



AKDENİZ ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ



Elif İlgin ÖZCAN

KİŞİSEL VERİLERİN KORUNMASI HUKUKU BAĞLAMINDA
SAĞLIK BİLİMLERİNDE YAPAY ZEKA KULLANIMI

Sağlık Hukuku Anabilim Dalı
Yüksek Lisans Tezi

Antalya, 2023



AKDENİZ ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ



Elif İlgin ÖZCAN

KİŞİSEL VERİLERİN KORUNMASI HUKUKU BAĞLAMINDA
SAĞLIK BİLİMLERİNDE YAPAY ZEKA KULLANIMI

Danışman

Doç. Dr. Selin SERT SÜTÇÜ

Sağlık Hukuku Anabilim Dalı

Yüksek Lisans Tezi

Antalya, 2023

T.C.
Akdeniz Üniversitesi
Sosyal Bilimler Enstitüsü Müdürlüğüne,

Elif Ilgın ÖZCAN'ın bu çalışması, jürimiz tarafından Sağlık Hukuku Anabilim Dalı Tezli Yüksek Lisans Programı tezi olarak kabul edilmiştir.

Başkan : Doç. Dr. Agah Kürşat KARAUZ (İmza)

Üye (Danışman) : Doç. Dr. Selin SERT SÜTÇÜ (İmza)

Üye : Dr. Öğr. Ü. Olgu ÖZDEMİR ERTÜRK (İmza)

Tez Başlığı:	Kişisel Verilerin Korunması Hukuku Bağlamında Sağlık Bilimlerinde Yapay Zeka Kullanımı
--------------	--

Onay: Yukarıdaki imzaların, adı geçen öğretim üyelerine ait olduğunu onaylarım.

Tez Savunma Tarihi : 12/07/2023

Mezuniyet Tarihi : 14/09/2023

AKADEMİK BEYAN

Yüksek Lisans Tezi olarak sunduğum “Kişisel Verilerin Korunması Hukuku Bağlamında Sağlık Bilimlerinde Yapay Zeka Kullanımı” adlı bu çalışmanın, akademik kural ve etik değerlere uygun bir biçimde tarafımdan yazıldığını, yararlandığım bütün eserlerin kaynakçada gösterildiğini ve çalışma içerisinde bu eserlere atıf yapıldığını belirtir; bunu şerefimle doğrularım.

(İmza)

Elif İlgin ÖZCAN



T.C.
AKDENİZ ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ



07/09/ 2023

TEZ ÇALIŞMASI ORJİNALLİK RAPORU BEYAN BELGESİ

Öğrenci Bilgileri	
Adı-Soyadı	Elif Ilgın ÖZCAN
Öğrenci Numarası	202052089002
Anabilim Dalı	Sağlık Hukuku Anabilim Dalı
Programı	Tezli Yüksek Lisans Programı
Danışman Öğretim Üyesi Bilgileri	
Unvanı, Adı-Soyadı	Doç. Dr. Selin SERT SÜTÇÜ
Yüksek Lisans Tez Başlığı	Kişisel Verilerin Korunması Hukuku Bağlamında Sağlık Bilimlerinde Yapay Zeka Kullanımı
Turnitin Bilgileri	
Ödev Numarası	2159680170
Rapor Tarihi	07/09/2023
Benzerlik Oranı	Alıntılar hariç: %3 Alıntılar dahil: %29
SOSYAL BİLİMLER ENSTİTÜSÜ MÜDÜRLÜĞÜNE, Yukarıda bilgileri bulunan öğrenciye ait tez çalışmasının a) Kapak sayfası, b) Giriş, c) Ana Bölümler ve d) Sonuç kısımlarından oluşan toplam 137 sayfalık kısmına ilişkin olarak Turnitin adlı intihal tespit programından Sosyal Bilimler Enstitüsü Tez Çalışması Orijinallik Raporu Alınması ve Kullanılması Uygulama Esaslarında belirlenen filtrelemeler uygulanarak yukarıdaki detayları verilen ve ekte sunulan rapor alınmıştır. Danışman tarafından uygun olan seçenek işaretlenmelidir: () Benzerlik oranları belirlenen limitleri aşmıyor ise: Yukarıda yer alan beyanın ve ekte sunulan Tez Çalışması Orijinallik Raporunun doğruluğunu onaylarım. () Benzerlik oranları belirlenen limitleri aşıyor, ancak tez/dönem projesi danışmanı intihal yapılmadığı kanısında ise: Yukarıda yer alan beyanın ve ekte sunulan Tez Çalışması Orijinallik Raporunun doğruluğunu onaylar ve Uygulama Esaslarında öngörülen yüzdelik sınırlarının aşılmasına karşın, aşağıda belirtilen gerekçe ile intihal yapılmadığı kanısında olduğumu beyan ederim.	
Gerekçe:	
Benzerlik taraması yukarıda verilen ölçütlere uygun olarak tarafımca yapılmıştır. İlgili tezin orijinallik raporunun uygun olduğunu beyan ederim.	
Doç. Dr. Selin SERT SÜTÇÜ	
İmza	

İÇİNDEKİLER

KISALTMALAR LİSTESİ	iv
ÖZET	vi
ABSTRACT	vii
GİRİŞ	1

BİRİNCİ BÖLÜM

YAPAY ZEKA ve KİŞİSEL VERİLERİN KORUNMASI HAKKINDA TEMEL BİLGİLER

1.1. Yapay Zeka Kavramı	4
1.1.1. Yapay Zeka Tanımı ve Özellikleri	4
1.1.2. Yapay Zeka Çeşitleri	7
1.1.2.1. Zayıf ve Güçlü Yapay Zeka	7
1.1.2.2. Dar, Genel ve Süper Yapay Zeka	7
1.1.2.3. Algı Seviyesine Göre Yapay Zeka Sınıflandırması.....	8
1.1.3. Yapay Zeka Öğrenme Türleri	8
1.1.3.1. Makine Öğrenmesi (Machine Learning).....	9
1.1.3.2. Derin Öğrenme (Deep Learning).....	11
1.1.4. Yapay Zekanın Kullanım Alanları	12
1.1.4.1. Yapay Zekanın Genel Kullanımı.....	13
1.1.4.2. Yapay Zekanın Sağlık Bilimlerinde Kullanımı.....	14
1.1.5. Yapay Zekaya İlişkin Hukuki Düzenlemeler.....	19
1.1.5.1. Uluslararası Hukuktaki Düzenlemeler.....	20
1.1.5.2. Ülkemizdeki Hukuki Durum.....	22
1.2. Kişisel Sağlık Verilerinin Korunması Kavramı.....	23
1.2.1. Kişisel Veri Kavramı	23
1.2.1.1. Tanım	23
1.2.1.2. Kapsam.....	25
1.2.1.3. Unsurlar.....	26
1.2.1.3.1. Veri.....	26
1.2.1.3.2. Belirli veya Belirlenebilir Kişi.....	27
1.2.1.3.3. Verinin Gerçek Kişiye İlişkin Olması.....	28
1.2.1.4. Özel Nitelikli Hassas Veri.....	29
1.2.2. Kişisel Sağlık Verisi Kavramı.....	30
1.2.2.1. Tanımı	30
1.2.2.2. Kapsamı	30
1.2.2.3. Korunmasının Önemi.....	31
1.2.3. Kişisel Sağlık Verilerinin Korunmasına İlişkin Hukuki Düzenlemeler	32
1.2.3.1. Uluslararası Hukuki Düzenlemeler.....	32
1.2.3.2. Ulusal Hukuki Düzenlemeler	37

İKİNCİ BÖLÜM

KİŞİSEL SAĞLIK VERİLERİNİN İŞLENMESİ ve YAPAY ZEKA

2.1. Kişisel Sağlık Verilerinin İşlenmesi.....	40
2.1.1. Temel Kavramlar.....	40
2.1.1.1. Kişisel Verilerin İşlenmesi.....	40
2.1.1.2. İlgili Kişi	41
2.1.1.3. Veri Sorumlusu ve Veri İşleyen	42
2.1.1.4. Veri Kayıt Sistemi	43
2.1.1.5. Merkezi Sağlık Veri Sistemi	43
2.1.1.6. Kişisel Sağlık Kaydı Sistemi.....	43
2.1.2. Kişisel Sağlık Verilerinin İşlenmesine Dair Genel İlkeler	44
2.1.2.1. Hukuka ve Dürüstlük Kurallarına Uygun Olma.....	44
2.1.2.2. Doğru ve Gerekliğinde Güncel Olma	45
2.1.2.3. Belirli, Açık ve Meşru Amaçlar için İşlenme	46
2.1.2.4. Amaç ile Bağlantılı, Sınırlı ve Ölçülü Olma	46
2.1.2.5. Kanunda Öngörülen veya Gereken Süre Kadar Muhafaza Edilme.....	47
2.1.3. Kişisel Sağlık Verilerinin İşlenme Şartları	47
2.1.3.1. Genel Olarak.....	47
2.1.3.2. İşlenme Şartları.....	48
2.1.3.2.1. Açık Rızanın Varlığı	49
2.1.3.2.2. Kişisel Verilerin Korunması Kanunu m.6/3 Hükmünde Sayılan İstisna Halleri	51
2.1.3.2.2.1. Kamu Sağlığının Korunması	52
2.1.3.2.2.2. Koruyucu Hekimlik.....	52
2.1.3.2.2.3. Tıbbi Teşhis, Tedavi ve Bakım Hizmetlerinin Yürütülmesi	52
2.1.3.2.2.4. Sağlık Hizmetleri ile Finansmanının Planlanması ve Yönetimi	53
2.1.3.2.3. Kişisel Verilerin Korunması Kurulunca Belirlenen Önlemlerin Alınması	54
2.1.3.3. Kişisel Verilerin Korunması m.28 Hükmü ile Düzenlenen İstisnai Haller	54
2.2. Yapay Zeka ile Kişisel Sağlık Verilerinin İşlenmesi	55
2.2.1. Genel Olarak	55
2.2.2. Yapay Zeka Tarafından Veri Kullanımı	56
2.2.3. Yapay Zekanın Veri Kullanımının Ortaya Çıkardığı Sonuçlar	58
2.2.3.1. Fırsatlar	58
2.2.3.2. Sorunlar.....	59
2.2.3.2.1. Yapay Zekanın Kişisel Sağlık Verilerinin İşlenmesine Dair Temel İlkeler Yönünden Problemler.....	60
2.2.3.2.2. Algoritmada Sapma ve Ayrımcılık Riski	62
2.2.3.2.3. Yapay Zeka Aracılığı ile Yapılan Çıkarımlara İlişkin Sorunlar.....	63
2.2.3.2.4. Sorumluluk	65
2.2.4. Sorunlara İlişkin Kabul Edilebilecek İlke ve Stratejiler.....	65
2.2.4.1. Tasarımda Gizlilik (Privacy by Design) ve Varsayılanlarda Gizlilik (Privacy by Default).....	67
2.2.4.2. Veri Koruma Etki Değerlendirmeleri ve Yapay Zeka Etki Değerlendirmeleri	69
2.2.4.3. Davranış Kuralları ve Sertifikasyonlar	73
2.2.4.4. Vijilans.....	74
2.2.4.5. İnsanın Sürece Katılması ve İnsan Gözetimi	75
2.2.4.6. İstatistiksel İşleme ve Bilimsel Araştırma için Veri Anonimleştirme.....	76

ÜÇÜNCÜ BÖLÜM

KİŞİSEL SAĞLIK VERİLERİNİN KORUNMAMASI DURUMUNDA YAPAY ZEKANIN ÖZEL HUKUK SORUMLULUĞU

3.1. Genel Olarak	79
3.2. Kişisel Sağlık Verilerinin Yapay Zeka İle İşlenmesi Sırasında İhlal Durumunda Sorumluluk	79
3.2.1. Kişisel Verilerin Korunması Yönüyle Sorumluluk	80
3.2.1.1. Başvurulabilecek Hukuki Yollar	80
3.2.1.1.1. Kişisel Verilerin Korunması Kanunu Hükümlerince Sorumluluk	80
3.2.1.1.2. Türk Medeni Kanunu Hükümlerince Sorumluluk	81
3.2.1.1.2.1. Önleme Davası	82
3.2.1.1.2.2. Durdurma Davası	83
3.2.1.1.2.3. Tespit Davası	83
3.2.1.1.3. Türk Borçlar Kanunu Hükümlerince Sorumluluk	84
3.2.1.1.3.1. Haksız Fiil Sorumluluğu	85
3.2.1.1.3.2. Sözleşme İlişkisinden Doğan Sorumluluk	86
3.2.1.1.3.2.1. Kişisel Sağlık Verilerinin İşlendiği Sözleşmeler	87
3.2.1.1.3.3. Sözleşme Benzeri Borç İlişkisinden Doğan Sorumluluk	89
3.2.1.1.3.4. Vekaletsiz İş Görme	91
3.2.1.1.4. Yapay Zekanın Veri İhlali Durumunda Açılacak Dava Tarafları	92
3.2.1.1.4.1. Davacı	92
3.2.1.1.4.2. Davalı	92
3.2.2. Yapay Zeka Sorumluluğu	92
3.2.2.1. Yapay Zekanın Hukuki Niteliği	93
3.2.2.2. Mevcut Düzenlemeler Işığında Yapay Zeka Sorumluluğu	95
3.2.2.2.1. Ürün Sorumluluğu	96
3.2.2.3. Yapay Zekaya Hukuki Nitelik Tanınması Durumunda Sorumluluk	98
3.2.2.4. Mevcut Hukuki Düzenle Sorumluluk Üzerine Genel Değerlendirme	99
3.2.2.5. Yapay Zeka ve Kusursuz Sorumluluk	100
3.2.3. Uygulanacak Hukuk Meselesi	101
3.2.4. Arbuluculuk	103
SONUÇ	105
KAYNAKÇA	110
Ö Z G E Ç M İ Ş	125

KISALTMALAR LİSTESİ

AB	: Avrupa Birliği
ABAD	: Avrupa Birliği Adalet Divanı
AI	: Artificial Intelligence
AİHM	: Avrupa İnsan Hakları Mahkemesi
AİHS	: Avrupa İnsan Hakları Sözleşmesi
AÜHFD	: Ankara Üniversitesi Hukuk Fakültesi Dergisi
AYM	: Anayasa Mahkemesi
B.	: Başvuru
bkz.	: Bakınız
BM	: Birleşmiş Milletler
Bs.	: Bası
C	: Cilt
CD	: Ceza Dairesi
CGK	: Ceza Genel Kurulu
CMAJ	: Canadian Medical Association Journal
Çev.	: Çeviren
D	: Danıştay
DPIA	: Data Protection Impact Assessment
E.	: Esas
Ed.	: Editör(ler)
GDPR	: The EU General Data Protection Regulation (Genel Veri Koruma Tüzüğü)
GK	: Genel Kurul
HD	: Hukuk Dairesi
HGK	: Hukuk Genel Kurulu
HHY	: Hasta Hakları Yönetmeliği
HIPAA	: Health Insurance Portability and Accountability Act
İDDK	: İdari Dava Daireleri Kurulu
İÜHFD	: İstanbul Üniversitesi Hukuk Fakültesi Dergisi
İÜHFM	: İstanbul Üniversitesi Hukuk Fakültesi Mecmuası
JIPITEC	: Journal of Intellectual Property, Information Technology and Electronic Commerce Law

K.	: Karar
KSVHY	: Kişisel Sağlık Verileri Hakkında Yönetmelik
KVK Kurulu	: Kişisel Verileri Koruma Kurulu
KVK Kurumu	: Kişisel Verileri Koruma Kurumu
KVKK	: Kişisel Verilerin Korunması Kanunu
m.	: madde
MÖHUK	: Milletlerarası Özel Hukuk ve Usul Hukuku Hakkında Kanun
No.	: numara
OECD	: Ekonomik Kalkınma ve İşbirliği Örgütü
R.G.	: Resmi Gazete
s.	: sayfa
S.	: Sayı
ss.	: sayfa aralığı
T.	: Tarih
T.C.	: Türkiye Cumhuriyeti
TBB	: Türkiye Barolar Birliği
TBB	: Türkiye Barolar Birliği
TBK	: Türk Borçlar Kanunu
TBMM	: Türkiye Büyük Millet Meclisi
TCK	: Türk Ceza Kanunu
TDK	: Türk Dil Kurumu
TMJ	: Türk Medeni Kanunu
TRAI	: Türkiye Yapay Zeka İnisiyatifi
UN	: United Nations
ÜGTDK	: Ürün Güvenliği ve Teknik Düzenlemeler Kanunu
vd.	: ve devamı
Y	: Yargıtay
YHGK	: Yargıtay Hukuk Genel Kurulu
YZ	: Yapay Zeka

ÖZET

Teknoloji ve dijitalleşme çağında “yapay zeka” ve “kişisel verilerin korunması” kavramları sıkça gündeme gelmektedir. Yapay zekanın kullanıldığı en önemli alanlardan biri sağlıktır. Sağlık bilimlerinde yapay zeka uygulamalarının faaliyette bulunabilmesi için veri hukukunca yüksek koruma öngörülen kişisel sağlık verilerine ihtiyaç duyulmaktadır. Yapay zekanın kişisel sağlık verilerini hukuka aykırı işlemesi ile veri ihlalleri oluşabilmekte, bazı durumlarda hukuka uygun işlemekten söz edilebilse de algoritma sapması kaynaklı zararlar meydana gelebilmektedir.

Tez ile sağlık bilimlerinde yapay zeka ile kişisel sağlık verilerinin işlenmesi halinde ortaya çıkabilecek sorunların belirlenmesi, bu sorunlara karşı başvurulabilecek önlemlerin incelenmesi ve kişisel sağlık verilerinin korunmaması durumunda yapay zekanın özel hukuk sorumluluğunun tespiti amaçlanmaktadır.

Tezimizin birinci bölümünde, yapay zeka ve kişisel verilerin korunmasına dair genel kavramlar ve hukuki düzenlemeler üzerinde durulmaktadır.

Tezimizin ikinci bölümünde, kişisel sağlık verilerinin işlenmesine ilişkin kurallar incelenip yapay zekanın kişisel sağlık verisi işlemesi, sonuçları ve oluşabilecek sorunlara dair önlemler üzerinde durulmaktadır.

Tezimizin üçüncü bölümünde, kişisel sağlık verilerinin yapay zeka ile işlenmesi sonucunda oluşabilecek zararlara karşı başvurulabilecek hukuki yollar ile sorumluluk tespiti üzerinde durulmaktadır.

Anahtar Kelimeler: Yapay Zeka (YZ), Kişisel Sağlık Verileri, Sorumluluk, Veri İşleme, Yapay Zekanın Hukuki Niteliği

ABSTRACT

Use of Artificial Intelligence in Health Sciences in the Context of Personal Data Protection Law

In the age of technology and digitalization, “artificial intelligence” and “protection of personal data” become a current issue. The field of healthcare is one of the most important areas where artificial intelligence is used. In order to operate artificial intelligence applications in the health sciences, personal health data, which is under strict protection by data law, are required. With the illegal processing of personal data by artificial intelligence, data violation occurs; in some cases, although there is a legal processing activity, damages may occur due to algorithm bias.

This thesis aims to determine the problems that may arise in the processing of personal health data by artificial intelligence in health sciences, to examine measures that can be taken against the problems, and to establish the liability of artificial intelligence in case personal health data is not protected.

The first part of the thesis focuses on general concepts and legal regulations on artificial intelligence and personal data.

In the second part, principles of processing personal health data are examined; and the personal health data processing of artificial intelligence, the consequences and measures for potential problems are discussed.

In the third part, the legal remedies and liability determination against the damages occur as a result of processing of personal health data by artificial intelligence are emphasized.

Keywords: Artificial Intelligence (AI), Personal Health Data, Liability, Data Processing, Legal Status

GİRİŞ

Teknoloji çağına girilmesi ile insanlık, izlerken “Nasıl, bir robot mu bunları yapacak hem de her adımında insan talimatı olmadan?!” dediğimiz ve “Bunlar gerçek hayatta olamaz, korkmayın.” diyerek çocukları rahatlatıp yalnızca bilim kurgu filmlerinde kalacağına inandığımız birtakım değişikliklere tanıklık etmeye başlamıştır. Yapay zekanın hayatımızda büyük yer edinmeye başladığını ve gelecekte daha da hayatımızın merkezinde yer edineceğini söylemek yanlış olmayacaktır. Teknoloji ve internet ile birlikte kişinin mülkleri kadar (ve hatta belki daha fazla) değerli hale gelen kişisel verilere bağlılık artmaktadır. Kişisel veri paylaşımı olmaksızın kişinin hayatını idame ettirebilmesi mümkün değildir. Kişisel veriye bağlılık, kişisel verinin korunması ihtiyacını da beraberinde getirmektedir.

Gelişen teknoloji ürünlerinin en önemlilerinden biri de yapay zekadır. Yapay zeka teknolojilerinin fayda sağlayabilmesi için öncelikle veriden yararlanarak makine öğrenmesi ve derin öğrenme gibi yöntemler ile eğitilmesi gerekmektedir. Yapay zekanın sıklıkla kullanıldığı alanlardan biri de sağlık bilimleridir. Hastalığın teşhisinin yapılabilmesi, tedavi sürecinin seçilebilmesi için yapay zeka uygulamalarına başvurulmakta; tedavi sürecinde yapay zekalı robotların yardımı ile ameliyatlara gerçekleştirilebilmekte; yaşlı ve rehabilitasyon hastalarında ilaç takibinin sağlanabilmesi için yardımcı robotlardan yardım alınmaktadır. Bunların gerçekleştirilebilmesi için yapay zeka kişisel sağlık verilerine ihtiyaç duymaktadır. Kişisel sağlık verilerinin ihlali halinde kişinin toplum içerisinde yer bulamaması, iş ilişkisine son verilmesi gibi sonuçlar ortaya çıkabilmektedir. Bu gibi durumlarla karşılaşma kaygısı ile kişinin sağlık hizmeti almaktan kaçınabilme ihtimali doğmakta, bu durum ise hem kişi sağlığı hem de toplum sağlığı için tehlike arz etmektedir. Bu sebeple kişisel sağlık verisinin işlenebilmesi özel korumaya tabi tutulmaktadır.

Tezin amacı; sağlık bilimlerinde yapay zeka ile kişisel sağlık verilerinin işlenmesi halinde ortaya çıkabilecek sorunların belirlenmesi, bu sorunlara karşı başvurulabilecek önlemlerin incelenmesi ve veri ihlali durumunda başvurulabilecek sorumluluk yollarının sunulmasıdır. Tez çalışmamızda, yapay zekanın sağlık bilimlerinde kullanımı üzerinde durulmakta, diğer endüstrilerde yapay zeka kullanımına dair örnekler verilmekle birlikte farklı alanlarda yapay zeka kullanımı hakkında derinlemesine bir inceleme yapılmamaktadır.

Çalışmamızın birinci bölümü; yapay zeka ve kişisel verilerin korunmasına dair genel bilgilendirme sağlayacaktır. Yapay zekanın tanımı, türleri, öğrenme teknikleri ve sağlık bilimleri odaklı olarak kullanım alanları üzerinde durulacaktır; ulusal ve uluslararası düzeyde yapay zekanın nasıl etkiler doğurduğu incelenecektir. Kişisel sağlık verileri, tanımı ve kapsamı

açıklanarak kişisel sağlık verilerinin korunmasına ilişkin ulusal ve uluslararası hukuki düzenlemeler üzerinde durulacaktır.

Çalışmamızın ikinci bölümü; kişisel sağlık verilerinin işlenmesine ilişkin kurallar ve kişisel sağlık verisi ile yapay zeka ilişkisine ait bilgilendirmeleri içerecektir. Bölümde kişisel sağlık verilerinin işlenmesine dair temel kavramlar açıklanacak; kişisel sağlık verilerinin işlenmesine dair genel ilkeler ve işlenme şartları incelenecektir. Bölümün devamında; yapay zeka ile kişisel sağlık verilerinin işlenmesi, yapay zekanın kişisel sağlık verisi kullanımı ve veri kullanımı sonucunda ortaya çıkacak fırsatlar ile olası sorunlar tespit edilecektir. Ortaya çıkabilecek sorunlara ilişkin izlenebilecek strateji ve önlemler ile bölüm sonlandırılacaktır.

Çalışmamızın son bölümünde; kişisel sağlık verilerinin yapay zeka aracılığı ile işlenmesi sonucu ortaya çıkan ihlallerin yarattığı zararlar karşısında başvurulabilecek yollar üzerinde durulacak, başvurulacak yolların hukuki dayanaklarına değinilecek ve yapay zekanın hukuki niteliğinden söz edilerek, yapay zeka kaynaklı ihlallerde sorumluluk tespiti ile bölüm sonlandırılacaktır.

BİRİNCİ BÖLÜM

YAPAY ZEKA ve KİŞİSEL VERİLERİN KORUNMASI HAKKINDA TEMEL BİLGİLER

Yapay zeka, altmış yılı aşkın süredir araştırılan karma hale gelmiş bir disiplin alanıdır. Bilgisayar bilimcisi Alan Turing ve John von Neumann, 1950’lerin başında günümüzde kullanılan bilgisayarların temeli niteliğinde kabul edilebilecek olan, programlanarak çeşitli faaliyetleri gerçekleştirebilen makineyi oluşturmuştur¹. Bunun ardından Turing, “Computing Machinery and Intelligence” isimli makalesinde bu makinelerin insanlar gibi düşünebileceğini ileri sürmüştür². Makalenin ardından “Logic Theorist” isimli ilk yapay zeka programı geliştirilmiştir³. John McCarthy, Darmouth Konferansı’nda bu disiplin alanı için yapay zeka isimlendirmesini yapmıştır⁴. Konferansın ardından bir süre yapılan çalışmalar arttırılmış; fakat 1970’li yıllarda bilgisayarların hiçbir zaman insan akli ile yarışamayacağına dair eleştiriler sebebiyle⁵ yapılan araştırmalara destekler azalmış, bir süre Yapay Zeka Kışı dönemine geçilmiştir⁶. 1997 yılında dünya satranç şampiyonu Kasparov’un Deep Blue isimli uzman sisteme yenilmesinin üzerine yapay zeka kışında birtakım yapay zeka çalışmaları devam etmiştir. 2010 yılı itibarıyla yapay zekaya ilişkin yeni bir süreç başlamıştır. 1970’lerden beri süregelen Endüstri 3.0 ile makinelerin otomatikleştirilmesi⁷, Endüstri 4.0’da ise akılsız makineler ve insan gücünün yanına bir de yapay zeka sistemlerinin katıldığı “akıllı” bir dönem olmaya başlamıştır.

¹Council of Europe, “History of Artificial Intelligence”, (erişim tarihi: 10.6.2023) <https://www.coe.int/en/web/artificial-intelligence/history-of-ai> ; Yılıyaer, Abudureyimu, **Karşılaştırmalı Örnekler Üzerinden Yapay Zekâ ve Kişisel Verilerin Korunması**, İstanbul Ticaret Üniversitesi Dış Ticaret Enstitüsü Uluslararası Ticaret ve AB Hukuku Anabilim Dalı, Yayınlanmamış Doktora Tezi, İstanbul, 2021, s.20.

²Council of Europe, History of Artificial Intelligence.

³ Bostrom, Nick, **Superintelligence: Paths, Dangers, Strategies**, Oxford University Press, Oxford, 2014, s.5.; Yılıyaer, s.20.

⁴McCarthy, John, “What is AI? Basic Questions”, (erişim tarihi: 19.1.2023), <http://jmc.stanford.edu/artificial-intelligence/what-is-ai/index.html>

⁵Bostrom, s.6-7.; Yılıyaer, s.22.

⁶Council of Europe, History of Artificial Intelligence.

⁷Yavuz Tiftikçigil, Burcu/Yavaş, Hilal Kuvvetli, “Yeniliğin Dönüştürücü Gücü ve Endüstri Devrimleri: Türkiye’nin Endüstri 4.0’daki Konumu Üzerine Bir Değerlendirme”, **Farklı Perspektiflerden Endüstri 4.0 Yazıları I**, Ed. Ayşen Altun Ada & Fulya Mısırdalı Yangil, Gazi Kitabevi, Ankara, 2020, s.9.

Yapay zekanın durgun kalmasının ardından bir anda yeniden gündem konusu olmasındaki en önemli sebep, dijitalleşme sürecinin başlamış olmasıdır. Günümüzde, hayatımızda sağlıktan hukuka her alanda dijitalleşme yoluna gidilmektedir. İnternet kullanımının da artması sayesinde yapay zeka tarafından verilere ulaşım kolaylaşmaktadır. Algoritmaların hesaplanmasını hızlandırmak için bilgisayar grafik kart işlemcilerinin yüksek verimliliğinin keşfi⁸ sayesinde, veri işleminin hızı önemli ilerleme kat etmiş; veri topluluklarının dijitalleşme ile büyük veri haline gelmesi ile de bu keşif birleşince yapay zeka çağının ortaya çıkışına ve dolayısıyla hukuki etkilerinin de ortaya çıkmasına yol açmıştır.

1.1. Yapay Zeka Kavramı

İki bin yılı aşkın süredir görme, öğrenme, hatırlama, sebeplendirmenin nasıl gerçekleştiğini araştıran araştırmacılar için zeka kavramı en eski disiplin alanlarından biri olarak kabul ediliyor iken yapay zeka kavramı da en yeni araştırılan disiplin olarak karşımıza çıkmaktadır⁹. Hayatımızın içinde bu kadar yer etmeye başlamış bir alanın hem tanımının hem de niteliklerinin doğru tespit edilebilmesi, türleri ve öğrenme sistemlerinin anlaşılabilmesi; gelecekte yaşanacak sorunların önüne geçmek ve bu sorunları hukuki düzenlemeler ile kontrol altında tutabilmek için gerekmektedir.

1.1.1. Yapay Zeka Tanımı ve Özellikleri

Yapay zeka tanımı yapılmadan önce yapay ve zeka kavramlarının incelenmesi araştırma açısından yarar gösterecektir. Türk Dil Kurumu'na göre yapay; “*doğadaki örneklerine benzetilerek insan eliyle yapılmış veya üretilmiş, yapma, suni, doğal karşıtı*” şeklinde tanımlanmaktadır¹⁰. Oxford Dictionary tanımına göre yapay; doğal olan şeylerin kopyalanarak yapılmış veya üretilmiş hali; gerçek olmayan, insan eliyle yaratılan; doğal olarak gerçekleşmeyendir¹¹.

Türk Dil Kurumu zeka kavramını “*insanın düşünme, akıl yürütme, objektif gerçekleri algılama, yargılama ve sonuç çıkarma yeteneklerinin tamamı, anlayış, dirayet, zeyreklik, feraset*” şeklinde tanımlamaktadır¹². Oxford Dictionary tanımına göre zeka; öğrenme, anlama

⁸Council of Europe, History of Artificial Intelligence.

⁹Russell, Stuart J. Russell/Norvig, Peter, **Artificial Intelligence A Modern Approach**, Prentice-Hall, Englewood Cliffs, New Jersey, 1995, s.3.

¹⁰Türk Dil Kurumu, Güncel Türkçe Sözlük, “yapay”, (erişim tarihi: 13.1.2023), <https://sozluk.gov.tr>

¹¹Oxford Dictionary, (erişim tarihi: 13.1.2023), <https://www.oxfordlearnersdictionaries.com/definition/english/artificial>

¹² Türk Dil Kurumu, Güncel Türkçe Sözlük, “zeka”, (erişim tarihi: 13.1.2023), <https://sozluk.gov.tr>

mantıklı bir şekilde düşünme, iyi şekilde yapabilme yeteneğidir¹³. İnsanın çevresini tanıyarak, etkileşime geçtikleri yardımıyla düşünme, öğrenme; öğrendiğini kaydederek harekete geçme ve bu doğrultuda eylemlerini mantıklı bir şekilde gerçekleştirebilmesi yeteneğini zeka olarak addetmek yanlış olmayacaktır. Burada yapılan tanım canlılar üzerinden yapılmış olup zekanın doğal özelliğidir. Bunun yanı sıra gelişen teknoloji ile her şey kopyalanabilir hale gelmiş hemen hemen her şeyin yapayı üretilmektedir.

Yapay zeka, süreç içerisinde farklı farklı tanımlamalar ile ifade edilmektedir. Yapay zekanın isim babası Profesör John McCarthy yapay zekayı akıllı makineler yapmak için kullanılan bilim ve mühendislik olarak tanımlamaktadır. McCarthy'e göre yapay zeka, biyolojik olarak gözlemlenebilir yöntemlerle sınırlanması gerekmeksizin dünyadaki hedeflere ulaşma yeteneği olan makinelerdir¹⁴.

Avrupa Birliği Komisyonu yapay zekayı “*Belirli bir otonomiye sahip olan, belirli hedefleri gerçekleştirmek için çevresini analiz edip faaliyette bulunmak suretiyle zeki davranışlar sergileyen sistemler*” şeklinde tanımlamaktadır¹⁵. Avrupa Yapay Zeka Üst Düzey Uzman Grubu (High-Level Expert Group on Artificial Intelligence) ise AB Komisyonu’nun yapay zeka tanımını geliştirmiştir. Uzman Gruba göre yapay zeka sistemleri; kendisine karmaşık bir amaç verildiğinde veri toplayarak çevrelerini algılayan, toplanan verileri yapısal olsun ya da olmasın yorumlayarak, akıl yürüten ve fiziksel veya dijital boyutta hareket eden beşeri yazılım (ve muhtemelen donanım) sistemlerini ifade etmektedir¹⁶.

İnsan durumlar arasında ilişkilendirme yapabilen, düşünerek deneyim ve öğrendiklerinden sonuçlar çıkarabilen ve buna ilişkin kararlar alıp nihayete erdirebilen bir canlıdır. Bu durumu sağlayan insan zekasıdır ve yapay zeka ile bu yetenek taklit edilmektedir.

İnsan zekasının bileşenleri: öğrenme, akıl yürütme, problem çözme, algılama ve dili anlamadır¹⁷. İnsan zekasını taklit ederek oluşan yapay zekalı makinelerin de ortak özellikleri

¹³ Oxford Dictionary, “the ability to learn, understand and think in a logical way about things; the ability to do this well”, (erişim tarihi: 13.1.2023), <https://www.oxfordlearnersdictionaries.com/definition/english/intelligence?q=intelligence>

¹⁴ McCarthy, John, “What is AI? Basic Questions”.

¹⁵ **Artificial Intelligence for Europe**, European Commission, COM(2018) 237 Final, Brüksel, 25.4.2018, (erişim tarihi: 20.1.2023) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A237%3AFIN>

¹⁶ **A Definition of AI: Main Capabilities and Disciplines**, High-Level Expert Group on Artificial Intelligence, Brüksel, 18.12.2018, (erişim tarihi: 20.1.2023), s.6.

¹⁷ Kapancı, Berk, “Özel Hukuk Perspektifinden Bir Değerlendirme: Yapay Zeka ve Haksız Fiil Sorumluluğu”, **Gelişen Teknolojiler ve Hukuk II: Yapay Zeka**, Ed. Doç. Dr. Eylem Aksoy Retornaz & Dr. Öğr. Üyesi Osman Gazi Güçlütürk, On İki Levha Yayıncılık, İstanbul, 2021, s.129.

vardır. Yapay zekalı makinelerin iletişime açık, kendini tanıyan ve kendi ile ilgili bilgileri bilebilen, dış dünyadaki bilgiye açık, bir hedef belirlemiş ve buna yönelik harekette bulunan, alternatif çözüm bulabilecek yaratıcılığa sahip olması gerekmektedir¹⁸. Bu sayılan özellikler yapay zekalı makinenin zeki olduğundan bahsedebilmek için gereken şartlardır. Bir başka deyişle elimizdeki makine bilgi alışverişine açık değilse, varlığı hakkında öz bilgisi yoksa, gözlemlemiyor veya öğrenmiyorsa, öğrendiklerini harekete geçirmiyorsa yahut tecrübelerini ve gözlemlerini kullanarak başarısız olduğunda alternatif çözümler üretmiyorsa zeki bir oluşumdan bahsetmek mümkün değildir. Yapay zeka insan zekasının bileşenlerini taklit ederek doğal zekaya ilişkin eylemlerin kopyasını oluşturmaktadır. Yapay zekalı makineler dokunma, tat, görme, işitme gibi farklı algı sensörleri aracılığı ile veriler elde edip bu verileri işleyerek hareket etmektedir¹⁹. Yapay zekanın taklit etme yeteneğine sahip olabilmesi için öncelikle elinde veri olması gerekmektedir. Veri olmaksızın yapay zeka yakıtı olmayan bir otomobile benzetilebilecektir.

Yapay zeka örneklerine bakıldığında hayatımızın birçok yerinde yapay zeka ile çalışan robotların olduğunu ve bu fiziki makine olmaksızın da birçok alanda yapay zeka ile karşılaştığımızı görebilmekteyiz. Satranç oyununda dünya şampiyonu ile yarışan Deep Blue ile başlayan yapay zeka örneklerini, ev robotları, insansı robotlar, TAY gibi sohbet robotları, insansız araçlar, akıllı evler takip etmektedir²⁰. Gelişen teknoloji ile yapay zeka hayatımızın her aşamasında karşımıza çıkmaktadır. Örneğin; yapay zeka ile gelen e-posta içeriğinin gerekli olup olmadığının doğal dil işleme yoluyla tespiti; görüntü tanıma ve işleme yoluyla yüz tanıma ya da plaka okumaları yapılmaktadır²¹.

¹⁸ Dülger, Murat Volkan, “Bir Hukuk Kurgu Denemesi: Yapay Zekalı Varlığın Hukuki Sorumluluğu (Olabilir Mi?)”, **Hukuk ve Daha Fazlası Dergisi**, 2017, s.7. (Hukuki Sorumluluk)

¹⁹ **Kapancı**, s. 130.

²⁰ Sert Sütçü, Selin, “Endüstri 4.0’da Yapay Zekanın Hukuki Sorumluluğu” **Farklı Perspektiflerden Endüstri 4.0 Yazıları I**, Ed. Ayşen Altun Ada & Fulya Mısırdalı Yangil, Gazi Kitabevi, Ankara, 2020, s.58-59.; Bozkurt Yüksel, Armağan Ebru/ Bak, Başak, “Yapay Zeka”, **Futurist Hukuk**, Aristo Yayınları, İstanbul, 2018, s.20.

²¹ Büyüközkan Feyzioğlu, Gülçin, “Dijitalleşen Dünyada Yapay Zeka, **Gelişen Teknolojiler ve Hukuk II: Yapay Zeka**, Ed. Doç. Dr. Eylem Aksoy Retornaz & Dr. Öğr. Üyesi Osman Gazi Güçlütürk, On İki Levha Yayıncılık, İstanbul, 2021, s.10.

1.1.2. Yapay Zeka Çeşitleri

Yapay zeka uygulamalarının çeşitliliği, eğitilme ihtiyacı ve dış dünyayı algılama farklılıklarına göre çeşitli sınıflandırmalara konu edilmektedir²². Bir sınıflandırmaya göre yapay zeka; zayıf ve güçlü yapay zeka olmak üzere iki gruba ayrılmaktadır. Bir diğer sınıflandırmaya göre yapay zeka; dar, genel ve süper yapay zeka olmak üzere üç grup halinde incelenmektedir. Bir başka sınıflandırmada ise yapay zekanın; salt kreatif yapay zeka, sınırlı hafıza kapasitesi olan yapay zeka, “zihin kuramı”na dayalı yapay zeka ve bilince sahip kendi varlığının farkında olan yapay zeka olmak üzere dört çeşidi bulunmaktadır.

Zayıf ve dar yapay zeka temelde aynıdır. Genel ve süper yapay zeka ise güçlü yapay zekanın alt alanları olarak kabul edilebilecektir.

1.1.2.1. Zayıf ve Güçlü Yapay Zeka

Önceden belirlenmiş konular için programlanmış ve yalnızca o belirli konularda sonuç verebilen yapay zeka, zayıf yapay zekadır²³. Güçlü yapay zeka, herhangi bir öğretilmeye ihtiyaç duymaksızın insan beynini taklit ederek insan gibi düşünen, çalışan, bağımsız seçimler yapan ve iletişimde bulunan yapay zeka türüdür²⁴. Günümüzde güçlü yapay zekadan söz etmek henüz mümkün değildir.

1.1.2.2. Dar, Genel ve Süper Yapay Zeka

Dar yapay zeka için yapılan zayıf yapay zeka tanımına eklenecek herhangi bir ifade bulunmamaktadır. Dar yapay zeka, yalnızca programlandırıldığı ve ona öğretilen konularda hareket edebilen yapay zeka türü olarak tanımlanabilecektir. Online alışveriş sırasında size yardımcı olabilir miyim diye yanda beliren yardımcı asistan Chat botları buna örnek verilebilecektir. Dar yapay zeka kendisine öğretilenin daha ilerisinde bir işlem gerçekleştirememektedir. Bir oyunu yenme amaçlı yapay zekanın banka borcu ödemek gibi alakasız bir işi başarması beklenmemelidir²⁵. Genel yapay zeka ise güçlü yapay zeka ile eşdeğer görülebilecektir. Genel yapay zeka insan gibi düşünüp hareket ederek hayata katılabilecektir. Genel yapay zeka, herhangi bir müdahaleye gerek kalmaksızın insan gibi hareket ederek dar

²² Kapancı, s.131-133.

²³ Ersoy, Çağlar, **Robotlar, Yapay Zeka ve Hukuk**, 3. Baskı, On İki Levha Yayıncılık, İstanbul, 2018, s.30.

²⁴ Bozkurt/Bak s. 9.

²⁵ Demir, Ozan, “Sürdürülebilir Kalkınma İçim Yapay Zeka”, **Yapay Zeka ve Gelecek**, Ed. Gonca Teli, Doğu Kitabevi, İstanbul ,2019, s. 61.

yapay zekalar arasında iletişimi sağlayıp eylemde bulunabilecektir²⁶. Süper yapay zeka ise, insanı taklit etmenin ötesinde insanüstü zekaya sahiptir²⁷.

1.1.2.3. Algı Seviyesine Göre Yapay Zeka Sınıflandırması

Yapay zekanın sınıflandırılmasında bir diğer ayrım: reaktif yapay zeka, sınırlı hafıza kapasitesi olan yapay zeka, “zihin kuramı”na dayalı yapay zeka ve bilince sahip, kendi varlığının farkında olan yapay zekadır²⁸.

Reaktif yapay zeka, çevresini algılayıp gördükleri üzerine tepkiler vermektedir. Sadece bir alanda uzmanlaşabilen bu yapay zeka türüne Deep Blue, AlphaGo isimli oyuncu yapay zekalar örnektir.

Sınırlı hafıza kapasitesi olan yapay zeka, karar verip eylemde bulunabilmesi için sınırlı bir hafıza kapasitesine ihtiyaç duyan yapay zeka türüdür. Sürücüsüz araçlar, Chatbotlar, Alexa bu tür yapay zekaya örnektir.

Zihin kuramına dayalı yapay zeka, insan davranışları üzerinde etkisi bulunan, duygu ve düşünceleri anlayabilme kapasitesine sahip yapay zekadır. Bir başka deyişle, sosyal zeka sahibi olan yapay zeka da denilebilecektir. Örneğin; henüz gerçek hayatta karşımıza çıkmayan fakat bilim kurgu kitaplarında yer edinmiş I, Robot (Ben Robot) kitabındaki Robbie gibi karakterler.

Bilince sahip kendi varlığının farkında olan yapay zeka; kendi varlığının bilincinde olup diğer kişilerin duygularını okuyabilecek ön seziye sahip yapay zeka türüdür. Her ne kadar bilim kurgu filmlerinde karşımıza çıkmakta olsa da bilince sahip kendi varlığının farkında olan yapay zeka örnekleri henüz karşımıza çıkmamaktadır.

1.1.3. Yapay Zeka Öğrenme Türleri

Yapay zekanın eylemde bulunabilmesi için öncelikle öğrenmesi, ardından öğrendiklerini uygulayarak tecrübe etmesi ve bunu tekrarlaması gerekmektedir. Yapay zeka birden fazla yöntem ile öğrenme şartını gerçekleştirebilmektedir. Bunlardan en çok rastlananları makine öğrenmesi ve derin öğrenmedir.

²⁶ Demir, s.62.

²⁷ Kapancı, s.131.

²⁸ Bozkurt/Bak, s9-11.; Kapancı s. 132-133.

1.1.3.1. Makine Öğrenmesi (Machine Learning)

Yapay zekanın öğrenmesi denince akla öncelikle makine öğrenmesi gelmektedir. Makine öğrenmesi, bilgisayarlara açıkça programlama gerekmeksizin bilgiyi öğrenebilme yetisi veren çalışma alanı olarak ifade edilebilmektedir²⁹. Makine öğrenmesi her olayda tecrübe kazanarak öğrenen bir çocuğun kopyası gibidir, makine öğrenmesi de tıpkı çocuk gibi elindeki veriyi gözlemlemekte, öğrenmekte ve buna göre kendisine model belirleyerek harekette bulunmaktadır³⁰. Makine öğrenmesi algoritmaları, kendi kendine uyarlanabilen ve deneyimle kendine yeni desenler elde edebilecek şekilde tasarlanmaktadır³¹. Makine öğrenmesinde elde var olan veriler yardımıyla yeni veriler ile karşılaşılması durumunda da benzer çıktılar üretebilen bir model oluşturulması amaçlanmaktadır³².

Makine öğrenmesinde adımlar şu şekilde gerçekleşmektedir³³: öncelikle veri seti tanımlanarak analize hazır hale getirilmekte, uygun makine öğrenimi algoritması seçilmekte, seçilen algoritmaya dayalı bir analitik model geliştirilmekte, bu model test verileri ile eğitilmekte ve model çalıştırılarak uygulanmaktadır. Makine davranışı çevresini gözlemlemesi ve bu çevre ile etkileşimi ile ortaya çıktığı için beklenenden farklı aksiyon alanları oluşabilmektedir³⁴. Makine öğrenmesinde gruplar, öğrenme seti içerisinde yer alan benzer sonuçlar ile eşleme yapacak kurallara tabidir³⁵. Bu şekilde bir genelleme ile her zaman doğru sonuçlara ulaşılması beklenememektedir. Gereksiz e-postaların belirlenmesinde kullanılan öğrenme setindeki tüm örnek e-postalar bir şehirden gönderilmişse, gereksiz e-posta filtresinin o şehirden gelen önemli bir e-postayı da gereksiz olarak etiketlemesi ihtimali vardır³⁶. Makine

²⁹ Sodhi, Pinky/ Awasthi, Naman/ Sharma, Vishal, "Introduction to Machine Learning and Its Basic Application in Python", (January 6, 2019). **Proceedings of 10th International Conference on Digital Strategies for Organizational Success**, s.1356, (erişim tarihi: 19.1.2023), <http://dx.doi.org/10.2139/ssrn.3323796>

Zorlu, Mustafa: "Yapay Zeka ve Telif Hakkı", **Türkiye Barolar Birliği Dergisi**, C. 2019, S.142, s.311.

³⁰ Güçlütürk Osman Gazi/ Kadioğlu, Yasin Murat, "Yapay Zeka ve Regülasyon", **Gelişen Teknolojiler ve Hukuk II: Yapay Zeka**, Ed. Doç. Dr. Eylem Aksoy Retornaz & Dr. Öğr. Üyesi Osman Gazi Güçlütürk, On İki Levha Yayıncılık, İstanbul, 2021 s.82-83.

³¹ Lalitha, R., "AI vs. Machine Learning vs. Deep Learning", **Artificial Intelligence (AI) Recent Trends and Applications**, Ed. S. Kanimozhi Suguna/ M. Dhivya/ Sara, Paiva, CRC Press, Boca Raton, 2021, s.75.

³² Theodoros, Chiou, "Copyright lessons on Machine Learning: what impact on algorithmic art?", **Journal of Intellectual Property, Information Technology and Electronic Commerce Law (JIPITEC)**, C.10, S.3, 2019, s.399.

³³ Lalitha, s.75.

³⁴ Kangal, Zeynel T., **Yapay Zeka ve Ceza Hukuku**, On İki Levha Yayıncılık, İstanbul, 2021, s. 25.

³⁵ Güçlütürk, Osman Gazi, **Yapay Zeka ve Verinin Kullanımı**, On İki Levha Yayıncılık, İstanbul, 2022, s.74.

³⁶ Güçlütürk, s.74.

öğrenmesi modellerinde veri setindeki bir verinin model oluşumuna nasıl etki ettiğinin tespiti çok zordur; dolayısıyla ön yargı tespiti ve ortadan kaldırması da çok zordur. Örneğin; COMPAS isimli algoritma, yeniden suç işleme potansiyelini ölçmek için hakimler tarafından yurt dışında kullanılan bir algoritmadır; yapılan araştırmalar bu algoritmanın belli kökenli insanların yeniden suç işleme potansiyelini diğer insanlardan daha yüksek hesapladığını göstermektedir³⁷. Bu durumun sebebi yapay zeka algoritmalarında yalnızca girdiler ile sınırlı kalınmaması; insan emri veya yeni bir öğretim gerekmeksizin talimatların değişerek yeni algoritmalar üretilebilmesidir³⁸. Makine öğrenimi algoritması tekniği ile çalışan bir yapay zekanın sağlık sektöründe kullanımında ön yargılı davranması, çok keskin zararlara sebep olabilecektir. Yeniden suç işleme ihtimalini hesaplarken etnik kökene dayalı çıktılar üreten bir sistemin, sağlık hizmeti sunulması hakkında çalışan bir yapay zeka kullanımında etnik köken veya yaşa dayalı ayrımcılık yapmayacağı ve kişinin temel hakkından yoksun kalmasına sebep olmayacağı maalesef kesin olarak söylenemeyecektir.

Yapay zekanın makine öğrenmesi çalışma prensibi Google arama motoru üzerinden şu şekilde açıklanabilmektedir³⁹: sürekli internet bağlantıları arasında dolaşıp yeni siteler arayıp keşfeden Google tarayıcıları, bu web sitelerini birçok veriden yararlanarak belirleyip Google sunucularına iletmekte ve bu bilgiler Google tarafından hatırlanır hale gelmektedir. Google bu şekilde öğrenmekte ve öğrenmesinin ardından herhangi bir arama söz konusu olduğunda konuyu tespit edebilecek bilgiyi algılayıp öğrenme sürecinde edindiği bilgiler ile algoritma sayesinde ilgili internet sitelerini aratana sunmaktadır.

Makine öğrenmesinin bir başka örneği ise oyuncu yapay zekalar üzerinden verilebilmektedir. Satranç oynamak amacıyla ortaya çıkan bir yapay zeka, satranç algoritmaları aracılığı ile makine öğrenmesini gerçekleştirmektedir; öncelikle oyuna dair kurallar girdi olarak algoritmaya eklenmekte, önceki satranç oyun verileri aracılığı ile eğitilmekte ve bu şekilde satranç oynama yetisine sahip hale gelip gelişebilmektedir⁴⁰.

³⁷ Güçlütürk, s.75; Larson, Jeff/ Mattu, Surya/ Kirchner, Lauren/ Angwin, Julia: “How We Analyzed the COMPAS Recidivism Algorithm”, **ProPublica (blog)**, 2016, (erişim tarihi: 20.1.2023), <https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm>

³⁸ Kaya, İsmail, “AI vs. Algorithms: What’s the Difference?”, **Cmswire**, 26.10.2018, (erişim tarihi: 20.1.2023), <https://www.cmswire.com/information-management/ai-vs-algorithms-whats-the-difference/>

³⁹ **Zorluel**, s.309-310.

⁴⁰ **Yılıyaer**, s.27.

1.1.3.2. Derin Öğrenme (Deep Learning)

Yapay zeka öğrenme türlerinden ikincisi; derin öğrenmedir. Bir tür makine öğrenme tekniği olan derin öğrenme; insanın karmaşık problemler karşısında gözlem, analiz yapma ve karar alma gibi özelliklerini kopyalayan, verilerden yararlanarak durumu algılayıp buna yönelik özellik çıkarma, dönüştürme ya da sınıflandırma yapan yapay zeka tekniğidir⁴¹. Derin öğrenme ile karmaşık halde sunulmuş bilgiler, işlenmek için katmanlar yardımı ile ayrılarak kolayca yorumlanabilen etiketlere çevrilmektedir⁴².

Derin öğrenme süreci şu şekilde gerçekleşmektedir⁴³: Problemin tanımı yapılarak derin öğrenmeye uygun olup olmadığı tespit edilmektedir. Derin öğrenmeye uygun olması durumunda, ilgili veri kümesi tanımlaması yapılarak veri kümesi analiz için hazırlanmakta ve uygulanacak derin öğrenme algoritması seçilmektedir. Seçilen algoritma önce tanımlı veriler ile eğitilmekte, ardından eğitilmiş model tanımsız veriler ile test edilmektedir.

Derin öğrenmeyi geleneksel makine öğrenmesinden ayıran, otomatik özellik çıkarım kabiliyetidir⁴⁴. Bu sebeple de öğrenmek için birçok veriye ihtiyaç duymaktadır. McKinsey Global Institute Raporu'nda derin öğrenmenin yapay zeka öğrenimi için ne kadar çok veri işlendiğinin en iyi örneği olduğu belirtilmektedir⁴⁵.

Derin öğrenme uygulamaları; mühendislik, sağlık, çeviri bilimi gibi birçok alanda kullanılmaktadır. Derin öğrenmenin başarılı örneklerinden biri Google Translate'in diller arası çeviri için kullandığı algoritmalarıdır⁴⁶. 2015 yılında Google Translate uygulama üzerinden derin sinir ağları sayesinde yirmiden fazla dil arasında görsel çeviri yapabilecek hale gelmiştir.

⁴¹ Kayaalp, Kıyas/ Süzen, Ahmet Ali, **Derin Öğrenme ve Türkiye'deki Uygulamaları**, Ankara, İKSAD Yayınevi, 2018, S.7, s.7. (erişim tarihi: 16.6.2023)

https://www.researchgate.net/publication/327666072_Derin_Ogrenme_ve_Turkiye%27deki_Uygulamalari

⁴² Calo, Ryan/Evtimov, Ivan/Fernandes, Earlane/Kohno, Tadayoshi/O'Hair, David, "Is Tricking a Robot Hacking?", **University of Washington Tech Policy Lab**, Seattle, 2018, s.4, (erişim tarihi: 21.1.2023), <https://digitalcommons.law.uw.edu/techlab/5>

⁴³ Kayaalp/Süzen, s.11.

⁴⁴ Büyüközkan Feyzioğlu, s.7.

⁴⁵ Henke, Nicolaus/ Bughin, Jacques/ Chui, Michael/ Manyika James/ Saleh Tamim/ Wiseman Bill/ Sethupathy Guru, **The Age of Analytics: Competing in a Data-driven World**, McKinsey & Company, 2016, (erişim tarihi: 3.2.2023), s.23 <https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-age-of-analytics-competing-in-a-data-driven-world>

⁴⁶ Castelvechi, Davide, "Deep Learning Boosts Google Translate Tool", **Nature**, 2016, (erişim tarihi: 10.3.2023), <https://doi.org/10.1038/nature.2016.20696>

Google Translate'in görselden çeviri yapma süreci şu şekilde gerçekleşmektedir⁴⁷: öncelikle bir fotoğraf ile karşılaştığında fotoğraf karesinde bulunan harfleri, birbirine benzer renge veya görüntü lekelerine sahip belirsiz görüntü noktalarını tespit ederek arka plandaki cisimlerden ayırmaktadır. Bunlar muhtemel harflerdir ve birbirlerine yakın konumları ile belli bir sıralama içinde olduğundan okunabilir hale gelmektedir. Bunun üzerine uygulama her harfin gerçekten ne olduğunu tespit etmektedir. Bu sırada derin öğrenmeden yararlanılmaktadır. Google uygulamanın farklı harflerin tespitini yapabilmesi için gereken öğrenmeyi neyin harf olup olmadığı üzerinden eğiten bir sistem kullanmaktadır⁴⁸. Harflerin tespitinin gerçekleşmesi üzerine bu harfler, potansiyel bir kelime olarak algılanarak çevirilerinin yapılması için sözlükte aranmaktadır. Potansiyel kelime ile kast edilen, "Super" kelimesinin bir önceki aşamada "5uper" olarak algılanması durumunda da algoritma kelimenin çevirisini "Super" olarak bulabilmesidir. Son olarak ise, çevirisi yapılmış orijinal kelimenin taranan fotoğraftaki konumuna, harfleri çevreleyen renklere bakarak diğer dilde karşılığı olan kelime yerleştirilmektedir.

1.1.4. Yapay Zekanın Kullanım Alanları

Yapay zeka hayatımızın her yerinde kendini göstermeye başlamıştır. Türkiye Yapay Zeka İnisiyatifi Girişimi 2017 yılı Çalıştay Raporunda yapay zekanın gelecekte girmedığı alan kalmayacağını; akıllı ev uygulamaları, eğitim, emniyet, enerji, tarım, sağlık, üretim her alana dokunacağını belirtmektedir⁴⁹. Yapay zekanın hayatımızdaki yerini anlamak için genel kullanım alanlarını ve sağlık alanında kullanımını incelemek gerekmektedir.

⁴⁷ Good, Otavio (Google Research Team), "How Google Translate Squeezes Deep Learning onto a Phone", **Google AI Blog**, 30.07.2015, (erişim tarihi: 13.3.2023), <https://ai.googleblog.com/2015/07/how-google-translate-squeezes-deep.html>

⁴⁸ Derin öğrenmenin gerçekleştirilebilmesi için Evrişimli Sinir ağı(Convolutional Neural Network – CNN-) sistemi kullanılmaktadır.

⁴⁹ **1. Çalıştay Raporu**, Türkiye Yapay Zeka İnisiyatifi(TRAI), 9.5.2017, (erişim tarihi: 15.3.2023), <https://turkiye.ai/wp-content/uploads/2021/12/TRAI-Calistay-Raporu-2017.pdf>

1.1.4.1. Yapay Zekanın Genel Kullanımı

Yapay zeka sistemleri yazılım tabanlı veya donanım tabanlı olarak karşımıza çıkabilmektedir⁵⁰. Yazılım tabanlı yapay zeka sistemlerine Alexa gibi sesli asistanlar, yüz tanıma sistemleri; donanım tabanlı yapay zeka sistemlerine ise robotlar ve otonom arabalar örnektir⁵¹.

Donanım tabanlı yapay zeka sistemlerinden olan robotların kullanıldığı endüstri alanları gün geçtikçe artmaktadır. Tarım, otomobil endüstrisi, eğlence, kurtarma ve ev hizmetleri yapay zekanın kullanıldığı alanlardan birkaçıdır⁵². Burada bahsedilen robot kavramı yapay zekaya sahip robotlardır, yapay zekaya sahip olmayan robotlar kapsam dışında tutulmaktadır. Her yapay zeka robot olmak zorunda değildir, aynı şekilde her robot da yapay zeka değildir⁵³. Farklı sektörlerde yapay zeka kullanımı sadece robotlar için değil tüm yapay zeka sistemleri için artmaktadır.

Yapay zeka kullanımı yedi alanda özetlenebilmektedir⁵⁴: Hiper kişileştirme, otonom sistemler, tahmine dayalı analitik ve karar desteği, konuşma ve insan etkileşimi, kalıp ve anormallik tespiti, tanıma ve hedef odaklı sistemler (Bulmaca çözümü).

Hiper kişileştirme, makine öğrenmesi yoluyla her birey için profil geliştirilmesi ve bu profilin zamanla ilgili içerik görüntüleme, ilgili ürün önerme gibi farklı amaçlarla kullanılmasıdır. Günümüzde pazarlama ve finans sektöründe kullanımı oldukça fazladır. Netflix'in kullanıcısının profilini çıkararak önerdiği film ve diziler buna örnek olarak sayılabilmektedir.

Otonom sistemler; minimum insan müdahalesi ile bir görevi tamamlayan, hedefe ulaşan, çevresindekilerle etkileşime geçen yazılım veya donanım sistemleridir. Otonom sistemler, bağımsız olarak makine öğrenmesi ile dış dünyayı gözlemleyip, dışarıdaki bir etken kaynaklı gelecekte gerçekleşebilecek davranışı öngörüp ona göre plan yaparak hareket etmektedir. Otonom sistemler genellikle ulaşımda karşımıza çıkmaktadır.

⁵⁰ Ersoy, s.7.

⁵¹ **A Definition of AI: Main Capabilities and Disciplines**, High-Level Expert Group on Artificial Intelligence, s.7.

⁵² Lenzen, Manuela, **Künstliche Intelligenz: Was sie kann&was uns erwartet**, Verlag C.H. Beck, Münih, 2018, s.97.

⁵³ Bozkurt Yüksel, Armağan Ebru, “Yapay Zekanın Buluşlarının Patentlenmesi”, **Uyuşmazlık Mahkemesi Dergisi**, Y. 6, S.11, 2018, s.592.

⁵⁴ Walch, Kathleen (Cognitive World), “The Seven Patterns of AI”, **Forbes**, 17.09.2019, (erişim tarihi: 13.3.2022) <https://www.forbes.com/sites/cognitiveworld/2019/09/17/the-seven-patterns-of-ai/>

Tahmine dayalı analitik ve karar desteği, makine öğrenmesi ve diğer bilişsel yaklaşımlar ile yaşanmış ve mevcut davranışların gelecekte oluşabilecek sonuçlarda nasıl etki doğurabileceğine ilişkin örüntülerin kullanımınıdır.

Konuşma ve insan etkileşimi; insanların kendi aralarında sağlayabildiği etkileşimi, insanlar ile makinelerin sağlayabilmesidir. Kullanılan Chat botları, ses asistanları ve çeviri programları bunun en rastlanan örneğidir.

Kalıp ve anormallik tespitinde, örüntüler ile olağanın dışında kalan durumların farkına varılmaktadır. Yapay zeka; makine öğrenmesi sayesinde oluşturduğu örüntüde, verinin mevcut örüntüdeki veriler ile uyuşup uyuşmadığını kontrol etmektedir. Bu kullanım alanı özellikle dolandırıcılık tespitlerinde karşımıza çıkmaktadır.

Tanıma, özellikle derin öğrenmenin en çok kullanıldığı alanlardandır. Derin öğrenme; fotoğraf, video, ses, obje tanıma ve sınıflandırmanın gelişmesinde çok büyük gelişme göstermektedir. Yüz tanıma amacıyla yapay zeka kullanımının en çok eleştirildiği ülkelerden biri olan Çin’de hem özel şirketler hem de hükümet tarafından birçok örneği vardır⁵⁵.

Hedef odaklı sistemler (Bulmaca çözümü), makine öğrenmesi ile oyunların kurallarını öğrenen makinelerin bu oyunlarda insanlar ile yarışmasında ve hatta insanları yenmesinde görülmektedir. Oyunların yanında hedef odaklı sistemler herhangi bir probleme en uygun çözümün tespitini yapmak için kullanılabilir.

1.1.4.2. Yapay Zekanın Sağlık Bilimlerinde Kullanımı

Sağlık hizmetleri içerisinde robotlar, yüksek riskli doğasından dolayı diğer alanlara kıyasla daha yavaş yer edinmiştir⁵⁶. Buna rağmen sağlık sektöründe robot ve diğer yapay zeka çeşitlerinin kullanımı günümüzde azımsanamayacak düzeydedir.

Sağlık bilimlerinde iki tür yapay zeka bulunmaktadır. Sağlık bilimlerinde yer alan yapay zeka türlerinin ilki; uzman sistemlerdir, bunlar sağlık çalışanlarının görevlerini yerine getirirken kullandıkları elektronik araçlardır. Sağlık bilimlerinde yer alan bir diğer yapay zeka türü; uzman sistemlerden farklı olarak, tamamen otonom bir şekilde sağlık çalışanı gibi hareket ederek teşhis koyup hastanın onamının alınması üzerine tedavi sürecini başlatabilen, bu süreçte

⁵⁵ Brown, Tristan G./Statman, Alexander/Sui, Celine, “Public Debate on Facial Recognition Technologies in China”, **MIT Case Studies in Social and Ethical Responsibilities of Computing**, 2021, s.3. (erişim tarihi: 15.3.2023) <https://dspace.mit.edu/handle/1721.1/144299>

⁵⁶ Matthews, Kayla, “5 Industries that Robotics Have Disrupted Drastically”, **Robotics Business Review**, 27.09.2019, (erişim tarihi: 13.3.2023), <https://www.roboticsbusinessreview.com>

tanımlanan özelliklerin dışına da çıkarak talimatsız da hareket edebilenlerdir⁵⁷. Sağlık çalışanı gibi otonom hareket eden yapay zeka türü, henüz sağlık sisteminde mevcut değildir. Sağlık sektörünün tamamen robotların eline bırakılması henüz mümkün görülmemektedir; çünkü özellikle cerrahi alanlarda detaylı hastalık teşhisi için hastanın ameliyata girmesi gerekmekte, cerrahlar ameliyat esnasında süre ile yarışarak tedavi ve tıbbi müdahale yöntemine karar vermektedir; yapay zekanın öğrenmeyi gerçekleştirmek için kullandığı veri miktarı düşünüldüğünde henüz bu tür ameliyatlarda tek başına başarılı olacağına inanmak mümkün görünmemektedir⁵⁸. Bilgi düzeyinin yanında; hukuk, sağlık gibi alanlarda her adımın yalnızca yapay zeka eli ile yürütülmesinin mümkün olmamasının bir sebebi de yapay zekanın katı kurallara daha bağlı olmasıdır. Bilgisayar sistemleri aracılığı ile katı kurallardan sapma perspektifi çok da mümkün değildir⁵⁹. Bir ameliyat sırasında gelişebilecek komplikasyonlar için hızlı karar verme ve önceden yapılan planlamaların değişikliği hayati önem taşıyabildiği için yapay zekanın tek başına sağlık sektörünü ele geçirmesi en azından yakın gelecekte beklenmemektedir.

Sağlık bilimlerinde yapay zeka kullanımının artmasındaki başlıca sebepler; yaşlı nüfusun ve dolayısıyla bakım ihtiyacının artmış olması, sağlığı tehdit eden hastalıkların sayısının gün geçtikçe artması, yaşam kalitesinde düşüşler yaşanması, gelişen pazarda maliyet ve rekabetin artması ve gelişen bilişim teknolojileri ile yapay zeka kullanımının mümkün hale gelmesidir⁶⁰.

Sağlık bilimlerinde yapay zeka ve robotik kullanımının avantajları şu şekilde sıralanabilmektedir⁶¹:

⁵⁷ Kluge, Eike-Henner W., “Artificial Intelligence in Healthcare: Ethical Considerations”, **Healthcare Management Forum**, C. 33, S.1, 2020, s.47. (erişim tarihi: 18.3.2023) <https://journals.sagepub.com/doi/pdf/10.1177/0840470419850438>

⁵⁸ Say, Cem, **50 Soruda Yapay Zeka**, 23. Bs., 7 Renk Basım Yayım ve Filmcilik, İstanbul, 2022, s.147-148. ; Ford, Martin, **Robotların Yükselişi Yapay Zeka ve İşsiz Bir Gelecek Tehlikesi**, Çev.: Cem Duran, 11. Bs., Kronik Kitap, İstanbul, 2022, s.185.

⁵⁹ Fateh-Moghadam, Bijan, “Innovationsverantwortung im Strafrecht: Zwischen strict Liability, Fahrlässigkeit und erlaubttem Risiko – Zugleich ein Beitrag zur Digitalisierung des Strafrechts”, **Zeitschrift für die gesamte Strafrechtswissenschaft**, C.131, S.4, 2019, s.870, (erişim tarihi: 20.3.2023). <https://doi.org/10.1515/zstw-2019-0031>

⁶⁰ Akalın, Betül/Veranyurt, Ülkü, “Sağlık Hizmetleri ve Yönetiminde Yapay Zeka”, **Acta Infologica**, C.5, S.1, 2021, s.232-233. (erişim tarihi: 15.3.2023) <https://dergipark.org.tr/tr/pub/acin/issue/63212/850857>

⁶¹ Ellahham, Samer/ Ellahham, Nour, “Use of Artificial Intelligence for Improving Patient Flow and Health Delivery”, **Journal of Computer Science & Systems Biology**, C.12, S.3, 2019, s.5, (erişim tarihi: 16.3.2023)

Yapay zeka ve robotik kullanımı sağlık çalışanları arasında bilgi paylaşımını kolaylaştırmakta, sağlık hizmetlerinin kalitesini iyileştirmekte, daha iyi teşhis ve tedavi imkanı sağlamakta, veriler tıbbi araştırmalarda kullanılabilmekte, maliyet ve harcanan zamanı azaltarak sağlık hizmetlerinde verimi arttırmakta, hasta takibini kolaylaştırmakta, bulaşıcı hastalık tahmini ve yavaşlatması için kullanılmaktadır.

Sağlık bilimlerinde yapay zeka kullanımı ile sağlık çalışanları üzerindeki baskı, sağlık hizmeti maliyetleri azalacak ve özetle hastaların hayat kalitesi gelişecektir⁶².

Tıbbi müdahale aşamaları teşhis, tedavi ve hastalıktan koruma amaçlarından birine sahip olunan müdahaleleri içine almaktadır⁶³. Sağlık bilimlerinde yapay zeka tıbbi teşhiste bulunma, tedavi gibi tıbbi müdahale aşamalarında kendini göstermektedir⁶⁴. Bunun dışında yapay zeka; idari yönetim, klinik karar desteği, izlem yapma amacıyla da kullanılabilir⁶⁵.

Kişinin sahip olduğu düşünülen fiziksel veya mental bir rahatsızlığın olup olmadığını bulmak, var ise rahatsızlığın ne olduğunun tespitine yönelik yapılan faaliyetler teşhis faaliyetleridir⁶⁶. Hastalıkların yapay zeka ile daha erken ve doğru tespit edilmesi mümkün hale gelmektedir⁶⁷. Günümüzde meme kanseri tespiti için kullanılan yapay zeka algoritmaları ortalama bir radyoloji uzmanı kadar güvenilir tespitte bulunabilmektedir⁶⁸. Aynı şekilde günümüzde en çok rastlanan kötü tümör türlerinden cilt kanserinin tespiti için kullanılan yapay

https://www.researchgate.net/publication/336742991_Use_of_Artificial_Intelligence_for_Improving_Patient_Flow_and_Healthcare_Delivery

⁶² Schönberger, Daniel, “Artificial intelligence in healthcare: a critical analysis of the legal and ethical implications”, International Journal of Law and Information Technology, C.27, S.2, 2019, s.172, (erişim tarihi: 18.3.2023), <https://doi.org/10.1093/ijlit/eaz004>

⁶³ Yılmaz, Battal, **Açıklamalı-İçtihatlı Hekimin Hukuki Sorumluluğu**, 4. Bs., Adalet Yayınevi, Ankara, 2020, s.23.

⁶⁴ Kangal, s.5.

⁶⁵ Reddy, Sandeep/ Fox, John/ Ourohit, Maulik P., “Artificial Intelligence-enabled Healthcare Delivery”, **Journal of the Royal Society of Medicine**, C.112, S.1, s.23, (erişim tarihi: 18.3.2023), <https://journals.sagepub.com/doi/pdf/10.1177/0141076818815510>

⁶⁶ Yenerer Çakmut, Özlem, **Tıbbi Müdahaleye Rızanın Ceza Hukuku Açısından İncelenmesi**, Legal Yayınları, İstanbul, 2003, s.35.

⁶⁷ Hoşgör, Haydar, **Sağlıkta Yapay Zeka ve Robotik**, Dora Yayıncılık, 2022, s.52

⁶⁸ Palmer, Whitney J., “AI Algorithm Reaches Equivalent Accuracy of Average Radiologist”, **Diagnostic Imaging**, 27.8.2020, (erişim tarihi: 18.3.2023), <https://www.diagnosticimaging.com/view/ai-algorithm-reaches-equivalent-accuracy-of-average-radiologist>

zeka, uzman dermatologlarla aynı kulvarda kabul edilebilecek başarıya ulaşmaktadır⁶⁹. Covid döneminde robot kullanımı ile hastalık şüphesi olan kişilerden örnekler alınmakta, sağlık çalışanlarının hayatını riske atmadan bulaşıcı hastalık tespiti yapmakta, hastalığın ne şekilde devam edeceğini tahmin ederek sağlık çalışanlarına yardım etmekteydi⁷⁰.

Hastalık teşhisinde kullanılan yapay zekaya kalp hastalıklarının teşhisi için kullanılan IBM Watson, uzman doktor ile eşdeğer bir şekilde cilt kanserini tespit edebilen SkinVision ve göz hastalıklarını tespit eden birtakım algoritmalar örnektir⁷¹. Watson doğal dil işleme ile çalışan bir yapay zeka uygulamasıdır, hasta ve sağlık çalışanlarının semptomları açıklayıp teşhisi sorması üzerine Watson bu soruyu anlayıp geniş bir literatür taraması yapıp hastanın elektronik medikal veri kaydını da göz önünde bulundurarak hastalık hakkında tanılama yapmakta ve bunu hasta ve ilgili sağlık uzmanı ile paylaşmaktadır⁷². Watson, makine öğrenmesi ile öğrenmesini gerçekleştiren bir yapay zeka ürünüdür. Watson'a makine öğrenmesi esnasında girdi olarak işlenen verilerin teorik veriler olup gerçek hastalara ait bilgiler olmadığı ortaya çıkmıştır, makine öğrenmesi ile işleyen yapay zeka ürünlerinin kendisine sunulan veri kadar iyi olabileceği de göz önünde bulundurulduğunda Watson'ın doğru ve güvenli sonuçlar vermediği tartışılmakta ve birçok hastane IBM ile Watson için yaptığı anlaşmayı sona erdirmektedir⁷³.

Erken teşhiste yapay zeka kullanımına dair Crycadia's iTBra ve CardioDiagnostics verilebilecek diğer örneklerdir. Crycadia's iTBra'nın giyilmesi ile meme kanserine dair erken teşhiste bulunulabilmekte; bir başka giyilebilir teknoloji ürünü olan CardioDiagnostics ile kişinin kalp ritmi takip edilmekte ve gereken durumlarda erken teşhis ve müdahale sağlanmaktadır⁷⁴.

⁶⁹ Esteva, Andre/ Kuprel, Brett/ Novoa, Roberto A./ Ko, Justin/ Swetter, Susan M./ Blau, Helen M./ Thrun, Sebastian, "Dermatologist-level classification of skin cancer with deep neural networks" . **Nature**, S.542, 25.1.2017, s.115, (erişim tarihi: 18.3.2023), <https://doi.org/10.1038/nature21056>

⁷⁰ Karagöz, Jülide Güzin, **Sağlıkta Dijital Dönüşüm, Yapay Zeka (AI) ve Nesnelerin İnterneti (IoT)**, Kutlu Yayınevi, İstanbul, 2018, s.69-70.; Tunç, Aybike, "Güncel Teknoloji ve Kişisel Veri", **Kişisel Verilerin Korunmasına Akademik Bakış- KVKK Akademi Derleme Çalışması**, Ed. Pınar Çağlayan Aksoy/ Hüseyin Can Aksoy, Ütopya Grafik, Ankara, 2023, s.304.

⁷¹ Longoni, Chiara/ Bonezzi, Andrea/ Morewedge, Carey K., "Resistance to Medical Artificial Intelligence", **Journal of Consumer Research**, C. 46, S. 4, 2019, s. 629. (erişim tarihi: 18.3.2023) , <https://doi.org/10.1093/jcr/ucz013>

⁷² Miller, Adam, "The Future of Healthcare Could Be More Elementary With Watson", **CMAJ**, C.185, S.9, 2013, s.367, (erişim tarihi: 20.3.2023) <https://doi.org/10.1503/cmaj.109-4442>)

⁷³ Konam, Sandeep, "Where Did IBM go wrong with Watson Health?", **Quartz**, (erişim tarihi: 20.3.2023), <https://qz.com/2129025/where-did-ibm-go-wrong-with-watson-health>

⁷⁴ Karagöz, s.47.

Hastanın rahatsızlığı ile ilgili konulan teşhisin doğruluğu hakkında ya da teşhis konulmasının ardından uygulanacak tedavi hakkında karar verilmesi gerekmektedir, bu karar yalnızca hangi tedavinin uygulanacağı ile sınırlı değildir, bazı durumlarda kimin tedavi göreceğine, hayati riskin ne kadar olduğuna karar vermek gerekmektedir. Bu tür durumlarda karar almada sağlık çalışanlarına destek sağlayan yapay zekalar vardır⁷⁵. Hekimler demans ve erken hafıza kaybı hastalıklarını tespit edebilmek için hasta test sonuçları ile medikal verileri birleştiren Quest Diagnostic Quanam'dan yararlanmakta, bu şekilde teşhis konulması kolaylaşmaktadır⁷⁶. Covid-19 döneminde hastalık teşhisi konulan kişiler için ölme riski tahmini ve hastanede tedavi için önceliği tespit etmek için akıllı Karar Destek sistemi kullanılmış ve öngörülerinde bu sistemin doğruluk payının çok yüksek olduğu tespit edilmiştir⁷⁷.

Tedavi, teşhisi konulan hastalığın hafifletilmesi, iyileştirilmesi ya da ortadan kaldırılmasıdır⁷⁸. Tedavi faaliyetlerinin gerçekleştiği esnada da yardımcı yapay zeka uygulamaları vardır. Örneğin, AiCure tarafından geliştirilen uygulama aracılığı ile hasta durumları gözlemlenmekte ve hastanın ilaç tedavisine bağlı kalıp kalmadığı sağlık çalışanına bildirilmektedir⁷⁹.

Tıbbi müdahalenin robotlar desteği ile gerçekleştirilmesi bir yenilik değildir, 1990'lı yıllar itibariyle Zeus, Da Vinci ve Monalisa isimli üç robot birçok ameliyatın gerçekleşmesinde görev almaktadır⁸⁰. Günümüzde cerrahi müdahalelere destek için cerrahi robotlar; lojistik eylemleri gerçekleştirmek için hastane lojistik robotları; rehabilitasyon robotları; robot hemşireler ve canlı sağlık çalışanlarının bulunamayacağı ortamlarda çalışması gereken telepresence robotları sağlık hizmetlerinde yer edinmektedir⁸¹.

Tıbbi müdahale sürecinin dışında yapay zekanın tıbbi araştırmalarda, ilaç keşfinde ve gelişiminde kullanımı zorunlu hale gelmektedir⁸². İlacın toksisite tahminini yapan Deeptox, ilaç keşfi için uygun denek adayının bulunmasına destek olan DeepChem mevcut yapay zeka örnekleridir; kişiselleştirilmiş ilaç teknolojisini mümkün hale getirmek için bireyin gen

⁷⁵ Pourhomayoun, Mohammad/ Shakibi, Mahdi, "Predicting mortality risk in patients with COVID-19 using machine learning to help medical decision-making" , **Smart Health**, C.20, 200278, 2021, (erişim tarihi: 20.3.2023), <https://doi.org/10.1016/j.smhl.2020.100178>

⁷⁶ Karagöz, s.48.

⁷⁷ Pourhomayoun / Shakibi, s.7.

⁷⁸ Hakeri, Hakan, **Tıp Hukuku**, 20. Bs., Seçkin Yayıncılık, Ankara, 2020, s.53.

⁷⁹ Karagöz, s.48.

⁸⁰ Karagöz, s.69.

⁸¹ Karagöz, s.69-70.

⁸² Hoşgör, s. 63.

haritasını çıkararak gen tipine uygun ilaç üretimini sağlayabilecek yapay zeka için de çalışmalar sürmektedir⁸³.

Yapay zeka desteğinin sağlık bilimlerine en önemli katkılarından biri hem teşhis hem de tedavide oluşabilecek ölümcül hataları azaltmak olarak değerlendirilebilmektedir⁸⁴. Yapay zeka hastanın öyküsü, ilaçların toksikliği ve yan etkilerine erişebiliyor ise oluşabilecek hataların önüne geçebilecektir⁸⁵. Doktorların olası bir malpraktis davasında sorumluluktan kurtulabilmek için defansif tıbbı sığındığı bir gerçektir. Bunun için doktorlar aslında durum için şart olmayan test ve taramaları da talep edebilmektedir. Yapay sistem desteği ile gereksiz tarama ve testlere gerek kalmayacaktır. Bu sayede test masrafları ve dolaylı olarak doktorun hata payındaki düşme sayesinde zorunlu sigorta masrafları da düşecektir⁸⁶.

1.1.5. Yapay Zekaya İlişkin Hukuki Düzenlemeler

Yapay zekanın dünden bugüne hayatımızda gösterdiği etkileşim ve gelecekte de hayatımızın merkezinde olacağı ortadadır. Avrupa Birliği kurumları ve büyük şirketler, yapay zeka odaklı ilerleyen değişimler uyarınca hem gelecekte yapay zeka kaynaklı oluşabilecek sorunları önceden öngörüp ona göre davranabilmek hem de yapay zekanın değiştirdiği tüketici eğilim ve değişimlerine uyum sağlayarak ayakta kalabilmek için araştırma ve yatırım yapmaktadır⁸⁷. Bunların yanında artık devletler de yapay zekanın önemini fark etmiş ve konu hakkında düzenlemeler yapmaya başlamıştır⁸⁸.

Güney Kore’de “The Robot Special Act” ve “Zeki Robotların Geliştirilmesinin ve Yaygınlaştırılmasının Desteklenmesine Dair Kanun”; Japonya’da “Fukuoka Dünya Robot Bildirgesi” ve Avrupa Birliğinin çeşitli çalışmaları bu düzenlemelere örnektir⁸⁹. Teknoloji ile gelecek olası etkiler ve sonuçları araştıran “Responsible Research and Innovation”; Avrupa’da yapay zeka kullanımını geliştirmeyi amaçlayan “SPARC” ve yapay zeka hakkında etik tartışmalar üzerinde duran “EURON” başlıca Avrupa Birliği çalışmalarıdır⁹⁰. Uluslararası çalışmalar yalnızca Avrupa Birliği’nde değil OECD gibi uluslararası birliklerde de

⁸³ Hoşgör, s.64.

⁸⁴ Ford, s.179.

⁸⁵ Ford, s.180.

⁸⁶ Ford, 180.

⁸⁷ Bozkurt/Bak, s. 17-18.

⁸⁸ Bozkurt/Bak. s.27.

⁸⁹ Ersoy, s.39-40.

⁹⁰ Sert Sütçü, s. 65.

gözenmektedir. 22/05/2019 tarihinde Ekonomik Kalkınma ve İşbirliği Örgütü (OECD) Yapay Zeka Hakkında Öneriler adlı bir belge düzenlemiştir⁹¹.

1.1.5.1. Uluslararası Hukuktaki Düzenlemeler

Avrupa Komisyonu 2018 yılında Avrupa'nın yapay zeka stratejisini yayımlamıştır⁹². Yapay Zeka Stratejisi uyarınca etik ve hukuki boyutta incelemeler yapıp alanda destek sağlaması için Avrupa Yapay Zeka Üst Düzey Uzman Grubu⁹³ yetkili kılınmaktadır.

Avrupa Komisyonu 2020 yılında yapay zeka üzerine yayımladığı bir raporunda ürün güvenliği ve sorumluluğuna dair direktifin⁹⁴, eşitlik hakkında mevcut olan direktiflerin⁹⁵, tüketiciyi korumaya ilişkin kuralların⁹⁶, kişisel verilerin korunması ve özel hayatın gizliliğine ilişkin kuralların⁹⁷ “yapay zeka” kavramı dahil edilmese de prensipte uygulanabilir olduğunu,

⁹¹ OECD, **Recommendation of the Council on Artificial Intelligence**, OECD/LEGAL/0449, 22.05.2019, (erişim tarihi: 17.3.2023), <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449#mainText>

⁹² **Artificial intelligence for Europe**, European Commission.

⁹³ <https://ec.europa.eu/digital-single-market/en/high-level-expert-group-artificial-intelligence>, (erişim tarihi: 17.3.2023),

⁹⁴ Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety

⁹⁵ Council Directive 2000/43/EC of 29 June 2000 implementing the principle of equal treatment between persons irrespective of racial or ethnic origin, Council Directive 2000/78/EC of 27 November 2000 establishing a general framework for equal treatment in employment and occupation, Council Directive 2004/113/EC of 13 December 2004 implementing the principle of equal treatment between men and women in the Access to and supply of goods and services, Directive 2006/54/EC of the European Parliament and of the Council of 5 July 2006 on the implementation of the principle of equal opportunities and equal treatment of men and women in matters of employment and occupation

⁹⁶ Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive'), Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council Text with EEA relevance

⁹⁷ Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA

fakat yapay zekaya ilişkin oluşabilecek risklerin ele alınması için yeterli uygulanabilirlikte olup olmadığı, yasal araçlarda değişikliklerin yapılmasının gerekip gerekmediğini değerlendirmenin önemli olduğunu belirtmektedir⁹⁸. Bu raporun ardından 22/04/2021’de yapay zekanın güvenilirliğini arttırmak adına Yapay Zeka (Yapay Zeka Yasası) Hakkında Uyumlaştırılmış Kurallar Belirleyen ve Mevcut Birlik Mevzuatlarını Değiştiren Tüzük Önerisi⁹⁹’nde bulunulmuştur. Son günlerde Avrupa Birliği’nin yapay zeka ile ilgili gündeminde yapay zekanın sorumluluğu yer almaktadır. 28/09/2022 tarihinde Yapay Zekanın Sözleşme Dışı Sorumluluğu’nun Kabulü Yönetmelik Önerisi’nde bulunulmuştur¹⁰⁰.

14 Haziran 2023 tarihinde Avrupa Birliği Komisyonu tarafından önerilen Yapay Zeka Tüzüğü, Avrupa Parlamentosu tarafından onaylanmıştır. Söz konusu tüzük, yapay zekayı düzenlemeyi amaçlayan ilk yatay düzenleme olma özelliğine sahiptir¹⁰¹. Tüzük, risk odaklı olarak yapay zeka sistemlerini sınıflandırıp, bu sınıflandırmalara dayanarak birtakım gereklilik ve yükümlülükler öngörmektedir. Bu şekilde amaçlanan, yapay zeka kullanımı ile sağlık alanı da dahil birçok sektörde ekonomik ve sosyal yarar sağlanırken, yapay zeka kullanımının sebep olabileceği güvenlik sorunları ve temel hakların ihlallerine karşı kişilerin korunmasıdır¹⁰². Tüzük, yalnızca Avrupa Birliğinde kurulmuş yapay zeka sistem sağlayıcılarını değil, yapay zeka sistemini Avrupa Birliği pazarına sunan AB üyesi olmayan ülkeler ile sağlayıcısı veya kullanıcısı AB sınırları içerisinde yer almasa da yapay zeka sistemi tarafından üretilenlerin AB

; Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

⁹⁸ **White Paper on Artificial Intelligence- A European Approach to Excellence and Trust**, European Commission, Brussels, COM (2020) 65 Final, Brüksel, 19.2.2020, s.13, (erişim tarihi 17.3.2023), https://commission.europa.eu/system/files/2020-02/commission-white-paper-artificial-intelligence-feb2020_en.pdf

⁹⁹ Proposal for a Regulation of the European Parliament and Of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, (erişim tarihi:04.09.2023) https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC_1&format=PDF

¹⁰⁰ Proposal for a Directive of the European Parliament and of the Council on adopting non-contractual civil liability rules to artificial intelligence (AI Liability Directive), (erişim tarihi 18.03.2023), https://commission.europa.eu/system/files/2022-09/1_1_197605_prop_dir_ai_en.pdf

¹⁰¹ **Artificial Intelligence Act Briefing**, European Parliamentary Research Service, European Parliament, Haziran 2023, s.1, (erişim tarihi: 04.09.2023), [https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI\(2021\)698792_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf)

¹⁰² **Artificial Intelligence Act Briefing**, s.2.

içerisinde kullanılması durumunda bu kişileri de etkilemektedir¹⁰³. Tüzük m.5 hükmü; kabul edilemez riskli yapay zeka uygulamalarını yasaklamaktadır. İlgili maddeye göre; subliminal teknikler aracılığıyla insanları manipüle edip kendilerine veya başkalarına zarar verecek ya da vermesini muhtemel hale getirecek eylemlere sebep olacak sistemler, çocuk ya da engeli olan hassas gruplarda yer alan kişilere zarar verebilecek ya da istismarına sebep olması muhtemel sistemler, kamu otoritelerince insanları sosyal puanlamaya tabi tutan sistemler, kanunun uygulanması amacıyla eş zamanlı uzaktan biyometrik tanıma sistemlerinin kamuya açık alanda kullanılmasını sağlayan sistemler bu grupta yer almaktadır. Tüzük m.6 hükmü; insanların güvenliği ya da temel hakları üzerinde olumsuz etki oluşturabilecek sistemleri yüksek riskli yapay zeka sistemleri olarak tanımlamakta ve bunlar için birtakım yükümlülükler öngörmektedir. Yapay zeka sistemi Avrupa Birliği sağlık ve güvenlik uyum düzenlemelerinden birinin kapsamına giriyor ya da bir ürünün güvenlik eklentisi olarak kullanılıyorsa veya yapay zeka sistemi üçüncü kişi ön uyum incelemesi gerektiren kendi başına bir ürün ise yüksek riskli yapay zeka sistemi olarak kabul edilmektedir¹⁰⁴. Yüksek riskli yapay zeka sağlayıcısının ürünü pazara sunmadan önce Avrupa Birliği merkezli bir veri tabanına kaydolması, uygunluk değerlendirmesi yapması, risk yönetimi, teknik sağlamlık, veri eğitimi ve yönetimi, şeffaflık, insan gözetimi ve siber güvenlik gibi konularda birtakım şartlara uyması gerektiği m.8 ve m.15 hükümleri arasında düzenlenmektedir. Düşük riskli yapay zeka sistemleri uyum ya da herhangi bir ek yükümlülüğe tabi tutulmamaktadır. Tüm bunlar göz önünde bulundurulduğunda etki alanı Avrupa Birliği sınırları dışına çıkan bir düzenleme olan Tüzük, yapay zekanın anayasası niteliği taşımaya adaydır. Yapay Zeka Tüzüğü, Avrupa Birliği'nin Genel Veri Koruma Tüzüğü gibi alanında standart belirleyici öncü bir düzenleme olup yapay zekaya ilişkin kurallar düzenlenmesinde rehber olacaktır.

1.1.5.2. Ülkemizdeki Hukuki Durum

Ülkemizde henüz yapay zekaya ilişkin kanun veya kanun teklifi yoktur. Fakat Ağustos 2021'de ilk Ulusal Yapay Zeka Stratejisi yayımlanmıştır. Strateji planının ana odakları ve hedefleri arasında idari ve hukuki düzenlemelerin yapay zeka sebepli dönüşüm ile uyumlu hale getirilmesi ve yapay zeka kaynaklı oluşabilecek sonuçları öngörebilmek üzere araştırmalar

¹⁰³ Artificial Intelligence Act Briefing, s.3.

¹⁰⁴ Artificial Intelligence Act Briefing, s. 5.

yapılması yer almaktadır. Yapay zeka etik ve hukuki açıdan takip edilecek, buna ilişkin faaliyetler düzenlenerek uluslararası düzenlenen faaliyetlerin takibi sağlanacaktır¹⁰⁵.

Yapay zekanın popülerleşmesi ile birlikte regülasyon ihtiyacı kendini göstermektedir. Özellikle ayrımcılık yapılmaması gereken alanlarda yapay zeka kullanımına ilişkin yasal düzenlemelerin geç kalınmadan yapılması mantıklıdır¹⁰⁶. Sağlık bilimleri de bu alanlar arasında yer almaktadır.

1.2. Kişisel Sağlık Verilerinin Korunması Kavramı

Kişisel sağlık verilerinin korunması kavramının anlaşılabilmesi için öncelikle kişisel veri kavramının ve kişisel sağlık verisi kavramının anlaşılması gerekmektedir. Kavramların anlaşılabilmesi için tanım, kapsam yönünden değerlendirmeler yapılarak öneminin ortaya konması gerekmektedir.

1.2.1. Kişisel Veri Kavramı

Kişisel veri kavramı uzun zamandan beri tartışılan düzenleme yapılması planlanan konulardan bir tanesi idi. Kişisel veri kavramı, günümüzde kapsamı ve unsurları hakkında ortak görüşlerle birçok hukuki metinde tanımlanmaktadır.

1.2.1.1. Tanım

Türk Dil Kurumu, veri kelimesini “*bilgi, data*” ya da “*bir araştırmanın, bir tartışmanın, bir muhakemenin temeli olan ana öge, muta, done.*” şeklinde tanımlamaktadır¹⁰⁷. TDK “kişisel” kelimesinin tanımını “*Kişi ile ilgili, kişiye ilişkin, kişinin kendi malı olan, şahsi, zati*” şeklinde yapmaktadır¹⁰⁸. Bu doğrultuda kişisel veri, kişi ile ilgili herhangi bir bilgi olarak kabul edilebilecektir.

95/46/EC sayılı “Bireylerin Kişisel Verilerinin İşlenmesi ve Serbestçe Dolaşımı Karşısında Korunmasına İlişkin Direktifi m.2 hükmünde kişisel veri “*‘kişisel veriler’, kimliği belirli veya belirlenebilir bir gerçek kişiyle (‘veri sahibi’) ilgili herhangi bir bilgi*” şeklinde belirtilmektedir.

¹⁰⁵ **Ulusal Yapay Zeka Stratejisi 2021-2025**, T.C. Sanayi ve Teknoloji Bakanlığı, Türkiye Cumhuriyeti Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, Ağustos 2021, (erişim tarihi: 18.03.2023), <https://cbddo.gov.tr/SharedFolderServer/Genel/File/TR-UlusalYZStratejisi2021-2025.pdf>

¹⁰⁶ **Schönberger**, s.172-173.

¹⁰⁷ Türk Dil Kurumu, Güncel Türkçe Sözlük, “veri”, <https://sozluk.gov.tr/>, (E.T: 28.03.2023)

¹⁰⁸ Türk Dil Kurumu, Güncel Türkçe Sözlük, “kişisel”, <https://sozluk.gov.tr/>, (E.T: 28.03.2023)

Avrupa Birliği Genel Veri Koruma Tüzüğü m.4 hükmünde yapılan tanımlamalarda kişisel veri “*tanımlanmış veya tanımlanabilir bir gerçek kişiye ilişkin her türlü bilgi*” olarak kabul edilmektedir.

Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair 108 sayılı Avrupa Konseyi Sözleşmesi m.2/a ile “kişisel veri” kavramı benzer şekilde tanımlanmaktadır.

Kişisel verilerin korunmasına ilişkin esas ve usulleri düzenleyen 6698 sayılı Kişisel Verilerin Korunması¹⁰⁹ Kanunu¹¹⁰ m.3 hükmünde kişisel verilerin korunmasına ilişkin birtakım tanımlar yapılmaktadır. İlgili maddeye göre kişisel veri, “*Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi*”yi ifade etmektedir.

Kişisel veri, belirli ya da belirlenebilir nitelikteki kişiye ilişkin her türlü bilgidir¹¹¹.

Kişisel veri tanımı mahkeme kararlarında da adı geçen düzenlemelere paralel şekilde yer bulmaktadır.

Anayasa Mahkemesi kararlarında kişisel veri “*belirli veya kimliği belirlenebilir olmak şartıyla- bir kişiye ilişkin bütün bilgiler*” i ifade etmektedir¹¹².

Yargıtay’a göre kişisel veri “*belli veya belirlenebilir olan gerçek veya tüzel bir kişiye ilişkin her türlü bilgi*” demektir¹¹³.

Danıştay ise kişisel veriyi Anayasa Mahkeme kararlarına atıfta bulunarak kişisel verinin “*belirli veya kimliği belirlenebilir olmak şartıyla, bir kişiye ilişkin bütün bilgiler...*”¹¹⁴ olarak kabul edilmesi gerektiğini belirtmektedir. Başka bir kararında Anayasa Mahkemesi kişisel veriyi “*kişiyi doğrudan veya dolaylı olarak belirlenebilir kılan tüm veriler*”¹¹⁵ şeklinde tanımlamaktadır.

¹⁰⁹ R.G.: T. 7.4.2016/S. 29677.

¹¹⁰ Kişisel Verilerin Korunması Kanunu, tezimizin geri kalanında KVKK kısaltması ile kullanılacaktır.

¹¹¹ Aksoy, Hüseyin Can, **Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması**, Çakmak Yayınevi, Ankara, 2010, s.2.; Aydın, Akgül, Kişisel Verilerin Korunmasında Yeni Bir Hak: “Unutulma Hakkı” ve AB Adalet Divanı’nın “Google Kararı”, **Türkiye Barolar Birliği Dergisi**, S.116, 2016, s.12.

¹¹² Anayasa Mahkemesi Kararı – 2.B., B. 2018/6161 T. 28.6.2022; Anayasa Mahkemesi Kararı- 1.B., B. 2018/30296 T. 7.9.2021; Anayasa Mahkemesi Kararı – GK, B. 2016/4060 T. 17.9.2020 (E.T: 29.03.2023)

¹¹³ Bkz. Yargıtay Kararı - HGK., E. 2014/56 K. 2015/1679 T. 17.6.2015; Yargıtay Kararı- HGK., E.2017/1340 K.2018/1622 T.6.11.2018 (E.T: 29.03.2023)

¹¹⁴ Danıştay Kararı – İDDK., E.2020/420 K. 2022/214 T. 31.1.2022; Danıştay Kararı – İDDK., E.2019/3167 L. 2021/734 T. 8.4.2021 (Erişim Tarihi: 29.03.2023) www.lexpera.com.tr

¹¹⁵ Danıştay Kararı – İDDK., E. 2019/763 K. 2020/1861 T. 15.10.2020; Danıştay Kararı 8.D., E. 2017/3719 K.2022/2180 T.30.3.2022 Erişim Tarihi: 29.03.2023) www.lexpera.com.tr

Bir kişinin belirli ya da belirlenebilir olması ise verilerin gerçek kişi ile ilişkilendirilmesi ile o kişinin tanımlanabilir hale getirilmesi anlamına gelmektedir¹¹⁶.

1.2.1.2. Kapsam

Kişiyi belirli veya belirlenebilir kılan bilgilerin kapsamı dar olarak kabul edilmemelidir. Uluslararası düzenlemeler, ulusal düzenlemeler ve içtihat göstermektedir ki kişisel veri ile kast edilen geniş bir kavramdır.

Kişisel verilerin korunmasına dair temel mevzuat olan KVKK’de kişisel veri kavramı için geniş bir tanım bulunmaktadır. KVKK Tasarı Gerekçesi m.3 hükmü kişisel veri kapsamı hakkında bilgi verici niteliktedir. Gerekçe hükmüne göre kişinin kesin teşhisini sağlayan adı-soyadı, doğum tarihi ve yeri gibi bilgiler gibi kişinin ailevi, fiziki, ekonomik özelliklerine ilişkin bilgiler ile bu bilgilerin kayıtlarla ilişkilendirilmesi sonucu kişinin dolaylı yoldan tanınmasına yardımcı olabilecek bilgiler de kişisel veri kapsamında kabul edilmelidir. Gerekçede sayılan kişisel veri örnekleri arasında kişinin kimlik numarası, aracının plakası, fotoğrafı, parmak izi, genetik bilgileri, telefon numarası yer almaktadır. Bunlar kişisel veri örneği olmak ile birlikte kişisel veri bunlar ile sınırlı değildir.

Yargıtay Hukuk Genel Kurulu bir kararında, Avrupa İnsan Hakları Sözleşmesinde kişisel veri kavramının içeriğinin belirtilmediğini; fakat Avrupa İnsan Hakları Mahkemesinin ilgili olay değerlendirilerek bu içeriğin belirlendiğini belirtmektedir. İlgili kararda kişisel verilerin sayılanlarla sınırlı olmamakla birlikte neler olabileceği “*Kişisel verilerin sınırlı bir şekilde sayılması mümkün değil ise de, bireyin kimliğini ortaya çıkartan, bir kişiyi belirli kılan ve karakterize eden kişinin kimlik, ekonomik ve dijital bilgileri, tabiiyeti, kanaatleri, ırk, siyasî düşünce, felsefî inanç, din, mezhep veya diğer inançları, dernek, vakıf ve sendika üyeliği, sağlık bilgileri, fotoğrafları, parmak izi, sağlık verileri, telefon mesajları, telefon rehberi, sosyal paylaşım sitelerinde yazdığı veya paylaştığı yazılar, fotoğraf, ses veya görüntü kayıtları*” şeklinde sayılmaktadır¹¹⁷.

Anayasa Mahkemesi birçok kararında kişisel veri kavramının kapsamını Kişisel Verilerin Korunması Kanunu’nun yürürlüğe girmesinden bile önce: “...Bu bağlamda adı, soyadı, doğum tarihi ve doğum yeri gibi bireyin sadece kimliğini ortaya koyan bilgiler değil; telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, IP adresi, e-posta adresi, hobiler, tercihler, etkileşimde bulunulan kişiler, grup üyelikleri, aile bilgileri,

¹¹⁶ Türkiye Büyük Millet Meclisi 26. Yasama Yılı, 1. Yasama Dönemi, Kişisel Verileri Korunması Kanunu Tasarısı (1/541) ve Adalet Komisyonu Raporu, Gerekçesi, Madde 3 Gerekçesi, (erişim tarihi, 30.3.2023), <https://www5.tbmm.gov.tr/sirasayi/donem26/yil01/ss117.pdf>

¹¹⁷ Yargıtay Kararı – HGK., E.2017/1340, K.2018/1622, T. 6.11.2018, (erişim tarihi: 1.4.2023), www.lexpera.com.tr

sağlık bilgileri gibi kişiyi doğrudan veya dolaylı olarak belirlenebilir kulan tüm veriler" “ şeklinde değerlendirmektedir¹¹⁸. Anayasa Mahkemesi 12.10.2015 tarih ve 2015/32 E., 2015/102 K. sayılı Genel Kurul kararında teknolojik gelişmeler göz önünde bulundurulduğunda kişisel veri kavramının sınırlı sayı ilkesi ile belirlenmesinin mümkün olmadığı, bu kapsamın doktrin, uygulama ve yargı kararları ile belirlenip gelişip değişeceğinden kuşku olmadığı belirtilmektedir¹¹⁹.

1.2.1.3. Unsurlar

Kişisel verinin varlığından bahsedebilmek için gerekli birtakım unsurlar vardır. Bu unsurlar verinin bir kişiye ilişkin olması ve kişinin belirli ya da belirlenebilir nitelikte olmasıdır¹²⁰. 25.4.2018 Avrupa Birliği Genel Veri Koruma Tüzüğü yürürlüğe girene kadar kişisel verilerin korunması ve gizlilik hakkında sorunların çözümü için kurulmuş olan Madde 29 Çalışma Grubu (Article 29 Data Protection Working Party) kişisel verinin unsurlarını herhangi bir bilgi (veri), ilgili olma, belirli ya da belirlenebilir olma ve gerçek kişi olmak üzere dörde ayırmaktadır¹²¹:

Gerek ulusal gerek uluslararası kaynaklarda gerekse doktrindeki tanımlara bakıldığında kişisel verinin unsurları veri, verinin gerçek kişiye ilişkin olması ve veri sahibinin belirlenebilir nitelikte olması olarak sayılabilmektedir.

1.2.1.3.1. Veri

Kişisel verinin tanımı, belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi olarak yapılmaktadır. Kişisel veriden söz edebilmek için öncelikle bir verinin varlığı gerekmektedir.

Bilgi ve veri kavramları günümüzde her ne kadar birbirinin yerine kullanılsa da aslında farklı kavramlardır. Veri, bilgiden daha geniş bir kümeyi kapsıyor olmakla birlikte yalnızca

¹¹⁸ Anayasa Mahkemesi Kararı – GK. E.2013/122 K.2014/74, T. 9.4.2014; Anayasa Mahkemesi Kararı – GK. E.2014/180, K.2015/30, 19.3.2015; Anayasa Mahkemesi Kararı- 1.B., B. 2018/30296 T. 7.9.2021; fiziksel ve elektronik adreslere ve kayıtların kişisel veri olduğuna ilişkin: Anayasa Mahkemesi Kararı – GK. E.2013/84, K. 2014/183, T. 4.12.2014, (erişim tarihi: 1.4.2023), www.lexpera.com.tr

¹¹⁹ Anayasa Mahkemesi Kararı – GK. E.2015/32 K.2015/102, T. 12.11.2015(erişim tarihi: 1.4.2023), www.lexpera.com.tr

¹²⁰ Küzeci, Elif, **Kişisel Verilerin Korunması**, On İki Levha Yayıncılık, 4. Bs., İstanbul, 2020, s.9.

¹²¹ **Opinion 4/2007 on the Concept of Personal Data**, Article 29 Data Protection Working Party, 01248/07/EN, WP 136, 20.6.2007, s.6, (erişim tarihi: 1.4.2023), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf

alıcı için anlamlı olan veriler bilgi kapsamında değerlendirilmelidir¹²². Kullanıcı için anlamlı hale getirilen veriye bilgi denir¹²³.

Verinin içerdiği bilginin biçimi hakkında belirli sınırlamalar mevcut değildir. Belirli ya da belirlenebilir kişiye ait oldukça bilgi alfabetik, sayısal, çizgesel, fotografik veya akustik herhangi bir formda olabilmektedir¹²⁴.

Veri bilgisayar ortamında işlenmiş elektronik bir veri olabileceği gibi manuel yollarla da işlenebilmektedir¹²⁵. KVKK m.2 hükmünde kanunun kapsamı belirtilmektedir, ilgili hüküm de veri işlemenin tamamen veya kısmen otomatik olabileceği gibi otomatik olmayan yollarla da işlenebileceğini göstermektedir. Verinin kayıt altında tutuluşu, kağıt üzerinde olabileceği gibi bilgisayar hafızasında da olabilmektedir¹²⁶.

Verinin, kişi tarafından gizli tutulmaya çalışılan bir veri olması da gerekmemektedir¹²⁷. Nitekim kişinin yeme alışkanlıkları ve hobilerinin bile kişisel veri kapsamında yer aldığını düşündüğümüzde, bu bilgiler gizlenmek bir yana dursun kişilerin sosyal medya aracılığı ile herkesin ulaşımına açık durumda olabilmektedir. Bilginin nesnel veya öznel olma şartı olmadığı gibi bu bilgilerin doğru olması şartı da aranmamaktadır. Kişinin belli bir hastalığının olup olmadığına ilişkin nesnel bilgiler de güvenilir olup olmadığına ilişkin öznel bilgiler de doğru olup olmadığı kontrol edilmeksizin kişisel veri olarak kabul edilmektedir¹²⁸.

1.2.1.3.2. Belirli veya Belirlenebilir Kişi

Kişisel veriden bahsedebilmek için, verinin sahibinin belirli veya belirlenebilir bir kişi olması gerekmektedir. Bir veriden kişinin kim olduğu açık bir şekilde tespit edilebiliyor ise kişinin kimliği belirli; mevcut veriler ile kişinin kim olduğunun tespit edilebilmesi ihtimali var

¹²² Dülger, Murat Volkan, **Kişisel Verilerin Korunması Hukuku**, 3. Bs., Hukuk Akademisi Yayıncılık, İstanbul, 2020, s.153. (Dülger, Kişisel Verilerin Korunması)

¹²³ Küzeci, s.10-11.

¹²⁴ **Opinion 4/2007 on the Concept of Personal Data**, Article 29 Data Protection Working Party, s.7.

¹²⁵ İmançlı, Canan, **Kişisel Sağlık Verilerinin Korun(a)mamasından Doğan Özel Hukuk Sorumluluğu**, On İki Levha Yayıncılık, İstanbul, 2020, s.41.

¹²⁶ **Opinion 4/2007 on the Concept of Personal Data**, Article 29 Data Protection Working Party, s.7.

¹²⁷ **Opinion 4/2007 on the Concept of Personal Data**, Article 29 Data Protection Working Party, s.6; Aksoy, s.14.

¹²⁸ Aksoy, s.14-15.

ise kişinin kimliği belirlenebilir¹²⁹. Bir verinin kişisel veri olabilmesi için kişiyi diğer kişilerden ayırt edebilir nitelikte olması gerekmektedir.

Bir verinin kişiyi belirli veya belirlenebilir hale getirip getirmeyeceği olaydan olaya değişebileceği için her somut olayda ayrı ayrı değerlendirilmelidir¹³⁰. Avrupa Birliği Genel Veri Tüzüğü m.4 hükmünde yapılan tanıma paralel olarak kişinin adı ile doğrudan belirlenebilir; kimlik numarası, üzerine kayıtlı telefon numarası, yaşı, mesleği gibi ölçütlerin bir araya gelmesi ile dolaylı olarak da belirlenebilir olduğunu söylemek doğru olacaktır¹³¹. Örneğin; mobese kameraları ile sürekli trafikteki araçlar kayıt altında tutulmaktadır. Direkt bakılması durumunda bu araçların herhangi bir kişiyi doğrudan belirli kıldığını söylemek mümkün değilken; bir trafik kazası olması durumunda aracın plakası tespit edilerek hangi gerçek kişiye ait olduğu tespit edilebilmektedir. Kişinin isim olarak belirlenemediği durumlarda dahi diğer kişilerden ayırt edilerek tam kimliği belirlenmese de kişiyi belirlemiş olmak kişinin belirli ya da belirlenebilir olması şartı için yeterlidir¹³².

1.2.1.3.3. Verinin Gerçek Kişiyne İlişkin Olması

Kişisel verinin KVKK ile yapılan tanımı uyarınca öncelikle gerçek bir kişiye ilişkin olması gerekmektedir. Hukukumuzda, tüzel kişilerin kişisel verisinden bahsetmek mümkün değildir. Kişisel verilerin korunması ile asıl amaçlanan kişinin temel hak ve özgürlüklerini korumak iken, tüzel kişilerin de kişisel verisinden bahsedilmesi kanunun amacını aşacak bir durumdur¹³³. Kişisel Verileri Koruma Kurulu'nun 19.11.2018 tarihli 2018/131 sayılı kararında da tüzel kişiliğe ait elektronik ortamda yer alan verilerin başka bir tüzel kişilik tarafından talep edilmesi hakkında yapılan başvuruda Kurul, tüzel kişiliğe ait verilere erişilmesi yönündeki talebin Kanun kapsamında değerlendirilemeyeceği sebebi ile başvuruyu reddetmektedir¹³⁴. Fakat tüzel kişiye ait olup gerçek kişi ile ilişkilendirilebilen verilerin olması durumunda, tüzel kişide bulunan verinin de veri koruma hukuku kapsamında korunması gerekmektedir¹³⁵.

¹²⁹ Orak, Beşir, **Kişisel Sağlık Verilerinin Korunması**, Yetkin Yayınları, Ankara, 2020, s.25; **Opinion 4/2007 on the Concept of Personal Data**, Article 29 Data Protection Working Party, s.12; **Aksoy**, s.21.

¹³⁰ **Aksoy**, s.24; **Dülger**, s.158.; **İmançlı**, s.48; Yılmaz, Sabire Sanem, **Tıp Alanında Kişisel Verilerin Korunması**, 4. Baskı, Seçkin Yayıncılık, Ankara, 2020, s.54.

¹³¹ **İmançlı**, s.48.

¹³² **Dülger**, s.161. (**Dülger**, Kişisel Verilerin Korunması)

¹³³ **Orak**, s.25.

¹³⁴ Kişisel Verileri Koruma Kurulu'nun 19.11.2018 tarihli 2018/131 sayılı Karar Özeti: (<https://kvkk.gov.tr/Icerik/5423/2018-131>) (E.T.: 1.4.2023)

¹³⁵ **Dülger**, s.172. (**Dülger**, Kişisel Verilerin Korunması)

Türk Medeni Kanunu m.28/1 hükmü kişiliğin doğum ile başlayıp ölümle sona erdiğini belirtmektedir. Kişinin ölümünün ardından hak ve borçlarından bahsedilememektedir¹³⁶. Gerçek kişinin ölümü sonrasında kişiliği son bulmaktadır. Ölüm ile birlikte kişilik hakları sona erdiği için ölen adına mirasçılar kişisel verilerin korunmasına ilişkin haklardan yararlanamamaktadır¹³⁷. Bir bilginin kişisel veri kapsamında kabul edilebilmesi için verinin yalnızca o kişiye ait olması şartı arandığı anlamına gelmemektedir. Tıbbi müdahale esnasında, hastanın öyküsünü alırken doktor, hastanın ailesindeki bireylere ilişkin de bilgiler alabilmektedir. Hastanın ailesine ait bu bilgiler hasta için kişisel veri kabul edilmektedir¹³⁸. Bilginin, kişinin hak ve menfaatlerini etkileyip etkilememesi kişisel veri kabul edilmesinde önem arz etmektedir¹³⁹. Bir başka deyişle ölmüş kişinin kişisel verisi başka insanları etkiliyor ise o veri artık etkilenen kişinin kişisel verisidir ve korunması gerekmektedir. Ölen kişinin genetik bir hastalığının olmasına dair kişisel verisi aynı zaman ölen kişinin çocukları için de kişisel veri niteliğinde olup korumaya tabidir¹⁴⁰.

1.2.1.4. Özel Nitelikli Hassas Veri

Kişisel veriler, genel nitelikli kişisel veriler ve özel nitelikli (hassas) kişisel veriler olarak ikiye ayrılmaktadır. Genel nitelikli kişisel veriler hukuki düzenlemelerde sayılanlar ile sınırlı değilken, özel nitelikli (hassas) veriler sınırlı sayıdadır.

Kişisel Verilerin Korunması Kanunu m.6/1 hükmünde özel nitelikli (hassas) veriler, “*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 veriler*” ile sınırlı olarak sayılmaktadır.

Kanun Gerekçesi m.6 hükmünde özel nitelikli (hassas) verilerin, veri sahibi için mağduriyet ya da ayrımcılığa yol açabilecek nitelikte olduğu ve bu sebeple hakkında ayrı bir koruma öngörüldüğü belirtilmektedir. Özel nitelikli (hassas) verilerin işlenme şartları, genel nitelikli verilerin işlenme şartlarından daha sıkıdır.

¹³⁶ Oğuzman, Kemal/ Seliçi, Özer/ Oktay Özdemir, Saibe, **Kişiler Hukuku**, 21. Bs., İstanbul, 2022, s.19

¹³⁷ Develioğlu, Hüseyin Murat, **6698 sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü Uyarınca Kişisel Verilerin Korunması Hukuku**, On İki Levha Yayıncılık, İstanbul, 2017, s. 32.

¹³⁸ Yılmaz, s.56.

¹³⁹ **Opinion 4/2007 on the Concept of Personal Data**, Article 29 Data Protection Working Party, s.9.

¹⁴⁰ Develioğlu, s.32.

1.2.2. Kişisel Sağlık Verisi Kavramı

Korunma ihtiyacı genel kişisel verilerden daha yüksek olan kişisel sağlık verisinin gerekli korumaya ulaşabilmesi için öncelikle kavramın doğru bir şekilde anlaşılabilmesi gerekmektedir. Bu sebeple; kişisel sağlık verisinin tanımı, kapsamı ve yüksek korumaya ihtiyaç duymasının önemi üzerinde durulmalıdır.

1.2.2.1. Tanımı

Kişisel Verilerin Korunması Kanunu m.6 hükmünde sayılan özel nitelikli (hassas) verilerden birisi de sağlık verileridir. KVKK’de sağlık verisi tanımı yapılmamaktadır.

Avrupa Birliği Genel Veri Koruma Tüzüğü m.4/15 hükmünde sağlıkla ilgili veri “*sağlık hizmetlerinin sağlanması da dahil olmak üzere bir gerçek kişinin sağlık durumuyla ilgili bilgilerin açıklandığı, söz konusu gerçek kişinin fiziksel veya ruhsal sağlığına ilişkin kişisel veriler*” şeklinde tanımlanmaktadır.

Kişisel Sağlık Verileri Hakkında Yönetmelik m.4/j hükmünde kişisel sağlık verileri “*Kimliği belirli ya da belirlenebilir gerçek kişinin fiziksel ve ruhsal sağlığına ilişkin her türlü bilgi ile kişiye sunulan sağlık hizmetiyle ilgili bilgiler*” şeklinde belirtilmektedir.

Kişisel sağlık verisi, sağlık çalışanlarınca bilinip birbirlerine aktarılan veya başka bir meşru sebebe dayanılarak öğrenilen ve kişinin başkalarınınca bilinmesini istemeyeceği, hastaya ait kişisel verilerdir¹⁴¹.

1.2.2.2. Kapsamı

Kişinin ruhsal veya fiziksel sağlığına ilişkin her türlü bilgi kişisel sağlık verisi kapsamında yer almaktadır. Kişisel sağlık verisi kapsamı geniş kabul edilmektedir. Sağlık verileri; kişinin geçmişteki, güncel ya da gelecekte oluşabilecek sağlık durumuna ilişkin tıbbi teşhis, tanı, tedaviye ilişkin bilgiler, spor bilgileri, özellikle sağlık sigortasına işlenen verileri içermektedir¹⁴².

Sağlık verilerinin korunması temel hak ve özgürlüklerin korunması kapsamında değerlendirildiğinden, sağlık verisinin kapsamı da geniş tutulmalıdır¹⁴³. Kişinin doğrudan sağlık kuruluşlarında tutulan sağlık kayıtlarının yanında bu kişilerin egzersiz bilgileri,

¹⁴¹ Hakeri, s.1318.

¹⁴² Yılmaz, s.59.

¹⁴³ Orak, s.30.

muhasabe kayıtları, sigorta şirketlerine gönderilen veriler gibi birçok veri birleşerek kişinin sağlık verileri haline gelebilmektedir¹⁴⁴.

Sağlık verilerine doğrudan veya dolaylı olarak erişilebilmektedir¹⁴⁵. Bir kişinin satın aldığı bir sağlık ürünü, o kişi hakkında doktor tarafından konan teşhisi belirlenebilir hale gelmesini sağlamakta ve dolayısıyla da kişinin tanımlanabilir hale gelmesine neden olmaktadır. Kişisel verinin doğrudan sağlık ile ilgili tıbbi veri olması gerekmemektedir; medikal olmamasına rağmen verinin başka veriler ile eşleşince sağlık verisi haline gelebilmesi, medikal olmayan verinin ilgili kişinin sağlık durumu ile ilişkilendirilebilmesi durumunda sağlık verisi kapsamı içinde değerlendirilmesi gerekmektedir¹⁴⁶.

1.2.2.3. Korunmasının Önemi

Kişilerin sağlık verilerinin korunmayabileceğini düşünmesi durumunda, sağlık hizmetine ihtiyaç duymalarına rağmen tıbbi yardım almamayı tercih edebileceği ve dolayısıyla hem kendi sağlıklarını hem de bulaşıcı bir hastalık söz konusu olduğunda toplum sağlığını tehdit edebilecekleri ortadadır. Kişinin sağlık verilerinin ifşa edilmesi durumunda ise kişilerin aşağılanma, toplumdan dışlanma ihtimali doğacak; kişi ailesinden ve işinden uzaklaştırılmış olacaktır¹⁴⁷. Bu sebeplerle kişisel sağlık verilerinin korunmasına dair gerekli adımlar atılmak zorundadır.

Yargıtay Ceza Genel Kurulu bir kararında: *“Sağlık verileri kişilerin iş güvenliğini, toplum içindeki statüsünü ve sigorta kapsamını etkileyen hassas bilgilerdir. Ayrıca sağlık verileri kişilerin sosyal yaşantısı ve psikolojik durumları hakkında bilgi edinilmesine neden olabilir.”*¹⁴⁸ diyerek sağlık verilerinin korunmamasının yaratabileceği olumsuzluklara yer vermektedir. Sağlık verilerinin kişinin iş durumunu ve toplum içindeki statüsünü etkilediğine dair birçok örnek bulunmaktadır. HIV hastası olan T.A.A hastalığı sebebiyle işsiz kalmış, ardından açtığı davada gizlilik talebinin reddedilmesi üzerine maddi ve manevi varlığın korunması ve özel hayatın gizliliğinin ihlaline dayanarak AYM’ye başvurmuştur. AYM, HIV’e dair verileri, kişisel sağlık verisi olarak değerlendirmiştir ve *“HIV pozitif durumda olan kişiler yönünden bu hastalık sadece bir sağlık sorunu olmayıp sosyal yaşamda ön yargılarla karşılaşmaları, damgalanmaları ve toplumdan dışlanmaları gibi problemlere de yol açarak ilgili kişilerin özel hayatının diğer boyutlarını da etkilemektedir. Söz konusu dışlanma, damgalanma ve ön yargıların özellikle iş hayatında mevcut*

¹⁴⁴ Yılmaz, s.59.

¹⁴⁵ Yılmaz, s.59.

¹⁴⁶ Dülger, Kişisel Verilerin Korunması, s.179.

¹⁴⁷ Orak, s.31.

¹⁴⁸ Yargıtay Kararı- CGK., E.2012/1514, K. 2014/312, T. 10.6.2014, (erişim tarihi: 2.4.2023), www.lexpera.com.tr

olması durumunda kişiler üzerindeki etkiler çok daha yıkıcı olabilmektedir. HIV pozitif kişilerin sırf bu nedenle çalışma hayatından uzaklaştırılmaları, bu kişilerin yeniden iş bulmalarını çok zorlaştıracağı gibi oldukça yüksek maliyetli olan ve hayat boyu alınması gereken tedaviye ulaşmalarını zorlaştırarak sağlıkları üzerinde ciddi sorunlar ortaya çıkarabilir.”¹⁴⁹ diyerek sağlık verilerinin korunmasının önemini ortaya koymaktadır. Avrupa İnsan Hakları Mahkemesi, kişisel sağlık verileri içeren kararlarında verinin Avrupa İnsan Hakları Sözleşmesi m.8 hükmü kapsamına düşüp düşmediğine ve açıklanıp açıklanmayacağına dair değerlendirme yapmakta ve sadece gerekli verinin açıklanıp açıklanmadığına bakmaktadır¹⁵⁰. Mahkeme kararları kişisel verilerin korunması için gösterilen önemi sunmaktadır. Kişisel verilerin korunması, özel hayatın gizliliğini koruma yönünden de devletin pozitif yükümlülükleri arasında kabul edilmektedir. Devlet, kişileri hem kamusal makamların hem de diğer bireylerin eylemlerinden doğabilecek risklere karşı korumakla yükümlüdür¹⁵¹.

1.2.3. Kişisel Sağlık Verilerinin Korunmasına İlişkin Hukuki Düzenlemeler

Kişisel sağlık verilerinin korunması hem uluslararası hem de ulusal düzenlemeler konu edilmektedir. Uluslararası ve ulusal düzenlemeler ile kişisel sağlık verileri özel bir hüküm altında ya da hekimin sır saklama yükümlülüğü ya da özel hayatın gizliliği hakkı adı altında korunmaktadır.

1.2.3.1. Uluslararası Hukuki Düzenlemeler

Kişisel verilerin korunmasına ilişkin ilk düzenlemeler 23 Eylül 1980 tarihinde Ekonomik Kalkınma ve İşbirliği Örgütü¹⁵² tarafından yayımlanan “Özel Yaşamın Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkeleri”¹⁵³’dir. OECD Rehber İlkeler üye ülkeler için bağlayıcı değildir fakat sonraki düzenlemeler için örnek oluşturmaktadır. Rehber ilkeler ulusal ve uluslararası düzenlemelerin içeriğinde etkili olmaktadır¹⁵⁴. Kişisel verilerin korunması hakkında rehberde düzenlenen sekiz ilke sonraki düzenlemelerde de karşımıza çıkmaktadır: veri sınırlılığı ilkesi (m.7), veri kalitesi ilkesi (m.8), belirli amaç ilkesi (m.9),

¹⁴⁹ Yılmaz, s.136.

¹⁵⁰ Hakeri, s.225-226.

¹⁵¹ Anayasa Mahkemesi Kararı – 1.B. B.2018/30296, T.7.9.2011, www.lexpera.com, (E.T.: 2.4.2023)

¹⁵² Ekonomik Kalkınma ve İşbirliği Örgütü çalışmamızın devamında OECD olarak kısaltılacaktır.

¹⁵³ OECD, **Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data**, OECD/LEGAL/0188, 23.09.1980, (erişim tarihi: 2.4.2023), <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188>

¹⁵⁴ Küzeci, s.131.

sınırlı kullanım ilkesi (m.10), veri güvenliği ilkesi (m.11), açıklık ilkesi (m.12), bireyin katılımı ilkesi (m.13), hesap verilebilirlik ilkesi (m.14)¹⁵⁵.

Birleşmiş Milletler¹⁵⁶ tarafından da kişisel verilerin korunmasına önem verilmektedir. BM Evrensel İnsan Hakları Bildirisi¹⁵⁷ m.12 hükmünde ve BM Bireysel ve Siyasal Haklar Uluslararası Sözleşmesi¹⁵⁸ m.17 hükmünde özel hayatın gizliliği hakkı düzenlenmektedir. BM İnsan Hakları Komitesi 16. Genel Yorumu¹⁵⁹ ile kişisel verilerin korunması hakkı özel hayatın gizliliği kapsamında kabul edilmektedir¹⁶⁰. BM kişisel verilerin korunmasına ilişkin çeşitli araştırmalar yapmakta ve birtakım rehber ilkeler yayımlamaktadır. BM tarafından 1990 yılında Bilgisayara Geçirilmiş Kişisel Veri Dosyalarına İlişkin Rehber İlkeleri¹⁶¹, 2015 yılında BM İnsan Hakları Konseyi “Dijital Çağda Özel Yaşamın Gizliliği Hakkı” adlı bir karar¹⁶² yayımlamıştır.

Kişisel verilerin korunması hakkında çalışmalar yürüten bir başka uluslararası kuruluş Avrupa Konseyi’dir. Avrupa İnsan Hakları Sözleşmesi¹⁶³ içerisinde kişisel verilerin korunmasına ilişkin ayrıca özel bir düzenleme bulunmamakla birlikte kişisel verilerin korunması hakkının Avrupa İnsan Hakları Mahkemesi kararlarında Sözleşme’nin Özel Hayata ve Aile Hayatına Saygı Hakkı başlıklı m.8 hükmü içerisinde değerlendirildiği görülmektedir. Mahkeme, iletişimin dinlenmesi, özel sektör ve kamu sektörü tarafından yapılan gözetimleri ve

¹⁵⁵ OECD, **Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data.**

¹⁵⁶ Birleşmiş Milletler, çalışmamızın devamında BM olarak kısaltılacaktır.

¹⁵⁷ United Nations General Assembly, Resolution 217 A, Universal Declaration of Human Rights, 10.12.1948, (erişim tarihi: 11.4.2023), <https://www.un.org/sites/un2.un.org/files/2021/03/udhr.pdf>

¹⁵⁸ United Nations General Assembly, Resolution 2200A (XXI), International Covenant on Civil and Political Rights, 16.12.1966, (erişim tarihi: 11.4.2023), https://treaties.un.org/doc/treaties/1976/03/19760323%2006-17%20am/ch_iv_04.pdf

¹⁵⁹ Birleşmiş Milletler İnsan Hakları Komitesi, **Birleşmiş Milletler’de İnsan Hakları Yorumları İnsan Hakları Komitesi ve Ekonomik, Sosyal ve Kültürel Haklar Komitesi 1981-2006**, Der. ve Çev. Lema Uyar, İnsan Hakları Hukuku Çalışmaları, İstanbul Bilgi Üniversitesi Yayınları, İstanbul, 2006, s.35-36, (erişim tarihi: 11.4.2023), https://insanhaklarimerkezi.bilgi.edu.tr/media/uploads/2016/05/05/BMde_Insan_Haklari_Yorumlari_1981_2006.pdf

¹⁶⁰ **Küzeci**, s.135.

¹⁶¹ UN General Assembly, **Guidelines for the Regulation of Computerized Personal Data Files**, 14.12.1990, (erişim tarihi: 11.4.2023), <https://www.refworld.org/pdfid/3ddcafaac.pdf>

¹⁶² UN General Assembly, **Human Rights Council, Twenty-eight session agenda item 3 (A/HRC/28/L.27)**, 24.3.2015, <https://www.ohchr.org/en/hr-bodies/hrc/regular-sessions/session28/list-reports>

¹⁶³ https://www.echr.coe.int/Documents/Convention_TUR.pdf (erişim tarihi: 20.4.2023)

kişisel verilerin depolanmasını m.8 hükmü kapsamında değerlendirmektedir¹⁶⁴. Bir kararında AIHM, muafiyet belgesinde başvurana ait sağlık verilerine izni olmadan yer verilmesini Sözleşmenin m.8 hükmüne aykırılık dahilinde değerlendirmektedir¹⁶⁵. Avrupa Konseyi’nin kişisel verilerin korunması hakkındaki temel düzenlemesi 1981 yılında kabul edilen 108 sayılı “Kişisel Verilerin Otomatik Olarak İşlenmesi Sırasında Gerçek Kişilerin Korunmasına İlişkin Sözleşme”¹⁶⁶dir¹⁶⁷. 108 sayılı Sözleşme, Avrupa Konseyi’ne üye ülkelerin dışında üçüncü ülkelerin de imzasına açık olup kişisel verilerin korunmasına ilişkin bağlayıcı nitelikteki tek uluslararası düzenleme olması ile önem arz etmektedir¹⁶⁸. 108 Sayılı Sözleşme ile kişisel verilerin korunmasını sağlamak için belirlenen asgari ilkeler verilerin belirli bir nitelikte olması (m.5), hassas verilerin özel olarak korunması (m.6), veri güvenliğinin sağlanması (m.7), ilgili kişinin bilgi alma, verilere erişim ve düzeltme hakkı (m.8) şeklinde belirtilmektedir. 108 Sayılı Sözleşme m.6 hükmünde sağlık verileri özel veri kategorileri içinde sayılmakta ve ayrıca korunması gerektiği belirtilmektedir. 1981 yılından bu yana kişisel verilerin korunması alanında birçok gelişme olması sebebiyle 108 Sayılı Sözleşmenin yetersiz kalmaya başladığı düşünülmektedir; 2018 yılında Avrupa Konseyi Bakanlar Komitesi, kendisine sunulan 108 sayılı Kişisel Verilerin İşlenmesine İlişkin Olarak Bireylerin Korunması Sözleşmesini Yenileyen Protokol Taslağını (CETS No.223)¹⁶⁹ kabul etmiştir. Bu protokol Sözleşme 108 + olarak anılmaktadır. 108 + ile daha güçlü bir veri koruma mekanizması sağlanması beklenmektedir¹⁷⁰. 108 Sayılı Sözleşmede belirlenen genel prensipler, 108 + metninde de korunmakta, bunlara ek olarak hesap verilebilirlik ve şeffaflık ilkeleri de işleme esnasında aranmaktadır¹⁷¹. Oviedo Sözleşmesi olarak da bilinen İnsan Hakları ve Biyotıp Sözleşmesi¹⁷²

¹⁶⁴ **Handbook on European Data Protection Law**, Council of Europe, European Court of Human Rights, European Data Protection Supervisor, European Union Agency for Fundamental Rights, Lüksemburg, 2018, s.23.

¹⁶⁵P.T. v. The Republic of Moldova Davası, Başvuru No: 1122/12, T. 26.05.2020, (erişim tarihi: 20.4.2023) (<https://hudoc.echr.coe.int/fre#%7B%22languageisocode%22:%5B%22ENG%22%5D,%22documentcollectionid%22:%5B%22GRANDCHAMBER%22,%22CHAMBER%22%5D,%22itemid%22:%5B%22001-202520%22%5D%7D%7D>)

¹⁶⁶ 108 sayılı “Kişisel Verilerin Otomatik Olarak İşlenmesi Sırasında Gerçek Kişilerin Korunmasına İlişkin Sözleşme”, (erişim tarihi: 20.4.2023), <https://rm.coe.int/1680078b37>

¹⁶⁷ 108 sayılı Sözleşme, 17 Mart 2016 tarihli 29656 sayılı Resmi Gazete’de yayımlanan onay kanunu ile Türkiye açısından bağlayıcı hale gelmiştir.

¹⁶⁸ **Küzeci**, s.144.

¹⁶⁹ Sözleşme 108+, (erişim tarihi: 20.4.2023), <https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1>

¹⁷⁰ **Küzeci**, s. 149.

¹⁷¹ **İmançlı**, s.22.

¹⁷² İnsan Hakları ve Biyotıp Sözleşmesi, (erişim tarihi: 20.4.2023), <https://rm.coe.int/168007cf98>

Avrupa Konseyi'nin kişisel verilerin korunmasına ilişkin bir başka düzenlemesidir¹⁷³. Söz konusu sözleşmenin m.10 hükmünde sağlık verilerinin korunması ve veri sahibinin haklarına yer verilmektedir, buna ek olarak hastalıkların sebebi olabilecek genlerle ilgili ayrıca yükümlülükler de düzenlenmektedir¹⁷⁴.

Avrupa Birliği'nin kurucu sözleşmelerinde, özel hayatın gizliliği veya kişisel verilerin korunmasına ilişkin herhangi bir hüküm bulunmamaktadır; Avrupa Birliği Adalet Divanı¹⁷⁵ tarafından, temel hak ihlalleri karşısında sözleşmeler yorumlanmış, üye devletlerin Anayasaları ve başta Avrupa İnsan Hakları Sözleşmesi¹⁷⁶ olmak üzere insan hakları sözleşmeleri esas alınmıştır. ABAD, Avrupa Birliği temel ilkelerinin bunlar ile uyumlu olacağını belirtmektedir¹⁷⁷. Avrupa Birliği Temel Haklar Şartı m.8 hükmünde kişisel verilerin korunmasına ilişkin düzenlemeler yer almaktadır. 1995 yılında 95/46/EC Kişisel Verilerin İşlenmesi ve Bu Tür Verilerin Serbest Dolaşımına Dair Bireylerin Korunması Direktifi¹⁷⁸ ile üye devletler arasında kişisel verilerin korunmasına ilişkin uyum sağlanmak istenmektedir. Avrupa'da ortak bir Pazar oluşturma düşüncesi doğrultusunda bu uyuma ihtiyaç duyulmakta ve bunun sağlıklı bir şekilde gerçekleştirilebilmesi için kişisel verilerin korunmasında da uyumun sağlanması gerekmektedir¹⁷⁹. Direktifin ilkeleri arasında; verinin kaynağını bilme hakkı, düzeltme hakkı, hukuk dışı işlemlere karşı başvuru hakkı, veri kullanımına izin vermeme hakkı yer almaktadır¹⁸⁰. Başlıca ilkeler ise m.6 hükmünde adil ve yasal işleme, amaç ile sınırlılık, ilgililik ve orantılılık, doğruluk ve güncellik, süreyle sınırlılık olarak görülmektedir. Direktif m.8 hükmünde sağlık verileri özel işleme kurallarına tabi tutulmaktadır. İlgili direktifin dışında Avrupa Birliği'nde özel düzenlemeler de mevcuttur. Örneğin; 2022/58 sayılı “Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Özel Hayatın Gizliliğinin

¹⁷³ İlgili sözleşme, 9 Aralık 2003 tarihli 25311 sayılı Resmi Gazete'de yayımlanan onay kanunu ile Türkiye açısından bağlayıcı hale gelmiştir.

¹⁷⁴ İmançlı, s.23.

¹⁷⁵ Avrupa Birliği Adalet Divanı çalışmamızın geri kalanında ABAD olarak kısaltılacaktır.

¹⁷⁶ Avrupa İnsan Hakları Sözleşmesi, (erişim tarihi: 20.4.2023), https://www.echr.coe.int/Documents/Convention_TUR.pdf

¹⁷⁷ **Handbook on European Data Protection Law**, Council of Europe, European Court of Human Rights, European Data Protection Supervisor, European Union Agency for Fundamental Rights, s.27.

¹⁷⁸ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, (erişim tarihi: 20.4.2023),

<https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML>

¹⁷⁹ Küzeci, s.183-184.

¹⁸⁰ Küzeci, s.186.

Korunmasına İlişkin Direktif¹⁸¹. Teknolojik gelişmeler ile birlikte uyum ihtiyacı Avrupa’da da gün geçtikçe artmakta, direktifler her ne kadar üye ülkelere yol göstermekte ise de doğrudan uygulamamakta, üye devletlerin iç hukukunda düzenleme yapması gerekmekte idi¹⁸². Bunun üzerine Avrupa Birliği veri koruma hukukunda bir dönüm noktası olan 2016/679 sayılı Genel Veri Koruma Tüzüğü¹⁸³’nü kabul etmiştir. Tüzüğün yürürlüğe girmesi 95/46 sayılı Direktifi mülga etmektedir. Tüzüğün m.4 hükmünde kişisel sağlık verileri tanımı yapılmakta, m. 9 hükmünde ise kişisel sağlık verileri özel nitelikli kişisel veri kapsamında değerlendirilerek koruma düzeyi genel kişisel verilerden daha sıkı tutulmaktadır.

Bunlara ek olarak sağlık verilerinin korunmasına ilişkin düzenlemelere hasta gizlilik hakkı adı altında Lizbon Hasta Hakları Bildirgesi m.4 hükmü, Amsterdam Bildirgesi m.4 hükmü, Hasta Haklarına İlişkin Avrupa Statüsü m.6 hükmü gibi birçok uluslararası düzenlemede rastlanmaktadır.

Avrupa sınırlarından çıkıldığında, ABD’de kişisel sağlık verilerinin korunması federal kanunlarla sağlanmaktadır. Health Insurance Portability and Accountability Act of 1996 (HIPAA) ile bireylerin sağlık verilerinin gizliliği hakkında çıkarları ve bu sağlık verilerinin işlenmesi ile kamu ve özel faaliyetleri gerçekleştirmenin topluma sağlayacağı çıkarlar arasında bir denge kurulması amaçlanmaktadır¹⁸⁴. Bu doğrultuda, düzenlemede kişisel sağlık verisinin işlenmesine ilişkin işleme sonucu oluşacak sosyal kazanç göz önünde bulundurularak koruma sıklığı belirlenmektedir.

¹⁸¹ 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), (erişim tarihi: 20.4.2023), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32002L0058&qid=1681980041287>

¹⁸² Akıncı, Ayşe Nur, **Avrupa Birliği Genel Veri Koruma Tüzüğü’nün Getirdiği Yenilikler ve Türk Hukuku Bakımından Değerlendirilmesi**, İktisadi Sektörler ve Koordinasyon Genel Müdürlüğü Bilgi Toplumu Dairesi Başkanlığı, 2017, s.10 (erişim tarihi: 20.4.2023), http://www.bilgitoplumu.gov.tr/wp-content/uploads/2017/07/AB_Veri_Koruma_Tuzugu.pdf

¹⁸³ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), (erişim tarihi: 20.4.2023), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679&qid=1681980103957>

¹⁸⁴ Tovino, A. Stacey, “The HIPAA Privacy Rule and the EU GDPR: Illustrative Comparisons”, **Scholarly Wokds**, 2017, s.975, <https://scholars.law.unlv.edu/facpub/1066> (erişim tarihi: 4.9.2023)

1.2.3.2. Ulusal Hukuki Düzenlemeler

2010 yılında yapılan Anayasa değişikliğine kadar kişisel verilerin korunmasına ilişkin özel bir hüküm Anayasa’da yer almamaktaydı¹⁸⁵. Anayasa “Özel Hayatın Gizliliği” başlıklı m.20/3 hükmü, kişisel verilerin korunmasını isteme hakkını düzenlemektedir. Kişisel verilerin korunmasını isteme hakkı yanında bireyler; kişisel verileri hakkında bilgilendirilme, veriye erişme, düzeltilmesini isteme, silinmesini isteme hakkına da sahiptir. İlgili hüküm kişisel verilerin korunmasına ilişkin düzenlemelerin Kanun ile yapılacağını belirtmektedir.

Hukukumuzda kişisel verilerin korunması hakkında temel düzenleme 6698 sayılı Kişisel Verilerin Korunması Kanunu’dur. Kanun m.6 hükmünde kişisel sağlık verileri, özel nitelikli kişisel veri kapsamında kabul edilmekte olup özel işleme şartları da aynı hükümde belirtilmektedir. KVKK, 95/46/EC Kişisel Verilerin İşlenmesi ve Bu Tür Verilerin Serbest Dolaşımına Dair Bireylerin Korunması Direktifi esaslı hazırlanmıştır. Fakat KVKK’nin kabulünden kısa bir süre sonra Avrupa Birliği Genel Veri Koruma Tüzüğü kabul edilmiş ve yürürlüğe girmesi ile 95/46/EC Direktifi’ni yürürlükten kaldıracağı belirtilmiştir. Avrupa Birliği içerisinde uyumun Genel Veri Koruma Tüzüğü ile sağlandığı göz önünde bulundurulduğunda hukukumuzda da Genel Veri Koruma Tüzüğü’ne uyumun ikincil düzenlemeler ile sağlanması gerekmektedir¹⁸⁶.

Kişisel verilerin korunmasını isteme hakkı bir kişilik hakkıdır¹⁸⁷. Kişilik haklarının ihlali durumunda ilgili kişi 4721 sayılı Türk Medeni Kanunu¹⁸⁸ m.23, m.24 ve m.25 hükümlerinden yararlanılabilecektir. Gerekli şartların gerçekleşmediği durumlarda kişisel verilerin işlenmesi hukuka aykırı bir fiildir, herhangi bir hukuka uygunluk sebebi olmadıkça kişisel verisi işlenmiş olan kişinin başvurabileceği dava yolları TMK m.25 hükmünde belirtilmektedir.

Kişilik haklarının ihlali durumunda ilgili kişi, zararın giderilmesi için 6098 sayılı Türk Borçlar Kanunu¹⁸⁹ hükümlerine başvurabilecektir. TBK m.49 ve devamı ya da TBK m.112 ve devamı hükümleri haksız fiil ya da borca aykırılık şeklinde uygulama alanı bulmaktadır. Söz konusu genel hükümlerin yanında işçiye ait kişisel verilerin işlenebilmesine ilişkin birtakım istisnai haller TBK m.419/1 hükmünde özel olarak düzenlenmektedir.

¹⁸⁵ İlgili değişikliği içeren Türkiye Cumhuriyeti Anayasasının Bazı Maddelerinde Değişiklik Yapılması Hakkında Kanunu 13 Ağustos 2010 tarihinde 27580 sayılı Resmi Gazete’de yayımlanmıştır.

¹⁸⁶ Akıncı, s.33.

¹⁸⁷ İmançlı, s.29.

¹⁸⁸ R.G.: T. 8.12.2001/S.24607.

¹⁸⁹ R.G.: T. 4.2.2011/S. 27836.

Kişisel Verilerin Korunması Kanunu m.14/3 hükmünde hak ihlali yaşayanların genel hükümlere dayanabileceği de belirtilmekte olup TMK ve TBK hükümlerinin kişisel verilerin korunması hakkının ihlali durumunda uygulanabileceği tekrarlanmaktadır.

5237 sayılı Türk Ceza Kanunu¹⁹⁰ m.135-139 hükümleri kişisel verilere ilişkin suç hallerini düzenlemektedir. Buna göre; kişisel verilerin kaydedilmesi, verileri hukuka aykırı olarak verme veya ele geçirme, verileri yok etmeme eylemleri TCK kapsamında suç olarak kabul edilmektedir.

Kişisel sağlık verilerine ilişkin düzenlemelerden bir diğeri de Hasta Hakları Yönetmeliği¹⁹¹'dir. Yönetmelik m.5 hükmünde kişisel sağlık verileri spesifik olarak belirtilmese de özel hayat ile aile hayatının gizliliği hakkı; m.16 hükmünde kişisel sağlık verilerinin veri sahibince talep edilebilmesi hakkı; m.17 hükmünde ise kişisel sağlık verisinin düzeltilmesini isteme hakkı düzenlenmektedir. Yönetmelik m.23 hükmünde sağlık hizmeti esnasında edinilen kişisel verilerin açıklanmamasının kural olduğu, ilgili kişinin rızası kişilik hakkından feragat anlamına geldiği durumda veriyi açıklayanın sorumluluğunun devam edeceği belirtilmektedir.

Kişisel Verilerin Korunması Kanunu'nun yürürlüğe girmesinin ardından kişisel sağlık verilerinin işlenmesine ilişkin birçok kez yönetmelik çıkarılmıştır. 20 Ekim 2016 tarihinde yürürlüğe giren Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelik iptal davasına konu edilmiş, yönetmeliğin KVK Kurumu kurulmadan ve göreve başlamadan yayımlanması sebebiyle Danıştay tarafından yürütmenin durdurulmasına karar verilmiştir¹⁹². Bunun ardından yürütmesi durdurulan yönetmelik üzerinden birtakım değişiklikler yapılarak yeniden bu yönetmelik Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetin Sağlanması Hakkında Yönetmelikte Değişiklik Yapılmasına Dair Yönetmelik şeklinde yayımlanmıştır. Ve bu yönetmelik hakkında da Danıştay *"... bir düzenlemenin tamamının yürütülmesinin durdurulması veya iptal edilmesi üzerine, bu kararın gereğini yerine getirecek yeni bir düzenleme yürürlüğe konulmadığı sürece, önceki düzenlemede kısmi değişiklikler yapılmak suretiyle hukuka aykırılığı saptanmış olan düzenlemenin canlandırılması hukuken mümkün değildir."*¹⁹³ diyerek yeniden yayımlanan yönetmeliği sakat kabul etmiş ve yürütmenin durdurulması kararı verilmiştir. 21 Haziran 2019

¹⁹⁰ R.G.: T. 12.10.2004/S. 25611.

¹⁹¹ R.G.: T. 1.8.1998/S.23420.

¹⁹² Dülger, Murat Volkan, "Kişisel Sağlık Verileri Yönetmeliğinin Yürütmesinin Durdurulmasına İlişkin Danıştay'ın 9.10.2018 Tarihli Kararına İlişkin Değerlendirme", 2021, (erişim tarihi:12.4.2023), <https://ssrn.com/abstract=3792286> (Dülger, Yönetmelik).; Danıştay Kararı, 15.D. 10488/10500, 6.7.2017 www.lexpera.com (E.T.:12.4.2023)

¹⁹³ Danıştay Kararı, 15.D. 2018/1490, 9.10.2018, (erişim tarihi: 12.4.2023), www.lexpera.com.tr

tarihinde yürürlüğe giren Kişisel Sağlık Verileri Hakkında Yönetmelik¹⁹⁴ ile söz konusu yönetmelikler yürürlükten kaldırılmıştır. KSVHY ile sağlık hizmeti sunucuları tarafından yürütülen süreç ve uygulamalara dair usul ve esasları düzenlemek amaçlanmaktadır. Yönetmelik m.4 hükmünde kişisel sağlık verisi tanımlanmakta, m.5 hükmünde kişisel sağlık verilerinin işlenmesine dair genel ilke ve esaslar belirtilmekte, kişisel sağlık verilerine kimler tarafından hangi şartlar altında erişilebileceği, m.13 hükmünde ilgili kişinin kişisel sağlık verilerinin düzeltilmesini talep hakkını nasıl kullanabileceği düzenlenmektedir.



¹⁹⁴ R.G.: T. 21.6.2019/S. 30808.

İKİNCİ BÖLÜM

KİŞİSEL SAĞLIK VERİLERİNİN İŞLENMESİ ve YAPAY ZEKA

Kişisel sağlık verilerinin, hassas veri niteliği taşımasından ötürü, özel koruma hükümleri uyarınca işlenmesi gerekmektedir. Kişisel sağlık verileri, hukukumuzdaki düzenlemeler doğrultusunda; veri kayıt sistemleri, merkezi sağlık veri sistemi, kişisel sağlık veri sistemi gibi kayıt alanlarında tutulmaktadır. Sağlık hizmeti almak için başvurulanan sağlık kuruluşu, doktor, eczane gibi birçok kişi tarafından sağlık verilerine erişim sağlanabilmekte ve sağlık verileri bu kişilerce işlenebilmektedir.

Kişisel sağlık verilerine erişimin artması yapay zekanın gelişimi için de faydalı olabilmektedir. Yapay zeka tarafından kişisel sağlık verilerinin işlenmesi sırasında uyulması gereken kurallar ve herhangi bir ihlal gerçekleşmesi durumunda oluşacak sorumluluk henüz özel hukuki düzenlemelerde yer almamaktadır. Yapay zeka ile kişisel (sağlık) verilerin(in) işlenmesine ilişkin özel bir düzenleme olmasa da mevcut veri koruma hükümleri yapay zeka ile işlemede de uygulanacaktır.

2.1. Kişisel Sağlık Verilerinin İşlenmesi

Kişisel sağlık verilerinin işlenmesi olağan hayat akışı içerisinde bir ihtiyaçtır. Tanı ve tedavinin gerçekleştirilmesi, iş hayatına başlanabilmesi ve toplum içinde yer alınabilmesi için kişisel sağlık verilerinin işlenmesi gerekmektedir.

Sağlık verilerine ilişkin müdahalelerin sınırlı olması gerektiğinden öncelikle kişisel sağlık verilerine ilişkin kavramların doğru bir şekilde tespit edilmesi ve kişisel sağlık verilerinin işlenebilmesine dair genel ilke ve şartlara uygun hareket edilmesi gerekmektedir.

2.1.1. Temel Kavramlar

Kişisel sağlık verilerinin işlenmesi esnasında birtakım temel kavramları bilmek gerekmektedir. Bu kavramlar KVKK ve KSVHY gibi yönetmelikler ile tanımlanmaktadır.

2.1.1.1. Kişisel Verilerin İşlenmesi

Kişisel verilerin işlenmesi, temel kanun olan KVKK m.3/1 (e) ve KSVHY m.4/1 (1) hükmünde “*kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her tür işlem*” olarak

tanımlanmaktadır. Kişisel verilerin işlenmesi, yalnızca kanun hükmünde sayılanlar ile sınırlı olmayıp; verinin muhafazası, sınıflandırılması ve kullanılması işlenme durumuna dair yalnızca örnektir¹⁹⁵. Kanun Gerekçesinde de kişisel verilerin işlenmesi kavramının verilerin ilk elde edildiği andan başlayarak gerçekleştirilmiş olan tüm işlem türlerini ifade eden geniş bir kavram olduğu belirtilmektedir¹⁹⁶.

Sağlık hizmetinden yararlanmak için hastaneye gidildiğinde tahlil sonucunun kayıt altında tutulması, konsültasyon için sonuçların bir başka hekim ile paylaşılması, sağlık durumunun hastanın yakınlarına açıklanması durumlarının hepsi kişisel sağlık verilerinin işlenmesi durumuna örnek olarak gösterilebilecektir.

2.1.1.2. İlgili Kişi

Kişisel Verilerin Korunması Kanunu m.3/1 (ç) ve KSVHY m.4/1 (f) hükümlerinde ilgili kişi “*kişisel verisi işlenen gerçek kişi*” olarak tanımlanmaktadır.

Kişisel sağlık verilerinin korunması söz konusu olduğunda genellikle ilgili kişi sağlık verisinin sahibi, yani sağlık hizmetinden yararlanandır¹⁹⁷. Kişinin sağlık hizmetinden yararlanırken hastanın ailesine ait sağlık öyküsünü de paylaşması gereken durumlar olabilmektedir. Hastanın doktor ile ailesine ait sağlık durumlarını paylaştığı durumlarda bu kişisel sağlık verisinin ilgili kişisi hem hasta hem de sağlık verisi paylaşılandır. Örneğin; doktora giden kişinin, kendisinde de bu hastalığın olmasından şüphelendiği bir durumda babasının bir gen hastalığına sahip olduğunu doktora aktarması. Babanın gen hastalığına sahip olması hem babanın hem de çocuğun kişisel sağlık verisidir. Dolayısıyla ilgili kişi hem sağlık hizmetinden yararlanan hem de sağlık verisi paylaşılan kişidir.

Kişisel sağlık verileri yalnızca sağlık hizmetinden yararlanırken kullanılmamaktadır. Bir spor merkezine kayıt esnasında veya bir iş ilişkisi içerisinde de sağlık verileri işlenmektedir. Bu durumda kişisel sağlık verilerinin ilgili kişisi somut olay değerlendirilerek tespit edilmelidir¹⁹⁸.

¹⁹⁵ Küzeci, s.371.

¹⁹⁶ TBMM Komisyon Raporu , s.7.

¹⁹⁷ Gürbüz Erel, İrem, **Sağlık Hukukunda Kişisel Verilerin Korunması** T.C. Kocaeli Üniversitesi Sosyal Bilimler Enstitüsü, Özel Hukuk Anabilim Dalı, Yayımlanmamış yüksek lisans tezi, Kocaeli, 2021, s.70.

¹⁹⁸ İmançlı,s.87.

2.1.1.3. Veri Sorumlusu ve Veri İşleyen

Veri sorumlusu ve veri işleyen farklı kavramlardır.

Kişisel Verilerin Korunması Kanunu m.3/1 (ı) hükmünde veri sorumlusu; “*kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi*” ifade etmektedir. Veri işleyen ise Kanunun m.3/1 (ğ) hükmünde; “*veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi*” olarak tanımlanmaktadır.

Veri sorumlusu, kişisel verinin işlenmesine dair amaç ve aracı belirlerken; veri işleyen, veri sorumlusunun verdiği yetki doğrultusunda veri sorumlusu adına kişisel veriyi işlemektedir¹⁹⁹. Veri işlenmesi sırasında veri işleyen, daha çok veri işlenmesinin teknik kısımları ile ilgilenmektedir²⁰⁰.

Veri sorumlusu ve/veya veri işleyen, gerçek kişi veya tüzel kişi olabilmektedir. Veri sorumlusu ya da veri işleyenin tüzel kişi olduğu durumlarda sorumluluk, görevi yerine getiren temsile yetkili organ veya kişiye değil; tüzel kişinin kendisine aittir²⁰¹.

Veri sorumlusu ve veri işleyenin tespiti, KVKK m.10 ve m.12 hükmünde düzenlenen yükümlülüklerin sahibinin kim olduğunun bilinebilmesi ve ilgili kişinin KVKK m.11 hükmünde belirtilen haklarını kullanabilmesi için önem arz etmektedir. Nitekim m.10 hükmünde düzenlenen bildirim yükümlülüğü için yalnızca veri sorumlusu sorumluluk sahibi iken m.12 hükmünde düzenlenen veri güvenliğine ilişkin yükümlüklerde müştereken sorumluluk söz konusudur.

Tanımdan da anlaşıldığı üzere veri sorumlusu, işlemenin amacını ve araçlarını belirleyen kişidir. Kişisel sağlık verilerinin işlenmesi durumunda sıklıkla karşılaşılabilen veri sorumluları; sağlık hizmeti sunucuları, hekimler, eczaneler, sigorta şirketleri, tıbbi laboratuvar ve görüntüleme merkezleri, işverenler ve idaredir²⁰².

¹⁹⁹ Küzeci, s.366; **Opinion 1/2010 on the concepts of “controller” and “processor”**, Article 29 Data Protection Working Party, 00264/10/EN, WP 169, 16.2.2010, s.33, (erişim tarihi: 16.4.2023), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf

²⁰⁰ Kişisel Verileri Koruma Kurumu, “Veri Sorumlusu ve Veri İşleyen, Kişisel Verileri Koruma Kurumu”, s.2, (erişim tarihi: 16.4.2023), <https://www.kvkk.gov.tr/Icerik/4195/Veri-Sorumlusu-ve-Veri-Isleyen>

²⁰¹ Dülger, Kişisel Verilerin Korunması, s.193-194.

²⁰² İmançlı, s.89-97.

2.1.1.4. Veri Kayıt Sistemi

Kişisel Verilerin Korunması Kanunu m.3/1 (h) hükmünde veri kayıt sistemi “*kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi*” olarak ifade edilmektedir. KVKK m.3 hükmü gerekçesi kişisel veri kayıt sisteminin elektronik ya da fiziki ortamda tutulan bir dosyalama sistemi olduğunu göstermektedir. Doktor tarafından bulaşıcı hastalık tanısı konan hastaların bir veri tabanına kaydedilmesi ya da kullanılan ilaca göre hastalara ait dosyalama sistemleri oluşturmaları bu duruma örnek olabilecektir.

2.1.1.5. Merkezi Sağlık Veri Sistemi

Merkezi sağlık veri sistemi, Sağlık Bakanlığı tarafından oluşturulan ve kişisel sağlık verilerinin toplandığı veri sistemidir²⁰³. Merkezi sağlık veri sistemleri ile amaçlanan herkesin sağlık durumlarının takibini ve hızlı bir şekilde sağlık hizmetlerinin etkinliğini sağlayabilmektir²⁰⁴. KSVHY m.21/3 hükmü sağlık hizmet sunucularının sahip oldukları kişisel sağlık verilerini merkezi sağlık veri sistemine göndermemesi durumunda hakkında yaptırım uygulanacağını düzenlemektedir.

2.1.1.6. Kişisel Sağlık Kaydı Sistemi

Mülga Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelik m.4/1 (e) hükmünde kişisel sağlık kaydı sistemi “*ilgili kişilerin sağlık verilerine kendilerinin veya yetki verdikleri üçüncü kişilerin erişimini sağlayan, e-devlet uygulamalarına uygun olarak kurulan sistem*” olarak tanımlamaktadır.

Kişisel Sağlık Verileri Hakkında Yönetmelik’te ise tanımlar arasında kişisel sağlık kaydı sistemine yer verilmemekte; fakat m.4/1 (d) hükmünde e-Nabız kavramı mülga Yönetmelikte tanımlanan kişisel sağlık kaydı sistemine benzer ifadeler içermektedir. İlgili hükme göre; “E-Nabız” sağlık veri sahipleri, doktorlar veya yetki verilmiş üçüncü kişilerin kişisel sağlık verilerine erişmek için kullanabileceği Sağlık Bakanlığınca kurulmuş sistemdir.

E-Nabız uygulaması insan hayatını kolaylaştırmaktadır. Hem hasta hem de hastanın izin vermesi durumunda doktorlar; hastanın eski ve güncel tetkik sonuçlarını, tanılarını ve tedavilerini görebilmektedir.

²⁰³ Kişisel Sağlık Verileri Hakkında Yönetmelik m.4/1 (r)

²⁰⁴ Kişisel Sağlık Verileri Hakkında Yönetmelik m.5/2

2.1.2. Kişisel Sağlık Verilerinin İşlenmesine Dair Genel İlkeler

Kişisel verilerin korunmasının sağlanabilmesi için ulusal ve uluslararası düzenlemelerde kişisel verilerin korunması hukukuna hakim farklı temel ilkeler yer almaktadır²⁰⁵. Kişisel verilerin işlenmesi esnasında bu temel ilkeler; veri işleme faaliyetinin uygun olması, özel (hassas) kişisel verilerin korunmasının sağlanması, veri sorumlusunun yükümlülükleri ile veri sahibinin hak ve sorumluluklarının belirlenebilmesini sağlamaktadır²⁰⁶.

Kişisel sağlık verilerinin işlenmesine dair genel ilkeler KVKK m.4 hükmünde hukuka ve dürüstlük kurallarına uygun olma; doğru ve gerektiğinde güncel olma; belirli, açık ve meşru amaçlar ile işlenme; amaç ile bağlantılı, sınırlı ve ölçülü olma; öngörülen veya gereken süre kadar muhafaza edilme şeklinde sayılmaktadır.

Kişisel Verilerin Korunması Kanunu m.4 hükmünde belirtilen genel ilkeler; genel kişisel veri için geçerli olduğu gibi özel (hassas) kişisel verileri için de geçerlidir. 2.1.2 numaralı başlık altında anlatılan tüm ilkeler, özel (hassas) kişisel veri grubunda yer alan kişisel sağlık verilerinin işlenmesi açısından da uyulması gereken ilkelerdir.

2.1.2.1. Hukuka ve Dürüstlük Kurallarına Uygun Olma

Hukuka ve dürüstlük kurallarına uygun olma ilkesi, hukuka uygunluk ve dürüstlük kurallarına uygunluk olarak iki unsurdan oluşmaktadır. Hukuka uygunluk ile bahsedilen yalnızca kişisel verilerin korunmasına ilişkin hükümlere değil, geniş kapsamda düşünülerek hukukun genel ilkelerine ve pozitif hukuk kurallarına uygun hareket edilmesidir²⁰⁷.

Kişisel verilerin korunmasının anayasal temel bir hak olduğu da göz önünde bulundurulduğunda kişisel sağlık verilerinin işlenebilmesi için işleme faaliyetlerinin kanunda açıkça öngörülmüş olması gerekmektedir.

Dürüstlük kuralı TMK m.2 hükmünde düzenlenmektedir. İlgili hükme göre; kişinin hak kullanımı ve borçlarını yerine getirmesi sırasında dürüstlük kurallarına uygun davranması gerekmektedir. Kişisel verilerin korunması bakımından dürüstlük kuralına uygunluğun sağlanması için veri işlenmesi esnasında veri sorumlusunca veri sahibinin çıkarlarını ve beklentilerini de gözeterek öngörülebilir işleme faaliyetlerinde bulunulması, aynı şekilde veri

²⁰⁵ Kişisel verilerin korunmasına hakim ilkelerine dair düzenleme örnekleri: 95/46/EC sayılı Yönerge m.6, 108 sayılı Sözleşme m.5, GDPR m.5; KVKK m.4

²⁰⁶ **Dülger**, Kişisel Verilerin Korunması, s.261.

²⁰⁷ **Dülger**, Kişisel Verilerin Korunması s.263; Kılınç, Doğan, “Anayasal Bir Hak Olarak Kişisel Verilerin Korunması”, **AÜHFD**, C. 61, S.3, 2012, s.1124.; Korkmaz, İbrahim, “Kişisel Verilerin Korunması Kanunu Hakkında Bir Değerlendirme”, **Türkiye Barolar Birliği Dergisi**, S. 124, 2016, s.100.

sahibince de veri sorumlusunun hak ve yükümlülükleri kapsamında çıkarlarını ve beklentilerini kabul ederek işlemeyi engelleyici harekette bulunulmaması gerekmektedir²⁰⁸. İşleme faaliyetlerinin, veri sahibi için şeffaf olmadığı veya veri işlenmesi hakkında bildirme ve uyarı yükümlülüklerine uygun hareket edilmediği durumlarda dürüstlük kuralına aykırılık söz konusudur²⁰⁹. Bunlara ek olarak kişisel verilerin işlenmesine dair diğer hakim ilkelere aykırı hareket edilmesi de dürüstlük kuralına aykırılık teşkil etmektedir²¹⁰. Veri sorumlusunun belirli bir amaç için topladığı veriyi amaç dışında işlemesi, gerekenden fazla veri toplaması, amacın ortadan kalkmasına rağmen veriyi yok etmemesi, veri sahibini bilgilendirmemesi ve işleme faaliyetlerinin açık belirli ve şeffaf olmaması gibi durumların da dürüstlük kuralına aykırı olduğu kabul edilmelidir²¹¹.

2.1.2.2. Doğru ve Gerekliğinde Güncel Olma

Kişisel verinin doğru ve gerektiği durumlarda güncel olmaması durumunda veri sorumlusunun veri işlemedeki belirli amacına ulaşması mümkün olmayacak ve veri işleme sırasında kişinin çıkarı ve manevi bütünlüğü zedelenebilecektir²¹².

Doğru ve gerektiğinde güncel olma ilkesi aynı zamanda veri sahibinin hakları ile de etkileşim halindedir. Kişisel veri sahibinin kişisel verilerine erişim hakkı vardır; fakat kişisel verilerin doğru olmadığı durumda kişi verilerine erişim sağlayamayacaktır, erişilemeyen kişisel veriye dair diğer hakların da kullanılması mümkün değildir²¹³. Verinin doğru veya güncel olmaması durumunda ise KVKK m.11/1 (d) hükmü uyarınca veri sahibinin yanlış veya eksikliğin düzeltilmesini talep hakkı mevcuttur.

Kişisel sağlık verileri açısından verinin doğru ve güncel olması ayrı bir öneme sahiptir. Kişinin hastalığının tespitinin ardından tedaviye başlanıldığında yaşanan gelişmeler çok önem arz etmektedir. Örneğin; bir ilaç ile tedaviye başlanmasının ardından kişinin tedaviye nasıl yanıt verdiği tedavinin ilerleyen aşamalarını da etkileyecekken; güncel olmayan veriye göre tedavinin devam ettirilmesi durumunda kişinin sağlık durumu eskisinden daha kötü hale gelebilecektir.

²⁰⁸ **Dülger**, Kişisel Verilerin Korunması s.265-266.

²⁰⁹ **Küzeci**, 230; **Kılınç**, s. 1124; **Develioğlu**, s.196.; **Özdemir**, s.137 Mendos Kuşkonmaz, Elif, **Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması**, İstanbul Üniversitesi, Sosyal Bilimler Enstitüsü, Kamu Hukuku Anabilim Dalı, Yayımlanmamış Yüksek Lisans Tezi, İstanbul, 2013, s.89.

²¹⁰ **Küzeci**, s.228; **Develioğlu**, s.44.

²¹¹ **Dülger**, Kişisel Verilerin Korunması, s.266-268; **Özdemir**, s.138, **Kuşkonmaz**, s.89.

²¹² **Dülger**, Kişisel Verilerin Korunması, s.294 ; **Develioğlu**; s.48.; **Korkmaz**, s.101.

²¹³ **Dülger**, Kişisel Verilerin Korunması, s. 294; **Özdemir**, s.139.

2.1.2.3. Belirli, Açık ve Meşru Amaçlar için İşlenme

Belirli, açık ve meşru amaçlar için işleme ilkesi ile işleme amacının sınırlandırılmasını öngörülmektedir²¹⁴. Veri sorumlusunun veri işleme faaliyetlerinde bulunma amacının açık, kesin olarak belirlenmiş ve meşru olması gerekmektedir. Amanın meşru olabilmesi için işleme amacının yasal bir temele dayanarak gerçekleştirilmesi, işleme için öngörülen tüm hukuki gerekliliklerin yerine getirilmesi ve işleme sayesinde elde edilen çıkarın toplama amacı ile uyumlu kabul edilebilmesi gerekmektedir²¹⁵. Veri sorumlusu tarafından işleme amacının belirlenmiş olması, bu amacı ve amacın uygun olduğu yasal düzenlemeyi yalnızca kendisinin bilmesi durumunda ilgili kurala aykırıdır; veri sorumlusunun işleme amacını ve dayanağını veri sahibine bildirme yükümlülüğü söz konusudur²¹⁶. Veri sahibine verisinin hangi amaçla toplandığı ve işleneceği açık ve anlaşılır bir şekilde aktarılmalıdır. Verilerin toplandığı amaçlara uygun işlenmesi gerekmektedir. Verilerin işlenebilmesi için verinin, veri sorumlusu tarafından yapılan iş veya sunulan hizmet ile bağlantılı ve bunlar için gerekli olması şarttır²¹⁷.

2.1.2.4. Amaç ile Bağlantılı, Sınırlı ve Ölçülü Olma

Kişisel verinin işlenebilmesi için belirlenen amaçla bağlantılı olması, amaç için ihtiyaç duyulandan daha az veya fazla kişisel verinin işlenmemesi gerekmektedir. Amaçla bağlantılı olma ile kast edilen, toplanan kişisel verilerin amaç ile ilişkili olmasıdır. Sağlık verileri düşünüldüğünde; sağlık hizmet sunucusunun sağlık hizmetinin gerektirdiğinden daha fazla veri işlemesi, ilkeye aykırılık teşkil edecektir. Örneğin; bir diş hastanesine gidildiğinde hastanın dişini etkilemeyecek başka hastalıklarına ilişkin verilerinin işlenmesi amaç ile bağlantılı kabul edilemeyecektir. Veri sorumlusunun toplanan veri üzerinde veri sahibine açıklanan amaçtan daha fazla işlem gerçekleştirdiği durumda amaç ile bağlantı ortadan kalkmaktadır. Bir spor merkezine kayıt esnasında toplanan sağlık verilerinin daha sonra spor merkezinin bir müşterisi tarafından üretilen bir tedavi ürününün reklamının yapılması amacı ile işlenmesi bu ilkeye aykırılık teşkil edecektir. Bir diğer örnek ise; tedavi için kişi tarafından sağlık kuruluşuna sağlanan sağlık verisinin sonradan hastanenin reklamının yapılması için kullanılamayacağıdır. Sınırlı veri işlenmesi gerekliliği asgari bir indirgeme anlamına gelmemektedir²¹⁸. Amanın

²¹⁴ **Küzeci**, s.231.

²¹⁵ Anı, Nevzat Ali, **Kişisel Verilerin İşlenmesi ve Açık Rıza**, T.C. İstanbul Üniversitesi, Sosyal Bilimler Enstitüsü, Özel Hukuk Anabilim Dalı, Yayınlanmamış Yüksek Lisans Tezi, İstanbul, 2018, s.93.

²¹⁶ **Dülger**, *Kişisel Verilerin Korunması*, s.273; **Anı**, s.93.

²¹⁷ **Dülger**, *Kişisel Verilerin Korunması*, s.278; **Anı**, s.93.; **TBMM Komisyon Raporu**, s.8.

²¹⁸ **Dülger**, *Kişisel Verilerin Korunması*, s.282.

gerçekleşmesi için yeterli olan miktarda, yalnızca amaçla ilgili veri işlenmesi gerekmektedir; aksi halde ölçülülük ilkesine de aykırılık oluşması söz konusudur ²¹⁹. Özellikle kişisel sağlık verilerinin en çok paylaşıldığı yer olan sağlık hizmet sunumu düşünüldüğünde; gerektiğinden daha az kişisel sağlık verisinin paylaşılması durumu yarardan çok zarara sebep olmaktadır. Kişinin sağlığına ilişkin birtakım verileri paylaştığı bazı verileri ise paylaşmadığı durumlarda doktor tarafından doğru teşhis konulması da doğru tedavinin uygulanması da zorlaşmakta, oluşan zorluğun da ötesinde kişinin ölümü ile sonuçlanabilmektedir.

2.1.2.5. Kanunda Öngörülen veya Gereken Süre Kadar Muhafaza Edilme

Kişisel verilerin belirlenmiş amaç için gerekenden daha uzun süre muhafaza edilmemesi gerekmektedir. Amaç gerçekleşmesine rağmen bir gün bu kişisel verilerin gerekebileceği veya bir başka amaç için kullanılabileceği düşüncesi hem ilgili ilke hem de “amaç ile bağlantılı ve sınırlı olması” gibi diğer ilkelere aykırılık teşkil etmektedir.

Kişisel verilerin elde tutulması, işlenmesi hem veri güvenliğini sağlamak yükümlülüğünden kaynaklı veri sorumlusu hem de herhangi bir ihlal durumunda uğrayabileceği zarardan kaynaklı veri sahibi için bir risk teşkil ettiğinden bu veriler mümkün olan en az süre muhafaza edilmelidir²²⁰. Kişisel verilerin muhafazasına ilişkin kanunda öngörülen süre veya amaç için gereken süre sona erdiğinde Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik hükümlerince verinin silinmesi, yok edilmesi veya anonim hale getirilerek saklanması gerekmektedir.

Kişisel sağlık verileri için hukuki düzenlemelerde farklı süreler bulunmaktadır. Fakat çoğu hukuki düzenlemede belirlenen süreler sağlık verilerini içeren kayıtların minimum tutulması gereken süreye yöneliktir²²¹.

2.1.3. Kişisel Sağlık Verilerinin İşlenme Şartları

2.1.3.1. Genel Olarak

Kişisel Verilerin Korunması Kanunu m.5/1 hükmü kural olarak genel kişisel verilerin ilgili kişinin açık rızası olmadan işlenemeyeceğini belirtmektedir. Söz konusu kural kişisel sağlık verileri için de geçerlidir. KVKK m.6/2 hükmü uyarınca da kişisel sağlık verilerinin ilgili kişinin açık rızası olmaksızın işlenememesi kuraldır. Kişisel sağlık verilerinin hiç

²¹⁹ İmançlı, s.122; Kılınç, s.1125.

²²⁰ Dülger, s.300-301; Küzeci, s. 245.

²²¹ Örneğin; Özel Hastaneler Yönetmeliği m.49; Radyoloji, Radyom ve Elektrikle Tedavi ve Diğer Fizyoterapi Müesseseleri Hakkında Kanun m.6.

işlenmemesini beklemek hayatın olağan akışına aykırı olacaktır. Örneğin; tanı ve tedavi için hastaneye başvuran hastanın geçmiş öyküsüne erişemeyen doktorun doğru tespitlerde bulunması ve doğru müdahaleyi sağlayabilmesini beklemek mümkün değildir. Yine de kişisel sağlık verilerinin hassaslığı göz önünde bulundurulduğunda, kişisel sağlık verilerine ilişkin müdahalelerin sınırlı olması gerektiğinin unutulmaması gerekmektedir²²².

2.1.3.2. İşlenme Şartları

Kanun koyucu KVKK m.5/2 hükmünde ilgili kişinin açık rızası gerekmeksizin işlenebileceği halleri saymaktadır. İlgili hükme göre “a) Kanunlarda açıkça öngörülmesi, b) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, ç) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, d) İlgili kişinin kendisi tarafından alenileştirilmiş olması, e) Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması, f) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması” hallerinde veri sahibinin açık rızası gerekmeksizin işleme yapılabilir. İlgili kanun hükmünde sayılanlar özel (hassas) veri kategorisinde yer alan sağlık verileri için yeterli değildir.

Özel (hassas) kişisel verilerinin işlenmesinde açık rıza şartı aranmayan haller KVKK m.6/3 hükmünde ayrıca düzenlenmektedir. İlgili kanun hükmünde özel (hassas) kişisel verilerin işlenme şartlarının sağlık ve cinsel hayata dair kişisel veriler ve diğer özel (hassas) veriler olmak üzere iki sınıfa ayrıldığı görülmektedir.

Kişisel Verilerin Korunması Kanunu m.6/3 hükmü uyarınca kişisel sağlık verilerinin ilgilinin açık rızası olmaksızın işlenebilmesi “kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından” işlenmesi şartlarına bağlanmaktadır. İlgili hüküm hem işleme amacı hem de veri sorumlusu olabilecek kişiler bakımından sınırlamalar içermektedir.

Sağlık verilerinin açık rıza aranmaksızın işlenebilme şartlarına dair ilgili hükümde kanunda açıkça öngörülme ibaresine yer verilmemektedir. Gerek sağlık verilerinin özel korumaya konu olması gerek temel hak ve özgürlüklerin yalnızca kanun ile sınırlandırılabilmesi ilkesi göz önünde bulundurulduğunda kişisel sağlık verilerinin

²²² İmançlı, s.84.

işlenmesinin açık rıza olmadığı durumda diğer amaçlarla birlikte işlenebilmesi için kanun ile öngörülmesi gerekmektedir²²³.

2.1.3.2.1. Açık Rızanın Varlığı

Kişisel sağlık verilerinin işlenebilmesi için temel gereklilik veri sahibinin açık rızasının varlığıdır. Burada açık ile kast edilen herhangi bir tereddüt oluşmayacak şekilde rıza verilmesidir²²⁴. Açık rıza KVKK m.3/1 (a) hükmünde “*belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza*” şeklinde tanımlanmaktadır. Bu tanım uyarınca kişisel sağlık verilerinin işlenmesi için gereken açık rıza kavramı, her iki durumda da hastanın/veri sahibinin önceden bilgilendirilmiş olması ve ardından serbestçe karar verebilmesi gerekmesi yönüyle tıbbi müdahalenin hukuka uygunluk nedenlerinden aydınlatılmış onama benzetilebilecektir²²⁵.

Açık rızanın belirli bir konuya ilişkin olma, bilgilendirilmeye dayanma ve özgür irade ile verilme olarak üç unsuru vardır. Veri sahibinin veri işlenmesine rıza verebilmesi için öncelikle neye rıza gösterdiğini bilmesi gerekmektedir. Bu sebeple veri sorumlusunun, veri sahibine işleme faaliyetine başlamadan ve rıza almadan önce veri işlenmesine dair gerekli bilgilendirmeyi yapması gerekmektedir.

Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliği²²⁶, bilgilendirmenin usul ve esaslarını düzenlemektedir. Açık rıza, bilgilendirilmenin yapıldığı anda verilememektedir. İlgili Tebliğ m.5/1 (f) hükmü aydınlatma yükümlüğü ile açık rızanın alınması işlemlerinin ayrı ayrı yerine getirilmesi gerektiğini düzenlemektedir.

Kişisel Verilerin Korunması Kanunu, veri sorumlusunun aydınlatma yükümlülüğü başlığı altında m.10 hükmünde veri sorumlusunun veya temsilcisinin kimlik bilgilerini, verilerin işleme amacını, aktarılma amacını ve aktarılacağı kişiyi, veri toplama yöntemi ve hukuki sebebini ve veri sahibinin haklarının veri sahibine açıklanması gerektiğini belirtmektedir. İlgili Tebliğ m.4 hükmünde de açık rızanın şartı olan bilgilendirilmenin şartları

²²³ Küzeci, s.376; Erarslan Türkmen, s.129.

²²⁴ KVKK Tasarı Gerekçesi, m.5 Gerekçesi

²²⁵ İmançlı, s.133-134.

²²⁶ Resmi Gazete, 28.4.2019, S.30758

aynı şekilde sayılmaktadır. Bilgilendirilmiş rızadan bahsedebilmek için bilgilendirmenin açık ve anlaşılır bir şekilde direkt veri sahibine yapılması gerekmektedir²²⁷.

Rızanın geçerli kabul edilebilmesi için belirli bir konuya ilişkin olması gerekmektedir. Veri sahibinin kişisel verilerinin işlenmesini açık uçlu ve belirsiz bir şekilde, genel irade açıklamasında bulunarak kabul ettiğini belirtmesi açık rıza olarak değerlendirilemeyecektir²²⁸. Veri sahibinin genel bir rıza anlaşması yaparak tıbbi verilerinin bir elektronik sağlık kaydı için toplanmasına ve geçmişteki ve gelecekte oluşabilecek tıbbi verilerinin tedaviye katılan sağlık çalışanlarınca kullanılmasına yönelik verdiği rıza geçerli bir rıza olmayacaktır²²⁹. Birden fazla sebeple işlemeye izin verilecek hallerde ayrı ayrı izinler alınmalı ve her bir iznin hangi kişisel veriler özelinde hangi amaçla verildiği belirtilmelidir²³⁰.

Rıza, veri sahibinin olumlu irade beyanını içermelidir²³¹. Veri sahibinin özgür iradesine dayanmayan rıza ise geçerli kabul edilemeyecektir. KVK Kurulu bir kararında özgür iradeye dayanma şartının yerine gelmesi için veri sahibinin rıza gösterdiği davranışı bilmesi ve rıza göstermenin kendi kararı olması gerektiğini; aksi takdirde cebir, tehdit, hata ve hile gibi durumlarda irade sakatlığı nedeniyle açık rızanın da sakatlanacağını belirtmektedir²³². Rızanın özgür irade ile verilip verilmediğinin özellikle hiyerarşinin mevcut olduğu ilişkilerde özenle belirlenmesi gerekmektedir²³³. Hiyerarşik ilişkiye işçi-işveren ilişkisi, doktor-hasta ilişkisi örnektir. Hasta-doktor ilişkisinde rızanın özgürce verildiğinden bahsedebilmek için veri sahibi olan hastanın verilerinin işlenmesine izin vermemesi durumunun herhangi bir şekilde tedavi hizmetine etkisi olmadığının açıkça belirtilmesi gerekmektedir²³⁴.

²²⁷ **Opinion 15/2011 on the definition of Consent**, Article 29 Data Protection Working Party, 01197/11/EN, WP187, 13.7.2011, s.20, (erişim tarihi: 16.4.2023), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf; **Anı**, s.133.; **Korkmaz**, s.108.

²²⁸ **KVK Kurumu**, Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi, Ankara, 2019, s. 48 ; Ayözger, Çiğdem, **Kişisel Verilerin Korunması (Elektronik Haberleşme Sektörüne İlişkin Özel Düzenlemeler Dahil)**, Beta Yayınları, İstanbul, 2016, s.22.; **Anı**, s.131.

²²⁹ **Working Document on the processing of personal data relating to health in electronic health records** Article 29 Data Protection Working Party, 00323/07/EN, WP131, 15.2.2007, s.9 (erişim tarihi: 18.4.2023), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp131_en.pdf ; **Develioğlu**, s.53.

²³⁰ **KVK Kurumu**, s.48.

²³¹ **KVK Kurumu**, s.47-48; **Anı**, s.148.

²³² KVK Kurulu Kararı – K.2019/165, 31.5.2019, (erişim tarihi:18.4.2023) www.lexpera.com.tr

²³³ **Dülger**, s.227.

²³⁴ **Küzeci**, s.267; **Anı**, s.140.

Özgürce verilen rıza hakkında bir diğer husus ise hizmetin kişisel verilerin işlenmesine rıza göstermesine bağlı olmamasıdır. KVK Kurulu bir kararında veri sorumlusunun üyelik sözleşmesi içerisinde kişisel verilerin işlenmesine ilişkin rızayı koşul olarak dayatmasının, hizmetin açık rıza şartına bağlanması olduğunu ve bu durumda da açık rızanın sakatlanacağını belirtmektedir²³⁵. Herhangi bir sağlık verisinin işlenmesine rıza gösterilmesinin sağlık hizmetinden yararlanmaya şart koşulduğu durumlarda da rıza geçerli olmayacaktır. Kişinin tedavi edilmeme ya da daha düşük kalitede tedavi edileceği tehdidi ile verdiği rıza özgür olarak nitelendirilemeyeceğinden açık rızanın varlığından da söz edilememektedir²³⁶.

Veri sahibi, kişisel verileri üzerinde denetim hakkı ve bilgilerinin geleceğini belirleme hakkının bir sonucu olarak²³⁷ kişisel verilerin işlenmesine ilişkin verdiği açık rızayı her zaman geri alma hakkına sahiptir²³⁸.

2.1.3.2.2. Kişisel Verilerin Korunması Kanunu m.6/3 Hükmünde Sayılan İstisna Halleri

Kişisel Verilerin Korunması Kanunu m.6/3 hükmü açık rıza aranmaksızın kişisel sağlık verilerinin işlenebileceği halleri; kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi şeklinde saymaktadır.

İşleme amacının yanında m.6/3 hükmü ile işleme faaliyeti yapabilecek kişiler de sınırlandırılmaktadır. İlgili hüküm uyarınca kişisel sağlık verileri, yalnızca sır saklama yükümlülüğü altında bulunan kişiler ya da yetkili kurum ve kuruluşlar tarafından açık rıza şartı aranmaksızın işlenebilmektedir.

Kişisel sağlık verilerine dair sır saklama yükümlülüğü altında bulunan kişilere sağlık çalışanları²³⁹, eczacılar²⁴⁰, sigorta şirketleri²⁴¹, işverenler²⁴² örnektir. Sağlık çalışanları ile kast edilen yalnızca doktorlar değildir. Doktora faaliyetleri için yardımcı olan “yardımcı personel” ve hastane işleticisi de sır saklama yükümlülüğü altındadır²⁴³.

²³⁵ KVK Kurulu Kararı – K.2020/173, 27.2.2020, (erişim tarihi:18.4.2023), www.lexpera.com.tr

²³⁶ **Working Document on the processing of personal data relating to health in electronic health records**, s.8.

²³⁷ **Dülger**, s.237; **Anı**, s.127.

²³⁸ **Küzeci**, s.271; **Anı**, s.164.

²³⁹ Tıbbi Deontoloji Nizamnamesi m.4

²⁴⁰ Türk Eczacıları Deontoloji Tüzüğü m.4

²⁴¹ 5684 sayılı Sigortacılık Kanunu m31/A

²⁴² 4857 sayılı İş Kanunu m.75/1; 6331 sayılı İş Sağlığı ve Güvenliği Kanunu m.15

²⁴³ **İmançlı**, s.153.

Kişisel Verilerin Korunması Kanunu m.6 hükmü gerekçesinden Sağlık Bakanlığı, sağlık kuruluşları ve Sosyal Güvenlik Kurumunun yetkili kurum ve kuruluşlar arasında olduğu anlaşılmaktadır.

2.1.3.2.2.1. Kamu Sağlığının Korunması

Toplumun sağlığının korunabilmesi amacıyla kişisel sağlık verileri veri sahibinin açık rızası gerekmeden işlenebilmektedir. Kamu sağlığını koruma faaliyetleri arasında bulaşıcı ve salgın hastalıkları önlemek, iş yerlerini, konutları, besini ve suyu korumak; kamunun sağlık durumunu izlemek, doğal afetlere karşı harekete geçmek, tıbbi tedavilerin kalitesini, erişilebilirliğini ve hesap verebilirliğini sağlamak gibi örnekler vardır²⁴⁴. COVID pandemisi süresince birçok sağlık verisinin herhangi bir rızaya gerek olmaksızın başta Sağlık Bakanlığı olmak üzere yetkili kurum ve kuruluşlarca işlenmesinin hukuki dayanağı olarak KVKK m.6/3 hükmünün hukuki gerekçe olarak kabul edilebileceği görüşündeyiz.

2.1.3.2.2.2. Koruyucu Hekimlik

Koruyucu hekimlik, herhangi bir hastalık olmaksızın onu engellemek veya mevcut bir hastalığın toplumda ilerlemesini durdurmayı amaçlamaktadır²⁴⁵. Koruyucu hekimlik faaliyetlerini yerine getirirken kişisel sağlık verileri herhangi bir açık rıza gerekmeksizin işlenmektedir. Örneğin; bir afet bölgesinde ortaya çıkan bulaşıcı bir hastalık üzerine bölgedeki görevli doktor ekibince bölgede yaşayan kişilere tıbbi durumlarını analiz edebilmek için sorular sorulması ve bunların kayıt altına alınması esnasında veri sahibinin açık rızası aranmamakta ve işleme faaliyeti hukuka uygun kabul edilmektedir²⁴⁶.

2.1.3.2.2.3. Tıbbi Teşhis, Tedavi ve Bakım Hizmetlerinin Yürütülmesi

Tıbbi teşhis, kişinin sahip olduğu düşünülen fiziksel veya mental bir rahatsızlığın olup olmadığını bulmak, var ise rahatsızlığın ne olduğunu tespit etmek için yapılan faaliyetlerdir²⁴⁷. Tedavi; mevcut bir hastalığın hafifletilmesi, iyileştirilmesi ya da ortadan kaldırılması için gerçekleştirilen tıbbi müdahaledir²⁴⁸. Tıbbi bakım ise yalnızca hastalık ve iyileşme durumu

²⁴⁴ Erarslan Türkmen, Sevgi, **Özel Nitelikli Kişisel Verilerin İşlenmesinde Açık Rızanın Aranmadığı Haller**, On İki Levha Yayıncılık, İstanbul, 2019, s. 175-176.

²⁴⁵ Clarke, E.A, "What is Preventive Medicine?", **Official Publication of the College of Family Physicians of Canada**, C.20, S.11, 1974, s.65.

²⁴⁶ Erarslan Türkmen, s.178.

²⁴⁷ Yenerer Çakmut, s.35.

²⁴⁸ Hakeri, s.53.

değil, hastaya sunulan sağlık hizmetini içeren süreçtir²⁴⁹. KVKK m.6/3 uyarınca teşhis, tedavi ve bakım hizmetleri amacıyla kişisel sağlık verisi işlenebilmesi için veri sahibinin açık rızası gerekmemektedir.

Kişisel sağlık verilerinin bu hüküm doğrultusunda işlenmesine; bir şikayet ile sağlık hizmet sunucusuna başvuran kişiye sağlık görevlilerince tanı konulabilmesi için gerçekleştirilen tetkik ve tahlil sonuçları, buna dayanarak konulan teşhisi ve tedaviye ilişkin bilgileri içeren bir rapor hazırlanması örnektir.

Kişisel Verilerin Korunması Kanunu m.6/3 hükmüne dayanarak hukuka uygun işleme yapıldığından bahsedilebilmesi için gerçekleştirilen işleme faaliyetinin zorunlu olması gerekmektedir. Sağlık Bakanlığınca kurulan sağlık veri sistemlerine kişisel sağlık verilerinin gönderilmesi zorunluluğuna ilişkin hükümler içeren 2015/17 sayılı Genelge Danıştay tarafından iptal edilmiştir, dolayısıyla E-nabız ve Sağlık Bakanlığı tarafından kurulmuş diğer ortak sistemler aracılığı ile kişisel sağlık verilerinin Sağlık Bakanlığına gönderilmesi zorunlu değildir ve hüküm amacı kapsamına girmemektedir²⁵⁰.

2.1.3.2.2.4. Sağlık Hizmetleri ile Finansmanının Planlanması ve Yönetimi

Sağlık hizmetleri, Sağlık Hizmetlerinin Yürütülmesi Hakkında Sağlık Bakanlığı Yönergesi m.4 (b) hükmünde “*insan sağlığına zarar veren çeşitli etmenlerin yok edilmesi ve toplumun bu etmenlerin etkilerinden korunması, hastaların tedavi edilmesi, bedensel ve ruhsal yetenek ve becerileri azalmış olanların rehabilite edilmesi için yapılan hizmetler*” olarak tanımlanmaktadır.

Kişisel Verilerin Korunması Kanunu m.6/3 hükmü uyarınca insan sağlığını korumak, tedavi ve rehabilitasyon için gereken faaliyetler ile bu faaliyetlerin finanse edilmesi için gerekli planların yapılması ve yönetilmesi sırasında kişisel sağlık verilerinin veri sahibinin açık rızası aranmaksızın işlenebilmektedir.

Özel hastanenin, sunulan sağlık hizmeti ücretini Sosyal Güvenlik Kurumu ya da sigorta şirketinden tahsis edebilmek için hastaya ait sağlık verilerini işlemesi bu duruma örnektir²⁵¹.

²⁴⁹ Childs, W. Alfred, “The Functions of Medical Care”, **Public Health Reports**, C.90, S.1, 1975, s.10, (erişim tarihi: 15.6.2023), <https://www.jstor.org/stable/4595138>

²⁵⁰ **Dülger**, *Kişisel Verilerin Korunması*, s.430.

²⁵¹ **Dülger**, *Kişisel Verilerin Korunması*, s.431.

İlgili hükümde belirtilen “sağlık hizmetleri ile finansmanının planlanması ve yönetimi” çok geniş ve soyut bir kavram olması sebebiyle ve aynı sonuca anonimleştirilmiş veriler ile de ulaşılabileceği sebebiyle eleştirilmektedir²⁵².

2.1.3.2.3. Kişisel Verilerin Korunması Kurulunca Belirlenen Önlemlerin Alınması

Kişisel Verilerin Korunması Kanunu m.6/4 hükmünce kişisel sağlık verilerinin işlenme şartlarından bir diğeri de KVK Kurulu tarafından belirlenmiş önlemlere uygun hareket edilmesidir. KSVHY m.20 hükmü ile de Kurul tarafından belirlenen önlemlere dikkat edilmesi gerektiği bir kere daha tekrarlanmaktadır.

7 Mart 2018 tarihli “Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler”²⁵³ adlı kararı ile KVK Kurulu kişisel sağlık verilerinin işlenmesi sırasında alınması gereken önlemlerin anlaşılmasını sağlamaktadır. Karar, KVK Kurumu’nun sitesinde yayımlanan Kişisel Veri Güvenliği Rehberi²⁵⁴,’nde belirtilen güvenlik düzeyini sağlamaya dair tedbirler de göz önünde bulundurularak uygulanmalıdır.

2.1.3.3. Kişisel Verilerin Korunması m.28 Hükmü ile Düzenlenen İstisnai Haller

Kişisel Verilerin Korunması Kanunu m.28 hükmünde, kanun kapsamı dışında tutulan bazı haller sayılmaktadır. İlgili hüküm uyarınca “a) *Kişisel verilerin, üçüncü kişilere verilmemek ve veri güvenliğine ilişkin yükümlülüklerle uyulmak kaydıyla gerçek kişiler tarafından tamamen kendisiyle veya aynı konutta yaşayan aile fertleriyle ilgili faaliyetler kapsamında işlenmesi, b) Kişisel verilerin resmi istatistik ile anonim hâle getirilmek suretiyle araştırma, planlama ve istatistik gibi amaçlarla işlenmesi, c) Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini, ekonomik güvenliği, özel hayatın gizliliğini veya kişilik haklarını ihlal etmemek ya da suç teşkil etmemek kaydıyla, sanat, tarih, edebiyat veya bilimsel amaçlarla ya da ifade özgürlüğü kapsamında işlenmesi, ç) Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi, d) Kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı*

²⁵² Selek, Ozan, “Genel Veri Koruma Tüzüğü Işığında Kişisel Verilerin İşlenmesinde Rıza Açıklaması”, *DEÜ Hukuk Fakültesi Dergisi*, C.21, S.2, s. 920.

²⁵³ Kişisel Verilerin Korunması Kurulu, 2018/10 s. Karar, 31.1.2018, <https://www.kvkk.gov.tr/Icerik/4110/2018-10> (E.T.: 18.4.2023)

²⁵⁴ **Kişisel Veri Güvenliği Rehberi**, Kişisel Verileri Koruma Kurumu, (Teknik ve İdari Tedbirler), (erişim tarihi: 18.4.2023), https://www.kvkk.gov.tr/yayinlar/veri_guvenligi_rehberi.pdf

makamları veya infaz mercileri tarafından işlenmesi.” hallerinde KVKK hükümleri uygulanmamakta ve işleme hukuka aykırılık teşkil etmemektedir.

Kişisel sağlık verileri bilimsel araştırmalarda da sıkça kullanılmaktadır. KVKK m.28/1 (b) hükmü bu araştırmalarda kullanılacak kişisel sağlık verilerinin anonimleştirilmesini zorunlu kılmaktadır.

Kişisel Verilerin Korunması Kanunu m.28/1 (c) hükmü de kişisel sağlık verilerinin kamu güvenliği ve düzeni gibi kamusal gerekliklerini, özel hayatın gizliliği ya da kişilik haklarını ihlal etmeden ve suç işlemek şartıyla bilimsel amaçlarla işlenebilmesine izin vermektedir.

Kişisel sağlık verileri bakımından bir değerlendirme yapıldığında, salgın hastalık ya da bulaşıcı hastalık gibi durumlarda kişisel sağlık verilerinin toplanması (ç) bendi altında düşünülebilmektedir. COVID sürecinde kişisel sağlık verilerinin işlenmesi artmıştır, m.28 (ç) hükmünde kamu sağlığına ilişkin bir hüküm bulunmaması kişisel sağlık verilerinin COVID döneminde sağlık verisi işlenmesinin bu hukuki dayanak kapsamında kabul edilip edilemeyeceğine dair birtakım düşüncelere sebep olmuştur. Bunun üzerine KVK Kurumu 27.03.2020 tarihli Kamuoyu duyurusu²⁵⁵nda mevcut durumun kamu güvenliğini ve kamu düzenini tehdit etmesi sebebiyle KVKK m.28/1 (ç) hükmü uyarınca kişisel sağlık verilerinin işlenmesinin hukuka uygun olduğunu belirtmektedir.

2.2. Yapay Zeka ile Kişisel Sağlık Verilerinin İşlenmesi

2.2.1. Genel Olarak

Algoritmalar ve makine öğrenmesine dayanan yapay zeka araçları hayatımızın her aşamasında etkili hale gelmektedir. Bankacılık, ticaret, sağlık hizmetleri yapay zekanın etkili olduğunu görebildiğimiz ve gün geçtikçe daha da etkili hale geleceği potansiyelini de öngörebildiğimiz alanlardır. Sağlık hizmetlerinde kimin sağlık hizmeti alma hakkına sahip olduğunun ya da hangi tedavinin uygun olduğunun tespitine ilişkin yapay zekadan yararlanılmaya başlanmaktadır. Sağlık hakkının önemi düşünüldüğünde bu alanda yapay zekanın tek başına karar vermesi uygun olmamakta, özellikle karar aşamasında destek bir araç olarak kullanılması fakat karar mekanizması haline gelmesine izin verilmemesi gerekmektedir.

²⁵⁵ KVK Kurumu, “Covid 19 ile Mücadele Sürecinde Kişisel Verilerin Korunması Kanunu Kapsamında Bilinmesi Gerekenler adlı Kamuoyu Duyurusu”, 27.03.2020, (erişim tarihi: 18.4.2023) <https://www.kvkk.gov.tr/Icerik/6721/KAMUOYU-DUYURUSU-Covid-19-ile-Mucadele-Surecinde-Kisisel-Verilerin-Korunmasi-Kanunu-Kapsaminda-Bilinmesi-Gerekenler->

Yapay zeka kullanımı hayatımıza birçok fayda sağlamakla birlikte birçok risk doğurabilme ihtimali de bulunmaktadır. İnsanlar, algoritmalar ve makine öğrenmesinin bu kadar yoğunlaştığı bir toplumun insan kalıp insancıl olmayı bırakması ihtimalini sorgulamaktadır²⁵⁶. Yapay zeka çağında kişisel verilerin işlenmesi de birçok olası soruna neden olmaktadır. İnternet kullanımı ile birlikte kişiler farkında olarak veya olmayarak eşi benzeri görülmemiş miktarda verisini ifşa etmekte, bu verilerin arasında sağlık verileri de yer almaktadır. Bu verilerin gözlemlenmesi ile kişinin davranış ve tercihleri tahmin edilebilmekte ve bunun sonucu olarak da ihtiyaç duymaları (ve bazen duymasalar bile) gözetim kapitalizmi altında kendilerine sunulabilmektedir. Söz konusu veri istismarı kişinin kendi verileri hakkında karar verme hakkını ihlal etmektedir²⁵⁷.

2.2.2. Yapay Zeka Tarafından Veri Kullanımı

Yapay zeka sürekli veri ihtiyacı içindedir²⁵⁸. Yapay zekanın gelişimi veri kullanımına dayanmaktadır, detaylı ve kesin bilgiler aracılığı ile yapay zekanın değeri de artmaktadır²⁵⁹. Yapay zekanın çalışabilmesi, öğrenebilmesi ve fayda sağlayabilmesi veri kullanımına bağlıdır.

Yapay zekanın öğrenebilmesi için çok fazla veri işlenmesine ihtiyaç duyulmaktadır. Teknolojik gelişmeler ile birlikte hem üretilen veriler hem de veri kullanımı artmaktadır. Anayasa Mahkemesi bir kararında ülkemizde en güçlü veri tekelinin idare olduğu, özel hayatı ve düşünce özgürlüğünü koruyabilmek için bu gücün sınırlandırılması gerektiğini belirtmektedir²⁶⁰. Veri kullanımındaki artış göz önünde bulundurulduğunda; teknolojinin gelişimiyle yapay zeka kişisel veri işlemede idareye rakip hale gelmekte hatta idareden daha fazla veriye erişebilmektedir. İdarenin de dijitalleşmeye uyum sağladığı ve bu sırada birtakım yapay zeka uygulamaları aracılığı ile de veri işlemekte olduğu görülmektedir.

²⁵⁶ Report by the Secretary General for the Ministerial Session in Helsinki, 16-17 May 2019, Ready for Future Challenges – Reinforcing the Council of Europe, Council of Europe, 2019, s.31 (erişim tarihi: 18.4.2023), <https://rm.coe.int/168093af03>

²⁵⁷ Report by the Secretary General for the Ministerial Session in Helsinki, 16-17 May 2019, Ready for Future Challenges – Reinforcing the Council of Europe, s.32.

²⁵⁸ Rasso, Filippo A./ Hilligos, Hannah/ Krishnamurthy, Vivek/ Bavitz, Christopher/ Kim, Levin, “Artificial Intelligence & Human Rights: Opportunities & Risks, Berkman Klein Center Research Publication, S.6, 2018, s.18, (erişim tarihi, 20.4.2023), <http://dx.doi.org/10.2139/ssrn.3259344>

²⁵⁹ Herve, Alan, “Data Protection and Artificial Intelligence: The European Union’s Internal Approach and Its Promotion through Trade Agreements”, Artificial Intelligence and International Economic Law: Disruption, Regulation, and Reconfiguration, ed.Shin-yi Peng, Ching-Fu Lin, and Thomas Streinz, Cambridge University Press. ss.193-214 s.196.

²⁶⁰ Anayasa Mahkeme Kararı, E. 2006/167, K.2008/86, 20.3.2008.

Bilişim ortamlarında birçok kullanıcı ve cihazlar tarafından sürekli olarak veri üretilmekte ve işlenmektedir. Verilerin veri setleri şeklinde bir araya gelmesi ile geleneksel işleme araçları ile yönetilemeyecek büyüklükte veri bütünü oluşmaktadır²⁶¹. Oluşan veri bütünlükleri, bir diğer adıyla büyük veri, yapay zekanın öğrenebilmesi için gereken veri kaynağını sağlamakta; yapay zeka da büyük verinin anlaşılmasına²⁶² yardımcı olmaktadır²⁶³. Büyük veri; toplanan ve analiz edilen veriler ile oluşan modelleri tespit etmede, grup ve toplulukların davranışlarını tahmin etmede kullanılmaktadır²⁶⁴. Büyük verinin içerisinde kişisel olmayan veriler, kişisel veriler ve kişisel sağlık verileri gibi özel (hassas) kişisel veriler yer almaktadır. Veri madenciliği ile tıbbi kayıtları da içeren veri bütünlüklerinin içerisindeki yararlı bilgiler keşfedilmekte, bunlara göre öngörü ve önerilerde bulunulması olanaklı hale gelmektedir²⁶⁵. Yapay zeka kişisel verilerden yararlanmanın yanında, yaptığı çıkarımlar sebebiyle daha fazla kişisel veri üretmektedir²⁶⁶.

Geleneksel kişisel veri işlenmesi ile yapay zeka çağında kişisel verilerin işlenmesi arasında işlemeyi gerçekleştiren kişi/mekanizma, işleme hızı ve işlenen verinin kapsamı açısından birtakım farklılıklar söz konusudur²⁶⁷. Günümüzde geleneksel yöntemlerin dışında artık kişisel veri işleme faaliyetlerinin, elektronik ve akıllı bağlantı noktaları sayesinde kişisel verilerin doğrudan gözetiminin sağlanması ve algoritmalar aracılığı ile işlenmesi ile gerçekleştirilmesi, kişisel verilerin gizliliğinin sağlanmasını zorlaştırmaktadır²⁶⁸. Örneğin; kişinin internet aracılığı ile ilaç satın aldığı veya herhangi bir hastalık belirtisine ilişkin arama yaptığı durumlarda kişinin sağlığına ilişkin belirlemeler yapılabilmekte ve kişinin sağlık verileri işlenebilmektedir. Yapay zeka çağında kişisel verilerin işlenmesi, hızı ve sayısı çok

²⁶¹ **Dülger**, Kişisel Verilerin Korunması, s.673.

²⁶² Büyük verinin anlaşılması, makine öğrenmesi sayesinde gerçekleştirilmektedir. Büyük veriden anlaşılabilir parçaların ve sonuçların çıkarılmasına veri madenciliği adı verilmektedir. **Dülger**, Kişisel Verilerin Korunması, s.674.

²⁶³ Mitrou, Lilian, “Data Protection, Artificial Intelligence and Cognitive Services: Is The General Data Protection Regulation (GDPR) ‘Artificial Intelligence-Proof?’”, 2018, s.17, <http://dx.doi.org/10.2139/ssrn.3386914>

²⁶⁴ **Guidelines on the protection of individuals with regard to the processing of personal data in a World of Big Data** Council of Europe, T-PD (2017)01, Strazburg, 23.1.2017, s.1, (erişim tarihi: 1.5.2023), <https://rm.coe.int/16806ebe7a>,

²⁶⁵ **Dülger**, Kişisel Verilerin Korunması, s.674.

²⁶⁶ **Mitrou**, s.21.

²⁶⁷ **Yılıyaer**, s146-153.

²⁶⁸ Andrew, Jane/Baker, Max, “The General Data Protection Regulation in the Age of Surveillance Capitalism”, **Journal of Business Ethics**, S.168, 2021, s.570, (erişim tarihi: 1.5.2023), <https://doi.org/10.1007/s10551-019-04239-z>

artmakta; dolayısıyla veri ihlalleri de çoğalmakta, işlenen ve oluşan veriyi korumak güçleşmektedir. Veri işleme hızı ve sayısının çok arttığı durumlarda artık müdahale de zorlaşmakta, herhangi bir ihlal söz konusu olduğunda bu durum fark edilememekte, fark edilene kadar ise birçok kaynağa yayılması söz konusu olmaktadır. Geleneksel kişisel veri işlemekten ayrılan bir başka nokta ise işlenen veri kapsamının artışıdır; nesnelerin interneti ve büyük veri gibi teknolojiler sayesinde yapay zeka çokça veri işlemesi gerçekleştirmekte ve kişileri portreleştirebilmektedir²⁶⁹. Özellikle sağlık alanında kişilerin hastalıklarını robotlar ile paylaşması durumunda oluşabilecek portreleştirme, kişisel verilerin korunması ve mahremiyete saygı açısından tehlikeler yaratabilecektir.

Kişisel verilerin korunmasına ilişkin temel düzenleme niteliği taşıyan KVKK ya da Avrupa Birliği'nin kişisel verileri koruması hukukunun temelinde olan Genel Veri Koruma Tüzüğü'nde açıkça yapay zekaya ilişkin açık bir hüküm yer almamaktadır. Fakat kişisel verilerin işlenmesine ilişkin faaliyetlerin KVKK ya da Genel Veri Koruma Tüzüğü'ne uyumlu şekilde gerçekleştirilmesi kuralı yapay zeka ile gerçekleştirilen işlemler için de esastır. Bir başka deyişle; yapay zeka ile veri işlenmesi durumunda da kişisel verilerin korunmasına ilişkin hakim ilkeler ve işleme şartlarına uygun hareket edilmesi gerekmektedir.

2.2.3. Yapay Zekanın Veri Kullanımının Ortaya Çıkardığı Sonuçlar

Kişisel verilerin yapay zeka tarafından kullanılmasının faydaları olduğu gibi bu sürecin sebep olabileceği birtakım sorunlar da vardır. Yapay zeka ile veri işlenmesi durumunda ortaya çıkabilecek sorunlara karşı tedbirler alınması gerekmektedir.

2.2.3.1. Fırsatlar

Veri işlemenin daha hızlı ve az maliyetli olması, verilerin daha verimli bir şekilde analiz edilebilmesi, yeni iş kollarının oluşmasına neden olarak ekonomiyi güçlendirebilmesi, tıbbi tanı ve teşhiste gelişim ve ilerleme sağlama, yaratıcılığı geliştirme yapay zeka ile veri işlenmesinin sağladığı fırsatlardan birkaçıdır²⁷⁰.

²⁶⁹ Yılıyaer, s.150.

²⁷⁰ Çavuşoğlu, Gökçe Filiz, **Kişisel Verilerin Yapay Zekayla İşlenmesinden Doğan Özel Hukuk Sorunları**, Yetkin Yayınları, Ankara, 2021, s.71.

Yapay zekanın yararlandığı büyük veri; toplumda yeniliklerin gerçekleşebilmesi için önemli bir değere sahip olup verimlilik, üretkenlik ve kamu sektörü performansını arttırmaktadır²⁷¹.

Sağlık bilimlerinde hızlı karar vermenin önemi açıktır. Kişisel sağlık verilerinin yapay zeka aracılığı ile işlenmesi sayesinde hastalıklar erken teşhis edilebilmekte ve birçok hastanın hayatı kurtulabilmektedir. Bunun yanında sağlık bilimleri hem hastalığın teşhisi hem tedavi hem de tedavi geliştirilmesi için gerekli olan bilimsel araştırmalar aşamasında ciddi yatırımlar isteyen bir alandır. Yapay zeka ile sağlık verilerinin işlenmesi bu ekonomik yükü hem hastanın hem de sağlık hizmet sunucularının üzerinden kaldırmaya yardımcıdır.

Kişisel sağlık verilerinin daha verimli şekilde analiz edilmesi sayesinde meydana gelebilecek hata ihtimali azalmaktadır. Bulaşıcı hastalıkların söz konusu olduğu zamanlarda yapay zeka, kişisel sağlık verilerini analiz ederek insan sağlığı riske atılmaksızın robotlar aracılığı ile sağlık hizmet sunumu gerçekleştirerek kamu sağlığını korumaktadır.

2.2.3.2. Sorunlar

Kişisel verilerin korunması hukuku bağlamında yapay zekanın yarattığı sorunlara; yapay zekayı eğitebilmek için “mümkün olduğunca fazla veri” toplanması, toplanan veriden yeni veri (t)üretilmesi, elde edilmiş verinin amaçla sınırlılık ilkesine aykırı işlenmesinin engellenememesi örnek gösterilebilmektedir²⁷². Yapay zeka aracılığı ile kişisel sağlık verilerinin işlenmesi durumunda temel ilkelerin birkaçına uyum sağlanması zorlaşmaktadır. Kişisel sağlık verilerinin işleme şartlarından olan açık rızanın varlığı şartının değerlendirilmesi de yapay zeka ile gerçekleşen işleme faaliyetlerinde sorunlu görülmektedir. Yapay zekanın temeli olan algoritmalarda sapma söz konusu olabilmekte, ayrımcılık temelli sonuçlar oluşabilmektedir.

Avrupa Konseyi Biyotıp ve Sağlık alanında İnsan Hakları Komitesi’nin bir raporu²⁷³ nda, sağlık hizmetlerinde yapay zekanın kullanılması ile birlikte doktor-hasta ilişkisinde gözlemlenebilecek etkiler; (1) Yüksek kalitede sağlık hizmetine erişimde eşitsizlik, (2) Sağlık uzmanları ve hastalar arasında yapay zeka kullanımı kaynaklı oluşan şeffaflık sorunu ve dolaylı olarak bilgilendirilmiş rıza şartına ilişkin oluşan sorunlar, (3) yapay zeka sistemlerinin sosyal

²⁷¹ **Guidelines on the protection of individuals with regard to the processing of personal data in a World of Big Data** Council of Europe, s.1.

²⁷² **Dölger**, Kişisel Verilerin Korunması, s.675.

²⁷³ **The Impact of Artificial Intelligence on the Doctor-Patient Relationship**, Council of Europe, s.4. (erişim tarihi: 1.5.2023), <https://rm.coe.int/inf-2022-5-report-impact-of-ai-on-doctor-patient-relations-e/1680a68859>

tarafılık riski, (4) hastaların refah hesabının seyrekleşmesi, (5) otomasyon kaynaklı yanlışlık, beceri kaybı ve sorumluluğun değişimi riski, (6) gizlilik hakkı üzerinde etki şeklinde belirtilmektedir.

Sağlık bilimlerinde yapay zeka kullanımının hasta gizliliği ve kişisel sağlık verilerinin korunması hakkını ihlale sebep olması durumunda, kişinin iş hayatı başta olmak üzere hayatının birçok kısmında ayrımcılığa uğrayabileceği ve uzun vadeli sağlık bakım maliyetlerinin yükselmesi durumu ile karşılaşılabilir²⁷⁴.

2.2.3.2.1. Yapay Zekanın Kişisel Sağlık Verilerinin İşlenmesine Dair Temel İlkeler Yönünden Problemler

Kişisel sağlık verilerinin işlenmesine dair dikkate alınması gereken temel ilkeler, hukuka ve dürüstlük kurallarına uygun olma; doğru ve gerektiğinde güncel olma; belirli, açık ve meşru amaçlar için işlenme; amaç ile bağlantılı, sınırlı ve ölçülü olma; kanunda öngörülen veya gereken süre kadar muhafaza edilme olarak sıralanmaktadır. İşleme faaliyetinin kim tarafından yapıldığı önemli olmaksızın bu temel ilkelere uyulması gerekmektedir.

Dürüstlük kuralına uygun veri işlemeden söz edebilmek için veri işleyen hukuka uygun bir şekilde alınmış açık rızaya ya da işleme konusunda açık bir hukuk kuralına dayanması, veri işleme faaliyetinin belirli amaç doğrultusunda en az veri işlenmesi yoluyla gerçekleştirilmesi gerekmektedir.

Kişisel sağlık verilerinin dürüstlük kurallarına uygun olarak işlendiğini söyleyebilmek için öncelikle veri sahibinin bilgilendirilmiş olması şarttır. Hasta-doktor arasındaki ilişki güvene dayanmaktadır. Bu sebeple hasta ve doktor arasında şeffaflık ve bilgilendirilmiş rıza çok önemli konseptlerdir²⁷⁵. Bununla paralel bir şekilde kişisel verilerin işlenmesi için en temel gereklilik de açık rızanın varlığıdır. Açık rızanın varlığından bahsedebilmek için öncelikle ilgili kişinin bilgilendirilmesi gerekmektedir. Yapay zeka ile kişisel verilerin işlenmesi durumunda ise çeşitli bağlantı noktaları ve algoritmalar aracılığı ile süreç devam etmektedir. Bunun sonucunda hem kişisel verilerin işlenmeye başlandığı ve diğer işlemeye ilişkin faaliyetlerin gerçekleştiği bağlantı noktaları değişebilmekte, hem de verisi işlenen kişinin doğrulanması konusunda problem söz konusu olmaktadır²⁷⁶. Kişisel sağlık verisi geleneksel zamanlarda

²⁷⁴ Wang, Chao/ Jieyu, Zhang/ Lassi Nicholas/ Zhang Xiaohan, "Privacy Protection in Using Artificial Intelligence for Healthcare: Chinese Regulation in Comparative Perspective" **Healthcare**, C.10, S. 10, 2022, s.1, (erişim tarihi: 1.5.2023), <https://doi.org/10.3390/healthcare10101878>

²⁷⁵ **The Impact of Artificial Intelligence on the Doctor-Patient Relationship**, Council of Europe, s.5

²⁷⁶ Yılıyaer, s167.

olduğu gibi yalnızca sağlık kuruluşlarının kayıtlarında bulunmamakta; giyilebilen araçlarda, dijital ve elektronik sağlık kayıt programlarında, radyolojik görüntülemelerde, ilaç şirketlerinde, sağlık araçları üreticilerinde de dağınık halde bulunmaktadır. Sağlık alanındaki büyük verilerin ölçeği ve karmaşıklığı; kişisel sağlık verilerinin nerede, kim tarafından ne amaçla kullanıldığının takip edilebilmesini zorlaştırmaktadır²⁷⁷. Bu durumlar bilgilendirmenin kapsamını ve kim tarafından yapılması gerektiğini tespitte sorun oluşturmaktadır. Klinik danışmanlık sağlayan, tanı ve tedaviye ilişkin önerilerde bulunan yapay zeka uygulamalarının kullanımında, bilgilendirmeyi doktorun mu yoksa yapay zeka üreticisinin mi yapması gerektiği gibi sorular henüz kesin cevaplanamamaktadır. Açık rızaya ilişkin bir diğer sorun ise yapay zekanın klinik tespitlerde ve önerilerde bulunduğu durumlarda ortaya çıkmaktadır. Klinik tespitlerin yapılması ve tanı konulması durumunda gerçekleştirilmesi gereken bilgilendirme aşaması yapay zekanın kullanımı ile birlikte sağlık uzmanından yapay zekaya, en azından yapay zekanın üreticisine taşınmaktadır fakat yapay zeka sistemlerinin girdileri çıktıya çevirme şeklini açıklamanın zorluğu/imkansızlığı göz önünde bulundurulduğunda hastanın yeterli ve anlaşılır seviyede bilgilendirilerek rızasının alınması sorun oluşturmaktadır²⁷⁸. Hastanın otonomisini korumak bir zorunluluktur²⁷⁹. Yapay zeka tarafından verilen kararların sağlık uzmanları tarafından çok iyi anlaşılması ve hastaya çok iyi anlaşılabilir ve değerlendirilebilir şekilde aktarılması gerektiği sağlık hizmetlerinin bir gerekliliğidir.

Yapay zeka ile veri işlenmesi durumunda karşılaşılabilecek sorunlar amaç ile sınırlılık ilkesi ve gerekenden fazla veri işlememe ilkeleridir²⁸⁰. Kişisel verilerin işlenmesine hakim ilkelerden bir diğeri de belirli, açık ve meşru amaçlar ile işlemenin yapılmasıdır. Belirli ve meşru amaç adına veriyi işleme ilkesine göre verinin, veri işleyen tarafından veri sahibine belirtilmiş amaç dışında bir amaç ile işlenmemesi gerekmektedir. Yapay zeka çoğunlukla büyük veri adı verilen veri yığınlarından yararlanmaktadır. Bu durumda verilerin işlenme amacının belirlenmesi mümkün değildir.

Veri, işlenme amacıyla bağlantılı olarak sınırlı ve ölçülü bir şekilde işlenmelidir. Bir başka deyişle amacın gerçekleşmesi için gerekli olmayan bir verinin işlenmemesi gerekmektedir. Fazla veri işlenmesi durumunda ihlalin de daha çok gerçekleştirildiği göz önünde bulundurulduğunda, bu durumun engellenebilmesi sınırlı veri işlenmesi ilkesi ile kabul

²⁷⁷ Wang/Jieyu/Lassi/Zhang, s.12

²⁷⁸ The Impact of Artificial Intelligence on the Doctor-Patient Relationship Council of Europe,, s.5.

²⁷⁹ The Impact of Artificial Intelligence on the Doctor-Patient Relationship, Council of Europe, s.18.

²⁸⁰ Özçelik, Şemsi Barış, “Yapay Zekanın Veri Koruma, Sorumluluk ve Fikri Mülkiyet Açısından Ortaya Çıkardığı Hukuki Gereksinimler”, *Adalet Dergisi*, S.66, 2021, s.96.

edilmektedir²⁸¹. Sağlık uzmanları yapay zekalara daha fazla veri sağlayabilmek adına hastalar için gerekli olmayan tetkikleri talep edebilmektedir. Gerekenden fazla veri elde edilmesi, veri ihlaline ilişkin gereksiz risk alma ve kişisel verilerin korunması hakkını ihlale sebep olmaktadır²⁸². Makine öğrenmesi sayesinde bir kez oluşturulan yapay zeka sisteminin sonraki adımlarda eylemleri dışarıdan müdahale olmaksızın gerçekleştiğinde, yapay zeka faaliyetlerine kendi karar verdiğinden, başta öngörülmemiş veriler yapay zeka tarafından toplanabilmekte ya da toplandığı amaçtan farklı amaçlarla kullanılabilir²⁸³.

Büyük verilerin işlenmesi ve analiz edilebilmesi ihtiyacı yapay zekanın doğuşu ve kullanımının artışına sebep olmuştur; çünkü büyük verinin karmaşıklığı ve hacmi düşünüldüğünde başka türlü kategorize edilmesi ve kullanılabilmesi mümkün değildir²⁸⁴. Büyük veri hayat kalitesinin sağlanabilmesi için çok önemlidir. Büyük veri ticari hayatta rahatlık ve güvenilirliği sağladığı gibi istatistik alanında da fazla katılımcı ve fazla veri aracılığıyla güvenli ve doğru sonuca ulaşabilmeyi sağlamaktadır²⁸⁵. Sağlık hizmetlerinde büyük verinin önemi ise istatistik alanına çok benzemektedir. Hastalıkların tespitinin hızlı ve daha az doktor hatasına tabi kalmasını sağlayan yapay zeka sistemleri göz önünde bulundurulduğunda, büyük veriden yararlanarak birçok hastaya ait test ve tetkikler işlenerek daha doğru ve güvenilir tanı koyma gerçekleştirilebilmekte ve önceki hastalara uygulanan tedavilere de ulaşılarak en kısa sürede en etkili sonucu verecek tedavi seçimi gerçekleştirilebilmektedir. Diğer yandan ise yapay zeka ile veri işlenmesi sonucunda açık rıza sonucu işleme yapılması, amaç ile sınırlılık ilkesi ve gerekenden fazla veri işlememe ilkesine uyumun zorlaşmasının temel nedeni yapay zekanın veri işleme esnasında büyük veriden yararlanmasıdır.

2.2.3.2.2. Algoritmada Sapma ve Ayrımcılık Riski

Yapay zeka ile kişisel verilerin işlenmesi durumunda ortaya çıkabilecek bir diğer sorun algoritma sapmasıdır. Yapay zeka tarafından veri işlenmesi algoritmalar aracılığı ile gerçekleştirilmektedir. Her ne kadar sağlık hizmetlerinde yapay zeka kullanımı ile doktor hatası riskinin azaltıldığı söylene de bu riskin tamamen ortadan kalktığını söylemek mümkün değildir; sonuçta yapay zeka da bir insan ürünüdür ve hataların oluşması mümkündür. Algoritma sapması (algorithmic bias), kullanılan algoritma türü ya da yanlış dizayn edilmiş

²⁸¹ Çavuşoğlu, s.57.

²⁸² *The Impact of Artificial Intelligence on the Doctor-Patient Relationship*, Council of Europe, s.55.

²⁸³ Özçelik, s.96.

²⁸⁴ Çavuşoğlu, s.65.

²⁸⁵ Çavuşoğlu, s.65.

algoritma sebebi ile sistemin ayrımcılık yapması ya da belli grupları ötekileştirmesi olayıdır²⁸⁶. Hatalı algoritmaya dayanarak veri işleyen yapay zeka rıza olmaksızın veri işleyebilmekte ya da verinin rıza dışında bir faaliyete uğramasına sebep olabilmektedir²⁸⁷.

Ayrımcılık riski yapay zekanın veri işlemesi ile oluşabilecek bir başka sorundur. Ayrımcılık riski ayrı bir sorun olmanın ötesinde algoritmada oluşan sapmanın bir sonucu da denilebilecektir. Yapay zeka veri ile beslenmesinin yanı sıra bu verilerden öğrenmekte, çıkarımlarda bulunmakta ve de yeni veriler üretmektedir. Yapay zekanın verileri işlemesi sonucunda yeni veriler veya sonuçlar ortaya koyması durumunda bazı ayrımcılık sorunları oluşabilmektedir. 1.1.3.1 başlığında anlatılan COMPAS ve TAY buna örnektir.

Yapay zekanın ayrımcı davranışları kendi içerisinde yarattığı bir durum değildir. Yapay zeka makine öğrenmesi sırasında kendisine eğitici veri olarak yüklenen veriler ile öğrenmeye başlamakta ardından bunlar arasında bir örüntü yaratarak öğrenme yolculuğuna devam etmektedir. Buradan da anlaşılacağı üzere yapay zekanın ayrımcı davranabilmesi için eğitici verilerin önyargılı olması gerektiği sonucu ile karşılaşıldığı görülmektedir²⁸⁸.

Yapay zekanın taraflılığı her alanda çok büyük sonuçlar doğurmayabilecek olsa da sağlık alanı için önem arz etmektedir. Yapay zeka tarafından hastalık teşhisine karar verilirken taraflı ve önyargılı davranırsa kişinin yaşam hakkına müdahale söz konusu olacaktır²⁸⁹.

2.2.3.2.3. Yapay Zeka Aracılığı ile Yapılan Çıkarımlara İlişkin Sorunlar

Yapay zeka yalnızca kişisel veriden yararlanmakla kalmamakta aynı zamanda bu verileri anlamlı hale getirmekte, yeni verilerin oluşmasına da neden olmaktadır. Örneğin; tetkikler arasından kişinin teşhisinin konulabilmesini sağlayan bir yapay zekanın çıkardığı bu hastalık sonucu yeni üretilmiş bir kişisel veridir²⁹⁰. Çıkarımlarda bulunan yapay zekaya Amazon'un öksürük sesine göre hastalık tahmininde bulunan ve ilaç önerisinde bulunabilen

²⁸⁶ Kuśmierczyk, Małgorzata, "Algorithmic Bias in the Light of the GDPR and the Proposed AI Act", Ed. Maciej Olejnik, Wiktoria Morawska, **(In)equality. Faces of modern Europe**, Wydawnictwo Centrum Studiów Niemieckich i Europejskich im. Willy'ego Brandta, Wrocław, s.2, (erişim tarihi: 3.5.2023), <http://dx.doi.org/10.2139/ssrn.4117936>

²⁸⁷ Çavuşoğlu, s.65.

²⁸⁸ Çavuşoğlu, s.78.

²⁸⁹ Yılıyaer, s.159.

²⁹⁰ Yapay zeka aracılığı ile yapılan çıkarımların kişisel veri olarak kabul edilip edilmeyeceği konusu tartışmalıdır. Nitekim Madde 29 Çalışma Grubu tarafından kişisel veri olarak kabul edilmekte ve kişisel veri koruma hukukuna ilişkin dikkat edilmesi gerekenler bu çıkarımlar için de geçerlidir. Avrupa Birliği Adalet Divanı tarafından ise bu verilerin durumu belirsiz kabul edilmektedir. Yılıyaer, s.163-164.

Alexa ürünü²⁹¹ örnektir. Yapay zekanın tahmin edilemezlik özelliği göz önünde bulundurulduğunda, hastalık analizi yaparken kişinin başka kişisel verilerine dair analizler de gerçekleştirilmesi söz konusu olabilmekte, bu şekilde gerçekleştirilen çıkarımlar ise kişisel verilerin korunması hakkının ihlali anlamına gelmektedir²⁹². Bir başka deyişle, kişinin hastalığının tespiti için verilerinin kullanımına rıza gösterdiği durumda onay verilenin dışında kişisel veriler de yapay zeka tarafından analiz edilip işlenebilmekte, bu durum ise belirli amaç doğrultusunda işleme ilkesinin ihlaline yol açmaktadır.

Gelişmiş bilgisayar programları ve yapay zeka liderliğindeki büyük verinin kişisel verilerden özel bilgi niteliği taşıyan çıkarımlarda bulunduğu algoritmik tahmin sürecinde, artık önemli olan kullanılan verinin kendisinin yanında yapay zeka algoritmasının yaptığı çıkarımdır. Algoritmalar tarafından oluşturulan yardımcı teşhis ve tedaviye ilişkin algoritmik tahminler sayesinde artık temel veri doğrudan bilinmese de veri ihlallerinin oluşması riski oluşmakta olup derin öğrenme algoritmaları tarafından gerçekleştirilen tahminlerin sonucunun da asıl verinin devamı olarak görülmesi ve hukuk tarafından korunması gerekmektedir²⁹³.

Yapay zeka çağında çıkarımlar yoluyla da birçok sağlık kişisel verisi oluşmaktadır. Çıkarım ile ortaya çıkan kişisel verilerin gizliliğine ilişkin tehditler her zaman öngörülememektedir özellikle bu öngörülememezlik sebebiyle sağlık verileri gibi hassas verileri koruma konusunda etkili önlemlerin alınması gerekmektedir²⁹⁴.

Nesnelerin interneti ve akıllı şehirler aracılığı ile kişinin sağlık durumu; izleme cihazları ile uyku ve egzersiz alışkanlık takibi; yorgunluk algılama sistemleri ile kişinin sağlık durumunu ortaya koyan çıkarımlarda bulunulabilen yapay zeka uygulamalarının varlığı söz konusu olup; çıkarım yolu ile bu hassas verilere ulaşılmasını sağlayan diğer veri türlerinin de hassas veri gibi korunması ihtiyacı doğmaktadır²⁹⁵.

²⁹¹ Spanu, Anca, “Amazon’s new Alexa will know someone is sick by listening to their voice” **Healthcareweekly**, 10.10.2018, <https://healthcareweekly.com/amazon-alexa/> , (erişim tarihi:2.5.2023) ; Cook, Jamesi: “Amazon Patents New Alexa Feature That Knows When You’re Ill and Offers You Medicine”, **The Telegraph**, 09.10.2018, <https://www.telegraph.co.uk/technology/2018/10/09/amazon-patents-new-alexa-feature-knows-offers-medicine/>

²⁹² Çavuşoğlu, s.79.

²⁹³ Wang/Jieyu/Lassi/Zhang s.12.

²⁹⁴ Yılıyaer, s.170.

²⁹⁵ Yılıyaer, s.168-169.

2.2.3.2.4. Sorumluluk

Yapay zeka aracılığı ile kişisel veri işlenmesi sırasında oluşabilecek veri ihlalleri, gerekli olandan fazlası verinin toplanması ya da veri sahibinin haberi olmaksızın veri toplanması durumunda toplama aşamasında; verinin toplanmasının ardından farklı platformlarda paylaşılması veya uygun olmayan şekilde kullanılması durumunda ya da algoritmik tahmin aşamasında ortaya çıkabilmektedir²⁹⁶. Yapay zeka sistemleri; yapay zeka geliştiricisi, üreticisi, kullanıcı gibi birçok faktörü içermektedir; fazla faktör içeren yapay sistemin beklenmeyen şekilde davranışlar sergilemesinde, zararı tespit edip sebeplerini bulmak; dolayısıyla da sorumluluğu tespit etmek pek de kolay olmamaktadır²⁹⁷.

Yapay zeka aracılığı ile kişisel veri işlenmesinin sorumluluk yönünden yarattığı bir diğer sorun ise, uygulama ve müeyyide mekanizmalarındaki eksiklik sebebiyle yeterli etkin koruma oluşturulamayacak; sorumluluğa sebebiyet verebilecek şekilde insana zarar veren potansiyel sonuçlar ile yapay zeka sistemleri arasında sorumluluk boşluğu meydana gelebilecektir. Yapay zeka ile birlikte sürece birçok birey, organizasyon, makine, algoritma ve kullanıcının katılımı, insan-bilgisayar etkileşimi ve algoritmanın tahmin edilemezliği sorunundan ötürü belirsiz bir hız ve ölçüde felaket risk senaryoları oluşabilmektedir²⁹⁸.

2.2.4. Sorunlara İlişkin Kabul Edilebilecek İlke ve Stratejiler

Yapay zeka aracılığıyla kişisel verilerin işlenmesinin yaratabileceği sorunlar birçok ülke için kaygı konusudur. Oluşabilecek sorunları ve buna ilişkin önerileri içeren uluslararası belgeler, raporlar ve ulusal strateji planları da mevcuttur. Kişisel verilerin işlenmesi durumu için önleyici yaklaşım benimsendiği görülmektedir²⁹⁹. Kişisel verilerin korunmasına ilişkin

²⁹⁶ Wang/Jieyu/Lassi/Zhang s.12.

²⁹⁷ **The Impact of Artificial Intelligence on the Doctor-Patient Relationship**, Council of Europe, s.15.

²⁹⁸ Council of Europe, Parliamentary Assembly, **Artificial Intelligence in health care: medical, legal and ethical challenges ahead**, Doc.15154, 22.10.2020, s.15, (erişim tarihi: 3.5.2023), <http://www.assembly.coe.int/LifeRay/SOC/Pdf/TextesProvisoires/2020/20200922-HealthCareAI-EN.pdf>

²⁹⁹ Çekin, Mesut Serdar, “6698 sayılı Kişisel Verilerin Korunması Hakkında Kanun’un Big Data (Büyük Veri) ve İrade Serbestisi Açısından Değerlendirilmesi”, **İÜHFİM**, C.74, S.2, 2016, s.641-642.; **Guidelines on the protection of individuals with regard to the processing of personal data in a World of Big Data**, Council of Europe, s.3.

benimsenmiş olan bu yaklaşım yapay zeka kullanımında da aynı şekilde uygulanabilmektedir³⁰⁰.

Avrupa Konseyi 2019 yılında yapay zeka ve kişisel verilerin korunmasına ilişkin bir kılavuz³⁰¹ yayımlamıştır. Söz konusu kılavuz yapay zeka geliştiricileri, üreticileri ve hizmet sağlayıcılarının dikkat etmesi gereken birtakım durumları içermektedir. Buna göre; veri işlemenin tüm aşamalarında yapay zeka geliştiricileri, üreticiler ve hizmet sağlayıcılarının insan haklarına uygun yaklaşım belirlemesi, kasıtsız ve gizli olsa dahi olası önyargılardan ve ayrımcılık riskinden kaçınmaları gerekmektedir. Yapay zeka geliştiricileri, süreç içerisinde kullanılması gereken veriyi tespit edip gereksiz veri kullanımından kaçınılmalıdır. Yapay zeka geliştiricileri, gizlilik ihlalini engellemek için sentetik veriler kullanılması önerilmektedir. Sentetik veri, gerçek verileri yaymak yerine, popülasyon modellerinden üretilmiş verilerin yayımlandığı bir gizlilik yaklaşımıdır³⁰². Yapay zeka geliştirici, üretici ve sağlayıcıları bağımsız akademik kuruluşlar aracılığıyla kullanılan algoritmalarda herhangi bir sapma olup olmadığını tespit etmesi sağlanabilecektir. Bu sayede şeffaflık sorununa bir çözüm getirilebilecektir. Bir diğer dikkat edilmesi gereken unsur kişinin kendi karar alma özgürlüğüne çok müdahale edilmemesidir. Bir başka deyişle; otomatik karar alan yapay zeka uygulamalarından kaçınılması gerekmektedir. Yapay zeka geliştiricileri, üreticileri ve hizmet sağlayıcılarının, ürün ve hizmetlerinde yapay zeka uygulamalarına alternatifler sunması ve kullanan kişiye seçim özgürlüğü tanınması kullanıcıların güvenini artıracaktır. Yapay zeka geliştirici, üretici ve hizmet sağlayıcıları hesap verebilirliği destekleyen algoritma gözetimi benimsemelidir.

Sağlık bilimlerinde yapay zeka kullanımı, sağlık hizmetlerinde ilerleme sağlamanın yanı sıra; ihtiyaç duyduğu veri büyüklüğü sebebiyle şeffaflık ve hasta güveni konusunda birtakım kaygılar doğurmaktadır. Yapay zekanın tahmin yeteneği mahremiyet ve ayrımcılık ile ilgili de endişelere sebep olmaktadır³⁰³.

Yapay zekanın sağlık hizmetleri alanına girişi ile birlikte, hastanın konumu, hastanın sağlık ile ilgili arayışı ya da hassasiyeti değişmemekte, bu durumda yalnızca sağlık hizmetini

³⁰⁰ **Guidelines on Artificial Intelligence and Data Protection**, Council of Europe, T-PD(2019)01, Strazburg, 25.1.2019, s. 21. (erişim tarihi 3.5.2023), <https://rm.coe.int/guidelines-on-artificial-intelligence-and-data-protection/168091f9d8>,

³⁰¹ **Guidelines on Artificial Intelligence and Data Protection**, Council of Europe, T-PD(2019)01, Strazburg, 25.1.2019, <https://rm.coe.int/guidelines-on-artificial-intelligence-and-data-protection/168091f9d8>

³⁰² https://ec.europa.eu/eurostat/ramon/coded_files/OECD_glossary_stat_terms.pdf

³⁰³ **Strategic Action Plan on Human Rights and Technologies in Biomedicine (2020-2025)**, Council of Europe, s.8-9, (erişim tarihi: 4.5.2023) <https://rm.coe.int/strategic-action-plan-final-e/1680a2c5d2>

sağlayan değişmektedir³⁰⁴. Dolayısıyla hasta hakları ve bu doğrultuda hastanın mahremiyeti ve kişisel verilerinin korunmasını isteme hakkının varlığı devam etmektedir. Oviedo Sözleşmesi m.4 hükmüne göre sağlık hizmeti sunucularının bağlı olduğu mevcut standartlar gibi yapay zeka uygulamalarını hazırlayan geliştirici, üretici ve servis sağlayıcılar için de sağlık alanında gerçekleşecek herhangi bir müdahalede belirli standartlar olması gerekmektedir³⁰⁵. Eskiden var olan hasta-doktor ilişkisi yerini hasta-doktor-yapay zekaya bırakmaktadır. Bu noktada yapay zekanın kişisel sağlık verilerini kullanması ile insan hayatına sağlanan katkı da göz önünde bulundurularak kişisel verilerin korunması hakkı ile yenilik yaratma ihtiyacı arasında bir denge kurulması gerekmektedir. Sağlık ve mahremiyet, dolayısıyla kişisel verilerin korunması hakkı, hiçbir zaman birbirinin alternatifi olarak görülmemelidir, aksine her zaman birbirlerini destekler nitelik taşınmalıdır³⁰⁶. Yapay zekanın eğitilmesi ve test edilmesi için veri kullanımında, yeni amaçla veri kullanımı ve veriye üçüncü Kişiler tarafından erişimi ile oluşabilecek birçok sorunun olmasının yanında alınabilecek tedbirler vardır.

2.2.4.1. Tasarımda Gizlilik (Privacy by Design) ve Varsayılanlarda Gizlilik (Privacy by Default)

Yapay zeka çağında kişisel verilerin korunması amacıyla önleyici yaklaşım benimsendiğinin en önemli göstergeleri tasarımda gizlilik ve varsayılanda gizlilik ile risk değerlendirmeleridir.

Tasarımda Gizlilik (Privacy by design), Genel Veri Koruma Tüzüğü m.25 hükmü ve resital 78’de yer bulmaktadır. Tasarımda gizlilik, kişinin kendisine veya içerisinde bulunduğu gruba dair fiziksel, sosyal, psikolojik ve bilgisel erişimi kontrol etme ve sınırlama hakkına ilişkin gerekliliklerin süreç başından itibaren düzenli ve kurallı bir şekilde işlemesi şeklinde hukuki gizlilik kavramı ile bilgi teknolojilerinin sınırlarının arasında bir tanıma sahip olabilecektir³⁰⁷. Tüzük maddesine göre veri sorumlusunun, veri işlemesi faaliyetinin mahiyeti, kapsamı, bağlamı ve amaçlarının yanında bu faaliyetler esnasında ilgili kişi açısından oluşabilecek olasılıklar ve riskleri dikkate alması, işleme faaliyetleri başlamadan veri minimizasyonu ilkesi gibi ilkelerin etkili bir şekilde uygulanması ve kişisel verilerin

³⁰⁴ **The Impact of Artificial Intelligence on the Doctor-Patient Relationship**, Council of Europe, s.4.

³⁰⁵ **The Impact of Artificial Intelligence on the Doctor-Patient Relationship**, Council of Europe, s.5; s.24-25.

³⁰⁶ **Artificial Intelligence in health care: medical, legal and ethical challenges ahead** Council of Europe, s.4.

³⁰⁷ Carboni, Andrea/Russo,Dario/Moroni, Davide/Barsocchi, Paolo, “Privacy by design in systems for assisted living, personalised care and wellbeing: A stakeholder analysis”, **Frontiers in Digital Health**, C.4, 2023, s. 2, <https://www.frontiersin.org/articles/10.3389/fdgth.2022.934609/full>

korunmasına ilişkin gerekliliklere uygun davranılmasına ilişkin güvencelerin entegre edilmesi için uygun teknik ve organizasyonel tedbirleri uygulaması gerekmektedir. Uygulanabilecek tedbirlere örnek olarak; kişisel verilerin takma ad ile saklanması, kişisel verilerin yapılandırılmış ve yalnızca makine tarafından okunabilir formatta saklanması, veri sahipleri tarafından veri işlemeye müdahale edilmesine uygun hareket edilmesi, kişisel verinin işlenmesine ilişkin bilgilendirme yapılması, veri işleyenleri veri minimizasyonuna uygun hareket etme konusunda yükümlü kılacak sözleşmeler yapılması; iç politikalar benimsenmesi, veri koruma konularına ilişkin güncel eğitimler verilmesi gösterilebilecektir³⁰⁸. Alınabilecek tedbirlerin yeterli olup olmadığının tespiti, günün teknolojik koşulları ile ilişkilidir; teknolojinin gelişmesi ile birlikte veri sorumlusunun tasarımda gizlilik bünyesinde aldığı tedbirleri de günün koşullarına uygun teknoloji şartlarına uyumlu hale getirmesi beklenmektedir³⁰⁹.

Tasarımda gizlilik ilkesinin uygulanabilmesi için veri sorumlusu; kişisel verilerin korunmasına ilişkin ilkelerine karşı riskleri, bu risklerle karşılaşma ihtimallerini ve bunlara karşı hafifletici önlemleri belirlemelidir³¹⁰. Veri sorumlusu bu risklerin belirlemenin yanında veri sahibini veri işleme sürecine ilişkin anlaşılabilir şekilde bilgilendirmelidir. Bu bilgilendirmenin içerisinde, veri sahibinin muhatabının yapay zeka olduğu da yer almalıdır³¹¹.

Varsayılanlarda Gizlilik (Privacy by default) ürün veya hizmetin son kullanıcıya ulaşmadan önce gizlilik kurallarının, bir başka deyişle kişisel verilerin korunması hukukunun, otomatik olarak uygulanmış ve buna uygun şekilde faaliyet göstermeye hazır halde olmasıdır³¹². Genel Veri Koruma Tüzüğü m.25/2 hükmü veri sorumlusunun kişisel verilerin işlenmesi, saklanması ve ulaşılabilirliği yönünde korumanın sağlanabilmesi için gereken teknik ve organizasyonel tedbirleri varsayımsal olarak eklemesi gerektiğini ifade etmektedir. Büyük veri dünyasında kişisel verilerin işlenmesi durumunda veri sorumlusu ve veri işleyenin işleme faaliyetinin her aşamasında varsayılan gizlilik ile uyumlu hareket etmesi beklenmektedir.

³⁰⁸ **Guidelines 4/2019 on Article 25 – Data Protection by Design and by Default**, European Data Protection Board, 13.11.2019, s.6,8., (erişim tarihi: 12.5.2023), https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf

³⁰⁹ **Guidelines 4/2019 on Article 25 – Data Protection by Design and by Default**, European Data Protection Board, s.8.

³¹⁰ **Guidelines 4/2019 on Article 25 – Data Protection by Design and by Default**, European Data Protection Board, s.9.

³¹¹ Öğretmen Kotil, Zeynep, **Kişisel Verilerin Korunması Çerçevesinde Yapay Zeka**, On İki Levha Yayıncılık, İstanbul, 2022, s.190.

³¹² **Carboni/Russo/Moroni/Barsocchi**, s.2-3.

Burada kast edilen mevcut verinin en az seviyede tutulması; herhangi bir olası gizli taraflılık ya da ayrımcılık veya kişinin temel hak ve özgürlüklerine müdahale anlamına gelebilecek her türlü işlemde hem toplama hem de analiz aşamalarında kaçınması gerektiğidir³¹³. Teknik olarak mümkün olduğu sürece, veri sorumlusu ve var ise veri işleyen tarafından varsayılan gizlilik koşulları öncelikle az miktarda veri üzerinde simülasyon ile test edilmeli, ardından yüksek miktarda veri üzerinde kullanılmalıdır; bu sayede olası taraflılık daha kolay tespit edilebilecek, veri minimizasyonuna dair delil elde edilmiş olacak ve risk etki değerlendirmesinde karşılaşılabilecek olumsuz sonuçlar azaltılmış olacaktır³¹⁴. Hassas kişisel verilerin korunması için daha sıkı tedbirler alındığı bilinmektedir. Sağlık verilerinin de içerisinde yer aldığı hassas kişisel verilerin kullanılması durumunda uygulanan varsayılan gizlilik yaklaşımı, aynı zamanda hassas kişisel verilere ulaşılmasını sağlayan genel kişisel veriler için de geçerli olmalıdır³¹⁵.

2.2.4.2. Veri Koruma Etki Değerlendirmeleri ve Yapay Zeka Etki Değerlendirmeleri

Yapay zeka çağında kişisel verilerin işlenmesine ilişkin benimsenen yaklaşımın yalnızca önleyici değil aynı zamanda risk odaklı da olduğu veri koruma etki değerlendirmesi etkisi ile görülmektedir. Veri koruma etki değerlendirmeleri, Genel Veri Koruma Tüzüğü ile birlikte karşımıza çıkmaya başlamış bir durumdur. Genel Veri Koruma Tüzüğü, kişisel verilerin korunmasına ilişkin ortaya çıkan teknolojik gelişmeler kaynaklı sorunlara etkin koruma sağlamayı amaçlamaktadır³¹⁶. Bu amacı gerçekleştirmek için başvuru yollarından birisi de bazı durumlarda kişisel verilerin işlenmesine ilişkin faaliyeti gerçekleştirmeden önce, veri sorumlusu tarafından veri koruma etki değerlendirilmesinin gerçekleştirilmesidir. Hukukumuzda kişisel verilerin korunmasına ilişkin temel düzenleme olan KVKK'de veri koruma etki değerlendirmesine ilişkin açık bir hüküm bulunmamakla birlikte KVK Kurumu'nun 2019/78 no'lu kararında doğrudan hesap verilebilirlik ilkesine yer verilmekte,

³¹³ **Guidelines on the protection of individuals with regard to the processing of personal data in a World of Big Data**, Council of Europe, s.4.

³¹⁴ **Guidelines on the protection of individuals with regard to the processing of personal data in a World of Big Data**, Council of Europe, s.4. ; **Guidelines on Artificial Intelligence and Data Protection**, Council of Europe s.25.

³¹⁵ **Guidelines on the protection of individuals with regard to the processing of personal data in a World of Big Data**, Council of Europe, s.4.

³¹⁶ **Opinion of the European Data Protection Supervisor on the Data Protection Reform Package**, European Data Protection Supervisor, 2012, s.2, (erişim tarihi:12.5.2023), <https://rm.coe.int/guidelines-on-artificial-intelligence-and-data-protection/168091f9d8>

Yapay Zeka Alanında Kişisel Verilerin Korunmasına Dair Tavsiyeler içerisinde de kişisel veri işlemeye dayalı yapay zeka uygulamalarında veri korunmasına ilişkin yüksek risk öngörülmüşse mahremiyet etki değerlendirmesi yapılması gerektiği belirtilmektedir³¹⁷.

Veri koruma etki değerlendirmeleri; veri işleme faaliyetlerini tanımlama, gereklilik ve ölçülülükü değerlendirme ve işleme faaliyetinin gerçek kişinin hak ve özgürlükleri üzerinde oluşturabileceği riski hesaplamaya yardımcı bir süreçtir³¹⁸. Her veri işleme faaliyetinden önce veri koruma etki değerlendirmesine başvurma zorunluluğu yoktur. Genel Veri Koruma Tüzüğü m.35 hükmü uyarınca yüksek risk bulunan veri işleme hallerinde veri koruma etki değerlendirmesine başvurulması zorunlu tutulmaktadır. Yüksek riskin varlığı olan haller; otomatik işlemeye dayanan ve gerçek kişiyle ilgili yasal sonuçlar doğuran ya da kişiyi önemli ölçüde etkileyen kararların dayandığı gerçek kişilerle ilgili kişisel verilerin kapsamlı ve sistematik bir şekilde değerlendirildiği durumlar, büyük oranda özel nitelikli (hassas) verilerin işlendiği ya da mahkumiyet kararları ve güvenlik tedbirleri ile ilgili kişisel verilerin işlenmesi gereken durumlar, kamuya açık alanların sistematik olarak gözetlenmesi durumları olarak belirtilmektedir.

Sağlık verileri, özel nitelikli (hassas) kişisel veri arasında yer almaktadır. Dolayısıyla sağlık verilerinin işlenmesine ilişkin faaliyette bulunmadan önce veri sorumlusu tarafından veri koruma etki değerlendirmesi yapılması ve buna ilişkin raporun veri koruma otoritesine sunulması gerekmektedir. Veri sorumlusunun belirlenen riski kabul edilebilir seviyelere indirgeyecek önlemleri alamadığı durumlarda, veri koruma otoritesine danışması gerekmektedir³¹⁹. Bir hastaneye bağlı olmaksızın çalışan özel hekimin sağlık verisini işlemesi durumunda ise herhangi veri koruma etki değerlendirmesi yapılması gerekmemektedir³²⁰.

Yapay zekaya dayalı sağlık uygulaması projesinde veri işlenmesine ilişkin hazırlanabilecek veri koruma etki değerlendirmesi veri bazlı değerlendirme, veri sahibi bazlı

³¹⁷ Bayram, Öykü Beste, “Bir Uyum Aracı Olarak Veri Koruma Etki Analizinin Türk Hukuku Bakımından Değerlendirilmesi”, *Kişisel Verileri Koruma Dergisi*, C.4, S.1, 2022, s.48-49.

³¹⁸ **Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for purposes of Regulation 2016/679**, Article 29 Data Protection Working Group, 17/EN, WP 248 rev.01, 4.10.2017, (erişim tarihi: 15.5.2023), https://iapp.org/media/pdf/resource_center/WP29-GDPR-DPIA-guidance_final.pdf

³¹⁹ **Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for purposes of Regulation 2016/679**, Article 29 Data Protection Working Group, s.19.

³²⁰ **Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for purposes of Regulation 2016/679**, Article 29 Data Protection Working Group, s.12.

değerlendirme, proje bazlı değerlendirme ve güvenlik riskleri ile önlemler olmak üzere dört temel değerlendirmeden oluşmaktadır³²¹.

Sağlık verilerini içeren yapay zekaya dayalı farazi bir uygulama için nasıl veri koruma etki değerlendirmesi yapılması gerektiğine dair bir çalışma yapılmıştır. Farazi uygulamada hastaların kronik hastalıkları ve durumlarını daha iyi kontrol edebilmesi için tasarlanacak farazi bir sağlık uygulaması planlanmış, iki yüz hastanın kronik hastalıklarına ilişkin günlük aktivitelere ilişkin veriler akıllı saat, telefon gibi akıllı giyebilir araçlar ile toplanmış; hastaların sağlıklarını etkileyebilecek madde tüketimleri, beslenme şartları kendilerinden öğrenilmiş; hasta öyküsü doktorlarından elde edilerek algoritmalar aracılığı ile kullanılmıştır³²². Bu projeye ilişkin veri koruma etki değerlendirmesi yapılırken öncelikle veri bazlı değerlendirme yapılması gerekmektedir. Veri bazlı değerlendirme aşamasında, yapay zeka sisteminde kullanılacak verinin kişisel verilerin korunması hukuku bağlamında özellikle amaç ile sınırlılık, şeffaflık, doğruluk, data minimizasyonu ve rıza açısından değerlendirmesi ve açıklanması yapılmaktadır³²³. Bu aşamada, kullanılan verinin türü, hangi formatta olduğu, ne ölçüde işleneceği; verinin kaynağının neler olduğu ve buna ilişkin güvenliğin sağlanması adına alınan önlemleri; verinin kim tarafından toplandığı ve kimlerce ulaşılabilir olduğu; verinin kullanım amacından farklı amaçlarla gelecekte işlenip işlenmeyeceği; veri işleme faaliyetinin ne kadar süre ile devam edeceği, nasıl ve ne zamana kadar saklanacağı; işleme faaliyetinin gerçekleştirilmesi için hangi teknolojilerin kullanılacağı; verinin saklanma ve toplanma aşamasındaki güvenliğinden kimin sorumlu olduğuna ilişkin değerlendirme yapılması beklenebilecektir³²⁴. İkinci aşama olan veri sahibi bazlı değerlendirmede veri sahibinin güvenliğini kazanmak ve kendi kaderini tayin hakkını korumak amaçlanmaktadır. Bu aşamada sağlık verisi sahibinin sahip olduğu hakların nasıl kullanılabilmesine ilişkin değerlendirmeler yer almaktadır, veri sahiplerinin verdikleri rızayı zorlanmadan geri almasına ilişkin izlenecek yol, verilerinin silinmesini isteme hakkı, işlenen verilerine ilişkin bilgileri indirme ve verilerinin taşınmasını isteme hakkına ilişkin mekanizmalara dair bilgilendirme ve değerlendirmeler bu aşamada gerçekleştirilmektedir³²⁵. Üçüncü aşamada, veri işlemeye ilişkin hukuki dayanaklar, projenin sebebi ve proje süresince veri sorumlusu ve veri işleyen tarafından

³²¹ Várkonyi, Gizem Gültekin/ Gradišek, Anton, “ Data Protection Impact Assessment Case Study for a Research Project Using Artificial Intelligence on Patient Data”, **Informatica**, C.44, S.4, s.500-503. <https://www.informatica.si/index.php/informatica/article/view/3253>

³²² Várkonyi/ Gradišek, s. 499.

³²³ Várkonyi/ Gradišek, s.500.

³²⁴ Várkonyi/ Gradišek s.501.

³²⁵ Várkonyi/ Gradišek s 500-501.

takip edilecek önlemler değerlendirilmektedir³²⁶. Büyük verinin kullanıldığı durumlarda, güvenlik riskleri olacağından oluşabilecek riskler ve gerekli güvenlik sistemlerine ilişkin değerlendirmelerin de projeye başlamadan yapılması gerekmektedir.

Kişisel veri etki değerlendirmesi yapılırken gerçekleştirilen tüm bu değerlendirmeler ışığında gerek uygulamada veri işlenirken ortaya çıkabilecek güvenlik sorunları, gerek sağlık verisi işlenen hastanın haklarında gerçekleşebilecek ihlaller; gerekse proje bazlı gerçekleşebilecek riskler önceden belirlenmekte ve olası çözümler de öngörülmektedir. Bu şekilde yapay zekanın kullanılması ile ortaya çıkan hesap verilebilirlik problemine de veri işleme sürecine şeffaflık katarak bir çözüm üretilebilmiş olmaktadır.

Yapay zeka bağlantılı veri ihlallerinin önüne geçilmesini sağlayabilmek için bir diğer etki değerlendirmesi de yapay zekanın kendisi için yapılmalıdır. Veri işlenmesinde yapay zekanın kullanıldığı durumlarda, makine işlemesi modellerinin tahmin edilemezliği de göz önünde bulundurulduğunda, kişisel veri hedeflenmese de kişisel veriye dayanarak oluşan sosyal küçük düşürmeler oluşabilmektedir. Örneğin; bazı etnik grupların kişisel veri niteliği taşıyan etnik kökenlerine dayanarak bazı hastalıklara daha meyilli kabul edilmektedir³²⁷. Avrupa Birliği Yapay Zeka Üst Düzey Uzman Grubu gibi uzmanlar, yapay zekanın yer aldığı durumlarda yalnızca kişisel veri etki değerlendirmesinin yeterli olmadığını bunun yanında daha geniş niteliğe sahip olan yapay zekanın yaratabileceği etik sorunları da içeren bir yapay zeka etki değerlendirmesinin de yapılarak şeffaflığın sağlanmasını önermektedir³²⁸. Söz konusu yapay zeka etki değerlendirmesi ilerleyen süreçlerde gerçekleşebilecek sorunların önceden düşünülerek bu sorunlara ilişkin alınabilecek önlemleri belirlemek için kullanılan risk yönetim sistemidir³²⁹.

Yapay zeka eli ile veri işlemenin söz konusu olduğu durumlarda, gerçekleştirilecek etki değerlendirmeleri ışığında, veri işlemeye dair risk tespitleri baştan yapılacak, risk seviyesinin çok düşük olduğu haller dışında veri işlemenin yapılmasına izin verilmeyecektir³³⁰.

³²⁶ Várkonyi/ Gradišek s.502.

³²⁷ Stahl, Bernd Carsten/ Schröder Doris/ Rodrigues, Rowena, "Privacy", **Ethics of Artificial Intelligence Case Studies and Options for Addressing Ethical Challenges** , Springer, 2022, s.33. https://doi.org/10.1007/978-3-031-17040-9_9

³²⁸ Stahl/ Schröder/Rodrigues, s.33-34.

³²⁹ Stahl, Bernd Carsten/ Schröder Doris/ Rodrigues, Rowena, s.18.

³³⁰ Öğretmen Kotil, s.288.

2.2.4.3. Davranış Kuralları ve Sertifikasyonlar

Genel Veri Koruma Tüzüğü m.40 hükmü davranış kurallarına, m.42 hükmü ise sertifikasyona ilişkin düzenlemeleri içermektedir. Veri koruma etki değerlendirmelerinin aksine davranış kuralları ve sertifikasyonlar zorunlu değil, gönüllü önlemlerdir³³¹. Davranış kuralları, işletme tarafından veri işlemenin gerçekleştirilebilmesi için şart koşulmuş kurallar bütünüdür³³². Sertifikasyon, veri işleme faaliyetlerinin hukuka uygun olarak gerçekleştiğine ilişkin bağımsız güvence aracıdır³³³.

Genel Veri Koruma Tüzüğü m.42 hükmüne göre üye devletler, düzenleyici otoriteler ve komisyonun sertifikasyon, damga ve işaretler aracılığı ile veri sorumlusu ve veri işleyen tarafından gerçekleştirilen veri işleme faaliyetlerinin veri koruma hukukuna ilişkin düzenlemeye uygun gerçekleştirildiğini gösterilmesini desteklemelidir. Sertifikasyon mekanizmaları hem veri sahipleri için hem de iş ilişkisi içerisinde veri sorumlusu ve veri işleyen arasında veri işleme sürecinin şeffaf hale gelmesini ve de dolayısıyla hesap verilebilirliğin artmasını sağlamaktadır³³⁴.

Sertifikasyon, yalnızca akredite bir belgelendirme kuruluşu veya yetkili denetim makamı tarafından, belgelendirme kriterlerinin karşılandığını belirten bağımsız kanıt değerlendirmesinin ardından verilebilmektedir³³⁵. Sağlık bilimlerinde yapay zekanın kullanılması durumunda ise, sertifikasyonun kamu kuruluşlarınca verilmesi gerekmektedir³³⁶.

Sertifikasyon kriterlerinin açık, anlaşılır ve pratik uygulamaya izin verecek şekilde formüle edilmesi gerekmektedir³³⁷. Sertifikasyon esnasında, kişisel verilerin korunması

³³¹ **Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation**, European Data Protection Board, Version 3.0., 4.6.2019, s.5, (erişim tarihi: 1.5.2023), https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12018-certification-and-identifying_en

³³² **Öğretmen Kotil**, s. 198 ; Kamara, Irene, “Article 40. Codes of Conduct”, **The EU General Data Protection Regulation (GDPR) – A Commentary**, Ed. Christopher DOCKSEY, Cristopher Kuner, Lee A. Bygrave, Laura Drechsler, Oxford University Press, Oxford, 2020, s.721.

³³³ **Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation**, European Data Protection Board, s.8.

³³⁴ **Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation**, European Data Protection Board, s. 6.

³³⁵ **Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation**, European Data Protection Board, s.8; GDPR m.42/5

³³⁶ **Artificial Intelligence in health care: medical, legal and ethical challenges ahead**, Council of Europe, s.17.

³³⁷ **Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation**, European Data Protection Board, s.15.

düzenlemelerine uyum tespit edilirken tasarımda gizlilik, varsayılanda gizlilik ve gerektiği durumlarda veri koruma etki değerlendirmesi yapılması gerekliliğine uygun hareket edilip edilmediğine ilişkin değerlendirmeler de kriterler arasında yer almaktadır³³⁸. Belirlenen kriterler hayat boyu geçerli kabul edilmemeli; yasal düzenlemede bir değişiklik olduğu, Avrupa Birliği Adalet Divanı tarafından şart ve hükümler yorumlandığı veya teknik açıdan değişimler olduğunda sertifikasyon işlemlerini gerçekleştiren kuruluş tarafından kriterler hakkında gerekli güncellemeler yapılmalıdır³³⁹.

2.2.4.4. Vijilans

Algoritmavijilans (algoritma gözetimi), sağlık hizmetlerinde algoritmaların olumsuz etkilerinin değerlendirilmesi, izlenmesi, anlaşılması ve önlenmesi ile ilgili bilimsel yöntem ve faaliyetler olarak tanımlanabilecektir³⁴⁰. Geliştiriciler tarafından öngörülün ya da öngörülmesin sağlık hizmeti içerisinde kullanılan algoritmaların etkinlik ve eşitlik açısından değerlendirilmesi ve izlenmesi, gerekli ve hatta etik bir zorunluluktur³⁴¹. Teknik hususların dışında algoritmaların performansı farklı verilere karşı farklı zamanlarda değişiklik gösterebilmektedir. Algoritmaların nasıl kullanıldığı, algoritmik çıktıların nasıl yorumlandığı konusunda algoritmalara duyulan güven eksikliği ve endişeler sağlık bilimlerinde de bir sorundur. Tahmin edilmesi zor olan algoritmik süreçte, herhangi bir sistemik faktörü algoritmanın performansını etkilemekte ve beklenmeyen etkilere sebep olarak hastaların zararına sebep olabilmektedir. Algoritma kullanımının sağlık bakım sistemlerinde yer edinmesi, doğal ve sistemik eşitsizlikler ve istenmeyen zarar potansiyelleri göz önünde bulundurulduğunda, sağlık hizmetlerinde algoritma geliştirilmesi ile uygulanmasında algoritmik gözlem sağlayan araçlar kullanılması gerekmektedir³⁴².

³³⁸ **Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation**, European Data Protection Board, s.15.

³³⁹ **Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation**, European Data Protection Board, s.21-22.

³⁴⁰ Rath, David, “Does Healthcare Need an ‘Algoritmovigilance’ Movement?”, **Healthcare Innovation**, 04.06.2020, <https://www.hcinnovationgroup.com/analytics-ai/artificial-intelligence-machine-learning/article/21140945/does-healthcare-need-an-algorithmovigilance-movement> ; Embi, Peter J., “Algoritmovigilance—Advancing Methods to Analyze and Monitor Artificial Intelligence–Driven Health Care for Effectiveness and Equity”. **JAMA Network Open**, C.4, S.4, 2021, s.2, (erişim tarihi: 1.5.2023), <https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2778569>

³⁴¹ Embi, s.2.

³⁴² Embi, s.2.

2.2.4.5. İnsanın Sürece Katılması ve İnsan Gözetimi

Yapay zeka çağında veri işlenmesi sırasında insanların özerkliğine saygı gösterilmesini sağlamak gerekmektedir. Yapay zeka sistemleriyle etkileşime giren insanlar, kendi kaderini tayin edebilmeli ve sürece katılabilmelidir. Yapay zeka sistemleri, insanlara haksız yere boyun eğdirmemeli, insanları zorlamamalı, aldatmamalı, manipüle etmemeli, koşullandırmamalıdır. Bu bahsedilenlerin gerçekleştirilebilmesi için insan merkezli tasarım ilkeleri benimsenmeli ve insan gözetimine yer verilmelidir³⁴³.

Kişinin yapay zeka ile ilgili süreç içerisindeki yerinin tespitinde öncelikle şu soruların değerlendirilmesi gerekmektedir³⁴⁴: Bireyi veya toplumu etkileyen yapay zeka sistemi etkileşimde bulunma, rehberlik etme ya da karar alma amacıyla mı tasarlandı? Yapay zekayı kullanan kişi veya yapay zeka kullanımından etkilenen kişi etkileşim mercisinin bir insan mı yoksa yapay zeka sistemi mi olduğu konusunda kafa karışıklığı yaşayabilir mi? Yapay zeka sistemi fazla güven sağlayarak insan özerkliğini etkileyebilir mi? Yapay zeka sistemi son karara istenmeyen bir şekilde müdahale ederek insan özerkliğini etkileyebilir mi? Yapay zeka sistemi, kendisini kullanan veya kullanımından etkilenen kişiler ile veya bunlar arasındaki sosyal etkileşimde aldatma yoluna başvuruyor mu? Yapay zeka sistemi, insan bağlılığı yaratma, bağımlılık davranışını teşvik etme veya kullanıcı davranışını manipüle etme riski taşıyor mu ve buna ilişkin önlemler alındı mı? Tüm bu sorular da yapay zeka kullanımının olduğu durumlarda, kişinin hala kendi hakkında karar verebilecek şartların korunması gerektiğini kanıtlar niteliktedir. Yapay zeka sistemlerinin kullanıcıları tarafından anlaşılması, değerlendirilmesi ve yapay zeka tarafından verilen kararlara meydan okuyabilmesi gerekmektedir, bu durum bireylerin kendi hakkında bilinçli seçimler yapabilmesinin desteklenmesidir³⁴⁵.

İnsan özerkliğinin önüne geçilmesini engelleyebilecek en iyi mekanizma insanın kendisidir. İnsan gözetimlerine ilişkin farklı yaklaşımlar mevcuttur. Yapay zeka sisteminin her karar aşamasında müdahale yeteneğine sahip olunan insan gözetim tipi hem istenmemektedir hem de mümkün değildir. Bir başka insan gözetimi yaklaşımı, yapay zeka sisteminin tasarımı

³⁴³ **Ethics Guidelines for Trustworthy AI**, High Level Expert Group on Artificial Intelligence, 8.4.2019., s.14 (erişim tarihi: 2.5.2023), https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60419

³⁴⁴ **The Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self assessment**, High Level Expert Group on Artificial Intelligence, , 17.6.2020, (erişim tarihi: 1.5.2023), s.7-8, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=68342

³⁴⁵ **Ethics Guidelines for Trustworthy AI**, High Level Expert Group on Artificial Intelligence, s.16.

esnasında insan gözetimi yapma ve müdahale etmenin mümkün olmasıdır. Son yaklaşıma göre ise yapay zeka sisteminin faaliyetleri denetleme ve sistemin ne zaman nasıl kullanılacağına ilişkin karar verme kabiliyetinin olması gerekmektedir³⁴⁶.

2.2.4.6. İstatiksel İşleme ve Bilimsel Araştırma için Veri Anonimleştirme

Genel Veri Koruma Tüzüğü m.89 hükmü gerekli güvenlik önlemlerinin alınması koşuluyla işleme faaliyetlerine izin vermektedir. KVKK m.28/1 hükmü uyarınca da kişisel veriler araştırma amacıyla işlenebilmekte, kanun hükümleri uygulanmamaktadır. Hükümlerde bilimsel araştırmanın tanımı yapılmamaktadır. Yapay zeka ile veri işlenmesinin bilimsel araştırma kapsamında değerlendirilip değerlendirilemeyeceğine ilişkin bir düzenleme yoktur. Yapay zekanın sağlık bilimlerinde kullanım alanları incelendiğinde, büyük veri kullanılarak kişisel sağlık verilerinin de işlenmesi yoluyla kanser gibi hastalıkların teşhisi için geliştirilen yapay zekalı uygulamaların bilimsel araştırma niteliği taşıdığı kanaatindeyiz.

Bilimsel araştırmalarda veri kullanımı ile kişilere bağlı sonuçlar elde edilmesinin ötesinde genel bir çıkarımda bulunabilme amacı mevcuttur ve bu çıkarımlar kişisel veri olarak kabul edilmemektedir³⁴⁷. Fakat bu bilimsel araştırmalarda kullanılan veriler ilk halinde hala kişisel veri niteliğindedir, bu durum ise gerekli önlemlerin alınmaması durumunda kişisel verilerin ihlaline sebep olabilecektir.

Verilen izinler sayesinde, yapay zeka uygulamalarının veri işleme mümkün gözükmektedir. Sağlık hizmet sunucuları tarafından merkezi sağlık veri sistemlerine aktarılan kişisel sağlık verileri, yapay zeka eğitimleri için kullanılabilir bir kaynaktır. Kişisel sağlık verilerinin bilimsel araştırmalarda kullanılabilmesi ve KVKK hükümlerine tabi olmaması için öncelikli şart bu verilerin anonimleştirilmiş olmasıdır. KVKK m.28/1 (b) hükmü bu araştırmalarda kullanılacak kişisel sağlık verilerinin anonimleştirilmesini zorunlu kılmaktadır. Anonim hale getirilmiş veri, başka veriler aracılığı ile bile kimliği belirli veya belirlenebilir gerçek kişi ile ilişkilendirilemeyecek hale getirilmiş veridir. Yapay zeka aracılığı ile bilimsel çalışmaların gerçekleştirilmesi için kullanılacak veri, çalışma başlamadan önce anonimleştirilerek işlenebileceği gibi, açık sağlık verisi halinde yayımlanmış diğer verilerin kullanılması yolu ile de gerçekleştirilebilecektir. Açık sağlık verisi, ücretsiz veya hazırlanma maliyetinden daha az bir bedel karşılığı internet üzerinden herkesin erişebileceği şekilde sunulan, herhangi bir kişinin üzerinde fikri mülkiyet hakkı olmayan ve herhangi bir amaçla serbest bir şekilde kullanılmaya müsait, makinelerce okunabilen, başka veri ve sistemler ile

³⁴⁶ **Ethics Guidelines for Trustworthy AI**, High Level Expert Group on Artificial Intelligence s.16.

³⁴⁷ **Yılıyaer**, s.202.

çalışabilen anonim haldeki sağlık verisini ifade etmektedir³⁴⁸. Açık sağlık verisi, herhangi bir amaçla serbest kullanıma açık olduğundan bilimsel araştırma bünyesinde yapay zeka tarafından da sorunsuz bir şekilde kullanılabilir.

Yapay zekanın bilimsel araştırma kabul edilerek veri işlemesi ile ilgili ortaya çıkan bir sorun ise yapay zeka çağında kişisel verilerin anonimleştirilmesinin etkisini kaybetmeye başlamış olmasıdır. Belirtildiği üzere yapay zekanın kişisel sağlık verilerini bilimsel araştırma amacıyla kullanabilmesinin ön şartı sağlık verisinin anonimleştirilmesidir; fakat yapay zekanın büyük veri kullanımından dolayı artık bir kere anonimleştirilmiş veri yeniden kişiyi belirli veya belirlenebilir kılacak hale dönüştürülebilmektedir. Bu sebeple sağlık verilerinin anonimleştirilmesi taraflılık ihtimalini ortadan kaldırmaya tek başına yeterli değildir³⁴⁹.

Anonimleştirmenin ortadan kaldırılmasını önlemek adına gerekli tedbirlerin alınmasının ve kişisel sağlık verilerinin açık veri haline getirilerek tekrar kullanıma sunulabilmesinin sağlanması adına yetkili kuruluşların olması ve konuya ilişkin denetimler yapması, bilimsel araştırmalarda kişisel sağlık verilerinin kullanımı mümkün kılabilir. Finlandiya’da sosyal ve sağlık verilerinin kullanımına ilişkin talep ve izinler Findata isimli yetkili kuruluş tarafından değerlendirilmektedir³⁵⁰, bu sayede kişisel sağlık verilerinin bilimsel araştırma amacı ile kullanılması kontrol mekanizması altında tutulmaktadır. Bu tür veri kullanımına ilişkin kontrol mekanizmalarının yanında gerekli korumaların ve hasta-sağlık uzmanları arasında güvenin de sağlanabilmesi için sağlık alanında kullanılan yapay zekalar için resmi siciller gerekmektedir³⁵¹. Resmi sicillere tescili için de kuruluşlar kurulum bu kuruluşlar arasında bir nevi konsültasyon sağlanır ise yapay zeka tarafından açık sağlık verileri kullanımı güvenli hale gelebilecektir.

Yapay zekanın sağlık verisi işlediği durumlarda veri ihlalinin önüne geçebilmek adına belirtilmiş olan önlemler alınsa dahi, kişisel sağlık verilerinin ihlali oluşabilmektedir. Yapay zeka ile veri işlenmesi esnasında anonimleştirilmiş veriler kullanılsa bile büyük veride yer alan verilerin yapay zeka tarafından hızlı bir şekilde birbiri ile bağlanması sayesinde kişi belirli hale gelebilmektedir. Devam eden veri işlemede ise bu gibi ihlal durumları oluşabilmektedir. Yapay zeka kullanımında oluşan veri ihlali kaynaklı zararlarda sorumluluğun belirlenmesi

³⁴⁸ KVKK m.3/1,a; KSVH m.4/1-2

³⁴⁹ **The Impact of Artificial Intelligence on the Doctor-Patient Relationship**, Council of Europe, s.6.

³⁵⁰ European Commission, “Data Governance Act explained” 30.08.2022, (erişim tarihi:1.6.2023) <https://digital-strategy.ec.europa.eu/en/policies/data-governance-act-explained#:~:text=The%20Data%20Governance%20Act%20>

³⁵¹ **The Impact of Artificial Intelligence on the Doctor-Patient Relationship**, Council of Europe s.60.

gerekmektedir. Aksi takdirde hukuk tarafından özel hükümlerle korunmakta olan kişisel sağlık verisi sahibinin mağduriyeti oluşacaktır.



ÜÇÜNCÜ BÖLÜM

KİŞİSEL SAĞLIK VERİLERİNİN KORUNMAMASI DURUMUNDA YAPAY ZEKANIN ÖZEL HUKUK SORUMLULUĞU

3.1. Genel Olarak

Sağlık bilimlerinde yapay zeka kullanımı sırasında birçok sağlık verisine ihtiyaç duyulmaktadır. Bu sağlık verilerinin kullanılması sayesinde daha hızlı ve az maliyetli tespitlerde bulunulabilmesi, verimliliğin sağlanması gibi fırsatların oluşmasının yanında kişisel sağlık verilerinin ihlali ihtimali de artmaktadır. Sağlık verilerinin ihlali durumunda veri sahibinin büyük zararlara uğraması söz konusudur. Yapay zeka ve sorumluluğa ilişkin özel hükümler henüz hukukumuzda düzenlenmemiş olsa da mevcut hükümler yapay zekanın kişisel sağlık verisini işlemesi ile ortaya çıkan zarar karşısında uygulama alanı bulabilmektedir.

Yapay zeka aracılığı ile kişisel sağlık verilerinin işlenmesi sırasında dikkat edilmesi gereken ilkelere uygun hareket edilmediği durumlarda, hukuka aykırı bir veri işleme faaliyeti söz konusudur. Yapay zeka ile kişisel sağlık verilerinin işlenmesi başlangıçta hukuka uygun olsa bile yapay zekanın kendini verilerle eğitmesinden kaynaklanan algoritma sapması ya da çıkarımlar nedeniyle zarara sebep olunabilmektedir. Bir başka deyişle; başlangıçta hukuka uygun olan işleme süreç içerisinde hukuka aykırı fiil haline gelebilmektedir. Hukuka aykırı gerçekleştirilen veri işleme faaliyeti sonucunda zarar görülmesi halinde sorumluluk ortaya çıkmaktadır. Sorumluluk kavramı, verilen zararın giderilmesine dair yükümlülüğü ifade etmektedir³⁵². Hukuka aykırı işleme sonucunda ortaya çıkacak sorumluluğun; tezimizin yapay zeka ile kişisel sağlık verisinin işlenmesi üzerine olması sebebiyle, öncelikle Kişisel Verilerinin Korunması Kanunu hükümlerince doğan sorumluluk ve yapay zeka sorumluluğu şeklinde iki bölümde incelemesi gerektiği kanaatindeyiz.

3.2. Kişisel Sağlık Verilerinin Yapay Zeka İle İşlenmesi Sırasında İhlal Durumunda Sorumluluk

Veri sahibi, yapay zekanın veri ihlallerine sebep olmasıyla meydana gelen zararın tazminini isteme hakkına sahiptir. Kişisel sağlık verilerinin yapay zeka ile işlenmesi sırasında ihlal söz konusu olduğunda hem kişisel verilerin korunamaması kaynaklı sorumluluğun hem de yapay zekanın sorumluluğunun incelenmesi gerekmektedir.

³⁵² Eren, Fikret, **Borçlar Hukuku Genel Hükümler**, 27. Bs., Yetkin Yayınları, 24. Baskı, Ankara, 2022, s.86.

3.2.1. Kişisel Verilerin Korunması Yönüyle Sorumluluk

Kişisel Verilerin Korunması Kanunu m.11/1 (ğ) hükmü uyarınca; kişisel sağlık verisi sahibi, kişisel sağlık verisinin kanun hükmüne aykırı şekilde işlendiği durumlarda oluşan zararın giderilmesini talep edebilmektedir. İlgili Kanun m.14/3 hükmü uyarınca; kişilik hakkı ihlal edilen kişinin, uğradığı zararın tazmini için genel hükümlere göre tazminat hakkı da saklı tutulmaktadır. KVKK m.14/3 hükmü olmasaydı dahi TMK m.5 hükmü uyarınca genel nitelikli hükümler tüm özel hukuk ilişkilerine uygulanabileceğinden, yapay zekanın kişisel sağlık verisini işlemesi sebebiyle oluşan tüm zararlar için tazminat hakkı saklı olacaktır.

Tazminat hakkı, kişisel sağlık verilerinin ihlalinin bir kişilik hakkı ihlali olması dolayısıyla, TBK m. 49 ve devamı hükümlerince haksız fiil sorumluluğu; bir sözleşme ilişkisinin olması durumunda TBK m.112 ve devamı hükümlerince sorumluluk şeklinde söz konusu olmaktadır. TMK m.24 ve m. 25 hükümleri uyarınca kişilik hakkı ihlaline uğrayan veri sahibinin maddi ve manevi tazminat yoluna başvurarak uğradığı zararın tazminini talep hakkı vardır. Tazminat davası yolunun dışında, veri sahibinin başvurabileceği diğer bir yol TMK m. 25 hükmünde öngörülen koruyucu davalar ile vekaletsiz iş görme davasıdır. TMK m.25 hükmüne göre veri sahibi hakimden; saldırının önlenmesini, saldırının devam etmesi durumunda saldırının durdurulmasını, saldırının etkilerinin devam ettiği durumlarda saldırı bitse bile saldırının hukuka aykırılığının tespitini isteyebilmektedir.

3.2.1.1. Başvurulabilecek Hukuki Yollar

Yapay zeka ile kişisel sağlık verilerinin işlenmesi sonucunda ortaya çıkan ihlal durumlarında, oluşan zararın karşılanması için tazminat davası; zarardan veri sahibini koruyabilmek için önleme, durdurma, tespit davaları; kendisine ait veri sayesinde elde edilmiş olan kazancın iadesi için vekaletsiz iş görme davası yoluna başvurulabilmektedir.

3.2.1.1.1. Kişisel Verilerin Korunması Kanunu Hükümlerince Sorumluluk

Kişisel Verilerin Korunması Kanunu m.11/1 (ğ) hükmü ilgili kişinin haklarını düzenlerken “*Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarar uğraması halinde zararın giderilmesini talep etme*” hakkına da yer vermektedir.

Kişisel sağlık verisi sahibi, zararın giderilmesini talep hakkını yazılı veya Kurul tarafından belirlenmiş bir başka şekilde veri sorumlusuna iletmesi gerekmektedir³⁵³. Veri sorumlusu kendisine iletilen bu talebi en geç otuz gün sonunda sonuçlandırmak

³⁵³ KVKK m.13/1.

zorundadır³⁵⁴.Veri sorumlusunun talebi reddetmesi ya da otuz gün içinde yanıt vermemesi durumunda ret cevabının öğrenilmesinden itibaren otuz; her halde en geç başvuru tarihinden itibaren altmış gün içerisinde Kurul’a şikayet yoluna başvurulabilmektedir³⁵⁵. Kurula şikayet yoluna başvurulabilmesi için öncelikle veri sorumlusuna başvurma ön şartı bulunmaktadır.

Kişisel Verilerin Korunması Kanunu m.14/3 hükmü uyarınca kişisel sağlık verilerinin ihlali sonucu bir zarar oluştuğunda; zarara uğrayan veri sahibinin genel hüküm niteliğinde olan TMK ve TBK’nin ilgili hükümlerine başvurarak zararının tazminini istemesi de mümkündür. KVKK m.15 hükmüne göre; Kurul tarafından şikayet üzerine veya re’sen gerekli inceleme yapılacak³⁵⁶; bunun sonucunda şikayetin ilgililerine şikayet tarihinden itibaren altmış gün içinde cevap verecek³⁵⁷, bu cevaba göre kurul kararı gecikmeksizin en geç otuz gün içinde yerine getirilecektir³⁵⁸.

3.2.1.1.2. Türk Medeni Kanunu Hükümlerince Sorumluluk

Türk Medeni Kanunu m.24 ve m. 25 hükümleri uyarınca kişilik hakkı ihlaline uğrayan veri sahibinin maddi ve manevi tazminat yoluna başvurarak uğradığı zararın tazminini talep hakkı vardır. Tazminat davası yolunun dışında, veri sahibinin başvurabileceği diğer bir yol TMK m. 25 hükmünde öngörülen koruyucu davalardır. TMK m.25/1 hükmü “*Davacı, hakimden saldırı tehlikesinin önlenmesini, sürmekte olan saldırıya son verilmesini, sona ermiş olsa bile etkileri devam eden saldırının hukuka aykırılığının tespitini isteyebilir.*” şeklindedir.

Önleme davası, durdurma davası ve tespit davası; kişisel sağlık verilerinin hukuka aykırı bir şekilde işlenmesi durumunda kişiye kişilik hakkını koruma imkanı tanıyan koruyucu davalardır. Kişilik hakkının bir yansıması olarak veri sahibi, kişisel verilerinin kaderini tayin hakkına sahiptir³⁵⁹. Kişisel verisinin kaderini tayin hakkına sahip olan veri sahibi, kişisel verinin kişilik hakkı olması sebebiyle, yapay zeka tarafından kişisel sağlık verilerinin işlenmesi ile gerçekleşen ihlallere karşı TMK m.25 hükmünde düzenlenen koruyucu davalara başvurabilmektedir.

³⁵⁴ KVKK m.13/2.

³⁵⁵ KVKK m.14/1.

³⁵⁶ KVKK m.15/1.

³⁵⁷ KVKK m.15/4.

³⁵⁸ KVKK m.15/5, m.15/6.

³⁵⁹ Turgut, Cemile, **Kişilik Hakkının Bir Görünümü Olarak Unutulma Hakkı**, On İki Levha Yayıncılık, 2021 s.10 ; Zafer, Hamide, “Sağlık Mesleği Mensuplarının Suçu Bildirmemesi Suçu (TCK m.280), **İÜHF**, C. 71, S.1, 2013, s.1328.

3.2.1.1.2.1. Önleme Davası

Kişisel sağlık verilerine ilişkin henüz herhangi bir saldırının mevcut olmadığı fakat kişilik hakkına ilişkin bir saldırı gerçekleşeceğine veya önceden gerçekleşen bir saldırının tekrarlanabileceğine ilişkin yakın ve ciddi bir tehlikenin varlığı durumunda önleme davası açılabilmektedir³⁶⁰. Önleme davası açılabilmesi için kusur ve zarar şartı aranmayıp kişisel sağlık verisinin haksız fiil veya sözleşmeye aykırılık şeklinde hukuka aykırı olarak işlenme tehlikesinin mevcut olması yeterlidir³⁶¹.

Kişisel sağlık verilerinin yapay zeka ile işlendiği durumlarda TMK m.25 hükmüne dayanarak önleme davası açılması mümkündür. Kişisel sağlık verilerinin de kişilik haklarının içerisinde yer aldığı göz önünde bulundurulduğunda, yapay zekanın kişisel sağlık verisini hukuka aykırı olarak işlemesi tehlikesinin olduğu bir durumda kişisel sağlık verisi sahibi tarafından önleme davası açılabilecektir. Herhangi bir hukuka uygunluk sebebi olmaksızın kişinin tetkik sonuçları ile yapay zekanın eğitileceğinin öğrenilmesi durumunda, kişi henüz yapay zekanın eğitime başlanmadan kişisel sağlık verisinin hukuka aykırı olarak işlenme tehlikesinin olduğu gerekçesi ile önleme davası yoluna başvurabilecektir. Önleme davasına başvurulabilmesi için henüz kişisel verinin ihlal edilmemiş olması, sadece tehlike boyutunda kalması gerekmekte; teknoloji çağında kaynak fazlalığı, işleme ve kullanmanın farklı farklı alanlarda hızlı bir şekilde gerçekleşmesi, tehlikenin saptanması saldırının gerçekleşmesi arasında geçen sürede kişinin önleme davası yoluna başvurmasını zorlaştırmaktadır³⁶². Yapay zeka bu süreci daha da hızlı bir hale getirmektedir; dolayısıyla yapay zeka aracılığı ile kişisel sağlık verilerinin işlenmesi durumunda önleme davası başvurulabilecek bir yol olmakla beraber bunun uygulamadan çok teorik bir bilgi olarak kalacağı kanaatindeyiz.

³⁶⁰ **Oğuzman/Seliçi/Oktay-Özdemir**, s.226; Dural, Mustafa/ Ögüz, Tufan, **Türk Özel Hukuku, Kişiler Hukuku**, C.2, Filiz Kitabevi, İstanbul, 2020, s.157.

³⁶¹ Zor, Abdülhamid, **Veri Sorumlusunun Yükümlülükleri ve Bu Yükümlülükleri İhlalinden Doğan Özel Hukuk Sorumluluğu**, On İki Levha Yayıncılık, İstanbul, 2020, s.195-196; **Oğuzman/Seliçi/Oktay-Özdemir**, s.226; Taştan, Furkan Güven, **Türk Sözleşme Hukukunda Kişisel Verilerin Korunması**, 2. Baskı, On İki Levha Yayıncılık, İstanbul, 2017, s.192.

³⁶² **Küzeci**, s.453; **Taştan**, s.196-197.

3.2.1.1.2.2. Durdurma Davası

Türk Medeni Kanunu m.25 hükmü uyarınca veri ihlali durumunda başvurulabilecek koruyucu dava türlerinden bir diğeri durdurma davasıdır. Kişilik hakkına karşı hukuka aykırı bir saldırı var ise bu saldırının sona erdirilmesi, yenilenmemesi veya saldırı sebebiyle oluşabilecek maddi ve manevi zararın önlenmesi için durdurma davası açılabilir³⁶³.

Durdurma davası açılabilmesi için kusur ve zarar şart olmayıp kişisel sağlık verisinin haksız fiil veya sözleşmeye aykırılık şeklinde hukuka aykırı olarak işlenmesi ve bu saldırının durdurulabilecek olması gerekmektedir³⁶⁴.

Kişisel sağlık verilerinin yapay zeka ile işlendiği durumlarda TMK m.25 hükmüne dayanarak durdurma davası açılması mümkündür. Kişisel sağlık verilerinin de kişilik haklarının içerisinde yer aldığı göz önünde bulundurulduğunda, yapay zekanın kişisel sağlık verisini hukuka aykırı olarak işlemesi durumunda oluşan saldırı için kişisel sağlık verisi sahibi tarafından durdurma davası açılabilir. Herhangi bir hukuka uygunluk sebebi olmaksızın kişinin tetkik sonuçları ile yapay zekanın eğitilmesi, kişisel sağlık verisinin hukuka aykırı olarak işlenmesi dolayısıyla kişisel sağlık verisine karşı bir saldırının mevcut olduğu gerekçesi ile durdurma davası yoluna başvurulabilir.

Kişisel sağlık verilerinin hukuka aykırı bir şekilde işlenmesi, dolayısıyla mevcut bir saldırının olması durumunda, veri sahibinin durdurma davası açma imkanının yanında KVKK m.11 hükmü neticesinde doğrudan veri sorumlusuna başvurarak saldırının sonlandırılmasını isteme hakkı da vardır. Daha hızlı sonuca ulaşılabilmesi bakımından durdurma davası yoluna başvurmadan veri sorumlusuna başvurulması daha mantıklı kabul edilebilmektedir³⁶⁵.

3.2.1.1.2.3. Tespit Davası

Türk Medeni Kanunu m.25 hükmünde düzenlenen koruyucu dava türlerinin sonuncusu tespit davasıdır. Kişilik hakkına karşı oluşan hukuka aykırı saldırı sona ermiş fakat etkileri devam etmekte ise tespit davası açılabilir³⁶⁶. Kişisel verilerin de kişilik hakkı kapsamında yer alması sebebiyle; kişisel verinin ihlal edildiği, ihlalin artık devam etmediği ama

³⁶³ Zor, s.196; Oğuzman/Seliçi/Oktay-Özdemir, s.224; Dural/Öğüz, s.156.

³⁶⁴ Zor, s.197; Oğuzman/Seliçi/Oktay-Özdemir, s.224, Dural/Öğüz, s.156; Taştan, s.193.

³⁶⁵ Taştan, s.195; Zor, s.198.

³⁶⁶ Oğuzman/ Seliçi/ Oktay-Özdemir, s.228; Akipek, Jale/ Akıntürk, Turgut/Ateş, Derya, **Türk Medeni Hukuku Hukuku Başlangıç Hükümleri Kişiler Hukuku**, 18.Bs., Beta Yayınları, İstanbul, 2022. s.398.

hala etkilerinin devam ettiği durumlarda kişisel veri sahibi tarafından tespit davası yoluna başvurulabilmektedir³⁶⁷.

Kişisel sağlık verilerinin yapay zeka ile işlendiği durumlarda TMK m.25 hükmüne dayanarak tespit davası açılması mümkündür. Kişilik hakları içerisinde yer alan kişisel sağlık verilerinin hukuka aykırı bir şekilde işlendiği fakat artık işlenme faaliyetinin devam etmediği durumlarda hala kişisel sağlık verisinin işlenmesinin etkileri devam etmekte ise tespit davası açılabilir. Herhangi bir hukuka uygunluk sebebi olmaksızın kişinin kişisel sağlık verilerinin yapay zekanın eğitiminde girdi olarak kullanılması ile yapay zeka uygulamasının algoritmada sapma ve ayrımcılık içeren örüntüler oluşturmada durumunda, her ne kadar kişisel sağlık verilerinin işlenme durumu sona erse de kişi sağlık hizmeti alımında etkilenebilmektedir.

3.2.1.1.3. Türk Borçlar Kanunu Hükümlerince Sorumluluk

Veri sahibinin tazminat hakkı TMK m.25/3 hükmünde belirtilmektedir. Tazminata ilişkin hükümler TBK hükümlerinde düzenlenmektedir. TBK m.49 ve devamı hükümlerince haksız fiil sorumluluğuna; TBK m.112 ve devamı hükümlerince sözleşme ilişkisinden doğan sorumluluğa; TMK m.2 dürüstlük kuralına dayanan sözleşme benzeri borç ilişkilerinden doğan sorumluluğa dayanarak yapay zeka ile kişisel sağlık verilerinin işlenmesi sebebiyle oluşan zararların tazminini talep edilebilmektedir.

Tazminat davası ile haksız bir eylemin gerçekleşmesinden sorumlu olan kişi tarafından mağdurun uğradığı zarar tazmin edilmektedir³⁶⁸. Mağdurun uğradığı bu zarar maddi ve manevi olabilmektedir. Kişilik hakkının ihlalinden doğan elem, acı ve ızdırabın telafi edilmesi amacıyla³⁶⁹ kişisel sağlık verisi ihlal edilen veri sahibi manevi tazminat yoluna; hukuka aykırı şekilde kişisel verilerinin korunması hakkına saldırı gerçekleşmesi neticesinde oluşan malvarlığında azalma veya malvarlığındaki olası bir artışın engellenmiş olması sebebiyle oluşan zararın telafisi amacıyla³⁷⁰ ise maddi tazminat yoluna başvurmaktadır.

Kişisel sağlık verileri, hassas veri niteliği taşıdığından, herhangi bir ihlal söz konusu olduğunda kişinin sosyal hayatında büyük etkiler yaratmaktadır. Bu durum, kişisel sağlık verisine ilişkin gerçekleşen ihlallerde kişinin manevi tazminat yoluna başvurma ihtimalini arttırmaktadır. Kişisel sağlık verilerinin işlenmesi yolu ile yapay zekaların tanı ve tedavi tespiti

³⁶⁷ Yılmaz, Süleyman/Çavuşoğlu, Gökçe Filiz, **Kişisel Verileri Koruma Hukuku**, Yetkin, Ankara, 2020, s.129.

³⁶⁸ Oğuzman, Kemal/Öz, Turgut, **Borçlar Hukuku**, 17. Bs., Filiz Kitabevi, C.2., İstanbul, 2022, s.69 (C.2)

³⁶⁹ Oğuzman/Öz, C.2, s.257.; Eren, s.805; Kılıçoğlu, Ahmet M., **Borçlar Hukuku Genel Hükümler**, 26. Bs., Turhan Kitabevi, Ankara, 2022, s.422.

³⁷⁰ Oğuzman/Öz, C.2, s. 39-40; Eren, s.544; Kılıçoğlu, s.283.

gerçekleştirdiği durumlarda ortaya çıkabilecek herhangi bir algoritma sapması ya da ayrımcılık durumunda kişinin uğrayacağı bedensel zarar, yanlış tedavi masrafları gibi zararlar içinde maddi tazminat yolu ile tazmininin sağlanması gerekmektedir.

Tazminat hakkı; haksız fiil, sözleşme ilişkisi, sözleşme benzeri borç ilişkisinden kaynaklanabilmektedir.

3.2.1.1.3.1. Haksız Fiil Sorumluluğu

Türk Borçlar Kanunu m.49 hükmü ile haksız fiil sorumluluğu düzenlenmektedir. İlgili hüküm; kişi kusurlu ve hukuka aykırı bir eylemde bulunarak bir başkasına zarar verdiği durumlarda, ortada bu eylemi yasaklayan herhangi bir hukuk kuralı veya herhangi bir sözleşme olmasa dahi, oluşturduğu zararın tazminini sağlamakla yükümlü olduğunu belirtmektedir. Kişisel sağlık verisine ilişkin herhangi bir sözleşme ilişkisi şartı olmaksızın verilerin hukuka aykırı bir şekilde işlenmesi durumunda, işleme faaliyetinde bulunan veri sorumlusunun TBK m.49 hükmünce haksız fiil sorumluluğu doğmaktadır.

Haksız fiil sorumluluğundan söz edebilmek için öncelikle hukuka aykırı fiil, kusur, zarar ve nedensellik bağının varlığı gerekmektedir³⁷¹. Kişisel sağlık verilerinin KVKK m.6 hükmünde düzenlenen hukuka uygunluk halleri olmaksızın işlenmesi durumu, hukuka aykırı veri işlenmesi ve dolayısıyla hukuka aykırı fiile örnektir. Kamu sağlığının korunması; koruyucu hekimlik; tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi; sağlık hizmetleri ile finansmanın planlanması ve yönetimi amaçlarından birisi veya kişisel sağlık verisi sahibinin açık rızası da olmadan kişisel sağlık verisinin işlendiği durumlarda hukuka aykırı fiil söz konusu olmaktadır. Tedavi olmak için sağlık verilerinin işlenmesine izin vermiş bir hastanın kişisel sağlık verilerinin ilerleyen süreçte doktor tarafından bilimsel araştırmalarda kullanılması hukuka aykırı fiile örnektir. Yapay zeka uygulamalarının geliştirilebilmesi için kişisel sağlık verilerinin kullanılmasının da bilimsel araştırma kapsamında değerlendirilebileceği düşünüldüğünde; yapay zeka aracılığı ile veri işlenmesi durumunda da sağlık verilerinin işlenmesine ilişkin rıza tedavi amacı ile verilmiş ise yapay zekanın geliştirilmesi ve eğitilmesi için kullanılması durumu hukuka aykırılık teşkil etmektedir.

³⁷¹ Oğuzman/Öz, C.2, s.1; Eren, s.540.

3.2.1.1.3.2. Sözleşme İlişkisinden Doğan Sorumluluk

Kişisel sağlık verilerinin işlenebilmesi için genellikle bir sözleşme ilişkisi olması gerekmektedir. Sözleşme ilişkisinden doğan sorumluluktan söz edebilmek için borca aykırı davranış, zarar, uygun illiyet bağı ve kusur unsurlarının varlığı gerekmektedir³⁷². Borca aykırılığın söz konusu olabilmesi için ön koşul geçerli bir sözleşmenin varlığıdır³⁷³. Geçerli bir sözleşmenin olabilmesi için öncelikle karşılıklı ve birbirine uygun olarak açıklanan irade beyanları gereklidir³⁷⁴. İrade beyanlarının yanı sıra sözleşmenin geçerli olması için tarafların ehil olması; sözleşme konusunun emredici hukuk kurallarına, kamu düzenine, genel ahlaka ve kişilik haklarına aykırı olmaması; imkansız olmaması ve irade beyanlarının sağlıklı olması şarttır³⁷⁵.

Sözleşmenin asli veya yan ediminin kişisel sağlık verilerinin işlenmesi olduğu durumlarda veri sorumlusunun gerekli özeni göstermemesi, yükümlülüklerini yerine getirmemesi borca aykırılık doğurmaktadır. Kişisel sağlık verilerinin işlenmesi, veri sorumlusu ve veri işleyen arasında yapılan veri işleme sözleşmesinin asli edimi olarak karşımıza çıkmaktadır³⁷⁶. Taraflar arasında yapılan sözleşmelerde kişisel sağlık verilerinin korunması yan edim yükümlülüğü olarak belirlenmiş olabileceği gibi edim niteliği taşımaksızın ifaya yardımcı yan yükümlülük olarak da belirlenebilmektedir³⁷⁷. Kişisel sağlık verilerinin işlenmesinin ifaya yardımcı yan yükümlülük olduğu durumlara doktor tarafından gerçekleştirilen tedavi borcunun ifasında rastlanılmaktadır³⁷⁸.

Kişisel sağlık verilerinin sözleşmenin asli edimi, yan edimi ya da ifaya yardımcı yan yükümlülüğü olarak belirlenip belirlenmemesinin kişisel sağlık verilerinin korunması edimine etkisi yoktur. Kişisel sağlık verilerinin kişilik varlığı olması sebebiyle her koşulda koruma yükümlülüğü söz konusudur; herhangi bir sözleşme ilişkisinde işlenen verilerin korunması gerekmektedir³⁷⁹.

³⁷² Oğuzman, Kemal/Öz, Turgut, **Borçlar Hukuku Genel Hükümler**, 20. Bs., Filiz Kitabevi, C. 1, İstanbul, 2022, s.378-380 (C.1)

³⁷³ Kılıçoğlu, s.131; Nomer, Ergin, **Devletler Hususi Hukuku**, 23. Bs., Beta Yayınları, İstanbul, 2021, s.64

³⁷⁴ TBK m.1.

³⁷⁵ Oğuzman/Öz, C.1, s.80-90.

³⁷⁶ Taştan, s. 109.

³⁷⁷ Taştan, s.109.

³⁷⁸ Gürbüz Erel, s. 144.

³⁷⁹ Taştan, s.110.

Kişisel sağlık verilerinin sözleşme ilişkisinden doğan sorumluluk kapsamında ihlali, borcun hiç ifa edilmemesi ya da gereği gibi ifa edilmemesi şeklinde oluşabilmektedir³⁸⁰. Kişisel sağlık verilerinin hukuka aykırı şekilde işlenmesi, borcun gereği gibi ifa edilmemesi durumunu doğurmaktadır³⁸¹. Doktor ya da hastane tarafından tedavinin yapılabilmesi amacıyla kişisel verilerini paylaşan hasta verilerinin tedavi sürecinden sonra da saklanarak hastalıkların tespitinin yapılabilmesini sağlayan bir yapay zeka sisteminin geliştirilebilmesi için kullanılması durumunda hukuka aykırı bir şekilde işleme söz konusudur, dolayısıyla borca aykırılığa dayanarak TBK m.112 hükmü uyarınca zararın giderilmesi talep edilebilecektir.

3.2.1.1.3.2.1. Kişisel Sağlık Verilerinin İşlendiği Sözleşmeler

Tedavi sözleşmesi (hekimlik sözleşmesi), hastaneye kabul sözleşmesi, iş sözleşmesi, tetkik ve inceleme sözleşmesi kişisel sağlık verilerinin işlendiği başlıca sözleşmelerdir.

Hekimlik sözleşmesi, serbest çalışan doktor tarafından hastaya belli bir süre sınırı olmaksızın ve herhangi bir sonuç vaat edilmeksizin hastanın menfaat ve iradesi ile tıp bilimine uygun teşhis ve tedavi uygulaması için kurulan sözleşmedir³⁸².

Hekimlik sözleşmesinin serbest çalışan bir doktor için asli edimleri teşhis ve tedavi hizmeti sağlama; hasta için ise alınan sağlık hizmetinin karşılığında ücret ödemedir³⁸³. Asli edimlerin yanı sıra hekimlik sözleşmesi kapsamında doktorun sır saklama yükümlülüğü, dolayısıyla kişisel sağlık verilerinin korunmasını sağlama yükümlülüğü yan edimi de söz konusudur³⁸⁴. Hekimlik sözleşmesi içerisinde doktor ve hasta arasında vekalet sözleşmesi ilişkisi mevcuttur. TBK m.506/2 hükmü ile doktor için hem özen hem de sadakat yükümlülüğü düzenlenmektedir. Sadakat yükümlülüğü, doktorun sağlık hizmeti sunumunun herhangi bir aşamasında öğrendiği hastaya ait kişisel sağlık verilerinin korunmasını da içermektedir³⁸⁵.

Hastaneye kabul sözleşmesi, yataklı teşhis ve tedavi hizmeti sunan özel hastane ile hasta arasında kurulan sözleşmedir³⁸⁶. Hastaneye kabul sözleşmesinin tarafları hastane işleticisi ve

³⁸⁰ Oğuzman/Öz, C.1, s.369 ; Gürbüz Erel, s.144.

³⁸¹ Taştan, s.112; Özdemir, Hayrunnisa, **Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması**, Seçkin Yayınları, Ankara, 2009, s.104 (Özdemir, Kişisel Veri)

³⁸² Özdemir, Hayrunnisa, “Hekimin Hukuki Sorumluluğu”, **Erciyes Üniversitesi Hukuk Fakültesi Dergisi**, C.11, S.1, 2016, s.40 (Özdemir, Hukuki Sorumluluk); İmançlı, s.211; Hakeri, s.888

³⁸³ Özdemir, Hukuki Sorumluluk, s.41-49.

³⁸⁴ Taştan, s.110.

³⁸⁵ Özdemir, Hukuki Sorumluluk, s. 63.

³⁸⁶ Hakeri, s.894; İmançlı s.215.

hasta olup doktor burada ifa yardımcısıdır³⁸⁷. Hastaneye kabul sözleşmesi vekalet, eser, satım, hizmet sözleşmesinin unsurlarını içermesi sebebiyle karma nitelikli bir sözleşmedir³⁸⁸. Hastaneye kabul sözleşmelerinde asıl edim tıbbi tedavinin sağlanması ve karşılığında hasta tarafından ücret ödenmesi olduğundan vekalet sözleşmesi hükümleri söz konusudur. Bu durumda hekimlik sözleşmesinde belirtildiği gibi TBK m.506/2 hükmü uyarınca özel hastane işleticisinin sadakat ve sır saklama yükümlülüğü mevcuttur³⁸⁹. Hastaneye kabul sözleşmesinin edimlerinin ifası sırasında kişisel sağlık verilerinin korunmaması durumunda hastane işleticisi, yan yükümlülüğüne aykırı hareket etmiş olacağından borca aykırılık söz konusu olacaktır. Bunun yanı sıra doktor tarafından gerçekleştirilen bir ihlal söz konusu olduğunda ise TBK m.116 hükmü sebebiyle ifa yardımcısının hukuka aykırı eyleminden ötürü özel hastane işleticisinin kusursuz sorumluluğuna başvurulması gerekmektedir. Doktor veya başka bir sağlık görevlisinin hukuka aykırı bir şekilde kişisel sağlık verilerini işlemesi durumunda bu kişilerin sözleşmenin tarafı olmamasından dolayı borca aykırılık sebebiyle sözleşmeden kaynaklı sorumluluğa dayanılamayacaktır.

Tetkik ve inceleme sözleşmeleri, hastanın hastalığının tanısının konulabilmesi için gereken tıbbi görüntüleme işlemleri ve laboratuvar işlemlerinin gerçekleştirilmesi ve bunun karşılığında hasta tarafından bir ücret ödenmesi edimlerini içeren isimsiz sözleşmelerdir. Tetkik ve inceleme sözleşmeleri doğrultusunda edimlerin gerçekleştirilmesi için kişisel sağlık verilerinin işlenmesi söz konusudur. Tetkik ve inceleme sözleşmelerinin eser sözleşmesi olması sebebiyle tetkik ve inceleme işlemlerini gerçekleştiren yüklenicinin sadakat borcu dolayısıyla kişisel sağlık verilerinin hukuka uygun işlemesi ve koruması gerekmektedir³⁹⁰.

Sağlık verilerinin işlendiği bir başka sözleşme, iş sözleşmeleridir. İşverenler, iş başvuruları zamanından başlayarak düzenli olarak sağlık raporları istemekte; çalışanlarının kişisel sağlık verileri üzerinde yüksek düzeyde erişime sahip olmaktadır. İş veren ve işçi arasında hiyerarşinin varlığı göz önünde bulundurulduğunda kişisel sağlık verilerinin korunması ayrı bir önem arz etmektedir. Nitekim TBK m.419 hükmü ile işçiye ait kişisel verilerin kullanımı sözleşmenin ifası için zorunlu olma hali ile sınırlandırılmaktadır. Sağlık verilerinin hassas veri niteliği taşıdığına ve hakkındaki özel düzenlemelerden ötürü iş sözleşmesinin ifası açısından gerekli olsa dahi işveren tarafından işlenmemesi gerektiğine

³⁸⁷ **Hakeri**, s.894.

³⁸⁸ **İmançlı**, s.215-216; **Hakeri**, s. 895.

³⁸⁹ **İmançlı**, s.216.

³⁹⁰ **İmançlı**, s.221.

dikkat etmek gerekmektedir³⁹¹. İşçinin üstlendiği edimin ifası için kişisel sağlık verisinin kullanılması zorunlu değil ise işveren tarafından işlenmemesi gerekmektedir³⁹². İş ilişkisi içerisinde işçinin sağlık verilerine ihtiyaç duyulmasının temel sebebi işverenin işçiye gözetme borcu kaynaklı iş yerinde sağlık ve güvenlik koşullarının sağlanabilmesi olduğundan sağlık raporlarına ihtiyaç duyulmaktadır³⁹³. Burada göz önünde bulundurulması gereken sağlık verilerinin tamamına erişimin gerekmediği, iş yeri hekimince kişisel sağlık verilerinin değerlendirmesinin yapılarak işverene bu değerlendirmenin iletilmesinin yeterli olduğudur³⁹⁴. Bu sayede kişisel sağlık verilerine ilişkin iş sözleşmesi doğrultusunda oluşabilecek ihlallerin önüne geçilmesi sağlanabilecektir. İşveren tarafından işçiye ait kişisel sağlık verilerinin işlenmesinin hukuka aykırı olmadığı durumlarda ise İş Kanunu m75/2 hükmü doğrultusunda sır saklama yükümlülüğü öngörülmekte olup TBK m.417/1 hükmü ile birlikte yorumlandığında işçinin kişiliğini korumanın işverenin yükümlülüğü olduğu ortadadır. İşçinin kişisel sağlık verilerinin işveren tarafından hukuka aykırı olarak işlenmesi durumunda, işveren işçinin uğradığı zararı borca aykırılık kaynaklı tazmin ile sorumludur³⁹⁵.

3.2.1.1.3.3. Sözleşme Benzeri Borç İlişkisinden Doğan Sorumluluk

Herhangi bir sözleşme ilişkisi kurulmadan önce veya sözleşme ilişkisinin artık mevcut olmadığı durumlarda da sorumluluktan söz etmek mümkündür. Tazminat talebinin bir başka hukuki dayanağı da dürüstlük kuralı kaynaklı sözleşme benzeri borç ilişkisinden doğan sorumluluktur.

Culpa in contrahendo sorumluluk, taraflardan birinin henüz sözleşme ilişkisi kurulmadan önce gerçekleştirilen görüşmeler esnasında dürüstlük kurallarına aykırı olarak kusurlu davranışının yarattığı zararları tazmin etme yükümlülüğüdür³⁹⁶. Söz konusu görüşmelerin ardından herhangi bir sözleşme ilişkisinin kurulmadığı ya da sözleşmenin geçersiz olduğu hallerde de culpa in contrahendo sorumluluk devam etmektedir³⁹⁷. Örneğin; henüz herhangi bir hekimlik sözleşmesi mevcut değilken kişisel sağlık verilerini içeren tetkik sonuçlarını doktor ile paylaşan kişi ilerleyen zamanda bu doktora tedavi olmasa dahi doktor,

³⁹¹ Çekin, s.270.

³⁹² Kartal, Serhat, **Türk Hukukunda İş Sözleşmesinin Sağlık Sebepleriyle Sona Ermesi**, On İki Levha Yayınları, İstanbul, 2020, s.168.

³⁹³ İmançlı, s.219.

³⁹⁴ Çekin, s.270-271.

³⁹⁵ İmançlı, s.220.

³⁹⁶ Oğuzman/Öz, C.1, s.37; Eren,1265.

³⁹⁷ Oğuzman/Öz, C.1, I, s.38.

kişisel sağlık verilerini hukuka aykırı bir şekilde işleme yoluna başvuramayacaktır; aksi takdirde zararın tazmini ile yükümlüdür. Doktorun, tanı veya tedavi için kendisine başvurmuş hastaya gerçek dışı izlenim vererek sağlık durumu hakkında yanlış bilgiler paylaşması da culpa in contrahendo sorumluluk örneklerindedir³⁹⁸. Bu duruma örnek olarak; sırf hastalardan daha fazla kişisel sağlık verisi toplayarak tetkikler üzerinden kanser teşhisi yapan bir yapay zeka uygulamasını eğitmeyi amaçlayan doktorun hekimlik sözleşmeleri sırasında gerek olmamasına rağmen kişisel sağlık verisi toplaması gösterilebilecektir.

Yargıtay Hukuk Genel Kurulu'nun 13.2.2013 tarihli E. 2012/ 13-1220, K. 2013/239 kararı; sözleşme görüşmeleri sırasında taraflar arasında dürüstlük kuralı temelli bir güven ilişkisi oluştuğu, bu güven ilişkisi sebebiyle tarafların birbirlerinin kişilik ve mal varlıklarına herhangi bir zarar vermemek için gereken dikkat ve özeni gösterme yükümlülüğü altında olduğunu ve görüşmeler arasında kişiler arasında artık hukuki bir ilişkinin doğması söz konusu olduğundan haksız fiil sorumluluğuna değil borca aykırılık hükümlerinin uygulanmasının uygun olacağını belirtmektedir³⁹⁹.

Dürüstlük kuralına dayanan bir başka sözleşme benzeri borç ilişkisi ise culpa post pactum perfectum (sözleşmenin art etkisi)dir. Sözleşmenin sona ermesi ile birlikte gerçekleşen hukuka aykırı fiillerden doğan zararlar haksız fiil kaynaklı sorumluluğa tabidir; çünkü artık ortada uygulanabilecek bir sözleşme hükmü dolayısıyla borca aykırılık söz konusu değildir. Fakat bazı hallerde sözleşme sona erse dahi dürüstlük kuralı ve güven ilişkisi sebebiyle bazı yükümlülükler devam eder ve bu hallerde herhangi bir ihlal söz konusu olduğunda sözleşmenin art etkisi kaynaklı sorumluluk söz konusudur. Doktorlar, tedavi sözleşmesi sona ermiş olsa dahi sadakat yükümlülüğü uyarınca sağlık verilerini hukuka uygun işleme yükümlülüğü altındadır⁴⁰⁰.

Sözleşmenin nisbiliği ilkesi gereği sözleşmeler yalnızca taraflar arasında hak ve borçlar doğmaktadır⁴⁰¹. Fakat bu durum sözleşmenin tarafı olmayan kişilerin sözleşmeden etkilenmediği anlamına gelmemektedir. Sözleşmeden etkilenen ama sözleşmenin tarafı olmayan üçüncü kişilerin uğradığı zararların tazmini için dayanak üçüncü kişiyi koruyucu etkili sözleşme olarak kabul edilebilecektir. Doktor ile hasta arasında hekimlik sözleşmesi kurulmaktadır, bu sözleşme uyarınca doktorun hasta tarafından kendisi ile paylaşılmış olan kişisel sağlık verilerini koruma yükümlülüğü söz konusudur. Hastalığının doğru tanısının

³⁹⁸ İmançlı, s.228; Özdemir, Hukuki Sorumluluk, s.37.

³⁹⁹ YHGK, E.2012/13-1220, K. 2013/239, T.13.2.2013), (erişim tarihi: 29.5.2023), www.lexpera.com

⁴⁰⁰ Özdemir, Kişisel Veri, s.157.

⁴⁰¹ Gürbüz Erol, s.155.

konulabilmesi adına ailesindeki diğer fertlerin sağlık durumlarını da doktor ile paylaşan hastanın babasının kişisel sağlık verisinin ihlal edilmesi durumunda sözleşmeye aykırılık söz konusu olacaktır. Fakat baba bu sözleşmenin tarafı olmadığından sözleşmeye aykırılık kaynaklı sorumluluğa dayanamayacaktır. Bu durumda babanın başvurabileceği sorumluluğun kaynağı dürüstlük kuralına dayanan sözleşme benzeri borç ilişkilerinden üçüncü kişiyi koruyucu etkili sözleşme kaynaklı sorumluluktur. Bu duruma kişisel verileri işleme sözleşmesi de örnek gösterilebilmektedir. Veri sorumlusu ve veri işleyen arasında kişisel verileri işleme sözleşmesi akdedildiğinde, veri sorumlusu kendine ait kişisel verileri değil üçüncü kişilere ait kişisel verilerin işlenmesi için veri işleyene başvurmaktadır. Dolayısıyla bu senaryoda kişisel veri ihlali söz konusu olduğunda bu zarara uğrayacak kişi sözleşmenin tarafları değil, veri sahibinin kendisidir⁴⁰². Bir doktor tarafından toplanan kişisel sağlık verilerinin yapay zeka geliştiricisine verilmesi ile yapay zekanın eğitilmesinin sağlanması durumunda, yapay zekanın gerçekleştirdiği işleme ile verisi ihlal edilen kişi veri sahibi olup zararlarının tazmini için başvurusunda haksız fiil veya sözleşmeden kaynaklı sorumluluk değil dürüstlük kuralına dayalı sorumluluk söz konusu olacaktır.

3.2.1.1.3.4. Vekaletsiz İş Görme

Türk Medeni Kanunu m.25/3 hükmü uyarınca; kişilik hakkı ihlal edilen kişinin tazminat dışında başvurabileceği bir diğer yol da vekaletsiz iş görme hükümleridir. Söz konusu iş görme, iş sahibi için değil iş görenin menfaati için gerçekleştirildiğinden gerçek olmayan vekaletsiz iş görme şeklindedir⁴⁰³.

Türk Borçlar Kanunu m.530 hükmü iş sahibinin, iş görenin menfaatine yapılmış olması durumunda, iş görmeden doğan faydaları edinme hakkı olduğunu belirtmektedir. Hüküm doğrultusunda; kişilik hakkı olan kişisel verisi saldırıya uğrayan kişi, vekaletsiz iş görme hükümlerine dayanarak, kendisine ait veri sayesinde elde edilmiş olan kazancın iadesini isteyebilmektedir.

Kişinin rızası olmaksızın sağlık verilerinin yapay zekanın eğitilmesi amacıyla yapay zeka üreticisine satılması halinde, veri sahibi satıştan elde edilen haksız kazancı talep etme hakkına vekaletsiz iş görme hükümlerince sahiptir.

⁴⁰² **Gülbüz Erol**, s.156.

⁴⁰³ **Zor**, s.202; **Eren**, s.831.

3.2.1.1.4. Yapay Zekanın Veri İhlali Durumunda Açılacak Dava Tarafları

3.2.1.1.4.1. Davacı

Kişisel Verilerin Korunması Kanunu ve TMK hükümlerince açılabilmesi belirtilen davalarda davacının kim olabileceğini tespit ederken öncelikle dikkat edilmesi gereken KVKK'nın kapsamının m.2 hükmü uyarınca yalnızca gerçek kişiler ile sınırlandırılmasıdır. Bu durumda kişisel sağlık verisinin işlenmesi ile veri ihlaline uğramış gerçek kişi tazminat; önleme, durdurma ve tespit davasında; vekaletsiz iş görme davasında davacı sıfatına sahip olabilmektedir.

3.2.1.1.4.2. Davalı

Kişisel sağlık verilerinin hukuka aykırı bir şekilde işlenmesi sebebiyle oluşan ihlallerde KVKK m.11 hükmü uyarınca gerçek veya tüzel kişi olan veri sorumlusu davalı konumundadır⁴⁰⁴. Yapay zeka aracılığı ile kişisel sağlık verilerinin işlenmesinde oluşabilecek ihlallerde sorumluluğuna başvurulacak kişi yine veri sorumlusudur.

KVKK m.12/2 hükmüne göre veri sorumlusunun yanında veri işleyen de varsa oluşan ihlallerde müştereken sorumluluk söz konusu olduğundan hem veri sorumlusu hem de veri işleyenden zararın tazmin talep edilebilmektedir⁴⁰⁵.

Yapay zekanın da denklem içerisinde yer aldığı durumlarda veri sorumlusunun ve dolayısıyla sorumluluğuna başvurulabilecek kişinin kim olduğunun tespit edilebilmesi için öncelikle yapay zekanın veri sorumlusu sıfatına sahip olup olmadığı sorununun çözülmesi gerekmektedir.

3.2.2. Yapay Zeka Sorumluluğu

Hak sahipliği ve borç yükümlülüğü, kanun koyucu tarafından toplumun sosyal yapısı göz önünde bulundurularak kişilik sıfatı aracılığı ile tanımlanmaktadır⁴⁰⁶. Bir diğer deyişle, yalnızca kişilik tanınanlar hak sahibi olabilmekte ve borç yükümlülüğü altında olarak sorumlu kabul edilebilmektedir. Farklı dönemlerde ve farklı yerlerde hukuki kişilik tanımlanması farklı

⁴⁰⁴ Taştan, s.202; Zor, s.207; Çavuşoğlu, s.137.

⁴⁰⁵ Taştan, s.202; Zor, s. 207.

⁴⁰⁶ Öztan, Bilge, **Medeni Hukukun Temel Kavramları**, Turhan Kitabevi, Ankara, 2014, s.221; Akipek/Akıntürk/Ateş, s.229-230.; Akdağ, Şükrü Yakup, “Yapay Zekanın Sorumluluğu Üzerine Düşünceler”, Ed. Başak Baysal, **Sorumluluk Hukuku Seminerler 2018**, İstanbul, 2019, s.10.; Kasap Atilla, “Güncel Gelişmeler Işığında Türk Hukukunda Yapay Zeka Varlıkları ve Hukuki Kişilik”, **Türk-Alman Üniversitesi Hukuk Fakültesi Dergisi**, C.4, S.2, 2022, Atilla, s.491,496.; Kara Kılıçarslan, Seda, “Yapay Zekanın Hukuki Statüsü ve Hukuki Kişiliği Üzerine Tartışmalar”, **Yıldırım Beyazıt Hukuk Dergisi**, C.4, S.2, 2019, s.372.

hukuk düzenlerinde farklı kapsamlarda yapılmıştır⁴⁰⁷. Geçmişten günümüze hak sahibi olup belli yükümlülükleri olan kişiler arasında Hindu putları, Yeni Zelanda’da bir kabilenin atası olarak kabul ettiği Whanganui nehri, bazı hukuklarda gemiler ve evcil hayvanlar yer almaktadır⁴⁰⁸. Günümüzde yapay zekanın önemi ve gün geçtikçe hayatımızda artan yeri düşünüldüğünde; yapay zeka için de kişilik tanınmasını beklemek yanlış olmayacaktır. Hukukumuzca, kanun koyucu tarafından kişilik bahsedilmeyen varlıkların mahkeme kararı ile kişi kabul edilmesi mümkün değildir, bu sebeple kişiliğin kanun koyucu tarafından hukuki düzenlemelerde yer alması önem arz etmektedir⁴⁰⁹.

3.2.2.1. Yapay Zekanın Hukuki Niteliği

Yapay zekanın hukuki niteliğini belirleyebilmek adına ortaya çeşitli görüşler atılmaktadır. Bu görüşler; yapay zekanın başlı başına herhangi bir hukuki statü tanımlanması gerekmeksizin var olması gerektiği ve dolayısıyla sorumluluğu olamayacağı, yapay zekanın kölelik statüsünde olduğu, yapay zekanın tüzel kişi olduğu, yapay zekanın temsilcisi olarak kendisini üreten kişilerin sorumluluğu olması gerektiği, yapay zekanın yapay insan modeli olduğu görüşü şeklindedir⁴¹⁰.

Yapay zekaya hukuki kişilik tanınması gerekmediğini savunan bir görüşe göre; yapay zeka ile ortaya çıkabilecek sorunlar sigorta sistemlerinin entegrasyonu ile çözülebilecektir, dolayısıyla yapay zeka eşya olarak kabul edilebilecektir⁴¹¹. Ülkemizde mevcut düzenlemelere bakıldığında yapay zekanın niteliği eşyadır⁴¹².

Yapay zekaya hukuki kişilik tanınması gerekmediğini savunan başka bir görüşe göre; her ne kadar yapay zeka eşya kadar basite indirgenemeyecek olsa da kendisinin hiçbir zaman insan olması da mümkün görünmediğinden köle olarak kabulü gerekmektedir⁴¹³. Köleliğin

⁴⁰⁷ Akdağ, s.9.

⁴⁰⁸ Akdağ, s.9.

⁴⁰⁹ Kasap, s. 495

⁴¹⁰ Sert Sütçü, s.71.

⁴¹¹ Ersoy, s.85; Kara Kılıçarslan, s.379 Pérennou, Thomas, “State of the Art On Legal Issues”, 2014, s.10, (erişim tarihi: 4.6.2023), <https://ethicaa.greyc.fr/media/files/ethicaa.delivvable.1.pdf>.

⁴¹² Sert Sütçü, s.71; Güner, Cemil, “Yapay Zekanın Verdiği Zarardan Doğan Sözleşme Dışı Sorumluluğa Uygulanacak Hukuk”, *Uyuşmazlık Mahkemesi Dergisi*, C.8, S.15, 2020, s.242.

⁴¹³ Kara Kılıçarslan, s.378-379.

kaldırılması için verilen mücadeleler düşünüldüğünde bu görüşe hukuki bir çözüm de sunmadığı ortada olduğundan karşı çıkılmaktadır⁴¹⁴.

Yapay zekaya hukuki kişilik tanınması gerektiğini savunan bir görüşe göre; yapay zekanın insan olmadığı, insanı taklit eden bir mekanizma olduğu ortadadır; fakat bu araçları basit bir makine ya da eşya olarak görmek mümkün değildir; en azından bu araçlar için insan dışındaki varlıklara tanındığı gibi tüzel kişilik tanınarak hukuki tanıma verilmesi gerekmektedir⁴¹⁵.

Yapay zekaya hukuki kişilik tanınması gerektiğini savunan bir başka görüşe göre; yapay zekanın insan olmadığı fakat insana özgü otonom yapıya sahip olması sebebi ile tüzel kişilik statüsünden ayrılmakta, kendisi için yeni kişilik modellerine ihtiyaç duyulmaktadır⁴¹⁶.

Yapay zekaya hukuki kişilik tanınmasına ilişkin bir başka görüşe göre; yapay zeka ile insan arasında vekalet ilişkisinin varlığı söz konusudur⁴¹⁷.

Sayılanların yanında Avrupa Parlamentosu'nun 2017 tarihli bir raporu⁴¹⁸ ile yapay zekaya gerçek kişi ve tüzel kişiden ayrı bir hukuki statü türü olarak elektronik kişilik verilmesi önerilmektedir⁴¹⁹. Rapora göre elektronik kişilik tanınan yapay zekanın hak ve borçlarından söz edilebilecek; sorumluluğunun doğduğu durumlarda zararın tazmininin sağlanabilmesi için sigorta ya da tazminat fonuna başvurulabilecektir⁴²⁰.

Mevcut sistemde yapay zekaya tanınmış gerçek veya tüzel kişilik bulunmamaktadır. Yapay zekaya herhangi bir hukuki kişilik tanınmamaktadır. Dolayısıyla sebep olduğu zararlardan ötürü yapay zekanın sorumluluğundan söz etmek ve yapay zekanın davalı sıfatına sahip olması da mümkün değildir⁴²¹.

⁴¹⁴ **Ersöy**, s.95; **Bak**, Başak, “Medeni Hukuk Açısından Yapay Zekanın Hukuki Statüsü ve Yapay Zeka Kullanımından Doğan Hukuki Sorumluluk”, **Türkiye Adalet Akademisi Dergisi**, S.35, 2018, s.218.

⁴¹⁵ **Kara Kılıçarslan**, s.379-380.

⁴¹⁶ **Kara Kılıçarslan**, s.381; **Bak**, s.230.; **Ersöy**, s.87

⁴¹⁷ **Ersöy**, s.92.

⁴¹⁸ **Report with Recommendations To the Commission on Civil Law Rules on Robotics**, (erişim tarihi: 8.6.2023), https://www.europarl.europa.eu/doceo/document/A-8-2017-0005_EN.html

⁴¹⁹ **Bak**, s.217.; **Ersöy**, s.87; **Kara Kılıçarslan**, s.380.

⁴²⁰ European Parliament, Directorate-General for Internal Policies of the Union, Nevejans, Nathalie, **European Civil Law Rules in Robotics (Study)**, Publications Office of the European Union, s.15, (erişim tarihi: 10.6.2023) <https://op.europa.eu/en/publication-detail/-/publication/19ea0f1c-9ab0-11e6-868c-01aa75ed71a1/language-en> [https://www.europarl.europa.eu/RegData/etudes/STUD/2016/571379/IPOL_STU\(2016\)571379_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2016/571379/IPOL_STU(2016)571379_EN.pdf)

⁴²¹ **Çavuşoğlu**, s.138.

3.2.2.2. Mevcut Düzenlemeler Işığında Yapay Zeka Sorumluluğu

Gün geçtikçe teknolojinin hayatımızda daha fazla yer etmesi yapay zeka sistemlerine de daha sık rastlamamıza sebep olmaktadır. Yapay zeka kullanımı birçok alan gibi sağlık bilimlerini de etkilemekte, bu durum fayda ile birlikte birtakım riskleri de beraberinde getirmektedir. Tanıdan tedaviye, ilaç üretiminden hasta bakımına yapay zeka insan hayatına dokunmaktadır; bu sırada yapay zeka hem gelişebilmek için kişisel sağlık verileri ile eğitilmekte hem de bu veriler sayesinde faaliyet gösterebilmektedir. Yapay zekanın veri kullanımı sırasında ve sonrasında gösterdiği faaliyetlerde kişiler zarar görebilmektedir. Yapay zekanın veri işleme ile oluşan zarar bir sözleşmeden doğabileceği gibi haksız fiilden de kaynaklanabilmektedir. Yapay zekanın sebep olduğu bir zarar söz konusu olduğunda sorumluluğun süjesinin kim olduğu tespit edilmeli ve zarar tazmin edilmelidir. 3.2.2.1 bölümünde belirtildiği üzere, hukukumuzda yapay zekaya henüz kişilik tanınmamaktadır, dolayısıyla yapay zekanın veri işlemesinden oluşan zararların tazmini için bizzat yapay zekanın sorumlu olacağı kabul edilemeyecektir.

Yapay zekanın veri işleme ile ortaya çıkan zararların sebebi yazılım ya da donanımı ile ilgili kusurlar olabileceği gibi yapay zeka sisteminin herhangi bir insan müdahalesi olmaksızın kendi kendini eğittiği esnada ortaya çıkan yapay zekanın otonom kararı kaynaklı bir zarar da olabilmektedir⁴²². Henüz mevcut hukuk düzenlemelerimizde, yapay zekaya hukuki kişilik tanınmadığı için yapay zekanın sözleşme ilişkilerinde taraf olarak kabulü söz konusu değildir, yapay zekayı içeren kişisel sağlık verilerini işleme faaliyetlerinde yapay zekanın, sözleşmenin gerçekleştirilmesine yardımcı bir mekanizma veya sözleşmenin edimi olarak kabul edilmesi gerekmektedir⁴²³. Herhangi bir sözleşmenin olmadığı durumlarda da sözleşme sorumluluğunda olduğu gibi yapay zekanın hukuki niteliği önem arz etmektedir, yapay zekanın sorumluluk süjesi olabilmesi için öncelikle faaliyete kişisel katılım ile hesap verebilirlik döngüsünde yer alması gerekmektedir⁴²⁴.

Yapay zekanın faaliyetlerinden oluşan zararalarda mevcut sorumluluk hükümlerinin uygulanabilmesi için zararın doğmasına sebep veren kişinin kullanıcı, üretici ya da ürün sahibi gibi belirlenebilir kişi olması gerekmektedir⁴²⁵.

⁴²² Eroğlu Sarı, s.34.

⁴²³ Eroğlu Sarı, s.36.

⁴²⁴ Murphy, Robin R./ Woods, David D., "Beyond Asimov: Three Laws of Responsible Robotics", **IEEE Intelligent Systems**, C. 24, S.4, 2009, s.15-16, <https://ieeexplore.ieee.org/document/5172885>

⁴²⁵ Pepito, Joseph Andrew/Vasquez, Brian A./ Locsin, Rozzano C. "Artificial Intelligence and Autonomous Machines: Influences, Consequences, and Dilemmas in Human Care." **Health**, C.11, S.7, 2019, s. 936. <https://doi.org/10.4236/health.2019.117075>

3.2.2.2.1. Ürün Sorumluluğu

Üreticinin hatalı ve kusurlu üründen dolayı kusursuz sorumluluğu hakkında temel düzenleme 7223 sayılı Ürün Güvenliği ve Teknik Düzenlemeler Kanunu⁴²⁶’dur⁴²⁷. Kanun ürün güvenliğine ilişkin bir kanun olduğundan terim, kavram ve tanımlar ürün sorumluluğuna uygulanırken birtakım yanlış anlaşılmalara sebep vermeye açıktır⁴²⁸.

Ürün Güvenliği ve Teknik Düzenlemeler Kanunu m.6 hükmü uyarınca ürünün üreticisi, ürünün verdiği zararı giderme yükümlülüğü altındadır. Kanunun m.3/1 (g) hükmüne göre üretici “ürünü imal ederek veya ürünün tasarımını veya imalatını yaptırarak kendi isim veya ticari markası ile piyasaya arz eden gerçek veya tüzel kişi”yi ifade etmektedir. Yapay zeka tüketici malı olan bir üründür⁴²⁹. Ürün niteliği taşımakta olan yapay zekanın meydana getirdiği zarar üretici tarafından tazmin edilmelidir. Üreticinin kusursuz sorumluluk hallerinden biri olan ürün sorumluluğu söz konusudur⁴³⁰. Ürün sorumluluğu, düzgün ve güvenli olmayan bir ürün sebebiyle, kişinin vücut bütünlüğü ya da malvarlığında oluşabilecek bir zararın tazminini sağlayan sorumluluk çeşididir⁴³¹.

Hukuka uygun olmayan eylemlerde bulunan bir yapay zeka uygulaması ayıplı bir üründür. 6502 sayılı Tüketicinin Korunması Hakkında Kanun⁴³² m.8 hükmü uyarınca ayıplı mal, tüketiciye teslim anında tarafların kararlaştırdığı modele uygun olmayan ya da objektif olarak sahip olması gereken özelliklere sahip olmayan maldır. Ürün sorumluluğu, ayıplı maldan doğabilmesinin yanında yalnızca tüketici hukukunun konusu olan ayıplı mal ile sınırlı değildir ve ayıplı mal sorumluluğundaki gibi sözleşme ilişkisi söz konusu olmak zorunda değildir⁴³³. Bir ürünün ayıplı olarak kabul edilmemesi için öncelikle üretici tarafından yasal şartlara uygun

⁴²⁶ RG.: T.12.3.2020/S.31066

⁴²⁷ İlgili Kanun, 85/374 sayılı Avrupa Birliği Konsey Yönergesi’ni esas alarak düzenlendiğinden, 3.2.2.2.1. başlığında hem Yönerge hem de Türk hukukuna atıflar ile üreticinin sorumluluğundan bahsedilmektedir.

⁴²⁸ Polat, Cemre, “Türk ve Avrupa Birliği Hukukunda Ürün Sorumluluğu”, **Ankara Üniversitesi Hukuk Fakültesi Dergisi**, C. 70, S.4, 2022 , ss.973-1041 <https://doi.org/10.33629/auhfd.988504>

⁴²⁹ **Liability for Artificial Intelligence and Other Emerging Digital Technologies**, Expert Group on Liability for New Technologies, s.15-16 (erişim tarihi: 10.6.2023), https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/JURI/DV/2020/01-09/AI-report_EN.pdf; **Pepito**, s.938-939; **Eroğlu Sarı**, s.86

⁴³⁰ Kanışlı, Erhan, “Ürün Güvenliği ve Teknik Düzenlemeler Kanunu (ÜGTDK) Uyarınca Üreticinin Sorumluluğu, **İstanbul Hukuk Mecmuası**, C.78, S.3, 2020, s.1422; Doğan, Vahit, **Milletlerarası Özel Hukuk**, 8. Bs., Savaş Yayınevi, Ankara, 2022, s.245.

⁴³¹ **Kanışlı**, s.1419; **Doğan**, s.233.

⁴³² RG.: T.28.11.2013, S.28835

⁴³³ **Doğan**, s.234.

şekilde tasarlanmış ve üretilmiş olması gerekmektedir⁴³⁴. Bunun yanında yapay zekanın beklenen güvenliği sağlayarak çevresine zarar vermemesi gerekmektedir⁴³⁵. 7223 sayılı Kanun m.3/1 (e) hükmü ile güvenli ürün “*kullanım süresi, hizmete sunulması, kurulumu, kullanımı, bakımı ve gözetimine ilişkin talimatlara uygun ve normal kullanım koşullarında kullanıldığında risk taşımayan veya sadece ürünün kullanımına özgü asgari risk taşıyan ve insan sağlığı ve güvenliği için gerekli düzeyde koruma sağlayan ürün*”ü ifade etmektedir. Kişisel verilerin ihlal edilmesi durumunda kişinin zarara uğrayabileceği ve veri güvenliğinin sağlanmasının da beklenen güvenlik standartları arasında değerlendirilmesi gerektiği göz önünde bulundurulduğunda; kişisel verilerin korunması için gerekli tedbirleri almadan üretilmiş bir yapay zeka ürününün de ayıplı ürün olarak kabul edilmesi gerektiği kanaatindeyiz.

Yapay zeka üreticisinin tasarım hatası, üretim hatası ve pazarlama hatası olmak üzere üç temel ürün hatasından söz edilebilmektedir⁴³⁶. Yapay zekanın programlanması sırasında oluşan hatalar tasarım hatasıdır. Programlanma sırasında yapay zekanın dışarıdan gelebilecek tehlikelerden korunmasına dair gerekli koruma mekanizmaları geliştirilmemiş ise tasarım hatasından söz edilebilecektir⁴³⁷. Yapay zeka ile kişisel sağlık verilerinin işlendiği durumlarda dikkat edilmesi gereken teknik korumaların sağlanmaması sonucunda veri ihlaline sebep verildiği durumlarda oluşan zarardan yapay zeka üreticisinin tasarım hatası kaynaklı ürün sorumluluğu oluşacaktır. Üretim hatası, ürünün üretildiği esnada ortaya çıkan hatalardır⁴³⁸. Pazarlama hatası, ürün tüketicisine yeterli bilgilendirme sağlanmaması durumunda ortaya çıkan hatadır⁴³⁹. Yapay zeka ile veri işlendiği durumlarda, ürünün kullanımı sırasında toplanacak verilerin hangilerinin zorunlu, hangilerinin izne dayalı olduğu ve hangi koşullarda işleme yapılacağı hakkında tüketiciye bilgi verilmemesi sebebiyle oluşabilecek zararlar pazarlama hatası kaynaklı kabul edilebilecektir.

Yapay zeka, yalnızca kendisine verilen veri ve komutlara bağlı kalmamakta, kendi kendini eğiterek kontrol altında kalmadan eylemlerde bulunabilmektedir. Bu durum yapay zekanın üreticisinin dahi yapay zeka tarafından gerçekleştirilen faaliyetleri ve potansiyel zararları tahmin edebilmesini engellemektedir. Üretici tarafından yapay zeka eylemlerinin öngörülememesi, yapay zekanın faaliyetinin gerçekleşmesindeki illiyet bağıını ortadan

⁴³⁴ **Ethics Guidelines for Trustworthy AI**, High Level Expert Group on Artificial Intelligence, s.6

⁴³⁵ **Eroğlu Sarı**, s.87; **Pepito**, s.935-936.

⁴³⁶ Barfield, Woodrow, "Liability for Autonomous and Artificially Intelligent Robots", **Paladyn, Journal of Behavioral Robotics**, C. 9, S.1, 2018, s.196. <https://doi.org/10.1515/pjbr-2018-0018>

⁴³⁷ **Kapancı**, s.180.

⁴³⁸ **Eroğlu Sarı**, s.86.

⁴³⁹ **Barfield**, s.196.

kaldırmamaktadır⁴⁴⁰. Üreticilerin yapay zekanın davranışını öngöremez hale gelmelerinden ötürü sorumluluğunun olmadığı kabulü durumunda, yapay zekanın faaliyetinden zarar görenler için katlanılması beklenemeyecek bir mağduriyet doğmaktadır. Yapay zeka makine öğrenmesi sebebiyle dışarıdan müdahale olmaksızın kendi kendine geliştirdiği faaliyet sebebiyle kişiye zarar verdiğinde, bu durum ürünün sahip olduğu öğrenme kapasitesinin bir sonucu olduğundan üreticinin sorumluluğu devam etmektedir⁴⁴¹.

Ürün sorumluluğu kapsamında, yapay zekanın veri ihlali ile zarara uğrayan kişilerin, kusursuz sorumluluk hükümlerine dayanarak üreticiye karşı maddi manevi tazminat talebinde bulunma hakkı bulunmaktadır.

3.2.2.3. Yapay Zekaya Hukuki Nitelik Tanınması Durumunda Sorumluluk

Mevcut hukuk düzenimizde henüz yapay zekaya hukuki kişilik tanınmamaktadır. Bu hali ile yapay zeka eşya olarak kabul edilmekte ve direkt kendisine yöneltilebilen bir sorumluluk söz konusu olamamaktadır. Yapay zekanın hukuki niteliğine dair yapılan son öneri Avrupa Parlamentosunca hazırlanan Rapor'da yer almaktadır. Bu sayede yapay zekanın sebep olabileceği zararların tazminine yönelik sorunlar çözülebilecektir. Rapora göre; yapay zekaya elektronik kişilik tanınması gerekmektedir. Bu sayede yapay zekanın sebep olduğu bir zararda elektronik kişiliği olan yapay zekaya dava açılabilir⁴⁴². Yapay zekanın sebep olduğu zararın tazmininin sağlanabilmesi için sigorta programı ve tazminat fonu gibi önerilerde bulunmaktadır⁴⁴³.

Elektronik kişiliğin kabul edilmesi halinde TBK m.49 ve devamı hükümleri kıyasen uygulanabilir hale gelebilecektir⁴⁴⁴. TBKm.49 hükmü uyarınca yapay zekanın haksız fiil sorumluluğundan söz edilebilecektir. Bunun için hukuka aykırı fiil, zarar, nedensellik bağı ve kusur şartının sağlanması gerekmektedir.

⁴⁴⁰ Eroğlu Sarı, s.84.

⁴⁴¹ Haagen, Christian, *Verantwortung für Künstliche Intelligenz: ethische Aspekte und zivilrechtliche Anforderungen bei der Herstellung von KI-Systemen*, 1. Baskı, Nomos, Baden-Baden, 2021 s.320

⁴⁴² *Suggestion for A Green Paper On Legal Issues in Robotics*, EuRobotics, The European Robotics Coordination Action, 31.12.2012, s.61 (erişim tarihi 11.6.2023), https://www.unipv-lawtech.eu/files/euRobotics-legal-issues-in-robotics-DRAFT_6j6rvjyp.pdf

⁴⁴³ *European Civil Law Rules in Robotics*, s.6,14-16.

⁴⁴⁴ Eroğlu Sarı, s.53.

3.2.2.4. Mevcut Hukuki Düzendeki Sorumluluk Üzerine Genel Değerlendirme

Yapay zekaya kanun koyucu tarafından henüz herhangi bir hukuki statü tanınmamasından dolayı, kişisel sağlık verilerinin hukuka aykırı şekilde işlenmesi sonucunda oluşacak zararların sorumluluğu yapay zekaya ait olamamaktadır. Kişisel sağlık verilerinin hukuka aykırı olarak işlendiği durumlarda sorumluluğun ileri sürülebileceği asıl kişi veri sorumlusu olup veri işleyen varlığı durumunda ise müteselsil sorumluluk söz konusudur. Yapay zekanın veri işlemesi sonucunda doğan zararlardan yapay zeka üreticisi kusursuz sorumlu olması 3.2.2.2.1 başlığında açıklanmıştır.

Yapay zeka üreticisi, veri sorumlusu ya da veri işleyen olabilecektir. KVKK m.3/1 (1) hükmü uyarınca veri sorumlusu “*kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi*” olarak tanımlanmaktadır. Örneğin; yapay zeka üreticisi bir sağlık uygulaması için bir algoritma kullanarak hastaların kişisel tıbbi geçmişini, tetkik sonuçlarını içeren hasta verilerini analiz etmek istemektedir. Bu veri setine ulaşabilmek için bir hastane ile anlaşma yaptığında, hastaneden elde ettiği veri seti sayesinde algoritmasını geliştirecek, yapay zeka uygulamasını bu veriler ile eğitebilecek ve hastalara teşhis ve tedavi önerisinde bulunan bir sağlık uygulaması geliştirebilecektir. Bu örnekte yapay zeka üreticisi, veri setinin kullanım amacını ve raporlanma şeklini kararlaştıran taraf olduğundan kişisel sağlık verilerini işleme amacını ve araçlarını belirlemekte olduğundan veri sorumlusudur. KVKK’de düzenlenmiş yükümlülüklerini yerine getirmediği takdirde, hukuka aykırı işleme dolayısıyla oluşacak zararlardan ve yapay zekanın kişisel veri işlemesi sonucunda ortaya çıkabilecek algoritmik sapma, ayrımcılık gibi durumlardan kaynaklanan zararlardan, veri sorumlusu sıfatını taşıyan yapay zeka üreticisi sorumlu olacaktır.

Yapay zeka üreticisi veri işleyen sıfatı ile de sorumlu olabilmektedir. KVKK m.3/1 (ğ) hükmünde veri işleyen “*veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi*” olarak düzenlenmektedir. Örneğin; bir hastane, hastaların MR görüntülerini yapay zeka aracı ile analiz edip teşhise karar vermek için destek sağlamak amacıyla bir yapay zeka üreticisi ile anlaşma yapmaktadır. Hastane, yapay zeka üreticisine sağlık veri tabanında yer alan MR görüntülerini sağlamakta; yapay zeka üreticisi de bu sağlık verilerini işleyerek hastalık tespitinde bulunabilecek algoritma üzerinde çalışmaktadır. Bu durumda; kişisel sağlık verisinin işlenme amacı hastane tarafından belirlenmekte, yapay zeka üreticisi verileri veri sorumlusu olan hastanenin verdiği yetkiye dayanarak işlemektedir. Yapay zeka üreticisinin işleme sırasında veriyi sağlayan hastanenin talimat ve düzenlemesine uymak zorunda olduğu da göz önünde bulundurulduğunda; yapay zeka üreticisi veri işleme sürecine

katılımından dolayı veri işleyen sıfatı ile sorumlu olmaktadır. KVKK m.12/2 hükmü uyarınca veri sorumlusu olan hastane ve veri işleyen yapay zeka üreticisi müştereken sorumludur.

3.2.2.5. Yapay Zeka ve Kusursuz Sorumluluk

Hukukumuzda yapay zekaya ilişkin özel bir kusursuz sorumluluk hali düzenlemesi bulunmamaktadır. Yapay zekadan kaynaklanan zararlarda da TBK uyarınca kusur sorumluluğu esas, kusursuz sorumluluk istisnaidir. TBK ve TMK’de düzenlenen mevcut kusursuz sorumluluk hallerinin yapay zeka açısından incelemesi ise şu şekilde yapılabilecektir:

Yapay zekanın TBK m.66 hükmünde düzenlenen adam çalıştırmanın kusursuz sorumluluğu haline dahil edilmesi mümkün değildir; çünkü adam çalıştırmanın sorumluluğundan söz edilebilmesi için yapay zekanın öncelikle kendi haksız fiili için kusurlu sorumluluğa sahip olabilecek kişiliğinin olması ve arada bir istihdam ilişkisinin olması gerekmektedir⁴⁴⁵.

Türk Borçlar Kanunu m. 67 hayvan bulunduranın kusursuz sorumluluğu hükmü; yapay zekanın zekası, öğrenmesi ve eylemlerde bulunması niteliği bakımından hayvan ile karşılaştırılamayacak kadar komplike olduğunu ve dolayısıyla hayvan bulunduranın kusursuz sorumluluğunun yapay zekayı değerlendirmede yeterli olamayacağını göstermektedir⁴⁴⁶. Hayvan bulunduranın sorumluluğunun kıyas yolu ile yapay zekadan kaynaklanan zararlara uygulanması mümkün değildir⁴⁴⁷.

Türk Medeni Kanunu m.369 hükmü ev başkanının küçük ve kısıtlının eylemlerinden kaynaklanan kusursuz sorumluluğunu düzenlemektedir. İlgili hükümde ev başkanının sorumluluğuna sebep olan kişiler sayıldığından kıyas yolu ile yapay zekanın eylemlerine uygulanması hukukumuzca mümkün değildir⁴⁴⁸.

Mevcut düzenlemelerden yapay zeka ile oluşan zararlara uygulanması için en benzer olan TBK m. 71 tehlike sorumluluğu hükmüdür. İlgili hüküm uyarınca; yapay zekanın bir işletme mahiyet veya faaliyetinde kullanılması ve tehlike arz etmesi durumunda tehlike sorumluluğuna konu olması mümkündür; bu unsurlardan birinin eksikliği halinde yapay zeka kullanımı sonucu oluşan zararın tehlike sorumluluğu kapsamında değerlendirilmesi mümkün değildir⁴⁴⁹.

⁴⁴⁵ **Bak**, s.222-223; Onur, “Yapay Zekanın Sebep Olduğu Zararlardan Doğan Sorumluluk”, **Türkiye Barolar Birliği Dergisi**, S.147, İstanbul, 2020, s.271.

⁴⁴⁶ **Bak**, s.223.

⁴⁴⁷ **Sarı**, s.273.

⁴⁴⁸ Akkurt, Sinan Sami, “Yapay Zekanın Otonom Davranışlarından Kaynaklanan Hukuki Sorumluluk”, **Uyuşmazlık Mahkemesi Dergisi**, C.7, S.13, 2019, s.49.

⁴⁴⁹ **Sarı**, s.299.

Sayılan mevcut kusursuz sorumluluk halleri, yapay zekanın gelişimi düşünüldüğünde yetersiz olup yeni bir önermede bulunmamaktadır⁴⁵⁰. Yapay zekanın hukuki niteliğine dair yapılan son öneri Avrupa Parlamentosunca hazırlanan Rapor'da yapay zeka kullanımı tehlikeli faaliyet olarak kabul edilmekte ve oluşabilecek zararlar için tehlike esasına dayanan kendine özgü bir kusursuz sorumluluk hali düzenlenmesi ve yapay zekaya elektronik kişilik hukuki statüsü tanınması önerilmektedir⁴⁵¹.

Yapay zekaya kişilik tanınması halinde; yapay zekanın ayırt etme gücüne sahip olmaması ya da ayırt etme gücünü yitirmesi durumunda oluşabilecek zararlarda kusur şartı aranmaksızın TBK m.65 hakkaniyet sorumluluğu hükmü gereği sorumluluk söz konusu olabilecektir. Fakat hukuki kişilik tanınmaksızın yapay zekanın hakkaniyet sorumluluğunun temeli olan ayırt etme gücünden yoksun kişi olarak kabul edilmesi ve dolayısıyla hakkaniyet sorumluluğuna başvurulabileceğinin söylenmesi mümkün değildir⁴⁵². Yapay zekanın ayırt etme gücünün kaybolduğu durumlar için; teknik aksaklıklar, üretimde ya da tasarımda ortaya çıkan hatalar ile dışarıdan sisteme müdahale edilmesi durumu örnek gösterilebilecektir⁴⁵³. Örneğin; yapay zekanın hacklenmesi sonucunda yapay zekanın faaliyeti ile kişisel sağlık verilerinin ihlalden doğan zarar ortaya çıkmakta ise yapay zekanın ayırt etme gücü kaybı söz konusu olacak, yapay zekanın verdiği zarardan TBK m.65 hükmü uygulanabilecektir. Yapay zekanın öğrenmesi sırasında gerçekleşen faaliyetlerde oluşan zararlarda ise, yapay zekanın üreticisinin sorumluluğu söz konusu olabilecektir⁴⁵⁴.

3.2.3. Uygulanacak Hukuk Meselesi

Yapay zeka uygulamaları, genellikle tek ülkede kullanılmak için tasarlanmamaktadır. Bu durum yapay zekanın faaliyetinden doğan bir zararda sorumluluğa karşı uygulanacak hukuku etkilemektedir. Hukuki bir olay ya da ilişkinin yabancı bir hukuk düzenini de ilgilendirdiği durumlarda, bir başka deyişle yabancılık unsuru içeren konularda, hangi hukukun uygulanacağını tespiti gerekmektedir⁴⁵⁵.

Yapay zekanın verdiği zarara ilişkin uyuşmazlığın yabancı unsur içermesi durumunda; kanunlar ihtilafı hukuku ile uygulanacak hukukun tespiti için uygulama alanı bulmaktadır.

⁴⁵⁰ **Bak**, s.223.

⁴⁵¹ **Bak**, s. 224.

⁴⁵² **Sarı**, s.268.

⁴⁵³ **Eroğlu Sarı**, s.55.

⁴⁵⁴ **Eroğlu Sarı**, s.57.

⁴⁵⁵ **Doğan**, s.6-7.

Yapay zekanın sorumluluğu kaynaklı uyuşmazlıklarda uygulanacak hukuka dair herhangi özel bir düzenleme bulunmamaktadır. Yapay zeka uygulamaları tarafından kişisel veriler kaydedildiğinde veri ihlali ile kişilik hakkının ihlali doğmakta; maddi ya da manevi zarar sebebiyle sorumluluk doğabilmektedir⁴⁵⁶. Yapay zeka faaliyetleri ile şahıs ve malvarlığında meydana gelen zararlarda uygulanması gereken sorumluluk haksız fiil sorumluluğudur; 5718 sayılı Milletlerarası Özel Hukuk ve Usul Hukuku Hakkında Kanun haksız fiil sorumluluğuna ilişkin düzenlemeler, yapay zeka için de uygulanabilecektir⁴⁵⁷.

Yabancılik unsuru taşıyan uyuşmazlığa uygulanacak hukukun tespit edilebilmesi için öncelikle uyuşmazlığın kaynağı olan hukuki ilişkinin hakim hukukuna göre vasıflandırılması gerekmektedir⁴⁵⁸. Hukuki işlemin vasıflandırılmasının ardından, uygulanacak hukukun tespiti için MÖHUK hükümlerinin incelenmesi gerekmektedir.

Yapay zekanın faaliyetleri ile verdiği zarar MÖHUK m.34 ve devamı hükümlerince değerlendirilmelidir. Haksız fiil kaynaklı uyuşmazlıklarda kusurlu ya da kusursuz sorumluluk olması fark etmeksizin uygulanacak hukukun tayini aynıdır⁴⁵⁹.

Milletlerarası Özel Hukuk ve Usul Hukuku Hakkın Kanun'un m.35 hükmü yapay zeka ile veri işlemesinden doğan zararlar hakkında sorumluluk uyuşmazlıklarına uygulanabilecektir. Yapay zeka tarafından işlenen kişisel verilerin hatalı bir işlemle başka kullanıcılar tarafından erişilebilir hale gelmesi ya da kişisel verinin alenileşmesi durumunda uğranılan zararın tazmini için uygulanacak hukukun tespiti MÖHUK m.35 hükmü ile belirlenecektir⁴⁶⁰. MÖHUK m.35 hükmü: “ (1) Kişilik haklarının, basın, radyo, televizyon gibi medya yoluyla, internet veya diğer kitle iletişim araçları ile ihlâlden doğan taleplere, zarar görenin seçimine göre;

a) Zarar veren, zararın bu ülkede meydana geleceğini bilecek durumda ise zarar görenin mutad meskeni hukuku,

b) Zarar verenin işyeri veya mutad meskeninin bulunduğu ülke hukuku veya

c) Zarar veren, zararın bu ülkede meydana geleceğini bilecek durumda ise zararın meydana geldiği ülke hukuku,

uygulanır.

(2) Kişilik haklarının ihlâlinde cevap hakkı, süreli yayınlarda, münhasıran baskının yapıldığı ya da programın yayınlandığı ülke hukukuna tâbidir.

(3) Maddenin birinci fıkrası, kişisel verilerin işlenmesi veya kişisel veriler hakkında bilgi alma hakkının sınırlandırılması yolu ile kişiliğin ihlâl edilmesinden doğan taleplere de uygulanır.” şeklindedir.

⁴⁵⁶ Güner, s.235; Akkurt, s.43-44.

⁴⁵⁷ Güner, s. 236-237.

⁴⁵⁸ Doğan, s.180., 183; Nomer, s.104.

⁴⁵⁹ Doğan, s.445.; Nomer, s.356; Güner, s.245.

⁴⁶⁰ Güner, s.246.

Yapay zeka ile kişisel veri ihlaline, kişinin hastane bünyesinde saklı tutulması gereken sağlık kayıtlarının hastane tarafından kullanılan yapay zeka uygulamasınca internet sitesinde yayımlanması veya hasta dışındaki kişilere e-mail ile gönderilmesi örnek verilebilecek ve örnekte kişinin kişilik hakkı ihlali söz konusu olacaktır⁴⁶¹. Bu durumda; MÖHUK m.35/3 uyarınca kişisel verilerin ihlalinin doğan taleplere de m.35 hükmü uygulanmaktadır.

Yapay zeka tarafından gerçekleştirilen veri ihlallerinde uygulanacak hukuk veri sahibinin mutad meskeni hukuku; yapay zeka üreticisinin işyeri ya da mutad meskeninin bulunduğu ülke hukuku; veri ihlalinin meydana geldiği ülke hukukudur. Yapay zekanın birden fazla ülkede kullanıldığı göz önünde bulundurulduğunda; zararın birden çok yerde aynı anda ortaya çıkabiliyor olmasının, birçok ülke hukukunun söz konusu uyuşmazlığa uygulanabilir hale gelmesine sebep olduğu kanaatindeyiz. Bu belirtilen hukuklar için zarara uğrayan veri sahibinin seçimlik hakkı söz konusudur. Bu sayılan hukuklara ek olarak; MÖHUK m.34/5 hükmü uyarınca haksız fiil sonrasında taraflar uyuşmazlığa uygulanacak hukuku seçebilecektir⁴⁶². Yapay zekanın sebep olduğu zararlarda da kusursuz sorumluluk hükümleri uyarınca yapay zeka üreticisi, kullanıcısı ve zarar gören kişinin anlaşarak uyuşmazlığa hangi hukukun uygulanacağını seçmesi mümkündür⁴⁶³.

Yapay zeka tarafından veri işleme sonucunda oluşan zarar ayıplı yapay zeka ürünü sebebiyle oluşmuş ise yapay zeka üreticisinin sorumluluğu kapsamındaki uyuşmazlıklar için uygulanacak hukuk MÖHUK m.36 hükmünde “İmal edilen şeylerin sebep olduğu zarardan doğan sorumluluğa, zarar görenin seçimine göre, zarar verenin mutad meskeni veya işyeri hukuku ya da imal edilen şeyin iktisap edildiği ülke hukuku uygulanır. İktisap yeri hukukunun uygulanabilmesi için zarar verenin, mamulün o ülkeye rızası dışında sokulduğunu ispat edememiş olması gerekir.” şeklinde düzenlenmektedir.

Yapay zekalı uygulamanın ayıplı olmasından kaynaklı ortaya çıkan zararda uygulanacak hukuk üreticinin mutad meskeni veya işyeri hukuku veya ürünün satıldığı yerdir.

3.2.4. Arabuluculuk

Mahkemelerdeki artan iş yükü ve adaletin sağlanması için gereken masrafların azaltılması amacıyla günümüzde alternatif uyuşmazlık çözümlerine başvurulmaya başlanmıştır. Arabuluculuk, alternatif uyuşmazlık çözüm yollarından biridir.

⁴⁶¹ Güner, s.255.

⁴⁶² Tütüncübaşı, Uğur, **Akit Dışı Borç İlişkilerinde Hukuk Seçme Serbestisi**, Adalet Yayınları, Ankara 2018, s.155.

⁴⁶³ Güner, s.248

6325 sayılı Hukuk Uyuşmazlıklarında Arabuluculuk Kanunu m.2/1 (b) arabuluculuğu *“Sistematik teknikler uygulayarak, görüşmek ve müzakerelerde bulunmak amacıyla tarafları bir araya getiren, onların birbirlerini anlamalarını ve bu suretle çözümlerini kendilerinin üretmesini sağlamak için aralarında iletişim sürecinin kurulmasını gerçekleştiren, tarafların çözüm üretmediklerinin ortaya çıkması halinde çözüm önerisi de getirebilen, uzmanlık eğitimi almış olan tarafsız ve bağımsız bir üçüncü kişinin katılımıyla ve ihtiyari olarak yürütülen uyuşmazlık çözüm yöntemi”* olarak ifade etmektedir.

Arabuluculuk, bir uyuşmazlığı çözmek için tarafların kendi istekleri ile arada yargı gücüne sahip olmayan bir üçüncü kişi (arabulucu) sayesinde iletişim sağlanarak uyuşmazlık taraflarının uyuşmazlığı çözmek için kendilerinin üretimde olduğu bir uygulamadır⁴⁶⁴.

Mahkemelerin yükünün azaltılması amacıyla bazı uyuşmazlıklar için arabuluculuk yalnızca ihtiyari olmaktan çıkarılmış ve dava şartı haline getirilmiştir. Arabuluculuğun dava şartı olduğu uyuşmazlıklar kanun ile düzenlenmektedir. 7036 sayılı İş Mahkemeleri Kanunu m.3; Tüketicinin Korunması Hakkında Kanun m. 73/A/1; 6102 sayılı Türk Ticaret Kanunu m.5/1 hükümleri arabuluculuğun dava şartı olduğu halleri düzenlemektedir. Belirtilen hükümler; yapay zekanın veri ihlalleri dolayısıyla ortaya çıkan uyuşmazlıkları kapsamamaktadır. Bu uyuşmazlıklarda, arabuluculuk yoluna gidilmeksizin dava yoluna başvurulabilmektedir.

Arabuluculuğun dava şartı olmadığı hallerde, taraflar ihtiyari arabuluculuk yoluna başvurabilecektir. Tarafların hakkında serbestçe karar verebildikleri özel hukuku ilgilendiren konular, arabuluculuğa konu edilebilecekken kamu düzenine ilişkin ya da çekişmesiz yargı işlerinin arabuluculuğa uygun olmadığı belirtilmelidir⁴⁶⁵. Yapay zekanın veri işlemesi ile ortaya çıkan uyuşmazlıklarda, tarafların isteği üzerine arabuluculuk yoluna başvurulabilecektir.

⁴⁶⁴ Bárrios, Luísa, “European Mediation and Indigenous Mediation”, *Teisé*, C. 115, 2020, s.135., (erişim tarihi: 11.6.2023), <https://www.journals.vu.lt/teise/article/view/18463>

⁴⁶⁵ HUAK m.1/2; Kekeç, Elif Kısmet, **Arabuluculuk Yoluyla Uyuşmazlık Çözümünde Temel Aşamalar ve Taktikler**, Adalet Yayınevi, Ankara, 2011, s.92; Yılmaz, Demet, **Türk İş Uyuşmazlıklarında Dava Şartı Olarak Arabuluculuk**, Marmara Üniversitesi Sosyal Bilimler Enstitüsü Özel Hukuk Anabilim Dalı, Yayınlanmamış Yüksek Lisans Tezi, s.48.

SONUÇ

Teknoloji çağının ana unsurlarından biri olan yapay zeka her geçen gün insanı şaşırtacak başarılarla imza atmaktadır. Yapay zekanın kullanım alanları artmakta, yapay zeka günümüzün vazgeçilmez bir parçası haline gelmektedir. Bu alanların içerisinde sağlık bilimleri de yerini almaktadır. Yapay zeka ile artık hastaların hayatı kurtarılabilmektedir. Hastanın hayatını kurtarmak ile kast edilen, yapay zekanın tedaviye tek başına karar vermesi ya da tedavi sürecini tek başına gerçekleştirerek ameliyatlara tamamen otonom bir şekilde müdahil olması değil; genellikle teşhis evresinin yapay zeka ile gerçekleştirilmesidir. Günümüzde birçok hastalık yapay zeka sayesinde erken teşhis edilmekte ve erken müdahalede bulunularak hayati risk ortadan kaldırılmaktadır. Sağlık bilimlerinde yapay zeka ile kalıp ve anormallik tespitleri yapılmakta; tahmine dayalı analitik ve karar desteği sağlanmaktadır. Sağlık gibi hassas bir konunun yalnızca yapay zekanın ellerine bırakılmasının kabulü zor olduğu için yapay zekanın sağlık hizmetinin tarafı olmaktan çok aracısı olarak karşımıza çıkmaya devam edeceği düşünülmektedir.

Sağlık bilimlerinde yapay zekanın kullanılması sayesinde sağlık uzmanları arasında kolaylıkla bilgi paylaşılabilen, hizmet kalitesi artmakta, daha doğru teşhis konularak uygun tedavi imkanı sağlanmakta, kişiselleştirilmiş ilaç üretimine destek olunmakta, bulaşıcı hastalık dönemlerinde sağlık çalışanlarının zarara uğramadığı bir şekilde hasta tedavisi gerçekleştirilmekte, bulaşıcı hastalıkların tahmini ve yavaşlatılması sağlanabilmektedir.

Yapay zekanın faaliyette bulunabilmesi için öncelikle çevresini ve müdahil olacağı durumları analiz etmesi gerekmektedir. Bunun gerçekleşebilmesi için yapay zekanın veriye ihtiyacı vardır. Yapay zeka, kendisine sağlanan verileri işleyerek öğrenmektedir. Sağlık bilimlerinde yapay zeka kullanımında, yapay zekanın kişisel sağlık verileri ile eğitilmesi gerekmektedir.

Korumaya en çok ihtiyaç duyan veri türlerinden biri kişisel sağlık verileridir. Kişinin ruhsal ve fiziksel durumuna ilişkin her türlü verinin, yapay zeka tarafından işlenmesi sürecinde ve sonrasında koruması sağlanmalıdır. Sağlık verilerinin ifşa olması durumunda kişinin statüsünü etkileyerek toplumdan ve hatta aile hayatından dışlanmalar söz konusu olabileceğinden kişisel sağlık verileri, ulusal ve uluslararası hukuki düzenlemelerde genel verilere kıyasla daha sıkı bir koruma altına alınmaktadır. Teknolojik gelişmeler ışığında yeterliliği ve uygulanabilirliği gün geçtikçe daha problemli hale gelse de kişisel sağlık verilerini korumaya yönelik mevcut hukuki düzenleme hükümleri yapay zekanın sağlık bilimlerinde gerçekleştirdiği kişisel sağlık verilerinin işlendiği durumlarda da geçerli kabul edilmelidir.

Kişisel Verilerin Korunması Kanunu m.28 hükmünde bilimsel çalışmalar için kişisel verilerin kullanılması durumunda bu Kanun hükümlerinin uygulanmayacağı belirtilmektedir. Yapay zekanın eğitilmesi için kişisel sağlık verilerinin kullanılması bilimsel çalışma olarak değerlendirilebilecek olsa da ilgili hükümde verilerin anonimleştirilmesi şartı yer almaktadır. Günümüzde yapay zekanın büyük veriyi işleyerek anonimleştirmeyi etkisiz hale getirmesi, yapay zekanın kişisel sağlık verilerini işlemesini bilimsel amaç kabul edilmesi durumunda dahi Kanun'un kapsamında değerlendirme zorunluluğunu ortaya çıkarmaktadır

Kişisel sağlık verilerinin her koşulda işlenmesi mümkün değildir. Kişisel sağlık verilerinin işlenebilmesi için kural hastanın açık rızasının varlığıdır. Yapay zeka tarafından kişisel sağlık verilerinin işlenebilmesi için, veri sahibinin kişisel sağlık verilerinin yapay zeka tarafından ne amaçla işleneceğini bilmesi ve özgür bir şekilde olumlu irade beyanında bulunması gerekmektedir. Açık rızanın olmadığı durumlarda sağlık verilerinin işlenebilmesi için işleme konusunda açık bir hukuk kuralına dayanılması gerekmektedir. Hukukumuzda, yapay zeka ile ilgili herhangi özel bir düzenleme bulunmamaktadır. KVKK m.6/3 hükmünde kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi hallerinde açık rıza şartı aranmayacağı yönünde belirtilen istisnai işleme halleri yalnızca sır saklama yükümlülüğü altında bulunan kişiler ile yetkili kurum ve kuruluşlar için geçerlidir. Bu durumda yapay zeka tarafından kişisel sağlık verilerinin işlenmesi için açık rıza şarttır.

Kişisel sağlık verilerinin işlenmesi sırasında; sağlık verilerinin doğru ve gerektiğinde güncel olması, işlemenin hukuka ve dürüstlük kurallarına uygun olması, işleme amacının belirli, açık ve meşru olması, işlemenin belirlenen amaç ile bağlantılı, sınırlı ve ölçülü olması ve veri muhafazasının kanunda öngörülmüş ya da işlemenin gerektirdiği süre kadar olması gerekmektedir. Yapay zeka tarafından kişisel sağlık verilerini işleme faaliyetlerinde de bu ilkelere uyumlu hareket edilmesi beklenmektedir.

Sağlık bilimlerinde yapay zeka kullanımının birçok faydası olduğu gibi veri kullanılmasının sonucunda birçok sorun da ortaya çıkabilmektedir. Yapay zeka ile veri işlenmesi sırasında, yapay zekanın eğitimi için çok fazla veriye ihtiyaç duyulması, veriden yeni veri türetilmesi, açık rızanın alınabilmesinin kolay ve her zaman mümkün olmaması ve bu doğrultuda amaçla sınırlılık ilkesine aykırı faaliyetlerde bulunulması gibi sonuçlar oluşmakta, bu durum ise sağlık verilerinin işlenebilmesine ilişkin temel ilkelere aykırılık oluşturarak hukuka aykırı veri işlemesine neden olmaktadır.

Kişisel sağlık verileri yapay zeka tarafından hukuka uygun işlenmeye başlansa dahi sürecin devamında hukuka aykırılık oluşabilmektedir. Yapay zeka ile kişisel sağlık verilerini

hukuka uygun işleme gerçekleştirilse de algoritma sapması ve ayrımcılık kaynaklı zararlar ortaya çıkabilmektedir. Kişisel sağlık verilerinin işlenmesi sırasında oluşan bir algoritma sapması ve sağlıkta ayrımcılık, sağlık hakkına telafisi güç zararlar verebilecektir. Yapay zeka ile veri işlenmesi sırasında, yapay zeka tarafından çıkarımlarda bulunulmakta ve yeni veri üretimi gerçekleştirilmektedir. Üretilen verinin işlenmesi yönünden hukuka uygunluk sorunları oluşabilmektedir.

Yapay zekanın kişisel sağlık verilerini işlemesi sırasında çok faktörlü bir süreç oluşmasından dolayı meydana gelen bir zararın hangi eylemden kaynaklandığı ve sorumluluk süjesinin kim olacağını tespit etmek kolay olmamaktadır. Bu sebeple zararın doğmasından kaçınabilmek adına, yapay zekanın kişisel sağlık verilerini işlemesi sırasında ve sonrasında oluşabilecek sorunların çözülebilmesi için önleyici bir yaklaşım benimsenmesi gerekmektedir.

Yapay zeka aracılığı ile kişisel sağlık verilerinin işleneceği durumlarda, öncelikle Tasarımda Gizlilik, Varsayılanda Gizlilik uygulamalarına uygun tasarlanması, böylece kişisel sağlık verilerine ilişkin ortaya çıkabilecek ihlallerin baştan önlenmesi için çaba gösterilmesi gerekmektedir. Yapay zeka ile kişisel sağlık verileri işlenmeden önce Veri Koruma Etki Değerlendirmeleri ve Yapay Zeka Etki Değerlendirmeleri oluşturulmalı, ortaya çıkabilecek ihlaller baştan tespit edilmeli ve ihlalden kaçınmak için gereken tedbirler bu doğrultuda belirlenmelidir. Vijilans ile insanın sürece katılımı sayesinde algoritmaların takibi gerçekleştirilerek oluşabilecek bir algoritma sapmasının ve zararlarının önüne geçilmelidir.

Hayatın içinde bu kadar yer edinen yapay zekanın, faaliyetleri ile birtakım zararlara sebebiyet vermesi beklenmeyen bir durum değildir. Yapay zekanın veri işlemeye olan ihtiyacı, veri işleme sırasında sebep olabileceği zararları da beraberinde getirmektedir. Yapay zekanın kişisel sağlık verisi işlemesi sonucu oluşan zararlara karşı veri sahibi hem KVKK hem de diğer kanunlarca koruma altındadır. Sağlık verisi ihlal edilen ve yapay zeka tarafından verisinin işlenmesi sonucunda zarara uğrayan kişi, zararlarının tazminini veri sorumlusundan talep edebilecek, veri sorumlusunun tazmin talebine yanıt vermemesi ya da olumsuz yanıt vermesi durumunda Kurul'a şikayet yoluna başvurabilecektir. KVKK m.11 hükmünde düzenlenen zararın tazmini için veri sorumlusuna başvurma hakkı; TMK ve TBK'de yer alan genel hükümlere dayanarak kişinin, tazminat davası, koruyucu davalara ya da vekaletsiz iş görme davası yoluna başvurmasına engel olmayacaktır.

Yapay zeka tarafından kişisel sağlık verilerinin işlenmesi dolayısıyla meydana gelen zararların tazmininde sorumlunun kim olacağını tespit etme problemi ortaya çıkmaktadır. Kişisel sağlık verilerinin hukuka aykırı olarak işlendiği durumlarda sorumluluğun ileri sürülebileceği asıl kişi, veri sorumlusu olup; veri işleyen varlığı durumunda ise müteselsil

sorumluluk söz konusudur. Yapay zeka bazı durumlarda kişisel sağlık verilerini işleme amacını ve nasıl işleyeceğini kendi belirleyerek veri sorumlusu gibi hareket etmekte, bazı durumlarda ise sağlık verilerinin ne amaçla ve nasıl işleneceğini belirleyen hastane, doktor gibi veri sorumlusunun istekleri doğrultusunda kişisel sağlık verilerini işleyebilmektedir. Veri sorumlusu ya da veri işleyen kişiden bahsedebilmek için öncelikle ortada bir kişilik olması gerekmektedir. Yapay zekaya henüz hukuki nitelik tanınmadığı için yapay zekanın direkt sorumluluğunda bahsetmek mümkün değildir. Yapay zeka veri sorumlusu ya da veri işleyen sıfatına sahip olamamakta dolayısıyla sorumlu tutulamamakta fakat zarara sebep olabilmektedir. Toplumda düzenin ve bireyin güveninin sağlanabilmesi için oluşan zararların tazmini de şarttır. Mevcut hukuki düzenlemeler ışığında; yapay zekanın kişisel sağlık verilerini işleme sırasında eylemleri ile verdiği zarardan yapay zeka üreticisinin sorumlu tutulması gerekmektedir. Ürün sorumluluğu kapsamında, yapay zekanın veri ihlali ile zarara uğrayan kişilerin, kusursuz sorumluluk hükümlerine dayanarak üreticiye karşı maddi manevi tazminat talebinde bulunma hakkı bulunmaktadır. Bu durumda, mevcut hukuki düzenlemelere göre davalı kişi üretici olacaktır.

Yapay zeka kişisel sağlık verilerinin işlenmesi sırasında tek bir ülkede faaliyet göstermemektedir. Dolayısıyla ortaya çıkan uyuşmazlıkların çözümünde uygulanacak hukuk problemi oluşmaktadır. Yapay zeka tarafından gerçekleşen veri ihlalleri için uygulanacak hukuk MÖHUK m.35 uyarınca veri sahibinin seçimine bırakılmaktadır. Veri sahibinin mutad meskeni hukuku, yapay zeka üreticisinin işyeri ya da mutad mesken hukuku ya da veri ihlalinin meydana geldiği ülke hukuku uyuşmazlığa uygulanabilecektir. Veri ihlali dışında oluşan zararlar için veri sahibi MÖHUK m.36 hükmü uyarınca üreticinin mutad meskeni ya da işyeri hukuku ya da ürünün satıldığı yer hukuku arasından seçim yapacaktır.

Yapay zeka ve kişisel verileri koruma alanının hukuk bilgisinin yanında teknik bilgi de gerektiren alanlar olması ve henüz hukuki düzenleme mevcut olmadığı için oluşabilecek kaygıları ortadan kaldırmak adına bu konuda ortaya çıkan bir uyuşmazlık söz konusu olduğunda; tarafların ihtiyari olarak arabuluculuk yoluna başvurabilmesi, yapay zeka ve kişisel verilerin korunması alanında uzmanlaşmış bir arabulucu ile uyuşmazlığı mahkeme yoluna başvurmadan çözmesi tarafımızca önerilebilecektir.

Yapay zeka hakkında hukuki düzenlemelerin yapılması ihtiyacı gün geçtikçe artmaktadır. Mevcut hukuki düzenlemelerin kişisel verilerin korunması açısından yetersiz kalmaya başlaması sebebiyle revizeye ihtiyaç duyulmaktadır. Özellikle sağlık gibi hassas veri içeren alanlarda yapay zeka kullanımına dair veri koruma hukukunun öncüsü Genel Veri Koruma Tüzüğü ile yapay zeka hukukunun öncüsü Yapay Zeka Tüzüğü'ne uyumlu özel hukuki

düzenlemeler ile oluşabilecek uyuşmazlıkların en hızlı şekilde ortadan kaldırılması gerekmektedir.



KAYNAKÇA

I. KİTAP VE MAKALELER

- Akalın, Betül/Veranyurt, Ülkü: “Sağlık Hizmetleri ve Yönetiminde Yapay Zeka”, **Acta Infologica**, C.5, S.1, 2021, ss.231-240, (erişim tarihi:15.3.2023), <https://dergipark.org.tr/tr/pub/acin/issue/63212/850857>
- Akdağ, Şükrü Yakup: “Yapay Zekanın Sorumluluğu Üzerine Düşünceler”, Ed. Başak Baysal, **Sorumluluk Hukuku Seminerler 2018**, İstanbul, 2019, ss. 1-22.
- Akıncı, Ayşe Nur: **Avrupa Birliği Genel Veri Koruma Tüzüğü’nün Getirdiği Yenilikler ve Türk Hukuku Bakımından Değerlendirilmesi**, İktisadi Sektörler ve Koordinasyon Genel Müdürlüğü Bilgi Toplumu Dairesi Başkanlığı, 2017, (erişim tarihi: 20.4.2023), http://www.bilgitoplumu.gov.tr/wp-content/uploads/2017/07/AB_Veri_Koruma_Tuzugu.pdf
- Akipek, Jale/Akıntürk, Turgut/Ateş, Derya: **Türk Medeni Hukuku Başlangıç Hükümleri Kişiler Hukuku**, 18.Bs., Beta Yayınları, İstanbul, 2022.
- Akkurt, Sinan Sami: “Yapay Zekanın Otonom Davranışlarından Kaynaklanan Hukuki Sorumluluk”, **Uyuşmazlık Mahkemesi Dergisi**, C.7, S.13, 2019, ss.39-59, <https://doi.org/10.18771/mdergi.581875>
- Aksoy, Hüseyin Can: **Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması**, Çakmak Yayınevi, Ankara, 2010.
- Andrew, Jane/Baker, Max: “The General Data Protection Regulation in the Age of Surveillance Capitalism”, **Journal of Business Ethics**, S.168, 2021, ss. 565-578, <https://doi.org/10.1007/s10551-019-04239-z>
- Anı, Nevzat Ali: **Kişisel Verilerin İşlenmesi ve Açık Rıza**, T.C. İstanbul Üniversitesi, Sosyal Bilimler Enstitüsü, Özel Hukuk Anabilim Dalı, Yayımlanmamış Yüksek Lisans Tezi, İstanbul, 2018.
- Aydın, Akgül: Kişisel Verilerin Korunmasında Yeni Bir Hak: “Unutulma Hakkı” ve AB Adalet Divanı’nın “Google Kararı”, **Türkiye Barolar Birliği Dergisi**, S.116, 2016, ss.. 11-38, (erişim tarihi: 15.6.2023), <http://tbbdergisi.barobirlik.org.tr/m2015-116-1440>
- Ayözger, Çiğdem: **Kişisel Verilerin Korunması(Elektronik Haberleşme Sektörüne İlişkin Özel Düzenlemeler Dahil)**, Beta Yayınları, İstanbul, 2016.
- Bak, Başak: “Medeni Hukuk Açısından Yapay Zekanın Hukuki Statüsü ve Yapay Zeka Kullanımından Doğan Hukuki Sorumluluk”, **Türkiye Adalet Akademisi Dergisi**, S.35, 2018, ss.211-232.

- Barfield, Woodrow: "Liability for Autonomous and Artificially Intelligent Robots", **Paladyn, Journal of Behavioral Robotics**, C. 9, S.1, 2018, ss. 193-203, <https://doi.org/10.1515/pjbr-2018-0018>
- Bárrios, Luísa: "European Mediation and Indigenous Mediation", **Teisè**, C. 115, 2020, ss.134-146, (erişim tarihi: 15.6.2023), <https://www.journals.vu.lt/teise/article/view/18463>
- Bayram, Öykü Beste: "Bir Uyum Aracı Olarak Veri Koruma Etki Analizinin Türk Hukuku Bakımından Değerlendirilmesi", **Kişisel Verileri Koruma Dergisi**, C.4, S.1, 2022, ss. 38-53.
- Birleşmiş Milletler İnsan Hakları Komitesi: **Birleşmiş Milletler'de İnsan Hakları Yorumları İnsan Hakları Komitesi ve Ekonomik, Sosyal ve Kültürel Haklar Komitesi 1981-2006**, Der. ve Çev. Lema Uyar, İnsan Hakları Hukuku Çalışmaları, İstanbul Bilgi Üniversitesi Yayınları, İstanbul, 2006, (erişim tarihi: 15.6.2023), https://insanhaklarimerkezi.bilgi.edu.tr/media/uploads/2016/05/05/BMde_Insan_Haklari_Yorumlari_1981_2006.pdf
- Bostrom, Nick: **Superintelligence: Paths, Dangers, Strategies**, Oxford University Press, Oxford, 2014.
- Bozkurt Yüksel, Armağan Ebru: "Yapay Zekanın Buluşlarının Patentlenmesi", **Uyuşmazlık Mahkemesi Dergisi**, Y. 6, S.11,2018, ss. 585-622, (erişim tarihi: 15.6.2023), <https://www.uyusmazlik.gov.tr/Resimler/Pdfler/Makaleler/20-06-2018yuksel.pdf>
- Bozkurt Yüksel, Armağan Ebru/ Bak, Başak: "Yapay Zeka", **Futurist Hukuk**, Aristo Yayınları, İstanbul, 2018, ss. 5-37.
- Brown, Tristan G./Statman, Alexander/Sui, Celine: "Public Debate on Facial Recognition Technologies in China", **MIT Case Studies in Social and Ethical Responsibilities of Computing**, 2021, (erişim tarihi: 15.3.2023), <https://dspace.mit.edu/handle/1721.1/144299>
- Büyüközkan Feyzioğlu, Gülçin: "Dijitalleşen Dünyada Yapay Zeka, **Gelişen Teknolojiler ve Hukuk II: Yapay Zeka**, Ed. Doç. Dr. Eylem Aksoy Retornaz & Dr. Öğr. Üyesi Osman Gazi Güçlütürk, On İki Levha Yayıncılık, İstanbul, 2021, ss. 1-20.
- Calo, Ryan/Evtimov, Ivan/Fernandes, Earlane/Kohno, Tadayoshi/ O'Hair, David: "Is Tricking a Robot Hacking?" **University of Washington Tech Policy Lab**, Seattle, 2018, (erişim tarihi: 21.1.2023), <https://digitalcommons.law.uw.edu/techlab/5>
- Carboni, Andrea/Russo,Dario/Moroni, Davide/Barsocchi, Paolo: "Privacy by design in systems for assisted living, personalised care and wellbeing: A stakeholder analysis", **Frontiers**

- in **Digital Health**, C.4, 2023, (erişim tarihi: 15.6.2023), <https://www.frontiersin.org/articles/10.3389/fdgth.2022.934609/full>,
- Castelvecchi, Davide: “Deep Learning Boosts Google Translate Tool”, **Nature**, 2016, (erişim tarihi: 10.3.2023), <https://doi.org/10.1038/nature.2016.20696>
- Childs, W. Alfred: “The Functions of Medical Care”, **Public Health Reports**, C.90, S.1, 1975, ss. 10-14, <https://www.jstor.org/stable/4595138>
- Clarke, E.A.: “What is Preventive Medicine?”, **Official Publication of the College of Family Physicians of Canada**, C.20, S.11, 1974, s.65-68.
- Çavuşoğlu, Gökçe Filiz: **Kişisel Verilerin Yapay Zekayla İşlenmesinden Doğan Özel Hukuk Sorunları**, Yetkin Yayınları, Ankara, 2021.
- Çekin, Mesut Serdar: “6698 sayılı Kişisel Verilerin Korunması Hakkında Kanun’un Big Data (Büyük Veri) ve İrade Serbestisi Açısından Değerlendirilmesi”, **İÜHFM**, C.74, S.2, 2016, ss. 629-650.
- Demir, Ozan: “Sürdürülebilir Kalkınma İçim Yapay Zeka”, **Yapay Zeka ve Gelecek**, Ed. Gonca Teli, Doğu Kitabevi, İstanbul ,2019 ss.44-65.
- Develioğlu, Hüseyin Murat: 6698 sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü Uyarınca Kişisel Verilerin Korunması Hukuku, On İki Levha Yayıncılık, İstanbul, 2017.
- Doğan, Vahit: **Milletlerarası Özel Hukuk**, 8. Bs., Savaş Yayınevi, Ankara, 2022.
- Dülger, Murat Volkan: **Kişisel Verilerin Korunması Hukuku**, Hukuk Akademisi Yayıncılık, 3. Bs., İstanbul, 2020, (**Dülger**, Kişisel Verilerin Korunması)
- Dülger, Murat Volkan: “Bir Hukuk Kurgu Denemesi: Yapay Zekalı Varlığın Hukuki Sorumluluğu (Olabilir Mi?)”, **Hukuk ve Daha Fazlası Dergisi**, 2017, ss.4-10. (**Dülger**, Hukuki Sorumluluk)
- Dülger, Murat Volkan: “Kişisel Sağlık Verileri Yönetmeliğinin Yürütmesinin Durdurulmasına İlişkin Danıştay’ın 9.10.2018 Tarihli Kararına İlişkin Değerlendirme”, 2021, (erişim tarihi: 12.4.2023) <https://ssrn.com/abstract=3792286> (**Dülger**, Yönetmelik)
- Ellahham, Samer/Ellahham, Nour: “Use of Artificial Intelligence for Improving Patient Flow and Health Delivery”, **Journal of Computer Science & Systems Biology**, C.12, S.3, 2019, ss.1-6, (erişim tarihi: 16.3.2023), https://www.researchgate.net/publication/336742991_Use_of_Artificial_Intelligence_for_Improving_Patient_Flow_and_Healthcare_Delivery

- Embi, Peter J.: “Algorithmovigilance—Advancing Methods to Analyze and Monitor Artificial Intelligence–Driven Health Care for Effectiveness and Equity”. **JAMA Network Open**, C.4, S.4, 2021.
- Erarslan Türkmen, Sevgi: **Özel Nitelikli Kişisel Verilerin İşlenmesinde Açık Rızanın Aranmadığı Haller**, On İki Levha Yayıncılık, İstanbul, 2019.
- Eren, Fikret: **Borçlar Hukuku Genel Hükümler**, 27. Bs., Yetkin Yayınları, Ankara, 2022.
- Ersoy, Çağlar: **Robotlar, Yapay Zeka ve Hukuk**, 3. Bs., On İki Levha Yayıncılık, İstanbul, 2018.
- Esteva, Andre/Kuprel, Brett/Novoa, Roberto A./Ko, Justin/ Swetter, Susan M./Blau, Helen M./Thrun, Sebastian: “Dermatologist-level classification of skin cancer with deep neural networks”, **Nature**, S.542, 25.01.2017, ss. 115–118.
- Fateh-Moghadam, Bijan: “Innovationsverantwortung im Strafrecht: Zwischen strict Liability, Fahrlässigkeit und erlaubtem Risiko – Zugleich ein Beitrag zur Digitalisierung des Strafrechts”, **Zeitschrift für die gesamte Strafrechtswissenschaft**, C.131, S.4, 2019, ss. 863-887, (erişim tarihi: 20.3.2023) <https://doi.org/10.1515/zstw-2019-0031>
- Ford, Martin: **Robotların Yükselişi Yapay Zeka ve İşsiz Bir Gelecek Tehlikesi**, Çev.: Cem Duran, 11. Bs., Kronik Kitap, İstanbul, 2022.
- Good, Otavio (Google Research Team): “How Google Translate Squeezes Deep Learning onto a Phone”, **Google AI Blog**, 30.07.2015, (erişim tarihi: 13.3.2023), <https://ai.googleblog.com/2015/07/how-google-translate-squeezes-deep.html>
- Güçlütürk Osman Gazi/Kadıoğlu, Yasin Murat: “Yapay Zeka ve Regülasyon”, **Gelişen Teknolojiler ve Hukuk II: Yapay Zeka**, Ed. Doç. Dr. Eylem Aksoy Retornaz & Dr. Öğr. Üyesi Osman Gazi Güçlütürk, On İki Levha Yayıncılık, İstanbul, 2021, ss.75-118.
- Güçlütürk, Osman Gazi: **Yapay Zeka ve Verinin Kullanımı**, On İki Levha Yayıncılık, İstanbul, 2022.
- Güner, Cemil: “Yapay Zekanın Verdiği Zarardan Doğan Sözleşme Dışı Sorumluluğa Uygulanacak Hukuk”, **Uyuşmazlık Mahkemesi Dergisi**, C.8, S.15, 2020, ss.229-272.
- Gürbüz Erel, İrem: **Sağlık Hukukunda Kişisel Verilerin Korunması** T.C. Kocaeli Üniversitesi Sosyal Bilimler Enstitüsü, Özel Hukuk Anabilim Dalı, Yayımlanmamış Yüksek Lisans Tezi, Kocaeli, 2021.
- Haagen, Christian: **Verantwortung für Künstliche Intelligenz: ethische Aspekte und zivilrechtliche Anforderungen bei der Herstellung von KI-Systemen**, 1. Bs., Nomos, Baden-Baden, 2021.
- Hakeri, Hakan: **Tıp Hukuku**, 20. Bs., Seçkin Yayıncılık, Ankara, 2020.

- Henke, Nicolaus/Bughin, Jacques/Chui, Michael/Manyika, James/ Saleh, Tamim/Wiseman, Bill/Sethupathy, Guru: **The Age of Analytics: Competing in a Data-driven World**, McKinsey & Company, 2016, (erişim tarihi: 3.2.2023) <https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-age-of-analytics-competing-in-a-data-driven-world>
- Hoşgör, Haydar: **Sağlıkta Yapay Zeka ve Robotik**, Dora Yayıncılık, 2022.
- İmançlı, Canan: **Kişisel Sağlık Verilerinin Korun(a)mamasından Doğan Özel Hukuk Sorumluluğu**, On iki levha Yayıncılık, İstanbul, 2020.
- Kamara, Irene: “Article 40. Codes of Conduct”, **The EU General Data Protection Regulation (GDPR) – A Commentary**, Ed. Christopher DOCKSEY, Cristopher Kuner, Lee A. Bygrave, Laura Drechsler, Oxford University Press, Oxford, 2020.
- Kangal, Zeynel T.: **Yapay Zeka ve Ceza Hukuku**, On İki Levha Yayıncılık, İstanbul, 2021.
- Kanışlı, Erhan: “Ürün Güvenliği ve Teknik Düzenlemeler Kanunu (ÜGTDK) Uyarınca Üreticinin Sorumluluğu”, **İstanbul Hukuk Mecmuası**, C.78, S.3, 2020, ss. 1413-1468.
- Kapancı, Berk: “Özel Hukuk Perspektifinden Bir Değerlendirme: Yapay Zeka ve Haksız Fiil Sorumluluğu”, **Gelişen Teknolojiler ve Hukuk II: Yapay Zeka**, Ed. Doç. Dr. Eylem Aksoy Retornaz & Dr. Öğr. Üyesi Osman Gazi Güçlütürk, On İki Levha Yayıncılık, İstanbul, 2021 ss.128-140.
- Kara Kılıçarslan, Seda: “Yapay Zekanın Hukuki Statüsü ve Hukuki Kişiliği Üzerine Tartışmalar”, **Yıldırım Beyazıt Hukuk Dergisi**, C.4, S.2, 2019, ss.363-389.
- Karagöz, Jülide Güzin: **Sağlıkta Dijital Dönüşüm, Yapay Zeka (AI) ve Nesnelerin İnterneti (IoT)**, Kutlu Yayınevi, İstanbul, 2018.
- Kartal, Serhat: **Türk Hukukunda İş Sözleşmesinin Sağlık Sebepleriyle Sona Ermesi**, On İki Levha Yayınları, İstanbul, 2020.
- Kasap Atilla: “Güncel Gelişmeler Işığında Türk Hukukunda Yapay Zeka Varlıkları ve Hukuki Kişilik”, **Türk-Alman Üniversitesi Hukuk Fakültesi Dergisi**, C.4, S.2, 2022, ss. 485-555.
- Kayaalp, Kıyas/Süzen, Ahmet Ali: **Derin Öğrenme ve Türkiye’deki Uygulamaları**, Ankara, İKSAD Yayınevi, 2018, ss.6-21.
- Kekeç, Elif Kısmet: **Arabuluculuk Yoluyla Uyuşmazlık Çözümünde Temel Aşamalar ve Taktikler**, Adalet Yayınevi, Ankara, 2011.
- Kılıçoğlu, Ahmet M. : **Borçlar Hukuku Genel Hükümler**, 26. Bs., Turhan Kitabevi, Ankara, 2022.

- Kılınç, Doğan: “Anayasal Bir Hak Olarak Kişisel Verilerin Korunması”, **AÜHFD**, C. 61, S.3, 2012, ss.1089-1172.
- Kluge, Eike-Henner W.: “Artificial Intelligence in Healthcare: Ethical Considerations”, **Healthcare Management Forum**, C. 33, S.1, 2020, ss.47-49
<https://journals.sagepub.com/doi/pdf/10.1177/0840470419850438> (E.T: 18.3.2023)
- Konam, Sandeep: “Where Did IBM go wrong with Watson Health?”, **Quartz**, (Erişim tarihi: 20.03.2023)
<https://qz.com/2129025/where-did-ibm-go-wrong-with-watson-health>
- Korkmaz, İbrahim: “Kişisel Verilerin Korunması Kanunu Hakkında Bir Değerlendirme”, **Türkiye Barolar Birliği Dergisi**, S. 124, 2016, ss.81-152.
- Kuśmierczyk, Małgorzata: “Algorithmic Bias in the Light of the GDPR and the Proposed AI Act”, Ed. Maciej Olejnik, Wiktoria Morawska, **(In)equality. Faces of modern Europe**, Wydawnictwo Centrum Studiów Niemieckich i Europejskich im. Willy’ego Brandta, Wrocław, <http://dx.doi.org/10.2139/ssrn.4117936>
- Küzeci, Elif: **Kişisel Verilerin Korunması**, 4.Bs., On İki Levha Yayıncılık, İstanbul, 2020.
- Lalitha, R.: “AI vs. Machine Learning vs. Deep Learning”, **Artificial Intelligence (AI) Recent Trends and Applications**, Ed. S. Kanimozhi Suguna/ M. Dhivya/ Sara, Paiva, CRC Press, Boca Raton, 2021, ss.83-82.
- Larson, Jeff/ Mattu, Surya/ Kirchner, Lauren/ Angwin, Julia: “How We Analyzed the COMPAS Recidivism Algorithm”, **ProPublica (blog)**, 2016, (erişim tarihi: 20.1.2023)
<https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm>
- Lenzen, Manuela: **Künstliche Intelligenz: Was sie kann&was uns erwartet**, Verlag C.H. Beck, Münih, 2018.
- Longoni, Chiara/ Bonezzi, Andrea/ Morewedge, Carey K: “Resistance to Medical Artificial Intelligence”, **Journal of Consumer Research**, C. 46, S. 4, 2019, ss. 629-650, (erişim tarihi: 20.3.2023), <https://doi.org/10.1093/jcr/ucz013>
- Matthews, Kayla: “5 Industries that Robotics Have Disrupted Drastically”, **Robotics Business Review**, 27.09.2019, (erişim tarihi: 13.3.2023),
<https://www.roboticsbusinessreview.com>
- Mendos Kuşkonmaz, Elif: **Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması**, İstanbul Üniversitesi, Sosyal Bilimler Enstitüsü, Kamu Hukuku Anabilim Dalı, Yayımlanmamış Yüksek Lisans Tezi, İstanbul, 2013.

- Miller, Adam: “The Future of Healthcare Could Be More Elementary With Watson”, **CMAJ**, C.185, S.9, 2013, ss. 367-368, (erişim tarihi: 20.3.2023), <https://doi.org/10.1503/cmaj.109-4442>
- Mitrou, Lilian: “Data Protection, Artificial Intelligence and Cognitive Services: Is The General Data Protection Regulation (GDPR) ‘Artificial Intelligence-Proof’?”, 2018 <http://dx.doi.org/10.2139/ssrn.3386914> (erişim tarihi:20.4.2023)
- Murphy, Robin R./ Woods, David D.: “Beyond Asimov: Three Laws of Responsible Robotics”, **IEEE Intelligent Systems**, C. 24, S.4, 2009, ss. 14-20. (erişim tarihi: 25.6.2023) <https://ieeexplore.ieee.org/document/5172885>
- Mustafa/ Öğüz, Tufan: **Türk Özel Hukuku, Kişiler Hukuku**, C.2, Filiz Kitabevi, İstanbul, 2020.
- Nomer, Ergin: **Devletler Hususi Hukuku**, 23. Bs., Beta Yayınları, İstanbul, 2021
- Oğuzman, Kemal/Öz, Turgut: **Borçlar Hukuku**, 17. Bs., Filiz Kitabevi, C.2., İstanbul, 2022, (Oğuzman/Öz, C.2).
- Oğuzman, Kemal/Seliçi, Özer/Oktay Özdemir, Saibe: **Kişiler Hukuku**, 21. Bs., İstanbul, 2022.
- Oğuzman, Kemal/Öz, Turgut: **Borçlar Hukuku Genel Hükümler**, 20. Bs., Filiz Kitabevi, C. 1, İstanbul, 2022, (Oğuzman/Öz, C.1).
- Orak, Beşir: **Kişisel Sağlık Verilerinin Korunması**, Yetkin Kitabevi, Ankara, 2020.
- Öğretmen Kotil, Zeynep: **Kişisel Verilerin Korunması Çerçevesinde Yapay Zeka**, On İki Levha Yayıncılık, İstanbul, 2022.
- Özçelik, Şemsi Barış: “Yapay Zekanın Veri Koruma, Sorumluluk ve Fikri Mülkiyet Açısından Ortaya Çıkardığı Hukuki Gereksinimler”, **Adalet Dergisi**, S.66, 2021, ss.66-87.
- Özdemir, Hayrunnisa: **Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması**, Seçkin Yayınları, Ankara, 2009, (Özdemir, Kişisel Veri).
- Özdemir, Hayrunnisa: “Hekimin Hukuki Sorumluluğu”, **Erciyes Üniversitesi Hukuk Fakültesi Dergisi**, C.11, S.1, 2016, ss.33-81 (Özdemir, Hekimin Hukuki Sorumluluğu).
- Öztan, Bilge: **Medeni Hukukun Temel Kavramları**, Turhan Kitabevi, Ankara, 2014.
- Palmer, Whitney J.: “AI Algorithm Reaches Equivalent Accuracy of Average Radiologist”, **Diagnostic Imaging**, 27.08.2020, (erişim tarihi: 18.3.2023), <https://www.diagnosticimaging.com/view/ai-algorithm-reaches-equivalent-accuracy-of-average-radiologist>

- Pepito, Joseph Andrew/Vasquez, Brian A./Locsin, Rozzano C.: "Artificial Intelligence and Autonomous Machines: Influences, Consequences, and Dilemmas in Human Care." **Health**, C.11, S.7, 2019, ss: 932-949. <https://doi.org/10.4236/health.2019.117075>
- Pérennou, Thomas: "State of the Art On Legal Issues", 2014, s.10, (erişim tarihi: 4.6.2023), <https://ethicaa.greyc.fr/media/files/ethicaa.delivrable.1.pdf>.
- Polat, Cemre: "Türk ve Avrupa Birliği Hukukunda Ürün Sorumluluğu", **Ankara Üniversitesi Hukuk Fakültesi Dergisi**, C. 70, S.4, 2022, ss.973-1041 <https://doi.org/10.33629/auhfd.988504>
- Pourhomayoun, Mohammad/Shakibi, Mahdi: "Predicting mortality risk in patients with COVID-19 using machine learning to help medical decision-making", **Smart Health**, C.20, 200278, 2021.
- Rasso, Filippo A./Hilligos, Hannah/Krishnamurthy, Vivek/Bavitz, Christopher/Kim, Levin: "Artificial Intelligence & Human Rights: Opportunities & Risks, Berkman Klein Center Research Publication, S.6, 2018, s.18, <http://dx.doi.org/10.2139/ssrn.3259344>
- Reddy, Sandeep/ Fox, John/ Ourohit, Maulik P.: "Artificial Intelligence-enabled Healthcare Delivery", **Journal of the Royal Society of Medicine**, C.112, S.1, ss.22-28, (erişim tarihi: 18.3.2023) <https://journals.sagepub.com/doi/pdf/10.1177/0141076818815510>
- Russell, Stuart J. Russell/Norvig, Peter: **Artificial Intelligence A Modern Approach**, Prentice-Hall, Englewood Cliffs, New Jersey, 1995.
- Sarı, Onur: "Yapay Zekanın Sebep Olduğu Zararlardan Doğan Sorumluluk", **Türkiye Barolar Birliği Dergisi**, S.147, İstanbul, 2020, ss.251-312.
- Say, Cem: **50 Soruda Yapay Zeka**, 23. Bs., 7 Renk Basım Yayım ve Filmcilik, İstanbul, 2022.
- Schönberger, Daniel: "Artificial intelligence in healthcare: a critical analysis of the legal and ethical implications", **International Journal of Law and Information Technology**, C.27, S.2, 2019, ss.171-203, (erişim tarihi: 18.3.2023), <https://doi.org/10.1093/ijlit/eaz004>
- Selek, Ozan: "Genel Veri Koruma Tüzüğü Işığında Kişisel Verilerin İşlenmesinde Rıza Açıklaması", **DEÜ Hukuk Fakültesi Dergisi**, C.21, S.2, ss.911-951.
- Sert Sütçü, Selin: "Endüstri 4.0'da Yapay Zekanın Hukuki Sorumluluğu" **Farklı Perspektiflerden Endüstri 4.0 Yazıları I**, Ed. Ayşen Altun Ada & Fulya Mısırdalı Yangil, Gazi Kitabevi, Ankara, 2020, ss.53-86.
- Sodhi, Pinky/ Awasthi, Naman/ Sharma, Vishal: "Introduction to Machine Learning and Its Basic Application in Python", (January 6, 2019). Proceedings of 10th International

- Conference on Digital Strategies for Organizational Success, ss.1354-1375, (erişim tarihi: 19.1.2023), <http://dx.doi.org/10.2139/ssrn.3323796>
- Spanu, Anca: “Amazon’s new Alexa will know someone is sick by listening to their voice” **Healthcareweekly**, 10.10.2018, (erişim tarihi: 2.5.2023), <https://healthcareweekly.com/amazon-alexa/>
- Stahl, Bernd Carsten/ Schröder Doris/ Rodrigues, Rowena: “Privacy”, **Ethics of Artificial Intelligence Case Studies and Options for Addressing Ethical Challenges**, Springer, 2022, ss.25-37. https://doi.org/10.1007/978-3-031-17040-9_9
- Stahl, Bernd Carsten/ Schröder Doris/ Rodrigues, Rowena: “Unfair and Illegal Discrimination”, **Ethics of Artificial Intelligence Case Studies and Options for Addressing Ethical Challenges**, Springer, 2022, ss.9-23, https://doi.org/10.1007/978-3-031-17040-9_9
- Taştan, Furkan Güven: **Türk Sözleşme Hukukunda Kişisel Verilerin Korunması**, 2. Bs., On İki Levha Yayıncılık, İstanbul, 2017.
- Theodoros, Chiou: “Copyright lessons on Machine Learning: what impact on algorithmic art?”, **Journal of Intellectual Property, Information Technology and Electronic Commerce Law (JIPITEC)**, C.10, S.3, 2019, ss. 398-411.
- Tunç, Aybike: “Güncel Teknoloji ve Kişisel Veri”, **Kişisel Verilerin Korunmasına Akademik Bakış- KVKK Akademi Derleme Çalışması**, Ed. Pınar Çağlayan Aksoy/ Hüseyin Can Aksoy, Ütopya Grafik, Ankara, 2023, ss. 297-319.
- Turgut, Cemile: **Kişilik Hakkının Bir Görünümü Olarak Unutulma Hakkı**, On İki Levha Yayıncılık, 2021.
- Tovino, A. Stacey: “The HIPAA Privacy Rule and the EU GDPR: Illustrative Comparisons”, **Scholarly Wokds**, 2017, ss.972-993, <https://scholars.law.unlv.edu/facpub/1066> (erişim tarihi: 04.09.2023)
- Várkonyi, Gizem Gültekin/ Gradišek, Anton: “Data Protection Impact Assessment Case Study for a Research Project Using Artificial Intelligence on Patient Data”, **Informatica**, C.44, S.4, ss. 497-505. <https://www.informatica.si/index.php/informatica/article/view/3253>
- Wang, Chao/Jieyu, Zhang/Lassi, Nicholas/Zhang, Xiaohan: "Privacy Protection in Using Artificial Intelligence for Healthcare: Chinese Regulation in Comparative Perspective" **Healthcare**, C.10, S. 10, 2022. <https://doi.org/10.3390/healthcare10101878>
- Yavuz Tiftikçigil, Burcu/Yavaş, Hilal Kuvvetli: “Yeniliğin Dönüştürücü Gücü ve Endüstri Devrimleri: Türkiye’nin Endüstri 4.0’daki Konumu Üzerine Bir Değerlendirme”,

- Farklı Perspektiflerden Endüstri 4.0 Yazıları I**, Ed. Ayşen Altun Ada & Fulya Mısırdalı Yangıl, Gazi Kitabevi, Ankara, 2020, ss. 1-52.
- Yenerer Çakmut, Özlem: **Tıbbi Müdahaleye Rızanın Ceza Hukuku Açısından İncelenmesi**, Legal Yayınları, İstanbul, 2003.
- Yılıyaer, Abudureyimu: **Karşılaştırmalı Örnekler Üzerinden Yapay Zekâ ve Kişisel Verilerin Korunması**, İstanbul Ticaret Üniversitesi Dış Ticaret Enstitüsü, Uluslararası Ticaret ve AB Hukuku Anabilim Dalı, Yayınlanmamış Doktora Tezi, İstanbul, 2021.
- Yılmaz, Battal: **Açıklamalı-İçtihatlı Hekimin Hukuki Sorumluluğu**, 4. Bs., Adalet Yayınevi, Ankara, 2020.
- Yılmaz, Demet: **Türk İş Uyuşmazlıklarında Dava Şartı Olarak Arabuluculuk**: Marmara Üniversitesi Sosyal Bilimler Enstitüsü Özel Hukuk Anabilim Dalı, Yayınlanmamış Yüksek Lisans Tezi, İstanbul, 2020.
- Yılmaz, Sabire Sanem: **Tıp Alanında Kişisel Verilerin Korunması**, 4.Bs., Seçkin Yayıncılık, Ankara, 2020.
- Yılmaz, Süleyman/Çavuşoğlu, Gökçe Filiz: **Kişisel Verileri Koruma Hukuku**, Yetkin, Ankara, 2020.
- Zafer, Hamide: “Sağlık Mesleği Mensuplarının Suçu Bildirmemesi Suçu (TCK m.280), **İÜHFM**, C. 71, S.1, 2013, ss.1327-1352
- Zor, Abdülhamid: **Veri Sorumlusunun Yükümlülükleri ve Bu Yükümlülükleri İhlalinden Doğan Özel Hukuk Sorumluluğu**, On İki Levha Yayıncılık, İstanbul, 2020
- Zorluel, Mustafa: “Yapay Zeka ve Telif Hakkı” **Türkiye Barolar Birliği Dergisi**, C. 2019, S.142, ss.305-356.

II. BELGE, ARAŞTIRMA VE RAPORLAR

A Definition of AI: Main Capabilities and Disciplines, High-Level Expert Group on Artificial Intelligence, Brüksel, 18.12.2018, (erişim tarihi: 20.1.2023).

Artificial Intelligence Act Briefing, European Parliamentary Research Service, European Parliament, Haziran 2023, (erişim tarihi: 4.9.2023), [https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI\(2021\)698792_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf)

Artificial Intelligence for Europe, European Commission, COM(2018) 237 Final, Brüksel, 25.4.2018, (erişim tarihi: 20.1.2023) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A237%3AFIN>

Council of Europe, Parliamentary Assembly, **Artificial Intelligence in health care: medical, legal and ethical challenges ahead**, Doc.15154, 22.10.2020, (erişim tarihi: 3.5.2023), <http://www.assembly.coe.int/LifeRay/SOC/Pdf/TextesProvisoires/2020/20200922-HealthCareAI-EN.pdf>

1. **Çalıştay Raporu**, Türkiye Yapay Zeka İnisiyatifi(TRAI), 9.5.2017, (erişim tarihi: 15.3.2023), <https://turkiye.ai/wp-content/uploads/2021/12/TRAI-Calistay-Raporu-2017.pdf>

Ethics Guidelines for Trustworthy AI, High Level Expert Group on Artificial Intelligence, 8.4.2019,, (erişim tarihi: 2.5.2023), https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60419

European Parliament, Directorate-General for Internal Policies of the Union, Nevejans, Nathalie, **European Civil Law Rules in Robotics (Study)**, Publications Office of the European Union, (erişim tarihi: 10.6.2023) <https://op.europa.eu/en/publication-detail/-/publication/19ea0f1c-9ab0-11e6-868c-01aa75ed71a1/language-en>
[https://www.europarl.europa.eu/RegData/etudes/STUD/2016/571379/IPOL_STU\(2016\)571379_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2016/571379/IPOL_STU(2016)571379_EN.pdf)

Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation, European Data Protection Board, Version 3.0., 4.6.2019, (erişim tarihi: 1.5.2023), https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12018-certification-and-identifying_en

Guidelines 4/2019 on Article 25 – Data Protection by Design and by Default, European Data Protection Board, 13.11.2019, (erişim tarihi: 12.5.2023), https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf

Guidelines on Artificial Intelligence and Data Protection, Council of Europe, T-PD(2019)01, Strazburg, 25.1.2019, (erişim tarihi: 3.5.2023), <https://rm.coe.int/guidelines-on-artificial-intelligence-and-data-protection/168091f9d8>

Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for purposes of Regulation 2016/679, Article 29 Data Protection Working Group, 17/EN, WP 248 rev.01, 4.10.2017, (erişim

tarihi: 15.5.2023), https://iapp.org/media/pdf/resource_center/WP29-GDPR-DPIA-guidance_final.pdf

Guidelines on the protection of individuals with regard to the processing of personal data in a World of Big Data Council of Europe, T-PD (2017)01, Strazburg, 23.1.2017, (erişim tarihi: 1.5.2023), <https://rm.coe.int/16806ebe7a>

Handbook on European Data Protection Law, Council of Europe, European Court of Human Rights, European Data Protection Supervisor, European Union Agency for Fundamental Rights, Lüksemburg, 2018,

KVK Kurumu, Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi, Ankara, 2019

Liability for Artificial Intelligence and Other Emerging Digital Technologies, Expert Group on Liability for New Technologies, (erişim tarihi: 10.6.2023), https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/JURI/DV/2020/01-09/AI-report_EN.pdf

OECD, **Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data**, OECD/LEGAL/0188, 23.09.1980, (erişim tarihi: 2.4.2023), <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188>

OECD, **Recommendation of the Council on Artificial Intelligence**, OECD/LEGAL/0449, 22.05.2019, (erişim tarihi: 17.3.2023), <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449#mainText>

Opinion 1/2010 on the concepts of “controller” and “processor”, Article 29 Data Protection Working Party, 00264/10/EN, WP 169, 16.2.2010, (erişim tarihi: 16.4.2023), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf

Opinion 15/2011 on the definition of Consent, Article 29 Data Protection Working Party, 01197/11/EN, WP187, 13.7.2011, (erişim tarihi: 16.4.2023), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf

Opinion 4/2007 on the Concept of Personal Data, Article 29 Data Protection Working Party, 01248/07/EN, WP 136, 20.6.2007, (erişim tarihi: 1.4.2023), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf

- Opinion of the European Data Protection Supervisor on the Data Protection Reform Package**, European Data Protection Supervisor, 2012, (erişim tarihi:12.5.2023), <https://rm.coe.int/guidelines-on-artificial-intelligence-and-data-protection/168091f9d8>
- Report by the Secretary General for the Ministerial Session in Helsinki, 16-17 May 2019, Ready for Future Challenges – Reinforcing the Council of Europe**, Council of Europe, 2019, (erişim tarihi: 18.4.2023), <https://rm.coe.int/168093af03>
- Report with Recommendations To the Commission on Civil Law Rules on Robotics**, (erişim tarihi: 8.6.2023), https://www.europarl.europa.eu/doceo/document/A-8-2017-0005_EN.html
- Strategic Action Plan on Human Rights and Technologies in Biomedicine (2020-2025)**, Council of Europe, (erişim tarihi: 4.5.2023) <https://rm.coe.int/strategic-action-plan-final-e/1680a2c5d2>
- Suggestion for A Green Paper On Legal Issues in Robotics**, EuRobotics, The European Robotics Coordination Action, 31.12.2012, (erişim tarihi 11.6.2023), https://www.unipv-lawtech.eu/files/euRobotics-legal-issues-in-robotics-DRAFT_6j6ryjyp.pdf
- The Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self assessment**, High Level Expert Group on Artificial Intelligence, , 17.6.2020, (erişim tarihi: 1.5.2023), https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=68342
- The Impact of Artificial Intelligence on the Doctor-Patient Relationship**, Council of Europe, (erişim tarihi: 1.5.2023), <https://rm.coe.int/inf-2022-5-report-impact-of-ai-on-doctor-patient-relations-e/1680a68859>
- Türkiye Büyük Millet Meclisi 26. Yasama Yılı, 1. Yasama Dönemi, Kişisel Verileri Korunması Kanunu Tasarısı (1/541) ve Adalet Komisyonu Raporu, (erişim tarihi, 30.3.2023), <https://www5.tbmm.gov.tr/sirasayi/donem26/yil01/ss117.pdf>
- Ulusal Yapay Zeka Stratejisi 2021-2025**, T.C. Sanayi ve Teknoloji Bakanlığı, Türkiye Cumhuriyeti Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, Ağustos 2021, (erişim tarihi: 18.03.2023), <https://cbddo.gov.tr/SharedFolderServer/Genel/File/TR-UlusalYZStratejisi2021-2025.pdf>
- UN General Assembly, **Guidelines for the Regulation of Computerized Personal Data Files**, 14.12.1990, (erişim tarihi: 11.4.2023), <https://www.refworld.org/pdfid/3ddcafaac.pdf>
- White Paper on Artificial Intelligence- A European Approach to Excellence and Trust**, European Commission, Brussels, COM (2020) 65 Final, Brüksel, 19.2.2020, (erişim

tarihi 17.3.2023), https://commission.europa.eu/system/files/2020-02/commission-white-paper-artificial-intelligence-feb2020_en.pdf

Working Document on the processing of personal data relating to health in electronic health records Article 29 Data Protection Working Party, 00323/07/EN, WP131, 15.2.2007, (erişim tarihi: 18.4.2023), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp131_en.pdf

III. İNTERNET KAYNAKLARI

<https://sozluk.gov.tr>

<https://www.oxfordlearnersdictionaries.com/definition/english/artificial>

Cook, Jamesi: “Amazon Patents New Alexa Feature That Knows When You’re Ill and Offers You Medicine”, **The Telegraph**, 09.10.2018, <https://www.telegraph.co.uk/technology/2018/10/09/amazon-patents-new-alexa-feature-knows-offers-medicine/>

Council of Europe, “History of Artificial Intelligence”, <https://www.coe.int/en/web/artificial-intelligence/history-of-ai>

European Commission, “Data Governance Act explained” 30.8.2022, <https://digital-strategy.ec.europa.eu/en/policies/data-governance-act-explained#:~:text=The%20Data%20Governance%20Act%20>

Kaya, İsmail “AI vs. Algorithms: What’s the Difference?”, 2018, <https://www.cmswire.com/information-management/ai-vs-algorithms-whats-the-difference/>

Kişisel Verileri Koruma Kurumu, “Veri Sorumlusu ve Veri İşleyen, Kişisel Verileri Koruma Kurumu”, <https://www.kvkk.gov.tr/Icerik/4195/Veri-Sorumlusu-ve-Veri-Isleyen>

KVK Kurumu, “Covid 19 ile Mücadele Sürecinde Kişisel Verilerin Korunması Kanunu Kapsamında Bilinmesi Gerekenler adlı Kamuoyu Duyurusu”, 27.03.2020, <https://www.kvkk.gov.tr/Icerik/6721/KAMUOYU-DUYURUSU-Covid-19-ile-Mucadele-Surecinde-Kisisel-Verilerin-Korunmasi-Kanunu-Kapsaminda-Bilinmesi-Gerekenler->

McCarthy, John, “What is AI? Basic Questions”, <http://jmc.stanford.edu/artificial-intelligence/what-is-ai/index.html>

IV. MAHKEME ve KURUL KARARLARI

Anayasa Mahkeme Kararı, E. 2006/167, K.2008/86, 20.3.2008. www.lexpera.com.tr

Anayasa Mahkemesi Kararı – 1.B. B.2018/30296, T.7.9.2011, www.lexpera.com.tr

Anayasa Mahkemesi Kararı – 2.B., B. 2018/6161 T. 28.6.2022, www.lexpera.com.tr

Anayasa Mahkemesi Kararı – GK, B. 2016/4060 T. 17.9.2020, www.lexpera.com.tr

Anayasa Mahkemesi Kararı – GK. E.2013/122 K.2014/74, T. 9.4.2014, www.lexpera.com.tr

Anayasa Mahkemesi Kararı – GK. E.2013/84, K. 2014/183, T. 4.12.2014, www.lexpera.com.tr

Anayasa Mahkemesi Kararı – GK. E.2014/180, K.2015/30, 19.3.2015, www.lexpera.com.tr

Anayasa Mahkemesi Kararı – GK. E.2015/32 K.2015/102, T. 12.11.2015, www.lexpera.com.tr

Anayasa Mahkemesi Kararı- 1.B., B. 2018/30296 T. 7.9.2021, www.lexpera.com.tr

Anayasa Mahkemesi Kararı- 1.B., B. 2018/30296 T. 7.9.2021, www.lexpera.com.tr

Danıştay Kararı – İDDK., E. 2019/763 K. 2020/1861 T. 15.10.2020, www.lexpera.com.tr

Danıştay Kararı – İDDK., E.2019/3167 L. 2021/734 T. 8.4.2021, www.lexpera.com.tr

Danıştay Kararı – İDDK., E.2020/420 K. 2022/214 T. 31.1.2022, www.lexpera.com.tr

Danıştay Kararı 8.D., E. 2017/3719 K.2022/2180 T.30.3.2022, www.lexpera.com.tr

Danıştay Kararı, 15.D. 10488/10500, 6.7.2017, www.lexpera.com.tr

Kişisel Verileri Koruma Kurulu'nun 19.11.2018 tarihli 2018/131 sayılı Karar Özeti:
(<https://kvkk.gov.tr/Icerik/5423/2018-131>)

Kişisel Verilerin Korunması Kurulu, 2018/10 sayılı Karar, 31.1.2018,
<https://www.kvkk.gov.tr/Icerik/4110/2018-10>

KVK Kurulu Kararı – K.2019/165, 31.5.2019, www.lexpera.com.tr

KVK Kurulu Kararı – K.2020/173, 27.2.2020, www.lexpera.com.tr

P.T. v. The Republic of Moldova Davası, Başvuru No: 1122/12, T. 26.05.2020,
<https://hudoc.echr.coe.int>,

Yargıtay Kararı - HGK., E. 2014/56 K. 2015/1679 T. 17.6.2015, www.lexpera.com.tr

Yargıtay Kararı – HGK., E.2017/1340, K.2018/1622, T. 6.11.2018, www.lexpera.com.tr

Yargıtay Kararı- CGK., E.2012/1514, K. 2014/312, T. 10.6.2014, www.lexpera.com.tr

Yargıtay Kararı- HGK., E.2017/1340 K.2018/1622 T.6.11.2018 www.lexpera.com.tr

YHGK, E.2012/13-1220, K. 2013/239, T.13.2.2013, www.lexpera.com.tr

Ö Z G E Ç M İ Ş

Adı ve SOYADI	Elif Ilgın ÖZCAN
EĞİTİM DURUMU	
Mezun Olduğu Lise	Adem Tolunay Anadolu Lisesi
Lisans Diploması	İhsan Doğramacı Bilkent Üniversitesi, Ankara, 2019.
Dönem Proje Konusu	Sağlık Hukukunda Kişisel Verilerin Korunması Kapsamında İdarenin Rolü ve Sorumluluğu
Yüksek Lisans Tez Konusu	Kişisel Verilerin Korunması Hukuku Bağlamında Sağlık Bilimlerinde Yapay Zeka Kullanımı
Yabancı Dil / Diller	İngilizce, Almanca
İŞ DENEYİMİ	
Stajlar	Ankara Barosu, Antalya Barosu
Çalıştığı Kurumlar	Antalya Barosu