ACIBADEM MEHMET ALİ AYDINLAR ÜNİVERSİTESİ
SAĞLIK BİLİMLERİ ENSTİTÜSÜ

BÜYÜK SAĞLIK VERİSİ VE ETİK: FAIR PRENSİPLERİ VE YENİ TEKNOLOJİ TABANLI SİSTEM ÖNERİSİ

GAMZE KAYA

YÜKSEK LİSANS TEZİ

BİYOETİK ANA BİLİM DALI

DANIŞMAN
Prof. Dr. Fatih Artvinli

İKİNCİ TEZ DANIŞMANI
Dr. Öğr. Üyesi Özkan Özdemir

İSTANBUL-2025

ACIBADEM MEHMET ALİ AYDINLAR ÜNİVERSİTESİ
SAĞLIK BİLİMLERİ ENSTİTÜSÜ

BÜYÜK SAĞLIK VERİSİ VE ETİK: FAIR PRENSİPLERİ VE YENİ TEKNOLOJİ TABANLI SİSTEM

GAMZE KAYA

YÜKSEK LİSANS TEZİ

BİYOETİK ANA BİLİM DALI

DANIŞMAN
Prof. Dr. Fatih Artvinli

İKİNCİ TEZ DANIŞMANI
Dr. Öğr. Üyesi Özkan Özdemir

İSTANBUL-2025

BEYAN

Bu tez çalışmasının kendi çalışmam olduğunu, tezin planlanmasından yazımına kadar bütün aşamalarda etik dışı davranışımın olmadığını, bu tezdeki bütün bilgileri akademik ve etik ilkeler içinde elde ettiğimi, bu tez çalışmasıyla elde edilmeyen bütün bilgi ve yorumlara kaynak gösterdiğimi ve bu kaynakları da kaynaklar listesine aldığımı, yine bu tezin çalışılması ve yazımı sırasında patent ve telif haklarını ihlal edici bir davranışımın olmadığı beyan ederim.

17.07.2025
Gamze Kaya

ÖNSÖZ VE TEŞEKKÜR

Öncelikle bu çalışmanın hazırlanmasında bilimsel kılavuzluklarıyla bana yol gösteren, yönlendirmeleri ve her aşamadaki yapıcı katkılarıyla bana rehberlik eden çok kıymetli danışmanlarım Prof. Dr. Fatih Artvinli'ye ve Dr. Öğr. Üyesi Özkan Özdemir'e gönülden şükranlarımı sunarım.

Akademik gelişimime ilham veren bakış açıları ve destekleyici tutumlarıyla bana yol gösteren değerli hocalarım Prof. Dr. Yeşim Işıl Ülman ve Dr. Öğr. Üyesi Ceren İlkan Rasimoğlu'na teşekkürlerimi sunuyorum.

Düşünme sevgisini bana ilk aşılayan, zihinsel ihtiyaçların bedensel olanlardan çok daha derin ve kalıcı olabileceğini öğreten sevgili babam Nedim Kaya'ya ve beni her daim destekleyen sevgili ablam Meryem Kaya'ya minnettarım.

Benimle ufuk açıcı tartışmalarda bulunan, karamsarlığa düştüğümde neşelendiren ve yardımlarını esirgemeyen değerli arkadaşlarım Burcu Saygıner, Semanur Özdemir ve Hilay Köse'ye süreci katlanılabilir kıldıkları için teşekkür borçluyum.

Bilgisayar ve informatik alanındaki teknik destekleriyle çalışmanın belirli aşamalarında katkılarda bulunan sevgili arkadaşlarım Zeynep Şevval Düvenci ve Muhammed Yusuf Yılmaz'a ayrıca teşekkürlerimle.

İÇİNDEKİLER

KISALTMA VE SİMGELER LİSTESİ

AİHS	Avrupa İnsan Hakları Sözleşmesi
API	Application Programming Interface (Uygulama Programlama Arayüzü)
BM	Birleşmiş Milletler
DAG	Directed Acyclic Graph (Yönlü Döngüsüz Grafik – blokzincir veri yapısı)
dBFT	Delegated Byzantine Fault Tolerance (Yetkilendirilmiş Bizans Hata Toleransı)
DLT	Distributed Ledger Technology (Dağıtık Defter Teknolojisi)
EHR	Electronic Health Record (Elektronik Sağlık Kaydı)
EMR	Electronic Medical Record (Elektronik Tıbbi Kayıt)
ESK	Elektronik Sağlık Kayıtları
FAIR	Findable, Accessible, Interoperable, Reusable (Bulunabilir, Erişilebilir, Birlikte Çalışabilir, Yeniden Kullanılabilir)
FHIR	Fast Healthcare Interoperability Resources (Hızlı Sağlıkta Birlikte Çalışabilirlik Kaynakları)
GDPR	General Data Protection Regulation (Genel Veri Koruma Tüzüğü)
HGP	Human Genome Project (İnsan Genom Projesi)
HIPAA	Health Insurance Portability and Accountability Act (Sağlık Sigortası Taşınabilirlik ve Sorumluluk Yasası)
HL7	Health Level 7 (Sağlıkta Veri Standardizasyon Protokolü)
IoT	Internet of Things (Nesnelerin İnterneti)
IPFS	InterPlanetary File System (Gezegenler Arası Dosya Sistemi – dağıtık dosya sistemi)
ISO	International Organization for Standardization (Uluslararası Standardizasyon Örgütü
KVKK	Kişisel Verilerin Korunması Kanunu
MDE	Model-Driven Engineering (Model Odaklı Mühendislik)
NHS	National Health Service (İngiltere'nin Ulusal Sağlık Servisi)

OECD	Organisation for Economic Co-operation and Development (Ekonomik İşbirliği ve Kalkınma Örgütü)
PBFT	Practical Byzantine Fault Tolerance (Pratik Bizans Hata Toleransı)
PoS	Proof of Stake (Hisse Kanıtı)
PoW	Proof of Work (İş Kanıtı)
SCP	Stellar Consensus Protocol (Stellar Ağı İçin Fikir Birliği Protokolü)
WHO	World Health Organization (Dünya Sağlık Örgütü)
ZKP	Zero-Knowledge Proof (Sıfır Bilgi Kanıtı)

ŞEKİLLER LİSTESİ

TABLOLAR LİSTESİ

ÖZET

Büyük Sağlık Verisi ve Etik: FAIR Prensipleri ve Yeni Teknoloji Tabanlı Sistem Önerisi

Bu tezde, büyük sağlık verisinin ortaya çıkardığı etik sorunlar incelenmiş ve bu sorunlara yönelik çözüm önerisi olarak FAIR veri yönetimi ilkeleri doğrultusunda değerlendirilmiş yeni teknoloji temelli bir sistem tartışılmıştır. Veri gizliliği, mahremiyet, şeffaflık, kontrol edilebilirlik ve güvenlik gibi temel etik ilkelere aykırı biçimde işleyen mevcut merkeziyetçi sağlık veri sistemlerinin, bireylerin verileri üzerindeki öznel denetimini sınırladığı ve veriye erişimde adaletsizlik yarattığı ortaya konmuştur. Bu sorunları aşmak amacıyla tez kapsamında merkezi olmayan (federe) sistemler, blokzincir teknolojisi, IPFS gibi yeni teknolojilerin sunduğu imkânlar etik bir perspektifle ele alınmış; birey hakları, eşitlik ve hesap verebilirlik ilkeleri ışığında yeni bir sağlık verisi yönetim modeli önerilmiştir. Önerilen yeni teknoloji tabanlı sistem, hızla büyüyen veri ekosisteminde karşılaşılan mevcut ve potansiyel etik sorunları gidermeye yönelik olarak tasarlanmış; veri gizliliği ve bilimsel ilerleme arasındaki dengenin kurulması gerekliliği vurgulanmıştır. Özellikle mahremiyet ve gizlilik gibi büyük sağlık verisi alanında en sık karşılaşılan etik meseleler değerlendirilmiş ve bu sorunlara yönelik çözümün yeni teknolojik yaklaşımlar aracılığıyla nasıl mümkün olabileceği tartışılmıştır

Anahtar Sözcükler: Etik, Büyük sağlık verisi, FAIR ilkeleri, Veri gizliliği, Blokzincir

ABSTRACT

Big Health Data and Ethics: FAIR Principles and a New Technology-Based System Proposal

This thesis examines the ethical issues raised by big health data and discusses a new technology-based system evaluated in line with FAIR data management principles to solve these issues. It is revealed that existing centralised healthcare data systems, which violate fundamental ethical principles such as data privacy, confidentiality, transparency, controllability, and security, limit individuals' subjective control over their data and create inequality in data access. To overcome these issues, the thesis examines the possibilities offered by new technologies such as decentralised (federated) systems, blockchain technology, and IPFS from an ethical perspective; a new health data management model is proposed in light of the principles of individual rights, equality, and accountability. The proposed new technology-based system is designed to address existing and potential ethical issues encountered in the rapidly growing data ecosystem, emphasising the need to strike a balance between data privacy and scientific progress. In particular, the most common ethical issues in the field of big health data, such as privacy and confidentiality, are evaluated, and how these issues can be addressed through new technological approaches is discussed.

Keywords: Ethics, Big health data, FAIR principles, Data privacy, Blockchain

1 GİRİŞ VE AMAÇ

Bu araştırmanın amacı, büyük sağlık verisinin kullanımında ortaya çıkan etik sorunları incelemek ve özellikle mahremiyet, bilgilendirilmiş onam ve adalet konularında çözüm önerileri sunmaktır. Günümüzde sağlık sektörü, genomik veri, klinik veri, biyomedikal veri gibi çeşitli büyük veri türleri ile hızlı bir dijital dönüşüm yaşamaktadır. Ancak bu veri zenginliği hem bireylerin mahremiyetini koruma hem de bu verilerin güvenli ve adil bir şekilde kullanılmasını sağlama konusunda önemli etik sorunları beraberinde getirmektedir.

Araştırma, FAIR (Findable, Accessible, Interoperable, Reusable) veri prensipleri (bulunabilirlik, erişilebilirlik, birlikte çalışabilirlik, yeniden kullanılabilirlik) çerçevesinde bu sorunları değerlendirerek, sağlık verisinin toplumsal faydaya katkı sağlarken mahremiyetin korunması arasındaki dengeyi incelemeyi hedeflemektedir. Ayrıca, yeni nesil teknolojilerin, özellikle federe sistem ve blockchain teknolojilerinin bu dengeyi nasıl etkileyebileceği ve mevcut etik çerçevelerin yeterliliği üzerine bir analiz sunulacaktır.

Bu çalışmada, sağlık verilerinin merkezi bir yapıda toplanmasının yarattığı gizlilik ve kontrol sorunlarına çözüm olarak, verinin üretildiği kurumda kalmasını esas alan federe bir sistem önerilmektedir. Önerilen modelde, federe sistemin altyapısında blokzincir teknolojisi kullanılarak, veriye erişim ve paylaşım süreçleri şeffaf ve izlenebilir hâle getirilmekte, böylece bireylerin veri üzerindeki kontrolü güçlendirilmekte ve etik riskler minimize edilmektedir.

Bu çalışmanın önemi hem Türkiye'de hem de uluslararası düzeyde, sağlık verisinin giderek artan kullanımının etik boyutlarına dikkat çekmesinde yatmaktadır. Sağlık verisinin güvenli ve etik yönetimi, sadece bireylerin temel haklarının korunması açısından değil, aynı zamanda toplumun sağlık alanındaki ilerlemeden en iyi şekilde faydalanabilmesi için kritik bir öneme sahiptir. Bu nedenle, bu araştırma, mevcut etik sorunları çözmeye yönelik yenilikçi yaklaşımlar, politikalar ve özellikle teknolojik çözümler geliştirilmesine katkıda bulunmayı amaçlamaktadır.

1.1 Büyük Veri Kavramı ve Sağlıkta Kullanımı

Günümüz dünyasında dijitalleşmenin hızlanmasıyla birlikte, bireylerin ve toplumların karar alma süreçlerini şekillendiren stratejik kaynaklardan biri haline gelen veri, gelecek için oldukça önemli bir güçtür. Teknolojinin gelişimiyle birlikte, günlük yaşamdan endüstriyel süreçlere kadar pek çok alanda veri üretimi ve kullanımı hızla artmaktadır. Bu durum, bireylerin, işletmelerin ve devletlerin veriye dayalı karar alma süreçlerine daha fazla yönelmesini de beraberinde getirmektedir. Verinin böylesine merkezi bir konuma gelmesi, sadece teknolojik gelişmelerin değil, aynı zamanda ekonomik, sosyal ve politik dinamiklerin de dönüşüm geçirmesine yol açmıştır. Veri odaklı stratejiler, şirketlerin rekabet avantajı elde etmesine, kamu politikalarının daha etkin hale gelmesine ve bireylerin yaşamlarını kolaylaştıran yenilikçi çözümler geliştirilmesine olanak tanımaktadır.

Bu noktada, verinin ne olduğu, nasıl üretildiği ve hangi süreçler aracılığıyla anlamlı hale getirildiği üzerinde durmak gerekir.

1.1.1 Veri tanımı

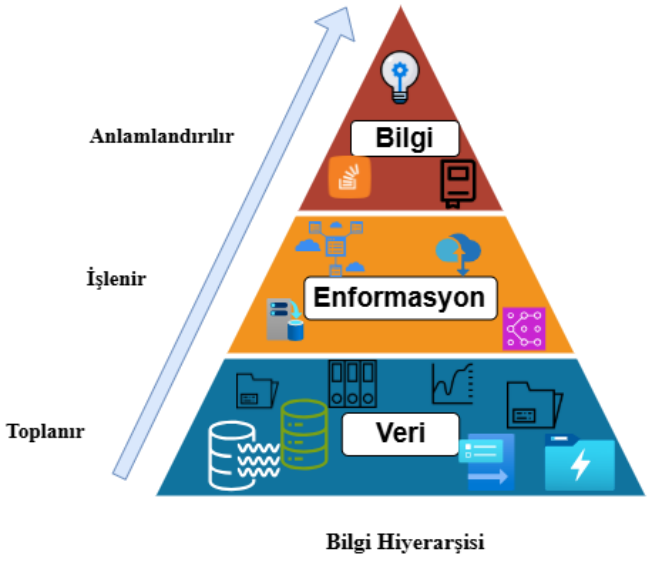
Veri (Data), ayrık, temel olgular veya gözlemlerdir. Henüz organize edilmemiş ve işlenmemişlerden oluşur (1). Bu nedenle, bir bağlama yerleştirilip yorumlanana kadar anlam veya değere sahip değillerdir (2). Başka bir deyişle, veri, tek başına bilgi değildir; aksine, çeşitli kaynaklardan toplanmış ve bir araya getirilmiş ham bir malzemedir (3). Veri, özellikle bir şeyler keşfetmek veya kararlar almak için incelenip kullanıldığında yeni olgular ve yeni bilgilerin oluşmasını sağlar.

Glaser'in "veri her şeydir" yaklaşımı, verilerin sadece görüşmelerde söylenilenlerden ibaret olmadığını, aynı zamanda nasıl söylenildiği ve hangi durumlar altında rapor edildiği gibi faktörleri de içerdiğini vurgular. Bu geniş anlayış, araştırmacıların, katılımcıların sözlü ifadelerinin yanı sıra, sözsüz iletişimlerini (yüz ifadeleri, beden dili, ses tonu gibi) ve verinin toplandığı bağlamı (fiziksel ve sosyal ortam, katılımcıların demografik özellikleri) da dikkate alması gerektiğini ifade eder. Kaynak ne olursa olsun, ister görüşme, ister gözlem, ister belge olsun hepsi bir veridir. Araştırma süreçlerinde her şey veri olarak görülebilir (4).

Veri tek başına bir anlam ifade etmediğinden anlamlı bir çıktıya dönüşebilmesi için enformasyona, ardından bilgiye evrilmesi gerekir.

Enformasyon (Information), verilerin sistematik bir şekilde işlenmesi, organize edilmesi ve yapılandırılması sonucunda ortaya çıkan anlamlı bir bütündür. Bu süreç, verilerin belirli bir düzene sokularak kullanılabilir hale getirilmesini sağlar (2). Ancak enformasyon, tek başına bilgi anlamına gelmez; bilgi, enformasyonun analiz edilmesi, bağlamsal olarak yorumlanması ve anlamlandırılmasıyla oluşan daha üst düzey bir kavramsal yapıdır. Bilgi, enformasyonun ötesine geçerek, onun pratik ve teorik bağlamlarda nasıl uygulanabileceğine dair bir içgörü sunar. Bu nedenle bilgi, enformasyondan daha derin ve bütüncül bir anlayış gerektirir ve insan zihninde sentezlenerek anlam kazanır. Bu hiyerarşik yapı, veriden enformasyona, enformasyondan bilgiye uzanan bir süreci ifade eder ve bu süreç, bilgi yönetimi ve bilgi teorisi gibi disiplinlerin temelini oluşturur (2, 5).

Bu üç kavram arasındaki ilişki şu şekilde özetlenebilir: Veriler, anlamlandırılmamış ham girdilerdir. Enformasyon, verilerin işlenmesiyle elde edilen ve bir miktar anlam içeren yapıdır. Bilgi ise, enformasyonun bağlam içinde anlaşılması ve eyleme dönüştürülmesiyle elde edilen ve karar verme süreçlerinde kullanılan üründür.



Şekil 1. Bilgi Hiyerarşisi

Veri, felsefi bir bakış açısıyla ele alındığında ise yalnızca soyut bir bilgi birikimi değil, aynı zamanda gözlem ve yorumlama süreçleriyle şekillenen dinamik bir olgu olarak değerlendirilir (6). Örneğin Michel Foucault veriyi yalnızca nötr bir bilgi kaynağı olarak görmektense, iktidar ilişkileriyle şekillenen bir öğe olarak değerlendirir. Verinin toplanması, yorumlanması ve kullanılması, yalnızca nesnel gözlemlerden değil, aynı zamanda toplumsal bağlamdan ve gücün işleyişinden de etkilenir. Foucault'nun "Bilginin Arkeolojisi" (1969) adlı eserinde, bilgi üretiminin toplumsal ve politik güç ilişkilerinden bağımsız olamayacağına dair vurgusu, verinin yorumlanmasında iktidarın rolünü ortaya koyar. Foucault'ya göre, bilgi sadece bir şeylerin bilinmesi değil, aynı zamanda güç ilişkilerinin şekillendirdiği bir araçtır (7).

Diğer bir önemli bakış açısı ise Byung-Chul Han'ın "Enfokrasi" adlı eserinden alınabilir. Han, günümüz toplumunda bilgi üretiminin ve paylaşılmasının, sadece bireylerin düşünsel özgürlüklerini değil, aynı zamanda iktidar yapılarını da nasıl dönüştürdüğünü tartışır. Han'a göre, dijital veri çağında güç, artık geleneksel iktidar mekanizmalarından çok daha karmaşık ve gözle görülemeyen yollarla işlemektedir. Bireyler dijital veriler yoluyla sürekli izlenmekte ve toplumsal bağlamda kendilikleri yeniden yapılandırılmaktadır (8). Bu düşünce, verilerin toplumsal, kültürel ve ekonomik bağlamda nasıl biçimlendiğini ve gücün işleyişinin veri toplama ve dağıtma süreçlerine nasıl yansıdığını açıklar.

1.1.2 Kişisel veri

Kişisel olana dair tanımlamalar, genellikle bir bireyin kimliğini belirlemeye yönelik unsurlar üzerinden şekillenir. "Kişisel" terimi, bireyi diğerlerinden ayıran ve onun benzersiz özelliklerini ortaya koyan her türlü nitelik veya bilgiyi ifade eder. Bu bilgiler, bireyin fiziksel kimliğinden, sosyal ilişkilerine, psikolojik özelliklerine kadar geniş bir spektrumda yer alabilir (9). Bir kişinin adı, yaşadığı yer, eğitim durumu, mesleki geçmişi gibi somut özellikler, genellikle kişiyi tanımlamak için yeterli olabilecek unsurlar arasında yer alır. Ancak yalnızca bu veriler, bir bireyin tam anlamıyla kimliğini ortaya koymaya yetmeyebilir. Zira sosyal çevresi, kültürel bağlamı, hatta psikolojik durumu gibi soyut faktörler de kişisel kimliğin önemli bir parçasını oluşturur. Bu nedenle, kişisel olanın kapsamı, hem bireyin fiziksel

varlıklarını hem de ona dair daha soyut, kimlik belirleyici nitelikleri içeren geniş bir çerçeveye sahiptir (10).

Kişisel veri, hem hukuki hem de etik açıdan ciddi bir sorumluluk alanı oluşturur; çünkü bu verilerin işlenmesi, depolanması ve paylaşılması, bireylerin temel haklarıyla doğrudan ilişkilidir (10).

Türkiye'de Kişisel Verilerin Korunması Kanunu (KVKK)**,** kişisel veriyi şu şekilde tanımlar: "Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi." Bu tanım, kişisel verilerin kapsamını yalnızca bireysel tanımlayıcı unsurların ötesine taşır; bireyin tıbbi durumu, biyometrik bilgileri, eğitim geçmişi, finansal durumu gibi çok farklı kategorilerdeki veriler de kişisel veri olarak kabul edilir. Bu veriler, yalnızca bir bireyi tanımlamakla kalmaz, aynı zamanda onun mahremiyetini, özgürlüğünü ve güvenliğini de doğrudan etkileyebilir (11) (6698 sayılı Kişisel Verilerin Korunması Kanunu, m. 3).

Avrupa Birliği'nin 2016/679 sayılı Genel Veri Koruma Tüzüğü (General Data Protection Regulation – GDPR), bir bireyin doğrudan veya dolaylı olarak "bir isim, bir kimlik numarası, konum verileri, bir çevrimiçi tanımlayıcı veya söz konusu gerçek kişinin fiziksel, fizyolojik, genetik, zihinsel, ekonomik, kültürel ya da sosyal kimliğine özgü bir ya da daha fazla unsur aracılığıyla" tanımlanabildiği her durumda, söz konusu bilginin kişisel veri olarak kabul edileceğini açık biçimde ortaya koymaktadır (12) (GDPR, 2016/679, Recital 30). GDPR, kişisel verilerin korunmasına dair geniş kapsamlı bir düzenleme sunmaktadır, ancak bu düzenleme ölen kişilerin verilerini kapsamadığını belirtir. Yani, ölüm sonrası kişisel verilerle ilgili herhangi bir koruma sağlanmaz. Ancak, birçok ülke bu konuda farklı düzenlemelere sahiptir ve bazı ülkeler ölüm sonrası kişisel verilere yönelik belirli kısıtlamalar getirebilir. Örneğin, Fransa gibi bazı ülkelerde ölen kişilerin kişisel verilerine yönelik yasalar vardır ve bu veriler bazı durumlarda korunabilir (13).

Kişisel verilerin önemi çoğu zaman yalnızca soyut düzeyde tartışılır; oysa bu verilerle olan ilişkimiz artık son derece gündelik, hatta sıradan hâle gelmiştir. Örneğin bir marketten küçük bir indirim kazanmak için ad, soyad, doğum tarihi, cinsiyet gibi temel kişisel bilgilerimizi paylaştığımızda, aslında bu verileri belirli bir ekonomik

değere karşılık teslim etmiş oluruz. Dışarıdan bakıldığında gönüllülük gibi görünen bu durum, aslında bireyin verisi üzerindeki kontrolünü kaybettiği bir rıza illüzyonuna işaret eder. Çünkü sonrasında bu verilere erişim sağlamak, silinmesini ya da sınırlandırılmasını talep etmek ya neredeyse imkânsızdır ya da son derece teknik ve zorludur (14). Dahası, bu verilerle ne yapıldığı konusunda çoğu zaman bilgilendirilmediğimiz gibi, bu verilerden üretilen değerin kimler arasında nasıl paylaşıldığı da tamamen belirsizdir. Oysa kişisel veri, yalnızca bireyin mahremiyetini değil; aynı zamanda dijital dünyadaki görünürlüğünü, temsilini, hatta haklara erişim kapasitesini belirleyen bir unsurdur (15). Bu nedenle, "veri kimindir?" sorusu yalnızca mülkiyet düzeyinde değil, özgürlük, eşitlik ve adalet düzeyinde de tartışılmalıdır (14).

Bugün kişisel veriler, sıradan bir hizmete erişmenin bile ön koşulu hâline gelmiş durumda. Kimi zaman bir uygulamayı kullanabilmek, kimi zaman bir randevu alabilmek, hatta kamu hizmetlerinden faydalanabilmek için bile verilerimizi vermeye zorlanıyoruz. Bu durum, dijital çağın bireye görünmeyen ancak etkili baskı biçimlerinden biridir. Görünürde gönüllü olan bu paylaşım, gerçekte çoğu zaman zorunlu bir razı oluş hâlidir (8). Kişisel verilerin bu kadar sistematik, geniş çaplı ve kontrolsüz biçimde toplanması; onları yalnızca "kişisel" olmaktan değil, aynı zamanda politik ve toplumsal bir mesele hâline getirmektedir. Çünkü bir toplumda verilerin kontrolü kimdeyse, birey üzerindeki güç de orada birikmektedir (14).

Dijital çağda kişisel verinin önemi: Dijital çağda, verinin fazla oluşu ve hemen hemen her alanda hızla büyüyen veri ekosistemi ve bu veri ekosisteminin bireyleri tanımlamak için farklı veri türlerini birbirine bağlama yeteneği, veri koruması açısından önemli ve giderek artan bir zorluk teşkil etmektedir.

Dijital teknolojiler ve çevrimiçi hizmetlerin yaygınlaşmasıyla birlikte, kişisel veri olarak kabul edilen bilgilerin kapsamı sürekli genişlemekte ve bu durum, verilerin doğru şekilde tanımlanması, sınıflandırılması ve korunmasının önemini artırmaktadır (16). Bu teknolojik gelişmelerle birlikte kurum ve kuruluşlar da, bireylerle ilgili birçok farklı türde veri toplamaya başlamış ve bu verilerin artan çeşitliliği, doğru sınıflandırma ve işleme gerekliliğini giderek kritik hale getirmiştir (17). Özellikle

verilerin farklı kaynaklardan bir araya getirilmesi, bireylerin kimliklerinin ortaya çıkarılması veya tahmin edilmesi açısından yeni zorluklar doğurmaktadır.

Özellikle veri çağında kişisel verilerin kapsamının sadece doğrudan kimlik bilgileriyle sınırlı olmadığını belirtmek önemlidir. Anonim veya parçalı veriler dahi, belirli bağlamlarda diğer bilgilerle birleştirildiğinde kişisel veri niteliği kazanabilir. Bu durum, özellikle veri analitiği ve yapay zeka teknolojilerinin gelişimiyle daha da karmaşık bir hale gelmiştir (18). Çoğu verinin depolandığı dijital ekosistemde, büyük veri analitiği ve yapay zeka sistemleri sayesinde bireylere ait farklı veri noktalarını bir araya getirerek tahminleme ve profil oluşturma süreçlerini hızlanabilmektedir. Kullanıcıların internet üzerindeki dijital izleri, satın alma alışkanlıkları, sosyal medya etkileşimleri veya mobil uygulama verileri, veri brokerleri ve şirketler tarafından analiz edilerek kişiselleştirilmiş hizmetler, hedef reklamlar ve hatta kredi skorları gibi alanlarda kullanılmaktadır (16, 19). Bu süreç, bireylerin davranışlarının öngörülebilir hale gelmesine ve kişisel verilerin ticari bir meta olarak değerlendirilmesine yol açmaktadır. Bu da dijital çağda hem kişisel verilerin hem de çoğu davranışımızın ne ölçüde önemli olduğunu vurgulamaktadır.

Sağlık verisi: Sağlık verisi, sağlıkla ilgili her türlü bilgi ve veriyi kapsar. Kişisel bilgiler içermek zorunda değildir. Genellikle toplum sağlığına dair genel bilgileri, anonimleştirilmiş verileri ve istatistiksel analizleri içerir. Sağlık verisi kişisel sağlık verisinden farklı olarak daha genel bir sağlık alanını kapsar (20). Ama gelişen teknoloji sayesinde sağlık verileri çok kolay bir şekilde kişiye indirgenebilir ve kişisel sağlık verisi haline gelebilir (21). Örneğin; bir bölgedeki grip vakalarının sayısı (anonim veriler) kişisel veri değil sadece toplumun sağlık verisini kapsamaktadır. Veya bir ildeki hastane yatak doluluk oranı o ildeki hastanelerin yatak doluluk oranından başka ne tür bilgiyi kapsayabilir? Genetik araştırmalardan elde edilen genel istatistikler de bu duruma örnek olarak verilebilir. Bakıldığında bu veriler kişisel bir sağlık verisini oluşturmaz. Ancak diğer üretilen sağlık verileri ile entegre edilerek bir bilgi ortaya konmak istense kişisel veriye kolayca erişilebilir. Özellikle sağlıkta büyük veri söz konusu olduğunda fazla sayıda sağlık verileri bir araya getirilerek bireyin kişisel sağlık verilerine ulaşabilir. Bu durumda kişisel sağlık verisi sağlık verisinin bir alt başlığı

olarak değerlendirilirken dijitalleşmeyle birlikte artık sadece kişisel sağlık verilerinden söz edilebilir.

1.1.3 Kişisel sağlık verisi

Kişisel sağlık verisi, hem fiziksel hem de ruhsal duruma ilişkin bilgiler içeren ve bireyin doğrudan ya da dolaylı biçimde kimliğini ortaya koyabilen özel nitelikli kişisel verilerdir (11). Bu tanımlayıcı niteliği nedeniyle, kişisel sağlık verisi, kişisel veriler içinde özel bir kategoriye dâhil edilmiş olup, hassas veri olarak kabul edilmektedir.

Türk hukuk sisteminde "hassas veri" kavramı, 6698 sayılı Kişisel Verilerin Korunması Kanunu'nda "özel nitelikli kişisel veriler" başlığı altında düzenlenmiştir. Kanunun 6. maddesine göre; bireylerin sağlık bilgileri, genetik verileri, dini inançları, siyasi görüşleri gibi bazı verileri, doğaları gereği ayrımcılığa yol açma potansiyeline sahip olduğu için daha sıkı koruma rejimi altına alınmıştır. Hassas veri, sadece kişiyi tanımlamakla kalmaz; onun hakkında ayrımcılığa, dışlanmaya veya zarar görmeye yol açabilecek özellikleri de açığa çıkarır. Hassas veriler ayrımcılık potansiyelleri nedeniyle diğer verilere oranla özel koruma gerektirir (11). Bu tür verilerin işlenebilmesi, ilgili kişinin açık rızasına veya kanunda öngörülen istisnai hallerin varlığına bağlıdır (22). 2024 yılında yapılan yasal revizyonla bu verilerin işlenme koşulları daha ayrıntılı biçimde düzenlenmiş olsa da, uygulamada bu düzenlemelerin nasıl hayata geçirileceği ve veri sorumlularının yükümlülüklerini ne ölçüde yerine getireceği halen belirsizliğini korumaktadır. Bu durum, mevzuattaki gelişmelere rağmen pratikte yeterli korumanın sağlanıp sağlanamayacağına dair soru işaretlerini beraberinde getirmektedir.

GDPR (Genel veri koruma yönetmenliği) sağlıkla ilgili verileri, gerçek bir kişinin fiziksel veya ruhsal sağlığıyla ilgili kişisel veriler olarak tanımlamaktadır (12). Bu, sağlık durumu hakkında bilgi veren sağlık hizmetlerinin sağlanmasını da içerir. Bu tanım oldukça geniş bir yelpazeyi kaplamakla beraber sağlık hizmetleriyle ilgili tüm verileri içerir. Tıbbi kayıtlardan ve tedavi geçmişlerine, teşhis sonuçlarına ve sağlık sigortası bilgilerine kadar uzanır. Günümüzde bireylerin akıllı cihazlarla (IoT-Internet of Things) ürettiği sağlık verileri de bu kapsamdadır (23).

Sağlık verilerin hassas yapısı, bu verilerin dikkatli ve bilinçli bir şekilde ele alınması gerekliliğini vurgular. Bireyin sağlığı ile ilgili tüm veriler (durum, teşhis, tedavi) kişisel olup, genetik verilerin de temelini oluşturur (24). Sağlık verilerin toplanması ve işlenmesi, teşhis, tedavi ve sağlık hizmetlerinin ilerlemesi açısından oldukça önemli bir kaynaktır. Bu veri sağlık hizmetlerinin ilerlemesini sağlarken hala kişisel sağlık verisi olarak ele alınmalı, bilinç ve sorumlulukla işlenip depolanmalıdır. Çünkü kişisel sağlık verileri başta birey olmak üzere toplumun da gerçek yaşamına dair bilgileri içerir (25).

1.1.4 Büyük veri (Big Data)

Son yıllarda teknoloji temelli dönüşümle birlikte, pek çok alanda paradigma değişimi yaşanmakta ve bu yeni anlayış, toplumsal yaşama giderek daha fazla entegre olmaktadır. Bu değişimin merkezinde, dijital teknolojilerin yaygınlaşması ve veri üretiminin olağanüstü biçimde artması yer almaktadır. Geleneksel veri toplama ve işleme yöntemlerinin ötesine geçilerek, günlük yaşamın her anında büyük miktarda veri üretilmekte ve bu veriler üzerinden çeşitli kararlar alınmaktadır. Günümüzde bireyler, dijital araçlar olmadan gündelik işlevlerini yerine getirmekte zorlanmakta; çünkü teknoloji, geçmişte zaman ve emek gerektiren birçok faaliyeti kolaylaştırmakta ve hızlandırmaktadır (26). Ancak bu kolaylık, aynı zamanda bireysel deneyimlerin, ilgi alanlarının, alışkanlıkların ve davranışsal eğilimlerin dijital ortamlara sürekli olarak veri biçiminde aktarılması anlamına gelmektedir. Bireylerin dijital teknolojilerle kurduğu bu yoğun etkileşim, her geçen gün daha fazla dijital iz bırakmalarına neden olmakta ve böylece "büyük veri" (big data) olarak adlandırılan devasa veri kümeleri ortaya çıkmaktadır. Büyük veri, sadece bireylerin kimliğini ve davranışlarını değil; aynı zamanda toplumların işleyişini, eğilimlerini ve geleceğe yönelik projeksiyonlarını da şekillendirebilecek güçte bir yapıya dönüşmektedir (27).

Dolayısıyla içinde bulunduğumuz çağ, yalnızca dijitalleşme süreciyle değil, bu dijitalleşmenin sonucu olarak ortaya çıkan veri yığınlarının yönetimiyle de tanımlanmaktadır (28). Bu noktada, büyük verinin tarihsel, felsefi ve bilimsel yönlerinin daha derinlikli olarak ele alınması gerekmektedir.

İnsan varolduğundan beri süregelen doğasıyla birlikte sürekli doğayı anlama, anlamlandırmaya çalışmıştır. Avcı toplayıcı insanlar doğasında gözlem yaparak, hayvanlara bakarak hangi bitkinin zararlı olduğunu hangi bitkinin yenilebilir olduğunu anlamaya çalışmıştır (29). Elde ettikleri gözlemsel verilerle ne yiyeceklerinin, nasıl yemeleri gerektiklerini öğrenmiş ve yaşamlarını sürdürmüşleridir. Daha sonraki aşamada toprağı nasıl kullanacaklarını, tarımı nasıl yapacaklarını, hayvanları evcilleştirerek ihtiyaçlarını nasıl gidereceklerini bularak yerleşik hayata geçmişlerdir (30).

Yerleşik hayata geçerek yavaş yavaş bir arada yaşamaya başlayan insanlar bu defa toplumun nasıl anlaşabileceğini, dili, kültürü, toplum yapısı üzerine düşünerek; insani değerleri, gelenek ve görenekleri, aileyi düşünerek bir yaşam alanı inşa etmiştir. Kendilerini hayata devam edebilecek bir konuma getiren insanlık bu defa doğayı, dönüşümü, evreni merak etmiş bu konuda fikirler öne sürmüştür. Her çağ yaşadıkları çağın sınırlılıkları içerisinde evreni ve oluşumuna dair gözlemler yaparak fikirler ortaya koymuştur (29).

Örneğin antik çağ bilimin yani evreni anlamanın sadece gözleme dayalı olduğu bir dönem olarak değerlendirilebilir. Eski Mısır'da ayın evreleriyle Nil Nehri'nin su seviyesi arasındaki ilişkiyi gözlemleyerek evrenin işleyişi hakkında bilgiler ortaya koymuştur. Bu ilişkiyi gözlemleyen bilim adamlarının yaptıkları şey "ne" sorunun cevabını bulmaktı. "Nasıl" sorusu o dönemlerde gelişmelerin merkezinde değildi çünkü daha ne olduğunu bilmedikleri şeyin nasıl olduğunu düşünmeleri olağan değildi (31). Gözleme dayalı bir korelasyon şeklinde ilerleyen bu dönemin bilimsel çalışmalarında, gözlenen olguların ölçülmesi, formüle edilmesi ve sonuçları değerlendirerek gelecek için bir öngörüde bulunulması mümkün değildi.

Orta Çağ'da ise bilgi, genellikle dini metinler ve antik Yunan ile Roma'nın eserlerine dayalıydı. Kilise ve dini otoriteler, bilginin en önemli kaynağıydı ve bilimsel çalışmalar bu otoritelerle uyumlu şekilde yürütülüyordu. Bilgi genellikle manastırlarda ve üniversitelerde toplanıyor, yazılı kaynaklar ve el yazmaları üzerinden aktarılıyordu. Ancak, Rönesans döneminde Antik Yunan ve Roma'dan gelen metinlerin yeniden keşfi, bilimsel düşüncenin uyanışına yol açtı. Artık bilgi, gözlem ve deney yoluyla daha doğrudan elde edilmeye başlandı. Özellikle Galileo, Kepler ve Copernicus gibi

bilim insanları, deneysel gözlemlerle bilimsel veriler toplamaya başladılar. Orta Çağ'dan Modern Çağ'a geçiş, bilimsel düşünce ve bilgi edinme yöntemlerinde köklü bir değişim yaşanmasını sağlamıştır (32).

Modern Çağ'a geçişle birlikte, bilimsel bilgi edinme yöntemleri hızla gelişmiştir. Deneysel yöntem ve empirizm, bilimsel keşiflerin temelini oluşturarak verilerin doğrudan gözlem ve deneyle toplanmasını sağlamıştır. Baskı makineleri, bilgilerin daha geniş kitlelere ulaşmasını sağlarken, istatistiksel yöntemler ile veriler daha sistematik bir şekilde analiz edilmeye başlanmıştır (33). Matematiksel modeller, doğa olaylarını anlamada önemli bir araç haline gelmiştir. Mikroskop ve teleskop gibi enstrümanların icadıyla, daha önce gözlemlenemeyen dünyalar keşfedilmiş ve veri toplama süreçleri hassaslaşmıştır (32). Thomas Kuhn'un Bilimsel Devrimlerin Yapısı (1962) gibi temel kaynaklar, bilimsel düşüncenin evrimini ve bu dönüşümün tarihsel boyutlarını daha detaylı bir şekilde ele alarak tartışmıştır (34) (33). Kısacası, Modern Çağ'da bilimsel bilgi, deneysel gözlem, teknolojik araçlar ve matematiksel analizler sayesinde daha doğru ve güvenilir hale gelmiş, verilerin toplanması ve işlenmesi süreci büyük bir dönüşüm geçirmiştir.

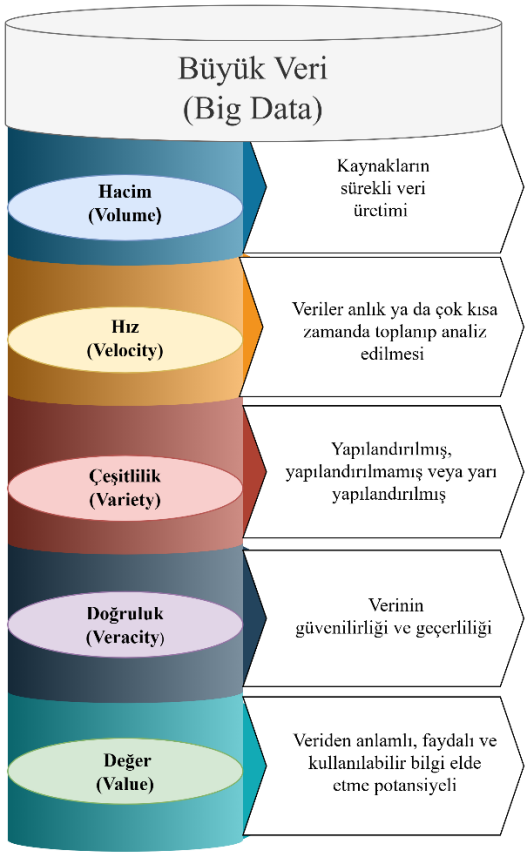
Bilgisayar teknolojilerinin gelişimiyle birlikte, bilimde elle yapılamayan karmaşık işlemler mümkün hâle gelmiş ve bu durum yeni bir paradigma yaratmıştır. Bu paradigma, veri üretiminin hızla arttığı, her şeyin ölçülebilir hâle geldiği bir veri ekosistemini beraberinde getirmiştir. Büyük veri, yalnızca bilgi miktarının artışıyla değil, aynı zamanda bu bilgiden anlam çıkarma kapasitesiyle de bilimsel yöntemlerde köklü değişiklikler yaratmıştır (35). Geleneksel bireysel araştırma modelleri yerini, bilişim ağlarıyla desteklenen çok paydaşlı ve hesaplamaya dayalı büyük bilim projelerine bırakmıştır. Özellikle internetin yaygınlaşmasıyla birlikte veri üretimi, depolanması ve paylaşımı olağanüstü bir hız kazanmış; böylece yaşadığımız çağ, büyük veri çağı olarak tanımlanır hâle gelmiştir (27).

Büyük Veri, literatürde en genel anlamıyla dünya genelindeki tüm bilgilerin dijital bir platformda toplanması ve bu bilgilere erişimin sağlanabilir olmasını ifade eder. Terim olarak ilk defa 1997 yılında NASA'da görevli bilim insanları Michael Cox ve David Ellsworth tarafından kullanılmıştır (36). Büyük Veri, sadece devasa miktardaki

bilginin dijital ortamda toplanmasını değil, aynı zamanda bu verilerin işlenebilir, analiz edilebilir ve anlam üretilebilir hâle getirilmesini ifade eder.

Bu kavramın özünü anlamak için sadece veri hacmine değil, aynı zamanda verilerin yapısına, üretim hızına ve güvenilirliğine de odaklanmak gerekir. Literatürde bu kapsam genellikle "5V" (Volume-Hacim, Velocity-Hız, Variety-Çeşitlilik Veracity-Doğruluk, Value-Değer) çerçevesinde ele alınır (25, 37-39).

Hacim, büyük verinin tanımlayıcı unsurudur; zira sensörlerden sosyal medyaya, tıbbi cihazlardan mobil uygulamalara kadar pek çok kaynak sürekli veri üretmektedir. Hız, bu verilerin anlık ya da çok kısa zaman aralıklarında toplanmasını ve analiz edilmesini ifade ederken; Çeşitlilik, yapılandırılmış (örneğin laboratuvar sonuçları), yapılandırılmamış (örneğin doktor notları) ya da yarı yapılandırılmış (örneğin XML dosyaları) farklı formatlardaki veri türlerini kapsar. Doğruluk ise verinin güvenilirliğini ve geçerliliğini tartışmaya açar. Değer, bu verilerden ne tür anlamlı sonuçlar çıkarılabildiğiyle ilgilenir. Ayrıca büyük veriden anlamlı, faydalı ve kullanılabilir bilgi elde etme potansiyelini temsil eder (40, 41). Bu çok boyutlu yapı, özellikle sağlık gibi yüksek hassasiyet gerektiren alanlarda büyük verinin potansiyelini ve risklerini birlikte değerlendirmeyi gerekli kılar.



Şekil 2. Büyük Verinin 5V Özelliği

Büyük veri, günümüzde endüstrilerin merkezine yerleşmiş önemli bir kaynak haline gelmiştir. Başlangıçta daha çok akademik araştırmalarda ve teknoloji geliştirmede kullanılan büyük veri, artık farklı sektörlerde ticari amaçlarla yoğun bir şekilde değerlendirilmektedir. Şirketler, büyük veri sayesinde iş süreçlerini daha verimli hale getirebilmekte, müşteri davranışlarını analiz edebilmekte ve bu analizler üzerinden pazarlama stratejileri geliştirebilmektedir. Büyük veriyi işleyebilme kapasitesi, organizasyonlara rekabet avantajı sağlayan bir unsur olarak öne çıkmaktadır. Özellikle yapay zeka ve makine öğrenimi gibi ileri teknolojilerle birleştiğinde, büyük veri şirketlerin karar alma mekanizmalarını dönüştüren bir güç haline gelmiştir (17).

Büyük verinin endüstrileşme süreci, teknolojik altyapıların gelişmesiyle ivme kazanmıştır. Bulut bilişim, veri depolama teknolojileri ve yüksek işlem kapasiteleri, şirketlerin devasa miktarlardaki veriyi toplayıp analiz etmelerine olanak sağlamıştır. Bu durum, finans, sağlık, perakende ve teknoloji gibi sektörlerde büyük veri tabanlı

yeni iş modellerinin doğmasına ve veri odaklı karar alma süreçlerinin yaygınlaşmasına yol açmıştır (42).

1.1.5 Sağlık alanında büyük veri

Büyük veri, sağlık sektöründe giderek daha merkezi bir rol oynamakta, tanı ve tedavi süreçlerinden sağlık politikalarının şekillendirilmesine kadar geniş bir etki alanına sahip olmaktadır. Sağlık, yalnızca bedensel iyilik hali değil, aynı zamanda sosyal ve ruhsal bütünlüğü de kapsayan çok boyutlu bir olgu olduğundan, bireyin yaşam kalitesi ve mutluluğu, büyük ölçüde sağlık durumu ile doğrudan ilişkilidir. Bundan dolayı sağlık alanında büyük veri birçok kaynaktan elde edilmektedir (43).

Elektronik sağlık kayıtları, genetik veriler, tıbbi görüntüler ve giyilebilir cihazlardan elde edilen biyometrik ölçümler gibi farklı kaynaklardan beslenen büyük veri, sağlık hizmetlerinin kişiselleştirilmesine, hastalıkların erken teşhisine ve sağlık sistemlerinin daha verimli yönetilmesine olanak tanımaktadır. Bu değişim, sağlık alanında yalnızca yöntemleri değil, veriye bakış açısını da büyük oranda dönüştürmüştür. Artık sağlık, bireysel deneyimler ve klinik gözlemlerle sınırlı olmaktan çıkıp, devasa veri setleri üzerinden analiz edilen kapsamlı bir bilgi ekosistemine dönüşmektedir. Bu bağlamda, büyük veri, sağlık hizmetlerinde yeni bir paradigma olarak öne çıkmakta ve hastalıkların öngörülmesinden tedavi süreçlerinin kişiselleştirilmesine kadar pek çok alanda değişimler yaratmaktadır (44, 45).

Örneğin, büyük veri analitiği klinik karar destek sistemleri aracılığıyla hekimlerin teşhis ve tedavi süreçlerinde daha bilinçli kararlar almasını sağlayarak sağlık hizmetlerinin etkinliğini artırmaktadır. Yapay zeka ve makine öğrenimi algoritmaları, bireylerin hastalık risklerini önceden tespit ederek erken müdahale imkânı sunmakta, böylece hastalıkların ilerlemeden kontrol altına alınmasına katkıda bulunmaktadır (41). Ayrıca, genetik ve biyomedikal verilerin analizi sayesinde kişiselleştirilmiş tıp uygulamaları geliştirilmekte, hasta odaklı tedavi yöntemleri belirlenerek sağlık hizmetlerinde bireyselleştirilmiş yaklaşımlar benimsenmektedir. Bunun yanı sıra, büyük veri analitiği sağlık politikalarının geliştirilmesinde de önemli bir rol oynamakta, toplum sağlığına yönelik daha bilinçli ve kanıta dayalı stratejilerin oluşturulmasına zemin hazırlamaktadır(46). Böylece büyük veri kullanımı hem

bireysel sağlık hizmetlerinin kalitesini artırmakta hem de toplum sağlığını koruma ve geliştirme amacı taşıyan geniş ölçekli politikaların şekillendirilmesine katkı sunmaktadır (47-50).

Ancak, büyük veri uygulamalarının sağlık alanına entegrasyonu yalnızca teknik bir dönüşüm değil, aynı zamanda etik ve hukuki açıdan da dikkatle ele alınması gereken bir süreçtir (41, 51). Bununla birlikte, sağlık alanında büyük verinin sunduğu olanakların etik bir çerçevede değerlendirilebilmesi için, bu sistemlerin güvenilirliği ve hesap verebilirliği büyük önem taşımaktadır. Hasta ile hekim arasındaki güven ilişkisi, sağlık hizmetlerinin niteliğini doğrudan etkileyen temel bir unsurdur; bu ilişkinin dijital sağlık teknolojileri bağlamında da sürdürülebilir olması, ancak veri güvenliğine ve etik ilkelere duyulan toplumsal güvenle mümkün olabilir (52). Büyük veri uygulamaları, bireylerin mahremiyetini ihlal etmeden, onların veri üzerindeki denetim hakkını gözeten şeffaf ve katılımcı mekanizmalarla yapılandırılmalıdır (44, 45). Özellikle sağlık gibi yüksek duyarlılığa sahip bir alanda, verinin yalnızca toplanması değil, aynı zamanda etik ilkelere uygun biçimde işlenmesi, saklanması ve paylaşılması da hayati öneme sahiptir. Bu nedenle, sağlık hizmetlerinde kullanılan büyük verinin yalnızca teknik değil, aynı zamanda etik, hukuki ve toplumsal yönleriyle de ele alınması gerekmektedir. Bu noktada, sağlık alanında hangi tür büyük verilerin üretildiği ve bu verilerin ne şekilde işlendiği sorusu önem kazanmaktadır. Bir sonraki bölümde, sağlık bağlamında kullanılan büyük veri türleri ayrıntılı olarak ele alınacaktır.

2 SAĞLIK ALANINDA BÜYÜK VERİ TÜRLERİ

Sağlık alanında büyük veri, farklı kaynaklardan elde edilen ve çeşitli amaçlarla işlenen geniş kapsamlı bilgi kümelerini ifade etmektedir (53). Bu veriler, doğrudan tıbbi süreçler sırasında sağlık çalışanları tarafından toplanabileceği gibi, bireylerin kendi rızalarıyla sunduğu bilgiler veya otomatik sistemler tarafından kaydedilen veriler şeklinde de elde edilebilir (41). Örneğin, hastane ortamında elektronik sağlık kayıtları (EHR-Electronic Health Record) aracılığıyla hasta öyküsü, laboratuvar sonuçları, görüntüleme verileri ve reçete bilgileri gibi yapısal sağlık verileri hekimler, hemşireler veya laboratuvar teknisyenleri tarafından kaydedilmektedir (54). Bunun yanı sıra, anketler, klinik araştırmalar ve epidemiyolojik çalışmalar yoluyla hasta deneyimleri, yaşam tarzı bilgileri ve hastalık seyri hakkında veri toplanmaktadır. Giyilebilir cihazlar ve uzaktan izleme sistemleri ise bireylerden sürekli veri akışı sağlayarak biyometrik ölçümler, kalp atış hızı, kan şekeri seviyesi gibi gerçek zamanlı sağlık göstergelerini kayıt altına almaktadır (28).

Toplanan verilerin kim tarafından işlendiği ve hangi amaçlarla kullanıldığı da büyük veri yönetimi açısından kritik bir konudur (36). Çoğu durumda, veriyi toplayan ile işleyen aktörler farklıdır; örneğin, hastane sistemleri hasta verilerini toplarken, bu veriler daha sonra ilaç geliştirme süreçlerinde veya halk sağlığı araştırmalarında biyoinformatik uzmanları ve veri analistleri tarafından işlenebilir (55). Ayrıca, sigorta şirketleri, ilaç firmaları ve sağlık politikalarını belirleyen kamu kurumları da bu verilerden faydalanarak analizler yapmaktadır (23). Ancak, bu süreçte hasta mahremiyetinin korunması ve veri paylaşımının etik ve hukuki çerçevede gerçekleştirilmesi büyük önem taşımaktadır. Özellikle hasta onamı, verinin kimler tarafından nasıl kullanılacağına dair açık bir bilgilendirme sürecini gerektirmekte ve bireylerin sağlık verileri üzerindeki kontrolünü sağlama açısından kritik bir unsur olarak değerlendirilmektedir (56). Dolayısıyla, sağlık alanında büyük veri türlerinin sınıflandırılması kadar, bu verilerin elde edilme yöntemleri, toplayıcı aktörler ve işleme süreçlerinin şeffaf bir şekilde tanımlanması da büyük önem taşımaktadır.

2.1 Klinik Veri

Bilgi teknolojilerinin sağlık hizmetlerine entegrasyonu, sağlık hizmetlerinin yürütülme ve belgelenme biçiminde köklü değişikliklere yol açmıştır. Günümüz dijital çağında, sağlık hizmetleri bireylere yönelik büyük miktarda veri üretmekte, işlemekte ve depolamaktadır. Sağlık hizmetleri geleneksel klinik anlatımın ötesine geçerek, modern sağlık merkezlerindeki veri tabanları; tanı, ilaçlar, laboratuvar test sonuçları ve radyolojik görüntüleme verileri gibi hastanın bakımını destekleyen yapılandırılmış bilgileri otomatik olarak kaydetmektedir. Sağlık alanındaki bu dönüşüm, hasta güvenliğini artırarak tanı ve tedavi süreçlerini hızlandırmakta ve yatak başında kolay erişim sağlamasıyla hastaların sağlık süreçleri için umut verici bir zemin oluşturmaktadır (43).

Klinik veri de bu dönüşümün bir parçası olarak, sağlık hizmetlerinin sunumunda kritik bir rol oynar. Klinik veri, hastaların teşhis, tedavi, takip ve bakım süreçlerine dair çeşitli tıbbi bilgilerin toplanmasını ve saklanmasını ifade eder. Bu veriler, hastaların demografik özelliklerinden (yaş, cinsiyet, etnik köken) başlayarak, tıbbi geçmişlerine (önceki hastalıklar, ameliyatlar, aile sağlık öyküsü) kadar geniş bir yelpazeyi kapsar (54).

Klinik verilerden elde edilen bulgular ve teşhisler, sağlık profesyonellerinin hastanın durumu hakkındaki gözlemlerini ve laboratuvar ile görüntüleme sonuçlarını içerir. Bunun yanı sıra, uygulanan tedavi süreçleri, ilaçlar, cerrahi müdahaleler ve rehabilitasyon gibi tıbbi müdahaleler de klinik verilerin önemli bir parçasını oluşturur. Klinik veriler genellikle elektronik sağlık kayıtları (ESK) sisteminde dijital olarak saklanır. Klinik veriler hasta bakımın merkezinde yer aldığından ESK için oldukça önemlidir. Bu nedenle elektronik sağlık kayıtlarının iyi benimsenmesi klinik verilerin ne kadar iyi desteklendiği ile ilgilidir. Klinik verilerin elektronik sağlık kayıtlarıyla entegre edilmesinin amaçlarından biri klinik verilerin yeniden kullanılabilirliğini de sağlamaktır; böylece, toplanan klinik veriler, sadece hasta bakımı ile ilgili değil, aynı zamanda araştırma ve politika geliştirme gibi diğer alanlarda da etkin bir şekilde kullanılabilir (57).

Bu tür verilerin araştırmalarda kullanılması; geniş çaplı epidemiyolojik çalışmaların yürütülmesi, hastalıkların erken teşhis edilmesi ve bireyselleştirilmiş tedavi yöntemlerinin geliştirilmesi açısından son derece değerli bir kaynak sunmaktadır (58). Özellikle bu veriler genomik verilerle birleştirildiğinde, hastalıkların genetik temellerini daha iyi anlamak mümkün olmakta, bu da yeni tedavi stratejilerinin geliştirilmesinin önünü açmaktadır (59).

Bu noktada klinik veriler bireylerin sağlığı açısından önemli bir rol oynamaktadır. Ancak klinik veriler tek başına büyük sağlık verisini oluşturmaz; yalnızca bu yapının bir bileşeni olarak karşımıza çıkar. Büyük sağlık verisi, klinik verilerin yanı sıra genomik, çevresel, davranışsal ve dijital iz verileri gibi pek çok farklı veri türünün entegre bir biçimde işlenmesiyle oluşur. Klinik verilerin sunduğu potansiyel, bu verilerin doğru yönetimi ve analizi ile daha da anlamlı hale gelir. Böylelikle hastalıkların daha iyi anlaşılması, kişiselleştirilmiş tedavi yaklaşımlarının geliştirilmesi ve sağlık hizmetlerinin daha verimli bir şekilde sunulması mümkün olur (57).

2.2 Biyomedikal Veri

Biyomedikal veri, sağlık alanındaki büyük veriyi oluşturan temel bileşenlerden biridir ve büyük ölçüde sağlık teknolojilerinin gelişimi sayesinde ortaya çıkmıştır. Özellikle laboratuvar ortamlarında teknolojinin yoğun şekilde kullanılması, biyomedikal verinin sürekli ve yüksek hacimlerde üretilmesine olanak tanımaktadır. Her gün yapılan deneyler, teşhis ve tedavi amaçlı testler, tıbbi görüntüleme uygulamaları gibi süreçler; büyük miktarda biyomedikal verinin ortaya çıkmasına neden olmaktadır.

Bu veri türü, insan sağlığı ve biyolojik süreçleri anlamaya yönelik olarak çeşitli tıbbi cihazlar ve laboratuvar yöntemleri aracılığıyla elde edilen kapsamlı ölçümleri içerir. Kan ve idrar testleri, tıbbi görüntüleme teknikleri (MR, tomografi, ultrason), biyopsi analizleri ve biyomarker çalışmaları biyomedikal verinin başlıca kaynakları arasında yer alır (60). Örneğin, bir hastanın kanındaki biyokimyasal bileşenlerin analizi, hekimlere daha kesin klinik değerlendirmeler yapma imkânı sunar. Bu

doğrultuda, biyomedikal veriler kişiselleştirilmiş tıp uygulamaları açısından önemli bir zemin oluşturur (60).

Tıbbi görüntüleme tekniklerinden elde edilen veriler tanı süreçlerini desteklerken, genetik verilerle birleştirildiğinde hastalık risklerinin öngörülmesine olanak sağlar. Aynı zamanda, bu veriler biyolojik mekanizmaların anlaşılması ve yeni tedavi stratejilerinin geliştirilmesinde de kritik rol oynar (40). Biyomedikal veri, yalnızca bireysel hasta yönetiminde değil, sağlık politikalarının şekillendirilmesi ve epidemiyolojik araştırmalarda da temel bilgi kaynağıdır.

Büyük sağlık verisi, çok kaynaklı ve çeşitliliği yüksek veri kümelerinden oluştuğundan; biyomedikal veri bu yapının önemli bir bileşeni olarak, hastalıkların biyolojik temellerini anlamamıza ve bireysel sağlık profillerine dayalı tedavi planlarının oluşturulmasına katkı sağlar (61).

Klinik veriden farklı olarak biyomedikal veri, daha spesifik ölçümler ve deneysel sonuçlara dayanır. Genellikle laboratuvar koşullarında üretilen bu veriler hem tedavi planlarının detaylandırılmasına hem de hastalara yönelik daha bilgilendirici geri bildirimlerin sunulmasına imkân tanır. Klinik ve biyomedikal verilerin entegre edilmesi, bireysel sağlık hizmetlerinde iyileştirme sağlarken, toplumsal sağlık stratejilerinde de yenilikçi yaklaşımların önünü açar.

Biyomedikal verilerin etkili yönetimi, sağlık hizmetlerinin kişiselleştirilmesi açısından büyük önem taşır. Bu bağlamda geliştirilen veri yönetim rehberleri, araştırmacıların verileri sistematik biçimde düzenlemesini ve bilim camiasıyla paylaşmasını kolaylaştırmaktadır (62).

Tanıdan tedaviye kadar uzanan tüm sağlık hizmeti süreçlerinde belirleyici rol oynayan biyomedikal veriler, hastalıkların anlaşılmasını kolaylaştırmakta ve yenilikçi, kişiye özgü tedavi yöntemlerinin geliştirilmesini desteklemektedir. Gelecekte biyomedikal verilerin daha bütüncül, güvenli ve erişilebilir biçimde kullanımı, tıpta kişiselleştirilmiş yaklaşımların yaygınlaşmasını sağlayacak, hem bireysel sağlık sonuçlarını hem de toplum sağlığını olumlu yönde etkileyecektir.

2.3 Davranışsal ve Çevresel Veri

Tarih boyunca çevresel ve davranışsal faktörler, sağlık krizlerinin oluşumunda ve çözümünde belirleyici olmuştur. Davranışsal ve Çevresel koşulların sağlığı doğrudan etkilediğinin geçmiş yıllarda da gördük çağımızda da hala görmekteyiz. Çevresel ve davranışsal faktörler, toplum sağlığını derinden etkileyen salgınların yayılmasında ve etkilerinin artmasında önemli rol oynamıştır. Örneğin orta çağdaki veba salgını, özellikle şehirlerdeki kötü hijyen koşulları, çöp yığınları, temiz su kaynaklarının yetersizliği ve kemirgenlerin varlığı gibi çevresel etkenler nedeniyle yayılmıştır. Şehirlerde yaşayan insanların dar sokaklarda ve sağlıksız yaşam koşullarında bulunması, salgının hızla yayılmasına ve halk sağlığının bozulmasına yol açmıştır. Yakın geçmişte (2020) yaşadığımız COVID-19 salgınında çevresel ve davranışsal faktörlerin sağlık üzerindeki etkilerine birçoğumuz şahit olduk. Örneğin COVID-19 salgını sırasında çevresel faktörler olarak kapalı ve havalandırması yetersiz alanlarda virüsün daha hızlı yayılabileceği öne çıkmıştır (63, 64). Ayrıca hava kirliliği ve yoğun nüfuslu şehirlerdeki koşullar, virüsün yayılmasını kolaylaştırmış bu da sağlığın hızla bozulmasına ve ölümlere yol açmıştır. Salgına yakalanma ve hasta olmanın diğer sebeplerinden biri de davranışlarımızdır. Maske takmamak, sosyal mesafe kurallarına uymamak gibi bireysel davranışlar, salgının kontrolsüz şekilde yayılmasına yol açmış başta toplum olmak üzere sağlığı olumsuz yönde etkilemiştir (63).

Son yıllarda yaşanan gelişmeler, çevresel ve davranışsal faktörlerin insan sağlığı üzerinde doğrudan etkili olduğunu açıkça ortaya koymuştur. Bu alanlara ilişkin veriler, yalnızca günümüz bireyleri için değil, aynı zamanda gelecek nesillerin sağlığı açısından da kritik öneme sahiptir. Çevresel ve davranışsal verilerin sağlık verileriyle ilişkilendirilmesi, hem kısa hem de uzun vadeli sağlık risklerinin daha kapsamlı biçimde değerlendirilmesine olanak tanır (51).

Çevresel veriler, bireyin fiziksel ortamıyla ilgili olup; hava kirliliği, su kalitesi, sanayi kirliliği ve iklim değişiklikleri gibi etmenleri barındırarak insan sağlığı üzerinde doğrudan etkilere sahiptir. Örneğin, hava kirliliği verileri, solunum yolu hastalıkları, kanser ve kalp hastalıkları gibi ciddi sağlık sorunlarıyla ilişkilendirilerek sağlık politikalarının şekillenmesinde kullanılmaktadır (25).

Davranışsal veriler ise bireylerin yaşam tarzlarıyla bağlantılıdır. Beslenme alışkanlıkları, sigara kullanımı, fiziksel aktivite düzeyi ve alkol tüketimi gibi bireysel tercihler, kronik hastalıklar için risk faktörleri olarak değerlendirilir. Örneğin, artan fast food tüketimi ve hareketsiz yaşam tarzı, 20. yüzyıl boyunca diyabet ve obezite gibi sağlık sorunlarının yaygınlaşmasına neden olmuştur (51).

Çevresel ve davranışsal veriler, sağlık sistemlerinde hastalık risk değerlendirmeleri yapılırken diğer büyük veri türleriyle, özellikle genomik verilerle entegre edilerek sağlık alanında yeni öngörülerin elde edilmesini sağlar. Bu veri etkileşimi, bireylerin genetik yatkınlıkları ile çevresel maruziyetleri arasındaki ilişkilerin analiz edilmesine olanak tanıyarak kişiselleştirilmiş sağlık stratejilerinin geliştirilmesini mümkün kılar. Örneğin, genetik olarak astıma yatkın bireylerin hava kirliliğine maruz kalmaları, hastalığın şiddetini artırabilir; bu da çevresel faktörlerin izlenmesinin klinik önemini göstermektedir.

Davranışsal ve çevresel veriler genellikle kamu kayıtları, dış sistemler ve bireylerin kendi bildirimleri aracılığıyla elde edilir. Bu veriler bağlamsal nitelikte olup, sağlık sonuçlarını etkileyen dışsal etkenlerin uzun vadeli takibi için kullanılır. Özellikle halk sağlığı araştırmaları ve epidemiyolojik çalışmalar kapsamında popülasyon düzeyindeki eğilimlerin analizinde rol oynar. Tarihsel olarak bulaşıcı hastalıkların yayılımı ve kronik hastalıkların gelişiminde belirleyici olan bu veriler, günümüzde büyük sağlık verisi kapsamında değerlendirilerek daha bütüncül ve öngörülü sağlık hizmetleri sunulmasına katkı sağlamaktadır. Bu tür verileri sürekli izleme ve etkili sağlık politikalarıyla desteklendiğinde, toplum sağlığının iyileştirilmesinde stratejik bir araç haline de gelebilmektedir.

2.4 Mobil ve Giyilebilir Teknoloji Verisi (IoT-Internet of Things)

Son yıllarda sağlık ve performans takibi oldukça önemli bir konu haline gelmiştir. Hem günlük aktiviteleri yerine getirmek bunun yanında da sağlıkla ilgili bilgi almak artık eskisi gibi kliniklere gidip de geleneksel cihazlarla öğreneceğimiz bir bilgi olmaktan çıkıp devrim niteliğinde bir hal aldı. Şu an öyle bir dijital dünyadayız ki kendi sağlık verimizi günlük yaşamda kullandığımız cihazlarla öğrenebiliyoruz.

Başlangıçta, sağlık verilerinin toplanması yalnızca klinik ortamlarla sınırlıydı ve veriler genellikle doktorlar tarafından yönetiliyordu. 20. yüzyılın sonlarına doğru, teknolojik ilerlemelerle birlikte sağlık sektörü dijitalleşmeye başladı, ancak bu veriler hâlâ oldukça geleneksel ve sınırlıydı. Veri toplama genellikle klinik ziyaretlerde alınan belirli sağlık ölçümleri yapmaktaydı (65).

Ancak 2000'lerin başlarından itibaren, dijital sağlık verileri toplama süreci büyük bir değişim geçirdi. Akıllı telefonların ve internetin yaygınlaşması, kişisel sağlık verilerinin toplanmasını hızlandırdı ve verilerin dijital ortamda daha kolay depolanmasını sağladı. Bununla birlikte, ilk giyilebilir sağlık teknolojilerinin ortaya çıkışı, bireylerin yalnızca hastalık durumlarını değil, sağlıklı yaşamlarını da takip etmelerini mümkün kıldı (66). Bu dönemde, bireyler yalnızca fiziksel aktiviteleri ve uyku düzenlerini izleyebiliyordu, ancak bu teknolojiler, kişisel sağlık yönetiminin ötesinde, sağlık verilerinin sağlık profesyonelleriyle paylaşılmasına olanak tanıdı.

Teknolojinin hızla gelişip günlük yaşamımıza entegre edilmesiyle, giyilebilir cihazlar daha sofistike hale geldi. Akıllı saatler, fitness bilezikleri ve mobil uygulamalar, artık yalnızca fiziksel aktiviteyi izlemekle kalmıyor; aynı zamanda kalp atış hızı, uyku düzeni, stres seviyesi, kan basıncı gibi biyometrik verileri de ölçebiliyor ve daha gelişmiş algoritmalar sayesinde kişiselleştirilmiş sağlık tavsiyeleri sunabiliyorlar (48). Bu tür cihazlar, veri toplamanın ötesine geçerek, sağlık yönetimi ve bireysel performans takibi için çok daha entegre ve işlevsel hale gelmiştir. Bu cihazlar, kullanıcıların sağlık durumlarını anlık olarak izlemelerine ve bu verileri uzmanlarla paylaşmalarına olanak tanırken, aynı zamanda kişiselleştirilmiş sağlık yönetiminin de kapılarını araladı.

Nesnelerin interneti (IoT- Internet of Things) olarak da adlandırılan giyilebilir teknolojik cihazlar, gerçek zamanlı olarak kendini raporlayan ve buna bağlı verimliliği arttırmaya yönelik eylemlerde bulunan ayrıca kişinin sağlığı ile ilgili önemli bilgileri diğer cihazlardan daha hızlı bir şekilde raporlayan cihazlar olmasıdır (67). Bu cihazlar, algılarımızın ötesindeki verilere erişmemizi sağlayarak sağlık durumumuz hakkında bilgi edinmemizi mümkün kılmaktadır. Günlük yaşamımızı bir sağlık nesnesine dönüştüren bu durum, sağlığı hastanelerden dijital ortama taşımaktadır. Artık teşhis ve tedavi süreçleri, yalnızca hastanelerde değil, dijital veriler aracılığıyla da

şekillenmektedir. Giyilebilir teknolojiler ve nesnelerin interneti, sağlığı fiziksel mekândan bağımsız hale getirerek onu dijital dünyanın bir parçasına dönüştürmektedir. Böylece sağlık, yalnızca hastanelerin değil, aynı zamanda veri ekonomisinin de bir unsuru haline gelmektedir.

2.5 Yüksek Çıktılı Veri (High-throughput Data)

Yüksek çıktılı veri, kısa sürede çok büyük miktarda ve çeşitlilikte verinin otomatik sistemler aracılığıyla üretilmesini ifade eder. Bu tür veriler genellikle biyoteknoloji ve biyomedikal araştırmalar bağlamında ortaya çıkar ve özellikle genetik, proteomik, transkriptomik gibi alanlarda kullanılır. "Yüksek çıktılı" ifadesi, klasik yöntemlerle uzun zaman alan ölçüm ve analiz süreçlerinin, gelişmiş teknolojiler sayesinde büyük ölçekte, eşzamanlı ve hızlı biçimde gerçekleştirilmesini vurgular (68).

Bu veri türü, özellikle yüksek çıktılı sekanslama (high-throughput sequencing, örn. yeni nesil dizileme teknolojileri) ve yüksek çıktılı tarama (high-throughput screening) teknikleriyle ilişkilidir. Örneğin, bir hastanın tüm genomunun kısa sürede dizilenmesi ya da binlerce ilaç adayının tek bir deney seti içinde test edilmesi, yüksek çıktılı veri üretimine örnek teşkil eder (69).

Yüksek çıktılı verinin temel özellikleri şunlardır:

- Hacim: Üretilen veri miktarı çok yüksektir (örneğin tek bir genom dizilemesi terabaytlarca veri üretebilir),
- Hız: Geleneksel yöntemlere göre çok daha kısa sürede veri toplanır,
- Çeşitlilik: Aynı anda birçok farklı biyolojik parametre ölçülebilir,
- Tekrarlanabilirlik ve otomasyon: İnsan hatasını minimize eden, makine destekli sistemlerle üretilir.

Bu tür veriler, özellikle sistem biyolojisi, kişiselleştirilmiş tıp ve büyük veri analitiği gibi alanlarda sağlık hizmetlerinin dijitalleşmesine önemli katkılar sunar. Ancak yüksek çıktılı veri, aynı zamanda ciddi analiz, saklama ve güvenlik gereksinimlerini de beraberinde getirir (70).

2.5.1 Genomik veri

İnsanoğlu tarih boyunca kendi doğasını anlamak ve anlamlandırmak için durmadan sorular sormuş ve cevaplayamadıkları, cevabı somut olarak gözle göremediklerini de doğaüstü olaylardan kaynaklandığını savunmuşlardır. Bu gözle görülemeyen ve bilinemeyene olan ilgi ve merak yıllar geçtikçe daha da artmış bununla birlikte birçok buluş ortaya çıkmıştır. Bu buluşlar bilimin daha da ilerlemesine ve doğaüstü olarak adlandırdıkları olayların aslında gerçek olarak var olduğunu da gözler önüne sermiştir. Gözle görülemeyeni gözle görülebilir kılan buluşlardan biri de mikroskoptur. Anton Van Leeuwenhoek'un bulunmasında ve gelişmesinde önemli katkı sağladığı mikroskop, insanların, çıplak gözle göremediği birçok yapı hakkında bilgi sahibi olmasını sağlayarak, bir bakıma birçok gelişmenin temelini oluşturmuştur. Ardından insanoğlu, bu buluşlar ve bilimin ilerleyişi sayesinde önce hücreyi, sonra çekirdeğini tanımlayarak, DNA çift sarmal yapısının çözülmesine (71) kadar giden yolun kapısını aralamıştır.

Mikroskobun icadıyla birlikte, daha önce çıplak gözle görülemeyen hücresel yapılar görünür hale gelmiş ve bu keşif, bilim insanlarının insan bedenini daha ayrıntılı bir şekilde incelemesine olanak sağlamıştır. Bu teknolojik gelişme, insan bedenine duyulan merakla birleşerek, genetik çalışmaların önünü açmıştır. İnsan Genom Projesi de bu gelişmelerin bir ürünü olarak, insanın genetik yapısını anlamaya yönelik büyük bir adım olmuştur (72).

İnsan genom projesi (HGP- Human Genome Project), insanın genetik yapısının haritasını çıkarmayı amaçlayan ve modern biyolojinin en önemli girişimlerinden biri olarak kabul edilen devrim niteliğinde bir projedir. 1990 yılında başlatılan ve 2003 yılında tamamlanan bu projeyle, insan DNA'sında bulunan yaklaşık 3 milyar baz çiftinin dizilimi belirlenmiştir. Proje, ABD Ulusal Sağlık Enstitüleri (NIH) ve Enerji Bakanlığı (DOE) tarafından yönetilmiş, uluslararası bir işbirliği içinde yürütülmüştür. HGP'nin temel hedefi, insan genomundaki genleri ve bu genlerin işlevlerini anlamaktır (73). Bu bilgi, insan biyolojisinin daha iyi anlamayı sağlamakla kalmamış, aynı zamanda genetik hastalıkların tanısı, tedavisi ve hatta önlenmesi için bir yol sunmuştur. HGP sayesinde, hastalıkların genetik temelleri daha iyi anlaşılmış,

farmakogenomik gibi kişiye özel tedavi yöntemlerinin gelişmesine zemin hazırlanmıştır (74).

İnsan genom projesini anlamak için, genom, gen, genetik kavramının ne anlamalara geldiğini de incelemek gerekir. Genom, bir organizmanın tüm genetik bilgisini taşıyan ve kromozomlarında bulunan DNA dizilerinin tamamını ifade eder. Genom, yalnızca genleri değil, aynı zamanda genler arasında kalan düzenleyici ve işlevsiz bölgeleri de içerir. Her hücredeki genom, organizmanın biyolojik işleyişini yöneten talimatları taşır ve türlere özgü bir yapıya sahiptir (73).

Gen, genomun içinde yer alan ve belirli bir proteinin veya fonksiyonel RNA molekülünün üretilmesi için gereken talimatları taşıyan DNA dizileridir. Genler, bir organizmanın tüm biyolojik süreçlerini kontrol eder ve bu süreçlerde önemli rol oynayan proteinlerin üretimini sağlar. Genomda, binlerce gen bulunur ve her biri farklı işlevlere sahip proteinleri kodlar (75).

Genetik ise, genlerin, kalıtımın ve genetik çeşitliliğin nasıl çalıştığını inceleyen bilim dalıdır. Genetik, organizmaların nesilden nesile aktarılan özelliklerinin nasıl ortaya çıktığını ve genetik bilginin nasıl bir organizmanın fenotipine (gözlemlenebilir özellikler) dönüştüğünü inceler. Genetik araştırmalar, hastalıkların nedenleri, kalıtımın mekanizmaları ve bireyler arasındaki genetik farklılıkları anlamamıza olanak sağlar. Kısaca genetik, kalıtsal özelliklerin ve organizmalar arasındaki değişkenliğin incelenmesidir (76).

Genomik, genetik bilginin tüm genom düzeyinde nasıl işlediğini, genler arası etkileşimleri ve bu bilgilerin organizmanın fenotipine nasıl yansıdığını araştırır. Genomik araştırmalar, bireysel genlerin ötesine geçerek, tüm genetik yapıyı incelemeyi hedefler ve biyomedikal araştırmalarda büyük önem taşır. Bütün genleri teker teker tanımlayarak birbirleri ve çevre ile etkileşimi inceleyen genomik alanı ortaya çıkan bilgiyi bilgisayar veritabanlarında işler, anlamlandırır ve saklar (77).

Kısaca özetlemek gerekirse, genom bir organizmanın genetik bilgisinin tamamıdır, genler bu bilginin işlevsel birimleridir, genetik bu genlerin işleyişini ve

kalıtımı inceleyen bilimdir, genomik ise genomun tamamını ve bu büyük yapının nasıl çalıştığını araştıran bir bilim dalıdır.

Genomik bilimin sunduğu en büyük avantajlardan biri, farklı organizmaların genetik bilgilerini karşılaştırma olanağı sağlamasıdır. Bu sayede, organizmalar arasındaki genetik benzerlikler ve farklılıklar evrimsel bir perspektifle incelenebilir ve biyolojik çeşitlilik daha iyi anlaşılabilir. Ayrıca, organizmaların ürettikleri proteinlerin çeşitliliği, sayısı ve işlevleri üzerine de detaylı bilgi edinme imkânı doğar. Genomik çalışmalar, bu bağlamda, yalnızca gen dizilimlerinin haritalanmasını değil, aynı zamanda bu dizilimlerin biyolojik işlevlerinin anlaşılmasını da içerir (74).

Genomik iki ana alana ayrılmaktadır: yapısal genomik ve fonksiyonel genomik. Yapısal genomik, genlerin fiziksel yapısının haritalanması ve gen dizilerinin belirlenmesi üzerine odaklanırken, fonksiyonel genomik ise bu genlerin işlevlerini, ifade biçimlerini ve biyolojik süreçlerdeki rollerini araştırır (74).

Yapısal genomik ve fonksiyonel genomik, genomik alanının iki temel bileşenidir. Yapısal genomik, bir organizmanın genomunun fiziksel yapısını, genetik dizilimlerini ve genlerin konumlarını inceleyerek genetik materyalin organizasyonunu anlamaya yönelik çalışmalardır. Bu disiplin, genetik haritalama, dizileme ve genom analiz yöntemlerini kullanarak genlerin ve genetik elementlerin yapısal özelliklerini ortaya koyar (78). Fonksiyonel genomik ise genlerin işlevlerini, etkileşimlerini ve bunların biyolojik süreçlerdeki rolünü araştıran bir alandır. Bu iki alan, genetik bilgilere dair bütünsel bir anlayış sağlayarak, hastalıkların mekanizmalarını, genetik varyasyonların etkilerini ve biyolojik süreçlerin nasıl işlediğini anlamamıza yardımcı olur (79).

Genomik verinin kullanım alanları arasında kişiselleştirilmiş tıp, hastalık araştırmaları, tarım ve biyoteknoloji, epidemiyoloji ve halk sağlığı ile klonlama ve genetik mühendislik yer alır. Kişiselleştirilmiş tıp, bireylerin genetik özelliklerine dayanarak daha doğru teşhis ve tedavi yöntemleri sunar (71). Hastalık araştırmalarında, kalıtsal hastalıkların ve kanserlerin genetik bileşenleri üzerinde yapılan çalışmalar, genetik varyasyonların tanımlanmasına yardımcı olur. Tarımda, genomik verilerle verimliliği artıran ve hastalıklara dayanıklı türler geliştiren biyoteknolojik uygulamalar yapılır. Epidemiyoloji alanında, patojenlerin genetik

özellikleri analiz edilerek bulaşıcı hastalıkların kontrolü sağlanır. Son olarak, genomik veriler, genetik mühendislik ve klonlama uygulamalarında, belirli genlerin manipülasyonu için temel oluşturur (72).

Genomik veri, özellikle günümüz bilimsel araştırmalarında ve sağlık uygulamalarında kullanılan merkezi bir veri türüdür. Bu verilerin analizi, genetik bilgilere erişimi artırmakta, sağlık alanında yeni gelişmelere yol açmakta ve bireylerin sağlık durumunu daha iyi anlamaya yardımcı olmaktadır. Genomik veri, kişiselleştirilmiş tıptan epidemiyolojiye kadar geniş bir uygulama yelpazesine sahip olduğu için, gelecekte daha fazla araştırma ve geliştirme için bir temel oluşturacaktır.

2.5.2 Proteomik veri

Proteomik fikrinin temeli, genomik çalışmaların başlamasıyla atılmıştır. Proteinlerin genetik bilginin son ürünü olduğu fikri, onları biyolojik süreçleri anlamak için kritik hale getirmiştir. İlk çalışmalar, 1970'lerde ortaya çıkan iki boyutlu jel elektroforezi (2D-GE) gibi teknolojilerle yapılmıştır. Bu yöntemle hücrelerdeki proteinler ayrıştırılabilir ve haritalanabilmiştir.

2000'lerin başında teknolojik cihazların gelişmesi ve insan genom projesinin tamamlanması (2003) ile proteomik çalışmalarına duyulan ilgi artmıştır. Yüksek performanslı sıvı kromatografisi[1] (HPLC) ve kütle spektrometresi[2] (MS) gibi ileri teknolojilerin geliştirilmesi, proteomik verilerin daha hızlı ve detaylı toplanmasını sağlamıştır (80). Modern dönemde ise proteomik çalışmalar, sistem biyolojisinin ve kişileştirilmiş tıp alanının yapı taşlarından biri haline gelmiştir.

Proteomik veri bir organizmanın veya biyolojik sistemin protein setine (proteom) ait bilgileri içerir. Proteom, bir genomun ifade ettiği tüm proteinleri temsil eder ve genetik, çevresel ve hücresel etkileşimlere bağlı olarak dinamik şekilde değişir. Proteom genomun aksine dinamik bir yapıya sahiptir. Proteom zamanla, farklı koşullar altında değişebilir (72). Örneğin, bir tırtıl ve kelebek aynı genoma sahip olmalarına

[1] Analitik kimyada kullanılan bir yöntemdir. Karışımları oluşturan bileşenlerin ayrıştırılması, özelliklerinin tanımlanması ve miktarlarının ölçülmesi amacıyla uygulanan bir analiz tekniğidir.

[2] Kütle spektrumu bir numunenin iyonik yük ve kütle oranına göre ayrışım yapan analitik bir yöntemdir.

rağmen, farklı proteomları nedeniyle farklı görünürler. Proteom sadece genler tarafından kodlanan proteinleri değil, aynı zamanda proteinlerin geçirdiği değişiklikleri de içerir. Bu değişikliklere post-translasyonel modifikasyonlar (PTM) denir (72, 81). Proteomik veri, bu proteinlerin türlerini, miktarlarını, yapısal özelliklerini, modifikasyonlarını, hücresel konumlarını ve işlevlerini anlamak için kullanılır (74). Belirli bir zamanda ve mekânda organizmanın sahip olduğu ve ifade ettiği bütün proteinlerin incelenmesi proteomik veri alanını oluşturur. Bu çalışmaların temel amacı, genlerin ve proteinlerin karmaşık etkileşimlerini anlamak ve bu bilgileri hastalıkların teşhis ve tedavisinde kullanmaktır (72).

Proteinler, hücresel işlevlerin yerine getirilmesinde ve biyolojik süreçlerin düzenlenmesinde önemli rol aldığından, proteomik analizler, hastalıkların biyolojik temellerini anlamamıza, biyobelirteçleri keşfetmemize, ilaç hedeflerini belirlememize ve tedavi yanıtlarını izlememize yardımcı olur. Özellikle kanser, kalp hastalıkları, nörolojik bozukluklar gibi karmaşık hastalıkların daha doğru bir şekilde teşhis edilmesi ve tedavi edilmesi için proteomik veriler büyük fırsatlar sunar(81).

2.5.3 Metabolomik veri

Metabolomik veri, bir organizmada ya da biyolojik bir örnekte bulunan tüm metabolitlere (küçük moleküllere) ait bilgileri ifade eder. Belirli bir zaman diliminde dokularda, hücrelerde ve fizyolojik sıvılarda bulunan küçük moleküllü metabolitlerin yüksek verimli teknolojiler kullanılarak saptanması, miktarının belirlenmesi ve tanımlanması da denilebilir. Bu küçük moleküller, lipidler, karbohidratlar, vitaminler, hormonlar ve diğer hücre bileşenlerini içerir ve genellikle molekül ağırlıkları 1.500 Da'un altındadır (74).

Metabolomik veri, 20. yüzyılın sonlarında, genomik ve proteomik alanlarındaki hızlı gelişmelerin bir uzantısı olarak ortaya çıkmıştır. "Metabolom" terimi ilk kez 1998 yılında Oliver ve arkadaşları tarafından kullanılmıştır ve bir organizmanın metabolik süreçlerinde yer alan tüm küçük molekülleri kapsar (82). Bu alandaki çalışmalara öncülük eden bilim insanları, biyolojik sistemlerin bütüncül bir yaklaşımla anlaşılabilmesi için genlerin, proteinlerin ve metabolitlerin birlikte değerlendirilmesi gerektiğini fark etmişlerdir (83).

Metabolomik çalışmalara verilen önem, bu alanın biyolojideki dinamik süreçleri anlamaya yöneliktir. Metabolitler, genetik, çevresel ve fizyolojik faktörlerin bir araya gelerek oluşturduğu karmaşık biyokimyasal reaksiyonların son ürünleridir. Bu nedenle metabolomik veri, biyolojik sistemlerin anlık durumunu yansıtan hassas bir araç olarak görülür. Özellikle tıpta ve biyoteknolojide metabolomik verinin değeri büyüktür. Kanser gibi karmaşık hastalıkların biyobelirteçlerini keşfetmek (84), kişiselleştirilmiş tedavi stratejileri geliştirmek ve ilaç yanıtlarını optimize etmek gibi uygulamalarda önemli rol oynar (82). Ayrıca, çevre bilimlerinde stres faktörlerine verilen tepkileri anlamak ve tarımda bitki metabolizmasını geliştirmek için de kullanılır. Biyolojik süreçleri anlamak için bir bütün değil parçalara ayrılarak bir bütünü oluşturan bu alanlar (proteomik, genomik, metabolmik, transkriptomik vb.) birbirleriyle entegre bir şekilde çalışarak fenotipi tanımlamaya ve genotip-fenotip boşluğunu doldurmaya yardımcı olur (85). Yüksek çıktılı olarak adlandırılan bu tür omik veriler özellikle günümüzde sıkça bahsedilen "kişileştirilmiş tıp" için de gelecek vaat eden bir alan haline gelmektedir.

2.5.4 Transkriptomik veri

Transkriptomik veri, bir hücre ya da dokuda belirli bir zamanda ifade edilen tüm RNA moleküllerinin (özellikle mRNA'ların) yüksek verimli dizileme teknolojileriyle analiz edilmesi sonucu elde edilen biyolojik veri türüdür. Bu veriler, gen ekspresyonunun çevresel koşullar, gelişimsel evreler ya da fizyolojik durumlara bağlı olarak nasıl değiştiğini göstermesi bakımından önemlidir (86). Genellikle RNA-Seq (RNA dizileme) yöntemi kullanılarak elde edilen transkriptomik veri üretim süreci; hücrelerden RNA izolasyonu, bu RNA'ların cDNA'ya dönüştürülmesi ve dizilenmesi aşamalarını içerir (87).

Transkriptomik veriler, gen ifadesindeki değişimleri analiz ederek genetik regülasyonun anlaşılmasına, hastalık mekanizmalarının aydınlatılmasına ve kişiselleştirilmiş tıbbın gelişmesine katkı sunmaktadır (88). Kanser, nörolojik hastalıklar ve enfeksiyonlar gibi pek çok alanda tanı ve tedavi hedeflerinin belirlenmesinde kullanılırken; aynı zamanda ilaç direnci mekanizmalarının incelenmesi, yeni biyobelirteçlerin keşfi ve kodlamayan RNA'ların işlevlerinin açıklanması gibi araştırma alanlarında da değerlendirilmektedir (89). Transkriptomik,

RNA-Seq teknolojisinin gelişimiyle birlikte 2000'li yıllarda yaygınlaşmış ve genomun dinamik ifadesini anlamaya yönelik temel araştırma alanlarından biri hâline gelmiştir.

2.5.5 Epigenomik veri

Epigenetik, DNA dizisinde herhangi bir değişiklik olmaksızın gen ifadesini ve fenotipi etkileyen kalıtsal mekanizmaları inceleyen bir alandır (90). Bu mekanizmalar arasında DNA metilasyonu, histon modifikasyonları ve kromatin yeniden düzenlenmesi gibi süreçler yer alır. Bu süreçlerin tümünü kapsayan epigenetik düzenin bütünü ise epigenom olarak adlandırılır. Epigenomik veri, bu düzenleyici mekanizmaların tüm genom düzeyinde sistematik olarak incelenmesiyle elde edilen bilgileri ifade eder. Genom dizisi sabit kalsa da, epigenomik veriler genlerin ne zaman ve hangi düzeyde ifade edileceğini belirleyen işaretleri içerir. Bu nedenle, epigenomik çalışmalar genetik bilginin hücresel bağlamda nasıl işlediğini anlamak açısından önemlidir (91).

Epigenomik veriler, özellikle hücre farklılaşması, gelişimsel biyoloji ve hastalık mekanizmalarının anlaşılması gibi alanlarda kullanılmaktadır. Örneğin, farklı hücre tiplerinde aynı genetik bilgiye rağmen farklı fonksiyonların ortaya çıkması epigenetik düzenleme ile mümkündür. Epigenetik bozuklukların, özellikle kanser, otoimmün hastalıklar ve nörodejeneratif hastalıklar gibi birçok sağlık sorununun temelinde yer aldığı gösterilmiştir (92). DNA metilasyonundaki değişiklikler veya histon proteinlerindeki modifikasyonlar, tümör baskılayıcı genlerin susturulmasına yol açarak hastalık gelişimine katkı sunabilir. Aynı zamanda çevresel etmenlerin, örneğin stres, toksinler veya beslenme gibi faktörlerin epigenetik izler bırakarak gen ifadesini değiştirebildiği, hatta bu etkilerin nesiller boyunca aktarılabildiği gösterilmiştir (93).

Epigenomik veriler, sadece hastalıkların anlaşılmasında değil, aynı zamanda tedavi stratejilerinin geliştirilmesinde de kullanılmaktadır. Özellikle epigenetik ilaçlar, gen ifadesi üzerinde düzenleyici etkiler oluşturarak kanser gibi hastalıklarda yeni tedavi olanakları sunmaktadır. Ayrıca, hücresel yeniden programlama süreçlerinde, yani somatik hücrelerin pluripotent kök hücrelere dönüştürülmesinde epigenetik yeniden düzenleme kilit rol oynamaktadır. Bu durum, rejeneratif tıp alanında epigenomiğin potansiyelini ortaya koymaktadır (90).

2.5.6 Diğer yüksek çıktılı veriler

Genomik, proteomik, transkriptomik, metabolomik ve epigenomik verilerin yanı sıra, farklı biyolojik süreçleri inceleyen çeşitli omik3 veri türleri de bulunmaktadır:

1) Lipidomik veriler: Hücrelerdeki tüm lipitlerin (yağ molekülleri) profillenmesiyle elde edilir. Özellikle enerji metabolizması, hücre zarları ve sinyal iletimi gibi süreçlerde önemli rol oynayan lipitlerin analizi için kullanılır.
2) Glikomik veriler: Proteinler ve lipitlere bağlı olan karbonhidrat yapılarını inceleyen verilerdir. Hücresel iletişim, bağışıklık yanıtı ve kanser biyolojisinde kritik öneme sahiptir.
3) Mikrobiyomik veriler: İnsan vücudunda yaşayan mikroorganizmaların genetik ve fonksiyonel bilgilerini içeren verilerdir. Özellikle bağırsak mikrobiyotası sağlık ve hastalık süreçlerinde önemli rol oynar.
4) Farmakogenomik veriler: Bireylerin genetik yapısına göre ilaçlara verdiği yanıtları belirleyen verilerdir. Kişiselleştirilmiş tıp ve ilaç geliştirme süreçlerinde kullanılır.
5) Toksikomik veriler: Çevresel toksinlerin ve kimyasalların biyolojik sistemler üzerindeki etkisini analiz eden verilerdir. Zehirli maddelerin organizmada yarattığı değişimleri anlamamızı sağlar.

Bu omik veri türleri, sağlık araştırmalarında büyük veri analitiğiyle birleştirilerek, hastalık mekanizmalarının anlaşılması, yeni tedavi yöntemlerinin geliştirilmesi ve kişiselleştirilmiş tıp uygulamalarının ilerletilmesine katkı sağlamaktadır (94).

3 Biyolojik sistemlerin bütüncül bir yaklaşımla incelenmesini ifade eden geniş bir terimdir.

3 SAĞLIK VERİSİNDE ETİK SORUNLAR

Etik, Yunanca “êthos” (ἦθος) kelimesinden türemiştir. Êthos, kelime anlamıyla, “karakter,” “alışkanlık” veya “doğru davranış” gibi anlamlara gelir. Antik Yunan'da “êthos” bireyin ya da bir toplumun ortak değerlerini ve yaşam biçimini ifade etmek için kullanılmıştır (95). Ardından bu kavram, Latinceye “ethica” olarak geçmiş ve “ahlak felsefesi” anlamında kullanılmaya başlanmıştır (96) (97). İnsanlık tarihinin en eski ve temel düşünce alanlarından biri olan etik kavramının tarihçesi, insanın doğru ve yanlış üzerine düşünmeye başladığı ilk dönemlere kadar uzanır (98). İlk kez Antik Yunan’da sistemli bir düşünce alanı olarak ele alınan “etik”, bu dönemdeki filozoflar tarafından, ahlak ve erdem kavramları üzerinde durularak ilerlemiştir.

İlk çağ filozoflarından Sokrates etik düşüncesinin öncüsü kabul edilir. Doğaya ve insana yönelik sorduğu sorularla, doğrunun ve doğru olanın ne olduğunu anlamaya çalışan Sokrates, sorularının cevabını “erdem” de bulmuş ve doğru yaşamın erdemli bir yaşam olacağını savunmuştur (99). Sokrates, bilginin erdem olduğunu ve kişinin doğruyu bildiğinde doğru olanı yapacağını düşünmüştür.

Sokrates’in öğrencisi Platon ise, etiği ideal devlet ve bireyin yaşamıyla ilişkilendirmiştir. Adalet, cesaret, ölçülülük ve bilgelik gibi erdemlerin uyum içinde olması gerektiğini vurgulamıştır. Aristoteles de etiği daha da pratik bir alan olarak ele almış ve yaptığımız ve yapacağımız bütün eylemlerde ölçülü olmamız gerektiğini vurgulamıştır (100). Aristoteles “Altın Orta” (mesotes) öğretisiyle dengeli bir yaşamın erdemli yaşam olduğunu savunmuştur. Aristoteles’in etik görüşü, “erdem etiği” olarak adlandırılan bir yaklaşım üzerine kuruludur. Onun etik düşüncesi, bireyin erdemli bir yaşam sürerek mutluluğa (eudaimonia) ulaşması gerektiğini savunur. Her insanın nihai amacının mutluluk olarak düşündüğünden o amaca yani mutluluğa ulaşmanın koşulu olarak da ölçülü/dengeli eylemek olduğunu düşünür (101). Aristoteles erdemi ise "iyi bir insanın iyi bir şekilde yapması gereken şey" olarak tanımlar. Ona göre erdem, karakterin bir özelliği olarak dengede olmayı gerektirir. Yani erdem iki aşırı uçtaki “orta yol” dur. Örneğin cesaret, korkaklık ve düşüncesiz atılganlık arasındaki orta yoldur. Cömertlik, savurganlık ve cimrilik arasındaki orta yoldur. Ayrıca Aristoteles’e göre erdemli bir yaşam sürmek için sadece doğru eylemi bilmek yetmez; bu bilgiyi

doğru zamanda ve doğru şekilde uygulamak gerekir. Aristoteles, bunu "pratik bilgelik" olarak adlandırır (102). Sadece insan bazında ele almaz erdemi, erdemi toplumsal bağlamda da değerlendirerek insanı "toplumsal bir hayvan" (zoon politikon) olarak tanımlar (100). Bu nedenle, bireysel mutluluk ancak toplumun genel iyiliğiyle uyum içinde olduğunda gerçek anlamını bulur.

Orta çağa gelindiğinde her alanda olduğu gibi etik alanı da büyük ölçüde dini düşüncelerle şekillenmiştir. Bu dönemde Hristiyanlık, İslam ve diğer büyük dinler, etik ilkelerin kaynağı olarak görülmüştür (103).

Aydınlanma döneminde etik düşünce, akıl ve bireysel özgürlük ekseninde yeniden inşa edilmiştir. Bu dönemin öne çıkan isimlerinden Immanuel Kant, evrensel bir ahlak yasasını savunarak "Kategorik İmperatif" ilkesini geliştirmiştir. Kant'a göre bir eylem, ancak evrensel bir yasa haline gelebiliyorsa ahlaki kabul edilebilir. Bu yaklaşım, "deontoloji" (ödev ahlakı) olarak adlandırılan bir etik anlayışına dayanır (104). Ahlakın temelini, insanın özgür iradesine ve akıl sahibi bir varlık olarak kendi eylemlerinden sorumlu olma kapasitesine bağlayan Kant, ahlaki davranışların zorunluluk ya da dışsal bir baskıyla değil, içsel bir ahlak yasasına (kategorik imperatife) uygun şekilde gerçekleşmesi gerektiğini vurgular (104).

Kategorik imperatif, evrensel bir ahlak yasasının temel ölçütüdür ve bir eylemin, herkes tarafından aynı şekilde uygulanabilir bir yasa haline gelip gelemeyeceğini sorgular. Örneğin, "Yalan söylemek yanlış mıdır?" sorusuna Kant'ın yaklaşımı, yalanın evrensel bir davranış haline gelmesi durumunda toplumsal güvenin yok olacağı ve iletişimin imkânsızlaşacağıdır. Bu nedenle, yalan söylemek evrensel ahlak yasasına aykırıdır. Kant'ın bu görüşleri, özellikle sağlık gibi insan hayatını doğrudan etkileyen alanlarda etik ilkelerin önemini artırmaktadır. Örneğin, bir hastanın tedavisinde doğru sonuçların paylaşılması yerine, deneycinin çıkarlarına uygun şekilde çarpıtılması, geri dönüşü olmayan sonuçlara, hatta bir hayatın kaybına yol açabilir.

Toplumsal bağlamda ise Kant'ın en dikkate değer görüşlerinden biri, insanın araçsallaştırılmaması gerektiğidir. Kant'a göre insan, kendi başına bir "amaç"tır ve hiçbir zaman yalnızca bir araç olarak kullanılmamalıdır. Bir bireyi yalnızca kendi

çıkarlarımız için bir araç olarak görmek, onun insan olarak sahip olduğu değeri yok saymaktır. Kant, her insanın "mutlak bir değer" taşıdığını ve bu değerin, insanın akıl sahibi ve özgür bir varlık olmasından kaynaklandığını savunur (99). Bu anlayış, insan onurunun korunmasının temelini oluşturur ve etik tartışmalarda güçlü bir referans noktasıdır.

Kant'tan sonra John Stuart Mill, utilitarizm (faydacılık) anlayışıyla etik tartışmalarına yeni bir boyut kazandırmıştır. Mill, eylemlerin sonuçlarına odaklanarak, en büyük mutluluğun en doğru eylem olduğunu savunmuştur (105). Yani iki eylemin sonucunda en fazla faydayı getiren eylemi doğru olarak kabul etmektedir. Mill'in bu görüşü sağlık alanında kaynakların etkin kullanımı ve toplumsal fayda açısından önemli avantajlar sunarken, bireysel hakların ihlali, adaletsizlik ve hesaplama zorluğu gibi etik sorunları da beraberinde getirir. Bu nedenle, faydacı ilkeler sağlık politikalarında ve tedavi kararlarında dikkatli ve dengeli bir şekilde uygulanmalıdır.

3.1 Etik Sorunlar

Felsefi düşünce ve bilimsel araştırmaların insana uygun en iyi uygulamasının yapılmasında disiplinler arası köprü görevi gören "etik" özellikle sağlık alanında gün geçtikçe daha da önem arz eden bir konu haline gelmektedir (106). Bilgi nesnesi insan olan sağlık alanı, insan ve değerlerine uygun bir biçimde eylemde bulunmayı kendine görev/ödev edinerek uygulamalar yapması gerekmektedir. Özellikle sağlık alanındaki bilgilerin hassas oluşu, bu bilgilerin daha da özenle ele alınmasını gerektirmektedir.

Aydınlanma döneminin etkisiyle şekillenmiş olan 19. ve 20. yüzyıl, bireysel haklar, toplumsal adalet ve bilimsel ilerlemeler gibi konulardaki gelişmeler doğrultusunda zenginleşmiştir. 20. yüzyıl ve sonrasında etiği ise modern etik olarak adlandırabiliriz. Modern dönemde etik, yalnızca soyut felsefi tartışmaların ötesine geçerek, somut sorunlar ve pratik durumlar karşısında çözümler sunmayı hedefleyen bir disiplin haline gelmiştir. Teorik alanın yanında pratik alana da gittikçe yoğunlaşmaya başlayan etik uygulamalı alanlara daha çok yönelerek, bu alanlar için çözüm önerileri sunar. Bu bağlamda uygulamalı etik, etik teorilerin günlük yaşam, politika, bilim, teknoloji, sağlık ve çevre gibi alanlara uygulanmasıyla ortaya çıkan etik sorunları ele alır (107). Tıp etiği, çevre etiği, teknoloji etiği ve veri etiği gibi alt

dallar gelişmiştir. Günümüzde etik, yapay zeka, biyoteknoloji ve büyük veri gibi konuların merkezinde yer almakta ve yeni zorluklara yanıt aramaktadır (98, 99).

Uygulamalı etik alanlarından biri olan Biyoetik alanı, yaşam bilimleri ve sağlıkla ilgili etik sorunları inceleyen; tıp, biyoteknoloji, genetik ve sağlık hizmetlerinde etik meseleleri ele almaktadır (108). Örneğin, genetik mühendisliği ile ilgili etik sorular, insan genlerinin manipüle edilmesinin sınırlarının ne olması gerektiğiyle ilgilidir. Aynı şekilde ötenazi, organ bağışı ve tıbbi araştırmalarda hasta hakları gibi konular biyoetiğin temel meseleleridir (109).

Ancak dijitalleşmenin hız kazandığı günümüzde, biyoetik alanı da geleneksel sınırlarını aşarak dijital teknolojilerin getirdiği yeni etik sorunlara odaklanmaya başlamıştır. Sağlık sistemlerinin dijital dönüşümü, yalnızca tanı ve tedavi süreçlerini değil; veri toplama, analiz, saklama ve paylaşım mekanizmalarını da köklü biçimde etkilemiştir. Bu bağlamda, büyük veri (big data) analitiğinin sağlık alanına entegrasyonu, biyoetik tartışmaların odağını giderek daha fazla kişisel sağlık verilerinin güvenliği, mahremiyeti ve denetimi gibi konulara kaydırmaktadır (110) (21, 111).

Biyoetik tartışmalarının büyük veriye doğru kaymasının başlıca sebebi ise; Büyük verinin sunduğu tüm potansiyellere rağmen, bu verilerin kullanımı beraberinde ciddi etik sorunları da getiriyor oluşudur. Bu sorunların temelinde, büyük veriden elde edilecek yararın yüksek olması beklenirken, verilerin yasal düzenlemeler ve etik kurallar çerçevesinde işlenmemesi yatmaktadır. Veri koruma yasalarına göre koruma yöntemleri ne yazık ki gerçek dünya da sıklıkla göz ardı edilebilmektedir. Özellikle mahremiyetin korunacağı, kişisel verilerin güvenli biçimde saklanacağı ve bireylerin verileri üzerindeki denetiminin sağlanacağı vaatlerine rağmen, veri işleme süreçlerinin bu ilkelere uygun biçimde yürütülmemesi ciddi şüpheler doğurmaktadır (51).

Tez boyunca detaylandırılan büyük verinin çeşitli aşamalarında yaşanan bu tür aksaklıklar, beklenen faydayı gölgede bırakarak ve bizleri etik sorunların odağına çekmektedir. Oysa veri sahipliği, özerklik, mahremiyet, adalet, gizlilik, bireylerin veri üzerindeki kontrolü, fayda sağlama ve zarar vermeme gibi ilkeler, mevcut yasal düzenlemelerin temelini oluşturur. Ancak bu ilkelerin pratikte etkili biçimde

uygulanmaması, özellikle veri paradigmasındaki dönüşümle birlikte, etik sorunların giderek daha görünür hale gelmesine neden olmaktadır.

Bu noktada, büyük veri kullanımına ilişkin etik problemler yalnızca teorik bir tartışma olmaktan çıkar; uygulamada bireylerin güvenini zedeleyen, toplumsal sonuçlar doğuran yapısal bir soruna dönüşür. Dolayısıyla, söz konusu etik sorunların çözümü için yalnızca yasal düzenlemelerin değil, aynı zamanda yeni teknolojik imkânların da devreye alınması gerekmektedir. Kısacası büyük verinin sağlıkta etik bir çerçevede kullanımı, teknolojik olanaklarla etik değerlerin dengelenmesini zorunlu kılmaktadır. Çözüm önerileri sunmadan önce etik meseleleri belirleyip ele almak çözümün ilk maddesi olacak ve çözüm yolunun önünü açacaktır.

3.1.1 Özerklik

Özerklik, genel olarak, bir bireyin kendi yaşamını şekillendirebilmesi ve kendi kararlarını verebilmesidir. Özerklik kavramını biraz daha detaylandıracak olursak; bir kişinin kendi değerleri, inançları ve hedefleri doğrultusunda, dışsal baskılardan veya müdahalelerden bağımsız bir şekilde, özgürce ve bilinçli olarak seçimler yapabilme kapasitesidir (109). Bu kavram, genellikle etik, felsefi ve psikolojik bağlamlarda önemli bir rol oynamaktadır ve bireyin karar verme süreçlerinde başkalarının etkisinden uzak, içsel bir irade ile hareket etme hakkını vurgular.

Sağlık hizmetleri bağlamında ise hastaların tedavi seçenekleri konusunda bağımsız kararlar alabilmesini ve kendi sağlıklarıyla ilgili kararları özgürce verebilmeleri anlamına gelmektedir (112). Bütün hasta bireylerin kendileriyle ilgili bilgileri bilme hakkı olduğundan kendi iradeleriyle istedikleri tedaviyi seçme özgürlüğüne sahiptirler. Ancak bu özgürlük durumu mutlak faydalarını ve onurlarını koruyacak şekilde olması daha doğrudur.

Hastanın kendi sağlık durumu hakkında bilgi edinme ve karar verme süreci yalnızca bireysel bir özerklik meselesi değildir, aynı zamanda bir iletişim ve bilgi paylaşımı sürecidir. Hastanın bilinçli kararlar alabilmesi için öncelikle mevcut sağlık durumu hakkında doğru ve yeterli bilgiye sahip olması gerekmektedir (108, 109).

Veri çağında özerklik ilkesi, yalnızca bireyin kendi hakkında bilgi sahibi olmasını değil, aynı zamanda kişisel sağlık verilerinin toplanması, işlenmesi ve paylaşılması süreçlerine aktif olarak katılabilmesini de kapsamaktadır. Bu bağlamda özerklik, bireyin kendi verisine dair karar süreçlerine dahil olması, bilgiye erişim hakkını kullanabilmesi ve gerektiğinde müdahale edebilmesini gerektirir. Verilerin paylaşımı sırasında bireylerin açık ve anlaşılır biçimde bilgilendirilmesi, rızalarının özgürce alınması ve verilerin kimler tarafından hangi amaçlarla kullanılacağının şeffaf biçimde açıklanması, özerklik ilkesinin etik açıdan gerekliliklerindendir. Ancak sağlık verilerinin büyük veri altyapılarında toplanması ve işlenmesi, "veri üzerindeki kontrolün kime ait olduğu" sorusunu gündeme taşımaktadır. Bu çerçevede, bireyin kendi verisi üzerindeki haklarını nasıl koruyabileceği ve veriye ilişkin karar yetkisinin veri sahibinde mi yoksa veriyi işleyen kurumlarda mı olması gerektiği gibi sorular, özerklik ilkesinin dijital çağdaki yeniden yorumlanmasını zorunlu kılmaktadır.

Bu bağlamda, büyük verinin merkezî yapılar tarafından kontrol edilmesi, bireyin kendi verisi üzerindeki söz hakkını zayıflatma tehlikesini beraberinde getirerek; veri üzerinde gerçek anlamda özerkliğin sağlamasını engelleyebilmektedir. Özerkliğin sağlanabilmesi için bireyin bu sürece aktif ve bilinçli biçimde katılımı teşvik edilmesi gereklidir. Veri sahipliğine dair belirsizliklerin giderilmesi, özerkliğin dijital çağda yalnızca teorik bir etik ilke değil, aynı zamanda teknolojik sistemlerle güvence altına alınması gereken dinamik bir hak olduğunu benimseyerek özerklik problemi ele alınmalıdır.

Tezin ilerleyen bölümlerinde, söz konusu özerklik sorunlarını azaltmaya yönelik, bireyin verisi üzerindeki kontrolünü güçlendirecek, şeffaflığı artıracak ve veri paylaşımını birey onamına dayandıracak bir çözüm önerisi olarak yeni teknoloji temelli merkezi olmayan sistem altyapısına dayalı bir model sunulacaktır. Bu öneri hem bireysel hakların güçlendirilmesine hem de etik veri yönetiminin tesis edilmesine katkı sağlaması beklenmektedir.

3.1.1.1. Aydınlatılmış onam

Aydınlatılmış onam (bilgilendirilmiş rıza), özellikle tıp, klinik uygulamalar ve biyomedikal araştırmalar bağlamında gelişmiş ve kökleşmiş bir etik ilkedir. Bu

kavram, bireyin kendi verileriyle ilgili bilinçli karar verme sürecinin temel taşı olarak kabul edilir. Veri mahremiyeti ve gizliliği yaklaşımlarında da merkezi bir yer tutan aydınlatılmış onam, kişinin verisinin ne amaçla kullanılacağını anlamasını ve buna onay vermesini gerektirir. Kadam (2017), bu tür rızayı, etik ilkeleri en iyi şekilde yansıtan ve bildirim-rıza ilişkisini en dikkatli biçimde kuran yöntem olarak tanımlar (113). Manson ve O'Neill (2007) ise bu çerçevede, veri toplayıcıların bireylere açık ve anlaşılır bilgi sunmalarını; bireylerin de bu bilgiler doğrultusunda rasyonel bir değerlendirme yaparak onam vermelerini gerekli gören bir yaklaşımı savunur (114).

Ancak büyük veri analitiği bu geleneksel yapıyı derinden sarsmaktadır. Büyük veriye dayalı analizlerin temel özelliği, çok büyük hacimli veri kümelerinde daha önceden öngörülemeyen örüntülerin, korelasyonların ve çıkarımların elde edilmesidir. Bu bağlamda, verilerin hangi bağlamda, nasıl bir yöntemle işleneceği ve hangi sonuçlara ulaşılacağı süreç başında net olarak belirlenememektedir (115). Bu belirsizlik, aydınlatılmış onamın özünü oluşturan "bilgilendirme" ilkesini uygulanamaz hâle getirmektedir. Çünkü kişi, verisinin hangi spesifik analizlerde ve hangi amaçlarla kullanılacağını bilmeden onam vermektedir.

Buradaki temel sorun, bireyin verisinin gelecekte ne şekilde kullanılabileceği konusunda ne yeterli bilgiye sahip olabilmesi ne de veri sürecine aktif bir biçimde katılabilmesidir. Bu pasif konum, yalnızca bireysel özerklik açısından değil, etik meşruiyet açısından da önemli sorunlar yaratmaktadır (116). Onamın yalnızca biçimsel bir prosedüre indirgenmesi ve "aydınlat ve geç" mantığıyla yürütülmesi, dijital çağda birey haklarını yeterince koruyamayan bir sistem doğurur. Bu noktada, büyük verinin dinamik ve sürekli dönüşen yapısının, durağan ve tek seferlik bir işlem olan aydınlatılmış onamla yapısal olarak uyuşmadığı görülmektedir. Söz konusu uyumsuzluk, modern veri etiğinin karşı karşıya kaldığı en temel problemlerden biridir (115).

Bu durumda büyük veri analizleriyle aydınlatılmış onam arasında yapısal bir gerilim bulunduğu açıktır. Bir yandan, büyük verinin hem bireysel hem toplumsal düzeyde sağlık alanında çığır açıcı katkılar sunma potansiyeli vardır. Ancak diğer yandan, bu verilerin bireylerin açık ve tam onamı olmaksızın farklı amaçlarla kullanılabilmesi, etik açıdan ciddi bir sorunu beraberinde getirir. Bu da büyük veri

çağında geleneksel aydınlatılmış onamın, bireyin verisi üzerindeki kontrolünü etkin biçimde sağlamada yetersiz kaldığını gösterir. Bu sorun bazı araştırmacılar tarafından rızanın ortadan kalkması şeklinde yorumlanmaktadır (116). Bu bağlamda, bireyin veri üzerindeki haklarını koruyabilmek adına iki alternatif onam yaklaşımı öne çıkmaktadır: geniş onam ve dinamik onam. Her iki model de bireyin verisinin toplanması ve kullanılması sürecine yönelik etik sorumlulukları farklı öncelikler temelinde ele alır.

3.1.1.2. Geniş onam

Geniş onam, bireyin verisinin yalnızca belirli bir araştırma kapsamında değil, gelecekteki farklı araştırmalarda da kullanılabilmesi için önceden genel bir onay verdiği yaklaşımdır (117). Özellikle biyobankalar ve büyük veri setlerinin kullanıldığı projelerde yaygın olarak tercih edilir. Bu onam modeli, araştırmalara esneklik kazandırmakta; verilerin daha geniş bağlamlarda tekrar işlenmesine olanak sunmaktadır (118).

Ancak geniş onam, bireylerin verilerinin gelecekte hangi amaçlarla ve kimler tarafından kullanılacağını tam olarak öngörememeleri nedeniyle etik açıdan ciddi tartışmalar doğurur. Geniş veri havuzlarında, elde edilecek sonuçların tahmin edilememesi ve verinin ileride nasıl bir bağlamda kullanılacağının belirsizliği, bireyin bilgilendirilmiş şekilde onam vermesini imkânsız kılmaktadır (116). Ayrıca, bu onam modeli verilerin daha fazla kuruma ve kişiye açılmasına da zemin hazırlayarak kötüye kullanım, mahremiyetin zedelenmesi ve veri güvenliğinin ihlali gibi riskleri beraberinde getirebilir (119).

Bu türde onam, "bilgilendirilmiş" olmanın gerektirdiği açıklık ve şeffaflığı tam anlamıyla sağlayamamakta, bireyin verisinin gelecekte nasıl bir kullanıma konu olacağına dair belirsizlikleri içerdiğinden dolayı klasik bilgilendirilmiş onam çerçevesine tam olarak yerleştirilememektedir (120). Korelasyonların hızla arttığı, verilerin anlamlarının bağlama göre değişebildiği büyük veri dünyasında geniş onam, etik açıdan daha da karmaşık bir hâl almaktadır (121).

3.1.1.3 Dinamik onam

Dinamik onam, bireylere veri kullanımı üzerinde sürekli kontrol ve güncellenebilir onam sağlama hedefi taşıyan bir modeldir. Bu yaklaşım, bireyin yalnızca başlangıçta değil, süreç boyunca düzenli olarak bilgilendirilmesini ve gerektiğinde onamını geri çekebilmesini mümkün kılar (116, 122). Böylece birey, verisinin hangi amaçlarla kullanıldığını takip edebilir ve katılımını bilinçli biçimde sürdürebilir.

Dinamik onamın birey lehine sağladığı bu şeffaflık ve kontrol avantajı, uygulamada bazı zorlukları da beraberinde getirir. Bireyin sağlık verilerinin kullanımıyla ilgili sürekli bilgilendirilmesi, onamını düzenli olarak güncellemesi ve süreci takip etmesi zaman ve çaba gerektirir (123). Özellikle sağlık ve teknoloji konularında yeterli bilgiye sahip olmayan bireyler için bu süreç karmaşık ve yorucu olabilir (124).

Dinamik onam, bireyin yalnızca veriye dair teknik süreçlerde değil, gündelik yaşamında da veriyle ilişkili karar alma süreçlerine entegre olmasını gerektirir. Bu nedenle bireyin sosyal yaşamına da yerleşmesi gereken bir katılım biçimi olarak değerlendirilebilir. Kendi sağlığına ilişkin kararlarda etkin olmak, bireyin etik özneliğinin güçlendirilmesi açısından önemlidir. Ancak bunun gerçekleşebilmesi, bireyin teknik altyapıya erişimi, dijital okuryazarlığı ve zaman olanakları gibi koşullara bağlıdır. Bu noktada, veri yönetişiminde rol alan diğer paydaşların da süreci destekleyici sorumluluklar üstlenmesi gereklidir (122).

Geniş ve dinamik onam modelleri, veri yönetimi süreçlerinde farklı öncelikler barındırır. Geniş onam modelinde toplumsal fayda ve bilimsel ilerleme esas alınırken, dinamik onam bireyin bilgilendirilme hakkını ve özerkliğini öncelemektedir. Ancak bu iki yaklaşım arasında etik açıdan ideal bir denge kurulabilmiş değildir. Dinamik onam birey merkezli, katılımcı bir model olsa da yapısal ve teknik erişim sorunları nedeniyle yaygın olarak uygulanamamaktadır. Öte yandan, geniş onam bireyin kontrolünü zayıflatarak veri etiği açısından ciddi tartışmalar doğurmaktadır. Bu nedenle, büyük sağlık verisinin yönetiminde her iki modelin güçlü yönlerini

harmanlayan ve etik ilkelere dayalı yeni onam yaklaşımlarının geliştirilmesi gerekmektedir.

3.1.1.4 Veri sahipliği ve kontrol

"Sahiplik" kavramı, bir şeyin ya da kişinin mülkiyetine veya yönetimine sahip olma özelliği anlamını taşır. Sahiplik, bireysel bir nesne, alan veya mülk üzerinde kontrol, kullanma, yararlanma ve devretme hakkına sahip olduğu olarak da tanımlanmaktadır (125). Sahiplik anlayışı, insanların örgütlenmesiyle ortaya çıkmıştır. İlkçağlarda insanlar, temel ihtiyaçları karşılamak üzere doğal kaynaklar üzerinde hak iddia etmeye başlamıştır. Bu dönemde sahiplik, topluluk düzeyinde geçerli olan bir anlayışla, kabile veya klan gibi topluluklara aitti. Ancak zamanla bireysel sahiplik ön plana çıkmaya başlamıştır(126).

Orta Çağ Avrupa'da feodal sistemin yaygınlaşmasıyla sahiplik kavramı daha çok toprak mülkiyeti etrafında şekillenmiştir. Feodal beyler, topraklar üzerinde hakimiyet kurmuş ve bu topraklarda yaşayan köylüler, feodal beye bağımlı olarak toprakları işleyebilmişlerdir. Burada bireysel mülkiyetten ziyade, bir otoritenin (feodal bey ya da kilise gibi) toprak üzerinde hak sahibi olduğu görülmüştür (127).

Aydınlanma dönemiyle birlikte bireysel özgürlük ve haklar kavramı gelişim göstermiştir. Özellikle John Locke gibi düşünürler, özgürlüğü bireyin emeğiyle kazandığı bir hak olarak görmüştür. Locke'nin bu bakış açısı bireysel haklar ile mülkiyet ilişkisine yeni bir boyut kazandırmıştır (128). Bu düşünce, Batı'da mülkiyet haklarının hukuki sistemlerde daha sağlam bir zemin bulmasına katkı sağlamıştır (129). Bugün, bireyler hem maddi hem de manevi varlıklar üzerinde geliştirilmiş hukuki haklara sahiptir. Kişisel mülkiyetin yanı sıra telif hakları ve fikri mülkiyet gibi kavramlar, bireylerin sahip oldukları değerleri koruma altına almaktadır (130).

Sahiplik kavramını büyük sağlık verisinde kullandığımızda, bireylerin sağlık verileri üzerindeki hakkı ve kontrolü, çok boyutlu bir tartışma alanı haline gelmektedir. Sahiplik, tarih boyunca maddi mülkiyet ve emek üzerinden kurulan bir hak iken (131), günümüzde büyük sağlık verisinin dijital dünyada giderek daha fazla önem kazanmasıyla, sağlık bilgileri üzerinde mülkiyet iddiası da farklı bir boyut kazanmıştır.

Bu bağlamda, sahip olunan varlık kavramı genişleyerek yalnızca fiziksel varlıkları değil, aynı zamanda dijital veriler ve bu verilerle yapılabilecek işlemleri de kapsar hale gelmiştir (132).

Geleneksel anlamda kullanılan sahiplik, bir nesne ya da mülk üzerinde fiziksel hakka sahip olma kapasitesini taşırken (131), büyük sağlık verinde sahiplik veya veriye sahip olma, sağlık geçmişi, genetik bilgi ve günlük yaşamlardan elde edilen çok çeşitli veriler üzerinde kontrol sağlar. Bireylerin sağlık verileri üzerindeki sahiplik hakkı, bu verilerin nasıl, kim tarafından ve hangi amaçla kullanılabileceğini, bilmelerine ve belirlemelerine imkân sağlar. Ancak sağlık verilerinin değerli bir bilgi kaynağı olarak ekonomik potansiyeli, bu sağlanan sahiplik sistemini daha karmaşık hale getirmektedir (133).

Sağlık verilerinin kime ait olduğu sorusu hem hastalar hem de sağlık hizmet sağlayıcıları açısından giderek karmaşık bir konu haline gelmektedir. Hastalar genelde kendi verilerinin sahibi olmak isterken, hastane veya sağlık hizmeti sağlayıcıları veriyi topladıkları ve analiz ettikleri için sahiplik haklarının kendilerinde olduğunu savunabilmektedir (133). Özellikle dijital sağlık platformları ve uygulamalarının yaygınlaşması, bu sahiplik konusunu daha da karmaşık hale getirir.

Bireylerin sağlık verileri üzerindeki sahipliği ve bu veriler üzerinde kontrol yetkisi, etik açıdan mahremiyet ve özerklik ilkeleriyle doğrudan ilişkilidir. Modern hukuk sistemleri ve etik çerçeveler, bireylerin kişisel sağlık verileri üzerinde hak sahibi olduğunu savunsa da büyük sağlık verisi bağlamında bu sahipliğin pratikte nasıl hayata geçtiği tartışmalıdır (134). Günümüzde veriler sadece bireyler tarafından üretilmekle kalmamakta; aynı zamanda sağlık hizmet sunucuları, teknoloji şirketleri, sigorta kurumları ve devletler tarafından toplanmakta, analiz edilmekte ve çoğu zaman merkezi sistemlerde depolanmaktadır (135).

Bu merkeziyetçi yapı, sağlık verisinin sahibinin kim olduğu sorusunu muğlaklaştırmaktadır. Bireylere ait olan veriler, merkezi veri tabanlarında birleştirildiğinde, veri üzerindeki fiili kontrol bireylerden ziyade veriyi işleyen kurumlara geçmektedir. Bu durum hem sahiplik hem de kontrol hakkı açısından bireylerin konumunu zayıflatmaktadır. Sağlık verisinin üretimi her ne kadar bireyin

kendisinden kaynaklansa da bu veriler çeşitli teknolojik araçlar ve uygulamalar aracılığıyla toplanmakta, depolanmakta ve farklı amaçlarla yeniden kullanılabilmektedir. Örneğin, giyilebilir cihazlar veya mobil sağlık uygulamalarıyla üretilen veriler, genellikle kullanıcıdan çok, veriyi işleyen şirketlerin veri tabanlarında anlam kazanır (132).

Büyük sağlık verisinin ölçeği ve kapsamı genişledikçe, bireylerin verileri üzerinde doğrudan bir kontrol sağlaması da giderek güçleşmektedir. Merkezi sistemlerde depolanan ve anonimleştirildiği iddia edilen verilerin bile izlenebilir olması, bireylerin verilerinin nasıl, ne zaman ve kim tarafından kullanıldığına dair denetim imkânlarını sınırlamaktadır. Verinin sürekli üretildiği ve işlendiği bir ortamda bireyin veri kontrolünü sürdürebilmesi pratikte mümkün olmamaktadır. Bu nedenle sahiplik ve kontrol kavramları, büyük veri bağlamında işlevini yitirme riskiyle karşı karşıyadır.

Verilerin merkezi yapılarda toplanması, bireyleri kendi sağlık verileri üzerindeki ahlaki öznellikten uzaklaştırmakta ve onları pasif veri sağlayıcısı veya veri üreticisi konumuna indirgemektedir. Oysa etik açıdan bireylerin sağlık verileri üzerinde sahiplik ve denetim hakları, yalnızca mahremiyetin korunması için değil, aynı zamanda bireysel özerkliğin sürdürülmesi için de önemlidir (133). Veri sahipliği ve kontrolü yalnızca teknik bir mesele değil, aynı zamanda bireyin kendilik haklarıyla doğrudan ilişkili bir etik meseledir.

Bu noktada, merkeziyetçi veri yapılarının yarattığı etik sorunların nasıl aşılabileceği ve bireyin sağlık verileri üzerindeki denetiminin nasıl yeniden tesis edilebileceği çözüm önerisi sonraki bölümlerde tartışılacaktır.

3.1.2 Mahremiyet ve gizlilik

Bugün "özel alan" dediğimiz şeyin, aslında oldukça politik ve tarihsel bir geçmişi vardır. Özel alan, batı literatüründe "private", "privato", "privat", "privée" gibi kavramlarla karşılığını bulmuş (17), uzun süre kamusal olanın karşıtı olarak düşünülmüş; bireyin kendi iç dünyasına çekildiği, başkalarının müdahalesinden uzaklaştığı bir alanı tanımlamak için kullanılmıştır (136). Ancak bu "özel alan", gerçekten bireyin özgürleştiği ve başkalarının müdahalesinden kaçtığı bir sığınak

mıdır, yoksa iktidar mekanizmalarının en derinlere nüfuz ettiği ve bu nedenle de en çok doğallaştırılan denetim biçimlerinden biri midir? sorusunu gündeme getirmektedir (8).

Bu bağlamda, özel alanla yakından ilişkili olan mahremiyet (privacy) kavramı üzerinde durmak gerekir. Mahremiyet, modern bireyin temel haklarından biri olarak kabul edilir ve yalnızca kişisel bilgilerin gizliliğini değil, aynı zamanda bireyin kendi bedeni, düşünceleri, ilişkileri ve yaşam tarzı üzerinde tasarruf hakkını da içerir (137). Bu noktada, mahremiyetin yalnızca bireysel bir tercih ya da bilgi gizliliği meselesi değil, daha geniş bir hak çerçevesinde ele alınması gerektiği açıktır. Nitekim "özel yaşam hakkı" (right to privacy), yalnızca mahremiyetin korunmasını değil, bireyin kişisel yaşamını serbestçe düzenleyebilmesini, bedeni ve kimliği üzerindeki tasarrufunu, aile ilişkilerini ve iletişimini dış müdahalelere karşı koruyabilmesini de kapsamaktadır (138).

Avrupa İnsan Hakları Sözleşmesi'nin 8. maddesi bu hakkı açıkça tanımakta; özel hayatın, konutun, aile yaşamının ve haberleşmenin gizliliğini güvence altına almaktadır. Bu yönüyle, özel yaşam hakkı, bireyin yalnızca "görünmez" olma talebini değil; aynı zamanda kimliğini oluşturma, ifade etme ve sürdürme özgürlüğünü de içine alan çok katmanlı bir haktır (139). Dijital teknolojiler çağında ise bu hakkın kapsamı genişlemekte; bireylerin çevrimiçi etkinliklerinden sağlık verilerine kadar pek çok unsur, özel yaşamın sınırlarını yeniden tanımlamaktadır (140).

Ancak burada mahremiyetin sadece bireysel haklarla sınırlı olmadığı, aynı zamanda toplumsal bir düzenin ürünü olduğu da göz ardı edilmemelidir. Ünlü sosyolog Émile Durkheim'e göre mahremiyet, yasaklık anlamına gelir ve toplumsal normlar ile bireyin haklarıyla bağlantılı olarak, herkesin erişemeyeceği; sadece kişinin rızasıyla paylaşılabilen bilgilerin bulunduğu bir alanı ifade eder (141).

Bu kavram, kişiye kendi hakkındaki bilgilerin ne şekilde ve ne ölçüde başkalarına paylaşılacağına karar verme hakkı tanır (52). Karar verme hakkı sağlık alanında daha da belirginleşir. Sağlık alanında bilgi ve iletişim teknolojilerinin yaygınlaşmasıyla birlikte, sağlık verileri de bu dönüşümün bir parçası olmuştur. Dijitalleşen sağlık verilerinin yetkisiz kişiler tarafından erişilebilir hale gelmesi, bireyin kendi hakkındaki

bilgilerin kiminle paylaşacağına dair olan karar verme hakkını da ihlal ederek, mahremiyetin korunmasını daha da önemli bir mesele haline getirmiştir (142, 143). Kişisel sağlık verilerinin dijitalleşmesi ve bu verilerin toplandığı platformların yaygınlaşması, bireylerin kimliklerinin anlık olarak ifşa edilme riskini de beraberinde getirmiştir (144, 145). Bu, mahremiyetin dijitalleşen dünyada karşılaştığı tehlikelerden yalnızca biridir. Sağlık alanının karmaşıklığı, bireyin sadece kişisel verilerinin değil, aynı zamanda ailesi ve toplumu hakkında sahip olduğu bilgilerin de önem taşıdığını gösterir. Sağlık hizmetleri için gerekli olan bu bilgiler, bireysel mahremiyetin ötesine geçerek, başkalarının mahremiyetini de etkileyen bir sorun haline gelir. Dolayısıyla, mahremiyetin kapsamı yalnızca bireye ait verilerle sınırlı değildir; toplumsal bağlamda başkalarının da mahremiyeti söz konusudur (52).

Mahremiyet kavramının yerine kullanılan ama aynı anlama gelmeyen bir diğer kavram da gizlilik kavramıdır. Yukarda bahsedildiği gibi mahremiyet, veri sahibinin o bilgiyi kimlerle paylaşabileceğinin veya bilginin kimler tarafından kullanılabileceği kararının kişinin elinde bulundurması anlamına gelirken, gizlilik bu bilginin gizli kalması, ilgisiz kişilerden saklanması, kişinin mahremine özen göstererek bilgiyi dışardaki kişilerden koruması anlamına gelir (146). Kısacası kişisel bilgilerin yalnızca yetkili ve izlenen kişilerle paylaşılmasını, diğer herkesin erişiminden korunmasını ifade eder. Aslında mahremiyet kişinin kendisine ait bilgiler için korunaklı anlan yaratması anlamına gelirken gizlilik ise kişinin kendisine ait bilgilerden oluşturduğu korunaklı alanın korunması anlamına gelir.

Bu bağlamda, gizlilik, mahremiyetin korunmasını sağlayan temel bir mekanizma olarak bireyin kişisel verilerini yetkisiz erişim ve dış müdahalelere karşı korumayı amaçlar (147). Ancak büyük veri çağında, mahremiyet ve gizlilik arasındaki sınır giderek belirsizleşmekte, hatta bu kavramlar geleneksel anlamlarını yitirmeye başlamaktadır. Büyük veri teknolojileri geleneksel anlamların ötesine geçerek, etik ilkelerin yeniden ele alınmasını ve yeni sınırların çizilmesini zorunlu kılmaktadır (148). Bu sınırların çizilmesinin en elzem yanı sağlık verileridir. Çünkü sağlık verileri, teşhis ve tedavi süreçlerinin geliştirilmesi açısından büyük bir potansiyel taşısa da, içerdiği kişisel ve hassas bilgiler nedeniyle mahremiyetin korunması açısından ciddi riskler barındırmaktadır. Bu veriler yalnızca bireyin sağlık durumunu değil, geçmişini,

genetik özelliklerini ve yaşam tarzını da içermekte, dolayısıyla bireysel mahremiyetin ötesinde ailesel ve toplumsal mahremiyet boyutlarını da gündeme getirmektedir (149).

Sağlık alanındaki verilerin korunmasının ve gizliliğin sağlanmasının ne kadar önemli olduğu ortadadır. Ama bahsedilen mahremiyet ve gizlilik sadece sağlık çalışanların sorumluluğuna değildir. Çünkü sağlık verilerinin dijitalleşmesi, bu bilgilerin yalnızca hasta ve hekim arasında paylaşılan bir sır olmaktan çıkarıp, çeşitli platformlar ve teknolojik araçlar aracılığıyla geniş çapta işlenmesine yol açmıştır. Bilindiği gibi günümüzde sağlık verisi sadece klinik ortamda değil, akıllı telefonlar, giyilebilir cihazlar ve diğer dijital sağlık sistemleri aracılığıyla da üretilmekte ve toplanmaktadır (150). Bu durum, mahremiyetin korunması sorumluluğunu yalnızca hekimlere değil, veriyi toplayan, işleyen ve saklayan tüm paydaşlara yüklemektedir.

Mahremiyetin korunmasına yönelik yaygın stratejilerden biri olan anonimleştirme, büyük veri çağında etkinliğini yitirmektedir (151). Anonimleştirme, bireyin kimlik bilgilerinin çıkarılmasıyla verilerin kimden geldiğinin gizlenmesini amaçlasa da büyük veri analitiği teknikleri sayesinde anonimleştirilmiş verilerin yeniden bireyle ilişkilendirilebilmesi mümkündür (150). Büyük veri tabanlarında veri çeşitliliği fazla olduğundan diğer verilerle ilişkilendirilerek bireyin kimliği ortaya çıkabilmektedir (152). Dolayısıyla, yalnızca anonimleştirme gibi geleneksel yöntemler yeterli olmayıp, çok katmanlı ve bütüncül bir veri güvenliği yaklaşımına ihtiyaç duyulmaktadır.

Mahremiyet genellikle yasalarla korunmaya çalışılsa da pratikte bu koruma ne yazık ki her zaman sağlanamıyor. Örneğin, Türk hukuk sisteminde verilerin korunmasına yönelik oluşturulan “Kişisel Verilerin Korunması Kanunu” (KVKK), bireylerin özel bilgilerini güvence altına almayı amaçlıyor. Ancak özellikle sağlık, güvenlik veya pazarlama gibi alanlarda, bireyden açık rıza alınmadan veri işlenmesi hâlâ yaygın. Bu da kişilerin özel yaşam hakkını zedeleyerek mahremiyetin ihlaline yol açıyor. Yani yasal çerçeve olsa da uygulama hem eksik kalıyor hem de etik ilkelere tam olarak dayanmıyor.

Bir örnek olarak, COVID-19 pandemisi sürecinde Hayat Eve Sığar (HES) uygulaması üzerinden kullanıcıların konum verileri, temaslı bilgileri ve sağlık

durumları gibi son derece hassas veriler toplanmış ve çeşitli kurumlarla paylaşılmıştır. Her ne kadar bu süreç yasal bir dayanağa oturtulmuş olsa da, verilerin kimlerle, hangi koşullarda ve ne kadar süreyle paylaşıldığına dair belirsizlikler etik bir sorun yaratmış; bireylerin rızasının yeterince açık ve bilgilendirilmiş olup olmadığı tartışmalı hale gelmiştir (153).

Tüm bu gelişmeler ışığında, sağlık verilerinin korunması ve mahremiyetin ihlal edilmemesi kritik bir etik sorumluluk olarak karşımıza çıkmaktadır. Bu sorumluluk yalnızca hekimlere değil; verileri toplayan, işleyen ve saklayan sağlık kurumlarına, kuruluşlara ve devletlere aittir. Ancak büyük sağlık verilerinin çoğunlukla merkezi veri tabanlarında depolanması, mahremiyetle ilgili endişelerin daha da belirginleşmesine neden olmaktadır. Zira bireyler, bu verilerin kimler tarafından işlendiği, hangi güvenlik önlemlerinin alındığı ve verilerin gerçekten ne ölçüde korunduğu konusunda yeterli bilgiye sahip değildir. Bu durum, mahremiyetin korunmasına yönelik güvenin zedelenmesine yol açmaktadır. Öte yandan, verilerin merkezi bir sistemde tutulması, bu sistemin tek bir hata veya saldırı noktasına karşı savunmasız hale gelmesi anlamına gelmektedir. Böylece, merkezi yapı nedeniyle oluşabilecek bir güvenlik açığı, milyonlarca kişinin sağlık verisinin aynı anda mahremiyet ihlaliyle karşı karşıya kalmasına neden olabilir. Son derece hassas olan ve mahremiyetin önemli olduğu sağlık verilerinde bu gibi sistemler karşılaşılan etik sorunların merkezinde yer almakta ve sağlık verilerinin hangi amaçlarla toplandığı, kimlerle paylaşıldığı ve nasıl korunduğu konularında yeterli şeffaflık sağlanmadığında, mahremiyet ihlallerini kaçınılmaz hale getirmektedir.

3.1.3 Şeffaflık

Şeffaflık, modern toplumlarda bilgiye erişim hakkı, yönetişim kalitesi ve etik sorumluluk gibi değerlerle iç içe geçmiş, çok boyutlu bir ilkedir. Temelinde, bireylerin ve toplumların kendilerini etkileyen karar süreçlerine dair bilgi sahibi olabilmeleri ve bu süreçleri sorgulayabilmeleri fikri yatar. Şeffaflık, sadece bilgi sunmak değil; bilginin erişilebilir, anlaşılır ve denetlenebilir olması anlamına gelir (154). Bu yönüyle şeffaflık, açıklık ve hesap verebilirlik ile olduğu kadar, bireysel haklar, güvenlik ve mahremiyetle de sürekli bir gerilim ilişkisi içerisindedir. Bu karmaşık yapısı

nedeniyle, şeffaflık yalnızca normatif bir değer değil; aynı zamanda pratikte yeniden tanımlanan ve bağlama göre şekillenen dinamik bir kavramdır (155).

Şeffaflık kavramı genellikle yolsuzluğa karşı bir kamu değeri olarak ele alınır ve bu bağlamda hesap verebilirlik ile yakından ilişkilidir. Şeffaflık, hükümetler ve kâr amacı gütmeyen kuruluşların açık karar alma süreçlerini benimsemesiyle eş anlamlı hale gelmiştir. Bu süreçler, bilgilerin kolay erişilebilir olmasını ve kamuoyunun denetimine açık bir karar mekanizmasının oluşturulmasını ifade eder (156, 157).

Jean Baudrillard, şeffaflığı "erişilebilirlik ve berraklığın bir gösterisi" olarak tanımlamış ve bu durumu modern toplumun yarattığı bir yanılsama olarak değerlendirmiştir (158). Ona göre, şeffaflık, her şeyin görünür kılınarak açık bir biçimde sunulmasını ifade eder. Ancak Baudrillard, modern dönemde şeffaflığın yalnızca bilgilendirme amacı taşımaktan öte, bir kontrol mekanizması ve otorite aracı haline geldiğini vurgular (159). Bu bağlamda, şeffaflık, hem bir açıklık idealini temsil ederken hem de iktidarın gizli bir biçimde güç ve otoriteyi pekiştirdiği bir araç olarak işlev görmektedir (157, 160). Örneğin, devletlerin güvenlik gerekçesiyle bireylerin kişisel verilerini toplaması ve takip politikaları uygulaması, özel yaşam alanlarını daraltarak şeffaflık ve mahremiyet arasında bir çatışma yaratabilir. Bu sebeple gerek kamu gerekse özel sektör, bireylerin güvenini koruyacak ve bilgi akışını dengeleyerek hak ihlallerinin önüne geçecek politikalar geliştirmekle yükümlüdür.

Büyük sağlık verisinin toplama, işleme ve depolama aşamaları, bireylerin mahremiyetine ve etik değerlere yönelik ciddi sorular doğururken, en temel sorunlardan biri olarak şeffaflık eksikliği öne çıkmaktadır. Sağlık verileri genellikle elektronik sağlık kayıtları, mobil uygulamalar, genomik taramalar ve giyilebilir cihazlardan elde edilmekte, bu verilerin toplanma ve işlenme süreçleri ise bireylerin bilgisi dışında gelişmektedir. Özellikle yapay zekâ ve makine öğrenimi gibi karmaşık algoritmaların kullanıldığı analiz süreçlerinin "kara kutu" işleyişine sahip olması (161), veri işleme süreçlerine dair bilgiye erişimi zorlaştırmakta ve hesap verebilirlik mekanizmalarını zayıflatmaktadır (143)

Tez kapsamında ele alınan büyük sağlık verisi ve beraberinde getirdiği etik sorunların temeli merkeziyetçi veri yönetimi modelinin oluşu, veri ekosistemindeki

şeffaflık sorununu daha da derinleştirmektedir. Verilerin tek merkezde toplanması, bireylerin verilerinin kimler tarafından ve hangi amaçlarla kullanıldığını bilmesini zorlaştırmakta; bu durum da bilgi asimetrisine ve veri sahipliğinin ihlaline yol açarak veri sürecine dair şeffaflık problemini oluşturmaktadır. Toplanan sağlık verilerinin hangi amaçla kullanıldığı, gizliliğin nasıl sağlandığı, veriye dayalı süreçlerin nasıl ilerlediği soruların sorulması bile sürecin yeterince şeffaf olmadığı ve bunun da bir etik problem olduğunu göstermektedir. Oysa şeffaflık, sadece veriye erişim değil, aynı zamanda verinin kullanım amaçlarının açıkça belirtilmesini ve bu süreçlerde bireylerin etkin şekilde bilgilendirilmesini de kapsar. Mevcut sistemde bu şeffaflık düzeyi sağlanmadığından, bireylerin veri üzerindeki kontrolü ciddi biçimde kısıtlanmakta ve etik açıdan sorumluluğu belirsiz, güvensizlik üreten bir yapı ortaya çıkmaktadır.

3.1.4 Yarar ve zarar

Biyoetikte temel ilkeden biri olan yarar sağlama (beneficence) ve onunla birlikte anılan zarar vermeme (non-maleficence) ilkesi, özellikle sağlık alanındaki uygulamalarda yol gösterici bir etik ölçüttür. Bu ilke, bireyin yaşam kalitesini artırmayı, sağlık hizmetinden olumlu sonuçlarla faydalanmasını sağlamayı ve aynı zamanda bu süreçte ona zarar verebilecek müdahalelerden kaçınmayı gerektirir. Beauchamp ve Childress'in ilkeler etiği yaklaşımı, bu iki ilkeyi ayrı ayrı tanımlar ancak pratikte çoğunlukla birlikte ele alır (109). Çünkü bireye yarar sağlama iddiası taşıyan her eylem, aynı zamanda ona zarar vermeme yükümlülüğü içerir. Bu ilke, sadece klinik karar alma süreçlerinde değil; araştırma etiği, halk sağlığı uygulamaları ve sağlık sistemleri düzeyinde de yönlendiricidir.

Yarar sağlama ve zarar vermeme ilkeleri, büyük sağlık verisinin işlenmesi ve kullanımı bağlamında yeniden düşünülmesi gerekir. Çünkü konu büyük veri olduğunda bu ilkeler yalnızca bireyin çıkarını gözetmeyi değil, aynı zamanda toplumsal yararı öncelemeyi ve potansiyel zararları önlemeyi de içerir. Ancak büyük sağlık verisinin geniş ölçekli, sürekli ve çoğu zaman otomatik olarak toplanan yapısı, bu ilkenin uygulanmasını belirli etik açmazlarla karşı karşıya bırakmaktadır.

Sağlık alanında büyük veri kişileştirilmiş tıptan halk sağlığına kadar uzanan çok yönlü fayda sağlar. Bu devasa veri bir yandan bireye ve topluma fayda sağlarken diğer

yandan bazı insan haklarının ihlal edilmesi, mahremiyet ve gizlilik gibi sorunların oluşumuna zemin hazırlayabilmektedir. Bu verilerin çoğunlukla bireylerin açık rızası alınmaksızın, ikincil amaçlarla veya ticari çıkarlar doğrultusunda kullanılması, bireylerin zarar görme riskini artırmaktadır (162). Zarar yalnızca fiziksel düzeyde değil; mahremiyet ihlalleri, damgalama, veri ayrımcılığı ya da yanlış algoritmik kararlar gibi sosyal ve psikolojik düzeylerde de ortaya çıkabilmektedir (140). Örneğin, sağlık verilerinin güvenliğinin sağlanamaması, bireylerin bilgileri dışında üçüncü taraflarla paylaşılması ya da siber saldırılar sonucu açığa çıkması da ciddi zarar potansiyelleri doğurur. Bu nedenle yalnızca potansiyel yarara odaklanmak, etik açıdan yetersiz bir yaklaşım olabilir.

Yarar-zarar ilkesinin bu bağlamda uygulanabilir hale gelmesi, ancak kapsamlı bir risk-fayda değerlendirmesi, veri minimizasyonu ilkesi, açık rıza süreçlerinin güçlendirilmesi ve anonimleştirme gibi zarar önleyici tekniklerin uygulanması ile mümkündür (17). Büyük sağlık verisinin etik yönetimi, yalnızca sağlık sistemine sağlayacağı yarar üzerinden değil, bireyin zarar görme olasılığı üzerinden de dikkatle ele alınmalıdır. Etik açıdan meşru bir veri kullanımı, bireylerin temel hak ve özgürlüklerini gözetirken aynı zamanda toplumsal faydayı da adil biçimde gözeten bir yapı gerektirir.

3.1.5 Veri güvenliği ve ihlaller

Kişisel sağlık verilerinin dijital ortama aktarılmasıyla sağlık alanındaki gelişmeler hızlanmış, sağlık çalışanlarının iş yükü azalmıştır. Yaşamımızın giderek veri dünyasına dönüşmesi, refah seviyemizi artırmış; özellikle sağlık alanında geçmişe kıyasla önemli faydalar sağlamıştır. Ancak verilerin artık fiziksel arşivlerde değil de dijital platformlarda ve çoğunlukla merkezi sistemlerde depolanması, üçüncü tarafların bu verilere erişimini kolaylaştırmıştır. Bu durum, verilerin güvenliğini tehdit etmiş ve ihlallere zemin hazırlamıştır.

Veri güvenliği, temelde verilerin depolandığı ve işlendiği yerlerde alınan önlemleri kapsar. Veri güvenliği de bireyin haklarıyla doğrudan ilişkili olup, özellikle verilerin depolayıcı ve işleyici taraflarının ihmallerinden kaynaklanan etik sorunlara işaret eder. Devletler, şirketler ve veri toplayıcılar, bireylerin haklarını korumakla

yükümlüdür. Ancak, bu sorumluluklar ihmal edildiğinde veri ihlalleri kaçınılmaz hale gelir.

Veri güvenliği ihlallerinin, sadece bireysel ya da kurumsal sorumluluklar ve hatalarla sınırlı kalmayıp, aynı zamanda verilerin nasıl toplandığı, saklandığı ve işlendiği yapılarla da doğrudan ilişkilidir. Bu bağlamda, özellikle sağlık alanında giderek daha yaygın biçimde kullanılan büyük veri sistemleri, veri güvenliği tartışmalarında merkezi bir konuma yerleşmiştir.

Büyük verinin sağlık sektöründe artan kullanımı, beraberinde ciddi yönetimsel ve etik sorunları da getirmektedir. Özellikle verinin hacmi büyüdükçe, güvenlik yönetimi daha karmaşık bir hâl almakta; milyonlarca hasta kaydının işlendiği sistemlerde veri kaybı, sızıntı ve ihlal risklerini kontrol etmek giderek zorlaşmaktadır (163). Bu artan hacim, yalnızca teknik zorlukları artırmakla kalmamakta, aynı zamanda bu verileri saldırganlar açısından daha cazip hâle getirmektedir. Sağlık sektörü, içerdiği hassas ve yüksek değerli bilgiler nedeniyle giderek daha fazla siber saldırının hedefi olmaktadır (164). Hastaların tıbbi geçmişleri, tanı bilgileri veya sigorta detayları gibi kişisel veriler, karaborsada yüksek meblağlarla el değiştirebildiği için, organize suç grupları ve bireysel saldırganlar açısından önemli bir motivasyon kaynağı oluşturur (165). Bu durum, bireysel kurumların ötesinde, tüm sağlık sistemlerinin güvenliğini tehdit edebilecek boyutlara ulaşabilmektedir.

Veri güvenliği ve ihlalleri, birçok farklı nedenden dolayı yaşanabilmektedir. Bu nedenlerden ilki teknolojik güvenlik açıklarıdır. Modern tehditlere karşı alınan teknolojik önlemler zaman zaman yetersiz kalabilmektedir. Eski yazılımlar, yeni nesil tehditleri algılayamamakta ve bu durum güvenlik açıklarına neden olmaktadır. Örneğin, 10 yıl önce etkili olan bir güvenlik protokolü, günümüzde teknolojinin hızla ilerlemesi sayesinde saldırganlar için kolay aşılabilir hale gelebilmektedir. Özellikle sağlık sektöründe kullanılan tıbbi cihazların eski sistemlerle çalışması, bu cihazları güncellemenin zor ve maliyetli olması nedeniyle riskleri artırmaktadır (166). Bu açıklar, saldırganlar için kolay erişim yolları oluşturur. Örneğin, WannaCry fidye yazılımı saldırısı, 2017 yılında İngiltere'nin Ulusal Sağlık Servisi'ni (National Health Service-NHS) hedef alarak hasta kayıtlarına erişimi engellemiş ve sağlık hizmetlerini aksatmıştır. Bu saldırının temel nedeni, sistemlerde eski Windows sürümlerinin

kullanılması ve gerekli güvenlik yamalarının yüklenmemiş olmasıdır. WannaCry, sistemlerdeki bir güvenlik açığını kullanarak hızla yayılmış ve birçok kurumun operasyonlarını sekteye uğratmıştır. NHS özelinde, acil durum hizmetlerinde ciddi aksaklıklar yaşanmış, hasta güvenliği riske atılmıştır. Bu olay, sağlık hizmetlerinde kullanılan teknolojik altyapının güncellenmesi ve güvenliğin artırılması gerekliliğini ortaya koyan çarpıcı bir örnek olarak dikkat çekmektedir. Bu olay, sağlık sektöründe veri güvenliği ihlallerinin ciddi sonuçlara yol açabileceğini göstermektedir (167).

Veri güvenliliği ve ihlalini diğer bir nedeni insan faktörüdür. Veri güvenliği açısından en zayıf halkalardan biri insan hatasıdır. Dikkatsizlik veya bilgi eksikliği, ciddi güvenlik ihlallerine yol açmaktadır. Örneğin, bir sağlık çalışanının yanlış bir bağlantıya tıklaması, tüm sistemin etkilenmesine neden olabilmektedir. Ayrıca, çalışanlar bilerek veya bilmeyerek hassas bilgileri sızdırabilme potansiyeline sahiptir. İnsan faktörü, teknolojiyle birleştiğinde güvenlik zincirini kıran temel unsurlardan biri haline gelir (164). 2018 yılında gerçekleşen SingHealth veri ihlali, Singapur'un en büyük sağlık kuruluşunun sistemlerini hedef almış ve 1,5 milyon hastanın bilgilerinin çalınmasıyla sonuçlanmıştır. Bu bilgiler arasında Singapur Başbakanı Lee Hsien Loong'un tıbbi kayıtları da yer almıştır. İhlalin temel nedenleri arasında çalışanların siber güvenlik farkındalığının düşük olması ve sistemlere yönelik düzenli güvenlik testlerinin yapılmaması öne çıkmıştır. Olay, SingHealth'in güvenlik açıklarını gidermek ve benzer durumları önlemek amacıyla kapsamlı reformlar başlatmasına yol açmıştır (168).

2025 yılı itibarıyla, Türkiye'de sağlık verilerine izinsiz erişimle ilgili kayda değer bir iddia gündeme gelmiştir. Journal 140 adlı YouTube kanalında yayımlanan bir videoda, 16 yaşındaki bir çocuğun Türkiye'deki sağlık verilerine nasıl izinsiz erişebildiği açıklanmaktadır. Video, pandemi döneminde ortaya çıkan ve bugüne kadar kamuoyuna duyurulmayan bir veri ihlalini gündeme getirmektedir. Olay, pandemi nedeniyle halkın evde daha fazla vakit geçirmesiyle başlar. Bu dönemde gençler, bilgisayar ve internet kullanımına daha fazla yönelirler. Çocuklar, sağlık uygulamalarına (MHRS, e-Nabız, HSYS) girerek sistemdeki açıkları tespit ederler ve birkaç saat içinde bu uygulamalardan milyonlarca sağlık verisini çekerler (169).

Sadece oyun oynayarak ve sistemleri kurcalayarak, hızla erişim sağladıkları bu veriler, güvenlik açıklarının ne kadar ciddi olduğunu gözler önüne sermektedir.

Veri ihlallerinin temelinde yatan başlıca nedenlerden biri, verilerin merkezi yapılarda toplu şekilde depolanmasıdır. Bu tür yapılar, veri ihlali gerçekleştiğinde etkisinin büyük olmasına yol açmaktadır. Veriler tek bir merkezde toplandığında, ihlalin nedeni ister siber saldırı ister yazılım hatası, isterse insan kaynaklı bir hata olsun, bu durum mahremiyetin ciddi biçimde ihlal edilmesine ve veri güvenliğinin ortadan kalkmasına neden olabilir. Özellikle günümüzde teknolojinin hızlı gelişimine rağmen, hâlâ eski yapılı ve merkeziyetçi sistemlerin tercih edilmesi, bu sistemleri kötü niyetli aktörler için daha cazip hedefler haline getirmektedir (170).

Bu noktada önemli bir soru gündeme gelmektedir: Eğer söz konusu veri ihlallerinde, veriler merkezi yapılar yerine merkezi olmayan/merkeziyetsiz/dağıtık (decentralized) ve mahremiyet ile güvenlik açısından daha gelişmiş teknolojilerle yönetilseydi, bu ihlaller yine aynı şekilde yaşanır mıydı? Ya da yaşansaydı, etkisi bu denli büyük olur muydu? Dağıtık sistemler, verilerin farklı noktalarda şifreli ve kontrollü biçimde tutulmasına olanak tanıyarak, bir noktadaki ihlalin tüm sistemi etkilemesini engelleyebilir. Bu tür sistemler, "tek hata noktası" (single point of failure) riskini ortadan kaldırarak genel güvenliği artırır (171).

Özellikle sağlık sistemlerinde kullanılan yazılım altyapılarının, veri depolama çözümlerinin ve güvenlik protokollerinin mahremiyet ve bütünlük açısından yeterince güçlü olmaması, veri ihlallerine zemin hazırlamaktadır. Merkezi yapıların sürdürülmesi hem teknolojik gelişmelere aykırı bir durumu yansıtmakta hem de etik açıdan sürdürülemez bir veri yönetimi anlayışını beslemektedir. Gelişen dağıtık teknolojilerin (örneğin blockchain tabanlı çözümler, IPFS, homomorfik şifreleme gibi) daha etkin şekilde kullanılması, bu tür ihlallerin hem önlenmesine katkı sağlayabilir hem de gerçekleşmesi durumunda etkisini sınırlayabilir.

3.1.6 Veri paylaşımı ve ikincil kullanım

Veri paylaşımı, aynı veri kaynaklarının birden fazla uygulama, kullanıcı veya kuruluş tarafından kullanılabilir hale getirilmesi sürecidir. Sağlık verilerinin

büyüklüğü ve bu verilerin sağladığı potansiyel fayda düşünüldüğünde, veri paylaşımı kritik bir öneme sahiptir. Hem bireysel sağlık hem de kamu yararı için veri paylaşımı vazgeçilmezdir. Bunun yanı sıra, dünya çapında ve uluslararası düzeyde veri paylaşımı, özellikle salgın hastalıklar gibi küresel tehditlerde durumu daha iyi anlamamıza ve hızlı çözümler geliştirmemize olanak tanır (25).

Veri paylaşımı, pek çok araştırma alanında köklü bir geçmişe sahiptir. Sosyal ve biyolojik bilimlerde araştırma bulgularını paylaşma ve disiplinler arası iş birliği oluşturma çabaları nispeten yeni bir yaklaşım olsa da diğer bazı alanlarda veri paylaşımı uzun süredir standart bir uygulama halindedir. Özellikle ekonomi ve meteoroloji gibi alanlar, uzun zamandır kamuya açık veriler üzerinden ilerlemektedir. Veri paylaşımının, bilimsel ilerlemeyi hızlandırma ve gelecekteki araştırmacılara önemli bir kaynak sağlama potansiyeline sahip olduğu vurgulanmıştır. Veri paylaşımının, gelecek nesil bilim insanları için önemli bir kaynak oluşturacağına dair güçlü bir görüş bulunmaktadır. Bununla birlikte, bilimsel topluluk içinde -özellikle belirli disiplinlerde- veri paylaşımı konusunda çekincelerin varlığını sürdürdüğü de göz ardı edilemez (172).

Veri paylaşımı, araştırmalarda önemli bir avantaj sunmaktadır. Büyük veya toplanması maliyetli veri setlerini herkesin erişimine açarak, bireysel araştırmacıların daha geniş bir etki yaratmasına olanak tanır. Bu yaklaşım, beklenmedik araştırma yollarının açılmasını sağlar. Üstelik bu durum yalnızca büyük ölçekli veri paylaşımı projeleri için geçerli değildir; nispeten küçük veri setleri bile paylaşıldığında, büyük veriye anlamlı katkılar sunabilir ve gelecekteki bilimsel keşifleri tahmin edilemeyecek şekillerde destekleyebilir. Örneğin, tıp alanında yapılan hasta düzeyindeki meta-analizler, geçmiş klinik çalışmaların verilerini kullanarak, bu çalışmaların orijinal amaçlarının ötesine geçen çok sayıda yeni bulgu ortaya koymuştur (173).

Bu bağlamda, veri paylaşımı yalnızca günümüzde bilimin tekrarlanabilirliğini ve güvenilirliğini artıran bir araç değil, aynı zamanda yarının bilimini şekillendiren bir itici güçtür. Bir veri setinin gelecekte ne kadar değerli olacağını önceden tahmin edemediğimiz düşünüldüğünde, veriyi paylaşmamanın gelecekteki bilim insanlarının önünde ciddi bir engel oluşturabileceği savunulabilir.

Veri paylaşımının araştırmacıların yürütebildiği çalışma türlerini dönüştürmesi birçok alanda faydalıdır. Örneğin; genetikte, klinikte, biyomedikal alanda ve yapısal biyolojide büyük paylaşımlı veri kümeleri yaygındır ve birçok araştırmacı bu alanlarda yeni keşifler yapmak için daha önce yayınlanmış veri kümelerini yeni olanaklar ve faydalar için kullanmıştır (172).

Büyük sağlık verilerinin paylaşılması ve ikincil kullanımı, sağlık hizmetlerini iyileştirme fırsatları sunarken, aynı zamanda birçok etik sorunu da beraberinde getirmektedir. Bu verilerin, bireylerin sağlık hizmetlerinden daha verimli yararlanmasını sağlama potansiyeli ile, kişilerin kendi verilerini kontrol etme hakkı arasında giderek derinleşen bir çelişki bulunmaktadır (174). Sağlık verileri, kişisel ve hassas bilgiler içerdiği için, bu verilerin gizliliği ve güvenliği, en kritik etik meselelerden biridir. Ancak, sağlık verilerinin paylaşımı için alınan onamların, gerçekten bilgilendirilmiş onam olup olmadığı sıkça sorgulanan bir konu olmuştur. Çoğu zaman, hastalar verilerinin araştırma ya da ticari amaçlarla nasıl kullanılacağı konusunda yeterince bilgi sahibi olmadan onay verirler. Bu da verilerin hastaların bilgisi dışında farklı amaçlarla kullanılmasına yol açabilmektedir. Ayrıca, sağlık verilerinin sahipliği konusunda yaşanan belirsizlikler, bu verilerin izinsiz olarak ticari kullanımlar için paylaşılmasına neden olabilmektedir (175).

Sağlık verilerinin teknoloji şirketleri ve ilaç firmaları tarafından, bireylerin açık onamı alınmadan ticari amaçlarla kullanılması ikincil kullanımın etik sorunlarını beraberinde getirmektedir. Özellikle, dijital sağlık uygulamaları ve giyilebilir cihazlar üzerinden toplanan sağlık verileri, kullanıcıların bilmediği şekilde satılması veya üçüncü taraflarla paylaşılması veri paylaşımı ve ikincil kullanımının etik sorunları arasında yer almaktadır. Örneğin, bir giyilebilir cihaz firması veya bir sağlık uygulaması, kullanıcıların sağlık verilerini toplamakta ve bu veriler yalnızca bireylerin kişisel sağlıklarını izlemek için kullanılacağını taahhüt etmektedir. Ancak şirket, kullanıcı onayı olmadan bu verileri büyük ilaç şirketlerine veya sigorta şirketlerine satabilme potansiyeline sahiptir (176). 2018'de, *Fitbit* gibi giyilebilir cihaz üreticilerinin, kullanıcılarının egzersiz verilerini ve kalp atış hızlarını, sağlık sigortası şirketleriyle paylaşarak, sigorta primi hesaplamalarında kullanabileceği iddiaları gündeme gelmiştir (177). Bu tür durumlar, sağlık verilerinin sahipliğinin ve

paylaşımının yeterince şeffaf olmaması nedeniyle etik sorunlara ve potansiyel kişisel mahremiyet ihlallerine yol açmaktadır.

Veri paylaşımının ve ikincil kullanımının, yalnızca gizlilik ve güvenlik endişeleriyle sınırlı kalmayıp, adalet ve eşitsizlik gibi önemli etik sorunları da gündeme getirdiği göz ardı edilmemelidir. Özellikle sağlık verilerinin ticari amaçlarla kullanılması, bazı toplulukları dezavantajlı duruma sokabilir ve bu durum, sağlık hizmetlerine erişimde eşitsizlik yaratabilir. Örneğin, kırsal bölgelerde yaşayan bireyler, şehir merkezlerine kıyasla daha az tıbbi teknolojiye erişime sahip olabilirler (178). Ancak, sağlık verileri genellikle daha gelişmiş şehir hastanelerinden toplanmaktadır. Bu durum, sağlık araştırmalarının ve tedavi yöntemlerinin sadece şehir merkezlerine yönelik olmasına ve dolayısıyla daha az gelişmiş bölgelerde sağlık hizmetlerine erişim konusunda eşitsizliklerin ortaya çıkmasına neden olabilir.

Benzer şekilde, düşük gelirli topluluklar, sağlık teknolojilerine ve giyilebilir cihazlara erişim konusunda engellerle karşılaşabilir. Bu topluluklar genellikle sağlık araştırmalarında daha az temsil edildiğinden, araştırmalardan elde edilen veriler çoğunlukla varlıklı ve şehirli bireylerin sağlık durumlarına odaklanır (179-181). Bu tür eşitsizlikler, sadece sağlık hizmetleri üzerinde değil, aynı zamanda araştırma sonuçları ve sağlık politikaları üzerinde de kalıcı etkiler yaratabilir. Bu yüzden, sağlık verisi paylaşımı ve ikincil kullanımı, adalet ve eşitlik ilkelerine dayalı olarak dikkatle düzenlenmelidir (176, 178).

3.1.7 Adalet ve eşitsizlikler

Varolmanın ve düşünmenin değerli kavramları adalet ve eşitsizlik birey ve toplum için vazgeçilemez kadim değerlerdir. Bundan yaklaşık 2400 yıl önce Aristoteles adalet ve eşitlik kavramı üzerinde düşünmüş, varlık için kavramın ne olduğunu açıklama girişiminde bulunmuştur. Adalet üzerine düşünen Aristoteles, 'eşit olmayanlara eşit davranmak adil değildir' diyerek adalet ve eşitlik kavramlarını toplumsal ve bireysel boyutlarını ele almış ve bu kavramların insan hayatında düzenleyici rolünü irdelemiştir (88). Bugün ise bu kadim kavramlar, büyük sağlık verisi çağında yeni bir boyut kazanmaktadır. Peki, büyük sağlık verisi, toplumsal eşitsizliklere rağmen herkes için adil bir sağlık sistemi yaratabilir mi?

Gelişmiş teknoloji ve bilgisayar sistemlerinin olmadığı bir dönemde, bireylerin ve toplumların günlük yaşamlarıyla ilgili bilgilere ulaşmak oldukça sınırlıydı. O dönemlerde sosyal bilimciler ve araştırmacılar, toplumların alışkanlıklarını ve ihtiyaçlarını daha iyi anlayabilmek için uzun soluklu ve kapsamlı saha çalışmaları yürütmek zorundaydılar. Günlük yaşam pratiklerini ve sosyal dinamikleri anlamak için aylar, hatta yıllar süren gözlemler, mülakatlar ve etnografik araştırmalar gerçekleştirilmekteydi. Bu süreçler, veri toplama ve analizinde günümüz teknolojik araçlarının sağladığı hız ve kolaylıktan yoksundu. Bu nedenle, o dönem yapılan çalışmalar, modern sosyal bilim yöntemleriyle kıyaslandığında daha fazla zaman ve emek gerektiren, ancak aynı zamanda daha sınırlı bir veri kapsamına sahip olan araştırmalar olarak değerlendirilebilir.

Büyük veri sayesinde toplumun bütün bireylerinin ayrı ayrı her türlü bilgisine erişmek oldukça kolay bir hal almıştır. Günümüzde artık her türlü veriye kolayca erişilebiliyor, dünyada saniyede toplanan veriler giderek artıyor ve büyük veri halini alıyor. Büyük veri her türlü endüstri ve organizasyon tarafından işletmeleri, kültürleri ve toplulukları şekillendirmek için kullanılabiliyor (182). Sağlık alanında da kullanılan büyük veri karşımıza bir dizi etik problemle çıkıyor. Sağlıkta büyük veri konseptiyle ele aldığımız bu alan kendi bünyesinde adalet ve eşitsizlik gibi sorunların önünü açabilirken, var olan bu sorunları daha da derinleştirme potansiyeline sahiptir.

Büyük sağlık verisi, sağlık hizmetlerini daha erişilebilir, daha hızlı ve daha doğru hale getirme potansiyeline sahip görülmektedir. Ancak, bu veriler aynı zamanda derinleşen bir eşitsizliğin aracı da olabiliyor (183). Örneğin, gelişmiş ülkelerdeki hastaneler, yapay zeka destekli analizlerle kanser teşhisini erken evrede koyabilirken, veri altyapısı olmayan düşük gelirli ülkelerde hastalar bu tür olanaklara erişim sağlayamıyor. Benzer şekilde, bireyler arasında da dijital uçurum derinleşmektedir (184).

Sağlık alanında adalet ilkesi, yalnızca herkesin eşit biçimde hizmet almasını değil, aynı zamanda ihtiyacı olanların önceliklendirilmesini de gerektirir. Ancak büyük sağlık verisinin hâkim olduğu günümüzde bu ilkenin uygulanabilirliği giderek daha karmaşık hâle gelmektedir. Zira dijitalleşme, yeni türden eşitsizlikleri de beraberinde

getirmiştir (185). Artık yalnızca gelir ya da coğrafi farklılıklar değil, veriye erişim ve veriden elde edilen faydaya katılım da sağlık alanındaki adaletin yeni problem alanlarındandır.

Kişisel verilerimiz, neredeyse her dijital etkileşimde sistematik olarak toplanıyor ve çok çeşitli alanlarda -ilaç geliştirme, yapay zekâ uygulamaları, pazarlama stratejileri- işlenerek yüksek ekonomik ve bilimsel çıktılara dönüştürülüyor (28). Ancak burada kritik bir sorun var: Bu verilerden doğan fayda kiminle paylaşılıyor?

Bireylerin genetik ya da sağlık verilerinden elde edilen bulgular, çoğu zaman büyük şirketlerin ya da merkezi kurumların tekelinde kalıyor. Bu durum, literatürde "yararın adil paylaşımı" (equitable sharing of benefit) ilkesi bağlamında ciddi bir etik problem olarak ele alınmaktadır (186, 187). Yani veri sahipleri, aslında kendilerine ait olan verilerden üretilen faydanın dışında bırakılmakta; şeffaflık ve adalet ilkeleri zedelenmektedir.

Bu tablo, nadir hastalıklar için geliştirilen ve "yetim ilaçlar" (orphan drugs) olarak adlandırılan ilaçlarda somut olarak karşımıza çıkıyor. Bu ilaçların büyük kısmı, küçük hasta gruplarından toplanan genetik ve klinik veriler üzerinden geliştiriliyor. Ancak geliştirme sürecinde katkısı olan bu bireyler, söz konusu ilaçlara ya yüksek fiyatlar nedeniyle erişemiyor ya da tamamen dışlanıyor (188). Veri onlardan, buluş onlardan; ama ortaya çıkan fayda? Yalnızca ticari bir varlık. Bu durum yalnızca ekonomik bir eşitsizlik değil; aynı zamanda özel yaşam hakkı, mahremiyet hakkı ve veri üzerinde tasarruf hakkı gibi temel insan haklarının da ihlali anlamına gelmektedir (187)

Dolayısıyla günümüzde verilerin korunması kadar, **v**erilerden doğan faydanın kiminle ve nasıl paylaşıldığı da temel bir etik mesele olarak tartışılmalıdır. Aksi hâlde birey, dijital ekosistemin yalnızca pasif bir "ham madde sağlayıcısı" haline gelecek; veri adaleti (data justice) hiçbir zaman tesis edilemeyecektir (189).

Veriye erişimin sınırlı olduğu bir düzlemde, bu veriler üzerinden yürütülen analizlerin ve geliştirilen sağlık politikalarının tüm toplumsal gruplar için adil sonuçlar üretmesi beklenemez. Bu durum, özellikle veri temelli yararın adil paylaşımı (data benefit-sharing) sorununu gündeme getirir. Nitekim, sosyoekonomik açıdan

dezavantajlı gruplara ait sağlık verileri araştırmalarda sıklıkla kullanılmakta; ancak bu araştırmalardan elde edilen çıktılar, çoğu zaman söz konusu toplulukların doğrudan yararına sunulmamaktadır. Bu durum yararın dağılımında adaletsizlik yaratmaktadır (190).

Büyük verinin getirebileceği diğer bir adalet ve eşitsizlik problemi, toplanan verilerin yanlılığıdır. Büyük veri kullanımının bireyler ve toplumlar arasında adaletsizlik yaratma riski büyük verinin sorunları arasında yerini alıyor. Büyük sağlık verisinin toplanması ve analizi genellikle teknolojik altyapıya erişimi olan, daha güçlü kaynaklara sahip bölgeler ve kuruluşlar tarafından gerçekleştirilir (178). Bu durum, dijital uçurumu derinleştirerek marjinalize edilmiş toplulukların yeterince temsil edilmediği veya göz ardı edildiği bir sistem ortaya çıkarmaktadır. Özellikle kendi kendine raporlanan veriler de, veri yanlılığı çok daha fazla gözlemlenmektedir (182). Kendi kendine raporlanan veriler, bireylerin kendi sağlık durumlarını, davranışlarını, sağlık hizmetlerini kullanma şekillerini veya diğer sağlıkla ilgili bilgileri doğrudan raporladığı verilerdir. Bu tür veriler genellikle anketler, sağlık izleme uygulamaları, çevrimiçi formlar veya bireylerin kendi sağlık kayıtlarını tuttuğu dijital platformlar aracılığıyla toplanır (191). Bu tür veriler, bireylerin sağlık durumları hakkında daha kişisel ve öznel bilgiler sunmasına olanak tanır. Ancak, bazı durumlarda kendi kendine raporlanan verilerde yanlılık (bias) ortaya çıkarabiliyor (184). Örneğin, yüksek gelirli bireyler daha fazla zaman ve kaynak ayırarak sağlık bilgilerini daha detaylı ve düzenli bir şekilde raporlayabilirken, düşük gelirli veya marjinalize edilmiş grupların bu tür raporlamalara katılımı sınırlı olabilmektedir. Bu da farklı gelir veya sosyal grup üyelerinin sağlık sorunlarının eşit düzeyde temsil edilmemesine neden oluyor (184).

Sağlık alanında büyük veri kullanımın diğer bir adalet ve eşitsizlik problemi olarak veri sahipleri ve veri toplayıcıları arasındaki güç asimetrisi olarak görünmektedir. Verilerin meta olarak kullanılması veri sahiplerini, veri üreticisi konumuna düşürerek kendi verileri hakkında herhangi bir hak talep edebilme durumunu ortadan kaldırmaktadır. Veri üzerinden veri sahiplerinden çok veri merkezlerini elinde barındıran teknoloji şirketi ve devletler, kurum veya kuruluş olarak görünebiliyor. Büyük sağlık verisinin genellikle daha fazla ekonomik ve politik güce sahip şirketler ve devletler tarafından kontrol edilmesi, verilerin ticari amaçlarla

kullanılmasına yol açabilir. Bu durum, sağlık hizmetlerinde bireysel hakların ve mahremiyetin ihlal edilmesine neden olurken veri sahipleri için metalaşmış veriden bir pay almayı da engelliyor (27). Bu durumda adalet ve eşitlik problemlerinin oluşumu, meta olarak kullanılan verilerde ücretlerin adaletli ve eşitlikçi bir biçimde dağılamamasından kaynaklanabiliyor. Meta olarak kullanılan verilerde veri toplayıcıları bireylerin verileri üzerinden para kazanabiliyorken veri sahipleri, veri üreticisi konumunda olup herhangi ücret alamıyor (192). Bireylerin kişisel bilgileri, büyük veri süreçlerinde metalaştırılarak ve özel alanlar ticarileştirilerek şirketler tarafından haksız kazanç elde edilebiliyor. Bireylerin ürettiği veriler, onların kontrolünden çıkarılarak**,** şirketler tarafından kâr amacıyla kullanılırken, bireylerin verileri üzerinde hak iddia etmesini zorlaştırarak ve mülksüzleşmeye yol açıyor (193).

Bu adaletsizlik sorunu sömürgecilik mantığıyla ilişkilendirilerek sorunun daha da derinleşmesine neden olabiliyor. Byung- Chul Han'ın "Enfokrasi" adlı kitabında teknolojik ilerlemenin günlük yaşantımızın kapitalizm mantığıyla sömürüldüğünü sistematik bir biçimde ele almaktadır (8). Özellikle verilerin, sanki bir sömürge toprağı gibi değerlendirildiği ve bu verilerden büyük şirketler tarafından haksız kazanç elde etmesi sorunu daha da tartışmaya açmaktadır.

Gelecekte yüksek ekonomik ve stratejik değere sahip olması beklenen büyük sağlık verilerinin, bireylerin mülkiyetinde değil de merkezi yapılarda toplanması ve kontrol edilmesi; veri sahipliğinin bireylerden uzaklaşarak belirli kurumlar veya platformlar etrafında tekelleşmesine yol açmaktadır. Bu durum, bireyin veri üzerindeki aktif rolünü zayıflatmakta ve onu edilgen bir konuma itmektedir.

3.1.7.1 Algoritmik önyargılar

Algoritmik önyargı, makine öğrenimi ve yapay zekâ sistemlerinin eğitim verilerindeki dengesizlikler veya modelleme süreçlerindeki önyargılar nedeniyle belirli gruplar aleyhine sistematik ayrımcılık yaratmasıdır (194). Bu durum, özellikle sağlık, işe alım, kredi değerlendirme ve yüz tanıma sistemleri gibi alanlarda ciddi etik sorunlara yol açmaktadır (195).

Büyük veri analizlerinde, belirli demografik grupların yeterince temsil edilmemesi ve geçmiş verilerin zaten var olan yapısal eşitsizlikleri yansıtması, algoritmik önyargıların oluşmasına zemin hazırlamaktadır. Bu durum, sağlık hizmetlerinde geliştirilen tanı ve tedavi yaklaşımlarının genellenebilirliğini sınırlamakta; dolayısıyla mevcut sağlık eşitsizliklerinin daha da derinleşmesine neden olabilmektedir (196).

Algoritmik önyargılar çeşitli faktörlerden oluşmaktadır. Bu faktörlerden ilki teknik önyargıdır. Algoritmayı oluşturmak için kullanılan eğitim, verilerin önyargılı olması durumunda ortaya çıkar. Yani algoritma için kullanılan veriler bir eşitsizlik durumunu teşkil ediyorsa algoritma da eşitsizlik içeren bir sonuç çıktısı çıkarır (197). Örneğin bir yüz tanıma algoritması ağırlıklı olarak beyaz yüzleri içeren bir veri kümesi üzerinden eğitilirse, yapay zeka da koyu tenli kişilerin yüzünü tanımakta zorluk çekecektir (198).

Algoritmik önyargıların oluşmasının ikinci faktörü ise tarihsel gelişim sürecinde oluşan önyargılardır. Makine öğrenimi algoritmaları eğitmek için genellikle geçmiş veriler kullanılmaktadır ve bu verilerde önceden varolan önyargıların bulunma potansiyeli mevcuttur. Örneğin 2023 yılında yapılan bir çalışmada (199), araştırmacılar kardiyovasküler hastalık riski, tedavisi ve sonuçlarındaki cinsiyet farklılıkları incelerken, geçmiş verilerde kadınların kardiyovasküler hastalık riskinin erkeklere kıyasla daha az vurgulanması nedeniyle, makine öğrenimi algoritmalarının algoritmik önyargı geliştirebileceğini ortaya koydu. Bu önyargı, kadınların riskinin daha düşük tahmin edilmesine ve dolayısıyla tedaviye erişimlerinin sınırlanmasına yol açabiliyor. Benzer bir sorun ise 2019 yılında yapılan bir çalışmada görüşmüştür. 2019 yılında yapılan bir araştırma, ABD'de sağlık hizmetlerinde kullanılan bir algoritmanın siyahi hastalara yeterli önemi vermediğini ortaya çıkarmıştır. Bu algoritma, hastaların gelecekteki sağlık ihtiyaçlarını tahmin etmek ve daha fazla tıbbi desteğe ihtiyaç duyan hastaları belirlemek için kullanılıyordu. Ancak, algoritma, geçmiş verilerde siyahi hastalara daha az sağlık harcaması yapıldığını gözlemlediği için, bu hastaları daha düşük riskli olarak sınıflandırmıştır (200). Bu durum, siyahi hastaların daha az tıbbi kaynağa erişimine yol açarak sağlık eşitsizliklerini arttırmıştır.

Tarihsel önyargı, teknik önyargı, toplumsal önyargı, otomasyon önyargı, -karar vericilerin, algoritma yanlış veya önyargılı sonuçlar üretmesine rağmen körü körüne algoritmaya güvenmesi durumunda ortaya çıkar- veri setlerinde cinsiyet ve ırk dengesizlikleri gibi birçok nedenden dolayı algoritmik önyargılar oluşmaktadır (201). Oluşan algoritmik önyargılar, sosyal eşitsizliğin devam etmesi ve toplumsal ilerlemenin engellenmesi gibi olumsuz sonuçlara yol açabilmektedir (197, 202). Bu durum da adaletsizlik ve eşitsizlik sorununu aşılamaz bir hal almaya başlar.

2.1.8 Büyük sağlık verisinde yeni etik sorular

Dijitalleşmenin hızla ilerlediği çağımızda, yalnızca teknolojik araçlar değil, bu araçların şekillendirdiği sosyal ilişkiler, bilgi üretim biçimleri ve değer sistemleri de dönüşüm geçirmektedir. Özellikle büyük veri çağında yalnızca teknolojik araçlar değil, bu araçların dönüştürdüğü kavrayış biçimleri de değişime uğramaktadır. Sağlık alanında da büyük verinin kullanımı, sağlık hizmetlerinin sunumunu, bireylerin sağlığa ilişkin karar alma süreçlerini ve toplumsal düzeyde sağlık politikalarının oluşumunu köklü biçimde değiştirmektedir (203).

Sağlık verisinin toplanma, işlenme ve kullanılma biçimleri; birey, topluluk ve kurumlar arasındaki etik ilişkileri derinden etkilemekte ve dönüştürmektedir. Bu dönüşüm yalnızca uygulamalara dair değil, etik ilkelerin kendisine de yöneliktir (203). Tıpta uzun süredir temel kabul edilen etik ilkeler -özerklik, zarar vermeme, yarar sağlama ve adalet- büyük veri teknolojilerinin işleyişinde çeşitli sınamalarla karşı karşıya kalmakta; bu ilkelerin içeriği, kapsamı ve uygulanabilirliği zaman zaman muğlak hâle gelebilmektedir. Dolayısıyla, büyük sağlık verisinin gelecekte doğurabileceği yeni durumlar ve uygulamalar, bu ilkelerin salt uygulanma biçimlerini değil, aynı zamanda felsefi arka planlarını da yeniden gözden geçirmeyi gerektirebilir. Bu noktada, etik ilkelerin sabit, evrensel ve tarih dışı yapılar değil, tarihsel ve bağlamsal koşullar içerisinde biçimlenen düşünsel yapılar olduğu fikri öne çıkmaktadır (204).

Bu çerçevede, Nietzsche'nin "tüm değerlerin yeniden değerlendirilmesi" (Umwertung aller Werte) çağrısı, dikkat çekici bir felsefi arka plan sunmaktadır. Nietzsche'ye göre, insanlık tarihinin belirli dönemlerinde baskın hâle gelen değer

sistemleri, zamanla kendi iç çelişkileriyle yüzleşmeye başlar ve artık yaşamı destekleyemez hâle gelir. Bu durumda, mevcut değerlerin ve ahlaki normların yeniden sorgulanması, hatta yerlerine yeni değerlerin geçirilmesi gerekebilir (205). Yani, Nietzsche belirli bir tarihsel dönemde mutlak kabul edilen değerlerin, yeni yaşam koşulları karşısında geçersizleşebileceğini ve yeniden ele alınması gerektiğini savunur. Bu düşünce, etik değerlerin sabitliğine değil, yaşamla ve toplumsal dönüşümle birlikte evrilebilirliğine vurgu yapmaktadır. Değerlerin yeniden değerlendirilmesi, Nietzsche için bir yıkım değil, tersine yaratıcı bir yeniden kurma sürecidir.

Benzer bir yaklaşım, büyük sağlık verisinin giderek daha karmaşık, öngörülemez ve çok katmanlı hâle geldiği günümüzde etik düşünceye de uygulanabilir. Sağlık verilerinin yalnızca bireysel değil, toplumsal, genetik ve davranışsal düzlemlerde yeni durumlar yaratması; verinin öngörüler üzerinden gelecek yaşam biçimlerini şekillendirmesi; öznelliğin veriyle temsil edilen biçimlere dönüşmesi gibi gelişmeler, yalnızca yeni etik sorunlar üretmekle kalmaz, aynı zamanda mevcut değerlerin yeterliliğini de sorgulatabilmektedir. Bu bağlamda, önümüzdeki yıllarda büyük sağlık verisiyle ilgili karşılaşılması muhtemel bazı etik sorunlar, yalnızca "yeni durumlar" olarak değil, aynı zamanda "yeni kavramsal sorunlar" olarak da ele alınmalı ve etik düşüncenin dönüşümüne alan açmalıdır. Çünkü her yeni teknoloji yalnızca teknik bir yenilik değil, aynı zamanda etik alanda da yeni düşünme biçimlerini zorunlu kılabilecek bir dönüşüm potansiyeli de taşımaktadır. Bu durumda büyük sağlık verisinin ürettiği karmaşık teknolojik ve toplumsal yapı karşısında, klasik etik ilkeler yetersiz kalabilir; bu nedenle yeni sorunlara yanıt verebilecek yeni etik kavramların geliştirilmesi gerekebilir (203).

Bu çerçevede, teknolojinin getirdiği yeniliklerle paralel biçimde evrilen bir etik düşünce anlayışı, yalnızca mevcut ilkelere bağlı kalmak yerine, yeni toplum ve yaşayış biçimlerine uygun değerler üretmeye yönelmelidir. Aşağıda, gelecekte büyük sağlık verisi alanında ortaya çıkabilecek bazı etik sorunlar bu perspektiften açıklanmıştır.

Veri çağında etik ilkeler, sabit bir ilke değil; dönüşen bir ihtiyaç olarak karşımıza çıkabilmektedir. Nietzsche'nin "değerlerin yeniden değerlendirilmesi" çağrısı, insanlık tarihindeki büyük kopuşların ardından gelen yeni anlam arayışlarının felsefi zeminini oluşturmaktadır. Bugün, büyük sağlık verisi alanında yaşanan dönüşüm de

böylesi bir kırılmaya işaret etmektedir (206). Dijital ontolojinin etkisiyle bireyin bedeni, kimliği ve geleceği sayısal kodlarla temsil edilecek olup; ontolojik veri özerkliği, etik bir meseleye dönüşebilecektir (207). Bu bağlamda etik, yalnızca bireysel mahremiyet ya da rıza çerçevesinde değil, aynı zamanda kolektif biyoveri adaleti, veri egemenliği ve biyoverisel ayrımcılık gibi çok katmanlı bir zeminde yeniden tanımlanmak zorunda kalabilecektir. Byung-Chul Han da, modern toplumda verinin yalnızca bir araç değil, bireyleri şekillendiren ve yönlendiren bir iktidar mekanizması olduğunu savunur(208). Ona göre veri, şeffaflık ve performans söylemi altında bireyleri denetim altına alan yeni bir norm koyucu güç hâline gelmiştir. Bu bağlamda, veri artık yalnızca bir araç değil, aynı zamanda norm koyucu bir iktidar mekanizması hâline gelmiştir (209). Nietzsche'nin "değerlerin yeniden değerlendirilmesi" çağrısıyla örtüşen bu dönüşüm, yalnızca geleneksel etik ilkelerin yetersiz kaldığı değil, aynı zamanda yeni etik soruların da kaçınılmaz biçimde gündeme geldiği bir çağın habercisidir. Büyük sağlık verisi alanında, veri temelli karar sistemlerinin yükselişiyle birlikte, bireyin kimliğinden mahremiyetine, rızasından gelecekteki potansiyeline kadar pek çok etik mesele kökten dönüşüme uğrama tehdidi altındadır. Artık etik, yalnızca geçmişin değerlerini korumak değil, aynı zamanda geleceğin belirsiz teknolojileri karşısında yeni değerleri inşa etmekle yükümlüdür.

Gelecekte ortaya çıkabilecek etik sorunlar, yalnızca teknolojik altyapıların değil, aynı zamanda insan kavrayışının da sınırlarını zorlamaktadır. Prediktif algoritmalar, bireyin henüz gerçekleşmemiş bir potansiyeli üzerinden etik kararlar verilmesine zemin hazırlarken; birey benliğinin çözünmesi, öznelliğin veri karşısında erimesine neden olmaktadır (210). Bu, "insan verisiyle mi tanımlanacak?" ya da "gelecek kuşakların verisel temsili etik açıdan nasıl korunacak?" gibi soruları gündeme getirir. Üstelik, bu algoritmik sistemler içinde etik sorumluluk bulanıklaşmakta, rıza kavramı içerikten yoksun bir formaliteye indirgenmektedir. Nietzsche'nin etik anlayışında olduğu gibi, burada da yeniden sorgulanması gereken bir değerler sistemi vardır: Sağlık, beden, benlik ve özgürlük gibi kavramlar, veri çağının ışığında yeniden düşünülmelidir.

3.2 Yasal Sorunlar

Dijital çağda bilgiye erişimin kolaylaşması, kişisel verilerin korunmasını zorunlu hale getirmiştir. Bu gereklilik hem ulusal hem de uluslararası düzeyde kapsamlı koruma mekanizmalarının geliştirilmesini gündeme getirmiştir.

Kişisel verilerin korunmasına yönelik yasal düzenlemelerin gelişimi büyük ölçüde teknolojik ilerlemelerin ve bu ilerlemelerin yol açtığı risklerin bir sonucu olarak şekillenmiştir. 20. yüzyılın ortalarında bilgisayar sistemlerinin yaygınlaşmasıyla birlikte kişisel bilgilerin toplanması, saklanması ve işlenmesi daha sistematik bir hale gelmiştir. Ancak bu durum, aynı zamanda veri güvenliğine ilişkin endişeleri de beraberinde getirmiştir (137). Özellikle devletlerin ve teknoloji şirketlerinin geniş çaplı veri tabanları oluşturması, bireylerin mahremiyetinin ihlal edilmesine yol açabileceği yönünde ciddi kaygılar doğurmuştur (211).

Yasal mevzuatlar kişisel verilerin mahremiyetini ve güvenliğinin sağlanması için oluşturulmuş ve uyulması gereken kurallar bütününden oluşmaktadır. Kişisel verilerin korunması, geçmişte yaşanan ve gelecekte yaşanması muhtemel ihlaller nedeniyle yasal düzenlemelerle güvence altına alınmış; özel yaşamın gizliliği, temel bir insan hakkı olarak kabul edilmiştir (17).

Oluşturulan bu kurallar bütünü sağlık alanında büyük veri kullanımı için tartışmalara neden olmaktadır. Geleneksel veri koruma yasaları, büyük verinin dinamik ve çok boyutlu doğasını tam olarak kapsayacak şekilde tasarlanmamıştır (212). Bu durum, özellikle bireylerin sağlık verileri üzerindeki hakları, verilerin ticari kullanımı ve sınır ötesi veri akışı gibi alanlarda belirsizlikler yaratmakta hak ihlaline sebep olmaktadır.

3.2.1 Uluslararası düzenlemeler ve standartlar

Küreselleşme ve dijitalleşme süreçlerinin hız kazanması, kişisel verilerin korunmasını yalnızca ulusal bir mesele olmaktan çıkararak uluslararası bir gereklilik haline getirmiştir. Bilgi akışının sınır ötesi niteliği, farklı ülkelerde uygulanan veri koruma politikalarının uyumlaştırılmasını zorunlu kılmıştır. Bu bağlamda, Avrupa Birliği Genel Veri Koruma Tüzüğü (General Data Protection Regulation- GDPR) gibi

kapsamlı yasal düzenlemeler, uluslararası standartların oluşturulmasına öncülük etmiştir. Bunun yanı sıra, Ekonomik İşbirliği ve Kalkınma Örgütü (Organisation for Economic Co-operation and Development - OECD) tarafından geliştirilen gizlilik ilkeleri ve Uluslararası Standardizasyon Örgütü (International Organization for Standardization - ISO) tarafından yayımlanan ISO 27001 Bilgi Güvenliği Yönetim Sistemi, Birleşmiş Milletler (BM) gibi standartlar, küresel ölçekte veri güvenliğinin sağlanmasına yönelik temel çerçeveyi oluşturmakta, veri koruma ve mahremiyetin küresel ölçekte sağlanmasına yönelik temel ilkeler benimseyerek bireylerin kişisel verileri üzerindeki denetimini güçlendirmeyi hedeflemektedir.

GDPR, bireylere verilerinin işlenmesi, erişilmesi ve silinmesi gibi konularda kapsamlı haklar tanıyarak, veri sorumlularına şeffaflık, hesap verebilirlik ve veri güvenliği gibi önemli yükümlülükler getirmektedir. Benzer şekilde, Kişisel Verileri Koruma Kanunu (KVKK) da Türkiye'de kişisel verilerin işlenmesine ilişkin usul ve esasları düzenleyerek, özel hayatın gizliliği ve veri mahremiyetini hukuki güvence altına almayı amaçlamaktadır (11, 12). Bu tür düzenlemeler, veri güvenliği ve bireysel hakların korunmasına yönelik küresel bir iş birliği çerçevesi oluşturmayı hedeflemektedir.

Büyük sağlık verisi, kişisel ve hassas bilgileri içermesi nedeniyle özel koruma gerektirir. GDPR, KVKK ve HIPAA gibi düzenlemeler, bireysel veri güvenliğini koruma amacı güderken, büyük sağlık verisinin işlenmesi açısından yetersiz kalmaktadır. Örneğin, GDPR Madde 6 (1-a), kişisel verilerin işlenmesi için bireyin açık rızasının alınmasını şart koşmaktadır (12) (GDPR, 2016, Madde 6). Ancak büyük veri analizlerinde, veriler farklı kaynaklardan sürekli olarak toplandığı için her bireyden açık rıza almak pratik olarak mümkün değildir. Ayrıca, büyük veri analitiği ile işlenen sağlık verileri genellikle öngörülemeyen amaçlar için yeniden kullanılabilir. GDPR'ın Madde 9 (2-a) hükmü, özel nitelikli verilerin işlenmesini de açık rızaya bağlamaktadır (12) (GDPR, 2016, Madde 9). Ancak büyük veri sistemleri, sürekli güncellenen veri kümelerinden oluştuğu için her yeni analizde tekrar rıza alma zorunluluğu veri bilimi süreçlerini ciddi şekilde yavaşlatmaktadır (213)

Benzer şekilde, Türkiye'deki KVKK Madde 5 (1) de kişisel verilerin işlenmesi için ilgili kişinin "açık rızasının alınmasını" zorunlu kılmaktadır (11) (KVKK, 2016,

Madde 5). Ancak sağlık büyük verisi, milyonlarca hastanın anonimleştirilmiş veya birleştirilmiş verilerinden oluştuğundan, bireysel rıza almaya dayalı bir sistem büyük ölçekli analizler için işlevsiz hale gelmektedir. Özellikle KVKK Madde 6 (2), özel nitelikli kişisel verilerin işlenmesi için de açık rıza gerektirdiğinden, büyük veri sistemlerinde otomatik analizleri ve makine öğrenmesi süreçlerini sınırlamaktadır (11) (KVKK, 2016, Madde 6). Bu durum, epidemiyolojik araştırmalar veya sağlık sistemlerini iyileştirmek için yapılan veri analizlerini zorlaştırmakta ve inovasyonu kısıtlamaktadır (214).

2024 yılında 6698 sayılı Kişisel Verilerin Korunması Kanunu'nda yapılan değişikliklerle, kişisel verilerin yurt dışına aktarımı başta olmak üzere bazı hükümler önemli ölçüde revize edilmiştir (215). Bu revizyonlar, özellikle veri işleyenlerin yükümlülüklerini kolaylaştırırken, veri sahiplerinin hakları açısından tartışmalı bir genişlemeye yol açmıştır. Değişikliklerin temelinde, veri aktarım süreçlerinin daha esnek hale getirilmesi ve uluslararası uyumluluğun artırılması hedeflenmiştir (216); ancak bu hedef doğrultusunda atılan adımlar, bireylerin kişisel verileri üzerindeki denetimini zayıflatabilecek niteliktedir.

Özellikle Kanun'un 9. maddesinde yapılan değişiklikler dikkat çekicidir. Bu maddeye göre artık kişisel verilerin yurt dışına aktarımı, yalnızca açık rıza ya da yeterli koruma düzeyi bulunan ülkelerle sınırlı olmayıp, Kişisel Verileri Koruma Kurulu'nun uygun gördüğü güvence yöntemleriyle de mümkün hale getirilmiştir. Yeni düzenleme uyarınca, veri sorumluları ile veri aktarımı yapılan taraflar arasında "bağlayıcı şirket kuralları", "standart sözleşmeler" ya da Kurul onaylı "taahhütnameler" ile aktarım gerçekleştirilebilecektir (216). Bu yöntemler her ne kadar pratikte uluslararası veri akışını kolaylaştırmayı amaçlasa da Kurul'un değerlendirme kriterlerinin şeffaf olmaması (217), bireylerin verilerinin hangi ülkeye, kimlere ve hangi koşullarda aktarıldığına dair bilgiye erişimini sınırlayabilir.

Bir diğer dikkat çekici değişiklik, Kurul'a daha geniş takdir yetkisi verilmiş olmasıdır. Revizyonla birlikte Kurul'un kişisel veri işleme ve aktarım süreçlerinde "risk temelli değerlendirme" yapma yetkisi güçlendirilmiş; böylece bireysel verilerin

kaderi, giderek daha fazla idari yorumlara bağlı hale gelmiştir (215, 216). Bu durum, verinin sahibinin rızasına dayalı koruma ilkesini zayıflatmaktadır.

Ayrıca, değişikliklerin kamu yararı, kamu sağlığı, kamu düzeni gibi belirsiz kavramlara dayanarak bazı durumlarda veri işlenmesini kolaylaştırdığı görülmektedir (215, 216). Bu belirsizlik, veri işleme süreçlerinde keyfiliğe yol açabilecek potansiyel tehlikeler barındırmaktadır. Her ne kadar Kanun hâlâ açık rıza, bilgilendirme yükümlülüğü ve veri minimizasyonu gibi birey merkezli koruma ilkelerini içerse de, revizyon sonrası düzenlemeler, bu ilkelerin uygulanmasını zayıflatacak şekilde geniş yorumlara açık hale gelmiştir.

KVKK 2024 yılında yapılan değişikliklerle birtakım güncellemeler geçirmiş ve örneğin açık rıza dışındaki bazı veri işleme şartları Avrupa Birliği Genel Veri Koruma Tüzüğü'ne (GDPR) daha yakın hâle getirilmiş olsa da (216), bu revizyonlar yapısal bir dönüşümden çok, biçimsel bir uyum izlenimi yaratmaktadır. Özellikle "meşru menfaat" gibi ucu açık gerekçelere dayanarak veri işleme izinlerinin genişletilmesi, bireyin rızasını işlevsiz kılmakta ve veri sahipliğinin özünü zayıflatmaktadır. Bu durum, bireylerin kendi verileri üzerindeki öznel denetim haklarını ortadan kalkmasına neden olabilir.

Bu noktada Türk Medeni Kanunu'nun 23. maddesi dikkat çekicidir. Maddeye göre: "Kimse, hak ve fiil ehliyetinden kısmen de olsa vazgeçemez; hukuka veya ahlaka aykırı olarak özgürlüğünden feragat edemez." Bu hüküm, bireyin özgürlüğünü devredilemez ve dokunulmaz kılarken, kişisel verilerin sınırsızca işlenebilmesini hukuken ve ahlaken sorunlu hâle getirmektedir (218). Zira dijital ortamda işlenen her veri, bireyin davranışlarını, karar alma süreçlerini ve hatta düşünsel yönelimlerini belirlenebilir kılmakta; böylece bireyin özerkliğini tehdit etmektedir (219). Başka bir deyişle, dijital mahremiyetin ihlali, bireyin özgürlüğünü ihlal anlamına gelmektedir. Bu da TMK m.23 kapsamında "özgürlükten feragat" anlamı taşımaktadır ki, bu açıkça hukuk düzenine aykırıdır.

Dolayısıyla KVKK'nın mevcut haliyle, bireyin özgürlüğünü bütüncül olarak koruduğunu söylemek mümkün değildir. Mahremiyet hakkı, yalnızca rıza mekanizmasına indirgenemez; zira rıza, günümüz dijital sistemleri içinde çoğu zaman

teknik, karmaşık ve yönlendirilmiş metinlerle sağlanan biçimsel bir onaya dönüşmüş durumdadır (220). Oysa bireyin dijital ortamdaki özgürlüğü, veriler üzerindeki maddi ve manevi tasarruf hakkını içerir (221, 222). Bu hak ise, Medeni Kanun'un kişiliğin korunmasına dair temel ilkeleriyle doğrudan ilişkilidir.

Kişisel sağlık verilerinin niteliği gereği, bu veriler yalnızca mahremiyet açısından değil, bireyin fiziksel, ruhsal, sosyal ve ekonomik bütünlüğü açısından da kritik öneme sahiptir (52). Türkiye'de bu alanı düzenleyen temel metin olan "Kişisel Sağlık Verileri Hakkında Yönetmelik", ilk bakışta kapsamlı bir düzenleme gibi görünse de dijitalleşen sağlık sistemleri, büyük veri uygulamaları ve ikincil veri kullanımı karşısında yetersiz kalabilmektedir. Yönetmelik, veri işleme süreçlerine dair bazı temel çerçeveleri sunmakta; açık rıza, veri sorumlusu yükümlülükleri ve veri güvenliği ilkelerine yer vermektedir (223). Ancak bu düzenlemeler, pratikte verinin gerçek yaşam döngüsünü tam anlamıyla kapsayamamakta, bireyin verisi üzerindeki denetim hakkını güçlendirmemekte ve teknolojik gelişmelere karşı uyumlu bir altyapı sunmamaktadır.

Öncelikle, yönetmelikte "açık rıza" kavramı son derece geleneksel ve yüzeysel bir biçimde ele alınmıştır. Bireyin bilgilendirilmiş bir biçimde rıza göstermesinin, çok katmanlı dijital sistemlerde neredeyse imkânsız hâle geldiği günümüzde, bu yaklaşım yeterli değildir (224). Açık rızanın içeriksel kalitesi yerine yalnızca formel varlığına odaklanmak, bireyin iradesini temsil etmeyen rıza prosedürlerine alan açmakta ve veri sahipliğini zayıflatmaktadır (225).

İkinci olarak, yönetmelikte "veri güvenliği"ne ilişkin getirilen yükümlülükler, büyük oranda soyut ilkeler düzeyinde kalmakta, teknik altyapının ne şekilde yapılandırılması gerektiğine dair somut bir çerçeve sunmamaktadır.

Türk hukuk sisteminde Kişisel Verilerin Korunması Kanunu (KVKK) temel düzenleyici olmakla birlikte, kişisel veriye doğrudan veya dolaylı şekilde yer veren farklı mevzuat metinleri de bulunmaktadır.

Örneğin Türk Ceza Kanunu'nun (TCK) 9. Bölümü, "Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar" başlığı altında bireylerin özel hayatının gizliliğini güvence altına almayı amaçlamaktadır (226). Bu bağlamda TCK'nın 134. maddesi, özel hayatın

gizliliğini ihlal suçunu tanımlarken; 135 ila 140. maddeleri arasında ise kişisel verilerin hukuka aykırı olarak kaydedilmesi, başkalarına verilmesi, yayılması veya ele geçirilmesi gibi fiiller suç olarak düzenlenmiştir (227). Ayrıca, verilerin yok edilmemesi ve bu verilerin belirli bir süre saklanması durumlarında da cezai sorumluluk öngörülmektedir (226).

Türk Ceza Kanunu, veri koruma açısından önemli bir caydırıcılık sağlamayı hedeflese de hukuki çerçevenin koruyucu niteliği büyük ölçüde cezalandırma esasına dayanmaktadır. Yani veriye ilişkin bir ihlal gerçekleştikten sonra devreye giren bir sistem söz konusudur (227). Oysa etik bir veri yönetim sistemi, yalnızca kötüye kullanımı cezalandırmakla yetinmez; verinin toplanmasından silinmesine dek tüm yaşam döngüsünü kapsayan, önleyici ve yönlendirici bir mekanizma kurmayı hedefler (222).

Bu açıdan değerlendirildiğinde, TCK'nın yaklaşımı hem bireysel veri özerkliği hem de büyük veri çağında ortaya çıkan yeni etik sorunlar karşısında sınırlı bir koruma sunmaktadır. Örneğin, TCK'da veri sahibinin bilgilendirilmiş onamına, veriye erişim hakkına veya verinin taşınabilirliğine ilişkin bir düzenleme bulunmamaktadır (228). Yine, verinin anonimleştirilmesi, amaçla sınırlı işlenmesi ya da makine öğrenmesi gibi tekniklerle türetilen çıkarımsal veriler (229) ile ilgili herhangi bir açık hüküm yer almamaktadır. Dolayısıyla yasa, teknolojik gelişmelerin ortaya çıkardığı yeni tehditlere karşı güncel ve önleyici bir koruma perspektifinden uzaktır (226).

Ayrıca, 134. maddede düzenlenen özel hayatın gizliliğine ilişkin hüküm de daha çok görüntü veya ses kaydının izinsiz alınması gibi somut ihlallerle sınırlı kalmakta, bireyin dijital ortamda bırakmış olduğu veri izlerinin özel hayat kapsamında değerlendirilip değerlendirilmeyeceği net değildir (227, 230). Dijital çağda özel hayatın kapsamı giderek genişlerken, hukuki düzenlemelerin hâlen fiziksel dünyadaki gizlilik anlayışına dayanması, çağın ihtiyaçlarını karşılamaktan uzaktır (222).

Bu durum, etik ilkelere dayalı bir veri koruma yaklaşımının hukuki düzenlemelerle desteklenmesi gerektiğini ortaya koymaktadır. Modern veri koruma rejimlerinde, veri öznelerinin yalnızca zarar görmemesi değil, kendi verileri üzerinde aktif kontrol sahibi olması hedeflenir. Bu da önleyici düzenlemelerle mümkündür

(162, 222, 231). Türk Ceza Kanunu'nun ise bu önleyici yapıyı tam anlamıyla sunamadığı, daha çok ihlal sonrası cezalandırma pratiği üzerine kurulu olduğu söylenebilir. Bu düzenlemeler, verinin yalnızca kötüye kullanımına karşı bir koruma sağlamaktadır. Hükümler, verilerin işlenmesi sürecindeki meşruiyet, şeffaflık, veri minimizasyonu veya bireyin veri üzerindeki kontrol hakları gibi temel etik ilkelerle doğrudan ilişkili değildir. Türk Ceza Kanunu'nun doğası gereği cezalandırmaya odaklanan bir metin oluşuyla açıklanabilir. Ceza hukukunun yapısı, genel olarak ihlal gerçekleştikten sonra devreye giren mekanizmalar barındırır. Bu nedenle, kişisel veri koruması açısından TCK'dan önleyici, yönetişimsel ve etik temelli bir yapı beklemek doğru olmayabilir. Ancak burada asıl sorun, veri yaşam döngüsünü kapsayan daha kapsamlı bir etik ve yönetsel sistemin hâlâ kurumsallaşmamış olmasıdır (222).

Tüm bu düzenlemeler bir arada değerlendirildiğinde, Türkiye'deki mevcut yasal çerçevenin büyük veri çağının gerektirdiği etik ilkelerle tam olarak örtüşmediği, hatta bazı durumlarda bireyin veri üzerindeki öznel haklarını zayıflatan uygulamalara zemin hazırladığı görülmektedir (226, 228, 230). Özellikle veri korumanın bir "paylaşım izni" çerçevesinde şekillendirilmesi, etik bir perspektiften tartışılmayı gerektiren temel sorunlardan biridir.

Türk hukuk sistemi bu tür yasalarla kişisel verileri koruma altına alırken, ABD'de yürürlükte olan HIPAA, sağlık verilerinin işlenmesi ve paylaşılması konusunda 45 CFR §164.508 ile yazılı açık rıza alınmasını zorunlu kılmaktadır (232) (HIPAA, 1996, 45 CFR §164.508). Ancak sağlık büyük verisi bağlamında bu gereklilik otomatik veri analizini ve gerçek zamanlı sağlık izleme sistemlerini büyük ölçüde yavaşlatmaktadır. Örneğin, bir hastanın verileri tedavi süreci için bir sağlık kuruluşundan diğerine aktarılırken, bu verilerin bilimsel araştırmalar veya yapay zeka destekli analizlerde kullanımı için yeni bir rıza süreci gerekmektedir (116). HIPAA'nın 45 CFR §164.506 hükmü, sağlık hizmeti sağlayıcılarının tedavi ve ödeme amaçlı veri işlemesine izin verse de (232) (HIPAA, 1996, 45 CFR §164.506), büyük veri perspektifinden bakıldığında bu kısıtlama verinin geniş çaplı analiz edilmesini ve farklı amaçlar için yeniden kullanımını engellemektedir.

Kısacası mevcut yasal çerçeve, GDPR, KVKK, HIPAA gibi yasalar, kişisel sağlık verilerinin işlenmesi için açık rıza gerektirir. Ancak büyük veri projelerinde, bu rızanın kapsamı ve süresi net değildir. Sağlık verisinin anonimleştirilmesi, yapay zeka ve makine öğrenmesi teknikleriyle geri döndürülebilir hale gelmektedir. Özellikle nadir hastalıklar veya genetik veriler gibi küçük veri kümeleri, anonimleştirilse bile bireylerin tespit edilmesine yol açabilmektedir (214).

Onam konusunda yönetmeliklerle birlikte etik bildirgeler de bireyden açık rıza alınmasının gerekliliğinden ve öneminden bahseder. Örneğin, Helsinki Bildirgesi, tanımlanabilir insan materyali ve verileri de dahil olmak üzere, insanlar üzerindeki tıbbi araştırmalarla ilgili etik ilkeleri belirler. Bildirgenin 25. maddesi, araştırmaya katılan bireylerin özgür ve bilgilendirilmiş onam vermesi gerektiğini ifade etmektedir. Ancak, büyük veri analizlerinde, bu onamın kapsamının tam olarak belirlenmesi zordur, çünkü veriler ilerleyen süreçte öngörülmeyen analizler için yeniden kullanılabilir (233).

Benzer şekilde, UNESCO Biyoetik ve İnsan Hakları Evrensel Bildirgesi'nin 6. maddesi, bireylerin tıbbi ve bilimsel araştırmalara katılımı için özgür ve bilgilendirilmiş onam vermesi gerektiğini vurgulamaktadır (187). Ancak büyük veri araştırmalarında, bireylerin verilerinin ne şekilde kullanılacağını öngörmesi güç olduğundan, onam sürecinin kapsamı yetersiz kalmaktadır. Ayrıca, Lizbon Hasta Hakları Bildirgesi'nin 4. maddesi, hastaların kişisel sağlık bilgilerinin gizliliğini koruma hakkını güvence altına almaktadır (234). Ancak büyük veri uygulamalarında, sağlık verileri anonimleştirilse bile, veri setleri birleştirildiğinde bireylerin kimlikleri yeniden belirlenebilir hâle gelmektedir. Bu durum, etik çerçevelerde belirtilen bireylerin veri mahremiyetini koruma ilkesine meydan okumaktadır.

Mevcut etik bildirgeler bireylerin verileri üzerindeki haklarını vurgulasa da, büyük veri analizlerinin doğası gereği, verilerin zaman içinde öngörülmeyen şekillerde kullanılması kaçınılmazdır. Büyük veri analizlerinde hastalardan alınan rızanın kapsamı ve verilerin gelecekteki kullanım alanları tam olarak belirlenememektedir. Verilerin farklı amaçlarla yeniden kullanımı veya beklenmedik analizlerde kullanılması, başlangıçta alınan onamın ötesine geçebilir. Bu durum, etik çerçevelerin öngördüğü bireysel kontrol ve onam ilkeleriyle çelişkilere yol açabilir (235).

Dolayısıyla, büyük veri analizlerinde, etik ilkeler ile pratik uygulamalar arasındaki bu uyumsuzluğun giderilmesi için yeni yaklaşımlara ihtiyaç duyulmaktadır.

Yönetmeliklerin ve etik bildirgelerin önemle vurguladığı diğer bir konu ise bireylerin kendi verileri hakkındaki söz sahipliğidir. Büyük sağlık verisi, devletler, özel şirketler ve araştırma kurumları tarafından merkezi bir biçimde toplanmakta ve analiz edilmektedir. Bu bağlamda, Avrupa İnsan Hakları Sözleşmesi (AİHS)'nin 8. maddesi, bireylerin özel ve aile hayatına saygı gösterilmesi hakkını güvence altına alır. Bu madde, kişisel verilerin korunmasını ve izinsiz erişimin engellenmesini da kapsar (236). Oviedo Biyotıp Sözleşmesi ise biyoetik, tıbbi araştırma, onam, özel yaşam ve bilgilenme hakkı gibi konularda ilkeler belirler. Bu sözleşmenin 5. maddesi biyomedikal araştırmaların etik ve insan onuruna saygılı bir şekilde yapılmasının önemini ve kişisel sağlık verilerinin korunmasını vurgular (237).

Dünya Sağlık Örgütü (WHO- World Health Organization), sağlık verilerine erişim ve bunların yönetilmesi konusunda rehberler yayınlamaktadır. WHO'nun yayınladığı "Dijital Sağlık Rehberi" nde, sağlık verilerinin doğru ve güvenli bir şekilde toplanması gerektiği, bireylerin bu verilere erişim hakkına sahip olduğu belirtilmiştir (238). Ancak, büyük veri projelerinde verilerin sahipliği ve yönetimi genellikle belirsizdir. Verilerin toplanması, depolanması ve paylaşılması süreçlerinde, bireylerin onamı ve bilgilendirilmesi konusunda eksiklikler yaşanabilir. Bu durum, kişisel verilerin korunması ve bireylerin mahremiyet haklarıyla çelişebilmektedir. Dolayısıyla, büyük sağlık verisi projelerinde etik ve yasal düzenlemelerin netleştirilmesi, bireylerin haklarının korunması için esastır (239).

Bu denli farklı yasaların mevcudiyeti kendi aralarında uyumlu oldukları yanların yanında uyumlu olmadıkları durumlarda mevcuttur. Farklı yasaların bulunduğu farklı ülkeler kendi iç hukukuna göre bu yasaları düzenleyebilmektedir. Farklı ülkelerdeki veri koruma yasalarının uyumlu olmaması, küresel sağlık araştırmalarında hukuki çatışmalara yol açmaktadır. Küresel sağlık verisi projelerinde, veri transferi yapılırken her ülkenin kendi yasal düzenlemelerine uymak zorunluluğu ortaya çıkmaktadır. Bu da sağlık verisinin güvenli bir şekilde paylaşılmasını zorlaştırmakta ve araştırmaların uluslararası işbirliklerini engellemektedir. Örneğin, Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR), kişisel verilerin yurtdışına aktarılmasında sıkı kurallar

koyarken, Sağlık Sigortası Taşınabilirlik ve Sorumluluk Yasası (HIPAA) ABD'deki sağlık verilerini korumaya yönelik farklı düzenlemelere sahiptir. Bu durum, her iki yasanın gerekliliklerine aynı anda uyulmasının zor olmasına yol açmaktadır. Ayrıca, OECD Sağlık Verisi Yönergeleri'nde, ülkeler arasında sağlık verisi transferini düzenleyen kurallar belirlenmiş olsa da her ülkenin bu yönergeleri kabul etmesi zorunlu değildir. Farklı ülkelerdeki veri koruma yasaları uyumlu olmadığından, küresel sağlık araştırmalarında hukuki çatışmalar ortaya çıkmaktadır(239). Bu farklılıklar, sağlık verisi paylaşımının sınırlarını çizerken, veri sahiplerinin haklarını ihlal etmeden doğru şekilde veri paylaşımının yapılması için global bir uyumun olmaması gibi büyük bir sorunu da beraberinde getirmektedir (240).

Yönetmelik ve etik bildirgelerle birlikte verilerin depolanması, işlenmesi ve kullanılması bazı uygulamalar ve şirketlerin elinde olabiliyor. Özellikle giyilebilir cihazların ürettiği sağlık verileri bireylerin kullandıkları uygulama ve cihazlara bağlı olarak depolama ve işleme işlemini gerçekleştiriyor. En çok kullanılan uygulama altyapılarından birini oluşturan Google'nin veri koruma yasası da büyük veri için işlevsiz kalabilmektedir. Google'ın veri güvenliği politikaları ve ilgili yasal çerçeveleri, genellikle sağlık verisinin işlenmesi, saklanması ve paylaşılması üzerine odaklanır. Google Health, Google Fit ve Google Cloud Healthcare API gibi platformlar aracılığıyla sağlık verisi analizleri yürütülmektedir. Ancak, büyük teknoloji şirketlerinin sağlık verisini kullanması bazı yasal ve etik sorunları da beraberinde getirmektedir. Google, sağlık verilerini toplarken genellikle GDPR (Genel Veri Koruma Yönetmeliği) ve HIPAA (Sağlık Sigortası Taşınabilirlik ve Sorumluluk Yasası) gibi uluslararası veri koruma düzenlemelerine uymaya çalışmaktadır (241).

GDPR, verilerin anonimleştirilmesi veya kullanıcıdan açık onay alınmasını zorunlu kılarken, Google'ın global veri paylaşım süreçlerinde bu düzenlemelere tam uyum sağlamak, farklı yasal düzenlemelerin birleşmesi nedeniyle karmaşık hale gelir. Örneğin, Google Drive uygulaması, araştırma projelerinde veri paylaşımı ve işbirliğini kolaylaştırmak adına büyük bir kolaylık sunmaktadır. Ancak, bu hizmetin sunduğu kolaylıklara rağmen, verilerin nasıl depolandığı, analiz edildiği ve işlenmeye devam ettiği konusunda belirsizlikler bulunmaktadır. Google'ın bu platformda kullanıcı verilerini toplama, saklama ve işleme süreçleri genellikle şeffaflık eksiklikleri ile

gölgelenmektedir. Bu durum, veri sahiplerinin verilerinin nasıl kullanıldığına dair yeterli bilgiye sahip olmamalarına ve olası veri güvenliği ihlallerine karşı savunmasız kalmalarına yol açmaktadır. Google gibi büyük teknoloji firmalarının sağlık verisini toplaması, kamuya açık sağlık araştırmalarını tehlikeye atabilirken belirli şirketlerin veri üzerinde tekel oluşturmasına neden olabilir (242).

Bir örnek olarak, 2016 yılında Google'ın yapay zeka birimi DeepMind ve İngiltere'nin National Health Service (NHS) arasındaki iş birliği, sağlık verilerinin gizliliği ve korunması konusunda ciddi eleştiriler almıştır. Bu iş birliği kapsamında, NHS, 1.6 milyon hasta verisini DeepMind ile paylaşmış ve bu veriler, akut böbrek yetmezliği gibi hastalıkları tespit etmek amacıyla kullanılan bir yapay zeka algoritmasının geliştirilmesinde analiz edilmiştir. Ancak, bu süreçte, hastaların açık rızalarının alınmaması ve verilerin kullanımı konusunda yeterli şeffaflık sağlanmaması, önemli bir etik ve yasal ihlal olarak değerlendirilmiştir (243). Sağlık verilerinin toplanması ve işlenmesi, özellikle kişisel veri koruma yasaları çerçevesinde açık bir rıza gerektirdiği için, NHS'nin veri paylaşımı ve kullanım süreçleri, veri güvenliği ve kişisel gizlilik hakları açısından sorgulanmıştır (244). Bu durum, sağlık verilerinin yönetimi ve gizliliği konusundaki şeffaflık eksikliklerinin ve rıza alma prosedürlerinin önemini vurgulamaktadır.

Onam, veri sahipliği, veri kontrolü ve bireyin veri haklarının tanımlanması ile bu haklara saygı gösterilmesi yönündeki düzenlemelerin en temel bileşenlerinden biri mahremiyet ve gizliliktir. Bu hakların tanınması ve korunması gerekliliği, esasen mahremiyet ve gizlilik ilkeleri çerçevesinde şekillenmektedir. İlgili yönetmelikler, etik bildirgeler ve uygulayıcı kurumların veri güvenliği politikaları incelendiğinde, özellikle sağlık verilerinin mahremiyetinin korunmasının öncelikli ve temel bir ilke olarak vurgulandığı görülmektedir. Örneğin, Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR), sağlık verilerini "özel nitelikli kişisel veriler" kategorisinde değerlendirmekte ve bu verilerin işlenmesine kısıtlamalar getirmektedir. GDPR'nin 9. maddesinin 1. fıkrası, sağlık verileri gibi özel nitelikli kişisel verilerin işlenmesini genel olarak yasaklamakta olup, 2. fıkra ise belirli koşullar altında bu yasağa istisnalar tanımlamaktadır (12). Buna göre, tıbbi teşhis, sağlık veya sosyal bakım hizmetlerinin sağlanması ya da sağlık sistemleri ve hizmetlerinin etkin yönetimi gibi durumlarda, bu

verilerin işlenmesine izin verilebilmektedir. Ancak bu işlemler, yalnızca mesleki gizlilik yükümlülüğü altındaki yetkili kişiler tarafından gerçekleştirildiğinde hukuka uygun kabul edilmektedir.

UNESCO Biyoetik ve İnsan Hakları Evrensel Bildirgesinde de bireylerin özel yaşamlarına ve kişisel verilerinin gizliliğine saygı gösterilmesi gerektiğini vurgular. Özellikle, 9. madde şu şekilde belirtilmiştir: "Kişilerin mahremiyeti ve kişisel bilgilerinin gizliliğine saygı gösterilmelidir. Mümkün olduğu ölçüde bilgiler, başta uluslararası insan hakları hukuku olmak üzere uluslararası hukuk ile bağdaşacak şekilde, toplanma veya onam verilme amacının dışında kullanılmamalı ve ifşa edilmemelidir." (187) (UNESCO, 2006, Madde 9)

Türkiye'de ise veri güvenliği ve kişisel verilerin korunmasıyla ilgili temel yasa, 6698 sayılı Kişisel Verilerin Korunması Kanunu'dur (KVKK). Bu kanunun 12. maddesi, veri sorumlularının kişisel verilerin hukuka aykırı olarak işlenmesini ve erişilmesini önlemek, verilerin muhafazasını sağlamak için uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almakla yükümlü olduğunu belirtir (11) (KVKK, 2016, Madde 12).

Türkiye'deki mevcut yasal düzenlemeler ve büyük veri ile ilgili; Filiz Bulut'un 2023 yılında tamamladığı "Sağlıkta Büyük Veri: Ulusal Düzenlemeler ve Veri Kayıt Sistemlerinin Tıp Etiği Açısından İncelenmesi" başlıklı doktora tezi, Türkiye'deki kişisel verilerin korunmasına yönelik temel düzenlemeleri ve sağlık hizmetlerinde kullanılan veri tabanlarını, uluslararası etik kılavuzlarda belirtilen toplum yararı, minimum veri, hassas veri, eşitlik ve adalet, özerklik ile mahremiyet ve gizlilik ilkeleri çerçevesinde değerlendirmiştir. Çalışmanın bulgularına göre, Türkiye'deki mevcut düzenlemelerin ve veri tabanlarının, belirtilen etik ilkelerle uyumlu olmadığı saptanmıştır. Özellikle, Kişisel Verileri Koruma Kanunu'nun 6. maddesinin 3. fıkrası ve 28. maddesinin, bu etik ilkelerle uyumsuz olduğu belirlenmiştir. Bu uyumsuzluğun temel nedenleri arasında, yasal düzenlemelerin günümüz teknolojik gelişmelerine ve büyük veri uygulamalarına ayak uyduramaması, veri mahremiyeti konusunda yeterli hassasiyetin gösterilmemesi ve uluslararası standartlara tam entegrasyonun sağlanamaması bulunmaktadır (17). Ayrıca, mevcut düzenlemelerin, bireylerin

özerklik ve mahremiyet haklarını tam olarak koruyamadığı ve veri güvenliği konusunda eksiklikler barındırdığı tespit edilmiştir.

Türkiye'deki sağlık veri tabanlarını da inceleyen Bulut, e-Nabız ve Merkezi Hekim Randevu Sistemi (MHRS) gibi uygulamalarda tespit ettiği eksiklikler arasında, veri güvenliği ve gizliliği konularında bazı zayıflıklar, kişisel verilerin korunmasına yönelik yetersiz denetimler ve sistemler arası entegrasyon eksiklikleri öne çıkmaktadır. Ayrıca, kullanıcıların sağlık verilerine erişim hakları ve onam süreçlerinin daha şeffaf hale getirilmesi gerektiği vurgulanmıştır. Bu bağlamda, Türkiye'deki ulusal düzenlemelerin, büyük veri uygulamalarının etik ve hukuki gerekliliklerine uygun hale getirilmesi için güncellenmesi ve uluslararası standartlarla uyumlu hale getirilmesi gerektiği sonucuna varılmıştır (17).

Söz konusu çalışmada dile getirilen bu değerlendirme, etik sorunların veri üretimindeki hız ve yaygınlıkla birlikte daha da karmaşık hâle geleceğini göstermesi açısından önemlidir. Veri temelli sağlık uygulamalarının yaygınlaşması, söz konusu tezde ifade edilen etik sorunların yalnızca akademik düzeyde değil, pratikte de sorun olmayı sürdürdüğünü ve giderek derinleştiğini göstermektedir. Büyük sağlık verisi alanında verilerin elde edilme biçimi, kullanımı ve paylaşımı konularında yaşanan etik sorunlar yalnızca sayıca artmakla kalmamakta, aynı zamanda giderek çok katmanlı bir hâl almaktadır. Özellikle veri sahipliğinin belirsizleşmesi, bireylerin rızasının etkisizleşmesi ve veri güvenliğinin görece zayıf kalması, bu sorunların önümüzdeki dönemde daha da derinleşeceğini göstermektedir.

3.3 Teknik Sorunlar

Büyük veri sağlık sektöründe faydalı yenilikler sunsa da beraberinde çözülmesi gereken teknik zorlukları da getirmektedir. Sağlık alanındaki elektronik sağlık kayıtları, genetik veriler ve tıbbi görüntüler gibi veri setlerinin işlenmesi ve analiz edilebilmesi için güçlü bir teknik altyapı ve kesintisiz bir lojistik sistem gerektirmektedir (28). Ancak sağlık verisinin doğası gereği hassas olması, yüksek güvenlik önlemleri gerektirmesinin yanı sıra teşhis, tedavi ve araştırma süreçlerinde hız ve doğruluk standartlarının sağlanmasını zorunlu kılmaktadır. Bu gereklilikler,

büyük sağlık verisinin yönetiminde çeşitli teknik engellerin ortaya çıkmasına neden olmaktadır.

Sağlık alanındaki büyük veri ile ilgili teknik sorunlar verinin toplanması, saklanması, işlenmesi ve paylaşılması aşamalarında karşılaşılan zorluklardır. Veri saklama kapasitesinin yetersizliği, sistemler arası uyumsuzluk ve gerçek zamanlı erişim sorunları, sağlık hizmetlerinin etkinliğini doğrudan etkileyen başlıca teknik altyapı problemleri arasındadır. Öte yandan, büyük ölçekli sağlık verilerinin toplanması, taşınması ve paylaşılması da lojistik açıdan ciddi sorunlar doğurmaktadır (245).

3.3.1 Teknik altyapı ve lojistik sorunlar

Sağlık sektöründe büyük veri kullanımı; verilerin hacmi, çeşitliliği ve yüksek akış hızından kaynaklı olarak birçok teknik ve altyapısal sorunu beraberinde getirmektedir. Bu sorunlar, sağlık verisinin etkili, güvenli ve sürdürülebilir biçimde işlenmesini engellemekte; karar destek sistemlerinin güvenilirliğini ve klinik süreçlerin işlevselliğini doğrudan etkilemektedir (246).

Bu çerçevede ilk sorun, veri kalitesinin ve bütünlüğünün sağlanamamasıdır. Sağlık verileri sıklıkla farklı kaynaklardan, dijital sistemlerden ya da manuel girişlerden elde edilmekte; bu da veriler arasında tutarsızlıklar, eksiklikler veya hatalı kayıtlar oluşmasına neden olmaktadır (28). Eksik veya yanlış girilen hasta bilgileri, tedavi süreçlerinde hatalı kararlar alınmasına yol açabilirken; bu durum sağlık hizmetlerinin güvenilirliğini tehlikeye atmaktadır.

İkinci olarak, sistemler arası birlikte işlerliğin sağlanamaması, veri yönetiminde önemli bir aksaklıktır. Sağlık kurumlarında kullanılan elektronik sağlık kayıt sistemleri arasında format, yazılım ve terminoloji farklılıkları bulunmakta; bu da veri entegrasyonunu zorlaştırmaktadır (28). Örneğin, bir kurumun hasta kayıtlarını Word belgelerinde tutarken, diğerinin Excel dosyaları kullanması gibi basit farklar bile analiz sürecini sekteye uğratabilmektedir. Daha geniş ölçekte, bir ülkenin sağlık sigortası sistemine göre kodlanmış veriler başka bir ülkenin otoriteleri tarafından yorumlanamayabilir. Bu nedenle HL7 (Health Level Seven International) ve FHIR

(Fast Healthcare Interoperability Resources) gibi uluslararası standartların kullanımı, veri uyumluluğu açısından kritik önem taşımaktadır (247).

Bir diğer temel sorun, veri depolama altyapısının yetersizliğidir. Tıbbi görüntüler, genetik dizilim verileri ve kapsamlı hasta kayıtları gibi büyük veri kümeleri yüksek kapasiteli ve güvenli depolama çözümleri gerektirmektedir. Ancak yerel sunucuların kapasitesi sınırlı olmakta; bulut tabanlı çözümler ise hem maliyet hem de veri güvenliği açısından çeşitli zorluklar doğurmaktadır (28). Özellikle küçük ölçekli veya düşük bütçeli sağlık kurumlarında bu verilerin uzun vadeli saklanması teknik ve ekonomik olarak sürdürülebilir olmayabilir (248).

Veri güvenliği ve erişim kontrolü, sağlık verilerinin yönetiminde karşılaşılan dördüncü temel sorundur. Sağlık verileri, hasta mahremiyetini doğrudan ilgilendirdiğinden ulusal ve uluslararası düzenlemelerle korunmak zorundadır (246). Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR) ve ABD Sağlık Sigortası Taşınabilirlik ve Sorumluluk Yasası (HIPAA) gibi düzenlemeler bu alanda çerçeve sunmaktadır. Ancak, eski yazılım altyapıları ve siber güvenlik açıkları, sağlık verilerini saldırılara açık hâle getirmektedir (163).

Beşinci olarak, veri transferi ve paylaşımı konusunda altyapı eksiklikleri göze çarpmaktadır. Farklı sağlık kurumları, laboratuvarlar ve araştırma merkezleri arasında yapılan veri paylaşımları yüksek bant genişliği ve güvenli ağ altyapıları gerektirmektedir. Kırsal ya da internet erişiminin zayıf olduğu bölgelerde büyük veri setlerinin transferi ciddi gecikmelere neden olabilmektedir (249). Ayrıca, veri paylaşımı sadece teknik değil, aynı zamanda hukuki ve etik sınırlamalara da tabidir; bu da uluslararası işbirliklerinde ilerlemeyi zorlaştırmaktadır.

Son olarak, büyük sağlık verisinin sürdürülebilir biçimde yönetilmesi için etkili yedekleme ve acil durum planlamalarının yapılması gerekmektedir (28, 247). Donanım arızaları, doğal afetler ya da siber saldırılar sonucunda veri kayıpları yaşanabilmekte; bu da doğrudan hasta güvenliğini tehdit etmektedir (248). Tek bir merkezde depolanan verilerin zarar görmesi hâlinde sistem tümüyle işlevsiz kalabilir. Bu nedenle, verilerin tek bir merkez yerine yerel olarak dağıtılmış yedekleme

sistemlerinde tutulması ve kriz anlarında alternatif erişim yollarının sağlanması önem arz etmektedir.

Tüm bu teknik ve altyapısal sorunlar dikkate alındığında, sağlıkta büyük verinin etkili biçimde yönetilebilmesi için uluslararası veri standartlarının benimsenmesi, birlikte işlerliği destekleyen yazılımların ve çerçevelerin geliştirilmesi, yeni teknolojilerinin güvenli biçimde yaygınlaştırılması, merkezi sistem yerine dağıtık ağ yapılarının kullanılması ve siber güvenlik önlemlerinin sürekli güncellenmesi gerekmektedir. Bu doğrultuda, veri yönetişiminin sağlam bir teknik temele dayandırılması, sağlık hizmetlerinde kalite, erişim ve güvenliği artırmada önemli bir adım olması beklenmektedir.

4 FAIR VERİ PRENSİPLERİ VE ETİK ÇERÇEVE

Veri yönetimine dair etik ve teknik sorumluluklar, dijitalleşmenin hızlanmasıyla birlikte daha görünür hâle gelmiştir. Büyük sağlık verisinin işlenmesinde karşılaşılan teknik ve altyapısal sorunlar, yalnızca teknolojik çözümlerle aşılabilecek geçici engeller değil, aynı zamanda verinin anlamlı, güvenli ve etik kullanımını da doğrudan etkileyen yapısal sınırlardır. Veri formatlarındaki tutarsızlıklar, erişim kontrolündeki eksiklikler ve paylaşım protokollerinin standartlaştırılamaması gibi sorunlar, büyük verinin potansiyelinden tam anlamıyla yararlanılamamasına neden olmaktadır. İşte bu noktada, veri yönetimine sadece teknik değil, aynı zamanda ilkesel bir çerçeveyle yaklaşmak gerekmektedir.

Bu bağlamda, özellikle son yıllarda araştırma verilerinin paylaşımı, erişimi ve yeniden kullanımı konusunda bir dizi ilke geliştirilmiştir. FAIR ilkeleri (Findable, Accessible, Interoperable, Reusable – Bulunabilir, Erişilebilir, Birlikte Çalışabilir, Yeniden Kullanılabilir), veri yönetiminde benimsenen en yaygın çerçeve hâline gelmiştir. Ancak bu ilkeler, veriye dair etik ve teknik standartları belirleyen ilk girişim değildir. FAIR'a benzer biçimde veri yönetimine yön veren başka ilkeler de bulunmaktadır.

Bunlardan ilki, kamu verilerinin şeffaflık temelinde paylaşımını önceleyen Açık Veri İlkeleridir (Open Data Principles). Özellikle ABD ve Avrupa Birliği tarafından geliştirilen bu yaklaşım, verilerin yeniden kullanılabilir ve makineler tarafından okunabilir biçimde sunulmasını savunur (250). Bunun yanı sıra, yerli topluluklara ait veriler üzerinde hak temelli bir yaklaşım geliştiren CARE Prensipleri (Collective Benefit, Authority to Control, Responsibility, Ethics; Kollektif Yarar, Kontrol Yetkisi, Sorumluluk, Etik) veri yönetimine sosyal adalet boyutunu dahil eder. Özellikle yerli halklara ait genetik, kültürel veya çevresel verilerin kullanımında etik bir çerçeve sunar (251).

FAIR prensiplerine tamamlayıcı nitelikte geliştirilen bir diğer yaklaşım da TRUST Prensipleridir (Transparency, Responsibility, User Focus, Sustainability, Technology; Şeffaflık, Sorumluluk, Kullanıcı Odaklı, Sürdürebilirlik, Teknoloji). Bu

ilkeler, güvenilir veri arşivlerinin yönetimine odaklanır (252). Klinik araştırmalarda ise veri güvenilirliğini önceleyen ALCOA+ İlkeleri (Attributable, Legible, Contemporaneous, Original, Accurate + Complete, Consistent, Enduring, Available) uzun süredir kullanılmaktadır. Atfedilebilirlik, okunabilirlik, zamanında kayıt, doğruluk gibi unsurlar bu yaklaşımın temelini oluşturur (253).

Her ne kadar veri yönetimi alanında farklı ilkeler ve rehberler geliştirilmiş olsa da, FAIR prensipleri günümüzde en çok kabul gören, en geniş kapsama sahip ve en yaygın biçimde uygulanan yapı hâline gelmiştir. Bu durumun birkaç temel nedeni bulunmaktadır.

Öncelikle FAIR ilkeleri, yalnızca teknik veri standartlarını belirlemekle kalmaz; aynı zamanda verinin etik kullanımına ilişkin beklentilere de yanıt verir. Verilerin bulunabilir, erişilebilir, birlikte çalışabilir ve yeniden kullanılabilir olması, bilimsel şeffaflığı ve hesap verebilirliği desteklerken (254), aynı zamanda araştırma etiğinin temel ilkeleriyle de örtüşmektedir. Bu yönüyle FAIR, teknik ve etik boyutları birlikte ele alan bütüncül bir çerçeve sunar.

FAIR prensiplerinin bu denli yaygınlaşmasının bir diğer önemli nedeni ise disiplinlerarası uyumluluğudur. Sağlık bilimlerinden çevre araştırmalarına, sosyal bilimlerden mühendisliğe kadar pek çok farklı alanda kolaylıkla uygulanabilmesi, bu ilkeleri evrensel kılan önemli bir özelliktir (255).

Ayrıca FAIR, açık bilim politikalarıyla da doğrudan örtüşmektedir (256). Özellikle Avrupa Açık Bilim Bulutu (European Open Science Cloud – EOSC) gibi girişimlerin FAIR uyumluluğunu zorunlu tutması, bu ilkelerin kurumsal düzeyde benimsenmesini hızlandırmıştır (257). Bu gelişmelerin arkasında yalnızca bilimsel gerekçeler değil, aynı zamanda politik ve ekonomik etkenler de bulunmaktadır. Horizon 2020, NIH (National Institutes of Health) ve Wellcome Trust gibi önde gelen ulusal ve uluslararası fon kuruluşları, FAIR uyumlu veri yönetimi planlarını fonlama süreçlerinde bir gereklilik olarak tanımlamıştır (258). Böylece FAIR, sadece önerilen değil, uygulamaya geçirilen bir standart hâline gelmiştir.

Son olarak, FAIR ilkelerinin geliştirilme sürecinin merkeziyetçi bir yapıya dayanmaması, yani araştırmacıların, kurumların ve veri yöneticilerinin bu sürece doğrudan katılabilmesi, ilkelere olan sahiplenmeyi artırmıştır. Bu katılımcı yapı, FAIR'ın yalnızca bir standart değil, aynı zamanda kolektif biçimde inşa edilmiş bir etik-teknik çerçeve olarak benimsenmesini sağlamıştır.

Bilimsel verilerin daha erişilebilir, şeffaf ve yeniden kullanılabilir hâle getirilmesini amaçlayan FAIR ilkeleri, 2016 yılında Wilkinson ve arkadaşları tarafından yayımlanan bir makale aracılığıyla bilim dünyasına kazandırılmıştır. Bu ilkeler, dijital bilimsel verilerin Findable (Bulunabilir), Accessible (Erişilebilir), Interoperable (Birlikte Çalışabilir) ve Reusable (Yeniden Kullanılabilir) olmasını hedeflemektedir. FAIR ilkeleri yalnızca veri yönetimiyle sınırlı kalmayıp, aynı zamanda yazılım, algoritmalar, protokoller ve bilimsel yayınların da bu standartlara uygun şekilde düzenlenmesini teşvik etmektedir (254).

FAIR terimi ilk kez 2014 yılında Hollanda'da, Lorentz Center (Leiden Üniversitesi) tarafından düzenlenen bir çalıştayda ortaya atılmıştır. Bu çalıştay, farklı bilim alanlarından gelen araştırmacıları bir araya getirerek dijital verilerin etkin biçimde yönetilmesi ve paylaşılması konusunda ortak bir çerçeve geliştirmeyi amaçlamıştır. Bu çerçevede FAIR ilkelerinin taslağı oluşturulmuş, ardından Wilkinson ve arkadaşları tarafından bu ilkelerin sistematik biçimde açıklanmasıyla FAIR ilkeleri resmiyet kazanmıştır (259).

FAIR ilkelerinin oluşturulması ve geliştirilmesi, Barend Mons'un öncülüğü ve geniş bir bilimsel topluluğun ve paydaşların ortak çabaları sonucunda gerçekleşmiştir (259). FAIR makalesinin yazarları disiplinlerarası bir yapıya sahiptir ve farklı ülkelerden bilim insanlarını bir araya getirmektedir. Makalenin birinci yazarı olan Mark D. Wilkinson, İspanya'daki Centro de Biotecnología y Genómica de Plantas (CBGP)'da görev yapan bir biyoinformatik uzmanıdır. Diğer yazarlar arasında Hollanda, İngiltere, Almanya, Fransa, Kanada ve Amerika Birleşik Devletleri'nden gelen uzmanlar yer almaktadır. Katılımcıların uzmanlık alanları arasında biyoinformatik, yapay zekâ, veri yönetimi, bilişim sistemleri, açık bilim politikaları ve yaşam bilimleri gibi birçok farklı disiplin yer almaktadır (259). Bu çeşitlilik, FAIR

ilkelerinin sadece teknik bir düzenleme olmadığını; aynı zamanda farklı bilimsel alanlara ve paydaşlara hitap eden evrensel bir yaklaşım sunduğunu göstermektedir.

FAIR ilkeleri, kısa sürede Avrupa başta olmak üzere birçok bölgede araştırma veri politikalarının temelini oluşturmaya başlamıştır. Özellikle Avrupa Komisyonu, Horizon 2020 ve devamı niteliğindeki Horizon Europe gibi büyük araştırma fonlama programlarına FAIR ilkelerini entegre ederek, bu ilkelerin geniş çapta benimsenmesini sağlamıştır (258). Avrupa Komisyonu'nun 2018 yılında yayımladığı "Turning FAIR into Reality (260)" (FAIR'i Gerçeğe Dönüştürmek) başlıklı rapor, bu sürecin önemli dönüm noktalarından biridir (260). Söz konusu rapor, Avrupa Açık Bilim Bulutu (European Open Science Cloud – EOSC) kapsamında veri yönetimi stratejilerinin FAIR ilkelerine göre yapılandırılmasını önermektedir (257).

FAIR ilkelerinin benimsenmesini destekleyen bir diğer önemli yapı ise GO FAIR girişimidir. 2017 yılında Hollanda, Almanya ve Fransa tarafından başlatılan GO FAIR (Global Open FAIR) girişimi, FAIR ilkelerinin uygulamaya geçirilmesini destekleyen bir uygulama ağı (implementation network) oluşturmayı hedeflemiştir (254). Bu girişim, araştırmacı toplulukları, kurumlar, veri sağlayıcıları ve politika yapıcılar arasında iş birliği sağlayarak, FAIR ilke ve standartlarının farklı bilimsel disiplinlere entegre edilmesini kolaylaştırmıştır (259).

Başlangıçta yaşam bilimleri alanında yaygın olarak uygulanmaya başlanan FAIR ilkeleri, günümüzde sağlık, çevre, sosyal bilimler ve mühendislik gibi farklı alanlarda da geniş kabul görmüştür (261). Küresel düzeyde birçok üniversite, araştırma merkezi, bilimsel yayınevi ve fon sağlayıcı kuruluş, veri yönetimi ve paylaşım politikalarını FAIR ilkeleri doğrultusunda yeniden yapılandırmaktadır. FAIR ilkeleri, yalnızca teknik bir düzenleme değil, aynı zamanda bilimsel bilginin etik ve sürdürülebilir paylaşımı açısından da önemli bir paradigma değişimini temsil etmektedir (256).

FAIR ilkeleri, özellikle sağlık gibi yüksek düzeyde hassasiyet gerektiren alanlarda veri yönetişimini daha etik ve paylaşılabilir kılmak için önemli bir zemin oluşturmaktadır. Bu bölümde ele alınacak olan FAIR Veri Prensipleri, verinin sadece erişilebilirliğini ve paylaşımını değil, aynı zamanda etik sorumlulukla yeniden kullanılabilirliğini de esas alan bütüncül bir yaklaşım sunmaktadır. Bu ilkelerin,

özellikle merkeziyetçi ve kapalı sistemlerin yol açtığı etik risklere karşı şeffaf, birlikte çalışabilir ve kullanıcı odaklı bir veri altyapısının inşasında nasıl işlevsel olabileceği tartışılacaktır.

4.1 FAIR Prensipleri

Sağlık alanında büyük veriyle ilgili sorunlar yalnızca sahada karşılaşılan zorluklarla sınırlı değildir. Bunun yanı sıra, toplanan büyük hacimli ve çeşitli yapıdaki verilerin dijital ortamda nasıl etkin bir şekilde kullanılacağı ve hangi ilkelerin benimsenmesi gerektiği de önemli bir tartışma konusudur. Veri dünyasında, araştırmacıların verileri bulabilmesi, bunlara erişebilmesi, birlikte çalışabilirliklerini sağlaması ve sürdürülebilirliğini garanti altına alması oldukça güç bir süreçtir.

Merkezi sistemlerde toplanan veriler, güvenlik ihlalleri yaşanma endişesi nedeniyle erişim kısıtlamalarına tabi tutulmakta, bu da araştırmacıların verilere ulaşmasını zorlaştırmaktadır (262). Bunun yanı sıra, farklı ülkelerde yürürlükte olan veri koruma mevzuatları arasındaki uyumsuzluk, araştırmacıların verileri yalnızca belirli kurallar çerçevesinde ve sınırlı bir biçimde kullanabilmesine neden olmakta, böylece büyük verinin sağlayabileceği potansiyel fayda azalabilmektedir. Ayrıca, verilerin depolanması ve işlenmesi sürecinde farklı formatların kullanılması hem makineler hem de insanlar için veriye erişimi zorlaştırarak, insan yararı ve etik ilkeler doğrultusunda etkin kullanımının önüne geçmektedir (28).

Bu durumda veri paylaşımı ve yönetimi bilimsel ilerlemenin sürdürülebilirliği açısından stratejik bir öncelik haline gelmiştir. Veriler, tek kullanımlık unsurlar olmadığından, bilimsel araştırmalar ve analizler için temel bir kaynak niteliğindedir. Bu nedenle, araştırmacıların ve sağlık profesyonellerinin bu kaynağı etkin bir şekilde kullanabilmesi ve uzun vadede erişilebilir kılabilmesi, gelecek nesillerin sağlığına ve bilimsel gelişmelere katkı sağlayacaktır.

Veri paylaşımı ve yönetimi, yalnızca teknik süreçlerin optimize edilmesiyle sınırlı kalmayıp; aynı zamanda güçlü bir altyapının inşası, araştırmacılar için açık erişimin sağlanması ve verinin yeniden kullanımını teşvik eden sürdürülebilir modellerin geliştirilmesi gibi unsurları da içermelidir. Açık bilim (Open Science) yaklaşımı, bu

bağlamda önemlidir. Açık bilim, bilimsel bilginin şeffaf, erişilebilir ve tekrar kullanılabilir olmasını hedefleyerek, bilginin yalnızca belirli paydaşlar tarafından değil, daha geniş bir bilim topluluğu ve toplum tarafından da etkin bir biçimde kullanılmasını sağlamaktadır (263). Bu paradigma değişimi, bilimin yalnızca sınırlı gruplar arasında değil, küresel düzeyde paylaşılan kolektif bir çaba olarak ilerlemesine katkıda bulunmaktadır.

FAIR İlkeleri, bilimsel araştırma çıktılarının bulunabilirliğini, erişilebilirliğini, birlikte çalışabilirliğini ve yeniden kullanılabilirliğini sağlamayı amaçlayan; Açık Bilim (Open Science) yaklaşımının gerekliliklerini karşılamaya yönelik geliştirilmiş bir veri yönetimi ilkeleri bütünüdür (256). Bu ilkeler bütünü, veri bağlamında ortaya çıkan zorlukların üstesinden gelmek üzere tasarlanmıştır. Çünkü Açık Bilim'in hedeflerine ulaşmak için büyük miktarda bilimsel veri ve meta verinin depolanması, işlenmesi ve sorgulanması gerekmektedir. Açık Bilim, bilimsel yayınlar, veriler ve metodolojiler gibi araştırma çıktılarının ücretsiz olarak erişilebilir ve kullanılabilir olmasını hedefler. FAIR İlkeleri ise, bu hedefe ulaşmak için veri paylaşım depolarının benimsemesi gereken bir dizi standardı tanımlar. Bu ilkeler, verinin ve üst (meta) verinin bulunabilir, erişilebilir, birlikte çalışabilir ve yeniden kullanılabilir olmasını sağlar. Bu bağlamda, FAIR prensipleri, verinin evrensel değerini ve araştırmalardaki rolünü dönüştüren bir yol haritası sunarak, verilerin araştırmacılar tarafından kolayca bulunabilmesi ve bilimin ilerleyişinde veri kullanımı için uygulanabilir bir çerçeve sunmaktadır. FAIR, verinin erişilebilirliğini ve şeffaflığını arttırmayı, araştırmacılara veriye dair anlayış kazandırmayı amaçlarken, verinin küresel bir bilimsel ekosistemde paylaşılarak daha geniş bir kitleye ulaşmasına olanak tanır. Bu prensiplerin her biri, verinin yalnızca bulunabilir olmasını değil, aynı zamanda çok çeşitli platformlarda etkili bir şekilde kullanılabilir olmasını sağlamak için tasarlanmıştır (254). FAIR, yalnızca veriyi değil, aynı zamanda bilimsel süreçleri dönüştürmeyi vaat eden, disiplinler arası işbirliğini güçlendiren ve bilimsel ilerlemeyi hızlandırır (259).

Günümüzde veri yönetiminin etkinliğini artırmak amacıyla geliştirilen FAIR veri yönetimi ilkeleri, bilimsel verilerin daha etkili, erişilebilir ve sürdürülebilir bir biçimde kullanılmasını sağlamayı hedefler. Bu ilkeler, verilerin Bulunabilirlik (Findability),

Erişilebilirlik (Accessibility), Birlikte Çalışabilirlik (Interoperability) ve Yeniden Kullanılabilirlik (Reusability) özelliklerini taşımasını amaçlar.

Bulunabilirlik (Findability)

FAIR ilkelerinin temel taşı olan Bulunabilirlik**,** verilerin ve ilgili meta verilerin dijital ortamda kolayca keşfedilebilir olmasını ifade eder. Bu, verinin yalnızca var olması değil; sistemli, indekslenmiş ve makine-insan etkileşimiyle kolaylıkla bulunabilir olması anlamına gelir. Bulunabilirliğin sağlanabilmesi için veriye eşsiz ve kalıcı bir tanımlayıcı (Persistent Identifier - PID), genellikle bir DOI, atanması gerekir (259). Aynı zamanda, veriyle ilişkili açıklayıcı ve standartlaştırılmış meta verilerin varlığı şarttır (254).

Bulunabilirlik ilkesinin amacı, veriye dair ilk temasın kolaylıkla kurulmasını sağlamaktır. Meta veri kullanımı, verinin içeriğine dair ön bilgi sunar ve kullanıcıyı - özellikle araştırma ortamlarında - karar verme sürecinde destekler (264). Bu nedenle, yalnızca veri değil, meta veri de indekslenebilir olmalıdır (265).

Şekil 3. Bulunabilirlik İlkesi Özellikleri

Bulunabilirlik, sonraki ilkelerin (özellikle Erişilebilirlik) ön koşuludur; çünkü bir veriye erişebilmek için önce onun bulunabilir olması gerekir.

Erişilebilirlik (Accessibility)

Bir verinin bulunabilir olması, onun erişilebilir olduğu anlamına gelmez. Erişilebilirlik, veriye ve meta veriye uygun koşullar altında erişimin sağlanabilir olmasını ifade eder. Bu erişim, hem insanlar hem makineler için mümkün olmalıdır (259). FAIR ilkeleri, erişimin her zaman açık olması gerektiğini söylemez; ancak erişim koşullarının açıkça tanımlanmasını talep eder. Örneğin, veriye yalnızca belirli izinlerle erişilebiliyorsa, bu durum meta veri düzeyinde açıklanmalıdır (255).

Erişilebilirlik aynı zamanda veri bütünlüğünü ve sürdürülebilirliğini de kapsar. Eğer asıl veri artık mevcut değilse bile, meta veriler erişilebilir olmaya devam etmelidir (254). Bu, bilimsel şeffaflık ve izlenebilirlik açısından önemlidir.

Şekil 4. Erişebilirlik İlkesi Özellikleri

Erişilebilirlik, bir sonraki ilke olan Birlikte Çalışabilirlik için zemin oluşturur; çünkü birlikte çalışabilir sistemlerin birbirine erişebilmesi teknik olarak mümkün olmalıdır.

Birlikte Çalışabilirlik (Interoperability)

Veri yalnızca erişilebilir değil, aynı zamanda diğer veriler ve sistemlerle birlikte çalışabilir olmalıdır. Birlikte çalışabilirlik, verilerin hem insanlar hem de makineler tarafından yorumlanabilir biçimde organize edilmesini ifade eder. Bu kapsamda, veri

ve meta veri, ortak ontolojiler, kontrollü sözlükler ve açık standartlar kullanılarak yapılandırılmalıdır (Boeckhout (259, 261).

Bu ilke, çok-disiplinli araştırmalarda hayati öneme sahiptir. Çünkü farklı araştırma alanlarından gelen veriler ancak anlamca ve teknik olarak uyumlu olduklarında birleştirilebilirler (264). Birlikte çalışabilirlik, örneğin biyomedikal veriler ile çevresel verilerin entegre edilmesi gibi karmaşık veri analizlerini mümkün kılar.

Şekil 5. Birlikte Çalışabilirlik İlkesi Özellikleri

Ayrıca birlikte çalışabilirlik, verinin yeniden kullanılabilirliğini doğrudan etkiler; çünkü anlamlı iş birliği ve analizler, verinin diğer veri kümeleriyle etkileşebilmesine bağlıdır.

Yeniden Kullanılabilirlik (Reusability)

FAIR ilkelerinin nihai hedefi, verinin yeniden kullanılabilirliğini sağlamaktır. Yeniden kullanılabilirlik; verinin yalnızca bir defa değil, farklı bağlamlarda ve kullanıcılar tarafından tekrar tekrar değerlendirilebilmesi anlamına gelir (259). Bunun gerçekleşebilmesi için veri; iyi tanımlanmış, net bir lisansla sunulmuş ve kullanım geçmişi (provenance) açıkça belirtilmiş olmalıdır (265).

Ayrıca, veri ve meta verinin anlamlı, bağlama özgü, eksiksiz ve kaliteli olması gereklidir (255). Bu kalite, yalnızca verinin ilk üretildiği araştırma için değil, sonraki araştırmalar için de güvenilirliğini belirler.

Şekil 6. Yeniden Kullanılabilirlik İlkesi Özellikleri

Yeniden kullanılabilirlik, diğer üç ilkeye doğrudan bağlıdır: Veri bulunamazsa erişilemez, erişilemezse birlikte çalışamaz ve sonuç olarak yeniden kullanılamaz. Bu nedenle yeniden kullanılabilirlik, FAIR ilke sisteminin hem hedefi hem de sınayıcı kriteri olarak değerlendirilebilir (261).

FAIR ilkeleri birbirinden bağımsız değil; birbirini tamamlayan ve destekleyen bir bütün olarak düşünülmelidir. Örneğin, birlikte çalışabilir olmayan bir verinin yeniden kullanılabilirliği zayıf olur; ya da bulunabilir olmayan bir veri, erişilebilirlikten yoksundur. Bu bütünsel yapı, veri yaşam döngüsü boyunca şeffaflık, sürdürülebilirlik ve bilimsel iş birliğini güçlendirir.

Aşağıdaki tabloda, bu ilkeler, her biri için kısa açıklamalar ve örneklerle birlikte özetlenmiştir:

Tablo 1. FAIR İlkeleri

İlke	Tanım	Bileşenler	Örnek
Bulunabilirlik	Veri ve meta verinin makine ve insan tarafından kolayca bulunması	PID, meta veri, indekslenebilirlik	DOI atanmış makale verisi
Erişebilirlik	Veriye belirli koşullarda erişim sağlanabilmesi	Açık erişim, tanımlı lisans, protokol	Lisanslı veri kümesine erişim
Birlikte Çalışabilirlik	Verinin diğer sistemlerle teknik ve anlamsal uyum içinde olması	Ortak ontolojiler, standart veri biçimleri	HL7-FHIR standardı
Yeniden Kullanılabilirlik	Verinin başka amaçlarla tekrar kullanılabilmesi	Açık lisans, açıklayıcı meta veri, veri geçmişi (provenance)	Klinik araştırma için yeniden analiz

FAIR prensiplerinin temel amaçları ise şu şekilde özetlenebilir:

- Veri keşfi ve entegrasyonunu kolaylaştırmak: İnsanlar ve bilgisayar sistemlerinin ihtiyaç duydukları verilere hızlıca ulaşmasını ve analiz edebilmesini sağlamak.

- Bilimsel araştırmada şeffaflığı ve tekrarlanabilirliği artırmak: Veriler, algoritmalar, araçlar ve iş akışlarının erişilebilir olmasını sağlayarak, araştırmaların doğrulanabilirliğini ve yeniden kullanımını desteklemek.

- Veri yönetimi ve depolama uygulamalarını geliştirmek: Veri üreticileri ve yayıncılarına, verilerini FAIR ilkelerine uygun hale getirme konusunda rehberlik ederek iyi veri yönetimi uygulamalarının benimsenmesini teşvik etmek.

- Veri ekosisteminin entegrasyonunu ve uyumunu güçlendirmek: Farklı veri kaynakları ve sistemler arasında birlikte çalışabilirliği artırarak daha bütünleşik bir veri ortamı oluşturmak.

- Bilimsel yayıncılıkta veri nesnelerinin değerini yükseltmek: Dijital veri nesnelerinin bilimsel yayın ekosisteminde temel bileşenler olarak kabul edilmesini sağlayarak, yayınların kalitesini ve etkisini artırmak.

- Mevcut veri kaynaklarının etkin kullanımını sağlamak: Verilerin daha erişilebilir ve yeniden kullanılabilir hale gelmesiyle, araştırma yatırımlarının verimliliğini en üst düzeye çıkarmak.

FAIR prensipleri, belirli bir teknoloji, standart veya çözüm dayatmaz; bunun yerine veri yöneticileri ve yayıncıları için bir rehber görevi görerek, mevcut uygulamaların verileri ne ölçüde FAIR hale getirdiğini değerlendirmelerine yardımcı olur. Farklı teknolojiler ve uygulamalar temelinde bütünleşik ve keşfedici yaklaşımları teşvik etmeyi amaçlar (259).

FAIR tek bir kişinin düşüncesinden ziyade farklı alanlardan birçok paydaş tarafından desteklenmektedir. Bu paydaşlar arasında akademi, endüstri, finansman ajansları (hem kamu hem özel), bilimsel yayıncılar, veri bilimi topluluğu, araştırmacılar, profesyonel veri yayıncıları ve yazılım ile araç geliştiriciler yer almaktadır (261). Finansman ajansları, uzun vadeli veri yönetimine daha fazla önem verirken, veri bilimi topluluğu, mevcut verilerin entegrasyonu ve keşfiyle ilerlemeyi amaçlamaktadır. Bu paydaşlar, veri keşfi ve yeniden kullanımındaki engelleri aşmak suretiyle büyük fayda sağlamaktadırlar. Ayrıca, FAIR prensipleri, veri paylaşımını teşvik ederek araştırmacılara itibar kazandırmak ve veri yeniden kullanımını kolaylaştırmak isteyen araştırmacılar için önemli bir araçtır (255).

4.2 FAIR Prensiplerinin Etik Boyutu

FAIR prensipleri, sağlık verisi yönetiminde etik açıdan son derece önemli bir rol oynamaktadır. Bu prensipler, sağlık verilerinin şeffaf, erişilebilir, güvenli ve yeniden kullanılabilir olmasını sağlayarak bir dizi etik sorunu çözmeye yöneliktir.

İlk olarak, veri erişilebilirliği ve şeffaflık açısından, FAIR prensipleri, verilerin eşit ve adil bir şekilde erişilebilir olmasını garanti eder. Sağlık verilerinin doğru bir şekilde etiketlenmesi ve dijital platformlarda erişilebilir hâle getirilmesi, yalnızca belirli gruplara değil, tüm araştırmacılara ve sağlık profesyonellerine şeffaf bir şekilde veri sunar. Bu durum, verilerin adil bir şekilde kullanılmasını teşvik ederken, aynı zamanda sağlık araştırmalarının ve toplum sağlığının gelişimine katkı sağlar (265). Böylece, verilerin erişilebilirliği sağlanarak, verilerin paylaşılmasının etik ve yasal sorumluluklar doğrultusunda yapılması mümkün hale gelir.

FAIR prensipleri, ayrıca yeniden kullanılabilirlik ilkesini de güçlendirir. Bu prensiplere göre, sağlık verileri sadece bir defa kullanılmak yerine, farklı araştırmalar ve analizler için yeniden kullanılabilir hâle getirilir. Bu, sağlık verilerinin bilimsel araştırmalara daha geniş çapta katkı sağlamasına olanak tanır.

Bir diğer önemli etik mesele, veri izlenebilirliği ve denetim gerekliliğidir. FAIR prensipleri, verilerin izlenebilirliğini sağlayarak, hangi verilerin kimler tarafından kullanıldığını şeffaf bir şekilde denetlemeye olanak tanır (266). Bu, sağlık verilerinin etik denetimini mümkün kılarak, veri suiistimallerinin önlenmesine yardımcı olur. Ayrıca, bu prensipler, sağlık verilerinin kullanılmasının etik sorumluluklara dayalı olmasını sağlar ve veri kullanımına ilişkin net bir denetim mekanizması kurar. Verilerin izlenebilirliği, kullanıcıların veri güvenliğine ve etik kullanımına dair sorumluluklarını yerine getirmelerini teşvik eder.

Son olarak, eşitlik ve adalet konusu, sağlık verisinin paylaşımında kritik bir rol oynar. FAIR prensipleri, sağlık verilerinin farklı sağlık kurumları ve araştırma grupları arasında eşit ve adil bir şekilde paylaşılmasını sağlar. Bu prensipler sayesinde, veriler yalnızca belirli bir grup ya da kurum tarafından tekelleştirilmektense, tüm paydaşlara eşit olarak sunulur. Bu durum, sağlık hizmetlerine erişimdeki eşitsizlikleri azaltır ve daha adil bir sağlık veri yönetimi sistemi yaratılmasına olanak tanır. Verilerin eşit bir şekilde dağıtılması, daha geniş bir araştırma yelpazesi oluşturularak sağlık alanındaki bilimsel işbirliğini teşvik eder.

FAIR prensipleri, sağlık verilerinin etik yönetimi açısından yenilikçi bir çerçeve sunar. Bu prensipler, sağlık verilerinin şeffaflık, gizlilik, yeniden kullanılabilirlik,

izlenebilirlik ve adalet gibi temel etik değerlere dayalı olarak yönetilmesini sağlar (267). Ayrıca, bu prensipler, sağlık verilerinin etik sorumluluklar çerçevesinde kullanılması ve bireylerin haklarının korunması için sağlam bir temel oluşturur. Böylece, sağlık verisi yönetimi daha güvenli, adil ve etik bir hale gelir. Bu da sağlık araştırmalarının toplumsal fayda sağlayacak şekilde yürütülmesine olanak tanır.

Ancak, FAIR prensipleri tek başına sağlık alanında büyük veriyle ilgili etik sorunları çözmez. Büyük veri ekosisteminde bireylerin kişisel sağlık verileri üzerindeki haklarının korunması, yalnızca teknik standartlarla değil, aynı zamanda etik ilkeler ve yasal düzenlemelerle güvence altına alınmalıdır. Bireylerin veri üzerindeki sahiplik haklarını koruma ve bu haklara uygun hareket etme yükümlülüğü, mahremiyet, onam mekanizmaları ve veri paylaşımı gibi konuları kapsayan etik ve yasal yönetmelikler çerçevesinde belirlenir.

FAIR, verinin kimler tarafından, hangi koşullarda ve hangi etik kurallar çerçevesinde kullanılacağını doğrudan düzenlemez. Dolayısıyla, yalnızca FAIR prensiplerine dayanarak bir veri yönetim modeli oluşturmak, bireysel hakları ve mahremiyeti koruma açısından yetersiz kalabilir. Bu nedenle, sağlık verisi gibi hassas bilgilerin yönetiminde, FAIR prensiplerini destekleyen ek etik ve hukuki düzenlemelere ihtiyaç duyulmaktadır (265).

Sağlık verisinin etik bir çerçevede yönetilmesi yalnızca bireylerin mahremiyetini korumak açısından değil, aynı zamanda bilimsel ilerleme ve toplum yararı açısından da büyük önem taşımaktadır. Doğru yönetilen sağlık verisi, hastalıkların daha iyi anlaşılması, kişiselleştirilmiş tıp uygulamalarının geliştirilmesi ve halk sağlığı politikalarının güçlendirilmesi gibi birçok alanda değer yaratabilir. Ancak, bu potansiyelin gerçekleştirilmesi için veri güvenliği, bireylerin rızası ve şeffaflık gibi etik ilkelerin gözetilmesi şarttır.

4.2.1 Bulunabilirlik ve erişilebilirliğin etik yansımaları

Verilerin bulunabilir olması, bilimsel araştırmaların şeffaflığı ve hesap verebilirliği açısından önemlidir. Ancak, veri bulunabilirliği artırıldığında yetkisiz erişim, veri güvenliği ve bireylerin mahremiyet haklarının ihlali gibi etik sorunlar

ortaya çıkabilmektedir. Bu etik sorunlar büyük verinin beraberinde getirdiği sorunlar arasında yerini almaktadır. FAIR veri prensipleri bu verinin etik kullanımı için prensipler ortaya atarak etik sorunlara çözüm önerisi sunmaktadır. Bahsedildiği gibi FAIR'in ilk prensibi Bulunabilirlik (Findability) 'tir. Bu prensip bilimin gelişimini ve insan yararını maksimize etmek için verilerin bulunabilir olmasını savunmaktadır.

Bakıldığında verilerin bulunabilir olması gizlilik ve mahremiyet açısından bir dizi sorunu beraberinde getirmektedir. Ama FAIR'in Bulunabilirlik prensibinden bahsettiği durum verilerin sırf bilimin gelişimi ve insan yararı için apaçık ortada olması değildir. FAIR burada bir denge meselesini çözer. Verilerin mahremiyeti korunarak bulunabilir olmasını kastederek mahremiyet ve insan yararı için bir dengeyi ifade eder. Yani FAIR, bulunabilirliği artırırken mahremiyeti koruyacak önlemler alınmasının gerekliliğinden bahseder. Verilerin yönetimsel zorluklarını ele alırken veri sahiplerinin de haklarının korunması gerektiğini de önemle vurgular. Örneğin; tanımlayıcıların kullanımının (DOI, URI gibi) öneminden ve gerekliliğinden bahseder. Bu tanımlayıcılar sayesinde veri, yetkili kullanıcılar tarafından keşfedilebilir hâle gelir ve anonimleştirilmiş veya sınırlı erişime sahip meta veri kullanımıyla hassas verilerin ifşası engellenir (256).

Tamamıyla açık erişim modelini desteklemek yerine kontrollü erişim modelini sunar aslında. Her verinin herkese açık olması gerektiğini söylemez; bunun yerine veri sahibi veya yöneticiler tarafından belirlenen erişim düzeylerinin uygulanmasını önerir. Örneğin, sağlık verisi için yetkilendirme gerektiren lisanslama modelleri oluşturulmasını savunur. FAIR prensiplerinin sunduğu bu çözümler, şeffaflık ve bilimsel fayda ile bireysel mahremiyeti sağlamaya yardımcı olarak bilimin gelişmesi ve toplum yararı arasındaki dengeyi kurar.

Verilerin sadece bulunabilir olması sorunların çözüldüğü anlamına gelmez. Veriler bulunduğunda etkili bir şekilde kullanılması ve yarar sağlaması için verilere erişilmesi de gerekir. Verilerin erişilebilir olması, bilimsel bilginin yaygınlaştırılması açısından önemlidir. Ancak, hassas veriler için sınırsız erişim sağlanması, mahremiyetin ihlali ve veri kötüye kullanımı gibi riskler doğurabilmektedir. FAIR prensipleri, erişilebilirlik ilkesinin, yalnızca fiziksel erişimden ibaret olmadığını, aynı zamanda etik yönetişim mekanizmalarıyla desteklenmesi gerektiğini savunur (254,

261). Veri erişiminin kontrollü olması ve yalnızca yetkilendirilmiş kişiler tarafından erişilebilir kılınması, hasta mahremiyetini güçlendirir. Bu durumu güçlendirmekle birlikte onam meselesine de bir çözüm önerisi getirir. Verilere kontrollü erişim, bireylerin özerkliğini koruyarak verilerin hem makineler hem de insanlar tarafından kolaylıkla bulunmasını sağlar. Bunu sağlarken etik ilkelere bağlı kalarak kurallar bütününü oluşturur. FAIR ilkeleri hassas veya kişisel olarak tanımlanabilir veriler söz konusu olduğunda bile, veri keşfini kolaylaştırmak için zengin meta verilerin yayınlanmasını ve verilere erişim sürecine ilişkin açık kuralların belirtilmesini savunmaktadır (264).

FAIR ilkeleri verinin erişilebilir olmasını sağlarken etik kaygıları da göz önünde bulundurmayı amaçlar. Ancak, FAIR doğrudan etik bir çerçeve sunmaz; bilimsel ilerleyiş ve insan yararı için veri yönetiminin kurallarını koyarak etik sorunların çözümünü bu kurallar üzerinden yapılması gerektiğini vurgular. Daha çok teknik ve yönetişimsel prensipler belirler.

FAIR'in erişilebilirlik ilkesi, verinin belirli standartlar çerçevesinde erişilebilir olmasını sağlarken, bu erişimin uygun hak yönetimi mekanizmalarıyla düzenlenmesini önerir (263). Örneğin, kişisel sağlık verileri gibi hassas bilgilerin yalnızca yetkili araştırmacılara açılması veya lisanslama mekanizmalarıyla korunması FAIR çerçevesinde mümkündür. Ancak, etik perspektiften bakıldığında, bu erişim mekanizmalarının nasıl tasarlandığı, kimin erişim sağlayacağı ve bireylerin veri üzerindeki kontrol haklarının nasıl korunacağı gibi sorular önem kazanmaktadır.

FAIR'in kendisi veriye etik bir yaklaşım kazandırmaya çalışsa da, bu ilkelerin pratikte nasıl uygulandığı ve yönlendirildiği büyük ölçüde veri yönetimi politikalarına, yasal düzenlemelere ve etik kurullara bağlıdır. Örneğin, bir veri tabanı FAIR prensiplerine uygun şekilde erişilebilir hale getirilmiş olsa da, eğer erişim politikaları etik açıdan adil değilse veya veri sahiplerinin rızasını yeterince gözetmiyorsa, etik ihlaller yaşanabilir.

Bu nedenle, FAIR erişilebilirliği dengeliyor gibi görünse de, verinin etik ilkeler doğrultusunda nasıl erişilebilir kılınacağını belirlemek için ek düzenlemelere, etik kurullara ve veri sahiplerinin haklarını güvence altına alan mekanizmalara ihtiyaç

vardır. FAIR, erişim haklarının yönetilmesini önerirken, bu hakların etik açıdan nasıl şekilleneceği konusunda doğrudan bir çerçeve sunmadığından, erişilebilirlik ilkesinin etik yansımaları, bireylerin haklarını ve bilimsel adaleti güvence altına almak açısından gereklidir.

4.2.2 Birlikte çalışılabilirlik ve gizlilik

FAIR veri prensipleri, araştırma verilerinin daha erişilebilir ve etkili kullanılmasını teşvik ederken, aynı zamanda etik ve hukuki açıdan çeşitli soruları da beraberinde getirmektedir. Özellikle birlikte çalışabilirlik ilkesi, verilerin farklı sistemler ve kurumlar arasında akışını sağlayarak bilimsel iş birliğini güçlendirirken, gizlilik kaygılarını da artırmaktadır. Sağlık verileri gibi hassas veri kategorilerinde, birlikte çalışabilirliğin teşvik edilmesi, "bireylerin mahremiyetini koruma gerekliliği ile nasıl dengelenmelidir" sorusunu gündeme getirmektedir.

FAIR diğer yasal yönetmeliklerden ve etik kurallardan farklı olarak verinin dijital ortamda en etkin şekilde kullanılmasını için oluşturduğu kurallar bütünü, sahadaki yasal yönetmelikler ve etik kurallar nedeniyle bir takım sorunla karşılaşmaktadır. Özellikle gizlilik sorunu verilerin birlikte kullanılabilmesi için engel teşkil etmektedir. Ancak FAIR prensipleri, kişisel sağlık verileri gibi hassas veriler için nasıl bir etik çerçeve oluşturulması gerektiğini söylememektedir**.** Kimin hangi veriye, hangi şartlar altında erişebileceği veya verilerin kötüye kullanımını önlemek için nasıl sınırlandırılması gerektiği gibi konular etik ve hukuki düzenlemelere bırakılmaktadır. Bu yüzden FAIR ilkeleri veri paylaşımını teşvik eden teknik prensipler sunarken*,* bu paylaşımın etik, sosyal ve hukuki boyutları halen tartışmaya açıktır. Özellikle sağlık alanında**,** birlikte çalışabilirliği artırırken bireylerin mahremiyet haklarını nasıl koruyabiliriz? sorusu kritik bir etik mesele olarak karşımıza çıkmaktadır.

FAIR'in araştırmacı odaklı yapısı, araştırmacıların veri paylaşımını ve işbirliğini teşvik etmeyi amaçlar. Ancak bireylerin veri hakları, mahremiyet, etik karar alma süreçleri ve sosyo-politik boyutlar gibi konular FAIR'in kapsamı dışında kalır. Bu nedenle, özellikle sağlık verisi gibi hassas bilgilerin yönetiminde, FAIR prensiplerinin ötesine geçen ek etik çerçevelerin gerekliliği ortaya çıkar.

4.2.3 Yeniden kullanılabilirliğin etik ve yasal sınırları

Verilerin paylaşılabilirliği ve yeniden kullanılabilirliği, özellikle sağlık alanı gibi yüksek etik duyarlılık gerektiren alanlarda, sadece teknik düzenlemelerle değil, aynı zamanda etik ilkeler ve yasal sınırlamalarla da şekillenmektedir. FAIR veri yönetimi ilkeleri kapsamında ele alınan yeniden kullanılabilirlik ilkesi, büyük sağlık verilerinin uzun vadeli bilimsel katkılara hizmet etmesini amaçlarken, bu süreçte bireysel hakların ve veri mahremiyetinin ne ölçüde korunabildiği tartışmaya açıktır.

FAIR veri yönetimi ilkelerinden biri olan yeniden kullanılabilirlik (reusability), verilerin yalnızca bir defaya mahsus değil, etik ve hukuki ilkelere uygun biçimde gelecekteki araştırmalarda da değerlendirilebilmesini öngörmektedir. Ancak özellikle sağlık alanında toplanan kişisel veriler söz konusu olduğunda, bu ilkenin uygulanabilirliği birtakım etik ve yasal sınırlarla karşı karşıya gelmektedir. Zira sağlık verilerinin yeniden kullanımına yönelik her girişim, bireyin mahremiyetinin ve veri üzerindeki kontrol hakkının korunmasıyla doğrudan ilişkilidir.

FAIR ilkeleri, verilerin yeniden kullanımını teşvik ederken, bu kullanımın şeffaf, belgelenmiş ve mümkünse açık lisanslı olması gerektiğini belirtmektedir (254). Ancak bu teknik çerçevenin ötesine geçildiğinde, verinin kimler tarafından, hangi amaçlarla ve hangi koşullarda yeniden kullanılacağı sorusu, etik tartışmaların merkezine yerleşmektedir. Bu noktada, bireyin verisi üzerindeki iradesinin tanınması ve verinin, veriyi üreten öznenin rızası olmaksızın dolaşıma sokulmaması, etik bir zorunluluk olarak ortaya çıkmaktadır.

Ayrıca, kişisel sağlık verilerinin yeniden kullanımı, yalnızca etik değil, aynı zamanda hukuki düzenlemelerle de sınırlandırılmıştır. Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR) ve Türkiye'de 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK), kişisel verilerin açık rıza olmaksızın yeniden kullanılmasını yasaklamakta ve veri işlemenin her aşamasında şeffaflık, veri sahibinin bilgilendirilmesi ve amaçla sınırlılık ilkelerini zorunlu kılmaktadır. Bu bağlamda, FAIR prensiplerinin "yeniden kullanılabilirlik" ilkesinin uygulanması, veri koruma mevzuatlarıyla uyumlu olmak zorundadır. Aksi takdirde, veri paylaşımı bilimsel bir katkıdan çok, etik bir ihlal riskini doğurabilir.

FAIR çerçevesinin gerektirdiği biçimde verinin yeniden kullanılabilir olması, yalnızca verinin teknik olarak erişilebilir olmasını değil, aynı zamanda üst verilerin (metadata) kullanımı açık bir biçimde tanımlamasını da gerektirir. Verinin nereden geldiği, hangi amaçla toplandığı, kimler tarafından hangi koşullarda erişilebileceği gibi bilgiler net olarak belirtilmediği sürece, veri etik açıdan yeniden kullanıma uygun hale getirilemez.

4.3.4 Mahremiyet ve gizlilik bağlamında FAIR prensiplerinin uygulanabilirliği

Büyük veri çağında sağlık verilerinin daha erişilebilir, paylaşılabilir ve yeniden kullanılabilir hale getirilmesi yönündeki çabalar, veri yönetiminde yeni etik ve teknik açılımları da beraberinde getirmiştir. FAIR veri yönetimi ilkeleri - Findable (Bulunabilir), Accessible (Erişilebilir), Interoperable (Birlikte çalışabilir) ve Reusable (Yeniden kullanılabilir) - bu çabaların merkezinde yer almakta ve özellikle araştırma ekosisteminde verinin barındırdığı potansiyel faydanın en iyi şekilde kullanılması ve kullanımının artırılması hedeflenmektedir. Ancak bu ilkelerin pratikte uygulanabilirliği, özellikle sağlık verisi gibi son derece hassas ve kişisel bilgiler içeren alanlarda, mahremiyet ve güvenlik (gizlilik) ilkeleriyle gerilimli bir ilişki içerisindedir. Bireylerin mahremiyet hakkının korunması, kişisel sağlık verilerinin yetkisiz erişime karşı güvence altına alınması ve verinin etik çerçevede yönetilmesi, FAIR ilkelerinin uygulanabilirliğini sınayan temel etik ve hukuki meseleler arasında yer almaktadır.

FAIR ilkeleri, sağlık verilerinin bilimsel araştırmalarda daha etkili kullanılabilmesini sağlamak adına oldukça işlevsel görünmekle birlikte, bireyin özel alanına dair bilgilerin kolayca bulunabilir ve erişilebilir hale gelmesi ciddi mahremiyet ihlalleri riskini de beraberinde getirmektedir. Özellikle açık erişimli veri havuzlarında verinin anonimleştirilmiş olsa dahi tekrar tanımlanabilir hale gelmesi, bireyin üzerindeki kontrolünü kaybetmesi anlamına gelir. Veriler üzerinde mahremiyet ve özerklik hakkı, yalnızca kişisel bilgilerin korunması değil, aynı zamanda bireyin bu bilgiler üzerindeki karar alma gücünü de ifade etmektedir. Bu bağlamda, FAIR ilkelerinin bireysel özerklik ve veri mahremiyetiyle çelişmeden uygulanabilmesi, etik açıdan önemli bir sınav niteliği taşımaktadır.

Gizliliğin korunması noktasında teknolojik çözümler önemli bir rol oynamaktadır. Özellikle anonimleştirme, şifreleme, farklılaştırılmış gizlilik (differential privacy) gibi veri koruma yöntemleri, FAIR ilkeleriyle uyumlu bir veri yönetimi altyapısı inşa etmek açısından umut vericidir. Bununla birlikte, bu tekniklerin her durumda yeterli düzeyde koruma sağlayamadığı da bilinmektedir. Örneğin, çok sayıda veri kümesinin birleştirilmesi yoluyla anonim hale getirilmiş verilerden dahi bireylerin kimliğinin yeniden ortaya çıkarılabileceği gösterilmiştir (268).

FAIR ilkelerinin uygulanabilirliği aynı zamanda hukuki düzenlemelerle olan uyumuna da bağlıdır. Avrupa Birliği'nin Genel Veri Koruma Tüzüğü (GDPR) ve Türkiye'deki 6698 Sayılı Kişisel Verilerin Korunması Kanunu (KVKK), kişisel verilerin işlenmesinde açık rıza, veri minimizasyonu ve amaçla sınırlılık gibi ilkeleri esas alır. Oysa FAIR ilkeleri, verinin yeniden kullanılabilirliğini artırmayı ve farklı bağlamlarda erişime açılmasını teşvik eder. Bu durum, veri sahiplerinin bilgilendirilmiş onamı alınmaksızın verilerinin ikincil amaçlarla paylaşılması ve kullanılması gibi uygulamalara zemin hazırlayabilmektedir. Dolayısıyla, FAIR ile GDPR/KVKK gibi düzenlemeler arasında denge kurulması, uygulamada oldukça dikkat gerektiren bir süreci işaret etmektedir.

Bu durumda, FAIR ilkelerinin mahremiyet ve güvenlik bağlamında uygulanabilirliğini artırmak adına alternatif veri yönetişimi modelleri de gündeme gelmektedir. Özellikle bireyin veri üzerindeki kontrolünü koruyan merkezi olmayan (federe) sistemler ve blokzincir teknolojileri, hem veri paylaşımını kolaylaştırmakta hem de güvenlik risklerini minimize etmektedir. Federe sistemler sayesinde veriler fiziksel olarak tek bir merkezde toplanmaksızın analiz edilebilir; böylece hem FAIR ilkeleriyle uyumlu bir erişilebilirlik sağlanır hem de mahremiyet daha güçlü biçimde korunur. Blokzincir ise şeffaf, izlenebilir ve bireyin onamını içeren veri erişim protokolleriyle bu dengeyi daha sürdürülebilir hale getirebilir

5 BÜYÜK SAĞLIK VERİSİ İÇİN ETİK YÖNETİM VE YENİ TEKNOLOJİ TEMELLİ ÇÖZÜM ÖNERİSİ

5.1 Etik Yönetim İhtiyacı

Günümüzde sağlık verilerinin güvenli ve etik bir biçimde paylaşımı, sağlık hizmetlerinde veri kullanımının yaygınlaşması ve veri odaklı tıbbi ilerlemelere yönelik artan talep doğrultusunda önemli bir meydan okuma haline gelmiştir. Sağlık alanında büyük verinin yaygın biçimde toplanması ve işlenmesi; sağlık hizmetlerinin kalitesinin artırılması, hastalıkların erken tanısının konulması ve halk sağlığının korunması gibi önemli avantajlar sunmaktadır. Ancak bu potansiyel faydalara rağmen, söz konusu verilerin mevcut -özellikle merkeziyetçi - sistemler aracılığıyla yönetilmesi, ciddi etik sorunları da beraberinde getirmektedir. Veri güvenliği, mahremiyet, adalet ve özerklik gibi temel etik ilkeler bu sistemler içerisinde yeterince korunamamakta; bu durum, büyük sağlık verisinin yönetiminde kapsamlı bir etik tartışma zemini doğurmaktadır.

Bu tartışma zemininde bir tarafta bireylerin mahremiyetini korumak ve veri sahiplerinin verileri üzerinde hak sahibi olduğu yer alırken diğer tarafta potansiyel olarak fayda sağlayacak verilerin bilimsel ilerleme, toplum yararı ve araştırmalar için kullanılması gerektiği ve dengenin sağlanması gerekliliği yer almaktadır. Bu dengeyi sağlama ihtiyacı, sağlık hizmetlerinde veri paylaşımına yönelik yaklaşımları yeniden şekillendirmeye aday yenilikçi teknolojilerin gelişimini teşvik etmektedir.

Bir önceki bölümde verilerin araştırmacılar için kolayca bulunabilmesi ve etik bir biçimde kullanılabilmesi için oluşturulan FAIR prensipleri dengenin sağlanabilmesi için yapılması gerekenlerden sadece biridir. Çünkü FAIR veri yönetimi ilkeleri, sağlık verilerinin bulunabilir, erişilebilir, birlikte çalışabilir ve yeniden kullanılabilir olmasını hedefleyen önemli bir çerçeve sunsa da bu ilkelerin uygulama alanında karşılaştığı güçlükler, yalnızca teknik veya yönetsel düzeyde değil; aynı zamanda yapısal ve sistemsel düzeyde de kendini göstermektedir. Özellikle büyük sağlık verisinin hâkim paradigmalardan biri olan merkeziyetçi veri yönetimiyle işleniyor olması, daha önceki bölümlerde ele alınan etik sorunların birçoğunun altyapısal nedenlerinden biri olarak değerlendirilmeye açıktır.

Merkeziyetçi sistemlerde sağlık verileri, ağırlıklı olarak ulusal düzeyde faaliyet gösteren kamu kurumları, sosyal güvenlik mekanizmaları ya da büyük ölçekli sağlık hizmeti sağlayıcıları tarafından toplanmakta ve işlenmektedir (262, 269, 270). Bu veriler, genellikle tekil veya sınırlı sayıdaki merkezi sunucu sistemlerinde depolanmakta; veri erişim ve kullanım yetkileri, çoğu zaman bireyin kendisinden çok, bu yapıların belirlediği politikalar çerçevesinde şekillenmektedir (271). Böyle bir sistemde, bireylerin verileri üzerindeki denetimlerinin sınırlandığı; verilerin, birey bilgisi veya doğrudan onayı dışında da işlenebilme riskinin bulunduğu ileri sürülebilir (262).

Öncelikle, bu sistemler veri gizliliği ve güvenliği açısından riskler barındırmaktadır. Verilerin tek bir merkezde toplanması, yetkisiz erişim, veri ihlali veya kötü niyetli saldırılar gibi tehditlere karşı sistemi savunmasız hale gelmesine neden olabilmektedir. Ayrıca merkezi sistemlerin tek hata noktalarına sahip olması, yani sistemin belirli bir noktasında meydana gelen bir aksaklığın tüm yapıyı etkilemesi, güvenilirliği azaltan ve toplu olarak mahremiyeti ihlal eden bir faktördür (272). Merkezi bir sistemde veri sahiplerinin verileri üzerindeki kontrolü sınırlıdır. Ayrıca, verilerin nasıl korunduğu, hangi süreçlerden geçtiği ve bu verilerin hangi alanlarda fayda sağladığı konusunda net bir bilgi yoktur (273). Yani, verilerin işlenme süreçleri ve güvenliği genellikle şeffaf değildir, bu da güven eksikliği ve belirsizlik yaratmaktadır.

Bütün bu etik sorunların çözülmesi ve sağlık verilerinin bilimsel ilerleme ile mahremiyet arasında uygun bir dengeye kavuşturulması, sağlık alanındaki büyük veriler için yeni bir etik yönetişim modelinin gerekliliğini ortaya koymaktadır. Etik yönetişim, verilerin bireysel hakları ihlal etmeksizin, toplum için faydalı bir şekilde kullanılmasını sağlayan bir çerçeve sunar. Bu çerçeve, bireylerin mahremiyetinin korunmasını, verilerinin güvenli bir biçimde işlenmesini ve verilerden elde edilecek yararın maksimize edilmesini hedeflemektedir. Etik yönetişim eksiklikleri, özellikle veri güvenliği ve şeffaflık gibi konularda ciddi endişelere yol açmakta olup, bu sorunların çözülmesi, veri kullanımının etkinliğini ve toplumun güvenini artıracaktır. Bahsedilen etik problemler ve bu sorunlara yol açan yapısal eksiklikler, sağlık verileri

yönetiminde daha işlevsel ve bütünsel bir etik yaklaşım geliştirilmesini zorunlu kılmaktadır.

5.1.1 Bireysel ve toplumsal açıdan etik veri yönetimi gerekliliği

Büyük sağlık verisi, hem bireysel hem de toplumsal düzeyde önemli fırsatlar ve riskler barındırmaktadır. Bireyler açısından bu veriler, sağlık hizmetlerinin kişiselleştirilmesini ve önleyici tedavi yaklaşımlarının geliştirilmesini mümkün kılarken; toplum düzeyinde epidemiyolojik araştırmalardan sağlık politikalarının şekillendirilmesine kadar geniş bir yelpazede kullanıma olanak tanır. Ancak bu potansiyel faydalar, verinin toplanması, saklanması ve paylaşılmasında etik ilkelerin gözetilmediği durumlarda ciddi sorunlara yol açabilir.

Veri güvenliği, mahremiyetin korunması ve bilgilendirilmiş onam süreçleri, bireylerin temel haklarının bir parçası olarak değerlendirilmelidir. Sağlık verisi yalnızca teknik bir unsur değil; aynı zamanda bireyin kimliği, yaşam tarzı ve hastalık geçmişi gibi oldukça kişisel bilgileri içeren bir bütün olarak ele alınmalıdır. Bu yönüyle sağlık verisinin yönetimi, yalnızca bireysel rızaya dayalı bir süreç olmaktan çıkmakta; toplumsal düzeyde şeffaflık, hesap verebilirlik ve adalet ilkeleriyle birlikte düşünülmesi gereken bir etik sorumluluk haline gelmektedir.

Dolayısıyla büyük sağlık verisinin yönetiminde yalnızca yasal düzenlemelere bağlı kalmak yeterli değildir. Aynı zamanda bu verilerin hangi amaçlarla kullanıldığı, kimler tarafından erişilebildiği ve veriye dair denetim mekanizmalarının nasıl çalıştığı gibi soruların etik bir çerçevede değerlendirilmesi gerekmektedir. Bu bağlamda, etik veri yönetimi ihtiyacı hem bireylerin veri üzerindeki kontrolünü sağlayacak hem de toplumun veri kullanımına yönelik güvenini artıracak sistemlerin geliştirilmesini zorunlu kılmaktadır.

Bireysel açıdan etik veri yönetimin gerekliliği, sağlık verilerinin hassas ve gizli niteliği nedeniyle temel bir zorunluluk haline gelmiştir. Özellikle artan siber güvenlik tehditleri, kişisel sağlık bilgilerinin izinsiz erişim ve kötüye kullanımına açık hale gelmesiyle bireylerin mahremiyetine yönelik ciddi riskler doğurmaktadır (274). Bu durum, veri sahiplerinin kendi sağlık verileri üzerindeki kontrolünü güçlendirecek

mekanizmaların geliştirilmesini gerekli kılmaktadır (275). Nitekim sağlık verilerinin merkezi bir sistemde depolanıyor ve yönetiliyor olması bireysel açıdan etik ilkeleri yeterince yerine getirmediği ve bireyin verisi üzerinde kontrolünün eksik olduğu görülmektedir (276). Bu durumda yeni bir sistem ve gelişen teknolojiyi kullanamaya duyulan ihtiyaç artmakta ve bir zorunluluk haline gelmektedir.

Toplumsal açıdan etik veri yönetim gerekliliği ise, sadece bireylerin değil, toplumun tamamının sağlık sistemine olan güvenini pekiştirme açısından önem arz etmektedir. Merkeziyetçi sistemin şeffaf ve denetlenebilen yapısı olmadığından, sağlık verilerinin kötüye kullanımının önüne geçmek her geçen gün daha da zorlaşmaktadır (277). Daha da zorlaşmasının asıl sebebi merkeziyetçi sistemlerde her ne kadar veriyi korumak için güçlü yöntemler kullanılsa da buna paralel olarak siber saldırılar ve yeni teknolojiler de gelişmekte olup veri ihlalini kaçınılmaz bir hale getirebilmesidir (278).

Toplumsal açıdan, özellikle araştırma ve geliştirme faaliyetlerinde veri bütünlüğünün sağlanması ise bilimsel ilerleme için elzemdir ve bu süreçte güvenilir veri altyapıları ve teknolojiler kullanılarak yeni bir sistemin oluşturulması etik standartların korunmasına da katkı sağlamaktadır (274).

5.1.2 Mevcut sistemlerin yetersizlikleri ve etik riskler

Günümüzde sağlık verilerinin yönetimi büyük ölçüde merkeziyetçi sistemlere dayanmaktadır. Örneğin Türkiye'de E-Nabız gibi dijital sağlık platformları, bireylerin sağlık geçmişini tek bir sistem altında toplayarak erişimi kolaylaştırmakta ve sağlık hizmetlerinin koordinasyonunu artırmayı amaçlamaktadır. Ancak bu gibi merkezi yapılar, beraberinde önemli etik riskleri ve sistemsel yetersizlikleri getirmektedir

Öncelikle, merkezi yapılar bireylerin verileri üzerindeki denetimini sınırlamakta ve veri kontrolünü yalnızca belli kurumların eline bırakmaktadır (272). Bu durum, bireylerin veri üzerinde söz sahibi olma hakkını zayıflatmakta ve bilgilendirilmiş onam ilkesini işlevsiz hâle getirmektedir (279). Bununla birlikte, veri güvenliğine yönelik yaşanabilecek ihlallerde zararın yayılımı çok daha geniş bir alana ulaşabilmekte, yüz binlerce bireyin verisi aynı anda risk altına girebilmektedir (280). Ayrıca merkezi sistemlerde şeffaflık ve hesap verebilirlik çoğu zaman sınırlıdır.

Vatandaşlar verilerinin kimlerle, ne zaman ve ne amaçla paylaşıldığını çoğu zaman bilememekte; bu da kamusal güvenin zedelenmesine yol açmaktadır (276). Bu belirsizlik, sağlık verilerinin araştırma ve politika yapımında kullanımı açısından da etik sorunlar doğurmakta; rıza dışında yapılan kullanımlar bireylerin mahremiyet haklarını ihlal edebilmektedir (52).

Öte yandan merkezi veri yönetim sistemlerini savunan görüşler de mevcuttur. Özellikle Çin ve Rusya gibi devletler, merkezi kontrolün ulusal güvenlik, veri bütünlüğü ve kamu düzeni açısından önemli olduğunu ileri sürmektedir (281) (282). Bu yaklaşımda, verinin devlet tekelinde tutulması sayesinde dış müdahalelere ve özel sektörün aşırı ticari manipülasyonlarına karşı daha güçlü bir koruma sağlanabileceği savunulmaktadır (282).

Merkeziyetçi veri depolama, işleme ve analiz sistemlerinin savunulmasındaki temel gerekçeler, özellikle gelişmekte olan ülkelerde sağlık verilerinin parçalı yapısını aşmayı ve sistematik bir sağlık bilgi altyapısı kurmayı amaçlamaktadır. Bu sistemlerin savunucuları, merkezi elektronik sağlık kaydı (EHR) depoları veya klinik veri ambarları gibi yapılar aracılığıyla hastalık sürveyansının ilerletilebileceğini (283), halk sağlığı araştırmalarının geliştirilebileceğini ve kanıta dayalı politika oluşturmanın daha sağlam bir zemine oturtulabileceğini öne sürmektedir (284). Çeşitli sağlık hizmeti bilgilerinin merkezi bir depoda birleştirilmesi, gelişmiş analitik çalışmalar, popülasyon sağlığı yönetimi ve kamu sağlığına yönelik daha bütüncül yaklaşımlar geliştirilmesi açısından elverişli görülmektedir (285). Ayrıca, hasta bilgileri, laboratuvar sonuçları ve klinik gözlemler gibi farklı kaynaklardan gelen verilerin bir araya getirilmesi sayesinde büyük ölçekli sağlık analizleri mümkün hâle gelmekte; bu da politika yapıcıların daha bilinçli kararlar almasına katkı sağlamaktadır (286). Bu yaklaşımın aynı zamanda, çok kurumlu verilerin gizliliği koruyan bir ortamda konsolide edilmesine imkân tanıdığı ve güvenilir kayıt bağlantısı ile veri birlikte çalışabilirliğini artırarak sistemin ölçeklenebilirliğini desteklediği savunulmaktadır (282).

Bazı görüşler ise, sağlık verilerinin merkezi bir yapıda toplanmasının kamu yararı açısından daha etkin sonuçlar doğurabileceğini savunmaktadır. Bu yaklaşıma göre, merkezi sistemler; kamu sağlığı tehditlerine karşı hızlı müdahale, kaynakların verimli

dağılımı ve ulusal düzeyde tutarlı sağlık politikalarının oluşturulması gibi avantajlar sunar (287). Ayrıca, veri setlerinin tek bir merkezde toplanması sayesinde epidemiyolojik analizlerin daha bütüncül ve hızlı yapılabileceği, böylece sağlık sistemlerinin genel işleyişinin iyileştirilebileceği ileri sürülmektedir (284). Bu çerçevede bireysel gizlilik risklerinin, ulusal sağlık güvenliği ve kamu yararı adına makul sınırlamalarla dengelenmesi gerekir (288).

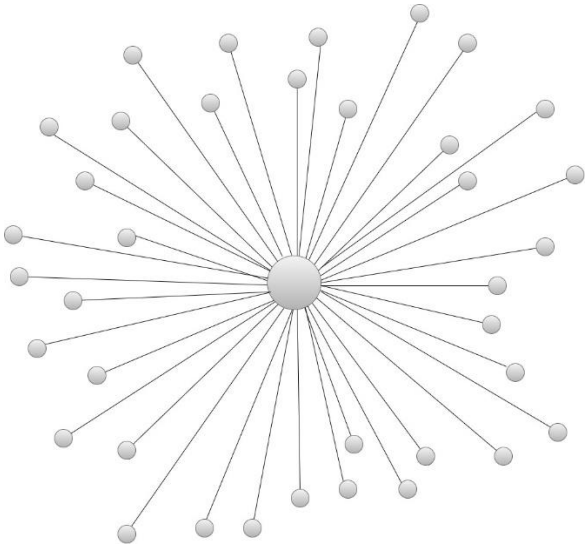
Ancak bu tezde önerilen federe sistem, hem bireyin veri üzerindeki kontrolünü artırmayı hem de güvenlik zaaflarını engelleyecek şekilde teknik ve etik altyapılarla güçlendirilmiş bir model sunmayı amaçlamaktadır. Dolayısıyla bu karşı argümanlar göz önüne alınarak sistemin güvenli, adil ve denetlenebilir biçimde yapılandırılması gerektiği açıktır.

Tüm bu nedenlerle, mevcut sağlık veri yönetim sistemleri etik açıdan yeniden değerlendirilmelidir. Birey haklarını ve toplumsal yararı birlikte gözeten, şeffaf, katılımcı ve güven temelli yeni modellerin geliştirilmesine açıkça ihtiyaç duyulmaktadır. Bu durumda mevcut sistemin zemin hazırladığı etik problemleri bertaraf etmek ya da minimalize etmek için yeni teknolojilerin sunduğu imkanlardan yararlanılması, her şeyden önce zarardan çok yarar sağlayacağı için tercih edilmelidir.

5.2 Merkeziyetçi Sistemlerin Etik Sorunları

Büyük sağlık verisinin merkezi yapılar altında toplanması, bu sistemlerin işlevselliği ve veri bütünlüğü açısından avantajlar sağlasa da, etik açıdan birçok önemli sorunu beraberinde getirmektedir. Veri yönetiminin merkezi aktörler tarafından gerçekleştirilmesi; bireylerin hakları, toplumun güvenliği ve sağlık hizmetlerinin adaletli sunumu gibi birçok boyutta etik riskler oluşturmaktadır.

Bu sorunların temelinde yatan mimariyi somutlaştırmak amacıyla merkeziyetçi sistemin ağ yapısı aşağıda görselleştirilmiştir.



Şekil 7. Merkezi Sistem Ağı

Şekil 7’de de görülebileceği gibi, merkeziyetçi sistemlerde tüm veriler tek bir merkezde toplanmakta ve bu merkez üzerinden yönetilmektedir. Merkeziyetçi sistem, verilerin ve yetkinin tek bir yerde veya tek bir kurumda toplandığı bir yapıdır. Bu tür sistemler genellikle merkezi bir otoriteye dayanır. Mevcut sağlık verisi yönetim sistemlerinin çoğunluğu merkeziyetçidir (272). Şekil 1'deki merkezi sistem ağı, merkeziyetçi sistemlerde tüm sağlık verileri tek bir merkezde toplandığını ve bu merkez üzerinden kontrol edildiğini temsil etmektedir. Verilerin bu şekilde merkezileştirilmesi, beraberinde güç yoğunlaşması ve veri tekelini getirmekte; bu da sistemin hem etkinliğini hem de güvenliğini zayıflatmaktadır. Merkeziyetçilik, büyük sağlık verisinin etik kullanımını sınırlandırmakta, veri erişiminde adaletsizlik yaratmakta ve aynı zamanda olası etik risklerin ortaya çıkmasına zemin hazırlamaktadır.

Merkeziyetçi sistemlerde, doğal afetler veya tıbbi tesis arızaları gibi durumlarda sistemin tamamen çökmesine veya verilere erişimin kesilmesine neden olabilecek tek bir hata noktası bulunur. Günümüzde sağlık verilerinin büyük bir kısmı merkeziyetçi sistemler aracılığıyla toplanmakta, saklanmakta ve işlenmektedir. Bu yapı, veriye dair tüm kontrolün sınırlı sayıda kurumun elinde toplanması anlamına gelmektedir (289). Oysa sağlık verisi gibi mahrem ve hassas bilgi türlerinde, bu durum birçok açıdan etik riskleri beraberinde getirmektedir

Merkeziyetçi sistemin beraberinde getirdiği en önemli etik risklerden ilki mahremiyet ve gizliliktir. Verilerin tek bir merkezde toplanması, bireylerin mahremiyetini tehdit eden önemli bir yapısal sorundur. Özellikle sağlık alanında, bireylere ait tanı, tedavi geçmişi, genetik veriler gibi son derece özel bilgilerin merkezi bir havuzda tutulması, bu sistemlerin hedef haline gelmesine neden olmaktadır (151). Bu da hem siber saldırı riskini artırmakta hem de olası veri ihlallerinde çok sayıda bireyin aynı anda zarar görmesine yol açmaktadır (171). Ayrıca merkezi sistemlerde, bireylerin kimliklerinin anonimleştirilmiş olsa bile çeşitli yöntemlerle tekrar tanımlanabilmesi mümkündür (290). Bu durum, bireyin mahremiyetinin gerçek anlamda korunamadığını göstermektedir.

Diğer etik risk ise adalet ve eşitliktir. Merkeziyetçi yapılarda, verilere erişim ve kullanım hakkı belirli kurumların tekelinde olabilmektedir. Bu durum, bilimsel çalışmalarda fırsat eşitliğini zedelemekte; veriyle çalışan araştırmacılar, kurumlar arası eşitsizliklerle karşı karşıya kalmaktadır (291). Ayrıca merkezi veri sistemleri, toplumun belirli gruplarına (örneğin azınlıklar, dezavantajlı bölgelerde yaşayanlar) dair verilerin eksik veya hatalı toplanmasına yol açabilmekte, bu da sağlık hizmetlerinin planlanmasında adaletsiz sonuçlara neden olabilmektedir. Yapay zekâ uygulamaları gibi veri temelli karar destek sistemleri de bu eşitsizlikleri çoğaltma riskine sahiptir (292).

Özerklik, veri sahipliği ve onam durumları da merkeziyetçi sistemlerde etik risk olarak değerlendirilmektedir (210). Bireylerin ürettikleri verilere erişim ve kontrolünün olmaması “verinin sahibi kim” sorusunu akıllara getirmektedir. Merkezi sistemlerde veriyi kontrol eden birey olmadığından, etik ilkelerden önemli bir yer kaplayan özerklik ilkesi de merkeziyetçi sistemin oluşturduğu riskle karşı karşıya kalmaktadır. Veri özerkliği, bireyin kendi verisi üzerinde söz sahibi olabilmesini ifade eder. Oysa merkezi sistemlerde, bireylerin verilerinin ne zaman, kimlerle ve hangi amaçlarla paylaşıldığına dair etkin bir kontrolü çoğu zaman mümkün olmamaktadır. Bu durum, bilgilendirilmiş onam ilkesini zayıflatmakta, hatta kimi zaman tamamen geçersiz kılmaktadır. Sonuç olarak bireylerin veri üzerindeki özneleşmiş hakları silikleşmekte, sadece veri üreticisi değil, aynı zamanda veri öznesi olan bireylerin iradesi göz ardı edilmektedir.

Merkeziyetçi veri sistemleri, yarar-zarar ilkesi açısından değerlendirildiğinde de ciddi etik sorunlar barındırmaktadır. Verilerin bilimsel ilerleme, toplumsal fayda ve birey yararına önemli katkılar sunma potansiyeline rağmen etkin biçimde kullanılamaması, bu potansiyelin göz ardı edildiğini göstermektedir. Dahası, söz konusu sistemlerin mahremiyet ihlallerine zemin hazırlayan yapısı, bireylerin zarar görme riskini artırmakta ve böylece yarar-zarar dengesini olumsuz yönde etkilemektedir. Bu tür sistemlerde veriye dayalı bilimsel araştırmalarda da çeşitli zorluklar ortaya çıkmaktadır. Büyük veri kümeleri çoğunlukla kamuya açık değildir ve belirli kurumların kontrolü altında tutulmaktadır. Bu durum, özellikle bağımsız ya da sınırlı bütçeye sahip araştırmacılar açısından veri erişiminde ciddi engeller yaratmakta; böylece bilimsel bilginin demokratikleşmesini sınırlandırmaktadır. Ayrıca, merkezi sistemlerde verilerin nasıl toplandığı, işlendiği ve sunulduğu süreçlerde şeffaflık eksiklikleri yaşanabilmekte; bu da bilimsel bulguların nesnelliğini ve güvenilirliğini zedeleyen bir ortam yaratmaktadır.

5.2.1 Mahremiyet ve güvenlik açıkları

Merkeziyetçi sağlık veri sistemleri, kapsamlı bir veri kontrolü sağlama amacıyla yapılandırılsa da, güvenlik ve mahremiyet açısından çeşitli riskleri beraberinde getirmektedir. Bu sistemler, verilerin belirli kurumlar ya da otoriteler tarafından merkezi biçimde depolandığı ve işlendiği yapılardır. Ancak bu yapı, güvenlik açıkları ve birey mahremiyetine yönelik tehditler açısından ciddi etik sorunlar doğurabilmektedir (293).

Merkezi sistemlerde tüm verilerin tek bir platformda toplanması, bu verileri siber saldırılara karşı son derece savunmasız hâle getirmektedir. Verilerin bütünlüğü, gizliliği ve güvenliği sağlanamadığında bireylerin sağlık geçmişleri, genetik bilgileri ve tedavi öyküleri gibi son derece hassas bilgiler kötü niyetli kişilerin eline geçebilmektedir (294). Bu tür ihlaller sadece kişisel zararlara değil, kamu sağlığına olan güvenin zedelenmesine de neden olmaktadır.

Mahremiyet açısından bakıldığında, merkezi sistemler çoğu zaman veri sahiplerinin rızasına dayalı kontrolünü zayıflatmakta ve kişisel sağlık verilerinin üçüncü taraflarla paylaşımında şeffaflık eksikliği yaratmaktadır. Bireylerin verilerinin

kimlerle paylaşıldığını, hangi amaçlarla kullanıldığını bilememesi mahremiyetin özüne aykırıdır (151).

Örneğin 29 Nisan 2025 tarihinde Courier-Mail gazetesinin yayımladığı bir habere göre, Avustralya Queensland'de faaliyet gösteren bir patoloji hizmeti sunucusunun, hastaların bilgisi ve onayı olmaksızın sağlık verilerini yurt dışındaki çağrı merkezlerine aktardığı ortaya çıkmıştır. Bu durum, federal ve eyalet düzeyindeki gizlilik düzenleyicilerinin soruşturma başlatmasına neden olmuştur. Haberde, Dr. Thomas Lyons adlı bir hekimin, büyük bir patoloji hizmeti sunucusuna yapılan çağrıların artık Malezya'dan yanıtlandığını fark etmesi üzerine endişelerini dile getirdiği belirtilmiştir. Avustralya Gizlilik Yasası 1988 ve Avustralya Gizlilik İlkeleri kapsamında, sağlık verileri "hassas bilgi" olarak sınıflandırılmakta ve özellikle uluslararası transferlerde sıkı kontroller gerektirmektedir. Şirketlerin, yabancı kuruluşların Avustralya gizlilik standartlarına uymasını sağlaması veya hastalardan açık rıza alması gerekmektedir. İhlaller, şirketler için 2,1 milyon dolara kadar para cezası ile sonuçlanabilir (295). Bu durum, veri transfer süreçlerinde etik dışı uygulamaların merkezi ve şeffaf olamayan sistemlerde daha kolay gizlenebileceğini göstermiştir.

Tüm bu durumlar, merkeziyetçi sistemlerin güvenlik açıkları ve mahremiyet ihlalleri yoluyla bireysel ve toplumsal zararları artırabileceğini göstermektedir. Bu bağlamda, sağlık verilerinin yönetiminde daha şeffaf, dağıtık ve birey odaklı sistemlerin geliştirilmesi etik bir zorunluluk hâline gelmiştir.

5.2.2 Merkezi veri kontrolü ve etik kısıtlar

Merkeziyetçi sistemlerin etik açıdan diğer sorunlu noktası, veri yönetiminin yalnızca belirli kurumlar veya devlet otoriteleri tarafından yürütülmesi, bireylerin verileri üzerindeki tasarruf haklarını sınırlandırılmasıdır. Bu tür sistemlerde bireyler çoğu zaman verilerinin kimler tarafından görüntülendiğine ya da ne amaçla kullanıldığına dair bilgi sahibi olamaz. Bireyler sürekli olarak veri üretir ve bu veriler sistem üzerinden kayıt altına alınır (272). Ayrıca, merkezi sistemlerde karar alma süreçleri şeffaf olmaktan uzaklaştıkça, etik ilkelere uygun veri kullanımı

sağlanamayabilir. Bu durum, bilgilendirilmiş onamın işlevsizleşmesine ve bireyin özerkliğinin ihlaline neden olmaktadır (275).

Merkeziyetçi veri yönetim sistemlerinde kontrolün tek bir otoriteye ait olması, veri sahipliği, işlem yetkisi ve şeffaflık gibi temel etik ilkeler açısından çeşitli kısıtlar doğurmaktadır (296). Bu yapılarda, "Veri üzerinde düzenleme, silme ve paylaşım yetkisi kimdedir?", "Verinin sahibi birey midir yoksa yalnızca üreticisi midir?" gibi sorular gündeme gelmektedir.

Karar alma süreçlerinin merkezi bir yapı tarafından yürütülmesi, veri sahibinin bilgilendirilmiş onam sürecine aktif biçimde katılımını sınırlayabilmekte; bireyin verisi üzerindeki denetimi sembolik düzeyde kalabilmektedir. Bu durum, başta mahremiyet, özerklik ve adil kullanım olmak üzere temel etik ilkelerin ihlal edilmesine zemin hazırlamaktadır. Ayrıca, merkezi sistemlerde şeffaflık ve hesap verebilirlik mekanizmalarının sınırlı olması, etik denetimi güçleştirmekte ve veri üzerindeki güç asimetrisini artırmaktadır (273, 279).

5.2.3 Erişim eşitsizliği ve adalet problemleri

Merkeziyetçi sistemler, dijital hizmetlere erişimi kısıtlı grupların sistem dışında kalmasına neden olabilmektedir (297). Özellikle kırsal bölgelerde yaşayan, düşük gelirli ya da dijital okuryazarlığı düşük bireyler için sağlık verisi yönetimine erişim hem teknik hem de bilgi eksikliği nedeniyle sınırlı kalmaktadır (298). Bu durum, sağlık verisinin üretimi ve kullanımında belirli grupların dışlanmasına ve sistemin adalet ilkesinden uzaklaşmasına yol açmaktadır. Ayrıca, veri eksikliği yaşayan bu bireyler gelecekte kişiselleştirilmiş sağlık hizmetlerinden daha az faydalanabilmekte, bu da eşitsizlikleri pekiştirmektedir (280).

Ek olarak, sağlık verilerinin sınırlı kurumların elinde tutulması, veriye erişimde ciddi eşitsizlikler yaratmaktadır (299). Bağımsız ya da düşük bütçeli araştırmacılar için bu sistemler, bilimsel çalışmalara katkı sunmak adına erişilmesi gereken büyük veri kümelerine ulaşımı neredeyse imkânsız hâle getirmektedir (277). Böylece hem bilgi üretiminde adaletsizlik oluşmakta hem de bilimsel bilginin demokratikleşmesi engellenmektedir (278, 300).

Kısacası, merkeziyetçi sistemlerin sunduğu kolaylıkların ötesinde, bu yapıların beraberinde getirdiği etik sorunlar ciddiyetle ele alınabilmelidir. Sağlık verisinin yalnızca güvenli değil; aynı zamanda adil, şeffaf ve birey haklarına duyarlı biçimde yönetilmesi gerekmektedir. Bu noktada, yeni teknolojilere dayalı alternatif sistem modelleri geliştirilmeli ve mevcut yapıların etik açıdan dönüşümü sağlanmalıdır.

5.3 Yeni Teknolojilere Dayalı Çözüm Önerileri

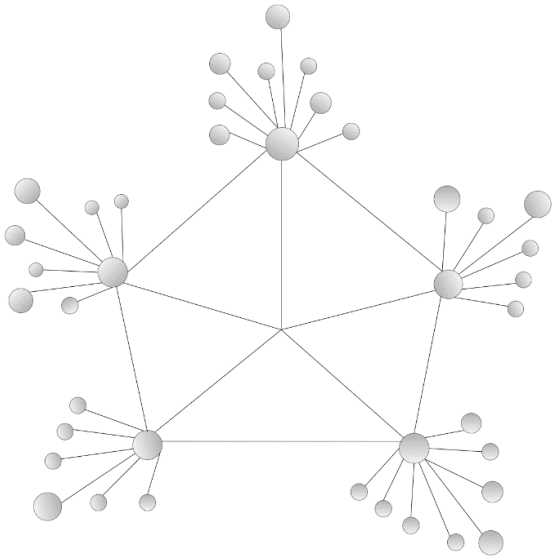
Büyük sağlık verisinin üretimi, toplanması ve işlenmesi süreçlerinde karşılaşılan etik sorunlar -özellikle veri güvenliği, mahremiyetin korunması, gizliliğin sağlanması, bireysel onamın yönetimi ve şeffaflık eksiklikleri- mevcut merkeziyetçi veri yönetim modellerinin yapısal sınırlılıklarını açığa çıkarmaktadır. Bu sorunların üstesinden gelebilmek için, veri erişimini denetleyebilen, yetkilendirmeyi dağıtık biçimde yöneten ve işlem geçmişini değiştirilemez biçimde kaydeden teknolojik altyapılara ihtiyaç duyulmaktadır. Bu bağlamda, merkezi olmayan (federe) sistem mimarileri ve blokzincir (blockchain) temelli uygulamalar, etik ilkelere daha uygun bir veri ekosisteminin inşasına olanak tanımaktadır. Federe sistem yapıları ve blokzincir gibi dağıtık veri teknolojileri; mahremiyetin korunması, veri sahipliğinin güçlendirilmesi ve etik yönetim ilkelerine uygunluk açısından önemli avantajlar sunmaktadır. Yeni teknolojiler sayesinde, veri güvenliğini artırmakla kalmayıp aynı zamanda bireylerin verileri üzerindeki kontrolünü güçlendirmek ve sağlık hizmetlerinde daha adil bir yapı inşa etmek mümkündür.

5.3.1 Merkeziyetçi olmayan (federe) sistem yaklaşımı

Federe sistemler, sağlık verilerinin merkezi bir sunucuya aktarılmaksızın, kaynağında tutulduğu dağıtık mimarilerdir. Yani verinin tek bir merkezde toplanmak yerine, veri kaynaklarında kalmaya devam ettiği ve sadece gerekli durumlarda belirli protokoller aracılığıyla erişime açıldığı bir yapı sunar. Bu modelde, her sağlık kurum veya kuruluşu kendi verilerini kendi sistemlerinde depolayıp kontrol ederken, sistemler arasında belirlenen standartlara uygun bir biçimde veri paylaşımı sağlanır. Bu tür yapılar, büyük verinin merkezi sistemlerde depolanmasından kaynaklanan önemli zorluklardan biri olan ‘tek hata noktası’ (single point of failure) riskini ortadan kaldırarak sistemin genel güvenliğini artırır. Merkeziyetçi sistemlerde, merkeze

yönelik gerçekleştirilen bir siber saldırı veya sistem arızası durumunda, tüm verilerin topluca sızması veya zarar görmesi riski söz konusudur (301). Buna karşılık, merkezi olmayan (federe) sistemler, verilerin tek bir merkezde toplanmasını engelleyerek her sağlık kurumunun kendi verisini kendi sisteminde yerel olarak barındırmasını sağlar. Böylece, tek bir noktadan kaynaklanan geniş çaplı veri ihlallerinin önüne geçilmiş olur.

Örneğin, A Hastanesi, B Tıp Merkezi ve C Aile Sağlığı Birimi'nden toplanan veriler, merkezi bir veri havuzuna aktarılmak yerine, her kurumun kendi altyapısında depolanır. Bu sayede bir kurumda yaşanan ihlal diğerlerini etkilemez. Bu tür sistemlerin başarılı bir örneği Estonya'da uygulanmaktadır; X-Road isimli altyapı sayesinde vatandaşların sağlık verilerine erişim şeffaf, izlenebilir ve blokzincir temelli kayıtlarla güvence altına alınmıştır. Ayrıca modern federe sistemlerde "federated learning" gibi yapay zekâ modelleri kullanılarak, veriler yerel sunucularda kalmaya devam ederken ortak bir modelin eğitilmesi mümkündür. Ek olarak, "differential privacy" gibi teknikler aracılığıyla verilerin anonimliği korunarak mahremiyet ilkeleri daha ileri düzeyde gözetilir. Bu sistemlerin yapısal farklarını daha net ortaya koymak amacıyla, federe sistemin genel ağ yapısı Şekil 8'de görselleştirilmiştir.



Şekil 8. Federe Sistem Ağı

Şekil 8' deki yapı, bilgi ya da veri yönetiminin belirli merkezler etrafında kümelendiği; ancak bu merkezlerin de birbirleriyle doğrudan etkileşim hâlinde olduğu

bir yarı-dağıtık mimariyi temsil etmektedir. Böyle bir yapı, veri güvenliğini ve esnekliğini artırırken, merkeziyetin getirdiği tekil arıza noktalarını da azaltmayı hedeflemektedir.

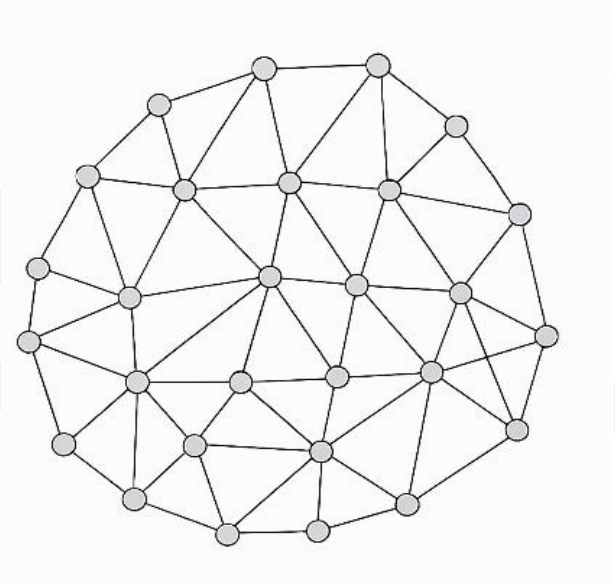
Ancak bu mimari yapı, tek başına veri gizliliği ve güvenliğini artırmakla birlikte, veri ekosisteminde bütüncül bir şeffaflık ve adalet sağlamaktan uzaktır. Önerilen federe sistem yaklaşımı, esasen yalnızca merkezi sistemlerin yapısal problemlerinden biri olan 'tek hata noktası' riskini azaltmakta ve kapsamlı veri ihlallerinin önüne geçilmesine katkı sunmaktadır. Verinin birey odaklı yönetimi, bireyin kendi verisi üzerinde daha fazla kontrol sahibi olması ve veri paylaşım süreçlerinin etik ilkelere uygun şekilde şeffaflaştırılması, ancak bu mimariyle entegre edilebilecek yeni teknolojik çözümlerle mümkün olabilir. Blokzincir, IPFS (InterPlanetary File System), Hashgraph gibi yeni nesil dağıtık teknolojiler; bireyin veri üzerindeki hak sahipliğini güçlendirmeye, işlem geçmişini açık ve denetlenebilir hâle getirmeye ve böylece daha güvenilir, etik açıdan sorumlu bir veri yönetim altyapısı kurmaya olanak tanımaktadır.

5.3.2 Blokzincir ve benzeri teknolojiler

Günümüzde dijital veri yönetiminde güven, şeffaflık ve bütünlük gibi kavramların önemi giderek artarken, bu ihtiyaçlara yanıt veren yeni teknolojik altyapılar da gelişmektedir. Blokzincir (blockchain) teknolojisi, sunduğu yapısal özelliklerle öne çıkmaktadır. Bu teknolojinin sağladığı güvenlik ve şeffaflık gibi avantajlar, doğrudan onun merkezi olmayan, yani dağıtık bir ağ yapısı üzerine inşa edilmiş olmasından kaynaklanmaktadır. Dolayısıyla blokzincir teknolojisinin etik ve teknik yönlerini değerlendirmeden önce, temelini oluşturan dağıtık ağ mimarisini kavramsal olarak açıklamak gereklidir.

Dağıtık ağ yapısı, verinin tek bir merkezde değil, ağ üzerindeki çok sayıda düğümde (node) eş zamanlı olarak bulunması ve işlenmesi esasına dayanır. Bu yapı, merkezi sistemlerde karşılaşılan tekil hata noktası sorununu ortadan kaldırarak sistemin daha güvenli, esnek ve ölçeklenebilir olmasını sağlar (274). Dağıtık sistemlerde her bir düğüm, sistemin genel işleyişine katkı sağlayan bağımsız bir birim olarak çalışır. Böylece herhangi bir düğümün devre dışı kalması, sistemin tamamını etkilemez; veri diğer düğümlerde yaşamaya devam eder (277). Bu yapı sadece teknik

bir tercih değil, aynı zamanda etik bir tercihtir. Zira verinin merkezi bir otorite tarafından kontrol edilmesi yerine çoklu ve özerk yapılar arasında dağıtılması, güç dengelerini eşitler ve veri sahipliğini bireylere daha yakın hâle getirir. Bu yönüyle dağıtık ağ yapısı, birey mahremiyetini koruyan, şeffaflığı teşvik eden ve veri güvenliğini artıran sistemlerin kurulmasında kritik bir rol oynamaktadır. Blokzincir teknolojisi de tam olarak bu dağıtık mimariyi temel alarak, her işlemi ağ üzerindeki tüm katılımcılarla paylaşarak güvenlik ve izlenebilirlik sağlamaktadır. Dağıtık ağ yapısı Şekil 9'da şematik olarak sunulmuştur.



Şekil 9. Dağıtık Ağ Yapısı

Şekil 9. merkezi bir otoriteye bağlı olmadan işleyen bir dağıtık ağ yapısını temsil etmektedir. Merkezi sistemlerin aksine veri tek bir noktada değil de ağa katılan bütün katılımcılarda bulunur ve yapılan her işlem ağ tarafından şeffaf bir şekilde izlenebilir (278). Yani tekelleşmeyi ve aracı sistemlerin ortadan kaldırarak, eşler arası (peer to peer) işlemi mümkün kılar. Ağda olan her bir düğüm (node), hem veri sağlayan hem de veri işleyen bir birim olarak sistemde aktif rol oynamaktadır. Bu yapı sayesinde veri, tek bir merkezde toplanmak yerine ağ genelinde eşzamanlı olarak paylaşılmakta ve saklanmaktadır. Böylece sistem, tekil bir hata noktasına karşı dirençli hâle gelirken, veri bütünlüğü ve güvenliği de artırılmış olur (302). Şekilde görüldüğü üzere, tüm düğümler birbirleriyle doğrudan bağlantı hâlindedir; bu, verinin yatay ve şeffaf bir biçimde paylaşılmasına olanak tanır. Bu mimari, blokzincir teknolojisinin temelini

oluşturmakta ve özellikle büyük sağlık verisi gibi hassas verilerin, daha şeffaf, güvenilir ve birey odaklı yani daha etik biçimde yönetilmesine imkân sağlamaktadır.

Blokzincir teknolojisi, ilk olarak mevcut sistemlerdeki güven sorununa yanıt olarak ve merkezi otoritelerin etkisini azaltma amacıyla geliştirilmiştir. Özellikle verilerin arka planda nasıl işlendiğine dair bilgi eksikliği, sürecin etik olup olmadığına dair belirsizlik yaratmakta ve bireyleri "bu süreçte yaşananlar tam olarak nelerdir?", "bu süreçte bilgilendirme eksikliğinin sebepleri nelerdir?" gibi sorulara yönlendirmektedir. Günümüzde sürekli artan veri üretimiyle birlikte, bu verilerin kimler tarafından tutulduğu, nasıl işlendiği ve ne şekilde korunduğu hâlâ büyük ölçüde belirsizdir. Bu belirsizlik, yalnızca etik ihlallere zemin hazırlamakla kalmamakta, aynı zamanda veri üzerindeki kontrolün az sayıda aktörün elinde toplanmasına ve gücün tekelleşmesine de yol açmaktadır. İşte bu noktada blokzincir teknolojisi, merkeziyetsiz ve dağıtık yapısıyla bu belirsizlikleri azaltma, veri süreçlerini şeffaflaştırma ve bireylerin veri üzerindeki denetimini yeniden tesis etme potansiyeline sahiptir. Aracı sistemlerin ortadan kaldırılmasını ve eşler arası (peer-to-peer) ağlar üzerinden işlem yapılmasını mümkün kılan bu teknoloji, güvenilirlik ve gizliliği ön planda tutarak (303) dijital çağın etik sorunlarına yenilikçi bir çözüm sunmaktadır.

Blokzincir teknolojisi ilk olarak 2008 yılında, Satoshi Nakamoto takma adını kullanan anonim bir kişi ya da grup tarafından yayımlanan "Bitcoin: A Peer-to-Peer Electronic Cash System" başlıklı teknik doküman (white paper) ile gündeme gelmiştir[4]. Bu belge, aracı kurumlara ihtiyaç duymadan dijital ortamda güvenli bir biçimde para transferi yapılabilmesini sağlayacak bir sistemin temelini, yani Bitcoin'in temelini atmak için ortaya çıkmıştır (304). Temel amaç, merkezi bir üçüncü tarafa ihtiyaç duymadan dijital para transferini güvenli ve eşler arası bir şekilde sağlamaktır. Bitcoin, merkezi bir otoritenin onayına ihtiyaç duyulmaksızın, düşük işlem maliyetleriyle küresel ölçekte ödeme yapılmasına imkân tanıyan ve kullanıcıya görece

[4] Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System [Internet]. 2008 [Erişim tarihi: 12 Nisan 2025]. Bu doküman, merkezi otoriteye ihtiyaç duymadan, eşler arası elektronik para transferi yapılabilmesini sağlayan blokzincir tabanlı dijital para sisteminin teknik altyapısını detaylandırmaktadır. Erişim Adresi: https://bitcoin.org/bitcoin.pdf.

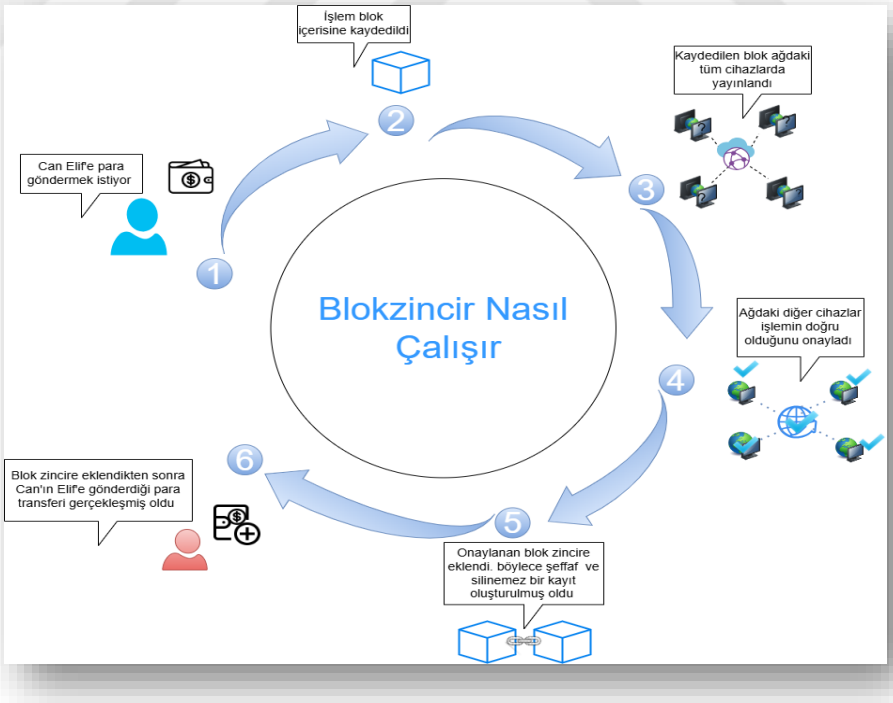
bir mahremiyet sunan merkeziyetsiz bir dijital kripto para birimidir (305). Bu sistemin temelinde yer alan blokzinciri teknolojisi ise, yalnızca Bitcoin gibi dijital para birimlerinin transferinde değil, çok daha geniş bir alanda kullanılabilen dağıtık bir kayıt tutma altyapısıdır (306).

Blokzincir teknolojisinin tarihsel gelişimi ve bu teknolojiyi mümkün kılan temel olaylar, aşağıdaki Şekil 10'de kronolojik olarak sunulmuştur.

Şekil 10. Blokzincir'in Zaman Şeması

Günümüzde çevrimiçi ortamda gerçekleşen para transferlerinde, işlemler genellikle merkezi bir otorite veya finansal kuruluş aracılığıyla yürütülmektedir. Bu aracı kurumlar, işlemin güvenliğini ve doğruluğunu sağlamakla yükümlü olup, tüm transfer kayıtlarını kendi veri tabanlarında saklamaktadır. Para transferi işlemleri, ulusal ya da uluslararası düzeyde geçerli olan yasal düzenlemelere uygun şekilde gerçekleştirilir ve çoğunlukla vergi otoritelerinin denetimine tabidir (305). Örneğin, Elif'in yurt dışında eğitim gören kardeşi Can'a 1000 TL göndermek istemesi durumunda, bu işlem bankacılık sistemine entegre olan güvenilir bir aracı kurum üzerinden gerçekleşir. Söz konusu kurum öncelikle Elif'in kimliğini doğrular, ardından hesabında yeterli bakiye olup olmadığını kontrol eder ve ilgili meblağı bloke

eder. Sonrasında Can'ın hesap bilgileri ve kimliği doğrulanarak transfer işlemi gerçekleştirilir; bu süreçte kurum belirli bir komisyon (örneğin 50 TL) kesintisi yapar. Tüm işlemin güvenliğinden ve takibinden aracı kurum sorumludur. Herhangi bir hata ya da uyuşmazlık durumunda işlem iptal edilebilir ya da yasal sürece konu olabilir. Ancak bu tür uluslararası transferlerin tamamlanması çoğu zaman birkaç iş gününü bulmakta, işlem maliyetleri ve bürokratik engeller kullanıcılar açısından önemli sınırlılıklar oluşturmaktadır. Geleneksel para transferlerinde, işlemler genellikle bankalar gibi merkezi aracı kurumlar üzerinden gerçekleştirilir ve bu süreçte işlem onayı, kayıt altına alma ve güvenlik gibi unsurlar söz konusu kurumlar tarafından sağlanır. Buna karşın, blokzincir teknolojisiyle gerçekleştirilen para transferlerinde, işlem bilgileri (örneğin gönderici ve alıcı adresleri, transfer edilen miktar ve zaman damgası) merkezi bir otoriteye gerek duyulmaksızın, tüm ağ katılımcılarına dağıtılmış şeffaf ve değiştirilemez bir kayıt defteri üzerinde açık biçimde izlenebilir şekilde kaydedilmektedir (305). Blokzincir teknolojisi aracılığıyla gerçekleştirilen para transferi süreci, Şekil 11'de gösterilmiştir.



Şekil 11. Blokzincirle Para Gönderim İşlemi

İlk olarak bitcoinle ismini duyuran blokzincir her geçen gün farklı alanlarda kullanılarak kullanıcılara güven ve şeffaflık tahsis etmektedir. 2013 yılı itibarıyla, blokzincirin potansiyeli yalnızca finansal işlemlerle sınırlı kalmamış; akıllı sözleşmeler (smart contracts), dijital kimlik, tedarik zinciri yönetimi, sağlık verilerinin paylaşımı gibi alanlarda da kullanılabileceği görülmüştür (274, 307, 308). Ethereum'un 2015 yılında kullanıma sunulması, blokzincirin programlanabilir yapısının ortaya çıkmasını sağlayarak teknolojiye yeni bir boyut kazandırmıştır. Bugün gelinen noktada blokzincir, güvenlik, şeffaflık, veri bütünlüğü ve merkeziyetsizlik gibi özellikleri sayesinde yalnızca bir teknoloji değil, aynı zamanda bilgiye erişim, paylaşım ve denetim konularında etik bir dönüşüm aracı olarak da değerlendirilmektedir (275, 276, 309-311).

5.3.2.1 Blokzincir'in temel özellikleri

Blokzincir, temel olarak, bilgilerin veya işlemlerin kaydedildiği, merkezi olmayan (decentralized), dağıtık (distributed) ve değişmez (immutable) bir dijital defterdir. Geleneksel sistemlerin aksine, tek bir kişi veya kurum tarafından kontrol edilmez. Bilgiyi ağdaki birçok katılımcı (düğüm/node) arasında kopyalayarak ve paylaşarak çalışır. Blokzincir tek başına veri saklamak için değildir**,** veri üzerinde işlem yapmak, kayıt tutmak ve güvenli onay mekanizmaları oluşturmak için kullanılan bir teknolojidir (307).

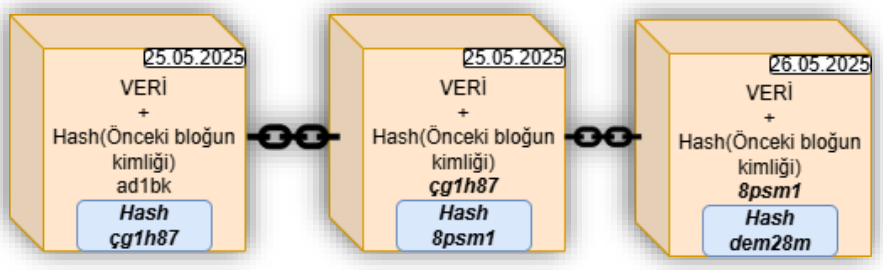
Blokzincir, adından da anlaşıldığı üzere verilerin bloklar hâlinde kaydedildiği ve bu blokların birbirine zaman sırasına göre bağlandığı bir dijital kayıt sistemidir. Her blok, belirli bir işlem kümesini içerir ve kendisinden önce gelen bloğa kriptografik olarak bağlıdır (304). Her bir blok temelde üç bileşen içerir.

1. Veri (İşlem bilgisi): Örneğin bir para transferi, sağlık kaydı ya da bir sözleşme.

2. Zaman damgası (timestamp): Blok ne zaman oluşturulduğunu belirtir.

3. Önceki bloğun kimliği (hash): Önceki bloğun şifresel özetidir. Hash, bir veriyi sabit uzunlukta ve benzersiz bir karakter dizisine dönüştüren matematiksel bir algoritmadır. Veride yapılan en küçük bir değişiklik, ortaya

çıkan hash'i tamamen farklılaştırır. Bu özellik sayesinde verinin bütünlüğü ve değişmezliği (immutability) sağlanır (312)



Şekil 12. Blokzincir'in Blok Oluşumu

Bir blok oluşturulup zincire eklendikten sonra, o bloktaki veriler değiştirilemez. Değiştirilmeye çalışılırsa, zincirin bütünlüğü bozulur ve sistem bunu fark eder (306).

Blokzincirin en dikkat çeken yönlerinden biri merkezi bir otoriteye ihtiyaç duymamasıdır. Veriler, merkezi bir sunucuda değil, ağa katılan tüm kullanıcıların (düğümlerin) bilgisayarlarında tutulur. Böylece tek bir merkezde toplanan verilerin silinmesi, değiştirilmesi veya çalınması riski azaltılmış olur (313).

Nasıl Çalışır?

1. İşlemler Gruplanır (Bloklar): Yapılan yeni işlemler (örneğin, para transferi veya bir tıbbi kayıt güncellemesi) belirli bir süre boyunca bir araya toplanır ve bir "blok" oluşturulur.

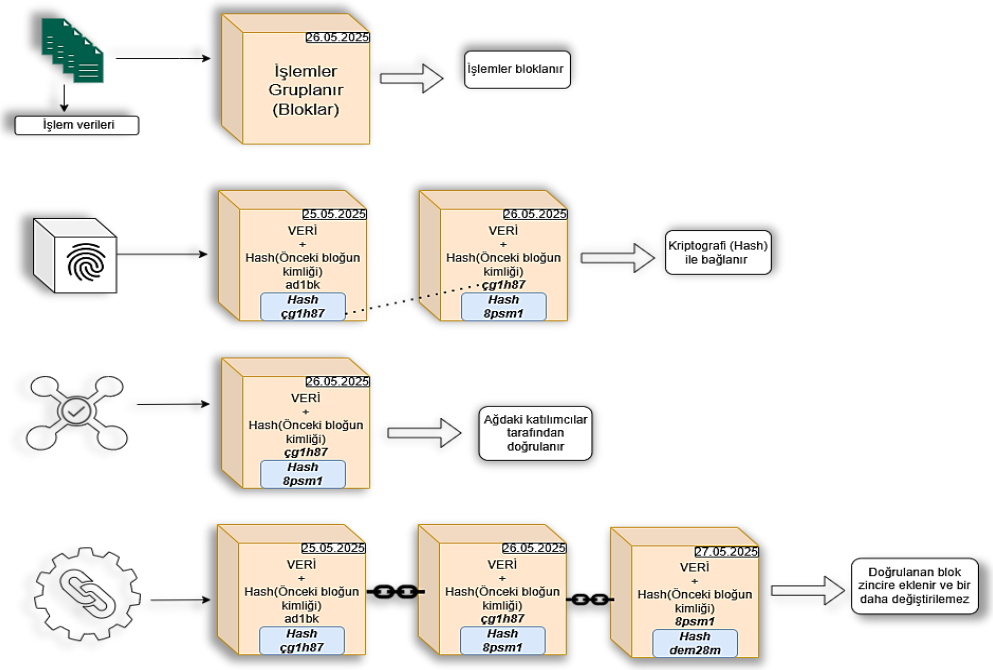
2. Kriptografi ile Bağlanır: Her blok, kendisinden önceki bloğun benzersiz bir dijital "kimliğini veya parmak izini" (kriptografik hash) içerir. Bu, blokların bir zincir gibi birbirine bağlanmasını sağlar (314).

3. Ağ Tarafından Doğrulanır (Konsensus): Blokzincir sistemlerinde, yeni bir işlemin geçerliliği ağdaki katılımcılar tarafından kolektif bir biçimde değerlendirilir. Bu sürece "konsensüs (mutabakat) mekanizması" adı verilir. En yaygın yöntemlerden biri olan Proof-of-Work (İş Kanıtı- PoW), işlemleri doğrulamak için yüksek işlem gücü ve enerji gerektiren matematiksel problemleri çözen düğümleri temel alır. Alternatifi olan Proof-of-Stake (Hisse

Kanıtı-PoS) ise, doğrulama yetkisini katılımcıların sistemde ne kadar dijital varlık bulundurduğuna göre belirler. Bu yöntem daha az enerji tüketse de güvenlik ve merkezileşme açısından çeşitli riskler doğurabilir. Buna karşın, Pratical Byzantine Fault Tolerance (Pratik Bizans Hata Toleransı-PBFT) mekanizması, yalnızca belirli ve güvenilir katılımcıların yer aldığı, izinli blokzincir ağları için geliştirilmiştir. PBFT, ağdaki katılımcıların çoğunluğunun doğru çalıştığı varsayımıyla, daha hızlı ve düşük maliyetli bir doğrulama süreci sunar (315). Bu özelliği sayesinde, veri gizliliği ve işlem doğruluğunun kritik olduğu sağlık gibi alanlarda, hem güvenilirliği hem de işlem hızını artırarak önemli bir avantaj sağlar.

4. Zincire Eklenir (Değişmezlik): Doğrulanmış blok, zincire eklenir ve bir kez eklendikten sonra, içerdiği bilgi değiştirilemez veya silinemez. Bir bilgiyi değiştirmek için zincirdeki tüm sonraki blokları da değiştirmek gerekir ki bu, dağıtık yapısı nedeniyle pratik olarak imkansızdır (316).

Aşağıdaki Şekil 13, bir blokun hangi adımlarla oluşturulduğunu ve zincire nasıl eklendiğini şematik olarak göstermektedir.



Şekil 13. Blokzincir Nasıl Çalışır

Farklı Türleri Vardır:

Blokzincirin farklı ihtiyaçlara uygun çeşitleri bulunur:

- Genel (Public): Herkesin katılabildiği ve işlemleri görebildiği açık ağlar (Bitcoin, Ethereum gibi). Tam şeffaflık ve merkeziyetsizlik gerektirir (IBM, n.d.).

- Özel (Private): Yalnızca önceden davet edilmiş veya yetkilendirilmiş katılımcıların işlem yapabildiği veya blok oluşturabildiği daha kısıtlı ağlar. Kayıtları gizli tutmak isteyen organizasyonlar için (IBM, n.d.).

- İzinli (Permissioned): Kimlerin ağa katılabileceği veya hangi işlemleri yapabileceği konusunda kısıtlamaların olduğu ağlardır (IBM, n.d.).

- Konsorsiyum (Consortium): Birden fazla organizasyonun blokzinciri sürdürme sorumluluğunu paylaştığı, yetkilendirilmiş katılımcılara sahip ağlardır (IBM, n.d.).

Türler arasındaki yapısal farkların anlaşılmasına yardımcı olmak üzere, temel özellikler aşağıdaki tabloda özetlenmiştir.

Tablo 2. Blokzincir Türleri

Tür	**Katılımcılar**	**Kullanım Alanları**	**Örnek**
Genel (Public)	Herkes	Kripto para, NFT	Bitcoin, Ethereum
Özel (Private)	Davetli/Yetkili kullanıcılar	Kurumsal iç sistemler	IBM Food Trust
İzinli (Permissioned)	Kısıtlı katılımcılar	Sağlık, tedarik zinciri	Hyperledger Fabric
Konsorsiyum	Belirli kurumlar arası paylaşım	Finans, sağlık, lojistik	R3 Corda, Energy Web Chain

5.3.2.2 Blokzincir teknolojisinin sunduğu çözümler

Blokzincir teknolojisi, özellikle güvenlik, şeffaflık ve verimlilik gibi konularda sunduğu çözümlerle sağlık sektörü de dahil olmak üzere birçok alanda dönüştürücü bir potansiyele sahiptir (317).

- Güvenin Yeniden Tanımlanması: Blokzincir, güvenin bireyler veya merkezi otoriteler yerine sistemin kendisine dayandırıldığı bir yapıdır. Bu sayede taraflar birbirlerine doğrudan güvenmek zorunda kalmadan işlem gerçekleştirebilir. Aracıların ortadan kalkmasıyla işlemler daha hızlı ve düşük maliyetli hâle gelir (318).

- Şeffaflık ve İzlenebilirlik: İşlemler, ağ katılımcıları tarafından izlenebilir biçimde kayıt altına alınır. Veri bloğa eklendiğinde tüm kullanıcılar tarafından görülebilir hâle gelir. Bu yapı, özellikle tedarik zinciri, klinik araştırmalar veya ilaç takibi gibi süreçlerde sahteciliği ve hataları azaltabilir (311).

- Güvenlik ve Veri Bütünlüğü: Dağıtık yapı ve kriptografi sayesinde veriler yetkisiz erişime karşı korunur. Blokzincirdeki kayıtların değiştirilemez oluşu, veri bütünlüğünün korunmasına ve bilginin doğruluğunun garanti altına alınmasına olanak tanır (319).

- Verimlilik ve Otomasyon: Akıllı Sözleşmeler: Akıllı sözleşmeler, blokzincir üzerinde otomatik olarak çalışan, önceden belirlenmiş kurallara göre kendi kendini yürüten dijital programlardır. İnsan müdahalesine gerek kalmadan, taraflar arasındaki anlaşmaların koşulları kodlanır ve bu koşullar sağlandığında işlemler otomatik olarak gerçekleştirilir. Bu sayede, güvenilirlik, şeffaflık ve işlem doğruluğu sağlanırken, aracıların ortadan kalkmasıyla süreçler hızlanır ve maliyetler azalır. Sağlık verisi yönetiminde akıllı sözleşmeler, veri paylaşımı izinlerinin kontrolü ve izlenmesi için kritik bir mekanizma olarak görev yapar (320). Blokzincir, belirli koşullar gerçekleştiğinde otomatik olarak devreye giren akıllı sözleşmeleri (smart contracts) barındırabilir. Bu sözleşmeler süreçleri hızlandırır, insan hatasını

azaltır ve aracıya olan ihtiyacı ortadan kaldırarak işlem maliyetlerini düşürür (321).

- Merkezi Otoritenin Azaltılması: Blokzincir teknolojisi ilk olarak merkezi otoriteye duyulan ihtiyacı ortadan kaldırmak amacıyla (örneğin Bitcoin örneğinde olduğu gibi) geliştirilmiştir (322). Bu yapı, yalnızca finans değil, sağlık gibi merkeziyetçi sistemlerin yoğun olduğu alanlarda da alternatif bir model sunabilir.

Blokzincir teknolojisi veri dünyasındaki temel zorluklara ve problemlere bir çözüm olarak da değerlendirilmektedir. Özellikle tez boyunca tartışılan büyük sağlık verisine ilişkin etik sorunlara yönelik de çeşitli çözüm olanakları sunmaktadır.

5.3.2.3 Blokzincir benzeri teknolojiler

Blokzincir teknolojisi, merkeziyetsiz yapısı, değiştirilemez kayıt özelliği ve işlem şeffaflığı ile büyük veri yönetiminde güvenli bir altyapı sunmaktadır. Ancak veri etiği bağlamında değerlendirme yapıldığında, yalnızca blokzincir teknolojisinin değil, benzer işlevlere sahip alternatif teknolojilerin de dikkate alınması gerekmektedir. Zira etik bir sistem tasarımı, yalnızca teknik yeterliliklere değil; mahremiyetin korunması, birey özerkliği, sürdürülebilirlik ve toplumsal adalet gibi değerlerle uyuma da dayanmalıdır. Sağlık verilerinin mahremiyeti, güvenliği ve bireylerin veri üzerindeki kontrolü gibi etik öncelikler, teknolojik altyapı seçiminde belirleyici faktörlerdendir. Bu nedenle yalnızca teknik etkinliği değil, aynı zamanda etik uyumluluğu yüksek sistemlerin tercih edilmesi gerekmektedir.

Blokzincir teknolojisinin temelini, verilerin merkezi bir otoriteye bağlı olmaksızın birçok farklı noktada tutularak kaydedilmesini sağlayan Dağıtık Defter Teknolojisi (Distributed Ledger Technology-DLT) oluşturmaktadır. Blokzincir, DLT'nin en yaygın ve bilinen uygulamalarından yalnızca biridir. DLT, verilerin tek bir merkezi sunucuda depolanması yerine, ağ üzerindeki birçok düğüm (node) aracılığıyla senkronize biçimde tutulmasına olanak tanır (323). Bu mimari, verinin tek bir otoritenin kontrolünden çıkmasını sağlarken, verilerin çoklu kopyalar halinde tutulması sayesinde hem şeffaflık hem de manipülasyona karşı direnç kazandırır. Her

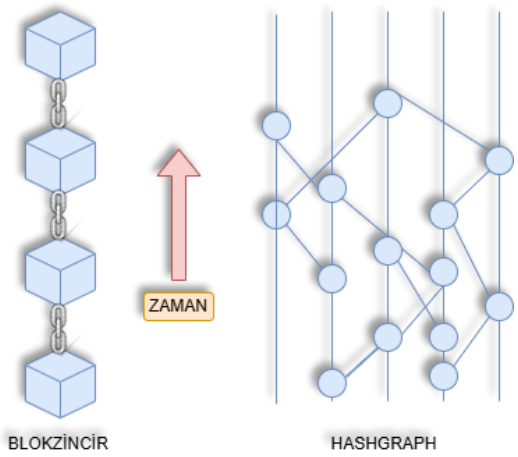
bir düğüm, verinin aynı versiyonuna sahip olduğundan sistemin bütünlüğü sürekli olarak karşılıklı denetlenebilir hâle gelir (324).

Etik açıdan değerlendirildiğinde, DLT tabanlı teknolojiler bireylerin mahremiyetinin korunması, veriye erişim hakkının denetlenebilir olması ve şeffaflık gibi temel etik ilkelerle büyük ölçüde örtüşmektedir (273). Merkeziyetsizlik, otoriter veri kontrolünü azaltırken kullanıcıya daha fazla kontrol ve güvenlik sunar. Bu nedenle, DLT tabanlı teknolojiler sağlık gibi yüksek hassasiyet gerektiren alanlarda etik yönetim açısından önemli fırsatlar sunar. Blokzincirin yanı sıra, DLT altyapısına sahip ve farklı işleyiş mekanizmalarına dayanan çeşitli teknolojiler de geliştirilmiştir. Aşağıda, blokzincire alternatif oluşturan bu teknolojilerin başlıcaları açıklanmaktadır.

Yönlendirilmiş Döngüsüz Grafik (Directed Acyclic Graph -DAG): Yönlendirilmiş Döngüsüz Grafik (DAG) yapısı, blok yerine işlemlerin birbirini onayladığı grafik tabanlı bir sistemdir. Bir işlem, ağdaki önceki işlemleri doğrulayarak sisteme girer. Bu paralel ve birbirine bağlı doğrulama, işlem hızını artırır ve işlem ücretlerini düşürür (325). DAG teknolojisi, madencilik ya da merkezi otoriteye ihtiyaç duymadan çalışır ve özellikle Nesnelerin İnterneti (IoT) cihazları arasında veri paylaşımı için uygundur (323).

Hashgraph: Hashgraph, blokzincire alternatif olarak geliştirilen ve zincir yerine yönlendirilmiş döngüsüz grafik (DAG) kullanan bir DLT türüdür. İşlemlerin ağdaki düğümler arasında yayılması gossip protokolü (dedikodu protokolü) ile sağlanır; burada her düğüm öğrendiği bilgiyi rastgele diğer düğümlere iletir ve bu şekilde bilgi hızla tüm ağa yayılır. Sanal oylama (virtual voting) yöntemiyle ağdaki tüm düğümler, işlem sırasını ve doğruluğunu gerçek oylama yapmadan simüle ederek mutabakat sağlar (325). Bu teknoloji yüksek hızda işlem yapabilmekte, enerji tüketimi düşük olmakta ve adil işlem sıralaması sağlamaktadır (326).

Blokzincir ve Hashgraph'a ait temel ağ yapıları, Şekil 14'te karşılaştırmalı biçimde sunulmuştur.

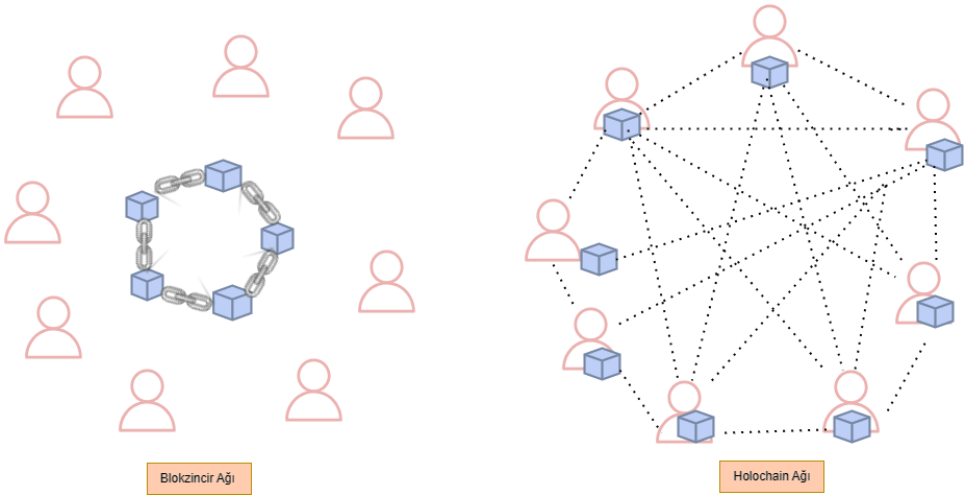


Şekil 14. Blokzincir ve Hashgraph Ağ Yapıları

Holochain: Holochain, tamamen dağıtık bir yapıya sahip olup her kullanıcının kendi verisini yerel olarak sakladığı ve ihtiyaç duyulduğunda paylaştığı bir teknolojidir. Merkezi bir defter bulunmadığı için veri sahipliği bireylere aittir. Bu özellik, mahremiyet ve veri özerkliği açısından oldukça güçlü bir etik altyapı sağlar (327). Enerji tüketimi düşük olup, ölçeklenebilirlik açısından da avantajlıdır. Ancak henüz yaygınlaşmamış olması, yasal ve kurumsal düzenlemelerde belirsizlikler yaratmaktadır (328).

Holochain teknolojisi, merkeziyetsiz yapısına rağmen, geliştirilme süreci ve yönetişimi büyük oranda özel bir şirket tarafından kontrol edilmektedir (328). Bu durum, teknolojinin tam anlamıyla açık kaynaklı ve topluluk odaklı bir yapıya ulaşmasını sınırlamaktadır. Ayrıca, kullanıcıların verilerini yerel cihazlarında saklaması mahremiyet açısından avantaj sağlasa da, sistemin bütüncül işleyişinin dış denetime açık olmaması nedeniyle şeffaflık ve denetlenebilirlik açısından kısıtlamalar ortaya çıkmaktadır (327).

Şekil 15'te blokzincir ve Holochain mimarilerinin ağ üzerindeki veri organizasyon biçimleri karşılaştırmalı olarak sunulmuştur. Blokzincir yapısı, işlemleri sıralı bloklarda tutan tekil bir zincir üzerinden işlerken; Holochain, her katılımcının kendi defterini tuttuğu ve sadece gerektiğinde ağ ile eşleştiği daha dağıtık ve ölçeklenebilir bir yapı sunar.



Şekil 15. Blokzincir ve Holochain Ağ Yapıları

InterPlanetary File System (IPFS-Gezegenler Arası Dosya Sistemi): IPFS, geleneksel internet protokollerinden farklı olarak, dosyaların içeriğe dayalı adresleme yöntemiyle dağıtık bir şekilde saklanmasını sağlayan bir sistemdir (329). Klasik dosya sistemlerinde dosyalar, belirli bir sunucuda depolanır ve erişim için bu sunucunun adresi kullanılır. Oysa IPFS'de dosyalar, içeriğinin benzersiz bir kriptografik özetine (hash) göre adlandırılır. Bu sayede, aynı dosya hangi düğümde olursa olsun, içeriği aynıdır ve bu hash kullanılarak dosyaya erişilir. Bu durum, verinin merkezî bir sunucuya bağlı kalmadan, ağdaki birçok düğümde eş zamanlı olarak dağıtık bir şekilde tutulmasını sağlar.

Örnek vermek gerekirse, bir sağlık kuruluşu IPFS kullanarak hasta raporlarını veya tıbbi görüntüleri depolayabilir. Bu dosyalar ağdaki birçok düğüme dağıtılır ve her biri dosyanın içeriğini doğrulayan benzersiz bir hash ile işaretlenir (330). Böylece, bir kullanıcı bu rapora erişmek istediğinde, dosyanın adresi olan hash'i kullanarak en hızlı veya en güvenilir düğümden veriyi alabilir. Eğer bir düğüm çevrimdışı olursa, dosya başka düğümlerden temin edilir. Bu sistem, sunucu kaynaklı kesintilere ve saldırılara karşı yüksek dayanıklılık sağlar (331). IPFS, doğrudan bir blokzincir (blockchain) teknolojisi değildir ancak blokzincirle entegre olarak kullanılabilir. Örneğin, sağlık verilerinin şifrelenmiş bir versiyonu IPFS'de depolanırken, veri erişim izinleri ve işlemlerin kaydı blockchain üzerinde tutulabilir. Bu sayede veri hem güvenli bir şekilde saklanır hem de işlemler değiştirilemez olarak kayıt altına alınır (331).

Sıfır Bilgi Kanıtı (Zero-Knowledge Proof - ZKP): ZKP doğrudan bir DLT türü olmayıp, blokzincir ve diğer DLT'lerde gizlilik ve güvenliği artıran bir kriptografi yöntemidir. Bir taraf, elindeki bilginin doğruluğunu, bilgiyi açığa çıkarmadan matematiksel olarak kanıtlar. Örneğin, bir kişi şifreyi paylaşmadan şifreyi bildiğini ispatlayabilir. Bu yöntem, sağlık verilerinin gizliliğini koruyarak doğrulama yapılmasını sağlar ve kimlik doğrulama sistemlerinde kullanılır (332).

Yukarıda açıklanan blokzincir ve benzeri dağıtık defter teknolojilerinin temel yapısı ve işleyişi ışığında, bu teknolojilerin sağlık verisi yönetimindeki potansiyelini daha kapsamlı değerlendirmek amacıyla bir SWOT analizi gerçekleştirilmiştir. Aşağıda sunulan SWOT analizi, bu teknolojilerin güçlü ve zayıf yönlerini, karşılaşılabilecek fırsatları ve tehditleri sistematik bir şekilde ortaya koyarak sağlık sektöründe uygulama alanlarına dair içgörüler sağlamaktadır.

Tablo 3. Yeni Teknolojilerin Güçlü ve Zayıf Yönleri

Teknoloji	Güçlü Yönler	Zayıf Yönler
Blokzincir	- Şeffaf ve değiştirilemez kayıtlar- Yasal çerçeveye daha uyumlu	- Enerji tüketimi yüksek (PoW)- Geri alınamazlık riski
Hashgraph	- Yüksek işlem hızı- Düşük enerji tüketimi- Sanal oylama ile mutabakat	- Tescilli yapı- Açıklık sınırlı
DAG	- Paralel işlem imkânı- Düşük işlem ücreti- Madencilik ihtiyacı yok	- Az yaygın kullanım- Teknik karmaşıklık
Holochain	- Veri bireyde kalır- Tam dağıtık yapı- Mahremiyet ve özerklik	- Yasal belirsizlikler- Kurumsal kabul düşük
IPFS	- Dağıtık dosya saklama- Sunucuya bağımlı değil- Saldırılara dirençli	- Blockchain ile birlikte kullanılmalı- Doğrudan işlem kayıt sistemi değil
ZKP	- Veriyi ifşa etmeden doğrulama- Mahremiyet koruması	- Teknik olarak karmaşık- Hukuki çerçeve belirsiz

Tablo 4. Yeni Teknolojilerin Fırsat ve Tehditleri

Teknoloji	Fırsatlar	Tehditler
Genel (Tüm Teknolojiler)	- Etik temelli sağlık altyapılar - Mahremiyet ve güvenlik için yenilikçi çözümler - Kişisel veri sahipliğini güçlendirme	- Devlet ve kurumların denetim eksikliği hissi, güven zedelenmesi - Hukuki altyapı eksiklikleri - Kullanıcı hatalarının geri döndürülemezliği

Tablo 5. Uygun Teknoloji Seçimi: Günümüz ve Gelecek Perspektifi

Dönem	En Uygun Teknoloji	Gerekçesi
Günümüz	Blokzincir	- Yasal çerçeveye en uygun - Yaygın ve güvenilir uygulama altyapısına sahip
Gelecek	Holochain	- Veri sahipliğini bireye vermesi - Mahremiyet odaklı yapısıyla etik açıdan güçlü bir aday

Genel değerlendirmede, mevcut yasal çerçeveye uyumu ve kurumsal adaptasyon kolaylığı açısından en uygun teknoloji blokzincir olarak öne çıkmaktadır. Ancak geleceğe dönük olarak Holochain, mahremiyet, veri özerkliği ve enerji verimliliği açısından daha güçlü bir etik potansiyel taşımaktadır. Bununla birlikte, IPFS gibi teknolojiler de özellikle veri depolama açısından şimdiden kullanılabilir durumdadır ve gelecekte dağıtık veri paylaşımı konusunda önemli katkılar sağlayabilir.

5.3.3 Sağlık verisinde blokzincir kullanımı ve potansiyel faydaları

Blokzincir teknolojisi, sağlık verilerinin güvenli, şeffaf ve birey merkezli yönetimini mümkün kılan yapısıyla etik açıdan önemli bir potansiyel taşımaktadır. Bu

teknolojinin en temel özelliği olan merkeziyetsizlik, verinin bütünlüğünü garanti altına alırken; geçmiş işlemlerin değiştirilemez biçimde kayıt altına alınması hem bireysel hem de kurumsal düzeyde hesap verebilirliği güçlendirmektedir (333).

Blokzincir teknolojisinin sağlık verilerinin yönetiminde kullanılması, sağlık hizmeti sunumunu ve organizasyonunu dönüştürme potansiyeline sahip çok yönlü faydalar sunmaktadır (307, 308). Bu faydalar aşağıda tematik başlıklar altında açıklanmıştır:

Veri Güvenliği ve Bütünlüğü

Blokzincir teknolojisi, verilerin güvenli, şeffaf, doğrulanabilir, kalıcı ve saldırılara karşı dayanıklı biçimde saklanmasını sağlar (308, 333). Değiştirilemezlik (immutability) özelliği sayesinde, veriler blok zincirine eklendikten sonra geriye dönük olarak manipüle edilmesi neredeyse imkânsızdır. Bu durum, özellikle hassas hasta verilerinin korunması açısından önem taşımaktadır (311). Ayrıca çok katmanlı şifreleme ve dijital imza gibi kriptografik yöntemlerle desteklenen sistem, merkeziyetsiz yapısı sayesinde tek bir saldırı noktasının bulunmaması nedeniyle yüksek dayanıklılık gösterir (274).

Hasta Verisi Sahipliği ve Kontrolü

Blokzincir, bireylerin kendi sağlık verileri üzerindeki kontrolünü artırmakta ve veri sahipliğini bireye geri vermektedir. Akıllı sözleşmeler aracılığıyla hastalar, kimlerin hangi verilere ne kadar süreyle erişeceğini belirleyebilir (310). Bu durum, mahremiyetin korunmasına ve hasta merkezli sağlık hizmeti anlayışının güçlenmesine katkı sunar.

Birlikte Çalışabilirlik ve Veri Paylaşımı

Farklı sağlık kurumları ve elektronik sağlık kayıt (ESK) sistemleri arasında güvenli ve etkili veri paylaşımı, blokzincirin sunduğu birlikte çalışabilirlik sayesinde kolaylaşmaktadır (304). Bu sistemler, parçalanmış sağlık altyapılarını birleştirerek daha iyi analiz olanakları ve entegre bakım modelleri geliştirir (310). Estonya gibi

ülkelerdeki uygulamalar, blokzincirin bu bağlamda pratikte de etkili kullanılabileceğini göstermektedir (319).

Verimlilik ve Maliyet Etkinliği

Blokzincir, idari işlemleri otomatikleştirerek ve aracı ihtiyacını azaltarak sağlık sektöründeki maliyetleri düşürebilir (307). Akıllı sözleşmelerin kullanımı, süreçlerin hızlanmasına ve insan hatalarının azaltılmasına katkı sağlar (309).

İlaç İzlenebilirliği ve Tedarik Zinciri Yönetimi

Sahte ilaçlarla mücadelede ve tıbbi ürünlerin izlenebilirliğinde blokzincir önemli bir rol oynar (311). Tedarik zinciri boyunca ilacın üretiminden son kullanıcıya kadar olan süreç dijital olarak kaydedilebilir. Örneğin, MediLedger gibi projeler bu alanda öncül uygulamalardır (319).

Klinik Çalışmalar ve Araştırma

Klinik deneylerde veri yönetimi, onam takibi ve yan etki bildirimi gibi süreçler blokzincir aracılığıyla daha şeffaf ve güvenilir şekilde yürütülebilir (309). Ayrıca çok merkezli çalışmalarda etik onay süreçlerinin standardize edilmesi ve araştırmacıların hesap verebilirliğinin artırılması mümkündür (310).

Aşılama Yönetimi

COVID-19 pandemisi sırasında blokzincir, sahtecilikle mücadele, dijital sertifikasyon ve uluslararası veri paylaşımı gibi alanlarda kullanılmıştır (319). Aşı dağıtım süreçlerinin otomatikleştirilmesi ve izlenebilir hale gelmesi, verimliliği artırmakta ve kaynak israfını azaltmaktadır.

Blokzincirin sağlık verisi yönetiminde nasıl işlediğini ve yukarıda bahsedilen potansiyel faydaların nasıl gerçekleşebileceğini göstermek için bir örnek üzerinden açıklama yapılabilir:

Örneğin, Ayşe Hanım kronik bir hastalık nedeniyle düzenli olarak tıbbi tetkik yaptırmaktadır. Sağlık verilerinin güvenliği ve gizliliği konusunda endişeleri

olduğundan, blokzincir tabanlı bir sağlık veri yönetim sistemine katılmaya karar verir. Bu sisteme kaydolurken, kendisine özel bir kriptografik anahtar çifti (özel ve genel anahtar) atanır. Özel anahtarı, sadece Ayşe Hanım'ın kendisine ait olup, verilerine erişim yetkisi vermek veya erişimleri iptal etmek için kullanılır. Ayşe Hanım, sağlık verilerinin depolandığı blokzincir ağına verilerini şifreli biçimde yükler. Bu veriler üzerinde tam kontrole sahiptir ve herhangi bir paylaşım isteği, ancak onun açık izniyle gerçekleşebilir. Örneğin, bir araştırma projesinde kullanılmak üzere verilerinin paylaşılması talep edildiğinde, ilgili kurumun talebi blokzincir üzerindeki akıllı sözleşme aracılığıyla Ayşe Hanım'a iletilir. Bu akıllı sözleşme, talebin kapsamını, kullanım amacını ve süresini otomatik olarak detaylandırır. Ayşe Hanım, akıllı sözleşme aracılığıyla bu koşulları inceleyip kabul eder veya reddeder. Kabul ettiği takdirde, verileri şifrelenmiş halde ilgili araştırmacıya erişim izni verilir; tüm erişimler blokzincirde şeffaf şekilde kayıt altına alınır. Bu sayede Ayşe Hanım, hangi verisinin kim tarafından, ne amaçla ve ne zaman kullanıldığını her an takip edebilir. Paylaşımı geri çekmek istediğinde ise, blokzincirin değiştirilemezlik özelliği nedeniyle verinin geçmişteki kullanım kayıtları silinemez, ancak gelecekteki erişimler iptal edilir.

5.4 Uygulama ve Gelecek Perspektifleri

Günümüzde sağlık verilerinin yönetimi, sadece teknolojik bir mesele olmanın ötesine geçerek, aynı zamanda etik, hukuki ve toplumsal bir mesele hâline gelmiştir. Bu nedenle yeni sistemlerin uygulanabilirliğinin değerlendirilmesi, potansiyel zorlukların öngörülmesi ve uzun vadeli politika çerçevelerinin oluşturulması büyük önem taşımaktadır.

Önerilen blokzincir altyapılı federe sistemin insanlar için sağlık sorunlarına yol açmayacak şekilde benimsemek oldukça önemlidir. Kişi merkezli, gizlilik odaklı, onam temelli, kurumlar arası birlikte çalışabilirlik sağlayan bu yapı sağlık verilerinin daha fayda sağlayacak şekilde kullanılmasını sağlayarak veri sorumlularına da veri sahipliği hakkını vermektedir. Sağlık verilerinin etik ilkelere uygun biçimde yönetilebilmesi amacıyla önerilen sistem tasarımının temel bileşenleri federe sistem ve blokzincir teknolojisinden oluşmaktadır. Tasarım, bir yandan bireylerin verileri üzerindeki denetimini artırmayı, diğer yandan ise büyük veri paylaşımında güvenlik,

şeffaflık ve hesap verebilirlik sağlamayı hedefleyen yeni teknoloji temelli sistem önerisini gündeme getirmektedir.

Önerilen modelde, sağlık verileri merkezi olmayan bir yapıda ele alınmakta; ancak bu verilerin doğrudan bireylerin kendi cihazlarında tutulması beklenmemektedir. Veriler, sağlık kurumları gibi yetkilendirilmiş veri noktalarında muhafaza edilmekte; bireyler ise bu verilere ilişkin erişim ve paylaşım izinlerini yönetebilmektedir. Bu yapı, veri sahipliğiyle birlikte karar verme yetisini de bireye bırakırken, veri işleyen taraflar için etik sorumluluğu netleştirmektedir.

Blokzincir teknolojisi, veri işlemlerinin bütünlüğünü ve izlenebilirliğini sağlamak üzere sisteme entegre edilmiştir. Her erişim ya da paylaşım eylemi, değiştirilemez ve şeffaf bir biçimde kayıt altına alınmakta, böylece hem sistem yöneticileri hem de veri sahipleri tarafından denetlenebilir hale gelmektedir. Bu kayıtlar üzerinden yapılan denetimler, olası kötüye kullanımları önlemeye katkı sağlarken araştırmacılar için de veri erişimini de kolaylaştırmaktadır.

Bu teknik altyapı, aynı zamanda FAIR veri ilkeleri (Bulunabilirlik, Erişilebilirlik, Birlikte Çalışabilirlik, Yeniden Kullanılabilirlik) ile uyumlu şekilde kurgulanmıştır. Ancak sistem, bu ilkelerin teknik düzeyde uygulanmasından öte, etik açıdan da güçlendirilmesini hedeflemektedir. Özellikle birey özerkliği, onam ve şeffaflık gibi değerlerin sistem tasarımının merkezine alınması bu yönüyle dikkat çekmektedir.

Teknik Altyapı Gereksinimleri

Önerilen sistemin uygulanabilmesi için hem federe sistem yapısının hem de blokzincir altyapısının sağlık bilişimiyle uyumlu bir şekilde yapılandırılması gerekmektedir. Veri sahipliği ve erişim denetimi ilkeleri doğrultusunda, sistemin aşağıdaki teknik bileşenleri içermesi öngörülmektedir:

- Federe Veri Paylaşım Ağı: Veriler, merkezi bir veri tabanında toplanmadan, çeşitli sağlık kurumları arasında paylaşılabilir hâle gelir. Her kurum, kendi veri setini yerel olarak tutar ve bu veriler, standartlaştırılmış ve birlikte çalışabilir bir biçimde, sistem aracılığıyla erişime açılır. Böylece, veri akışı merkeziyetsiz ancak kontrollü biçimde işler.

- Blokzincir Entegrasyonu: Sistem üzerindeki her veri paylaşımı veya erişim girişimi blokzincire kaydedilerek işlem geçmişi değiştirilemez şekilde korunur. Bu sayede, şeffaflık ve güvenlik birlikte sağlanır.

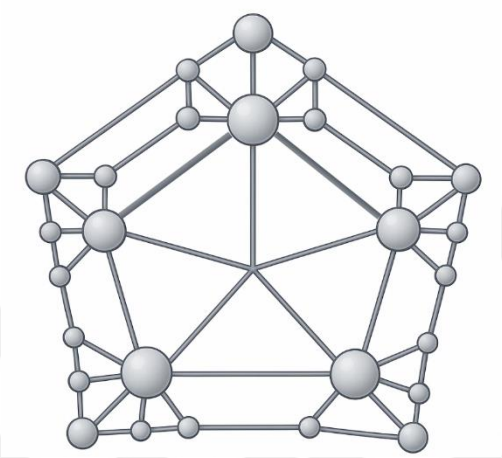
- Erişim Denetim Katmanı: Bireylerin, verilerini kimlerin, hangi zaman aralığında ve hangi amaçla kullanabileceğine dair yetkilendirme yapabilecekleri bir mekanizma oluşturulur. Bu katman, hem kullanıcıların hem de sağlık profesyonellerinin dijital kimlik doğrulamasına dayanır.

- Standartlaştırılmış Veri Formatları ve API'ler: Sağlık kurumları arasında etkili ve güvenli veri paylaşımının sağlanabilmesi için, verilerin belirli bir standart çerçevesinde düzenlenmesi gerekir. Bu noktada, HL7 FHIR (Fast Healthcare Interoperability Resources) gibi uluslararası kabul görmüş veri standartları büyük önem taşır. FHIR, sağlık verilerinin dijital ortamda yapılandırılmış ve birlikte çalışabilir şekilde paylaşılmasını sağlayan bir çerçevedir. Bu standart, hasta bilgileri, laboratuvar sonuçları veya reçeteler gibi sağlıkla ilgili birçok verinin sistemler arasında doğru ve eksiksiz aktarımını mümkün kılar. Bunun yanı sıra, farklı yazılım sistemlerinin birbirleriyle iletişim kurmasını sağlayan uygulama programlama arayüzleri (API'ler- Application Programming Interface) de birlikte çalışabilirlik açısından temel bileşenlerdendir (334). Sağlık hizmetlerinde kullanılan API'ler, hasta verisinin sadece ilgili ve yetkili kişilerce erişilmesini sağlar; böylece hem veri güvenliği hem de iş akışlarında hız ve verimlilik sağlanmış olur. Tüm bu teknolojiler, farklı kurumların birbirinden kopuk sistemleri arasında bir köprü görevi görerek, daha entegre ve hasta odaklı bir sağlık ekosistemi kurulmasına olanak tanır.

Yukarıda sıralanan teknik bileşenler, önerilen sistemin teorik çerçevesini oluşturmaktadır. Bu bileşenlerin nasıl bir ağ yapısı içerisinde işlediğini daha açık bir şekilde göstermek amacıyla, aşağıda iki ayrı şematik temsil sunulmuştur.

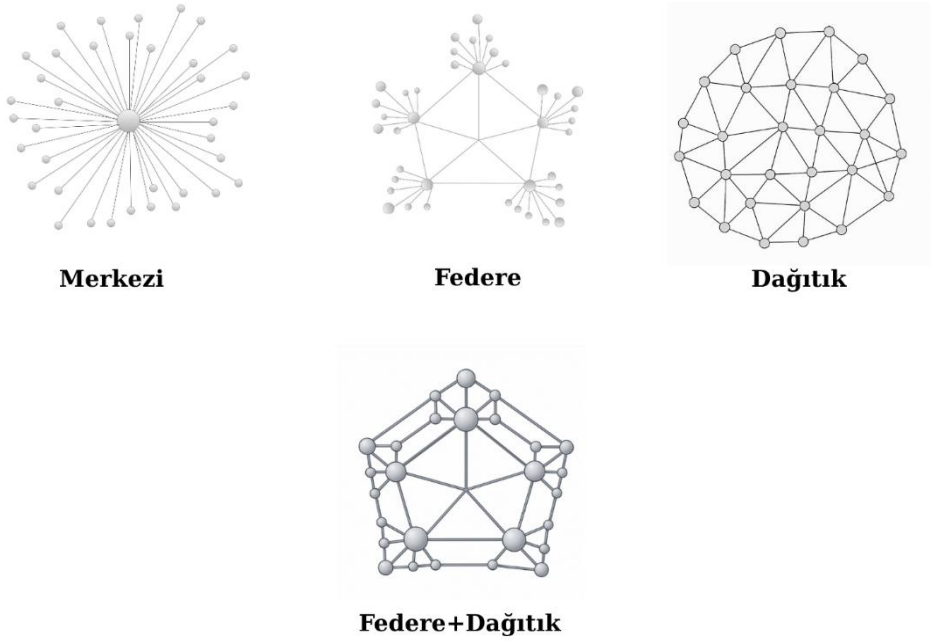
İlk görsel (Şekil 16), federe sistemin blokzincir teknolojisi ile entegre edildiği bir yapıyı temsil etmektedir. Bu yapıda, her bir düğüm (örneğin bir

sağlık kurumu), kendi verisini yerel olarak barındırırken, sistemin genel işleyişi, blokzincir sayesinde merkeziyetsiz ama senkronize bir biçimde yürütülmektedir. Veriye erişim, her kurumun kendi otoritesinde kalmakta; buna karşın erişim kayıtları ve işlem geçmişi, değiştirilemez şekilde blokzincire yazılmaktadır. Böylece, veri sahipliği korunurken, şeffaflık ve güvenlik ilkeleri de güvence altına alınmış olur.



Şekil 16. Federe Sistem + Blokzincir Yapısı

İkinci görselde (Şekil 17) ise bu teknik mimarinin daha iyi anlaşılabilmesi için, ağ yapılarının karakteristik farklarını gösteren karşılaştırmalı bir yapı sunulmuştur. Burada merkezi, federe, dağıtık ve önerilen yapı olan "federe + dağıtık" ağ modelleri yer almaktadır. Merkezi yapılarda tüm veri tek bir merkezde toplanırken, federe yapılarda her birimler kendi verisini korur. Dağıtık sistemlerde ise tüm düğümler eşit yetkilere sahiptir ve ağ yatay şekilde örgütlenir. Önerilen yapı ise bu iki yaklaşımı birleştirir: Veriler yerel sistemlerde kalır (federe), ancak bu sistemler, eşitler arası ve güvenli bir yapı içinde birbirleriyle etkileşime girer (dağıtık). Böylece hem ölçeklenebilirlik hem de etik veri yönetimi açısından güçlü bir model ortaya konmuş olur.



Şekil 17. Sistemlerin Ağ Yapıları

5.4.1 Yeni sistemlerin uygulanabilirliği

Federe sistemler ve blockchain teknolojileri, teknik olarak uygulanabilir olmakla birlikte, sağlık hizmetlerinin karmaşık yapısı nedeniyle entegrasyon süreçleri zaman ve kaynak gerektirmektedir. Bu tür sistemlerin başarıyla uygulanabilmesi için öncelikle teknik altyapının güçlendirilmesi, kurumsal kapasitenin artırılması ve sistemler arası birlikte çalışabilirliğin sağlanması gerekmektedir (307).

Uygulamada karşılaşılan en temel gereksinimlerden biri de tüm paydaşların (sağlık profesyonelleri, veri yöneticileri, yazılım geliştiricileri ve bireyler) sisteme dâhil edilmesi ve bilgilendirilmesidir. Bireylerin sistemin nasıl çalıştığını anlaması, verileri üzerindeki kontrolleri etkin biçimde kullanabilmeleri açısından kritik önemdedir. Bu nedenle, kullanıcı dostu arayüzler, açık iletişim politikaları ve şeffaf veri işleme süreçleri büyük önem taşımaktadır (309).

Literatürde, blokzincir tabanlı bir sağlık veri yönetim sisteminin mimarisinin belirli temel unsurları içermesi gerektiği öne sürülmektedir (274, 304, 307-311, 319, 333).

Blokzincir Türleri: Sağlık hizmetlerinin hassasiyeti göz önüne alındığında, genellikle izinli (permissioned) veya özel (private) blokzincir modelleri tercih edilmesi gerektiği ön görülmüştür

Özel Blokzincirler (Private Blockchains): Önceden davet edilen katılımcıların ağa dahil olduğu ve kayıtlara sınırlı, özel erişime sahip olduğu sistemlerdir. Bu, verilerin halka açık olmasını engeller. Hassas hasta verileri için özel bir blokzincir kullanılabilirken, hassas olmayan faaliyet verileri için yarı özel/konsensüs blokzinciri kullanılabilir (309, 310).

İzinli Blokzincirler (Permissioned Blockchains): İzinli blokzincirler (permissioned blockchains), katılımın kontrol altında tutulduğu, yani herkesin rastgele katılamadığı ve işlem gerçekleştiremediği blokzincir türleridir. Bu ağlarda, kimlerin ağa katılabileceği, hangi işlemleri yapabileceği, hangi verilere erişebileceği önceden tanımlanır ve bu kurallar sıkı şekilde uygulanır. Bu yapı, özellikle gizlilik, veri güvenliği ve yetki kontrolü gerektiren kurumsal sistemler için uygundur. Çünkü burada amaç, verilerin yalnızca güvenilir ve yetkilendirilmiş taraflar arasında paylaşılmasıdır (311, 319).

Sağlık sisteminde İzinli blokzincirin kullanımıyla ilgili bir örnek verecek olursak; izinli blokzincir kullanan bir sağlık sisteminde; hastaneler, sigorta şirketleri ve ilaç firmaları aynı ağda bulunsalar bile, her biri yalnızca kendi yetkisi dâhilindeki bilgilere erişebilir. Hastaya ait tüm sağlık geçmişine sadece hastane ulaşabilirken, sigorta şirketi yalnızca fatura ve poliçeyle ilgili kısımları görebilir. Bu ağlarda işlemler, yalnızca ağa önceden tanımlanmış olan yetkili katılımcılar tarafından doğrulanır ve onaylanır. Böylece hem işlem güvenliği sağlanır hem de gizli verilerin izinsiz erişimi engellenmiş olur. Ayrıca, akıllı sözleşmeler (smart contract / zincir kodu), sadece belirli kurumlar tarafından yürütülüp denetlenebilir. Bu da sistemin kurallara uygun işlemesini ve kötü niyetli manipülasyonları engeller (307, 309). Hyperledger Fabric bu yapının en iyi örneklerinden biridir. Ağa katılan her kurumun kimliği bellidir, erişim hakları nettir ve ağda gerçekleşen işlemler dışarıya kapalı şekilde yürütülür (303, 319).

Tam şeffaflık ve merkeziyetsizlik gerektiren halka açık (public) blokzincirler (Ethereum, Bitcoin gibi) sağlık verileri için zorlu olabilmektedir. Hassas veri

kategorisine giren sağlık verilerinin mahremiyetinin korunması için halka açık blokzincir türü uygun görülmemektedir (303, 307, 308).

Konsensüs Mekanizmaları: Konsensüs mekanizmaları, blokzincir teknolojisinin temel yapı taşlarından biridir. Bu mekanizmalar, ağda gerçekleştirilen işlemlerin geçerli olup olmadığına dair tüm katılımcı düğümlerin (nodes) ortak bir karara varmasını sağlar (303). Başka bir ifadeyle, bir işlemin blokzincire eklenmeden önce doğrulanması ve herkes tarafından kabul edilmesi, bu mekanizmalar aracılığıyla gerçekleşir. Bu süreç, sistemin güvenli, tutarlı ve hatalara karşı dayanıklı olmasını temin eder.

Sağlık sistemlerinde kullanılan blokzincir altyapıları, geleneksel halka açık blokzincir ağlarından farklı olarak daha çok izinli (permissioned) yapıda tasarlanır. Bu yapıların gereksinimleri doğrultusunda, enerji verimliliği yüksek, işlem gecikmesi düşük ve veri güvenliği sağlayan özel konsensüs mekanizmaları tercih edilmektedir (311). Aşağıda, bu bağlamda öne çıkan bazı konsensüs algoritmaları açıklanmaktadır.

Practical Byzantine Fault Tolerance (PBFT), özellikle katılımcı sayısının sınırlı olduğu küçük ve orta ölçekli ağlarda etkili bir biçimde çalışan bir uzlaşma protokolüdür. Bu mekanizma, bazı düğümlerin hatalı ya da kötü niyetli davranabileceği durumlarda bile sistemin doğru çalışmasını garanti eder. PBFT, yüksek işlem hacmi (throughput), düşük gecikme süresi (latency) ve düşük hesaplama gereksinimi ile öne çıkar. Bu özellikleri sayesinde, hassasiyet ve hızın ön planda olduğu sağlık sistemlerinde kullanılabilirliği oldukça yüksektir (303).

Delegated Byzantine Fault Tolerance (dBFT) ise PBFT'nin daha esnek ve ölçeklenebilir bir versiyonu olarak tanımlanabilir. Bu modelde tüm düğümler doğrudan işlem onaylamaz; bunun yerine, ağ katılımcıları tarafından seçilen temsilciler (delegates) yeni blokları oluşturur ve doğrular. Bu yaklaşım, sistemin daha hızlı çalışmasını ve gereksiz işlem yükünden kurtulmasını sağlar. Özellikle çok sayıda sağlık kurumunun birlikte çalıştığı geniş ağ yapılarında dBFT, verimlilik ve güvenlik açısından avantajlı bir çözüm sunar (303).

Bir diğer dikkat çekici mekanizma ise Stellar Consensus Protocol (SCP)'dir. SCP, katılımcıların kendi güvenilir alt gruplarını tanımlayarak yalnızca bu gruplarla uzlaşmasını esas alır. Böylece tüm ağa yayılan bir konsensüs süreci yerine, daha hızlı ve hedeflenmiş bir doğrulama yapılabilir. Bu esneklik, hem güvenlik hem de gizlilik açısından sağlık verisi içeren sistemlerde önemli avantajlar sağlar. SCP, aynı zamanda merkeziyetsizliğe açık yapısını korurken ölçeklenebilirliği de mümkün kılar. Bunun yanında, bazı sağlık blokzincir projeleri, genel mekanizmaları doğrudan uygulamak yerine sistemin doğasına uygun özel konsensüs modelleri geliştirmiştir. Örneğin, MedBlock gibi platformlar, ağın aşırı yüklenmesini önlemek, işlem süresini kısaltmak ve gizliliği korumak adına optimize edilmiş protokoller kullanmıştır. Bu tür özelleştirilmiş modeller, ağ performansını artırırken sağlık verilerinin hassas yapısına uygun bir yapı sunar (303).

Veri Yönetimi ve Depolama Stratejisi:

Sağlık verileri yüksek hacimli, çok boyutlu ve son derece hassas içerikler barındırır. Bu nedenle, bu tür verilerin hem güvenli bir şekilde saklanması hem de erişimlerinin doğru şekilde yönetilmesi büyük önem taşır. Önerilen sistem, federe veri altyapısı ile blokzincir teknolojisinin entegre bir biçimde kullanıldığı hibrit bir çözüm sunmaktadır.

Bu yapıda, asıl sağlık verileri (örneğin, laboratuvar sonuçları, görüntüleme verileri, elektronik sağlık kayıtları) doğrudan blokzincir üzerinde depolanmaz. Bunun yerine, veriler dağıtık ve güvenli biçimde federe veri sunucularında tutulur. Her veri üreticisi (hastane, laboratuvar, birey vb.) kendi veri sorumluluğunu üstlenir ve yalnızca kendi sisteminde barındırdığı veriler üzerinde işlem yapar. Bu yaklaşım, kişisel veri kontrolünü artırmakta ve Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR) gibi düzenlemelere uyumu kolaylaştırmaktadır.

Blokzincir bileşeni ise bu sistemde bir işlem kayıt defteri işlevi görür. Blokzincir üzerinde yalnızca:

- veri erişimlerine ilişkin zaman damgalı işlem kayıtları,
- veri parçalarına ait kriptografik özet değerler (hash),

- referans bağlantılar (örneğin IPFS veya benzeri sistemlerdeki içerik adresli veriler),

- ve gerektiğinde erişim izin bilgileri (consent metadata) yer alır.

Bu sayede, verilerin bütünlüğü ve değiştirilemezliği garanti altına alınırken, veri erişimi, sahipliği ve izne dayalı paylaşımı akıllı sözleşmeler (smart contracts) aracılığıyla güvenli bir şekilde yönetilebilir. Sistem, şeffaflık ve izlenebilirlik sunarken, veri gizliliğini de federe yapı sayesinde güçlü biçimde korur.

Kısacası, önerilen modelde:

- verinin kendisi federe sistemde güvenli biçimde saklanır,

- veriye ilişkin işlemler ise blokzincir üzerinde kayıt altına alınarak denetlenebilirlik sağlanır.

Bu yapı, sağlık verilerinin artan hacmiyle baş edebilmek için ölçeklenebilir**,** gizliliği ön planda tutan ve etik ilkelere duyarlı bir çözüm sunabilir.

Erişim Kontrolü ve Gizlilik Mekanizmaları:

Blokzincir tabanlı sistemler, hastanın kendi verileri üzerinde kontrole sahip olmasını ve kimlerin erişebileceğine izin vermesini sağlayabilir (335). İzinli blokzincirler, ağa katılımı ve veri görünürlüğünü kısıtlayarak gizliliği korur.

Etik açıdan da, blokzincir uygulamaları için veri egemenliği kritik öneme sahiptir; hastaların kendi verilerini kontrol etmeleri ve nasıl kullanılacağına karar vermeleri güven ve özerkliği teşvik eder. Merkezi olmayan mimariler, hastalara şeffaflık ve veri kontrolü aracılığıyla yetki verir. Bir blokzincir uygulamasında, veri sahibi, sahip olduğu verinin farklı kullanıcılar veya gruplarla farklı erişim seviyelerinde (özet veya tam veri) paylaşılmasını sağlayabilir (309).

Akıllı Sözleşmeler (Smart Contracts): Anlaşmaları kodlamak ve belirli koşullar tetiklendiğinde otomatik olarak yürütülmek üzere blokzincirde depolanan değiştirilemez dijital programlardır. Sağlık hizmetlerinde, müdahaleleri

otomatikleştirmek (sensörler aracılığıyla gerçek zamanlı bildirim gönderme gibi), ilaç takibi, aşı dağıtımını yönetme, tedarik zinciri sözleşmelerini otomatikleştirme gibi alanlarda güveni sağlamak için kullanılabilirler (319). Bu bileşenler ve yaklaşımlar, blokzincirin sağlık hizmetlerinde veri bütünlüğünü, gizliliğini, güvenliğini ve birlikte çalışabilirliğini destekleyen bir mimari çerçeve oluşturmasını sağlar.

Tablo 6. Federe Sistem ile Blokzincirin Etik ve Teknik SWOT Analizi

Kategori	Özellik	Açıklama
Güçlü Yönler	Gizliliğe duyarlı yapı	Hasta verileri sadece sahibi kurumda tutulur, mahremiyet korunur.
	İzlenebilirlik	Her işlem zincire kaydedilir, erişimler izlenebilir.
	Yasal uyumluluk	GDPR/HIPAA gibi regülasyonlara uyum sağlanır.
Zayıf Yönler	Kurulum karmaşıklığı	Entegrasyon teknik bilgi gerektirir.
	Bakım yükü	Her kurumun sisteminin ayrı olması bakım maliyetini artırır.
	Standart eksikliği	Veri formatları arasında uyumsuzluk olabilir.
Fırsatlar	Uluslararası veri paylaşımı	Farklı ülkeler arasında güvenli veri paylaşımı mümkün.
	Kişiselleştirilmiş tıp	Bütünleşik verilerle özel tedavi yöntemleri geliştirilebilir.
	Araştırma ve inovasyon	Anonimleştirilmiş veriler araştırmalarda kullanılabilir.
Tehditler	Bürokrasi ve direnç	Kurumlar yeni sistemlere geçişte direnç gösterebilir.
	Siber güvenlik riskleri	Zayıf güvenlik düğümleri ağı etkileyebilir.
	Veri kalitesi düşüklüğü	Farklı kurumlar farklı veri kalitesine sahip olabilir.

Blokzincir teknolojisi sağlık hizmetlerinde veri güvenliği, birlikte çalışabilirlik, hasta yetkilendirmesi, sahtekarlığın önlenmesi ve tıbbi kayıtların doğruluğu gibi alanlarda sayısız avantaj sunduğu görülmektedir. Blokzincirin benimsenmesi arttıkça, sağlık hizmeti sunumu, araştırma ve hasta sonuçları üzerindeki dönüştürücü etkisi giderek daha belirgin hale gelecek ve daha verimli, şeffaf ve hasta merkezli bir sağlık sisteminin önünü açacaktır (336).

5.4.2 Karşılaşılan zorluklar ve çözüm yolları

Gelişen teknolojinin etik ilkeler ışığında büyük sağlık verisine entegre edilmesi, geleceğe yönelik umut verici bir adım olarak değerlendirilebilir. Ancak, her teknolojik entegrasyon beraberinde belirli zorlukları da getirmektedir. Özellikle yüksek maliyetli altyapıların büyük veri sistemlerine uyarlanması, bu sürecin karmaşıklığını ve karşılaşılabilecek teknik sorunların boyutunu artırmaktadır. Blokzincir tabanlı merkeziyetsiz (federe) sistemlerin sağlık verisi bağlamında kullanımı, çeşitli avantajlar sunmakla birlikte, aşağıda sıralanan bazı güvenlik ve performans temelli zorluklarla karşı karşıya kalabilir.

Güvenlik Zorlukları ve Saldırı Riski:

Blokzincir teknolojisi doğası gereği güvenli kabul edilse ve kriptografik kanıtlar ile konsensüs mekanizmaları sayesinde "hacklenmesi imkansız" dense de, çeşitli saldırılara karşı dikkatli olunması gerekmektedir (303). Çeşitli saldırı türleri aşağıdaki gibidir:

- Sybil saldırısı: Bu tür saldırılarda bir saldırgan, çok sayıda sahte kimlikle ağa dahil olarak sistemin çoğunluğunu ele geçirmeye çalışır. Böylece mutabakat mekanizmasını manipüle etme ve karar süreçlerini etkileme potansiyeli doğar (303).

- Yarış saldırısı (race attack): Bir dijital varlığın aynı anda birden fazla işlemde kullanılmaya çalışılmasıdır. Özellikle işlemlerin ağ tarafından onaylanmadan geçerli kabul edilmesi hâlinde, satıcılar aldatılabilir ve dolandırıcılık riski ortaya çıkar (303).

- %51 saldırısı (majority attack): Ağın toplam işlem gücünün %50'sinden fazlasını kontrol eden bir madenci grubu, işlemleri geriye alabilir, çifte harcama yapabilir veya blokları yeniden yazabilir (337).

- Akıllı sözleşmelere yönelik saldırılar: Akıllı sözleşmelerdeki yazılım hataları, yetersiz izin kontrolleri veya hatalı mantık yapıları, kötü niyetli kullanıcıların sözleşmenin işleyişine müdahale etmesine olanak tanıyabilir. Bu durum, hem fonksiyonel bozulmalara hem de yetkisiz erişimlere yol açabilir (338).

Tüm bu nedenlerle, blokzincir teknolojisi güvenlik açısından avantajlar sunsa da yapısal veya uygulamaya özgü zayıflıkları nedeniyle tamamen saldırılardan muaf değildir. Ancak bu saldırı riskleri göz önünde bulundurulduğunda, blokzincir sistemlerinin kurulumu öncesinde kapsamlı güvenlik denetimlerinin yapılması, akıllı sözleşmelerin sistematik olarak test edilmesi ve erişim kontrollerinin açık ve sıkı biçimde tanımlanması gerekmektedir. Bu sayede, sistemin bütünlüğü korunabilir ve potansiyel güvenlik açıklarının önüne geçilebilir.

Birlikte Çalışabilirlik (Interoperabilite):

Sağlık sistemlerinde veriler farklı formatlarda, standart dışı yapılarda ve çeşitli bilgi sistemlerinde parçalanmış hâlde tutulmaktadır (319). Bu durum, hasta bakımı ve klinik karar alma süreçlerinde doğru ve zamanında bilgiye erişimi engelleyebilir. Benzer bir sorun, farklı yapısal özelliklere sahip blokzincir platformları (örneğin Ethereum, Hyperledger Fabric, Corda) arasında da görülmektedir. Bu platformların birbirleriyle doğrudan veri alışverişi yapamaması, sağlık alanındaki blokzincir uygulamalarının yaygınlaşmasının önünde önemli bir engel oluşturmaktadır (307).

Bu teknik sorunu aşmak için yazılım geliştirme süreçlerinde Model Odaklı Mühendislik (Model-Driven Engineering – MDE) yaklaşımı kullanılabilir. MDE, sistemin işleyişini önce platformdan bağımsız bir model olarak tanımlar; ardından bu modeli, farklı blokzincir ortamlarına özel biçimde dönüştürerek birlikte çalışabilirliği artırır (307)

Ancak birlikte çalışabilirliğin sadece teknik değil, aynı zamanda veri yönetimi ilkeleriyle de desteklenmesi gerekir. Bu bağlamda, FAIR veri yönetimi ilkelerinin (Bulunabilir, Erişilebilir, Birlikte Çalışabilir, Yeniden Kullanılabilir) benimsenmesi, blokzincir sistemleriyle sağlık verisinin yönetimi arasında köprü kurarak sadece teknik değil, aynı zamanda etik ve sürdürülebilir bir altyapı sunabilir.

Bu nedenle, MDE yaklaşımı ile birlikte FAIR ilkelerinin birlikte ele alınması hem teknik uyumluluk hem de etik sorumluluk açısından bütüncül bir çözüm önerisi olarak değerlendirilebilir.

Uygulama ve Entegrasyon:

Yeni blokzincir teknolojilerinin sürekli gelişimi ve sağlık sistemlerinin yapısal olarak karmaşık ve dinamik bir yapıya sahip olması, yerleşik ya da standartlaştırılmış çözümler üretmeyi zorlaştırmaktadır (307). Bunun birkaç temel nedeni vardır:

Teknolojik Değişkenlik: Blokzincir alanında sürekli olarak yeni mutabakat algoritmaları (ör. Proof-of-Stake, Proof-of-Authority, DAG tabanlı yapılar), ölçeklenebilirlik çözümleri (ör. sharding, sidechain'ler, layer 2 çözümleri) ve veri gizliliğine odaklı yöntemler (ör. zk-SNARK, homomorfik şifreleme gibi) geliştirilmektedir. Bu teknolojilerin henüz olgunlaşmamış olması, uzun vadeli güvenilirlik ve birlikte çalışabilirlik konularında belirsizlik yaratmaktadır (307).

Sağlık Sistemlerinin Heterojenliği: Farklı ülkelerde ve hatta aynı ülke içindeki farklı sağlık kurumlarında kullanılan sistemler (örneğin elektronik sağlık kayıt sistemleri, hastane bilgi sistemleri, sigorta yazılımları) hem teknik altyapı hem de veri formatları açısından büyük farklılıklar göstermektedir (303, 319). Bu çeşitlilik, evrensel bir blokzincir çözümünün uygulanmasını güçleştirmektedir.

Uyum ve Regülasyon Sorunları: Sağlık sektörü, yüksek düzeyde regülasyona tabidir. Blokzincir çözümlerinin veri gizliliği, hasta onamı, veri silme hakkı gibi regülasyonlara (ör. GDPR, HIPAA) nasıl entegre edileceği halen netleşmemiştir. Yeni teknolojilerin bu yasal çerçevelerle nasıl uyumlu hâle getirileceği zamanla gelişmektedir.

Standartların Eksikliği: Blokzincir tabanlı sağlık uygulamaları için evrensel kabul görmüş standartlar (ör. veri formatı, erişim protokolleri, birlikte çalışabilirlik çerçeveleri) henüz tam olarak oluşmamıştır. Bu da teknolojinin yaygınlaşmasının önünde önemli bir engel teşkil etmektedir.

Geliştirme ve Entegrasyon Maliyetleri: Blokzincir çözümleri genellikle özel olarak geliştirilmekte ve mevcut sistemlere entegre edilmesi karmaşık bir mühendislik süreci gerektirmektedir. Bu süreç, teknik yeterlilik, zaman ve maliyet açısından sağlık kurumları için caydırıcı olabilmektedir.

Yasal ve Etik Zorluklar:

Sağlık hizmetleri gibi hassas verilerin olduğu alanlarda, blokzincir sistemlerinin katı düzenlemelere (GDPR ve HIPAA gibi düzenlemeler zımnen veya açıkça bahsedilmiştir) uyması gerekmektedir. Merkeziyetsiz ve dağıtılmış yapıların bu düzenlemelerle nasıl uyumlu hale getirileceği bir zorluktur.

Blokzincir teknolojisinin tasarımı ve uygulanması, etik ilkelere uygun bir şekilde yapılmalıdır. Özellikle Proof-of-Work (PoW) gibi enerji yoğun mutabakat mekanizmalarının artış gösteren elektrik ihtiyacı nedeniyle potansiyel yan etkileri (örneğin "kripto-hasarlar" ve nihayetinde sağlık sorunları) ve çevreye verilebilecek zararlar endişe kaynağı olabilir. Sağlık gibi kamu yararına hizmet veren bir alanda böyle bir sistem kullanmak çevre etiği bağlamında sorunlar yaratabilir. Bu durum, sürdürülebilir ve etik bir sağlık sistemi sağlama yolunda nasıl uygulanması gerektiği konusunda düşünmeyi gerektirir. Proof-of-Stake (PoS) gibi alternatif mekanizmalar daha az enerji gerektirir.

Veri Yönetimi ve Gizlilik:

Hassas sağlık bilgilerini korumak blokzincir tabanlı veri paylaşım sistemlerinin en kritik zorluklarından biridir. Kullanıcı ve grup tabanlı gizli paylaşım gibi kriptografik algoritmalar bu zorluğun üstesinden gelmeye yardımcı olabilir. Ayrıca önerilen federe sistem, blokzincire yüklenecek olan veri oranını azaltarak verilerin federe olarak depolanmasını sağlar, yapılan işlem bilgilerini blokzincire kaydederek etik bir yapı sunar. Bunun yanı sıra yeni gelişen teknolojilerden olan IPFS

(InterPlanetary File System) teknolojisi de sağlık alanında güvenilir ve gizlilik vaat eden bir depolama sistemi olarak kullanılabilir. IPFS teknolojisi sağlık verileri bağlamında önerilen ve gelecek vaat eden bir teknoloji olarak değerlendirilebilir.

5.4.3 Politika ve düzenleme önerileri

Büyük verinin etik bir şekilde yönetilmesi yalnızca teknolojik çözümlerle mümkün değildir. Her ne kadar teknoloji insan yararına kullanım amacıyla geliştirilse de, kötüye kullanım potansiyeli de barındırmaktadır. Bu nedenle, teknolojik altyapının etik ilkelere uygun biçimde işleyebilmesi; güçlü, insan haklarını ve toplumsal değerleri önceleyen bir yasal ve yönetsel çerçeveyle desteklenmelidir.

Önerilen merkeziyetsiz yapı (federe sistem) ve blokzincir teknolojisi, etik ilkeler açısından önemli fırsatlar sunsa da, bu yapıların etkin ve güvenli biçimde uygulanabilmesi için kapsamlı düzenleyici çerçevelere ihtiyaç duyulmaktadır. Bu bağlamda hem birey haklarının korunması hem de veri yönetim süreçlerinin şeffaf ve hesap verebilir bir biçimde yürütülmesi açısından aşağıdaki politika ve düzenleme önerileri sunulmaktadır:

- Veri mülkiyeti hakkı açıkça tanımlanmalı; bireylerin kendi verileri üzerindeki sahipliği yasal güvence altına alınmalıdır.

- Federe sistemler ve blokzincir altyapılarının tanımı, kullanım koşulları ve tarafların sorumluluk alanları net biçimde belirlenmelidir.

- Veri kullanım amacı kamusal ve bilimsel fayda ile sınırlandırılmalı; ticari kullanımlara yönelik açık kısıtlamalar getirilmelidir.

- Etik kurullar ve veri yönetişim mekanizmaları genişletilmeli; bu yapılar farklı disiplinlerin katkısını içeren katılımcı modellerle desteklenmelidir.

Bu öneriler, yalnızca teknik değil aynı zamanda hukuki ve etik temeller üzerine kurulu bütüncül bir veri yönetim sistemi inşası için gereklidir.

Blokzincir teknolojisinin sağlık hizmetlerinde kullanımı, yalnızca teknik güvenlik vaatleriyle sınırlı değildir; aynı zamanda düzenleyici uyum, etik denetim, yönetişim

mekanizmaları ve politika yapım süreçleriyle de doğrudan ilişkilidir. Özellikle veri güvenliği, şeffaflık, bireysel mahremiyet ve hesap verebilirlik gibi etik ilkeler, bu teknolojilerin sağlık alanındaki uygulanabilirliğini şekillendiren başlıca faktörler arasında yer almaktadır.

Bu bağlamda, politika yapıcıların sadece teknolojinin teknik işleyişine odaklanmaları yeterli değildir. Aynı zamanda, çevresel sürdürülebilirlik, sosyal etkiler ve uzun vadeli etik sonuçlar gibi daha geniş bir perspektiften hareket etmeleri gerekmektedir. Özellikle farklı mutabakat mekanizmalarının çevresel etkileri ve güvenlik düzeyleri arasındaki farklar, teknoloji tercihlerini doğrudan etkilemektedir. Örneğin, Proof-of-Stake gibi mekanizmalar daha düşük enerji tüketimi sunarken, henüz Proof-of-Work kadar güçlü bir güvenlik seviyesi sağlayamayabilir (319). Bu da, özellikle hassas sağlık verilerinin söz konusu olduğu durumlarda, teknolojik tercihlere dair dikkatli bir değerlendirme yapılmasını zorunlu kılmaktadır.

Blokzincir tabanlı uygulamaların bir diğer temel sorunu ise, mevcut yasal düzenlemelerle olan uyum zorluklarıdır. Sağlık verilerinin yoğun biçimde regülasyona tabi olduğu alanlarda, bu teknolojilerin Avrupa Birliği'nin GDPR'si ya da ABD'nin HIPAA düzenlemeleri gibi veri koruma yasalarıyla uyumlu hâle getirilmesi önemli bir gündemdir. Blokzincirin değiştirilemez ve merkeziyetsiz yapısı, özellikle verinin silinmesi ya da düzeltilmesi gibi hakların uygulanmasını zorlaştırmakta; bu da teknolojinin yasal sistemlere entegrasyonunu karmaşıklaştırmaktadır (339).

Blokzincir sistemleri teoride yüksek güvenlik sunuyor olsa da pratikte veri girişlerinin doğruluğu garanti edilememektedir. Sisteme hatalı veya kötü niyetli veri girilmesi hâlinde, bu veriler blokzincir üzerinde kalıcı hâle gelebilmektedir. Ayrıca kullanıcıların onam verme süreçlerinde baskı altına alınması, yönlendirilmesi veya rızalarının ihlali gibi riskler de söz konusudur (303). Bu nedenle teknolojinin kendi kendine yeterli bir güvenlik altyapısı sunduğu varsayımı yeterli değildir; aynı zamanda yönetişim, düzenleme ve denetleme mekanizmalarının da aktif biçimde devrede olması gerekmektedir.

Bununla birlikte, blokzincirin düzenleyici taleplere göre yeniden yapılandırılabilir bir esnekliğe sahip olduğu da görülmektedir. Özellikle özel izinli blokzincirlerde,

akıllı sözleşmelerin yapılandırılması ve sistemin düzenleyici ihtiyaçlara göre uyarlanması mümkündür (303). Bu yönüyle blokzincir, katı ve değişmez bir sistem değil; çeşitli senaryolara göre adapte edilebilen bir altyapı olarak değerlendirilebilir.

Etik açıdan bakıldığında, blokzincir yönetişiminin yalnızca teknik değil, normatif bir zeminde de ele alınması gerektiği açıktır. Şeffaflık ile gizlilik arasındaki denge, adaletin sağlanması, bireylerin verileri üzerinde kontrol sahibi olması ve hesap verebilirlik gibi ilkeler, farklı etik teoriler bağlamında yeniden tartışılmaktadır (311). Bu teorik zemin, uygulamaların yalnızca etkin değil, aynı zamanda adil ve meşru olmasını da sağlamaya yöneliktir.

Blokzincirin yalnızca veri depolama ve paylaşım aracı değil, aynı zamanda doğrudan bir politika aracı olarak yeniden kurgulanabileceği de dikkat çekici bir yaklaşımdır. Özellikle çok kurumlu araştırma projelerinde etik onay süreçlerinin sadeleştirilmesi ve veri paylaşımının daha verimli hâle getirilmesi için blokzincirin kullanılabileceği öne sürülmektedir. Bu tür örnekler, geleneksel bürokratik yapılarla dijital altyapıların nasıl entegre edilebileceğine dair yenilikçi politika fikirleri sunmaktadır (309).

Son olarak, blokzincir teknolojisinin sağlık sistemleriyle entegrasyonu açısından karşılaşılan en temel sorunlardan biri de standartlaşma eksikliğidir. Farklı blokzincir platformlarının birbirinden oldukça farklı teknik özelliklere sahip olması, sistemler arası birlikte çalışabilirliği zorlaştırmakta; bu da sürdürülebilir ve yaygın bir kullanımın önünde engel teşkil etmektedir. Güvenlik, esneklik ve birlikte çalışabilirlik gibi gereksinimlerin dengeli bir biçimde gözetildiği mimari tasarımlar henüz istikrarlı biçimde yerleşmemiştir (307).

Özetle, blokzincir sistemlerinin sağlık hizmetlerinde uygulanmasının mevcut yasal çerçevelerle (HIPAA, GDPR gibi) uyum sağlaması gerektiğini, veri kalitesi ve rıza gibi konularda ek yönetişim ve düzenlemelerin gerekli olduğunu, teknolojinin kendisinin düzenleyici gereksinimlere göre yapılandırılabileceğini (örn. akıllı sözleşmeler, izinli blokzincirler), etik değerlendirmelerin politika için önemli bir zemin oluşturduğunu ve blokzincirin belirli alanlarda bir politika aracı olarak

kullanılabileceği açıktır. Ancak, alanın hala gelişmekte olduğu ve standart çözümlerin henüz tam olarak belirlenmediği de anlaşılmaktadır.

Ancak bu teknolojinin getirdiği olanaklar kadar, etik açıdan yeni sorumluluk alanları da doğurabileceği unutulmamalıdır. Örneğin, sistemin tasarımında veri sahibi bireylerin bilgilendirilmiş onamlarının nasıl alınacağı, acil durumlarda erişim yetkisinin nasıl belirleneceği gibi hususlar dikkatle planlanmalıdır.

5.4.4 Sağlık verilerinin gelecek perspektifi

Sağlık verilerinin geleceği, sadece teknik bir dönüşümü değil, aynı zamanda sağlık sisteminin temel işleyişini kökten değiştirecek bir paradigma kaymasını da beraberinde getirmektedir. Günümüzde dijitalleşme ile birlikte sadece hastane kayıtları değil; giyilebilir teknolojiler, genetik analizler, mobil sağlık uygulamaları ve yaşam tarzına ilişkin veriler de sağlık veri ekosistemine dahil olmaktadır. Bu gelişme, bireylerin yalnızca hastalandıktan sonra tedavi edilmesi anlayışını aşarak, hastalık ortaya çıkmadan önce risklerin belirlenmesi ve önlenmesine dayalı yeni bir sağlık yaklaşımının zeminini hazırlamaktadır.

Sağlık verilerinin gelecekteki kullanımları, tahmine dayalı analitik (predictive analytics), yapay zeka ve makine öğrenimi teknolojilerinin sağlık hizmetlerinde devrim yaratma potansiyeli bağlamında değerlendirilmektedir Veri analiz kapasitesinin artmasıyla birlikte, bireyin biyolojik ve çevresel özelliklerine göre potansiyel sağlık sorunları önceden öngörülebilecek, hatta erken uyarı sistemleriyle bu sorunların hiç ortaya çıkmaması sağlanabilecektir (340). Böylece sağlık hizmetleri, reaktif (tepkisel) olmaktan çıkıp proaktif ve öngörücü (predictive) bir yapıya evrilecektir. Bu durum, sağlık sisteminin merkezine artık hastalıkları değil, verileri ve bu verilerle sağlanan önleyici bilgeliği yerleştirmektedir.

Sağlık verilerinin geleceği bağlamında öngörülen bu yaklaşımlar, kronik hastalıkların artan yükünü ele almak ve reaktif tedavi modellerinden önleyici stratejilere geçişi sağlamak için kilit öneme sahiptir.

Sağlık verilerinin gelecekteki önemli kullanım alanları şunlardır:

- Erken Hastalık Teşhisi ve Önleyici Sağlık Hizmetleri: Tahmine dayalı analitik, diyabet, kardiyovasküler rahatsızlıklar ve kanser gibi hastalıkların erken başlangıcını tespit etmede dönüştürücü bir potansiyel sunmaktadır (341). Yapay zeka ve makine öğrenimi algoritmaları, hastalık modellerini ve risk faktörlerini yüksek hassasiyetle belirleme yeteneği sayesinde tanısal doğruluğu geleneksel yöntemlere göre %40'a kadar artırmıştır (340). Bu modeller, bireysel risk profillerine dayalı olarak kişiselleştirilmiş sağlık hizmeti önerileri sunmaktadır.

- Çeşitli Veri Kaynaklarının Entegrasyonu: Gelecekte, elektronik sağlık kayıtları (EHR'ler), giyilebilir cihaz verileri, demografik bilgiler ve genomik veriler gibi farklı veri setlerinin entegrasyonu ve analizi büyük önem taşıyacaktır. Bu entegrasyon, kapsamlı tahmine dayalı modellerin geliştirilmesine olanak tanıyacaktır (229, 340, 342).

- Gerçek Zamanlı İzleme ve Erken Uyarı Sistemleri: Giyilebilir cihazlar (Fitbit, Apple Watch gibi) ve Nesnelerin İnterneti (IoT) sensörleri, kalp atış hızı, kan basıncı ve aktivite düzeyleri gibi fizyolojik verileri sürekli olarak toplayarak tahmine dayalı sağlık hizmetleri için önemli bir rol oynamaktadır (343). Bu cihazlar, kronik hastalıkların erken uyarı işaretlerini tespit etmede ve yüksek riskli bireyler için sürekli izleme ve erken uyarı sistemleri sağlamada giderek daha önemli hale gelecektir (229). Örneğin, giyilebilir glikoz monitörleri diyabet yönetiminde, giyilebilir kalp atış hızı monitörleri ise kardiyak anomalileri belirlemede etkili olmuştur (342).

- Pandemi Tahmini ve Kaynak Tahsisi: Tahmine dayalı analitik, COVID-19 pandemisi gibi halk sağlığı krizlerini yönetmede kritik bir rol oynamıştır ve gelecekte de daha da oynayacaktır (342). Makine öğrenimi modelleri ve istatistiksel tahmin yöntemleri, vaka eğilimlerini, ölüm oranlarını ve sağlık hizmetleri taleplerini tahmin etmek için kullanılmaktadır. Bu modeller, kaynak tahsisini optimize ederek ve sağlık sistemleri üzerindeki yükü azaltarak halk sağlığı acil durumlarında veri odaklı karar almayı destekleyebilir (344).

- Hastalık Yönetimi ve Popülasyon Sağlığı Stratejileri: Tahmine dayalı analitik, bireysel düzeydeki müdahalelerin ötesine geçerek popülasyon sağlığı stratejilerine de uygulanacaktır (342, 344). Giyilebilir cihazları ve IoT sensörlerini entegre eden gerçek zamanlı izleme sistemleri, kardiyovasküler olayların erken uyarı işaretlerini belirlemede etkili olmuştur. Ayrıca, bu analitikler, yaşam tarzı değişiklikleri programları ve aşılama kampanyaları gibi önleyici müdahalelerin maliyet etkinliğini değerlendirerek sınırlı halk sağlığı kaynaklarının optimal tahsisini sağlayabilir (342).

- İleri Görüntüleme Analitiği ve Biyobelirteç Entegrasyonu: Kanser gibi hastalıkların erken teşhisi için yapay zeka algoritmaları, mamogramlar ve BT taramaları gibi tıbbi görüntüleri analiz etmede önemli doğruluk göstermiştir (229). Gelecekte, biyobelirteçler (protein seviyeleri, hormon reseptörleri, gen mutasyonları) ve genomik verilerin tahmine dayalı kanser modellerine entegrasyonu, erken teşhisin doğruluğunu daha da artıracaktır (343).

Ancak, tahmine dayalı analitiğin tam potansiyelini açığa çıkarmak için gelecekte veri gizliliği endişeleri, model tahminlerindeki önyargılar, mevcut sağlık altyapılarıyla entegrasyon engelleri, veri kalitesi ve etik hususlar gibi önemli zorlukların aşılması gerekmektedir. Bu zorlukların üstesinden gelmek için sağlık hizmeti sağlayıcıları, veri bilimcileri ve politika yapıcılar arasında disiplinlerarası işbirliği temel olacaktır (342). Ayrıca, hastaların veri güvenliği ve yapay zekanın etik kullanımı konusunda güvenini sağlamak da yaygın benimseme için hayati öneme sahiptir.

İşte bu dönüşüm, verinin güvenliğini, gizliliğini ve etik kullanımını her zamankinden daha önemli hâle getirmektedir. Çünkü artık yalnızca geçmişin değil, geleceğin de veriler üzerinden şekilleneceği bir döneme girilmektedir. Gelecek, şeffaf algoritmaların, birey merkezli veri kontrolünün ve güven temelli altyapıların üzerinde inşa edilmediği sürece, öngörülebilir olmaktan çok yönlendirilebilir bir yapıya bürünebilir. Bu nedenle, sağlık verilerinin geleceği, yalnızca teknolojik kapasiteyle değil, aynı zamanda etik ilke, toplumsal denetim ve birey mahremiyetiyle birlikte düşünülmelidir. Kısacası, sağlık verilerinin geleceği artık "gelecek" değildir; şimdi'nin içinde, derin bir şekilde şekillenmektedir. Ve bu şekillenişin yönü, verinin kimde

olduğu kadar, bu verinin kimin yararına, hangi sınırlar içinde ve ne amaçla kullanıldığına bağlı olacaktır.

Bu etik farkındalıkla, yalnızca teorik ilkelerin değil, aynı zamanda uygulamada etkili olan sistemlerin de değerlendirilmesi gerekmektedir. Bazı ülkeler, veri yönetişimini bu ilkeler doğrultusunda somut sistemlerle hayata geçirmiştir. Estonya, bu sistemi etkin biçimde uygulayan öncü ülkelerden biridir. Estonya'nın dijital altyapısı olan KSI Blockchain sistemi, kamu verilerinin bütünlüğünü sağlamak üzere geliştirilmiştir (345).

Bu tür yapılar, sadece Estonya ile sınırlı kalmayıp, Tayvan, Birleşik Arap Emirlikleri (BAE) ve Avrupa Birliği (AB) gibi çeşitli ülke ve bölgesel yapılarda da pilot projeler veya yapılandırma aşamasındaki stratejiler kapsamında test edilmektedir. Örneğin Tayvan'da Taipei Tıp Üniversitesi Hastanesi ile DTCO iş birliğinde geliştirilen "phrOS" isimli kişisel sağlık kayıt sistemi, blokzincir teknolojisini kullanarak hastaların elektronik tıbbi kayıtlarının güvenliğini ve transferini sağlamaktadır (346). Birleşik Arap Emirlikleri ise Sağlık ve Önleme Bakanlığı, sağlık çalışanlarının kimlik ve yeterlilik bilgilerini güvenli biçimde doğrulamak ve paylaşmak amacıyla blokzincir tabanlı bir sistem uygulamaya koymuştur (347). Ayrıca Dubai Sağlık Otoritesi, elektronik sağlık kayıtlarını blokzincir ile güvence altına almak üzere pilot projeler yürütmektedir (348). Avrupa Birliği düzeyinde ise, Avrupa Sağlık Veri Alanı (European Health Data Space) hedefleri doğrultusunda HealthData@EU Pilot Projesi başlatılmıştır. Bu proje ile sağlık verilerinin sınır ötesi paylaşımına olanak tanıyan, birlikte çalışabilir ve güvenli bir altyapının test edilmesi amaçlanmaktadır (349).

Sağlık verisinin kontrolünün bireye bırakıldığı, erişimlerin blokzincir teknolojisi ile denetlendiği bu modellerin, hem etik şeffaflık hem de teknolojik güvenlik açısından önemli bir paradigma değişimini temsil ettiği söylenebilir. Gelecek yıllarda, sağlık bilişimi alanında bu tür dağıtık ve güvenli altyapıların daha fazla konuşulması ve çeşitli ülkelerde ölçeklenerek uygulanması kuvvetle muhtemeldir. Bu bağlamda, sağlık verilerinin yönetiminde federe sistemlerin blokzincir teknolojileriyle bütünleştirilmesi, birey-merkezli, güvenli ve etik açıdan sürdürülebilir bir dijital sağlık sisteminin temelini oluşturacaktır.

Bu çalışmada önerilen sistem, mevcut sağlık verisi yönetiminde karşılaşılan etik ve yapısal sorunlara çözüm sunma potansiyeline sahiptir. Ancak, bu öneri, mutlak bir çözümden ziyade güncel teknolojik olanaklar çerçevesinde uygulanabilir ve etkili bir yaklaşım olarak değerlendirilmelidir. Teknolojik gelişmelerin hızla ilerlediği günümüzde, gelecekte farklı altyapılar, yeni güvenlik protokolleri ve alternatif veri yönetim teknolojileri ortaya çıkabilir. Dolayısıyla bu sistem, verinin merkeziyetçi yapılardan çıkarılması ve birey merkezli, denetlenebilir bir yapı kurulması açısından önemli bir adım olmakla birlikte, gelecekteki teknolojik yenilikler ışığında yeniden ele alınmalı ve güncellenebilir nitelikte olmalıdır. Zira veri her geçen gün büyüyerek hızla ilerlerken teknolojik gelişmelerden yararlanmamak geri kalmaya mahkûm bir tercih olur.

6 SONUÇ

Günümüzde dijital teknolojilerdeki hızlı gelişmelerle birlikte "büyük veri" kavramı, sağlık alanında da önemli bir yer edinmiştir. Büyük veri, yalnızca veri miktarının çokluğu ile değil; aynı zamanda hızla üretilmesi (velocity), çeşitli biçimlerde olması (variety), doğruluğunun ve güvenilirliğinin tartışmalı olması (veracity), değer taşıması (value) ve büyük hacimli olması (volume) gibi temel beş özellik üzerinden, yani 5V çerçevesinde tanımlanmaktadır.

Büyük sağlık verisi; yalnızca hastalık kayıtlarını değil, aynı zamanda klinik verileri, tıbbi görüntüleme sonuçlarını, genetik bilgileri, çevresel ve davranışsal verileri, mobil sağlık uygulamalarından elde edilen verileri ve hasta takibi gibi geniş ve çeşitli veri kaynaklarını kapsamaktadır. Bu kadar çok boyutlu ve hassas verinin toplanması, işlenmesi, depolanması ve paylaşılması, etik açıdan ciddi soruları ve sorunları da beraberinde getirmektedir. Özellikle veri gizliliği, veri güvenliği, mahremiyet, bireyin özerkliği, veri üzerindeki kontrol hakkı, şeffaflık eksikliği ve veri sahipliğine ilişkin belirsizlikler, sağlıkta büyük veri yönetiminin temel etik sorunlarını oluşturmaktadır.

Her ne kadar yasal ve etik yönetmeliklerle bu etik sorunların üstesinden gelineceği düşünülse de, mevcut yasa ve yönetmelikler, hem teknolojinin hızına ayak uydurmakta zorlanmakta hem de çağın özgün etik sorunlarına etkili çözümler sunmakta yetersiz kalmaktadır. Bu durum, yalnızca hukukî düzenlemeler ya da etik yönetmeliklerle büyük sağlık verisinden kaynaklanan etik sorunların tam anlamıyla çözülemeyeceğini ortaya koymaktadır. Bu nedenle çalışmada, teknolojinin neden olduğu etik sorunlara yine teknolojik çözümlerle yaklaşılması gerektiği düşüncesinden hareketle, kişisel verilerin korunmasına yönelik en uygun teknoloji ve sistem altyapıları araştırılmıştır. Özellikle merkeziyetçi olmayan yapıların ve etik değerlerle uyumlu teknolojilerin potansiyeli incelenmiş; çağımızın etik sorunlarını hafifletme kapasitesine sahip sistem önerileri geliştirilmiştir. Böylece, teknolojinin doğurduğu etik sorunlara yine etik bir vizyon sunan yeni teknolojiler aracılığıyla çözüm üretilebileceği savunulmuştur.

Bu etik sorunlara çözüm getirmek amacıyla ilk olarak ilkesel ardından da ilkeyi uygulayabilecek teknolojik yaklaşımlar geliştirilmiştir. İlkesel yaklaşımlar arasında

özellikle FAIR veri yönetimi ilkeleri dikkat çekmektedir. İngilizce "Findable, Accessible, Interoperable, Reusable" kavramlarının baş harflerinden oluşan FAIR ilkeleri; verinin bulunabilir, erişilebilir, birlikte çalışabilir ve yeniden kullanılabilir olması gerektiğini savunur. 2016 yılında geliştirilen bu ilkeler, büyük sağlık verisinin etik, şeffaf ve sürdürülebilir bir şekilde yönetilmesi için yol gösterici bir çerçeve sunmaktadır. Ancak, teorik olarak güçlü olan bu ilkelerin uygulamada başarıya ulaşabilmesi için, bunları destekleyecek teknik altyapılara da ihtiyaç vardır.

Bu bağlamda, tez kapsamında FAIR ilkelerini destekleyici iki temel teknolojik yapı önerilmiştir: blokzincir (blockchain) teknolojisi ve federe sistemler. Blokzincir, verilerin değiştirilemez ve geriye dönük olarak izlenebilir biçimde kayıt altına alınmasını sağlayan, dağıtık bir dijital kayıt sistemidir. Bu yapı, verinin yetkisiz erişimlere karşı korunmasını ve kayıtların şeffaflık içinde yönetilmesini mümkün kılarak güven duygusunu artırır.

Diğer yandan, federe sistemler merkezi bir veritabanına ihtiyaç duymadan, verilerin farklı kurum ve kuruluşlarda kalmasını ve gerektiğinde güvenli biçimde paylaşılmasını mümkün kılar. Bu yapı, hem bireylerin verileri üzerindeki denetimini artırmakta hem de veri sahipliği tartışmalarına çözüm sunmaktadır. Ayrıca, merkezileşmeden doğan güvenlik risklerini azaltarak veri mahremiyeti ve özerkliğinin korunmasına katkı sağlamaktadır.

Bu doğrultuda, büyük sağlık verisinin giderek daha kritik bir rol üstlendiği günümüz sağlık sistemlerinde, etik sorumlulukların ve veri temelli uygulamaların iç içe geçtiği çok katmanlı bir yapıyı gözler önüne sermektedir. Sağlık alanında dijitalleşme ve veri odaklı uygulamaların artmasıyla birlikte kişiselleştirilmiş ve hassas tıp yaklaşımları, bireylerin sağlık durumlarının henüz hastalık ortaya çıkmadan öngörülebilmesini mümkün kılmakta, böylece sağlık yalnızca tedavi edici değil aynı zamanda önleyici bir hizmet alanına dönüşmektedir.

Ancak bu dönüşüm, beraberinde önemli etik sorunlar doğurmaktadır. Sağlık verilerinin gizliliği, güvenliği, mahremiyeti ve veri sahipliği, yalnızca bireysel haklar açısından değil, aynı zamanda sağlık sistemlerinin sürdürülebilirliği ve kamu yararı

açısından da kritik önemdedir. Mevcut merkeziyetçi veri yönetim sistemlerinin bu etik sorumlulukları karşılamada yetersiz kaldığı çalışmada açıkça ortaya konmuştur.

Bu bağlamda tez, FAIR veri yönetimi ilkelerini (Bulunabilirlik, Erişilebilirlik, Birlikte Çalışabilirlik, Yeniden Kullanılabilirlik) yalnızca teknik değil, aynı zamanda etik bir çerçevede tartışmıştır. Sağlık verileri yalnızca birey temelli olarak değil, aynı zamanda gelecekteki bilimsel araştırmalar ve toplum sağlığı için de büyük potansiyele sahiptir. Bu nedenle verilerin araştırma platformlarında bulunabilir, erişilebilir, birlikte çalışabilir ve yeniden kullanılabilir olması, bilimsel ilerleme ve kamusal sağlık yararı açısından elzemdir. Bu çalışma, FAIR ilkelerini bu bağlamda ele alarak, özellikle araştırma temelli platformlardaki olası güçlükleri çözmeye katkı sunmaya aday olan FAIR'i ve söz konusu ilkeleri etik yönleriyle birlikte değerlendirmiştir.

Tüm bu değerlendirmeler doğrultusunda, tezde önerilen merkezi olmayan (federe) sistem ve blokzincir temelli sağlık veri yönetimi modeli, bireylerin verileri üzerindeki denetimini güçlendirirken, aynı zamanda araştırma ve kamu yararını da önceleyen bir yapı sunmaktadır. Açık rıza ilkesine dayalı, şeffaf, güvenli ve sürdürülebilir bu yapı, hem mevcut etik sorunlara çözüm üretme hem de gelecekteki sağlık politikalarının güven temelli gelişmesine katkı sağlama potansiyeline sahiptir.

Bu tez çalışması, büyük sağlık verisinin yönetiminde etik ilkelerin yalnızca teorik bir zemin olarak kalmaması, teknolojik ve toplumsal dönüşümler karşısında yenilenebilen, bağlama göre esneyebilen ve çok disiplinli katkılarla yeniden inşa edilebilen dinamik bir etik yapısını esas almaktadır. Çalışma, etiğin yeni teknolojik altyapılarla desteklenmesi ve birey ile toplum yararı arasında adil bir denge kurulması gerektiğini vurgulamaktadır. Sağlık verisinin geleceği, yalnızca teknik kapasiteyle değil; etik duyarlılık, hak temelli yaklaşım ve kolektif sorumlulukla şekillenmelidir.

7 KAYNAKLAR

1. Olson K. What are data? : SAGE Publications Sage CA: Los Angeles, CA; 2021. p. 1567-9.
2. Ardito L, Cerchione R, Mazzola E, Raguseo E. Industry 4.0 transition: a systematic literature review combining the absorptive capacity theory and the data–information–knowledge hierarchy. Journal of Knowledge Management. 2022;26(9):2222-54.
3. Coyle D, Manley A. What is the value of data? A review of empirical methods. Journal of Economic Surveys. 2024;38(4):1317-37.
4. Glaser BG. All is data. Grounded Theory Review: An International Journal. 2007;2(6).
5. Bellinger G, Castro D, Mills A. Data, information, knowledge, and wisdom. 2004.
6. Leonelli S. Data governance is key to interpretation: Reconceptualizing data in data science. Harvard Data Science Review. 2019;1(1).
7. Foucault M. Bilginin Arkeolojisi (1 b.). V Urhan, Çev) İstanbul: Birey Yayınları. 1999.
8. Han B-C. Enfokrasi: Dijitalleşme ve demokrasinin krizi: Ketebe Yayınları; 2022.
9. Akkurt SS. Kişisel veri kavramının hukukî niteliğine ilişkin yaklaşımlara mukayeseli bir bakış. Kişisel Verileri Koruma Dergisi. 2020;2(1):20-32.
10. Yeşiltuna O. Türkçe Hukuk Yazınında Kişisel Verilerin Korunması Üzerine Bir Araştırma (2000-2020). Kişisel Verileri Koruma Dergisi. 2022;4(1):25-37.
11. 6698 Sayılı Kişisel Verilerin Korunması Kanun'unun Amacı ve Kapsamı, (2016).
12. GDPR- (AB) 2016/679 sayılı Avrupa Parlamentosu ve Konsey Tüzüğü (Genel Veri Koruma Tüzüğü), (2016).
13. Chatellier R. Post-mortem data: Is there a digital life after death? 2025 [Available from: https://linc.cnil.fr/en/Post-mortem_data_is_there_a_digital_life_after_death.
14. Taylor L. What is data justice? The case for connecting digital rights and freedoms globally. Big Data & Society. 2017;4(2):2053951717736335.
15. Van Dijck J, Poell T, De Waal M. The platform society: Public values in a connective world: Oxford university press; 2018.
16. Zuboff S. Big other: surveillance capitalism and the prospects of an information civilization. Journal of information technology. 2015;30(1):75-89.
17. Bulut F. Sağlıkta Büyük Veri: Ulusal Düzenlemeler Ve Veri Kayıt Sistemlerinin Tıp Etiği Açısından Incelenmesi: Bursa Uludag University (Turkey); 2023.
18. Acquisti A, Gross R, editors. Imagined communities: Awareness, information sharing, and privacy on the Facebook. International workshop on privacy enhancing technologies; 2006: Springer.
19. Lyon D. Surveillance, Snowden, and big data: Capacities, consequences, critique. Big data & society. 2014;1(2):2053951714541861.
20. Subrahmanya SVG, Shetty DK, Patil V, Hameed BZ, Paul R, Smriti K, et al. The role of data science in healthcare advancements: applications, benefits, and future prospects. Irish Journal of Medical Science (1971-). 2022;191(4):1473-83.

21. Cohen IG, Lynch HF, Vayena E, Gasser U. Big data, health law, and bioethics: Cambridge University Press; 2018.
22. Bulut M. Özel Bir Hukuksal Koruma ve Veri Kategorisi Alanı: Hassas Kişisel Veriler. Ankara Barosu Dergisi. 2020;78(3):99-150.
23. Badawy M, Ramadan N, Hefny HA. Big data analytics in healthcare: data sources, tools, challenges, and opportunities. Journal of Electrical Systems and Information Technology. 2024;11(1):63.
24. Dündar A, Hacıvelioğlu D, Erdoğdu S, Gündüz N. Kişisel sağlık verilerinin kayıt ve korunmasına ilişkin tutumlar: İstanbul'da bir devlet hastanesi örneği. Türkiye Biyoetik Dergisi. 2024;11(1):17-27.
25. Sahay S. Big data and public health: Challenges and opportunities for low and middle income countries. Communications of the Association for Information Systems. 2016;39(1):20.
26. Kitchin R. Big Data, new epistemologies and paradigm shifts. Big data & society. 2014;1(1):2053951714528481.
27. Jacobs A. The pathologies of big data. Communications of the ACM. 2009;52(8):36-44.
28. Raghupathi W, Raghupathi V. Big data analytics in healthcare: promise and potential. Health information science and systems. 2014;2:1-10.
29. Harari YN. Hayvanlardan tanrılara sapiens: Hanifi Boyalan; 2019.
30. Diamond J. Tüfek, mikrop ve çelik: pegasus yayınları; 2022.
31. Arslan A. İlkçağ Felsefe Tarihi 2: Sofistler'den Platon'a (6. Baskı). İstanbul: Bilgi Üniversitesi Yayınları. 2017.
32. Salğar E. Bilimsel Devrim: Aristotelesçi Bilimden Modern Olana Geçişin Kısa Bir Öyküsü. FLSF Felsefe ve Sosyal Bilimler Dergisi. 2023(36):295-321.
33. Koyré A, Evrene KDS. Bilim ve Devrim Newton, çev. Nur Küçük, İstanbul: Salyangoz Yayınları. 2006.
34. Kuhn TS. Bilimsel devrimlerin yapisi: Alan; 1982.
35. Floridi L. Big data and their epistemological challenge. Philosophy & Technology. 2012;25(4):435-7.
36. Uçar A, İlkılıç İ. Büyük verinin sağlık hizmetlerinde kullanımında epistemolojik ve etik sorunlar. Sağlık Bilimlerinde İleri Araştırmalar Dergisi. 2019;2(2):80-92.
37. Patgiri R, Ahmed A, editors. Big data: The v's of the game changer paradigm. 2016 IEEE 18th international conference on high performance computing and communications; IEEE 14th international conference on smart city; IEEE 2nd international conference on data science and systems (HPCC/SmartCity/DSS); 2016: IEEE.
38. Bayrak T. A review of business analytics: A business enabler or another passing fad. Procedia-Social and Behavioral Sciences. 2015;195:230-9.
39. Laney D. 3D data management: Controlling data volume, velocity and variety. META group research note. 2001;6(70):1.

40. 40. Cremin CJ, Dash S, Huang X. Big data: historic advances and emerging trends in biomedical research. Current Research in Biotechnology. 2022;4:138-51.
41. Imran S, Mahmood T, Morshed A, Sellis T. Big data analytics in healthcare− A systematic literature review and roadmap for practical implementation. IEEE/CAA Journal of Automatica Sinica. 2020;8(1):1-22.
42. Labrinidis A, Jagadish HV. Challenges and opportunities with big data. Proceedings of the VLDB Endowment. 2012;5(12):2032-3.
43. Jensen PB, Jensen LJ, Brunak S. Mining electronic health records: towards better research applications and clinical care. Nature Reviews Genetics. 2012;13(6):395-405.
44. Ara A, Mifa AF. Integrating artificial intelligence and big data in mobile health: A systematic review of innovations and challenges in healthcare systems. Global Mainstream Journal of Business, Economics, Development & Project Management. 2024;3(01):01-16.
45. Xafis V, Schaefer GO, Labude MK, Brassington I, Ballantyne A, Lim HY, et al. An ethics framework for big data in health and research. Asian Bioethics Review. 2019;11(3):227-54.
46. Chen P-T, Lin C-L, Wu W-N. Big data management in healthcare: Adoption challenges and implications. International Journal of Information Management. 2020;53:102078.
47. Catalyst N. Healthcare big data and the promise of value-based care. NEJM Catalyst. 2018;4(1).
48. Dimitrov DV. Medical internet of things and big data in healthcare. Healthcare informatics research. 2016;22(3):156-63.
49. Dash S, Shakyawar SK, Sharma M, Kaushik S. Big data in healthcare: management, analysis and future prospects. Journal of big data. 2019;6(1):1-25.
50. Sabet C, Hammond A, Ravid N, Tong MS, Stanford FC. Harnessing big data for health equity through a comprehensive public database and data collection framework. NPJ Digital Medicine. 2023;6(1):91.
51. Shortreed SM, Cook AJ, Coley RY, Bobb JF, Nelson JC. Challenges and opportunities for using big health care data to advance medical science and public health. American journal of epidemiology. 2019;188(5):851-61.
52. Adeniyi AO, Arowoogun JO, Okolo CA, Chidi R, Babawarun O. Ethical considerations in healthcare IT: A review of data privacy and patient consent issues. World Journal of Advanced Research and Reviews. 2024;21(2):1660-8.
53. Altındiş S, Morkoç İK. Sağlık hizmetlerinde büyük veri. Ömer Halisdemir Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi. 2018;11(2):257-71.
54. Murdoch TB, Detsky AS. The inevitable application of big data to health care. Jama. 2013;309(13):1351-2.
55. Mcgrail K, Jones K, Akbari A, Bennett T, Boyd A, Carinci F, et al. A position paper on population data science: the science of data about people. Internatıonal Journal Of Populatıon Data Scıence. 2018;3(4).
56. 56. Okorie GN, Udeh CA, Adaga EM, DaraOjimba OD, Oriekhoe OI. Ethical considerations in data collection and analysis: a review: investigating ethical practices and challenges in modern data

collection and analysis. International Journal of Applied Research in Social Sciences. 2024;6(1):1-22.

57. Rosenbloom ST, Denny JC, Xu H, Lorenzi N, Stead WW, Johnson KB. Data from clinical notes: a perspective on the tension between structure and flexible documentation. Journal of the American Medical Informatics Association. 2011;18(2):181-6.
58. Cowie MR, Blomster JI, Curtis LH, Duclaux S, Ford I, Fritz F, et al. Electronic health records to facilitate clinical research. Clinical Research in Cardiology. 2017;106:1-9.
59. Sax U, Schmidt S. Integration of genomic data in electronic health records. Methods of information in medicine. 2005;44(04):546-50.
60. Jha AK, DesRoches CM, Campbell EG, Donelan K, Rao SR, Ferris TG, et al. Use of electronic health records in US hospitals. New England Journal of Medicine. 2009;360(16):1628-38.
61. Yu S, Li A, Chen Y, Wang D, Tang X. Heterogeneous network-based algorithms in the biomedical data mining: A review from technical perspective. Informatics and Health. 2024;1(2):111-22.
62. Fouad K, Vavrek R, Surles-Zeigler M, Huie J, Radabaugh H, Gurkoff G, et al. A practical guide to data management and sharing for biomedical laboratory researchers. Experimental Neurology. 2024;378:114815.
63. (WHO) WHO. Coronavirus disease (COVID-19): Ventilation and air conditioning 2021 [Available from: https://www.who.int/news-room/questions-and-answers/item/coronavirus-disease-covid-19-ventilation-and-air-conditioning.
64. (CDC) CfDCaP. Ventilation in buildings 2021 [Available from: https://www.cdc.gov/coronavirus/2019-ncov/community/ventilation.html.
65. Stoumpos AI, Kitsios F, Talias MA. Digital transformation in healthcare: technology acceptance and its applications. International journal of environmental research and public health. 2023;20(4):3407.
66. Premi G, Solainayagi P, Srinivasan C, Kuppusamy P, editors. Data Privacy and Confidentiality in Healthcare Applications of IoT-Enabled Wireless Sensor Networks. 2023 Second International Conference On Smart Technologies For Smart Nation (SmartTechCon); 2023: IEEE.
67. Kashani MH, Madanipour M, Nikravan M, Asghari P, Mahdipour E. A systematic review of IoT in healthcare: Applications, techniques, and trends. Journal of Network and Computer Applications. 2021;192:103164.
68. Mardis ER. Next-generation DNA sequencing methods. Annu Rev Genomics Hum Genet. 2008;9(1):387-402.
69. Ansorge WJ. Next-generation DNA sequencing techniques. New biotechnology. 2009;25(4):195-203.
70. Stephens ZD, Lee SY, Faghri F, Campbell RH, Zhai C, Efron MJ, et al. Big data: astronomical or genomical? PLoS biology. 2015;13(7):e1002195.
71. Watson JD, Crick FH, editors. The structure of DNA. Cold Spring Harbor symposia on quantitative biology; 1953: Cold Spring Harbor Laboratory Press.

72. Bal SH, Budak F. Genomik, proteomik kavramlarına genel bakış ve uygulama alanları. Uludağ Üniversitesi Tıp Fakültesi Dergisi. 2013;39(1):65-9.
73. Institute NHGR. Genome 2024 [Available from: https://www.genome.gov/genetics-glossary/Genome.
74. Başaran E, Aras S, Cansaran-duman D. Genomik, proteomik, metabolomik kavramlarına genel bakış ve uygulama alanları. Türk Hijyen ve Deneysel Biyoloji Dergisi. 2010;67(2):85-96.
75. Pearson H. Genetics: what is a gene? Nature. 2006;441(7092).
76. Griffiths AJ. An introduction to genetic analysis: Macmillan; 2005.
77. Yarman B, Gürkan H, Güz Ü, Aygün B. A new modeling method of the ECG signals based on the use of an optimized predefined functional database. Acta Cardiologica-An International Journal of Cardiology. 2003;58(3):59-61.
78. Martin DB, Nelson PS. From genomics to proteomics: techniques and applications in cancer research. Trends in Cell Biology. 2001;11(11):S60-S5.
79. Del Boccio P, Urbani A. Homo sapiens proteomics: clinical perspectives. Ann Ist Super Sanita. 2005;41(4):479-82.
80. Wilhelm M, Schlegl J, Hahne H, Gholami AM, Lieberenz M, Savitski MM, et al. Mass-spectrometry-based draft of the human proteome. Nature. 2014;509(7502):582-7.
81. Barrett J, Brophy PM, Hamilton JV. Analysing proteomic data. International Journal for Parasitology. 2005;35(5):543-53.
82. Fu J, Zhu F, Xu CJ, Li Y. Metabolomics meets systems immunology. EMBO reports. 2023;24(4):e55747.
83. Winder CL, Witting M, Tugizimana F, Dunn WB, Reinke SN, Education MS, et al. Providing metabolomics education and training: pedagogy and considerations. Metabolomics. 2022;18(12):106.
84. Akyol S, Ashrafi N, Yilmaz A, Turkoglu O, Graham SF. Metabolomics: An emerging “omics” platform for systems biology and its implications for huntington disease research. Metabolites. 2023;13(12):1203.
85. Goodacre R. Metabolomics–the way forward. Metabolomics. 2005;1(1):1-2.
86. Dong Z, Chen Y. Transcriptomics: advances and approaches. Science China Life Sciences. 2013;56:960-7.
87. Lowe R, Shirley N, Bleackley M, Dolan S, Shafee T. Transcriptomics technologies. PLoS computational biology. 2017;13(5):e1005457.
88. Wang Z, Gerstein M, Snyder M. RNA-Seq: a revolutionary tool for transcriptomics. Nature reviews genetics. 2009;10(1):57-63.
89. Hruz T, Laule O, Szabo G, Wessendorp F, Bleuler S, Oertle L, et al. Genevestigator v3: a reference expression database for the meta-analysis of transcriptomes. Advances in bioinformatics. 2008;2008(1):420747.
90. Allis CD, Jenuwein T. The molecular hallmarks of epigenetic control. Nature reviews genetics. 2016;17(8):487-500.

91. Busslinger M, Tarakhovsky A. Epigenetic control of immunity. Cold Spring Harbor perspectives in biology. 2014;6(6):a019307.
92. Ashe A, Colot V, Oldroyd BP. How does epigenetics influence the course of evolution? : The Royal Society; 2021. p. 20200111.
93. Yoshida K, Maekawa T, Zhu Y, Renard-Guillet C, Chatton B, Inoue K, et al. The transcription factor ATF7 mediates lipopolysaccharide-induced epigenetic changes in macrophages involved in innate immunological memory. Nat Immunol. 2015;16(10):1034-43.
94. Hasin Y, Seldin M, Lusis A. Multi-omics approaches to disease. Genome biology. 2017;18:1-15.
95. Demir G. Yükseköğretimde etik ilkelerin gelişimi ve önemi. RumeliDE Dil ve Edebiyat Araştırmaları Dergisi. 2023(34):403-20.
96. Çiftçioğlu C, Bozkurt Ö. İnsan Haklarının Etik İle İlişkisi. Turkish Academic Research Review. 2021;6(2):661-96.
97. Aktaş K. Etik-ahlâk ilişkisi ve etiğin gelişim süreci. Uluslararası Yönetim ve Sosyal Araştırmalar Dergisi. 2014;1(2):22-32.
98. Kuçuradi İ. Etik ve etikler. Türkiye Mühendislik Haberleri. 2003;423(1):7-9.
99. Höffe O. Etik: Bir Giriş: Runik Kitap; 2020. 120 p.
100. Aristoteles. Nikomakhos'a Etik. İstanbul: Sentez Yayıncılık; 2014.
101. Canfer H, Özcan Z. Nikomakhos'a etik bağlamında Aristoteles' in erdem etiği. Uludağ Üniversitesi İlahiyat Fakültesi Dergisi. 2019;29(1):277-96.
102. Molacı M. Aristoteles' in etik görüşü. Medeniyet ve Toplum Dergisi. 2018;2(1):37-57.
103. Griffioen A, Zahedi MS. 13 Medieval Christian and Islamic Mysticism and the Problem of a "Mystical Ethics". The Cambridge Companion to Medieval Ethics. 2019:280.
104. Akarsu B. Ahlâk öğretileri II: Immanuel Kant'ın ahlak felsefesi (ödev ahlakı): İÜ Edebiyat Fakültesi; 1968.
105. Mill JS. Utilitarizm [Utilitarianism]. Rostov-on-Don: Donskoy izdat dom publ. 2013.
106. Flynn J. Theory and bioethics. 2020.
107. Cevizci A. Uygulamalı etik. İstanbul: Say Yayınları; 2016.
108. Steinbock B. The Oxford handbook of bioethics: oxford university press; 2007.
109. Beauchamp TL, Childress JF. Principles of biomedical ethics: Edicoes Loyola; 1994.
110. Jecker NAS, Jonsen AR, Pearlman RA. Bioethics: an introduction to the history, methods, and practice: Jones & Bartlett Learning; 2007.
111. Ferretti A, Ienca M, Sheehan M, Blasimme A, Dove ES, Farsides B, et al. Ethics review of big data research: What should stay and what should be reformed? BMC medical ethics. 2021;22(1):51.
112. Entwistle VA, Carter SM, Cribb A, McCaffery K. Supporting patient autonomy: the importance of clinician-patient relationships. Journal of general internal medicine. 2010;25:741-5.
113. Kadam RA. Informed consent process: a step further towards making it meaningful! Perspectives in clinical research. 2017;8(3):107-12.
114. Manson NC, O'Neill O. Rethinking informed consent in bioethics: Cambridge University Press; 2007.

115. Andreotta AJ, Kirkham N, Rizzi M. AI, big data, and the future of consent. Ai & Society. 2022;37(4):1715-28.
116. Froomkin AM. Big data: Destroyer of informed consent. Yale JL & Tech. 2019;21:27.
117. Smilan LE. Broad consent—are we asking enough? Ethics & Human Research. 2022;44(5):22-31.
118. Zenker S, Strech D, Ihrig K, Jahns R, Müller G, Schickhardt C, et al. Data protection-compliant broad consent for secondary use of health care data and human biosamples for (bio) medical research: Towards a new German national standard. Journal of Biomedical Informatics. 2022;131:104096.
119. Cheah PY, Jatupornpimol N, Hanboonkunupakarn B, Khirikoekkong N, Jittamala P, Pukrittayakamee S, et al. Challenges arising when seeking broad consent for health research data sharing: a qualitative study of perspectives in Thailand. BMC medical ethics. 2018;19:1-11.
120. Maierà A. Consent and Technology: Is Dynamic Consent the Solution or Can an Interactive Website Solve the Problem of Consent? GDPR Requirements for Biobanking Activities Across Europe: Springer; 2023. p. 121-8.
121. Sheehan M, Thompson R, Fistein J, Davies J, Dunn M, Parker M, et al. Authority and the future of consent in population-level biomedical research. Public Health Ethics. 2019;12(3):225-36.
122. Budin-Ljøsne I, Teare HJ, Kaye J, Beck S, Bentzen HB, Caenazzo L, et al. Dynamic consent: a potential solution to some of the challenges of modern biomedical research. BMC medical ethics. 2017;18:1-10.
123. Kaye J, Whitley EA, Lund D, Morrison M, Teare H, Melham K. Dynamic consent: a patient interface for twenty-first century research networks. European journal of human genetics. 2015;23(2):141-6.
124. Prictor M, Lewis MA, Newson AJ, Haas M, Baba S, Kim H, et al. Dynamic consent: an evaluation and reporting framework. Journal of Empirical Research on Human Research Ethics. 2020;15(3):175-86.
125. Pierce JL, Furo CA. Employee ownership: Implications for management. Organizational Dynamics. 1990;18(3):32-43.
126. Loncarich K. Nature's law: The evolutionary origin of property rights. Pace L Rev. 2014;35:580.
127. Reynolds S. Tenure and property in medieval England. Historical Research. 2015;88(242):563-76.
128. Murray C. John Locke's theory of property, and the dispossession of indigenous peoples in the settler-colony. Am Indian LJ. 2022;10:55.
129. Çakır C. Bir Devlet Kuramı İnşası: John Locke'ta Siyasal Liberalizmin Temelleri A State Theory Constructıon: The Fundamentals Of Polıtıcal Lıberalısm In John Locke Kadir Caner Doğan. The Journal. 2018;11(57).
130. Medin B. Dijitalleşen dünyada fikri haklar sorunu. Kırıkkale Üniversitesi Sosyal Bilimler Dergisi. 2017;7(2):51-68.
131. Tatar DB. Mülkiyet ve fikrî mülkiyetin felsefi temelleri. Ankara: Astana Yayınları. 2014.
132. Mirchev M. Refreshed academic viewpoint on patient data ownership in digital health context. European Journal of Public Health. 2023;33(Supplement_2):ckad160. 1201.

133. Liddell K, Simon DA, Lucassen A. Patient data ownership: who owns your health? Journal of Law and the Biosciences. 2021;8(2):lsab023.
134. Contreras JL. The false promise of health data ownership. NYUL Rev. 2019;94:624.
135. Ballantyne A. How should we think about clinical data ownership? Journal of medical ethics. 2020;46(5):289-94.
136. Coll S. The social dynamics of secrecy: Rethinking information and privacy through Georg Simmel. The International Review of Information Ethics. 2012;17:15-20.
137. Solove DJ. The digital person: Technology and privacy in the information age: NyU Press; 2004.
138. Rubenfeld J. The right of privacy. Harvard Law Review. 1989:737-807.
139. European Convention on Human Rights (Article 8). Sect. Article 8 (1950).
140. Zuboff S. The age of surveillance capitalism. Social theory re-wired: Routledge; 2023. p. 203-13.
141. Durkheim E. Toplumsal İşbölümü, çev. Özer Ozankaya İstanbul: Cem Yay. 2006.
142. Froomkin AM. The death of privacy. Stan L Rev. 1999;52:1461.
143. Wu C. Data privacy: From transparency to fairness. Technology in Society. 2024;76:102457.
144. Kayaalp M. Patient privacy in the era of big data. Balkan medical journal. 2018;35(1):8-17.
145. Casanovas P, De Koker L, Mendelson D, Watts D. Regulation of Big Data: Perspectives on strategy, policy, law and privacy. Health and Technology. 2017;7(4):335-49.
146. İzgi MC. Mahremiyet kavramı bağlamında kişisel sağlık verileri. Türkiye Biyoetik Dergisi. 2014;1(1):201425-37.
147. Denning DE, Denning PJ. Data security. ACM computing surveys (CSUR). 1979;11(3):227-49.
148. Fodeh S, Zeng Q. Mining Big Data in biomedicine and health care. Elsevier; 2016. p. 400-3.
149. Wang S, Bonomi L, Dai W, Chen F, Cheung C, Bloss CS, et al. Big data privacy in biomedical research. IEEE Transactions on big Data. 2016;6(2):296-308.
150. ÜNSAL ÇZ. Biyotıp Araştırmaları ile ilgili Olarak,“Kişisel Veri-lerin Korunması Kanunu” ve “Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelik” Ne Diyor? 2018.
151. Yuan ZS, Singh MM. Privacy Risks in Health Big Data: A Systematic Literature Review. arXiv preprint arXiv:250203811. 2025.
152. Luo J, Wu M, Gopukumar D, Zhao Y. Big data application in biomedical research and health care: a literature review. Biomedical informatics insights. 2016;8:BII. S31559.
153. Cangil SM. The HES-code and the data protection during COVID-19 pandemic in Turkey. Bioethica. 2021;7(2):69-74.
154. Florini A. The right to know: transparency for an open world: Columbia University Press; 2007.
155. Ananny M, Crawford K. Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability. new media & society. 2018;20(3):973-89.
156. Ball C. What is transparency? Public integrity. 2009;11(4):293-308.
157. Castells M. End of millennium: John Wiley & Sons; 2010.
158. Baudrillard J. SimulacraandSimulation. Ann Arbor: The University of Michigan Press [1981]. 1994.

159. Baudrillard J. The transparency of evil: Essays on extreme phenomena: Verso books; 2009.
160. Keskin M, İşler EK. Dijital şeffaflık kavramı: Uluslararası literatürün PRISMA yöntemiyle sistematik incelenmesi. Türk Kütüphaneciliği. 2023;37(2):109-36.
161. Pasquale F. The black box society: The secret algorithms that control money and information: Harvard University Press; 2015.
162. Floridi L, Taddeo M. What is data ethics? : The Royal Society; 2016. p. 20160360.
163. Rumbold JMM, Pierscionek B. The effect of the general data protection regulation on medical research. Journal of medical Internet research. 2017;19(2):e47.
164. Kruse CS, Smith B, Vanderlinden H, Nealand A. Security techniques for the electronic health records. Journal of medical systems. 2017;41:1-9.
165. McGraw D. Building public trust in uses of Health Insurance Portability and Accountability Act de-identified data. Journal of the American Medical Informatics Association. 2013;20(1):29-34.
166. Jalali MS, Kaiser JP. Cybersecurity in hospitals: a systematic, organizational perspective. Journal of medical Internet research. 2018;20(5):e10059.
167. Chin K. Top 20 Worst HIPAA Violation Cases in History 2025 [
168. Kissi J, Dai B, Owusu-Marfo J, Bediako IA, Antwi MO, Akey BCA. A Revıew Of Informatıon Securıty Polıcıes And Procedures For Healthcare Servıces. Canadian Journal of Applied Science and Technology. 2018;6(2).
169. 140journos. Verilerimiz nasıl çalınıyor? YouTube2024.
170. Reddy J. Data breaches in healthcare security systems: University of Cincinnati; 2021.
171. Newaz AI, Sikder AK, Rahman MA, Uluagac AS. A survey on security and privacy issues in modern healthcare systems: Attacks and defenses. ACM Transactions on Computing for Healthcare. 2021;2(3):1-44.
172. Data sharing and the future of science. Nat Commun. 2018;9(1):2817.
173. Fournier JC, DeRubeis RJ, Hollon SD, Dimidjian S, Amsterdam JD, Shelton RC, et al. Antidepressant drug effects and depression severity: a patient-level meta-analysis. Jama. 2010;303(1):47-53.
174. Hulsen T, Jamuar SS, Moody AR, Karnes JH, Varga O, Hedensted S, et al. From big data to precision medicine. Frontiers in medicine. 2019;6:34.
175. Tamuhla T, Lulamba ET, Mutemaringa T, Tiffin N. Multiple modes of data sharing can facilitate secondary use of sensitive health data for research. BMJ Global Health. 2023;8(10):e013092.
176. Viberg Johansson J, Bentzen HB, Mascalzoni D. What ethical approaches are used by scientists when sharing health data? An interview study. BMC Medical Ethics. 2022;23(1):41.
177. Landi H. Fitbit, Apple user data exposed in breach impacting 61M fitness tracker records 2021
178. Rabin BA, Smith JD, Dressler EV, Cohen DJ, Lee RM, Goodman MS, et al. Designing for data sharing: Considerations for advancing health equity in data management and dissemination. Translational behavioral medicine. 2024;14(11):637-42.
179. Tekingündüz S, Kurtuldu A, Işık Erer T. Sağlık hizmetlerinde eşitsizlik ve etik. 2016.

180. Şimşek H, Kılıç B. Sağlıkta eşitsizliklerle ilgili temel kavramlar. Turkish Journal of Public Health. 2012;10(2):116-27.
181. Whitehead M. Eşitlik ve sağlık: kavram ve ilkeler. Türk Tabipleri Birliği Yayını, http://www ttb org tr/kutuphane/esiktlik_saglik pdf (3004 2019). 2001.
182. Sabet C, Hammond A, Ravid N, Tong MS, Stanford FC. Harnessing big data for health equity through a comprehensive public database and data collection framework. NPJ Digit Med. 2023;6(1):91.
183. Wesson P, Hswen Y, Valdes G, Stojanovski K, Handley MA. Risks and opportunities to ensure equity in the application of big data research in public health. Annual review of public health. 2022;43(1):59-78.
184. Cruz TM. Perils of data-driven equity: safety-net care and big data's elusive grasp on health inequality. Big Data & Society. 2020;7(1):2053951720928097.
185. Ogbunu CB. Data availability is social justice: Harvard Public Health; 2023 [Available from: https://harvardpublichealth.org/.
186. Galjaard H. Article 15: Sharing of benefits. The UNESCO Universal Declaration on Bioethics and Human Rights: Background, principles and application, Ethics series. 2009:231-41.
187. United Nations Educational SaCOU. Universal Declaration on Bioethics and Human Rights 2005.
188. Rodriguez-Monguio R, Spargo T, Seoane-Vazquez E. Ethical imperatives of timely access to orphan drugs: is possible to reconcile economic incentives and patients' health needs? Orphanet journal of rare diseases. 2017;12(1):1.
189. Dencik L, Hintz A, Redden J, Treré E. Exploring data justice: Conceptions, applications and directions. Taylor & Francis; 2019. p. 873-81.
190. Bull S, Roberts N, Parker M. Views of ethical best practices in sharing individual-level data from medical and public health research: a systematic scoping review. Journal of Empirical Research on Human Research Ethics. 2015;10(3):225-38.
191. Rosenman R, Tennekoon V, Hill LG. Measuring bias in self-reported data. Int J Behav Healthc Res. 2011;2(4):320-32.
192. Thatcher J, O'Sullivan D, Mahmoudi D. Data colonialism through accumulation by dispossession: New metaphors for daily data. Environment and Planning D: Society and Space. 2016;34(6):990-1006.
193. Harvey D. The'new'imperialism: accumulation by dispossession. Karl marx: Routledge; 2017. p. 213-37.
194. Yeşilkaya N. Algoritmik Adaletsizlik. Din Hukuk ve Teknoloji(Adnan Bülent Baloğlu-Yıldıray Sipahi, ed: 1 bs) DİB. 2023.
195. Ünal S, Sezgin AA. Büyük veri (big data)'nin yapay zeka uygulamalarında toplumsal sınıflandırmaya yönelik kaygılar. AJIT-e: Academic Journal of Information Technology. 2021;12(44):47-70.

196. Jain LR, Menon V, editors. AI Algorithmic bias: Understanding its causes, ethical and social implications. 2023 IEEE 35th International Conference on Tools with Artificial Intelligence (ICTAI); 2023: IEEE.
197. Mayson SG. Bias in, bias out. YAle lJ. 2018;128:2218.
198. Gebru T. Race and gender. The Oxford handbook of ethics of AI. 2020;4:253.
199. Ferrannini G, Maldonado JM, Raha S, Rao-Melacini P, Khatun R, Atisso C, et al. Gender differences in cardiovascular risk, treatment, and outcomes: a post hoc analysis from the REWIND trial. Scandinavian Cardiovascular Journal. 2023;57(1):2166101.
200. Obermeyer Z, Powers B, Vogeli C, Mullainathan S. Dissecting racial bias in an algorithm used to manage the health of populations. Science. 2019;366(6464):447-53.
201. Kordzadeh N, Ghasemaghaei M. Algorithmic bias: review, synthesis, and future research directions. European Journal of Information Systems. 2022;31(3):388-409.
202. Norori N, Hu Q, Aellen FM, Faraci FD, Tzovara A. Addressing bias in big data and AI for health care: A call for open science. Patterns. 2021;2(10).
203. Santos P, Nazaré I. The doctor and patient of tomorrow: exploring the intersection of artificial intelligence, preventive medicine, and ethical challenges in future healthcare. Frontiers in Digital Health. 2025;7:1588479.
204. Nietzsche F. Güç İstenci İstanbul: Say Yayınları; 2010.
205. Nietzsche F. Ahlakın Soykütüğü Üzerine. İstanbul: Kabalcı Yayınevi; 2004.
206. Williams M, Karim W, Gelman J, Raza M. Ethical data acquisition for LLMs and AI algorithms in healthcare. npj Digital Medicine. 2024;7(1):377.
207. Huang P-h, Kim K-h, Schermer M. Ethical issues of digital twins for personalized health care service: preliminary mapping study. Journal of Medical Internet Research. 2022;24(1):e33081.
208. Han B-C. Psikopolitika: Neoliberalizm ve Yeni İktidar Teknikleri: Metis Yayınları; 2020.
209. Han B-C. Şeffaflık Toplumu: Metis Yayınları; 2021.
210. Soria ST. Patient autonomy in the context of digital health. Bioethics. 2025;39(5):404-13.
211. Bennett CJ, Raab CD. The governance of privacy: Policy instruments in global perspective: Routledge; 2017.
212. Hoşnut Y. Uluslararası Düzenlemelerde ve Türkıye'de ˙ Kış ısel Ver ˙ ıler ˙ ın Korunması. Yeni Medya. 2019;2019(6):32-45.
213. Zanfir-Fortuna G. Follow the (personal) Data: Positioning Data Protection Law as the Cornerstone of EU's 'Fit for the Digital Age'Legislative Package. EDPS at. 2024;20.
214. Rubinstein IS. Big data: the end of privacy or a new beginning? Int'l Data Priv L. 2013;3:74.
215. KAYA MB. KVKK REFORMU 2024 DEĞİŞİKLİKLERİ.
216. Kişisel Verilerin Korunması Kanun'undaa Yapılan Değişiklikler, (2024).
217. Kurulu KVK. Kişisel Verileri Koruma Kurulu [Available from: https://kvkk.gov.ct.tr/.
218. Türk Medeni Kanunu, (2001).
219. Zuboff S. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power: PublicAffairs; 2019.

220. Regan P. Legislating privacy: Technology, social values, and public policy. The handbook of privacy studies. 1995:57.
221. Barocas S, Nissenbaum H. I2 Big Data's End Run around Anonymity and Consent. 2014.
222. Cavoukian A. Privacy by design: The 7 foundational principles. Information and privacy commissioner of Ontario, Canada. 2009;5(2009):12.
223. Kişisel Sağlık Verileri Hakkında Yönetmelik, Stat. 30808 (2019).
224. Barocas S, Nissenbaum H, editors. On notice: The trouble with notice and consent. Proceedings of the engaging data forum: The first international forum on the application and management of personal electronic information; 2009.
225. Solove DJ. Introduction: Privacy self-management and the consent dilemma. Harvard law review. 2013;126(7):1880-903.
226. Orhan U. Kişisel Verilerin Korunmasına İlişkin Türk Ceza Hukuku Düzenlemeleri Üzerine Değerlendirmeler. Ankara Üniversitesi Hukuk Fakültesi Dergisi. 2021;70(4):1359-84.
227. Türk Ceza Kanunu, (2004).
228. İtişgen R. Türk Ceza Hukukunda Kişisel Verileri Hukuka Aykırı Olarak Verme Veya Ele Geçirme Suçu. Türkiye Adalet Akademisi Dergisi. 2015;6(23).
229. Rana MS, Shuford J. AI in healthcare: transforming patient care through predictive analytics and decision support systems. Journal of Artificial Intelligence General Science (JAIGS) ISSN: 3006-4023. 2024;1(1).
230. Dülger MV. Kişisel verilerin korunması kanunu ve türk ceza kanunu bağlamında kişisel verilerin ceza normlarıyla korunması. İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi. 2016;3(2):101-68.
231. Gürses S, Van Hoboken J. Privacy after the agile turn. The Cambridge handbook of consumer privacy. 2018:579-601.
232. Health Insurance Portability and Accountability Act of 1996, 45 CFR § 164.506, (1996).
233. Association WM. WMA Declaration of Helsinki – Ethical Principles for Medical Research Involving Human Subjects: World Medical Association; 2013 [Available from: https://www.wma.net/policies-post/wma-declaration-of-helsinki-ethical-principles-for-medical-research-involving-human-subjects/.
234. Association WM. WMA Declaration of Lisbon on the Rights of the Patient. 1981.
235. Pathak M. Data Governance Redefined. European Data Protection Law Review. 2024;10(1):43-56.
236. European Convention on Human Rights, Article 8, (2020).
237. Oviedo Convention on Human Rights and Biomedicine, Article 5, (2024).
238. Dijital Sağlık Rehberi, (2020).
239. Kwon Y, Corren E, Garrido GM, Hoofnagle C, Song D. SoK: The Gap Between Data Rights Ideals and Reality. arXiv preprint arXiv:231201511. 2023.
240. Sidorenko E, Khisamova Z, editors. Big Data Regulation: The Main Risks and Ways to Neutralize Them. Proceedings of the International Scientific Conference "Smart Nations: Global Trends In The Digital Economy" Volume 1; 2022: Springer.

241. Google. Google Health, privacy and compliance: Google Support; 2024 [Available from: https://support.google.com/product-documentation/answer/14815921.
242. Spector-Bagdady K. Governing secondary research use of health data and specimens: the inequitable distribution of regulatory burden between federally funded and industry research. Journal of Law and the Biosciences. 2021;8(1):lsab008.
243. Powles J, Hodson H. Google DeepMind and healthcare in an age of algorithms. Health and technology. 2017;7(4):351-67.
244. News B. Google DeepMind's NHS deal under scrutiny: BBC News; 2017 [
245. Rajkomar A, Dean J, Kohane I. Machine learning in medicine. New England Journal of Medicine. 2019;380(14):1347-58.
246. Belle A, Thiagarajan R, Soroushmehr SR, Navidi F, Beard DA, Najarian K. Big data analytics in healthcare. BioMed research international. 2015;2015(1):370194.
247. Kuo M-H. Opportunities and challenges of cloud computing to improve health care services. Journal of medical Internet research. 2011;13(3):e1867.
248. Hashem IAT, Yaqoob I, Anuar NB, Mokhtar S, Gani A, Khan SU. The rise of "big data" on cloud computing: Review and open research issues. Information systems. 2015;47:98-115.
249. Hub RHI. Telehealth use in rural healthcare: Rural Health Information Hub; 2023 [Available from: https://www.ruralhealthinfo.org/toolkits/telehealth/1/barriers.
250. Wonderlich J. Ten principles for opening up government information. línea] Available: http://sunlightfoundation com/policy/documents/ten-open-data-principles/[Último acceso: 15 Abril 2016]. 2010.
251. Carroll SR, Garba I, Figueroa-Rodríguez OL, Holbrook J, Lovett R, Materechera S, et al. The CARE principles for indigenous data governance. Open Scholarship Press Curated Volumes: Policy. 2023.
252. Lin D, Crabtree J, Dillo I, Downs RR, Edmunds R, Giaretta D, et al. The TRUST Principles for digital repositories. Scientific data. 2020;7(1):144.
253. Guidance D. Guidance for industry. Center for Biologics Evaluation and Research (CBER). 1996.
254. FAIR G. FAIR Principles 2016 [Available from: https://www.go-fair.org/fair-principles/.
255. Chue Hong NP, Katz DS, Barker M, Lamprecht A-L, Martinez C, Psomopoulos FE, et al. FAIR principles for research software (FAIR4RS principles). Zenodo. 2022.
256. de Carvalho Castro JP, Romero LM, Carniel AC, Aguiar CD, editors. FAIR Principles and Big Data: A software reference architecture for Open Science. International Conference on Enterprise Information System; 2022: Universidade Federal de Minas Gerais.
257. Commission E. Prompting FAIR data practices in the European Open Science Cloud (EOSC). 2018.
258. CommissioN E. Horizon 2020 Programme: Guidelines on FAIR Data Management in Horizon 2020: European Commission; 2016 [Available from: https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-data-mgt_en.pdf.

259. Wilkinson MD, Dumontier M, Aalbersberg IJ, Appleton G, Axton M, Baak A, et al. The FAIR Guiding Principles for scientific data management and stewardship. Sci Data. 2016;3:160018.
260. Innovation ECD-GfRa. Turning FAIR into Reality – Final Report and Action Plan from the European Commission Expert Group on FAIR Data. 2018.
261. Boeckhout M, Zielhuis GA, Bredenoord AL. The FAIR guiding principles for data stewardship: fair enough? European journal of human genetics. 2018;26(7):931-6.
262. Abughazalah M, Alsaggaf W, Saifuddin S, Sarhan S. Centralized vs. Decentralized Cloud Computing in Healthcare. Applied Sciences. 2024;14(17):7765.
263. Lamprecht A-L, Garcia L, Kuzak M, Martinez C, Arcila R, Martin Del Pico E, et al. Towards FAIR principles for research software. Data Science. 2020;3(1):37-59.
264. Jacobsen A, de Miranda Azevedo R, Juty N, Batista D, Coles S, Cornet R, et al. FAIR principles: interpretations and implementation considerations. MIT Press One Rogers Street, Cambridge, MA 02142-1209, USA journals-info …; 2020. p. 10-29.
265. Barker M, Chue Hong NP, Katz DS, Lamprecht A-L, Martinez-Ortiz C, Psomopoulos F, et al. Introducing the FAIR Principles for research software. Scientific Data. 2022;9(1):622.
266. Delgado J, Llorente S. Security and privacy when applying FAIR Principles to genomic information. Integrated Citizen Centered Digital Health and Social Care: IOS Press; 2020. p. 37-41.
267. Castro JP, Aguiar CD, editors. Exploring Architectural Solutions for Implementing the FAIR Principles in Big Data Environments. Simpósio Brasileiro de Banco de Dados (SBBD); 2023: SBC.
268. Narayanan A, Shmatikov V, editors. Robust de-anonymization of large sparse datasets. 2008 IEEE Symposium on Security and Privacy (sp 2008); 2008: IEEE.
269. 269. Tariq S, Tariq S, Shoukat AA. Centralized healthcare database for ensuring better healthcare: Are we lagging behind? Pakistan Journal of Medical Sciences. 2024;40(3Part-II):257.
270. Mohammed N, Fung BC, Hung PC, Lee C-K. Centralized and distributed anonymization for high-dimensional healthcare data. ACM Transactions on Knowledge Discovery from Data (TKDD). 2010;4(4):1-33.
271. Li R, Romano JD, Chen Y, Moore JH. Centralized and Federated Models for the Analysis of Clinical Data. Annual review of biomedical data science. 2024;7.
272. Bazel MA, Mohammed F, Ahmed M, editors. Blockchain technology in healthcare big data management: Benefits, applications and challenges. 2021 1st International Conference on Emerging Smart Technologies and Applications (eSmarTA); 2021: IEEE.
273. Yaqoob I, Salah K, Jayaraman R, Al-Hammadi Y. Blockchain for healthcare data management: opportunities, challenges, and future recommendations. Neural Computing and Applications. 2022:1-16.
274. Zhang R, Xue R, Liu L. Security and privacy for healthcare blockchains. IEEE Transactions on Services Computing. 2021;15(6):3668-86.
275. Mann SP, Savulescu J, Ravaud P, Benchoufi M. Blockchain, consent and prosent for medical research. Journal of medical ethics. 2021;47(4):244-50.

276. Scheibner J, Ienca M, Vayena E. Health data privacy through homomorphic encryption and distributed ledger computing: an ethical-legal qualitative expert assessment study. BMC Medical Ethics. 2022;23(1):121.
277. Hasselgren A, Kralevska K, Gligoroski D, Pedersen SA, Faxvaag A. Blockchain in healthcare and health sciences—A scoping review. International journal of medical informatics. 2020;134:104040.
278. de Moraes Rossetto AG, Sega C, Leithardt VRQ. An architecture for managing data privacy in healthcare with blockchain. Sensors. 2022;22(21):8292.
279. Singh S, Sharma SK, Mehrotra P, Bhatt P, Kaurav M. Blockchain technology for efficient data management in healthcare system: Opportunity, challenges and future perspectives. Materials Today: Proceedings. 2022;62:5042-6.
280. Meisami S, Meisami S, Yousefi M, Aref MR. Combining blockchain and IOT for decentralized healthcare data management. arXiv preprint arXiv:230400127. 2023.
281. He A. State-centric data governance in China. CIGI papers; 2023.
282. Busygina I, Filippov M, Taukebaeva E. To decentralize or to continue on the centralization track: The cases of authoritarian regimes in Russia and Kazakhstan. Journal of Eurasian Studies. 2018;9(1):61-71.
283. Doutreligne M, Degremont A, Jachiet P-A, Lamer A, Tannier X. Good practices for clinical data warehouse implementation: A case study in France. PLOS Digital Health. 2023;2(7):e0000298.
284. Soumma SB, Shahriar F, Mahi UN, Abrar MH, Fahad MAR, Hoque ASML. Design and Implementation of a Scalable Clinical Data Warehouse for Resource-Constrained Healthcare Systems. arXiv preprint arXiv:250216674. 2025.
285. Broekstra R, Aris-Meijer J, Maeckelberghe E, Stolk R, Otten S. Trust in Centralized Large-Scale Data Repository: A Qualitative Analysis. J Empir Res Hum Res Ethics. 2020;15(4):365-78.
286. Scheibner J, Sleigh J, Ienca M, Vayena E. Benefits, challenges, and contributors to success for national eHealth systems implementation: a scoping review. J Am Med Inform Assoc. 2021;28(9):2039-49.
287. Bates DW, Saria S, Ohno-Machado L, Shah A, Escobar G. Big data in health care: using analytics to identify and manage high-risk and high-cost patients. Health affairs. 2014;33(7):1123-31.
288. Brat GA, Weber GM, Gehlenborg N, Avillach P, Palmer NP, Chiovato L, et al. International electronic health record-derived COVID-19 clinical course profiles: the 4CE consortium. NPJ digital medicine. 2020;3(1):109.
289. Ghosh PK, Chakraborty A, Hasan M, Rashid K, Siddique AH. Blockchain application in healthcare systems: a review. Systems. 2023;11(1):38.
290. Simon GE, Shortreed SM, Coley RY, Penfold RB, Rossom RC, Waitzfelder BE, et al. Assessing and Minimizing Re-identification Risk in Research Data Derived from Health Care Records. EGEMS (Wash DC). 2019;7(1):6.
291. Floridi L, Cowls J. A unified framework of five principles for AI in society. Machine learning and the city: Applications in architecture and urban design. 2022:535-45.

292. Eubanks V. Automating inequality: How high-tech tools profile, police, and punish the poor: St. Martin's Press; 2018.
293. Chang Y, Fang C, Sun W. A Blockchain-Based Federated Learning Method for Smart Healthcare. Computational Intelligence and Neuroscience. 2021;2021(1):4376418.
294. Shojaei P, Vlahu-Gjorgievska E, Chow Y-W. Security and privacy of technologies in health information systems: A systematic literature review. Computers. 2024;13(2):41.
295. Anon. Pathology labs under scrutiny over claims of patient data being sent offshore. The Courier-Mail. 2025.
296. Khan S, Khan M, Khan MA, Wang L, Wu K. Advancing Medical Innovation through Blockchain-Secured Federated Learning for Smart Health. IEEE Journal of Biomedical and Health Informatics. 2025.
297. Veinot TC, Ancker JS, Bakken S. Health informatics and health equity: improving our reach and impact. Journal of the American Medical Informatics Association. 2019;26(8-9):689-95.
298. Taylor L, Floridi L, Van der Sloot B. Group privacy. New challenges of data technologies Cham: Springer. 2017.
299. Leonelli S. Data-centric biology: A philosophical study: University of Chicago Press; 2019.
300. Bezuidenhout LM, Leonelli S, Kelly AH, Rappert B. Beyond the digital divide: Towards a situated approach to open data. Science and Public Policy. 2017;44(4):464-75.
301. Kuo T-T, Ohno-Machado L. Modelchain: Decentralized privacy-preserving healthcare predictive modeling framework on private blockchain networks. arXiv preprint arXiv:180201746. 2018.
302. Radanović I, Likić R. Opportunities for use of blockchain technology in medicine. Applied health economics and health policy. 2018;16:583-90.
303. Andrew J, Isravel DP, Sagayam KM, Bhushan B, Sei Y, Eunice J. Blockchain for healthcare systems: Architecture, security challenges, trends and future directions. Journal of Network and Computer Applications. 2023;215:103633.
304. Gross MS, Miller Jr RC. Ethical implementation of the learning healthcare system with blockchain technology. Blockchain in Healthcare Today, Forthcoming. 2019.
305. Kırbaş İ. Blokzinciri teknolojisi ve yakın gelecekteki uygulama alanları. Mehmet Akif Ersoy Üniversitesi Fen Bilimleri Enstitüsü Dergisi. 2018;9(1):75-82.
306. Tanrıverdi M, Uysal M, Üstündağ MT. Blokzinciri teknolojisi nedir? ne değildir?: alanyazın incelemesi. Bilişim Teknolojileri Dergisi. 2019;12(3):203-17.
307. Villarreal ERD, García-Alonso J, Moguel E, Alegría JAH. Blockchain for healthcare management systems: A survey on interoperability and security. IEEE Access. 2023;11:5629-52.
308. Cyran MA. Blockchain as a foundation for sharing healthcare data. Blockchain in Healthcare Today. 2018.
309. Ramachandran M. Ethics of Blockchain by Design: Guiding a Responsible Future for Healthcare Innovation. Blockchain in Healthcare Today. 2024;7:10.30953/bhty. v7. 362.

310.310. Hyrynsalmi S, Hyrynsalmi SM, Kimppa KK. The state of the art of the blockchain ethics in healthcare: A systematic literature review. Finnish Journal of eHealth and eWelfare. 2021;13(3):193–206-193–206.

311.311. Sharif MM, Ghodoosi F. The ethics of blockchain in organizations. Journal of Business Ethics. 2022;178(4):1009-25.

312.312. Narayanan A, Bonneau J, Felten E, Miller A, Goldfeder S. Bitcoin and cryptocurrency technologies: a comprehensive introduction: Princeton University Press; 2016.

313.313. Gupta MK, Dwivedi RK. Blockchain-Based Secure and Efficient Scheme for Medical Data. EAI Endorsed Transactions on Scalable Information Systems. 2023;10(5).

314.314. Azaria A, Ekblaw A, Vieira T, Lippman A, editors. Medrec: Using blockchain for medical data access and permission management. 2016 2nd international conference on open and big data (OBD); 2016: IEEE.

315.315. Saleh F. Blockchain without waste: Proof-of-stake. The Review of financial studies. 2021;34(3):1156-90.

316.316. Zheng Z, Xie S, Dai H, Chen X, Wang H, editors. An overview of blockchain technology: Architecture, consensus, and future trends. 2017 IEEE international congress on big data (BigData congress); 2017: Ieee.

317.317. Mohey Eldin A, Hossny E, Wassif K, Omara FA. Federated blockchain system (FBS) for the healthcare industry. Scientific Reports. 2023;13(1):2569.

318.318. Hasselgren A, Hanssen Rensaa J-A, Kralevska K, Gligoroski D, Faxvaag A. Blockchain for increased trust in virtual health care: Proof-of-concept study. Journal of Medical Internet Research. 2021;23(7):e28496.

319.319. Schinckus C. A Nuanced perspective on blockchain technology and healthcare. Technology in Society. 2022;71:102082.

320.320. Al-Khasawneh MA, Faheem M, Alarood AA, Habibullah S, Alzahrani A. A secure blockchain framework for healthcare records management systems. Healthcare Technology Letters. 2024;11(6):461-70.

321.321. Kumar R, Khan AA, Kumar J, Golilarz NA, Zhang S, Ting Y, et al. Blockchain-federated-learning and deep learning models for covid-19 detection using ct imaging. IEEE Sensors Journal. 2021;21(14):16301-14.

322.322. Kasyapa MS, Vanmathi C. Blockchain integration in healthcare: a comprehensive investigation of use cases, performance issues, and mitigation strategies. Frontiers in Digital Health. 2024;6:1359858.

323.323. Farahani B, Firouzi F, Luecking M. The convergence of IoT and distributed ledger technologies (DLT): Opportunities, challenges, and solutions. Journal of Network and Computer Applications. 2021;177:102936.

324.324. El Ioini N, Pahl C, editors. A review of distributed ledger technologies. On the Move to Meaningful Internet Systems OTM 2018 Conferences: Confederated International Conferences:

CoopIS, C&TC, and ODBASE 2018, Valletta, Malta, October 22-26, 2018, Proceedings, Part II; 2018: Springer.

325. Bai Y, Lee S, Seo S-H. A Survey on Directed Acyclic Graph-Based Blockchain in Smart Mobility. Sensors. 2025;25(4):1108.
326. Fu X, Wang H, Shi P, Zhang X. Teegraph: A Blockchain consensus algorithm based on TEE and DAG for data sharing in IoT. Journal of Systems Architecture. 2022;122:102344.
327. Zaman S, Khandaker MR, Khan RT, Tariq F, Wong K-K. Thinking out of the blocks: Holochain for distributed security in IoT healthcare. IEEE Access. 2022;10:37064-81.
328. Rahman A, Wadud MAH, Islam MJ, Kundu D, Bhuiyan TA-U-H, Muhammad G, et al. Internet of medical things and blockchain-enabled patient-centric agent through SDN for remote patient monitoring in 5G network. Scientific Reports. 2024;14(1):5297.
329. Benet J. Ipfs-content addressed, versioned, p2p file system. arXiv preprint arXiv:14073561. 2014.
330. Bauer DP. Getting Started with ethereum: a step-by-step guide to becoming a blockchain developer: Springer; 2022.
331. Bin Saif M, Migliorini S, Spoto F. Efficient and secure distributed data storage and retrieval using interplanetary file system and blockchain. Future Internet. 2024;16(3):98.
332. Zhou L, Diro A, Saini A, Kaisar S, Hiep PC. Leveraging zero knowledge proofs for blockchain-based identity sharing: A survey of advancements, challenges and opportunities. Journal of Information Security and Applications. 2024;80:103678.
333. Linn LA, Koo MB, editors. Blockchain for health data and its potential use in health it and health care related research. ONC/NIST use of blockchain for healthcare and research workshop Gaithersburg, Maryland, United States: ONC/NIST; 2016.
334. Bender D, Sartipi K, editors. HL7 FHIR: An Agile and RESTful approach to healthcare information exchange. Proceedings of the 26th IEEE international symposium on computer-based medical systems; 2013: IEEE.
335. Chen HS, Jarrell JT, Carpenter KA, Cohen DS, Huang X. Blockchain in healthcare: a patient-centered model. Biomedical journal of scientific & technical research. 2019;20(3):15017.
336. Aydin F, Başaran CH. Blockchain revolution: Transforming digital health for a secure future. Digital Healthcare, Digital Transformation and Citizen Empowerment in Asia-Pacific and Europe for a Healthier Society: Elsevier; 2025. p. 475-502.
337. Rathod N, Motwani D. Security threats on blockchain and its countermeasures. Int Res J Eng Technol. 2018;5(11):1636-42.
338. Aggarwal S, Kumar N. Attacks on blockchain. Advances in computers. 121: Elsevier; 2021. p. 399-410.
339. Zyskind G, Nathan O, editors. Decentralizing privacy: Using blockchain to protect personal data. 2015 IEEE security and privacy workshops; 2015: IEEE.
340. Rahman MH, Uddinb MKS, Hossanc KMR, Hossaind MD. The role of predictive analytics in early disease detection: a data-driven approach to preventive healthcare. Journal of the Learning Sciences. 2024;32(2):2024.

341. Venkatesh R, Balasubramanian C, Kaliappan M. Development of big data predictive analytics model for disease prediction using machine learning technique. Journal of medical systems. 2019;43(8):272.
342. Kothinti RR. Artificial intelligence in healthcare: Revolutionizing precision medicine, predictive analytics, and ethical considerations in autonomous diagnostics. World Journal of Advanced Research and Reviews. 2024;19(3):3395-406.
343. Bandi M, Masimukku AK, Vemula R, Vallu S. Predictive Analytics in Healthcare: Enhancing Patient Outcomes through Data-Driven Forecasting and Decision-Making. International Numeric Journal of Machine Learning and Robots. 2024;8(8):1-20.
344. Tasnim F, Nilima SI. Harnessing Predictive Analytics: The Role of Machine Learning in Early Disease Detection and Healthcare Optimization. Journal of Ecohumanism. 2025;4(3):312-21.
345. e-Estonia. e-Estonia – The Digital Society 2007 [Available from: https://e-estonia.com/solutions/cyber-security/ksi-blockchain/.
346. Intralink. Taiwan Digital Healthcare Report2020. Available from: https://www.intralinkgroup.com/Syndication/media/Syndication/Reports/Taiwan-Digital-Healthcare-Report-June-2020.pdf.
347. Insights L. UAE using blockchain for health worker credential checks 2020 [Available from: https://www.ledgerinsights.com/blockchian-health-credentials-uae/.
348. Gov1. Dubai Tests Blockchain for Securing Electronic Health Records 2020 [Available from: https://www.gov1.com/public-health/articles/dubai-tests-blockchain-for-securing-electronic-health-records-E0G7syOn13okbxx2/.
349. Pilot E. HealthData@EU Pilot – Towards the European Health Data Space 2023 [Available from: ttps://ehds2pilot.eu/.

8 EKLER

EK 1: Kavramlar Sözlüğü

Veri (Data): Ham, işlenmemiş bilgi parçacıklarıdır. Sağlık alanında kişinin tanısı, yaşı, laboratuvar sonuçları gibi unsurlar veri olarak kabul edilir.

Bilgi (Information): Verilerin anlamlı, bağlamlı ve kullanılabilir hâle gelmiş biçimidir. Veri işlendikçe bilgiye dönüşür.

Büyük Veri (Big Data): Geleneksel veri işleme yöntemleriyle analiz edilemeyecek kadar büyük, çeşitli ve hızlı biçimde üretilen veri topluluklarıdır.

Sağlık Verisi (Health Data): Bireylerin sağlık durumu, geçmiş hastalıkları, tanıları, tedavileri gibi bilgileri içeren verilerdir.

Kişisel Veri (Personal Data): Kimliği belirli veya belirlenebilir gerçek kişiye ait her türlü bilgidir. Sağlık verileri kişisel veri kapsamında değerlendirilir.

Anonimleştirme (Anonymization): Kişisel verilerin kimlikle ilişkilendirilemeyecek hâle getirilmesi sürecidir.

Etik (Ethics): İnsan davranışlarını doğru ya da yanlış açısından değerlendiren felsefi disiplindir.

Etos (Ethos): Toplumun ya da bir grubun değerler sistemini, alışkanlıklarını ve inançlarını ifade eder.

FAIR İlkeleri (FAIR Principles): Veri yönetiminde uluslararası kabul görmüş dört temel ilkedir: Bulunabilirlik, Erişilebilirlik, Birlikte Çalışabilirlik ve Yeniden Kullanılabilirlik.

Onam (Consent): Veri sahibinin, verisinin işlenmesine açık rıza göstermesi anlamına gelir.

Veri Sahipliği (Data Ownership): Veri üzerinde kontrol ve karar yetkisinin bireyde olması gerektiğini savunan ilkedir.

Blokzincir (Blockchain): Verilerin bloklar hâlinde sıralı ve değiştirilemez şekilde kaydedildiği, dağıtık ve merkeziyetsiz dijital kayıt sistemidir.

Blok (Block): İşlem kayıtlarını içeren veri grubudur. Her blok, bir önceki bloğun bilgisiyle bağlantılıdır.

Zincir (Chain): Blokların zaman sırasına göre birbirine bağlandığı yapıdır.

Dağıtık Defter (Distributed Ledger): Verilerin merkezi bir otorite yerine tüm ağ katılımcılarında kayıtlı olduğu sistemdir.

Kriptografi: Verilerin gizliliğini ve bütünlüğünü korumak için kullanılan şifreleme yöntemleridir.

Hash Fonksiyonu: Verileri sabit uzunlukta benzersiz dijital kodlara dönüştüren matematiksel algoritmadır.

Proof-of-Work (İş Kanıtı): Blok eklemek için bilgisayarların çözmesi gereken zor matematiksel problemlere dayalı doğrulama yöntemidir.

Akıllı Sözleşme (Smart Contract): Belirli koşullar gerçekleştiğinde otomatik çalışan dijital protokollerdir.

Merkeziyetsizlik (Decentralization): Veri kontrolünün tek merkezde değil, tüm ağ katılımcılarına dağılmış olması durumudur.

Düğüm (Node): Blokzincir ağına bağlı ve verilerin bir kopyasını tutan bilgisayardır.

Konsensüs Mekanizması (Consensus Mechanism): Ağdaki tüm düğümlerin aynı veri üzerinde uzlaşmasını sağlayan algoritmalardır.

Federe Sistem (Federated System): Verilerin merkezi bir noktada toplanmadan, her kurumun kendi verisini sakladığı sistem modelidir.

9 ÖZGEÇMİŞ