanbul: On İki Levha Yayıncılık. 2017.

TAVANİ, Herman T. **Ethics & Technology: Controversies, Questions and Strategies for Ethical Computing**. Wiley. 2015. ss. 117- 119.

TENE, Omer. “Privacy Law’s Midlife Crisis: A Critical Assessment of the Second Wave of Global Privacy Laws”. **Ohio State Law Journal**. C. 74. S. 6 (2013). ss.1217-1262.

TONG Xiao vd. “人工智能发展中的法律问题研究 (Yapay Zekanın Geliştirilmesinde Hukuki Sorunlar Üzerine Araştırma)”. **Government Legal System Research**. S. 10 (2019).

TOPALOĞLU, Mustafa. **Bilişim Hukuku**. Ankara: Karahan Yayınevi. 2005.

TOPCU, Neslihan. “Orwell’ın 1984’ü Çin’de Gerçek Mi Oluyor? -Sosyal Kredi Sisteminin Geçmişi. Bugünü ve Geleceği”. **İnsan ve Sosyal Bilimler Dergisi**. S. 3 (2). ss. 684-695.

TÜBİTAK. **Bilim ve Teknik**. S. 409 (Aralık) 2001.

USLU, Cennet. **Doğal Hukuk ve Doğal Haklar: İnsan Haklarının Felsefi Temelleri**. Ankara: Liberte Yayınları. 2009.

VARIAN, Hal R. “Beyond Big Data”. **Business Economics**. S. 49 (2014). ss. 27–31.

VARKONYI, Gizem Gültekin. “Robots with AI: Privacy Considerations in the Era of Robotics”. **Law 4.0**. Széchenyi István University. Győr. 2018.

WACHTER, Sandra ve MITTELSTADT, Brent. “A Right to Reasonable Inferences: Re-thinking Data Protection Law in the Age of Big Data and AI” (October 5, 2018). **Columbia Business Law Review**, 2019(2), Available at SSRN: <https://ssrn.com/abstract=3248829>.

WACHTER, Sandra. “Data Protection in the Age of Big Data”. **Nature Electronics**. ss. 6-7.

WACHTER, Sandra. “Normative Challenges of Identification in the Internet of Things: Privacy, Profiling, Discrimination and the GDPR”. **Computer Law Security Review**. (2017). ss. 436–449.

WACHTER, Sandra. “The GDPR and the Internet of Things: A Three-Step Transparency Model”. **Law Innovation Technol**. 2018. ss. 266–294.

WANG, Liming. “论个人信息权在人格权法中的地位 (Kişilik Hakları Hukukunda Kişisel Veri Haklarının Durumu Hakkında)”. **Academic Attention**. 2012.

WANG, Liming. “论个人信息权的法律保护 —以个人信息权与隐私权的界分为中心 (Kişisel Bilgi Haklarının Korunması- Kişisel Bilgi Hakları ve Gizlilik Hakları Arasındaki Ayrım)”. **Modern Law Science**. Vol. 35. S. 4 (Temmuz 2013).

WANG, Liming. “人工智能时代对民法学的新挑战 (Yapay Zekâ Çağında Medeni Hukukun Karşılaştığı Yeni Zorluklar)”. **东方法学 (Eastern Law)**. S. 3 (2018).

WARREN, Samuel D ve BRANDEİS, Louis. The Right to Privacy. **Boston: Harvard Law Review**. 1890.

WHITBY, Blay. **Yapay Zekâ- Yeni Başlayanlar İçin**. 1.b. İstanbul: İletişim Yayınları. 2005.

WINN, Jane K. **Consumer Protection in the Age of the ‘Information Economy’**. London: Routledge. 2006.

WRIGHT, David. “The State of The Art in Privacy Impact Assessment”. **Computer Law & Security Review**. C. 28. S. 1 (Şubat 2012). ss. 54-61.

WU, Handong. “人工智能时代的制度安排与法律规制 (Yapay Zekâ Çağında Kurumsal Düzenlemeler ve Yasal Düzenlemeler)”. **Legal Science**. 2017.

WU, Jun. **智能时代: 大数据与智能革命重新定义未来 (Akıllı Çağ: Büyük Veri ve Akıllı Devrim Geleceği Yeniden Tanımlıyor)**, Pekin: CITIC Publishing Grup. 2016.

WU, Weiguang. “从隐私利益的产生和本质来理解中国隐私权制度的特殊性 (Çin’in Mahremiyet Koruma Sisteminin Özelliklerini, Gizlilik Çıkarlarının Kaynağı ve Doğası Hakkında)”. **当代法学 (Contemporary Law Review)**. S. 4 (2017).

YANG, Qingwang ve ZHANG, Lei. “On the Artificial Legal Personality of Artificial Intelligence”. **Journal of Hunan University of Science & Technology**. S. 6 (2018).

YE, Mingyi. “个人信息的侵权法保护 (Kişisel Bilgilerin Korunması)”. **中国法学** (Chinese Journal of Law). S.4 (2018). s. 89.

YENİLMEZ, Kürşat. “**Bulanık Doğrusal Programlama Problemleri İçin Yeni Çözüm Yaklaşımları ve Duyarlılık Analizi**”. (Osmangazi Üniversitesi Fen Bilimleri Enstitüsü Yayınlanmamış Doktora Tezi). Eskişehir. 2001.

YİLİHAMU, Reyina. “各国数据保护的启示及对我国的启示 (Mukayeseli Hukukta Veri Korumanın Özellikleri ve Öneriler)”. **中国市场** (China Market). (2020). ss. 188-189.

YİTMEN, Elif. **Zihin Felsefesi Bağlamında Yapay Zekâ Üzerine Felsefi Bir İrdeleme**. (Maltepe Üniversitesi Sosyal Bilimler Enstitüsü Yayınlanmamış Yüksek Lisans Tezi). İstanbul. 2018.

YÜKSEL, Armağan Ebru Bozkurt vd. **Fütürist Hukuk**. İstanbul: Aristo Yayınevi. 2018.

YÜKSEL, Armağan Ebru Bozkurt. “Robot Hukuku”. **Türkiye Adalet Akademisi Dergisi**. S. 29 (2017).

YÜKSEL, Armağan Ebru Bozkurt. “Yapay Zekânın Buluşlarının Patentlenmesi”. **Uyuşmazlık Mahkemesi Dergisi**. 2018.

YÜKSEL, Armağan Ebru Bozkurt. **Yapay Zekâ. Endüstri 4.0 ve Robot Üreticiler**. 1.b. İstanbul: Aristo Yayınevi. 2019.

YÜKSEL, Mehmet. “Mahremiyet Hakkı ve Sosyo-Tarihsel Gelişimi”. **Ankara Üniversitesi SBF Dergisi**. S. 58-1 (2003).

ZAFER, Hamide. **Özel Hayatın ve Hayatın Gizli Alanının Ceza Hukukuyla Korunması**. 1. B. İstanbul: Beta Basım Yayın. 2010.

ZARSKY, Tal. “Incompatible: The GDPR in the Age of Big Data”. **Seton Hall Law Review**. C. 47. S. 4(2) (2017).

ZHANG, Xianli ve GAO, Qiqi. “人工智能时代公民的数据意识及其意义 (Vatandaşların Veri Farkındalığı ve Yapay Zekâ Çağındaki Önemi)”. **西南民族大学学报**. S. 12 (2017).

ZHANG, Xinbao. “从隐私到个人信息: 利益再衡量的理论与制度安排 (Gizlilikten Kişisel Bilgilere: Faydaların Yeniden Değerlendirilmesine Yönelik Teoriler ve Kurumsal Düzenlemeler)”. **中国法学 (Chinese Journal of Law)**. 2015. ss. 38-59.

ZHENG, Zhifeng. “人工智能时代的隐私保护 (Yapay Zekâ Çağında Gizlilik Koruması)”. **法律科学(西北政法大学学报)**. (2019).

ZHOU, Yuntao ve ZENG, Xianyi. **论宪法人格权与民法人格权:以德国法为中心的考察 (Anayasal Kişilik Hakları ve Medeni Hukuk Kişilik Hakları Üzerine: Alman Hukukuna Merkezli Bir Araştırma)**. Pekin: Çin Renmin Üniversitesi Yayınları. 2010.

ZİMMERMAN ve JOSEPH, Evan. “Machine Minds: Frontiers in Legal Personhood”. **SSRN**. (Nisan 2015). (Çevrimiçi) <https://ssrn.com/abstract=2563965>. (Erişim Tarihi: 02.07.2020).

ZORLUEL, Mustafa. “Yapay Zekâ ve Telif Hakkı”. **TBB Dergisi**. S.142 (2019).
II.Belge, Görüş, Araştırma ve Raporlar

ABAD. C- 201/14. Bara. 01.10.2015.

ABAD. C- 212/13. Rynes. 11.12.2014.

ABAD. C- 291/12. Schwartz. 17.10.2014.

ABAD. C- 342/12. Worten. 30.05.2013.

ABAD. C- 582/14. Breyer. 19.10.2016.

ABAD. C- 70/10. Scarlett. 11.24.2011.

ABAD. C-131/12 Google Spain. 13.05.2014.

ABAD. C-141/12. 2014.

ABAD. C-362/14. Schrems. 13.11.2015.

ABAD. C-372/12. 2014,

ABAD. C-434/16. Nowak, 26.02.2018.

AI HLEG. A Definition of AI: Main Capabilities and Scientific Disciplines. Brussels. 2018.

AI HLEG. Ethics Guidelines for Trustworthy AI. Brussels. 2019. (Çevrimiçi)
<https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai>
(Erişim Tarihi: 26.02.2021)

AİHM Kararı. M.S. v. Sweden (20837/92). Tarih: 27.08.1997. (Çevrimiçi)
http://www.hrcr.org/safrica/privacy/ms_sweden.html. (Erişim Tarihi: 06.02.2018).

AKSU, Halil. Türkiye Yapay Zekâ İnisiyatifi (Çalıştay Raporu). 2017.

Article 29 Data Protection Working Party. “Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC”. (Çevrimiçi) https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf (Erişim Tarihi: 25.02.2021).

Avrupa Konseyi. “108 No’lu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi”.

AYMK. Asli Alp ve Şükrü Alp. Başvuru No. 2014/18260. K.T. 4.10.2017.

BENNETT, Louise. “Reflections on Privacy. Identity and Consent in online Services”. Information Security Technical Report. 2009.

BM Karayolu Trafikine İlişkin Viyana Sözleşmesi.

Council of Europe. “History of Artificial Intelligence” (Çevrimiçi)
<https://www.coe.int/en/web/artificial-intelligence/history-of-ai>. (Erişim Tarihi: 12.11.2018).

Council of Europe. Handbook on European Data Protection Law. European Union Agency for Fundamental Rights. 2014.

Deputy Secretary of Defense. “Establishment of the Joint Artificial Intelligence Center”. 1010 Defence Pentagon. Washington. Haziran 2018.

EDPB. “Article 29 Working Party”. (Çevrimiçi) https://edpb.europa.eu/our-work-tools/article-29-working-party_en (Erişim Tarihi: 26.02.2021).

EPRS. Economic Impacts of Artificial Intelligence. 2019. Brussels.

EPSC. The Age of Artificial Intelligence Towards a European Strategy for Human-centric Machines. EPSC Strategic Notes. 2018.

European Commission. Article 29 Working Party Opinion 4/2007 on the Concept of Personal Data. Brussels. 2007. (Çevrimiçi) <https://www.clinicalstudydatarequest.com/Documents/Privacy-European-guidance.pdf> (Erişim Tarihi: 26.02.2021). s. 6.

European Commission. Ethics of Connected and Automated Vehicles: Recommendations on Road Safety. Privacy. Fairness. Explainability and Responsibility. Brussels. 2020.

European Commission. European Group on Ethics in Science and New Technologies-Statement on Artificial Intelligence. Robotics and Autonomous Systems. 2018. (Çevrimiçi) https://ec.europa.eu/research/egge/pdf/egge_ai_statement_2018.pdf (Erişim Tarihi:26.02.2021).

European Commission. National Strategies on Artificial Intelligence: a European Perspective in 2019. (Çevrimiçi) <https://ec.europa.eu/digitalinglemarket/en/artificial-intelligence> (Erişim Tarihi: 20.01.2021).

European Commission. On Artificial Intelligence- A European Approach to Excellence and Trust. Brussels. 2020.

Genel Mahkeme'nin (Beşinci Daire) 28.05.2012 tarihli Kathleen Egan. Margaret Hackett ve Avrupa Parlamentosu T-190/10 sayılı kararı.

Gola/Schomerus. 4a BDSg. Rn. 25.

Gola/Schomerus. Art. 28 Rn. 24.

House of Commons. Science and Technology Committee. "Robotics And Artificial Intelligence: Fifth Report of Session". 2016. (Çevrimiçi) <https://www.publications.parliament.uk/pa/cm201617/cmselect/cmsctech/145/145.pdf> (Erişim Tarihi: 12.06.2019).

IAF. Artificial Intelligence. Ethics and Enhanced Data Stewardship. 2017.

ICT. "United States Artificial Intelligence Market by Application 2021". Techsciresearch. (Çevrimiçi) <https://www.techsciresearch.com/report/united-states-artificial-intelligence-market-by-application-speech-recognition-image-recognition-etc-by-region-and-by-end-user-consumer-electronics-security-access-control-etc-competition-forecast-opportunities-2011-2021/676.html> (Erişim Tarihi: 24.09.2020).

IEEE. Ethically Aligned Design: A Vision for Prioritizing Human Well-Being with Artificial Intelligence and Autonomous Systems. 2016. (Çevrimiçi) https://standards.ieee.org/content/dam/ieee-standards/standards/web/documents/other/ead_v1.pdf (Erişim Tarihi: 20.01.2021).

Internet Society. "Artificial Intelligence and Machine Learning: Policy Paper". Internet Security. 2017. (Çevrimiçi) https://www.internetsociety.org/wp-content/uploads/2017/08/ISOC-AI-Policy-Paper_2017-04-27_0.pdf. (Erişim Tarihi: 02.07.2020).

İstanbul Barosu. Yapay Zekâ Çağında Hukuk 2020. İstanbul. 2020.

İstanbul, Ankara ve İzmir Baroları Çalıştay Raporu. Yapay Zekâ Çağında Hukuk. Ankara. 2019.

JOHN, McCarthy. “What Is Artificial Intelligence?”. Dartmouth proposal. 1955.

Katheleen Egan case T-190/10

Katz v. United States. 389 U.S. 347 (1967)

KRİTİKOS, Mihalis. Artificial Intelligence Ante Portas: Legal & Ethical Reflections. Brussel: EPRS | European Parliamentary Research Service. 2019.

KVKK. Kişisel Verilerin Korunması Kanunu ve Uygulaması. Ankara. 2017.

KVKK. Veri Sorumlusu ve Veri İşleyen. Ankara. 2019.

OECD. New Data for Understanding the Human Condition: International Perspectives. Paris. 2017.

OECD. Özel Yaşamın Korunması ve Kişisel Verilerin Sınır ötesi Akışına İlişkin Rehber İlkeleri. 1980.

Restatement of Torts. Second. 652C. 652E. 1977. The American Law Institute.

Roe v. Ingraham. 403 F. Supp. 931. S.D.N.Y. 1976.

Roe v. Wade. 410 U.S. 113 (1973)

SAMR, “个人信息安全规范” (Information Security Technology- Personal Information (PI) Security

Simittis. Simitis & 4a BDSG. Rn. 20

Specification), (Çevrimiçi) <https://www.tc260.org.cn/upload/2020-09-18/1600432872689070371.pdf> (Erişim Tarihi: 15.12.2020).

STOA. Understanding Algorithmic Decision-making: Opportunities and Challenges. Brussel. 2019.

STOA. The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence. Brussel. 2020.

TBMM. Kişisel Verilerin Korunması Kanunu Tasarısı (1/541) ve Adalet Komisyonu Raporu. 2017.

The Economist. Artificial Intelligence: Ethics. Frankenstein’s Paperclips. 2016.

The Norwegian Data Protection Authority. Artificial Intelligence and Privacy. Tollbugata. 2018.

U.S. Department of Commerce (P. Jonathon Phillips vd.). Four Principles of Explainable Artificial Intelligence. Washington. 2020.

UN General Assembly. Guidelines for the Regulation of Computerized Personal Data Files 1990.

Whalen v. Roe. 429 U.S. 589. 1977.

White House. “Artificial Intelligence for the American People”. (Çevrimiçi) <https://www.whitehouse.gov/ai/> (Erişim Tarihi: 20.01.2020).

ZHOU, Hanhua. 个人信息保护法-专家建议稿-及立法研究报告(Kişisel Bilgilerin Korunması Kanunu (Uzman Öneri Taslağı) ve Yasal Araştırma Raporu). Pekin: Kanun Yayınları. 2006. s. 79-80.

中国人大网 (Çin Ulusal Halk Kongresi). “中华人民共和国民法典 (Çin Halk Cumhuriyeti Medeni Kanunu)”. (Çevrimiçi) <http://www.npc.gov.cn/npc/c30834/202006/75ba6483b8344591abd07917e1d25cc8.shtml> (Erişim Tarihi: 12.12.2020).

中国人大网 (Çin Ulusal Halk Kongresi). “中华人民共和国民法总则 (Çin Halk Cumhuriyeti Medeni Kanun Genel Hükümleri)”. (Çevrimiçi) http://www.npc.gov.cn/zgrdw/npc/xinwen/2017-03/15/content_2018907.htm (Erişim Tarihi: 12.12.2020).

中央政府门户网 (Çin Merkezi Hükümet Sitesi). “中华人民共和国侵权责任法(Çin Halk Cumhuriyeti Haksız Sorumluluk Kanunu)”. (Çevrimiçi) http://www.gov.cn/flfg/2009-12/26/content_1497435.htm (Erişim Tarihi: 12.12.2020).

中央政府门户网 (Çin Merkezi Hükümet Sitesi). “全国人大常委会关于加强网络信息保护的決定 (İnternet Bilgileri Korunmasının Güçlendirilmesine Dair Karar)”. (Çevrimiçi) http://www.gov.cn/jrzg/2012-12/28/content_2301231.htm (Erişim Tarihi: 12.12.2020).

法律法规数据 (Kanunlar ve Yönetmelikler Veri tabanı). “中华人民共和国网络安全法 (Çin Halk Cumhuriyeti Siber Güvenlik Kanunu)”. (Çevrimiçi) <http://search.chinalaw.gov.cn/law/searchTitleDetail?LawID=394858&Query> (Erişim Tarihi: 12.12.2020).

III. Gazete ve Dergi Haberleri

AI4People. “AI4People's Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations”. (Çevrimiçi) <https://www.eismd.eu/wp-content/uploads/2019/03/AI4People%E2%80%99s-Ethical-Framework-for-a-Good-AI-Society.pdf> (Erişim Tarihi: 26.02.2021).

ALTUNBAŞ, Cansu. “Yapay Sinir Ağları (YSA)”. 13.02.2020. (Çevrimiçi) <https://medium.com/t%C3%BCrkiye/yapay-sinir-a%C4%9Flar%C4%B1-ysa-caec1cc0bf9f> (Erişim Tarihi: 15.11.2020). par. 2.

ANGWIN, Julia. “Machine Bias: Machine Bias Investigating Algorithmic Injustice”. 2016. (Çevrimiçi) <https://www.propublica.org/article/>. (Erişim Tarihi: 20.04.2020).

ATAŞOĞLU, Ahmet. “Bulanık Mantık 3: Bulanık Kurallar ve Çıkarım”. 14.08.2019. (Çevrimiçi) <https://ahmetatasoglu98.medium.com/bulan%C4%B1k-mant%C4%B1k-3-bulan%C4%B1k-kurallar-ve-%C3%A7%C4%B1kar%C4%B1m-8f9d411080c> (Erişim Tarihi: 15.11.2020). par. 5.

BHAGESHPUR, Kiran. “Data Is The New Oil-And That’s A Good Thing”. 15.11.2019. (Çevrimiçi) <https://www.forbes.com/sites/forbestechcouncil/2019/11/15/data-is-the-new-oil-and-thats-a-good-thing/#1d7137447304>. (Erişim Tarihi: 06.2020).

CALO, Ryan. “Robots and Privacy”. **Robot Ethics: The Ethical And Social Implications of Robotics**. der. Patrick Lin. Keith Abney ve George Bekey. Massachusetts: MIT Yayınları. 2012. ss. 187–202. s. 197-198.

CHU, Jennifer. “Artificial Intelligence Model Detects Asymptomatic Covid-19 Infections Through Cellphone-Recorded Coughs”. (Çevrimiçi) <https://news.mit.edu/2020/covid-19-cough-cellphone-detection-1029>. (Erişim Tarihi: 04.11.2020). par. 3.

DUTTON, Tim. “An Overview of National AI Strategies”. (Çevrimiçi) <https://medium.com/politics-ai/an-overview-of-national-ai-strategies-2a70ec6edfd> (Erişim Tarihi: 20.01.2020).

FABİANO, Nicola. “Ethics and the Protection of Personal Data”. **Systemics, Cybernetics and Informatics**. C. 17. S. 2 (2019). ss. 58- 65. s. 63.

GREENBERG, Andy. “An AI That Reads Privacy Policies So That You Don’t Have To”. (09.02.2018). (Çevrimiçi) <https://www.wired.com/story/polisis-ai-reads-privacy-policies-so-you-dont-have-to/>. (Erişim Tarihi: 09.07.2020).

KİRK, Jeremy. “EFF: Browsers Can Leave a Unique Trail on the Web”. (Çevrimiçi) <https://www.pcworld.com/article/188134/article.html>. (Erişim Tarihi: 07.07.2020).

NUREDDİN, Refik. “Optimizasyon Algoritmaları”. 17.06.2019. (Çevrimiçi) <https://medium.com/deep-learning-turkiye/optimizasyon-algoritmalar%C4%B1-ba3774968aa> (Erişim Tarihi: 15.11.2020). par. 14.

USLU, Metin. “Yapay Sinir Ağları (YSA) Nedir?” (Çevrimiçi) <http://kod5.org/yapay-sinir-aglari-ysa-nedir/> (Erişim Tarihi: 15.12.2020). par. 8.

YU, Cheng. “China Ahead of US, EU in AI and Data Privacy, Expert Says”. 2019. (Çevrimiçi)

<http://global.chinadaily.com.cn/a/201903/26/WS5c99b620a3104842260b29b8.html>. (Erişim Tarihi: 10.10.2019).

PİLLAİ, Monisha. “China Now Has AI-Powered Judges: Is AI arbitration the future?”. (Çevrimiçi) <https://radiichina.com/china-now-has-ai-powered-robot-judges/>. (Erişim Tarihi: 08.12.2020).

AKILLIOĞLU, Tekin. “İdari Usul ve Kişisel Verilerin Korunması”. 11.08.2014. (Çevrimiçi) <http://www.idare.gen.tr/akillioğlu-idariusul.htm>. (Erişim Tarihi: 04.10.2019).

ALLEN, Kerry. “China Facial Recognition: Law Professor Sues Wildlife Park”. BBC News. 08.11.2019. (Çevrimiçi) <https://www.bbc.com/news/world-asia-china-50324342> (Erişim Tarihi: 29.10.2020)

ANGWIN, Julia. “Machine Bias: Machine Bias Investigating Algorithmic Injustice”. 2016. (Çevrimiçi) <https://www.propublica.org/article/>. (Erişim Tarihi: 20.04.2020)

ANYOHA, Rockwell. “The History of Artificial Intelligence”. (Çevrimiçi) <http://sitn.hms.harvard.edu/flash/2017/history-artificial-intelligence>. (Erişim Tarihi: 12.10.2019).

ARNOLD, Ben. “Netflix User Anger over ‘racial Targeting’ of Movie Posters”. 22.10.2018. (Çevrimiçi) <https://www.yahoo.com/entertainment/netflix-users-anger-racial-targeting-movie-posters-104325948.html> (Erişim Tarihi: 15.10.2020).

AU, Lavender ve WILHELM, Benjamin. “China’s New Data Protection Law Won’t Rein in State Surveillance”. World Politic View. 28.10.2020. (Çevrimiçi)

<https://www.worldpoliticsreview.com/trend-lines/29174/china-s-new-data-protection-law-won-t-rein-in-state-surveillance> (Erişim Tarihi: 28.10.2020).

BARNEY, Doug “Major GDPR Fine Tracker – An Ongoing. Always-Up-To-Date List of Enforcement Actions”. CoreView. 31.10.2020 (Çevrimiçi) <https://www.coreview.com/blog/alpin-gdpr-fines-list/> (Erişim Tarihi: 04.11.2020).

BBC. “Griezmann Cuts Ties With Huawei Citing Fears Over Treatment of Uighurs”. 10.12.2020. (Çevrimiçi)

<https://www.theguardian.com/football/2020/dec/10/griezmann-cuts-ties-with-huawei-citing-fears-over-treatment-of-uighurs> (Erişim Tarihi: 15.12.2020).

BUTTARELLI, Giovanni. “A Smart Approach: Counteract The Bias in Artificial Intelligence”. 2016. (Çevrimiçi) https://edps.europa.eu/press-publications/press-news/blog/smart-approach-counteract-bias-artificial-intelligence_en (Erişim Tarihi: 12.10.2020)

CARA, “Casetext-Cara Legal & Fact Finder”, (Çevrimiçi) <https://www.welcome.ai/tech/legal/casetext-cara-legal-fact-finder> (Erişim Tarihi: 10.01.2021).

CASTELVECCHI, Davide. “Deep Learning Boosts Google Translate Tool”. 27.09.2016. (Çevrimiçi) <https://www.nature.com/news/deep-learning-boosts-google-translate-tool-1.20696>. (Erişim Tarihi: 10.2019).

CAVOUKIAN, Ann. “Operationalizing Privacy by Design: A Guide to Implementing Strong Privacy Practices”. (Çevrimiçi) <http://www.ontla.on.ca/library/repository/mon/26012/320221.pdf>. (Erişim Tarihi: 12.06.2018)

CAVOUKIAN, Ann. “Privacy by design: the 7 foundational principles”. (Çevrimiçi)
<https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf>.
(Erişim Tarihi: 12.07.2018)

CAVOUKIAN, Ann. “The 7 Foundational Principles”. 2006. (Çevrimiçi)
www.ipc.on.ca/images/Resources/gps.pdf (Erişim Tarihi: 24.09.2020).

CCTV. ““刷脸”时代你的脸安全吗? 嫌疑人 “AI” 换脸骗过人脸识别实施犯罪
(‘Yüzü Tanıma’ çağında, yüzünüz güvende mi?’”. (Çevrimiçi)
<https://tv.cctv.com/2020/10/27/VIDEDsY1h4IX1OGsj4FKDuSz201027.shtml>
(Erişim Tarihi: 28.10.2020)

CNIL. “Comment Permettre À L’homme De Garder La Main? Les Enjeux Éthiques
Des Algorithmes Et De L’intelligence Artificielle”. CNIL. 2017. (Çevrimiçi)
https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_garder_la_main_web.pdf (Erişim Tarihi: 29.06.2020). s. 18.

Comstock. J. “In Small Study. Aicure App Led to 50 Percent Improvement in
Medication Adherence”. (Çevrimiçi) <http://www.mobihealthnews.com/content/small-study-aicure-app-led-50-percent-improvement-medication-adherence>. (Erişim Tarihi: 01.09.2019).

COOK, James. “Amazon Patents New Alexa Feature That Knows When You’re Ill
and Offers You Medicine”. The Telegraph. 09.10.2018. (Çevrimiçi)
<https://www.telegraph.co.uk/technology/2018/10/09/amazon-patents-new-alexa-feature-knows-offers-medicine/> (Erişim Tarihi: 03.10.2020).

COPELAND, B.J. “Artificial intelligence”. (Çevrimiçi)
<https://www.britannica.com/technology/artificial-intelligence>. (Erişim Tarihi: 01.07.2020).

CPDP. “Profiling, Microtargeting and A Right to Reasonable Algorithmic Inferences”. 2019. (Çevrimiçi) https://www.youtube.com/watch?v=nN_sGuNhaOM (Erişim Tarihi: 12.09.2020).

CRAWFORD, Kate. “Artificial intelligence’s white guy problem”. The New York Times. 25.06.2016. (Çevrimiçi) <https://www.nytimes.com/2016/06/26/opinion/sunday/artificial-intelligences-white-guy-problem.html?r=2> (Erişim Tarihi: 12.06.2020).

CUKIER, Kenneth. “Big Data is Better Data”. (Çevrimiçi) https://www.ted.com/talks/kenneth_cukier_big_data_is_better_data. (Erişim Tarihi: 01.07.2020)

ÇETİN, Selin. “Yapay Zekâ. Veri Güvenliği ve GDPR”. (Çevrimiçi). 2018. <https://robotic.legal/yapay-zeka-veri-guvenligi-ve-GDPR/>. (Erişim Tarihi: 29.10.2019).

DİCKE, Ursula ve ROTH, Gerard. “Animal Intelligence and the Evolution of the Human Mind”. 2008. (Çevrimiçi) <https://www.Scientificamerican.Com/Author/Ursula-Dicke>. (Erişim Tarihi: 08.07.2018).

DÖNMEZ, Rasim Özgür. “Yapay Zekâ Uluslararası Siyaseti Nasıl Etkileyebilir?”. Fikir Turu. 2019. (Çevrimiçi) <https://fikirturu.com/2019/12/09/yapay-zeka-uluslararasi-siyaseti-nasil-etkileyebilir/> (Erişim Tarihi: 24.09.2020).

FAGGELLA, Daniel. “What Is Machine Learning?”. 2017. (Çevrimiçi) <https://www.techemergence.com/what-is-machine-learning/>. (Erişim Tarihi: 02.07.2020).

FRANCE, Adrienne La.. “How Self-Driving Cars Will Threaten Privacy”. The Atlantic. (2016).

GUNGOR, Deniz. “Avrupa Birliği’nden Abd’ye Yapılacak Veri Aktarımlarına İlişkin ‘Gizlilik Kalkani’ Anlaşmasının İptali”. Mondaq. 30.10.2020. (Çevrimiçi) <https://www.mondaq.com/turkey/privacy-protection/989728/avrupa-birli287i39nden-abd39ye-yapilacak-veri-aktarimlarina-304li351kin-gizlilik-kalkani-anla351masin-in-304ptali-> (Erişim Tarihi: 20.12.2020).

HEATON, J. B, POLSON, N. G ve WITTE, J. H. “Deep Learning in Finance”. ArXiv:1602.06561. (Ocak 2018). <http://arxiv.org/abs/1602.06561>.

HİNTZE, Arend. “Understanding the Four Types of AI. From Reactive Robots to Self-aware Beings”. 14.11.2016. (Çevrimiçi) <https://theconversation.com/understanding-the-four-types-of-ai-from-reactive-robots-to-self-aware-beings-67616>. (Erişim Tarihi: 03.10.2019).

HOEPMAN, Jaap Henk. “Privacy Design Strategies (The Little Blue Book)”. (Çevrimiçi) <https://www.cs.ru.nl/~jhh/publications/pds-booklet.pdf>. (Erişim Tarihi:15.10.2020).

HORTON, Helena ve COOK, James. “Facebook Accused of Targeting Young LGBT Users with ‘gay Cure’ Adverts”. The Telegraph. 25.08.2018. (Çevrimiçi) <https://www.telegraph.co.uk/news/2018/08/25/facebook-accused-targeting-young-lgbt-users-gay-cure-adverts/> (Erişim Tarihi: 1.10.2020).

HUNT, Elle. “Tay. Microsoft’s Ai Chatbot. Gets a Crash Course in Racism From Twitter”. 2016. (Çevrimiçi) <https://www.theguardian.com/technology/2016/mar/24/tay-microsofts-ai-chatbot-gets-a-crash-course-in-racism-from-twitter>. (Erişim Tarihi: 10.10.2019).

SMİTS, Jan. “Privacy in Europe”. Coursera. (Çevrimiçi)
<https://www.coursera.org/learn/privacy-eu/home/info> (Erişim Tarihi:20.01.2021).

KHARPAL, Arjun. “China is Building a Giant \$2.1 Billion Research Park Dedicated to Developing AI”. 03.06.2018. (Çevrimiçi) <https://www.cnb.com/2018/01/03/china-is-building-a-giant-2-point-1-billion-ai-research-park.html>. (Erişim Tarihi: 02.07.2020).

KIZRAK, Ayyüce. “Açıklanabilir, Sorumlu ve Güvenilir Yapay Zekâ”. (Çevrimiçi) <https://ayyucekizrak.medium.com/a%C3%A7%C4%B1klanabilir-sorumlu-ve-g%C3%BCvenilir-yapay-zeka-bece897c5ea9>. (Erişim Tarihi: 07.12.2020).

255

[ve-uygulamalar%C4%B1na-derinlemesine-bir-bak%C4%B1%C5%9F-d0fecaf7f61b](https://www.docplayer.biz.tr/3313838-Yapay-zeka-arastirma-ve-uygulama-alanlari.html)

(Eriřim Tarihi: 06.12.2020).

KOCABAŐ, Őakir. “Yapay Zekâ Arařtırma ve Uygulama Alanları”. DocPlayer. 2013. (Çevrimiçi) <https://docplayer.biz.tr/3313838-Yapay-zeka-arastirma-ve-uygulama-alanlari.html>. (Eriřim Tarihi: 09.06.2019).

KÜÇÜK, Mustafa. “Yapay Zekâ Nedir? Nereye Gidiyor?”. E-Bursum. 13.02.2019. (Çevrimiçi) <https://blog.e-bursum.com/yapay-zeka/> (Eriřim Tarihi: 06.12.2020).

LİBERATORE, Stacy. “Your AI Lawyer Will See You Now: IBM’s ROSS Becomes World’s First Artificially Intelligent Attorney”. MailOnline. (Çevrimiçi) <https://www.dailymail.co.uk/sciencetech/article-3589795/Your-AI-lawyer-IBM-s-ROSS-world-s-artificially-intelligent-attorney.html> (Eriřim Tarihi: 10.01.2021).

MİTTELSTADT, Brent Daniel. “The Ethics of Algorithms: Mapping the Debate”. Big Data & Society. (Çevrimiçi) <https://journals.sagepub.com/doi/full/10.1177/2053951716679679> (Eriřim Tarihi: 20.01.2021).

Not A Bug Splat. “A Giant Art Installation Targets Predator Drone Operators”. Not A Bug Splat. (Çevrimiçi) <https://notabugsplat.com/> (Eriřim Tarihi:08.12.2020)

OKTAY, Mücahit. “Amazon’dan Yüz Tanıma Teknolojisinin Polis Tarafından Kullanımına Erteleme Kararı”. 2020.06.11. (Çevrimiçi) <https://www.aa.com.tr/tr/dunya/amazondan-yuz-tanima-teknolojisinin-polis-tarafından-kullanımına-erteleme-kararı/1872922> (Eriřim Tarihi:17.11.2020).

ÖĞÜT, Sertaç. “Veri Madenciliği Kavramı ve Geliřim Süreci”. (Çevrimiçi) http://www.sertacogut.com/blog/wp-content/uploads/2009/03/sertac_ogut_-_veri_madenciligi_kavrami_ve_gelisim_sureci.pdf (Eriřim Tarihi: 16.12.2020).

PALMER, Danny. “GDPR: Only One In Three Businesses Are Compliant – Here’s What Is Holding Them Back”. ZDNet. (Çevrimiçi) <https://www.zdnet.com/article/GDPR-only-one-in-three-businesses-are-compliant-heres-what-is-holding-them-back/>. (Erişim Tarihi:04.11.2020).

PARİSER, Eli. “What Facebook and Google Are Hiding From the World- the Filter Bubble”. 2013. (Çevrimiçi) <https://www.youtube.com/watch?v=KraiSrmxql0>. (Erişim Tarihi 05.06.2020)

PROTALINSKI, Emil. “Facebook: Releasing Your Personal Data Reveals Our Trade Secrets”. (Çevrimiçi) <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> (Erişim Tarihi: 04.12.2020).

PUGET ve FRANCOİS, Jean. “What Is Machine Learning?”. (Çevrimiçi) https://www.ibm.com/developerworks/community/blogs/jfp/entry/What_Is_Machine_Learning?lang=en. (Erişim Tarihi: 04.10.2019).

SABAH. “Bulanık Mantık Nedir, Nasıl Uygulanır? Bulanık Mantık Tarihçesi ve Özellikleri ile İlgili Merak Edilenler”. 17.09.2020. (Çevrimiçi) <https://www.sabah.com.tr/yasam/2020/09/17/bulanik-mantik-nedir-nasil-uygulanir-bulanik-mantik-ozellikleri-nelerdir-tk1> (Erişim Tarihi: 15.12.2020).

SCHERER, Michael. “How Obama’s Data Crunchers Helped Him Win”. (Çevrimiçi) <https://edition.cnn.com/2012/11/07/tech/web/obama-campaign-tech-team/index.html>. (Erişim Tarihi: 01.07.2020)

ŞENER, Semih. “Yapay Zekâ. Makine Öğrenimi ve Derin Öğrenme Arasındaki Farklar”. 10.09.2018. (Çevrimiçi) <https://www.endustri40.com/yapay-zeka-makine-ogrenimi-ve-derin-ogrenme-arasindaki-farklar/>. (Erişim Tarihi: 11.2019).

TİMAN, Tjerk ve MANN, Zoltan. “Data Protection in The Era of Big Data for Artificial İntelligence: Trends, Existing Solutions and Recommendations for Privacy-Preserving Technologies”. BDV. 2019. (Çevrimiçi) https://www.bdva.eu/sites/default/files/Data%20protection%20in%20the%20era%20of%20big%20data%20for%20artificial%20intelligence_BDVA_FINAL.pdf (Erişim Tarihi: 15.10.2020).

TİNKER, Ben. “How Facebook ‘Likes’ Predict Race, Religion And Sexual Orientation”. CNN. 04.11.2018. (Çevrimiçi) <https://edition.cnn.com/2018/04/10/health/facebook-likes-psychographics/index.html> (Erişim Tarihi: 17.12.2020).

ULUKAN, Gözde. “Yapay Zekâ Destekli Rezervasyon Uygulaması Google Duplex. İos ve Android Cihazlar İçin Aktif Ediliyor”. 04.04.2019. (Çevrimiçi) <https://webrazzi.com/2019/04/04/yapay-zeka-destekli-rezervasyon-uygulamasi-google-duplex-ios-ve-android/>. (Erişim Tarihi: 03.10.2019).

WALSH, Ray. “Police Use of Secretive Facial Recognition Software Stopped by The Courts”. (Çevrimiçi) <https://www.politics.co.uk/comment-analysis/2020/08/13/police-use-of-secretive-facial-recognition-software-are-topped#:~:text=Government%20ministers%20and%20authorities%20were.out%20prematurely%2C%20if%20not%20illegally.&text=The%20ruling%20affects%20the%20use.has%20been%20brought%20before%20parliament> (Erişim Tarihi: 26.10.2020).

WANG, Lei. “大数据时代. 我们的隐私在’裸奔’? (Büyük veri çağı Mahremiyetimiz ‘çıplak mı?’)”. **Xinmin Wanbao**. 2018.10.07. (Çevrimiçi) <http://xmwb.xinmin.cn/resfile/2018-10-07/A05/A05.pdf> (Erişim Tarihi: 2020.11.17).

WRIGHT, David ve HERT, Paul De. “Introduction to Privacy Impact Assessment”. Springer Link. 2012. (Çevrimiçi) https://ezproxy.ticaret.edu.tr:2056/chapter/10.1007/978-94-007-2543-0_1#citeas (Erişim Tarihi: 28.10.2020). ss. 3-32.

WU, Yangyang. “IBM 宣布退出人脸识别：是道德楷模还是商业投机? (IBM, Yüz Tanımadan Çekildiğini Duyurdu: Etik Bir Model Mi Yoksa Bir İş Spekülasyonu Mu?)”. 19.06.2020. (Çevrimiçi) <https://tech.sina.com.cn/i/2020-06-19/doc-iircuyvi9289158.shtml?cref=cj>. (Erişim Tarihi: 02.07.2020).

XIA, Hongzhen. “个人信息保护法草案首次亮相 (Kişisel Bilgileri Koruma Yasası Taslağı Açıklandı)”. “Çin Halk Kongresi” Dergisi. 15.10.2020 (Çevrimiçi) <http://www.npc.gov.cn/npc/c30834/202010/569490b5b76a49c292e64c416da8c994.shtml> (Erişim Tarihi: 28.10.2020).

YU, Sheng. “人民网二评算法推荐：别被算法困在’信息茧房’ (People’s Daily Online’ın İkinci İnceleme Algoritması Önerisi: ‘Bilgi Kozası Odası’nda Mahsur Kalmayın)”. (Çevrimiçi) <http://opinion.people.com.cn/n1/2017/0919/c1003-29544724.html>. (Erişim Tarihi: 02.04.2020).

YUE, Shenshan. “‘刷脸’技术监管存在真空,须确立安全底线与法律边界 (‘Yüz Tanıma’ Teknik Denetiminde Bir Boşluk Var ve Bir Güvenlik Yasal Sınırlama Oluşturulmalıdır)”. 14.12.2020. (Çevrimiçi) <https://lvdao.sina.com.cn/news/2020-12-14/doc-iiznctke6448293.shtml> (Erişim Tarihi: 15.12.2020).