SAĞLIK VERİLERİNİN GİZLİLİĞİ GÜVENLİĞİ VE ERİŞİLEBİLİRLİĞİNE DAİR YASAL DÜZENLEMELER: KANADA İNGİLTERE VE TÜRKİYE KARŞILAŞTIRMASI

Meral TİMURTAŞ*Tutku EKİZ KAVUKOĞLU**Mehveş TARIM***

Öz: Sağlık verisi dijitalleşme sürecinde önemli bir dönüşüm geçirmektedir. Bu süreç, hastaların sağlık hizmetlerine erişimini kolaylaştırırken, sağlık verilerinin gizliliği ve güvenliği konusunda yeni zorluklar ortaya çıkarmaktadır. Kişisel sağlık verisinin paylaşımı ve erişilebilirliği, ülkeler arasında farklı yasal düzenlemelere tabidir. Bu çalışmanın amacı Kanada, İngiltere ve Türkiye'deki ulusal sağlık veri setlerinin kapsayıcılığı ve kullanılabilirliği, kişisel sağlık verisinin paylaşımı ve erişilebilirliği, gizlilik ve güvenliğine dair yasal düzenlemeleri ülkeler arası karşılaştırma yaparak değerlendirmektir. Çalışmada, ikincil veri analizi yöntemi uygulanmıştır. Bu kapsamda ulusal sağlık veri setlerinin kapsayıcılığı ve kullanılabilirliği, kişisel sağlık verisinin paylaşımı ve erişilebilirliği, gizlilik ve güvenliğine dair ÖECD'nin sağlık verisi yönetişimi araştırmasından elde edilen verilerin yanı sıra ilgili ülkelerin yasal düzenlemeleri kullanılmıştır. Bunlar doküman analizi yöntemi kullanılarak karşılaştırılmıştır. Ulusal sağlık veri setlerinin kapsayıcılığı ve kullanılabilirliği ülkeler arasında farklılık göstermektedir. Türkiye, diğer iki ülkeye kıyasla OECD'nin sağlık verisi yönetişimi araştırmasına göre daha kapsamlı ulusal sağlık veri setlerine sahiptir. Ancak Türkiye ile kıyaslandığında İngiltere ve Kanada'da sağlık verisinin araştırma amaçlı paylaşımının ve bu verilere erişilebilirliğin daha yüksek olduğu görülmektedir. Bu da kurumlar arası bilgi paylaşımının ve buna bağlı olarak iş birliğinin İngiltere ve Kanada'da daha yüksek olduğunu ortaya koymaktadır. Türkiye'nin düşük erişilebilirlik ve paylaşım oranı verilerin yeniden tanımlanmaması sonucu daha konservatif bir veri yönetimini işaret etmektedir. Yanı sıra sağlık verisinin gizliliği ve güvenliği, her ülkede yasal düzenlemelerle korunmaktadır. Ancak Kanada ve İngiltere, daha kapsamlı, köklü ve detaylı yasal düzenlemelere sahipken, Türkiye hızlı dijitalleşme sürecinde geliştirdiği yasal düzenlemeleri ve uygulamalarıyla öne çıkmaktadır. Sonuç olarak, bu farklı yaklaşımlar, sağlık hizmetlerinin etkinliği, hasta haklarının korunması ve veri güvenliği alanında ülkelerin kendine özgü ihtiyaçlarına ve dinamiklerine uygun çözümler geliştirdiğini göstermektedir. Her ülkenin koşullarına ve ihtiyaçlarına uygun olarak sağlık verisinin gizliliği ve güvenliği konusunda etkili yasal düzenlemeler yapması önemlidir. Bu düzenlemeler, hastaların mahremiyetini ve veri güvenliğini koruyarak sağlık hizmetlerinin kalitesini artırmaktadır.

Anahtar Sözcükler: Kişisel sağlık verisi, ulusal sağlık veri setleri, yasal düzenlemeler, gizlilik ve güvenlik

Legal Regulations Regarding The Privacy Security, and Accessibility of Health Data: A Comparison of Canada The UK and Turkey

Abstract: *Health data is undergoing significant transformation in the process of digitalization. While this process facilitates patients' access to healthcare services, it also presents new challenges regarding the privacy and security of health data. The sharing and accessibility of personal health data are subject to different legal regulations among countries. The aim of this study is to evaluate and compare the inclusiveness and usability of national health data sets, as well as the legal regulations concerning the sharing, accessibility, privacy, and security of personal health data in Canada, the UK, and Turkey. In the study, a secondary data analysis method was applied. In this context, data obtained from OECD's health data governance research on the comprehensiveness and usability of national health data sets, sharing and accessibility of personal health data, privacy and security, as well as legal regulations of relevant countries were used. These were compared using a document analysis method. The inclusiveness and usability of national health data sets vary among countries. Turkey has more comprehensive national health data sets compared to the other two countries, according to the OECD's health data governance research. However, compared to Turkey, the UK and Canada have higher rates of research-oriented sharing of health data and accessibility to these data. This indicates that interagency information sharing and collaboration are higher in the UK and Canada. Turkey's low accessibility and sharing rate suggest a more conservative approach to data management due to the lack of data redefinition. In addition, the privacy and security of health data are protected by legal regulations in every country. However, while Canada and the UK have more comprehensive, deep-rooted and detailed legal regulations, Turkey stands out with its legal regulations and practices developed in the rapid digitalization process. In conclusion, these different approaches show that countries develop solutions suitable for their own needs and dynamics in the areas of efficiency of health services, protection of patient rights and data security. It is important for each country to make effective legal regulations on the privacy and security of health data in accordance with its conditions and needs. These regulations increase the quality of health services by protecting the privacy of patients and data security.*

Key words: *Personal health data, national health data sets, legal regulations, privacy and security*

Giriş

Sağlık verileri, bireylerin tıbbi geçmişinden genetik bilgilerine kadar geniş bir yelpazeyi kapsayan hassas bilgileri içermekte ve birçok kişi tarafından her türlü kişisel bilginin en gizli olanları arasında sayılmaktadır. Bu hassasiyet, sağlık verilerinin gizliliği ve güvenliğinin özel bir önemle ele alınmasını gerektirmektedir. Bu nedenle, mahremiyetin korunması için bu gizliliğin ve güvenliğin korunması esastır. Gizlilik, verilere erişim yetkisi olmayan herhangi bir tarafa karşı erişim kontrolünü içermektedir ve bireylerin, grupların veya kurumların kendileriyle ilgili bilgilerin başkalarına ne zaman, nasıl ve ne ölçüde iletileceğini belirlemesi olarak tanımlanmaktadır (**Fernández-Alemán, 2013).**

Sağlık verilerinin güvenliği ise, hasta bilgilerinin yetkisiz erişime, kullanıma veya ifşa edilmeye karşı korunmasını ifade etmektedir. Bu verilerin korunması, bireylerin mahremiyetini sağlamanın yanı sıra, sağlık sistemlerinin güvenilirliğini ve etkinliğini de artırmaktadır **(Keshta ve Odeh, 2021)**. Bunun nedeni sağlık

*Arş. Gör. Dr., Marmara Üni., Sağlık Bil. Fak., Sağlık Bilş. ve Tekno. A.D.(ORCID No: (0000-0002-8382-1976)
**Dr. Öğr. Üyesi., Marmara Üni., Sağlık Bil. Fak., Sağlık Politikaları A.D.(ORCID No: 0000-0002-8498-630X)
***Prof.Dr., Marmara Üni., Sağlık Bil. Fak., Sağlık Politikaları A.D.(ORCID No: 0000-0002-3726-9439)

Geliş Tarihi / Received : 26.06.2024
Kabul Tarihi / Accepted : 06.02.2025

verilerinin gizliliği ve güvenliğinin, yüksek kaliteli, erişilebilir ve adil sağlık hizmeti sunumunun temel unsuru olması ve hizmet sunumunun merkezinde yer almasıdır **(Chung, ve ark., 2024).** Dolayısıyla sağlık verilerinin güvenliği sağlık hizmetlerinin gizliliğini, bütünlüğünü ve kullanılabilirliğini korumaya yönelik çeşitli yasal ve politik önlemleri gerektirmektedir.

Kişisel sağlık verilerinin gizliliği ve güvenliği konusu özellikle dijitalleşen dünyada bireylerin mahremiyetinin korunması açısından hükümetler için gittikçe artan bir öneme sahip olmaktadır **(Farayola ve ark., 2024; Quach ve ark., 2022).** Bunun nedeni, dijitalleşmenin sunduğu fırsatlar ve beraberinde getirdiği riskler arasındaki dengenin, ülkelerin yasal düzenleme kapasitelerine bağlı olmasıdır. Çok sayıda ülke sağlayacağı faydalar nedeniyle sağlık kayıtlarının dijitalleşmesine ilgi göstermiştir. Ancak ortaya çıkan mahremiyet endişelerini gidermeye yönelik yasal düzenlemelerin geliştirilmesinde pek çok ülke için halen eksikler olduğu ifade edilmektedir **(Keshta ve Odeh, 2021)**. Bunun nedeni hastaların mahremiyetini korumak ile çeşitli amaçlarla sağlık verilerinin paylaşımını sağlamak arasında bir denge kurma gerekliliğidir **(Wadmann ve ark., 2023).** Veri gizliliği, bireylerin sağlık bilgilerinin güvenli bir şekilde korunmasını gerektirmekte iken araştırma ve istatistik amaçlı veri paylaşımı sağlığı geliştirmede ve sağlıkta eşitsizliklerle mücadelede anahtar rol oynamaktadır **(Williamson ve Prybutok, 2024).** Bu ikilem, sağlık sistemlerinde etik ve pratik dengelerin nasıl kurulması gerektiğine dair önemli bir tartışmayı da beraberinde getirmektedir. Dolayısıyla sağlık verilerinin saklanmasına, bu verilere erişim sağlanmasına ve analiz edilmesine ilişkin süreçlerde veri gizliliğinin ve güvenliğinin sağlanması, hastaların sağlık bilgilerinin işbirliğine dayalı paylaşımının sağlanabilmesi sağlık kurumları ve politika yapıcı kurumlar için büyük değere sahiptir **(Shojaei ve ark., 2024).** Bu nedenle sağlık verilerinin gizliliği ve güvenliği korunacak şekilde paylaşımını sağlamaya dönük yasal düzenlemeler, sağlık sektöründe büyük ilgi gören bir konudur **(Nowrozy ve ark., 2024).**

Farklı ülkeler, sağlık verilerinin gizliliğini ve güvenliğini sağlama konusunda çeşitli yaklaşımlar geliştirmişlerdir. Bu çalışmada, 2010 yılından bu yana yayınlanmış olan dokümanların analiz edilmesi yoluyla Kanada, İngiltere ve Türkiye'deki ulusal sağlık veri setlerinin kapsayıcılık ve kullanılabilirlik durumunu, kişisel sağlık verisinin paylaşım ve erişilebilirlik koşullarını, sağlık verisinin gizliliği ve güvenliğine dair yasal düzenlemeleri karşılaştırmak amaçlanmaktadır.

1. Kavramsal Çerçeve

1.1. Sağlık verisi

Sağlık verisi kavramı farklı kaynaklarda çeşitli şekillerde tanımlanmıştır. Örneğin Dünya Hekimler Birliğinin tanımına göre kişisel sağlık verisi, bireyin fiziksel ve zihinsel sağlığına ilişkin kayıt altına alınmış bilgilerin tamamıdır **(The World Medical Association, 2008).** Bu tanım, sağlık hizmetlerinin başlangıcından itibaren toplanan bilgilerin önemine dikkat çekmektedir. Bunun yanı sıra, sağlık sunucuları tarafından toplanan bu veriler, yalnızca tıbbi teşhis ve tedavi süreçlerini değil, bireyin öznel olarak bildirdiği semptomlar ve ilaç kullanım bilgilerini de içermektedir. Sağlık sunucuları hastalara hizmet verme sürecinin en başından itibaren hastaya ait bilgiler almaktadır. Teşhis, tedavi ve takip süresi boyunca bu bilgiler toplanmaya devam etmekte ve belirli prosedürler çerçevesinde kayıt altına alınmaktadır **(Leonard ve ark., 2008).**

Sağlık verilerinin kapsamı, yalnızca bireylerin kendilerinden gelen bilgileri değil, sağlık sistemi içindeki diğer aktörlerden sağlanan bilgileri de içermektedir. Örneğin, bireylerden alınan semptomlar ve ilaç kullanımı gibi bilgilerin yanı sıra teşhis ve test sonuçları gibi doktorlardan gelen bilgiler, eczanelerden ve sigorta şirketlerinden gelen bilgiler de dâhil olmak üzere çok çeşitli bilgileri içermektedir **(Wiljer ve ark., 2008).** Bu yaklaşım, sağlık verilerinin çok boyutlu, bütüncül ve kapsamlı yapısını gözler önüne sermektedir. Bu nedenle Ekonomik İş birliği ve Kalkınma Örgütü (OECD) sağlık verilerini hassas veriler olarak tanımlamakta ve yüksek düzeyde koruma gerektiren veriler kategorisine sokmaktadır. Çünkü bireylerin herhangi bir yolla kendisine ruhsal, fiziksel, sosyal veya ekonomik olarak kayıp getirebilecek tüm değişkenler yüksek hassas veri kategorisine girmektedir. Bunlardan bazıları; bireylerin doğrudan tanımlanmasına yol açan bilgiler, zihinsel sağlık koşulları, HIV dâhil cinsel yolla bulaşan enfeksiyonlar, madde kullanımı ve tedavisi, cinsel sağlık, kürtaj, çocuk istismarına ilişkin bilgilerdir **(OECD, 2015).**

Bu tanımların ortak noktası, sağlık verilerinin bireylerin mahremiyetine doğrudan etki eden son derece hassas bilgiler olduğudur. Bu hassasiyet, sağlık verilerinin özel bir önemle ele alınmasını gerektirmektedir. Dolayısıyla, sağlık verilerinin güvenliğini ve gizliliğini sağlamak, etik ilkeler ve yasal düzenlemeler çerçevesinde titizlikle yönetilmesi gereken bir zorunluluktur.

1.2. Sağlık Verilerinin Politik ve Etik Açıdan Önemi

Kişisel sağlık verilerinin dijitalleşmeyle beraber elektronik ortama bağlanması ile verinin kaydı, işlenmesi, kullanımı, erişilebilirliği, gizliliği ve korunması daha karmaşık ve multidisipliner süreçler içermeye başlamıştır **(Fernández-Alemán, 2013).** Bu, entegre sağlık kayıtlarının analizi ile maliyetleri azaltma, bakım kalitesinde iyileşme, kanıta dayalı tıbbın teşviki ve kayıt tutma ve mobilite gibi birçok fayda sağlandığı gösterilmiştir **(Greenhalgh, 2010).** Bu faydalar sağlanırken aynı zamanda belirli riskler de ortaya çıkmaktadır. Bilgi hırsızlığı, siber korsanlık, veriye erişim yetkisi olmayanların erişimi gibi hususlar sağlık verilerini tehdit eden unsurlar olarak karşımıza çıkmaktadır **(Fernández-Alemán, 2013).**

Sağlık verilerinin uygunsuz şekilde kullanılması bireyler üzerinde nesnel zararların (istihdam veya sigortada ayrımcılık veya itibar kaybı gibi) yanı sıra psikolojik veya daha subjektif zararlara da yol açabileceğinden, sağlık verileri açısından riskler özellikle yüksektir. Gelişmiş ülkelerde yapılan araştırma verileri, birçok bireyin sağlık verilerinin güvenliğinin ve gizliliğinin ihlal edilmesinden ve ihlal edilen verilerin kötüye kullanılmasından endişe duyduğunu göstermektedir **(Arora, 2019).** Bu sebeple kişisel sağlık verilerinin erişimi, kullanılabilirliği ve buna bağlı olarak gizliliği

ve güvenliğinin korunması için hükümetler, hizmet sunucuları ve kâr amacı gütmeyen kuruluşlar çeşitli tedbirler ve kılavuzlar ortaya koymuştur. Kişisel sağlık verilerinin gizliliğini ve güvenliğini korumak için geliştirilen yasal düzenlemeler veya kılavuzlar kamu şeffaflığını arttırırken verilerin tutarlılık ve güvenilirliğini de sağlamaktadır **(Rosenfeld, 2017).**

Dünyada birçok ülke bu konuda belirli seviyelerde uygulamalar yapmaktadır. Bağımsız kuruluşlar, akreditasyon kuruluşları gibi organizasyonların belirlediği çeşitli rehberler bulunduğu görülmektedir. Uluslararası Standartlar Örgütü (ISO) tarafından belirlenen ISO / TS 13606-4: 2009; ISO 22857: 2013 standartları bunlardan bazılarıdır. Yanı sıra hızla gelişen sağlık bilgi teknolojileri alanında etik standartların korunması önemlidir. Teknolojiler ilerledikçe etik çerçeveler, yasal düzenlemeler ve uygulamalar da hasta haklarını koruyacak, gizliliği sağlayacak ve sağlık sistemine olan güveni artıracak şekilde gelişmelidir. Bu, sağlık hizmeti sağlayıcıları, teknoloji uzmanları, politika yapıcılar ve hastalar da dâhil olmak üzere tüm paydaşların ortak çabasını gerektirir. Sağlık hizmetlerinde bilgi teknolojilerinin kullanımında etik hususları önceliklendirmek, özerklik, mahremiyet ve adalet gibi temel değerleri koruyarak hasta bakımını ve halk sağlığını iyileştirmek önemlidir **(Adeniyi, 2024).**

Sağlık verilerinin politik ve etik yönetimi, ülkelerin sağlık sistemlerinin etkinliği ve vatandaşlarının haklarının korunması açısından büyük önem taşımaktadır. Dolayısıyla bu konuyla ilgili Türkiye'yi değerlendirmek, mevcut durumu ortaya koymak ve gelişim sağlamak açısından önemlidir. Kanada ve İngiltere, bu alandaki farklı yaklaşımları ve özellikleriyle dikkat çeken iki ülke olup, karşılaştırmalı analiz için anlamlı bir bağlam sunmaktadır.

Kanada, federal bir yapıya sahip olması nedeniyle sağlık politikalarında yerel ve ulusal düzeyde koordinasyonun önemli olduğu bir ülke olarak öne çıkmaktadır. Sağlık verilerinin yönetiminde, bireysel mahremiyet haklarını korumaya yönelik güçlü yasal düzenlemeleri ve Kişisel Bilgilerin Korunması ve Elektronik Belgeler Yasası (PIPEDA) gibi kapsamlı veri koruma çerçevelerini uygulamaktadır. Ayrıca, etik açıdan sağlık verilerine özel önem atfedilmesi ve eyalet düzeyinde halkın onay süreçlerine katılımı gibi hassasiyetler, Kanada'yı bu çalışmada incelemeye değer kılmaktadır.

İngiltere, ulusal sağlık sistemi olan NHS (National Health Service) ile merkezi bir sağlık veri yönetim modeline sahip bir örnek teşkil etmektedir. NHS, sağlık hizmetlerinde dijitalleşme ve büyük veri analitiği uygulamalarıyla dünyanın öncü sistemlerinden biri olarak kabul edilmektedir. İngiltere, veri Koruma Yasası ve bağlı etik standartlarla, bireysel hakları korumayı ve sağlık verilerinin sorumlu kullanımını dengelemede dikkat çeken bir modele sahiptir. Ayrıca, uluslararası işbirlikleri ve araştırma projelerinde sağlık verilerini stratejik olarak kullanması, bu ülkeyi analiz için uygun hale getirmektedir **(Karaca, 2023)**.

Kanada'nın federal yapısı ve yerel hassasiyetleri, İngiltere'nin ise merkezi ve yenilikçi modeli, çalışmada küresel bağlamda karşılaştırmalı dersler çıkarmak için ideal bir temel sunmaktadır. Dolayısıyla Kanada ve İngiltere bu konuda iyi örnekler olarak düşünülmüş ve karşılaştırma açısından belirlenmiştir. Türkiye'nin yanı sıra bu iki ülkeye yer verilmesi, sağlık verilerinin mahremiyeti, erişimi ve kullanımı gibi kritik konularda farklı perspektifler ve uygulama örnekleri sunarak yasal düzenlemelerin ve etik çerçevesinin daha derinlemesine anlaşılmasını sağlamaktadır.

2. Gereç ve Yöntem

Bu çalışmada Kanada, İngiltere ve Türkiye'nin kişisel sağlık verilerinin gizliliği ve güvenliği konusundaki uygulamalarını karşılaştırmaya yönelik literatür taraması yapılarak, ikincil veri analizi yöntemleri uygulanmıştır. Bu amaçla 2010 yılından bu yana ülkelerin bu konuya ilişkin yasal düzenlemelerini yansıtan resmi belgeler ve istatistiki verileri içeren dökümanlar analiz edilmiştir.

2.1. Araştırma Tasarımı

Bu çalışma ilgili ülkelerin sağlık verisi yönetimi üzerine uluslararası raporların, yasal düzenlemelerin, etik bildirgelerin ve uygulamaların incelendiği tanımlayıcı bir araştırmadır.

2.2. Veri Toplama

Veri toplama sürecinde aşağıdaki adımlar izlenmiştir:

* *İstatistiksel Veriler:* OECD'nin sağlık verisi yönetişimi araştırmasından elde edilen veriler kullanılmıştır. Bu veriler, Kanada, İngiltere ve Türkiye'nin sağlık veri setlerinin kapsayıcılığı ve kullanımı hakkında bilgiler sunmaktadır.

* *Yasal Çerçeveler:* Kanada, İngiltere ve Türkiye'de kişisel sağlık verilerinin korunmasına yönelik çeşitli yasal düzenlemeler bulunmaktadır. Kanada'da sağlık verilerinin korunmasına yönelik Gizlilik Yasası (The Privacy Act) ve Kişisel Bilgilerin Korunması ve Elektronik Belgeler Yasası (PIPEDA) federal düzeyde uygulanmakta ve eyalet düzeyindeki düzenlemelerle desteklenmektedir. Çalışmanın Kanada boyutunda bu yasal düzenlemeler esas alınmıştır. İngiltere'de ise Veri Koruma Yasası (The Data Protection Act), Ulusal Sağlık Hizmeti Yasası (The NHS Act) ve Avrupa İnsan Hakları Sözleşmesi'nin 8. maddesi, kişisel sağlık verilerinin gizliliğini korumak için temel alınan yasal çerçevelerdir. Çalışmanın İngiltere boyutunda bu yasal düzenlemeler esas alınmıştır. Türkiye'de, Kişisel Verilerin Korunması Kanunu (KVKK) ve 2019 tarihli Kişisel Sağlık Verileri Hakkında Yönetmelik ve Türk Tabipler Birliği (TTB)'nin etik bildirgeleri sağlık verilerinin korunmasını sağlayan temel düzenlemelerdir. Çalışmanın Türkiye boyutunda ise bu yasal çerçevelere odaklanılmıştır.

Veri kaynağı açısından OECD Sağlık Verisi Yönetişimi raporundan elde edilen verilerin, ülkelerin kendi raporlamalarına dayalı olduğu ve bu nedenle veri doğruluğu ve tutarlılığı konusunda sınırlılıklar içerebileceği dikkate alınmalıdır. Her ne kadar OECD ülkelerden alınan verilerin doğruluğunu teyit etmek ve tutarlılığını saptamak için belirli metodolojik çerçeveler kullansa da ülkeler arası veri paylaşımı farklılıkların ve raporlama süreçlerinin sonuçlara etkisi olabileceği göz önünde bulundurulmalıdır.

2.3. Veri Analizi

Toplanan veriler, aşağıdaki yöntemler kullanılarak analiz edilmiştir:

* *Doküman Analizi:* Doküman analizine belirli bir çerçevede gerçekleştirilmiş ve çalışmanın amacına uygun dokümanlar dahil edilmiştir. Bu dokümanlar arasında sağlık veri setlerinin kapsamı, bunların paylaşımı ve erişilebilirliğine dair yasal düzenlemeler ve bu düzenlemelerin uygulamalarına ilişkin bilgiler bulunmaktadır. Seçilen dokümanların dahil edilme kriterleri; ülkelerin ulusal sağlık verisi politikalarını yansıtmaları, 2010 sonrası yayınlanmış olmaları ve sağlık verilerinin gizliliği ve güvenliğiyle ilgili düzenlemelere doğrudan atıfta bulunmaları şeklindedir.

* *Karşılaştırmalı Analiz:* Kanada, İngiltere ve Türkiye'nin kişisel sağlık verilerinin gizliliği ve güvenliği konusundaki uygulamaları karşılaştırılmıştır. Bu karşılaştırma, her ülkenin sağlık verisi yönetimindeki yasal, teknolojik ve kurumsal farklılıklarını ortaya koymayı amaçlamaktadır.

* *İstatistiksel Analiz:* OECD tarafından sağlanan istatistiksel veriler, tablo ve grafikler kullanılarak görselleştirilmiş ve yorumlanmıştır. Bu veriler, ülkelerin sağlık veri setlerinin kapsayıcılığı ve kullanım oranlarını detaylı bir şekilde göstermektedir.

OECD (2015)'nin sağlık verisi yönetişimi araştırmalarından elde edilen istatistiksel veriler, tablolar ve grafikler aracılığıyla görselleştirilmiş ve yorumlanmıştır. Veriler, sağlık veri setlerinin kapsayıcılığı ve kullanım oranlarını değerlendirmek amacıyla sınıflandırılmıştır. Bu sınıflandırmada ülkelerin yasal, teknolojik ve kurumsal farklılıkları dikkate alınmıştır. Bu kapsamda ulusal sağlık veri setlerinin kullanılabilirliği, paylaşımı ve erişilebilirliğine dair veriler karşılaştırılmalı olarak sunulmuştur.

Kullanılabilirlik, paylaşım ve erişilebilirlik, verilerin nasıl yönetildiği ilgili farklı kavramlardır. Kullanılabilirlik, verinin belirli bir amaç için uygun, anlamlı ve doğru bir şekilde hazır olması anlamına gelmektedir. Örneğin, bir hastanın teşhis geçmişiyle ilgili veriler elektronik sağlık kayıtlarında güncel değilse, bu veri kullanılabilir değildir. Öte yandan paylaşım, verinin başka kişiler, kurumlar veya sistemlerle güvenli bir şekilde aktarılması ya da sunulması sürecidir. Erişilebilirlik ise kullanıcıların belirli bir veri setine kolay ve güvenli bir şekilde ulaşabilme durumunu ifade etmekte olup **(Goldberg ve ark., 2011)**; her zaman paylaşılabilirlik anlamına gelmemektedir. Örneğin, bir hastane çalışanı elektronik sağlık kaydına erişebilir, ancak bu veriyi başka bir kurumla paylaşma yetkisi olmayabilir. Ülkelerin sağlık verilerini yasal çerçeveler dâhilinde ne ölçüde erişilebilir ve paylaşılabilir kıldıkları veri güvenliği ve gizliliği açısından kritik göstergelerdir. Bu noktada yeniden tanımlama kavramı ise sağlık verilerinin ve sahiplerinin anonimleştirilmesi ile tekrar tanımlanması işlemidir **(Kaplan, 2015).** Dolayısıyla bu kavramlar sağlık verileri gibi hassas bilgilerin kullanımında kritik öneme sahiptir.

OECD (2015)'nin sağlık verisi yönetişimi araştırmalarında yer alan göstergeler ve ilgili kriterleri de bu kavramlara dayanmakta olup; aşağıda detaylandırılmıştır:

* *Ulusal Sağlık Veri Setleri Kapsayıcılığı ve Kullanılabilirliği Açısından Karşılaştırma:* OECD sağlık verisi yönetişimi araştırması kapsamında Ulusal Sağlık Veri Setlerinin Kapsayıcılığının ve Kullanılabilirliğini belirlemek için 7 faktörlü değerlendirmeye tabii tutulmuştur. Bu faktörler;

1. Ulusal düzeyde mevcut veri seti yüzdesi
2. Sağlık veri setlerinden nüfusun %80'i veya daha fazlasını kapsayanların oranı
3. Verilerin elektronik tıbbi veya idari kayıtlardan oto-

Tablo 1. Ulusal Sağlık Veri Setlerinin Kapsayıcılığının ve Kullanılabilirliğinin Karşılaştırılması

Sağlık Verilerinin Kapsayıcılığı ve Kullanılabilirliğine İlişkin Faktörler	Türkiye(%)	Kanada(%)	İngiltere(%)
1.Ulusal düzeyde mevcut veri seti yüzdesi	% 100	% 71	% 64
2.Sağlık veri setlerinden nüfusun %80'i veya daha fazlasını kapsayanların oranı	% 73	% 60	% 28
3.Verilerin elektronik tıbbi veya idari kayıtlardan otomatik olarak alındığı mevcut sağlık veri setlerinin yüzdesi	% 100	% 63	% 100
4.Aynı kişiye özel sağlık kimliğini kullanan veri setlerinin yüzdesi	% 0	% 50	% 78
5.Klinik terminoloji için standart kodların kullanıldığı mevcut veri setlerinin yüzdesi	% 80	% 100	% 100
6.Sağlık kalitesi veya sağlık sistemi performansı hakkında düzenli olarak rapor vermek için kullanılan mevcut veri setlerinin yüzdesi	% 0	% 100	% 40
7.Araştırma, istatistik ve/veya izleme için düzenli olarak kullanılan mevcut veri setlerinin yüzdesi	% 0	% 70	% 89

matik olarak alındığı mevcut sağlık veri setlerinin yüzdesi

4. Aynı kişiye özel sağlık kimliğini kullanan veri setlerinin yüzdesi
5. Klinik terminoloji için standart kodların kullanıldığı mevcut veri setlerinin yüzdesi
6. Sağlık kalitesi veya sağlık sistemi performansı hakkında düzenli olarak rapor vermek için kullanılan mevcut veri setlerinin yüzdesi
7. Araştırma, istatistik ve/veya izleme için düzenli olarak kullanılan mevcut veri setlerinin yüzdesidir.

Ayrıca ülkelerin ulusal 14 veri setine ait veriler, yukarıda verilen 7 kapsayıcılık ve kullanılabilirlik faktörüne göre incelenmiştir. Bu 14 veri seti ise; hastanede yatan hasta verileri, ruh ve sinir hastalıkları hastanesi yatan hasta verileri, acil sağlık verileri, birinci basamak sağlık verileri, reçeteli ilaç verileri, kanser kayıt verileri, diyabet kayıt verileri, kardiyovasküler hastalık kayıt verileri, ölüm verileri, resmi uzun süreli bakım verileri, hasta tarafından bildirilen sağlık sonuçları verileri, hasta deneyimleri anket verileri, nüfus sağlığı anket verileri ve nüfus sayımı veya kayıt defteri verilerinden oluşmaktadır **OECD (2015)**.

* *Kişisel Sağlık Verilerinin Araştırma ve İstatistik İçin Paylaşımı ve Erişilebilirliği Açısından Karşılaştırma:* Bu gösterge, **OECD (2015)** tarafından belirlenen 6 paylaşım ve erişim faktörünü karşılama yüzdelerine dayalı hesaplanmıştır. Bu faktörler;

1. Verilerin diğer veri sorumluları ve hükümet yetkilileri ile paylaşımı,
2. Devlet analistlerinin yeniden tanımlanmış verilere erişimi,
3. Üniversite ve kâr amacı gütmeyen araştırmacıların yeniden tanımlanmış veriye erişimi,
4. Sağlık hizmeti sunucularının yeniden tanımlanmış verilere erişimi,
5. Kâr amacı güden organizasyonların yeniden tanımlanmış verilere erişimi,
6. Yabancı hükümet, üniversite veya kâr amacı gütmeyen araştırmacıların yeniden tanımlanmış verilere erişimidir.

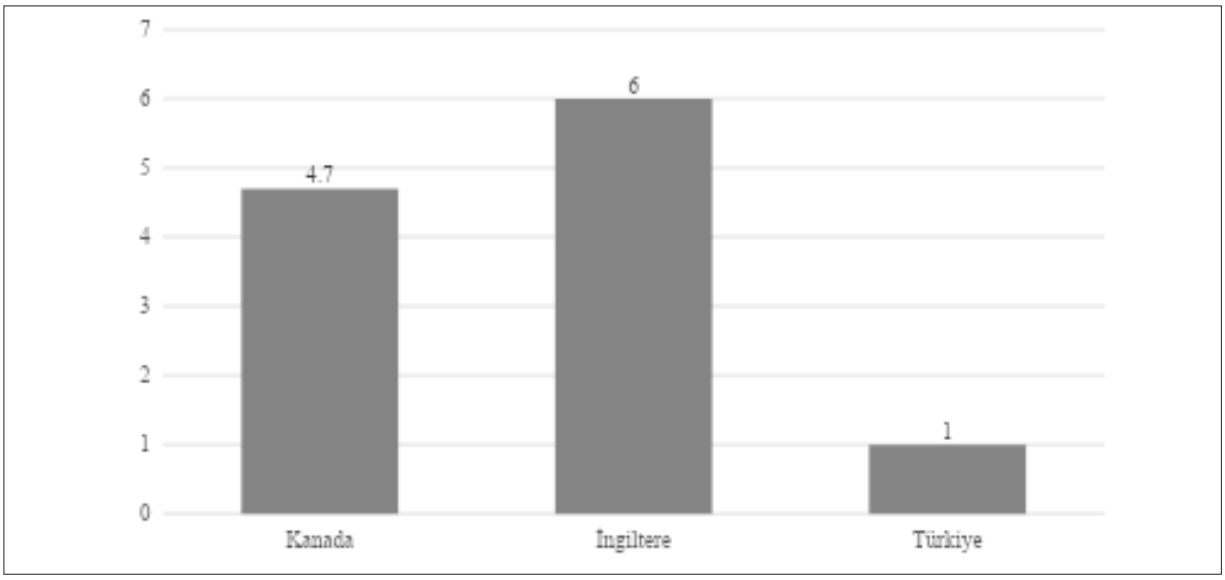
3. Bulgular

3.1. Ulusal Sağlık Veri Setleri Kapsayıcılığı ve Kullanılabilirliği Açısından Karşılaştırma

Sağlık verilerinin kapsayıcılığı ve kullanılabilirliği ile ilgili Kanada, İngiltere ve Türkiye'ye ait sonuçlar tablo 1'de gösterilmiştir **(OECD, 2015).**

Türkiye, araştırma kapsamındaki üç ülke arasında 14 kişisel sağlık verisinin tümü için ulusal sağlık veri setleri bulunan tek ülkedir. Kanada ve İngiltere için bu oranların sırasıyla %71 ve %64 olduğu görülmektedir. Sağlık hizmeti veri setlerinden nüfusun %80 ve daha fazlasını kapsayıcılığı yüzdelerine bakıldığında ise Türkiye'nin %73, Kanada'nın ise %60, İngiltere'nin %28 oranında olduğu görülmüştür.

İngiltere ve Türkiye'de sağlık verilerinin %100'ü elektronik tıbbi ve idari kayıtlardan alınmaktadır. Kanada'da ise bu oran %63'tür. İngiltere ondört veri setinin %78'inde kişiye özel sağlık kimlik numarasının aynı şekilde kullanılırken, Kanada'da bu oran %50'dir. Türkiye'de kişiye özel sağlık kimlik numarası yerine vatandaşlık numarası kullanıldığı için bu oran %0'dır. Kanada ve İngiltere'de mevcut veri setlerinin %100'ünde klinik terminoloji için standart kodların kullanılmaktadır. Türkiye'de bu oran %80'dir. Sağlık kalitesi veya sağlık sistemi performansı hakkında



Grafik 1. Sağlık verilerinin araştırma ve istatistik için paylaşım ve erişilebilirlik durumunun karşılaştırılması

Tablo 2. Ulusal Sağlık Verilerinin Paylaşım ve Erişilebilirlik Göstergelerinin Karşılaştırılması

Sağlık Verilerinin Paylaşım ve Erişilebilirlik Göstergeleri	Türkiye(%)	Kanada (%)	İngiltere (%)
Verilerin diğer veri sorumluları ve hükümet yetkilileri ile paylaşımı	% 0	% 75	% 100
Devlet analistlerinin yeniden tanımlanmış verilere erişimi	% 100	% 88	% 100
Üniversite ve kâr amacı gütmeyen araştırmacıların yeniden tanımlanmış verilere erişimi	% 0	% 88	% 100
Sağlık hizmeti sunucularının yeniden tanımlanmış verilere erişimi	% 0	% 88	% 100
Kâr amacı güden organizasyonların yeniden tanımlanmış verilere erişimi	% 0	% 75	% 100
Yabancı hükümet, üniversite veya kâr amacı gütmeyen araştırmacıların yeniden tanımlanmış verilere erişimi	% 0	% 63	% 100

düzenli olarak rapor vermek için kullanılan mevcut veri setlerinin yüzdesi Kanada'da %100 iken İngiltere'de %40, Türkiye'de ise %0'dır. Araştırma, istatistik ve/veya izleme için düzenli olarak kullanılan mevcut veri setleri Kanada'da %70 iken İngiltere' de %89, Türkiye'de ise %0'dır.

3.2. Kişisel Sağlık Verilerinin Araştırma ve İstatistik İçin Paylaşımı ve Erişilebilirliği Açısından Karşılaştırma

Grafik 1'de, sağlık verilerinin araştırma ve istatistik için paylaşım ve erişilebilirlik durumunun Kanada, İngiltere ve Türkiye'deki karşılaştırması sunulmaktadır. Bu grafik, OECD tarafından belirlenen altı paylaşım ve erişim faktörünü karşılama yüzdelerine dayalı hesaplanmıştır.

Sağlık verilerinin araştırma ve istatistik için paylaşım ve erişilebilirlik oranının Kanada'da yedi üzerinden yaklaşık 5, İngiltere'de 6, Türkiye'de 1 olduğu görülmektedir.

Kanada, İngiltere ve Türkiye'nin bu altı paylaşım ve erişim faktörü altındaki istatistikleri tablo 2'de sunulmaktadır **(OECD, 2015).**

Ülkelerin ulusal sağlık verilerinin erişilebilirlik faktörleri oranlarına bakıldığında İngiltere'de kişisel sağlık verilerinin diğer veri sorumluları ve hükümet yetkilileri ile paylaşım oranı %100 olduğu görülmektedir. Devlet analistlerinin yeniden tanımlanmış verilere erişimi, kâr amacı gütmeyen kuruluşlar ve üniversitelerin yeniden tanımlanmış verilere erişimi, sağlık hizmetleri sunucularının yeniden tanımlanmış verilere erişimi ve kâr amacı güden organizasyonların yeniden tanımlanmış verilere erişimi, yabancı hükümet ve kâr amacı gütmeyen kuruluşların yeniden tanımlanmış verilere erişimi de %100 oranında mümkündür (Tablo 2).

Kanada'da kişisel sağlık verilerinin diğer veri sorumluları ve hükümet yetkilileri ile paylaşım oranı %75'dir. Devlet analistlerinin yeniden tanımlanmış verilere erişimi %88, kâr amacı gütmeyen kuruluşlar ve üniversitelerin yeniden tanımlanmış verilere erişimi %88, sağlık hizmetleri sunucularının yeniden tanımlanmış verilere erişimi %88, kâr amacı güden organizasyonların yeniden tanımlanmış verilere erişimi %75, yabancı hükümet ve kâr amacı gütmeyen kuruluşların yeniden tanımlanmış verilere erişimi ise %63 oranında mümkündür (Tablo 2).

Türkiye'de devlet analistlerinin yeniden tanımlanmış verilere erişimi %100 oranındadır. Fakat üniversite ve kâr amacı gütmeyen araştırmacıların yeniden tanımlanmış veriye erişimi, sağlık hizmeti sunucularının yeniden tanımlanmış verilere erişimi, kâr amacı güden organizasyonların yeniden tanımlanmış verilere erişimi, yabancı hükümet, üniversite veya kâr amacı gütmeyen araştırmacıların yeniden tanımlanmış verilere erişimi %0'dır (Tablo 2).

3.3. Ulusal Sağlık Verilerinin Gizlilik ve Güvenliğine İlişkin Yasal Düzenlemeler ve Etik Bildirgeler Açısından Karşılaştırma

Mevcut araştırmada Kanada, İngiltere ve Türkiye örneklemine bakıldığında; kişisel sağlık verisinin korunması ve gizliliğine dair farklı seviyelerde ve yapılanmalarda önlemler alındığı görülmüştür.

Örneğin; İngiltere'de kişisel sağlık verileri, kişisel verilerin alt kategorisi olduğundan Avrupa İnsan Hakları sözleşmesinin kişisel verilerin gizliliği ve korunmasını içeren 8. maddesi ile ilgilidir. Bu kapsamda İngiltere'de kişisel sağlık verilerinin gizliliğini korumayı amaçlayan pek çok yasal düzenleme mevcuttur. Bu yasal düzenlemeler 2006 tarihli Ulusal Sağlık Hizmeti Yasası (The NHS Act), 2012 tarihli Sağlık ve Sosyal Bakım Yasası (The Health and Social Care Act), Veri Koruma Yasası (The Data Protection Act) ve İnsan Hakları Yasasından (The Human Rights Act) meydana gelmektedir. Bu yasal düzenlemeler aracılığıyla kişisel verilerin hastalara bakım sunanlarla paylaşılması sağlanmakta, ancak verilerin ikincil amaçlarla kullanılması için hastaların rızası gerekmektedir. Verilerin "ikincil amaçla kullanımı" ise şunları içermektedir:

* Hizmet kalitesinin gözden geçirilmesi ve iyileştirilmesi,

* Hangi tedavilerin en iyi sonucu verdiğinin araştırılması,

* Hangi klinik hizmetlerin sunulacağına karar verilmesi,

* Halk sağlığı hizmetlerinin planlanması.

İngiltere'deki Veri Koruma Kanunu, kişisel bilgilerin kuruluşlar, işletmeler veya hükümet tarafından nasıl kullanıldığını kontrol eden yasal düzenlemedir. Buna göre kişisel verileri kullanmaktan sorumlu olan herkesin ‹veri koruma ilkeleri› adı verilen katı kurallara uyması gerekmektedir. Bu kurallar şöyle sıralanmaktadır **(Data Protection Act, 2018):**

- Veriler adil, yasal ve şeffaf bir şekilde kullanılabilir.
- Veriler önceden belirlenmiş, açık ve net amaçlar için kullanılabilir.
- Veriler kullanım amacıyla ilgili ve yalnızca gerekli olanla sınırlı olacak şekilde kullanılabilir.
- Veriler doğru ve gerektiğinde güncel tutulmalıdır.
- Veriler gerekenden daha uzun süre saklanamaz.
- Veriler yasadışı veya yetkisiz işleme, erişim, kayıp, imha veya hasara karşı koruma da dâhil olmak üzere uygun güvenliği sağlayacak şekilde ele alınmalıdır.

Ayrıca İngiltere'de Veri Koruma Kanunu uyarınca hastaların sahip olduğu haklar şunlardır **(Data Protection Act, 2018):**

- Bireyler sağlık verilerin nasıl kullanıldığı hakkında bilgi alabilmektedir.
- Bireyler kişisel sağlık verilerine erişim sağlayabilmektedir.
- Bireyler kendisi hakkında herhangi bir kuruluşun sahip olduğu verilerin neler olduğu öğrenilebilir hale gelmiştir.
- Bireyler verilerini güncelleme ve silme yetkisine sahip olmuştur.
- Bireyler verilerin işlenmesini durdurma veya kısıtlama yetkisine sahip olmuştur.
- Bireyler kendine ait verileri farklı hizmetler için kullanmak istediğinde verilerin taşınabilirliği mümkün hale gelmiştir.
- Bireyler belirli durumlarda verilerin işlenmesine itiraz etme hakkına sahiptir.

Bu bilgilere ek olarak İngiltere'de veri koruma, gizlilik ve bilgi alma hakları konusunda merkezi bir otorite konumunda olan İngiltere Bilgi Komiserliği Ofisi'nin de (ICO - Information Commissioner's Office) mevcut olduğunu ifade etmek gerekmektedir. ICO, kişisel verilerin korunmasını sağlayan ve veri koruma yasalarının uygulanmasını denetleyen bağımsız ve düzenleyici bir organdır. ICO, veri koruma ihlallerine karşı caydırıcı cezalar uygulayabilmekte ve kamuoyuna veri koruma bilinci aşılamak için çeşitli kampanyalar yürütmektedir **(https://ico.org.uk/)**. İngiltere'de yürürlükte olan Veri Koruma Yasası'nda 2018'de yapılan düzenleme kapsamında ICO, veri paylaşımı için uygulama kodu yayınlamıştır. Bu uygulama kodu ilgili yasa kapsamında oluşturulan bir uygulama esası niteliğinde olup; veri koruma kanununa uygun olarak kişisel verilerin nasıl paylaşılacağı konusunda kuruluşlar için pratik bir rehberdir **(Data Protection Act, 2018).**

Ayrıca 2015 yılında İngiltere'nin de aralarında bulunduğu 63 ülkenin katılımıyla gerçekleşen 37. Uluslararası Veri Koruma ve Gizlilik Komiserleri Konferansı'nda kabul edilen Amsterdam Bildirgesi ile veri gizliliğinin güçlendirilmesine yönelik uluslararası işbirliğini ve politikaları teşvik etmeyi amaçlanmaktadır. İngiltere Bilgi Komiserliği Ofisi de bu konferansta yer almış ve bildiriyi desteklemiştir **(Amsterdam Bildirgesi, 2015).**

Araştırmaya dahil edilen diğer bir ülke olan Kanada'da ise ilk kişisel verilerin gizliliği ve korunmasına yönelik düzenleme 1977'de İnsan Hakları Kanunu ile yasalaşmıştır. Kanada'da ulusal düzeyde sağlık veri gizliliği koruma mevzuatı bulunmasa da federal düzeydeki bilgiler, eyalet / bölge ve belediye yasalarıyla güvence altındadır. 13 eyalet ve bölgenin her birinin genel kişisel bilgilerin gizliliği ile ilgili özel mevzuatı varken, bazılarının ise sağlık bilgilerinin korunmasına ilişkin özel mevzuatı vardır. Bazı eyaletlerde ise sağlık sektörüne özgü gizlilik mevzuatı beklemededir. Ayrıca Kanada federal hükümet departmanlarının kişisel bilgi işleme uygulamaları ve ulusal düzeydeki kişisel sağlık verilerinin gizliliği Kişisel Bilgi Koruma ve Elektronik Belgeler Yasası (PIPEDA) ve Gizlilik Yasası (The Privacy Act) kapsamındadır. Gizlilik Yasası, bir kişinin Kanada Hükümeti'nin kendisi hakkında tuttuğu kişisel bilgilere erişme ve bu bilgileri düzeltme hakkıyla ilgilidir. PIPEDA ise özel sektör kuruluşlarının Kanada genelinde ticari faaliyetler sırasında kişisel bilgileri nasıl topladığını ve kullandığını açıklamaktadır. Aynı zamanda federal olarak düzenlenen işler, teşebbüsler veya işletmeler için de geçerlidir. Kanada'daki doktorlar ticari faaliyetlerde bulundukları için PIPEDA'ya tabidir. Bu kapsamların dışında tutulan kişisel sağlık verilerinin olması olası değildir **(OECD, 2015; Swartz, 2004).**

Kanada'da da bu düzenlemelerin yanı sıra; Health Infoway isimli kar amacı gütmeyen kuruluş ile Ontario eyaleti Bilgi Komiserliği tarafından hazırlanan ortak raporda, elektronik klinik kayıtlardaki verilerin ikincil kullanımını sağlamak için tanımlama ve veri güvenliği de dâhil olmak üzere temel veri yönetişim mekanizmaları tanımlanmıştır **(Cavoukian ve Alvarez, 2012).** Dahası, Kanada'da ülke çapında sunulan sağlık hizmetlerini, sağlık sistemi performansını ve nüfus sağlığındaki iyileştirmeleri hızlandırmak için kullanılan karşılaştırılabilir ve eyleme dönüştürülebilir verileri sağlamak amacıyla Kanada Sağlık Bilgileri Enstitüsü (CIHI-Canadian Institute for Health Information) görev yapmaktadır. Bu enstitünün web sitesinden veri gizliliğinin korunması ile ilgili politikalara bireylerin erişim sağlaması mümkündür. Ayrıca CIHI, kişisel sağlık bilgilerinin ve tanımlanmamış verilerin toplanması,

kullanılması, paylaşılması ve saklanması ile ilgili politikaya sahip olmakla birlikte, gizlilik etki değerlendirmesi, personel gizliliği ve güvenliği eğitimi politikası ve güvenlik olayı yönetim protokolüne sahiptir. Yanı sıra Kanada'nın, Sağlık Bakan Yardımcıları Konferansı tarafından onaylanan Sağlık Sistemleri Kullanım Projesi kapsamında geliştirilen en iyi uygulama kılavuzlarına sahip olduğu bilinmektedir **(Health System Use Technical Advisory Committee, 2010).**

Araştırmaya dahil edilen diğer bir ülke olan Türkiye'de ise Mayıs 2006 tarihli ve 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu ile oluşturulan Sosyal Güvenlik Kurumu (SGK) MEDULA sistemi ile ödeme kapsamında olan bireylerin sağlık verileri elektronik ortamda kayıt altına almaktadır. Türkiye'de ulusal anlamda sağlık verisi toplama aracı MEDULA sistemidir **(Par ve Soysal, 2010)**. Türkiye'de 2019 yılında resmi gazetede yayınlanan kişisel sağlık verileri hakkında yönetmelikle sağlık hizmeti sağlayıcılarının yalnızca verdikleri hizmetin gereği ile sınırlı verilere erişimi mümkün kılınmıştır. Yanı sıra E-Nabız uygulaması ile bireylerin kişisel sağlık verilerinin kimlerle ve ne kadar süre paylaşacağını seçmesi sağlanmıştır.

E- Nabız hesabı olmayan vatandaşların verilerinin gizliliği istisna kabul edilmiştir. Mahremiyet düzeyi daha yüksek olan, başkaları tarafından görülmesi ve bilinmesi halinde kişilerin sosyal hayatını ve ruh sağlığını olumsuz etkileme riski taşıyan kişisel sağlık verilerinin ise bakanlıkça belirlenmesi kararlaştırılmıştır. Yeniden tanımlanmış verilerin devlet kurumları ve birimleri arasında paylaşımı hatta veri sahipleriyle verilerin tekrar eşleştirilmesi sağlık bakanlığı birim amirleri ve her bölümden en fazla üç kişinin erişimi mümkün olmuştur **(T.C. Cumhurbaşkanlığı Mevzuat Bilgi Sistemi, 2019).**

Türkiye'de 2019 yılında yürürlüğe giren Kişisel Sağlık Verileri Hakkında Yönetmelik bu konudaki en kapsamlı düzenlemeleri sunan yasal düzenleme olarak karşımıza çıkmaktadır. Yine 1998 tarihli Hasta Hakları Yönetmeliği de bireylerin ve hastaların kişisel sağlık verilerinin yönetimine dair yasal sınırlar sunmaktadır. Hasta Hakları Yönetmeliği'ne göre sağlık verileri kanun ile müsaade edilen haller dışında, hiçbir şekilde açıklanamaz; araştırma ve eğitim amacı ile yapılan faaliyetlerde de hastanın kimlik bilgileri, rızası olmaksızın kullanılamaz.

Yanı sıra Türk Tabipler Birliği (TTB) tarafından yayınlanan etik bildirgelerde sağlık verilerinin gizliliği ve güvenliği sıklıkla vurgulanmaktadır. Örneğin Hasta Hakları Bildirgesine göre hastanın kişisel bilgilerinin, tanı ve tedavisinin, sağlık durumunun ve her türlü özel bilgilerinin gizli tutulması ve korunması sağlanmalıdır. Bu bildirgeye göre elektronik ortamda tutulan kayıtların gizliliğinin sağlanması için gerekli ve yeterli önlemler alınmalıdır **(TTB, 2009)**.

TTB (2019)'nin etik bildirgelerinden olan Mahremiyet Hakkının Korunmasına İlişkin Bildirgede de konuya ilişkin "Hekimler, hastalarının kendisine verdiği ve hastalarına dair elde ettiği her türlü bilgiyi mesleki sır kapsamında değerlendirmeli ve bu bilgileri açıklamamalıdır." ifadesine yer verildiği görülmektedir.

Buradan hareketle; Kanada, İngiltere ve Türkiye'de ilgili konuya dair yürürlükte olan yasal düzenlemeler tablo 3'te özetlenerek sunulmaktadır.

4. Sınırlılıklar

Bu çalışmanın temel sınırlılıklarından biri kullanılan verilerin bir kısmının OECD tarafından yayımlanan Sağlık Verisi Yönetişimi raporundan elde edilmesinden kaynaklanmaktadır. OECD'nin ilgili rapor kapsamında kullandığı veriler ülkelerin kendi raporlamalarına dayandığından, verilerin doğruluğu ve tutarlılığı açısından sınırlılıklar içerebilirler. Bu nedenle elde edilen bulguların yorumlanmasında bir ihtiyat payı tanınması gerekliliği gözden kaçırılmamalıdır. Gelecekte yapılacak araştırmalarda kullanılacak ikincil veri kaynaklarının bağımsız veri doğrulama mekanizmasına sahip veri kaynaklardan müteşekkil olması önerilmektedir.

5. Tartışma

Sağlık verilerinin gizliliği ve güvenliği, tıp tarihinde uzun bir geçmişe sahiptir. Bu durum, Hipokrat yeminiyle de açıkça ifade edilmiş ve hastalara ait bilgilerin, ölüm sonrasında dahi sır olarak saklanması gerektiği belirtilmiştir. M.Ö. 400 lerde bile hasta ile sağlık hizmeti sunucusu arasındaki mahremiyet, büyük bir önem taşımıştır **(Scott, Jennett ve Yeo, 2004)**. Sağlık verilerinin gizliliği ve güvenliği tarih boyunca önemini korurken, günümüzde bu alandaki tehditler dijitalleşmeyle birlikte daha da karmaşık hale gelmiştir. Elektronik sağlık kayıtları ve kişisel sağlık kayıtlarının artışı, hasta bilgilerini dijital ortama taşırken mahremiyet ve güvenlik açısından yeni ve ciddi riskler ortaya çıkarmaktadır **(Shojaei ve ark., 2024)**. Bu durum, ülkelerin sağlık kayıtlarını korumaya yönelik stratejiler geliştirme ihtiyacını doğurmaktadır **(Keshta ve Odeh, 2021)**. Ülkelerin sağlık verilerinin korumaya yönelik geliştirdiği stratejiler bu konudaki yasal düzenlemelerine de yansımaktadır. Bu noktada farklı ülkelerin sağlık verilerinin gizliliği ve güvenliği konusundaki yasal düzenlemelerinin incelenmesi, bu alandaki en iyi uygulamaların belirlenmesi açısından kritik öneme sahiptir. Bu tür bir karşılaştırma, ülkelerin birbirinden öğrenmesini sağlayarak daha etkili ve güvenilir politikaların geliştirilmesine katkıda bulunabilir. Buradan hareketle mevcut çalışmada, Kanada, İngiltere ve Türkiye'nin kişisel sağlık verilerinin gizliliği ve güvenliği konusundaki uygulamaları karşılaştırılmıştır.

Mevcut araştırmada yapılan inceleme neticesinde Kanada'nın, kişisel sağlık verilerinin korunmasında ulusal ve eyalet düzeyinde çeşitli yasalarla güçlü bir yapı oluşturduğu görülmektedir. Benzer şekilde İngiltere de sağlık verilerinin korunmasına yönelik katı düzenlemeler benimsemiştir. Türkiye ise son yıllarda Kişisel Verilerin Korunması Kanunu (KVKK) ile bu alandaki düzenlemelerini güçlendirmiştir. Ayrıca Kanada ve İngiltere, veri paylaşımı ve erişimini daha geniş tutarak sağlık verilerinin araştırma ve kamu yararına kullanımını teşvik ederken, Türkiye daha korumacı bir yaklaşım sergilemektedir. Sağlık verilerinin araştırma ve istatistik için paylaşım ve erişilebilirlik oranının sırasıyla İngiltere'de ve Kanada'da en yüksek skora sahip olduğu görülmektedir. İngiltere'de ve Kanada'da kurumlar arası bilgi paylaşımının yüksekliği buna bağlı olarak

Tablo 3. Kişisel Sağlık Verilerinin Gizliliği ve Güvenliği ile İlgili Yasa, Yönetmelik Ve Bildirgeler

Ülkeler	Elektronik Sağlık Kayıtların Korunması ile İlgili Yasa veya Yönetmelikler
Kanada	• Kanada'daki her ülkenin (federal, eyalet ve bölge) kişisel bilgilerin toplanmasını, kullanılmasını ve ifşa edilmesini düzenleyen kendi gizlilik mevzuatı vardır. • Buna ek olarak, bazı illerde sağlık bilgilerini özel olarak ele alan özellikli sağlık bilgileri gizlilik mevzuatı vardır. • Ulusal düzeyde ise geçerli olan iki federal yasa vardır. Bunlar: 1. Gizlilik Yasası (The Privacy Act) https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-privacy-act/ • Kişisel Bilgilerin Korunması ve Elektronik Belgeler Yasası (The Personal Information Protection and Electronic Documents Act) (PIPEDA) https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/
İngiltere	• 2006 NHS Yasası https://www.legislation.gov.uk/ukpga/2006/41/contents • 2012 Sağlık ve Sosyal Bakım Yasası https://www.legislation.gov.uk/ukpga/2012/7/contents/enacted • 1998 İnsan Hakları Yasası https://www.legislation.gov.uk/ukpga/1998/42/contents • 2018 Veri Koruma Yasası https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted • Amsterdam Bildirgesi https://edps.europa.eu/sites/edp/files/publication/15-10-27_amsterdam_declaration_en.pdf
Türkiye	• 6698 sayılı 2016 Kişisel Verilerin Korunması Kanunu https://www.mevzuat.gov.tr/MevzuatMetin/1.5.6698.pdf • 1998 Hasta Hakları Yönetmeliği mevzuat.gov.tr/mevzuat?MevzuatNo=4847&MevzuatTur=7&MevzuatTertip=5 • 2019 Kişisel Sağlık Verileri Hakkında Yönetmelik https://www.resmigazete.gov.tr/eskiler/2019/06/20190621-3.htm • 2009 tarihli Türk Tabipler Birliği Hasta Hakları Bildirgesi https://www.ttb.org.tr/etik_bildirge.php • 2019 tarihli Türk Tabipler Birliği Mahremiyet Hakkının Korunmasına İlişkin Bildirge https://www.ttb.org.tr/etik_bildirge.php

işbirliğinin de yüksek olduğunu göstermektedir. Veri paylaşımı ve erişilebilirliği konularındaki göstergeler, her ülkenin sağlık verisi yönetiminde izlediği politikaların etkisini ortaya koymaktadır. Türkiye'nin sağlık verilerinin paylaşımı ve erişilebilirliği açısından diğer iki ülke ile kıyaslandığında daha düşük bir performans sergilediği görülmektedir. Halbuki sağlık verilerinin araştırma ve istatistik için paylaşımı sağlık hizmeti kalitesinin ve sistem performansının izlenmesinin ve iyileştirilmesinin yanı sıra daha iyi sağlık hizmeti ve sonuçlarına ulaşmak için yapılacak yenilikçi adımları destekleyen bir husustur. Bu nedenle Türkiye'nin kişisel sağlık verilerinin istatistiksel ve araştırma amaçlı kullanımı konusunda etkin bir süreç geliştirmesi ve toplumsal riskleri en aza indirerek toplumsal faydayı en üst düzeye çıkaracak şekilde düzenlenmiş veri yönetimini temin etmesi gerekmektedir **(OECD, 2015).**

Mevcut araştırma göstermektedir ki Kanada ve İngiltere gibi gelişmiş ülkeler veri paylaşımının topluma faydalı olduğunun, hatta bazı durumlarda veriyi paylaşmamanın bütünsel açıdan daha olumsuz etkileri olacağının bilincindedir. Sağlık verilerinin ne kadarının, kimler tarafından, nasıl ve ne amaçla kullanıldığı sağlık verisinin kapsayıcılığı ve kullanılabilirliğine ilişkin kaliteyi etkileyen unsurlardandır **(Amerikan Sağlık Yönetimi Enstitüsü, 2021).** Tabii burada temel prensip sağlık verisinin belirtilen araştırma hedeflerine uygun olarak mahremiyeti olumsuz etkilemeyecek şekilde kullanılmasıdır. Araştırmada görülmektedir ki sağlık verisinin araştırma ve istatistik için paylaşımı

beraberinde pek çok riskleri taşımasına rağmen gelişmiş ülkeler uygulamaya koydukları standart kodlar aracılığıyla riskleri bertaraf etmeye çalışmaktadırlar. Örneğin İngiltere'de veri paylaşımı için yayınlanan uygulama kodu, veri koruma kanununa uygun olarak kişisel verilerin nasıl paylaşılacağı konusunda kuruluşlar için fayda sağlayan bir rehber olarak değerlendirilmektedir. Bu tarz kodlar, yararları ve riskleri dengelemeye ve veri paylaşımını uygulamaya yardımcı olmaktadır. Türkiye'nin mevcut düzenlemeleri, özellikle Kişisel Verilerin Korunması Kanunu (KVKK) ile güçlendirilmiş olsa da, veri paylaşımını ve araştırma amaçlı kullanımını teşvik etme konusunda Kanada ve İngiltere gibi gelişmiş ülkelerin uygulamalarından uzak kalmaktadır. Türkiye'nin bu konudaki korumacı yaklaşımı, sağlık verilerinin güvenliğini ön planda tutsa da, araştırma ve istatistik amaçlı verilerin kullanımını sınırlayarak sağlık hizmetlerinin kalitesinin artırılmasını engellemektedir. Bu durumu iyileştirmek için Türkiye'nin sağlık verilerinin araştırma ve istatistik amaçlı kullanımını daha etkin hale getirecek bir strateji benimsemesi önemlidir. Ancak veri paylaşımına ilişkin tüm zorlukları çözecek bir düzenleme tek başına yeterli olmayacaktır.

Türkiye'de kültürel, teknik ve organizasyonel faktörler de dâhil olmak üzere veri paylaşımının önünde çeşitli engeller vardır. Birçok sağlık kuruluşu tarafından üretilen sağlık verisi değer yaratan bir kaynak olsa da, hasta mahremiyeti endişeleri sebebiyle araştırmacıların çoğu tarafından erişilebilir nitelikte değildir. Araştırma ve geliştirme amacı dahil olmak üzere tıbbi kayıtlara erişim, gizlilik ve güvenlik kısıtlamaları, verinin işlenmesi ile ilgili düzenlemeler nedeniyle sınırlandırılmaktadır. Ayrıca, araştırmacıların sağlık verisine erişimi her ne kadar mümkün olsa bile; verinin işlenmesi, korunması ve kullanımı konusundaki yasal gerekliliklerin yerine getirilmesi uzun bir süreç gerektirmekte olup bu durum, araştırma sonucundan ve bilginin paylaşılmasından sağlanacak faydayı da ciddi şekilde geciktirmektedir **(Deveci ve Esen, 2022).** Bununla birlikte her geçen gün bir adım daha öteye taşınan e-sağlık teknolojileri ile ilgili gelişmeler de veri güvenliği ve mahremiyete ilişkin kaygıları arttırmaktadır. Bu teknolojilerin sağlık sektörüne adaptasyonunun sağlanmasında öncelikle mahremiyet ve güvenlikle ilgili teknik konuların çözüme kavuşturulması gerekmektedir **(Söyler ve Averbek, 2022)**. Bunların üstesinden gelmek standardize edilmiş kodlardan daha fazlasını; uygulayıcıların, hükümetin ve düzenleyicilerin ortak çabasını gerektirecektir. Bu nedenle bu zorlukların üstesinden gelmek için sağlam güvenlik protokolleri, risk algılama, azaltma ve sürekli izleme mekanizmaları, güvenlik farkındalığına dair eğitim programlarına yatırım yapmak gibi çok yönlü yaklaşımı gerekmektedir **(Olaniyi ve ark., 2023)**. Devlet kurumları, sektör ortakları ve siber güvenlik uzmanları da dâhil olmak üzere paydaşlar arasındaki işbirliği, risklerle etkili bir şekilde mücadele etmek ve dijital çağda sağlık verilerinin gizliliğini ve güvenliğini korumak için hayati öneme sahiptir (**Farayola ve ark., 2024**).

Türkiye'de bu konuyu vurgulayan ve **Türk Tabipler Birliği (2019)** tarafından kabul edilen Mahremiyet Hakkının Korunmasına İlişkin Bildirgeye göre; devlet ve ilgili sağlık kurumu yönetimi kişisel sağlık verilerinin elektronik ortamda tutulması nedeniyle doğabilecek sakıncaların oluşmaması için gerekli her türlü önlemi almalıdır. Yanı sıra ülkelerde verilerin gizliliği ve güvenliğine ilişkin yürürlükte olan yasalara uyma gerekliliği ve sağlık verilerinin çok çeşitli amaçlarla kullanılabilmesinin önemi göz önüne alındığında, sağlık verilerinin kimliksizleştirilmesine yönelik süreçlerin etkin olması gerekmektedir. Aynı zamanda veri kimliksizleştirme ve risk yönetimine yönelik süreçlerin gelişen teknolojilere duyarlı olacak şekilde tasarlanması, ilgili risklerin yönetilmesi için büyük önem taşımaktadır **(Health System Use Technical Advisory Committee, 2010).** Konuya ilişkin İngiltere örneğine baktığımızda kişisel sağlık verilerinin ikincil amaçlarla kullanılması için hastaların rızasının gerektiği ve bu sürece ilişkin bir onay izni modeli geliştirdiği görülmektedir. Bu model, hastaların sağlıkla ilgili idari ve klinik veri tabanlarındaki verilerin gelecekteki kullanımlarına ilişkin seçimlerini ifade etmelerini sağlamaktadır. Böylelikle bireyler, pratisyen hekimlerine ulusal sağlık veri setlerinde tutulan verilerinin istatistik amaçlı veya araştırma projelerinde kullanılmasını istemediklerini belirterek vazgeçme hakkına sahiptir (OECD, 2015). Benzer şekilde Türkiye'de **Türk Tabipler Birliği (2019)** tarafından kabul edilen Mahremiyet Hakkının Korunmasına İlişkin Bildirgeye göre; hekimler, hastaların kendilerine ait sağlık verilerinin paylaşılması ile ilgili verdiği onamı her zaman geri alabileceğini ve bu durumun bireyin sağlık hizmetlerine erişimini engellememesi gerektiğini kabul etmektedir. Dahası bu bildirgeye göre hekimler, kişilerin kendilerine ait sağlık verilerinin düzeltilmesini ve silinmesini isteme hakkı olduğunu, kişisel sağlık verilerinin sahibinin sağlık kurumları değil, kişinin kendisi olduğunu kabul etmektedir. Bu anlamda hastaların zaman içinde rıza tercihlerini değiştirmelerine olanak tanıyan dinamik rıza platformlarının kullanılması, sağlık hizmetleri ve araştırmalarının gelişen doğasına uyum sağlayacağı ifade edilmektedir **(Haas ve ark., 2021).** Bu platformlar sürekli iletişim ve eğitim sağlayarak rızanın bilgilendirilmiş kalmasını sağlayabilmektedir. Bu bağlamda sağlık verilerinin paylaşılmasına dair hastaların rıza vermesine ilişkin sürecin iyileştirilmesi kapsamlı stratejiler gerektirmektedir. Ayrıca hastalara, rızalarının önemini ve dijital sağlık teknolojilerinin bakımları üzerindeki etkisini öğrenmeleri için eğitim kaynakları ve fırsatlar sağlamak, hastaların daha bilinçli kararlar vermesine olanak tanıyabilmektedir. **(Adeniyi, 2024).**

Mevcut araştırmada ulusal sağlık veri setlerinin kapsayıcılığı ve kullanılabilirliğine bakıldığında ise Türkiye'nin, ulusal düzeyde mevcut veri seti yüzdesi ve verilerin elektronik kayıtlardan otomatik olarak alındığı mevcut sağlık veri setlerinin yüzdesi bağlamında diğer iki ülkeyle kıyaslandığında daha avantajlı konumda olduğu görülmektedir. Sağlık verisinin kapsamlılığı, belirli bir kullanım için gereken verilerin mevcut olması ve kullanıcı tarafından erişilebilir olması anlamına gelmekte olup; **Amerikan Sağlık Yönetimi Enstitüsü (2021)**'ne göre sağlık verisinin kalite göstergelerinden biridir. Bunun nedeni hasta kayıtlarının kapsamlılıktan yoksun olmasının hasta güvenliğini, tedavinin sürekliliğini ve bakımın kalitesini tehlikeye atma potansiyelinin söz konusu olmasıdır

(Thoroddsen ve ark., 2013). Ayrıca ülkeler tarafından toplanan sağlık verilerinin ulusal düzeyde temsiliyeti, sağlığın belirleyici ölçütlerinin doğru yorumlanması için önemlidir. Bu veriler, aynı zamanda hükümetlerin yasal organlarının ve müdahalelerinin toplumun geneline yayılmasını sağlayacak şekilde düzenlenmesini ve değerlendirilmesini de mümkün kılar **(Nickelsen, 2001).** Türkiye'nin MEDULA ve E-Nabız gibi sistemler aracılığıyla entegre sağlık veri tabanlarının kullanılması ulusal düzeyde yaygınlaştırılmış veri setlerinin oluşmasını sağlamıştır **(İleri ve Uludağ, 2017).** Kanada'da ise sağlık bilgi sistemlerini organizasyonu ve kullanımı eyalet düzeyinde örgütlenmekte ve finanse edilmektedir. Bu nedenle ulusal düzeyde veri setleri daha az mevcuttur **(Karaca, 2023)**. İngiltere'de de bölgesel düzeyde toplanan veriler ulusal sağlık veri seti oranını düşürmüştür **(OECD, 2015)**. Ayrıca Kanada'daki federal devlet yapısı, İngiltere'de ise veri setlerinin kaynağının geri ödeme kapsamındaki hizmetlerden oluşması veri setlerinin nüfusu kapsayıcılığını azaltmıştır. Türkiye'nin bu konudaki avantajlı durumu özellikle halk sağlığının geliştirilmesine yönelik konuları veri odaklı bakım yaklaşımıyla ele almada bir fırsat olarak değerlendirilmektedir. Örneğin **Vinsensia ve ark. (2024)** tarafından yapılan çalışma, bulaşıcı hastalık tehditlerine yanıt verme yeteneği geliştirmek ve salgınlara verilen yanıtı iyileştirmek gibi halk sağlığı konularında büyük veriye dayalı analizlerin daha iyi çözümler sağladığını ortaya koymuştur. Bilgi teknolojisi ve veri analizindeki gelişmelere rağmen, hastalık kalıplarını ve eğilimlerini belirlemede Türkiye sağlık verilerinin potansiyelini yeterince kullanamamaktadır **(Deveci ve Esen, 2022).**

Sonuç olarak sağlık verilerinin gizliliği ve güvenliği konusundaki yasal düzenlemeler ve uygulamalar, sağlık sistemlerinin güvenilirliğini ve etkinliğini doğrudan etkileyeceği temelinden hareketle oluşturulan öneriler aşağıdaki gibidir:

- Türkiye'deki veri erişim politikaları gözden geçirilerek, araştırmacılar ve akademisyenler için sağlık verilerinin daha erişilebilir hale getirilmesi sağlanmalıdır. Böylelikle sağlık verilerinin daha etkin kullanılması ve sağlık hizmetlerinin iyileştirilmesi mümkün olacaktır.
- Kanada'da ve İngiltere'de sağlanan geniş veri erişimine rağmen bireylerin kişisel bilgilerinin korunması konusuna hassasiyetle yaklaşılması önemlidir. Bu nedenle Türkiye'de veri erişilebilirliğinin arttırılmasının yanı sıra veri paylaşım sürecinde güvenlik protokollerinin güçlendirilmesi ve bireylerin mahremiyetini korumaya yönelik önlemler alınması önerilmektedir.
- ISO standartları gibi küresel çerçeveler, sağlık verilerinin gizliliği ve güvenliğinde tutarlılık sağlayabilir. Bu nedenle ülkeler arasında iyi uygulamaların paylaşılmasının yanı sıra uluslararası standartların benimsenmesi de önemlidir.
- Gelecek araştırmalar için yol gösterici olma potansiyeli açısından, Türkiye, Kanada ve İngiltere'nin sağlık verilerinin gizlilik ve güvenliğinin elektronik sağlık kaydı sistemleri ve sağlık bilişimi finansmanı ile ilgili göstergeler üzerinden daha detaylı incelenmesi önerilmektedir. Ayrıca daha fazla ülke örneğinin dahil edilmesi ve teknolojik gelişmelerin zamanla getirdiği yeni risklerin dikkate alındığı düzenlemelerin izlenmesi, sağlık verilerinin yönetimi konusunda daha esnek ve uyarlanabilir politikaların oluşturulmasına katkı sağlayacaktır.

6. Sonuç

Bu çalışma, Kanada, İngiltere ve Türkiye'nin sağlık verilerinin gizliliği, güvenliği ve erişilebilirliği konusundaki yaklaşımlarını karşılaştırmalı olarak ele almıştır. Çalışmanın sonuçları, sağlık verisi gizliliği ve güvenliği konusunda ülkelerin kendi yasal, teknolojik ve kültürel dinamikleri doğrultusunda farklı stratejiler benimsediğini ortaya koymaktadır. İncelenen ülkeler arasında Türkiye, ulusal düzeyde kapsamlı veri setlerine sahip olması bakımından dikkat çekerken; veri paylaşımı ve verilere araştırma amaçlı erişilebilirlik noktasında Kanada ve İngiltere'nin daha açık politikalar izlediği görülmüştür. Kanada ve İngiltere, uzun yıllara dayanan düzenleyici altyapıları sayesinde, veri paylaşımının toplumsal ve bilimsel faydaya dönüşmesini desteklerken, Türkiye hızlı dijitalleşme sürecine paralel olarak veri güvenliğini ön planda tutan ancak paylaşım konusunda daha muhafazakar bir yaklaşım sergilemektedir. Gerek Kanada gerekse de İngiltere örneğinde göze çarpmaktadır ki sağlık verilerinin yönetimi, yalnızca devlet politikalarına bağlı kalmayan, aynı zamanda sağlık kuruluşları, akademi ve siber güvenlik uzmanları arasında aktif işbirliği gerektiren bir alan olarak öne çıkmaktadır. Bu bağlamda Kanada ve İngiltere bu tarz ortak çalışmalara dayalı stratejilerin veri güvenliğini artırdığının ve sağlık hizmetlerinin kalitesini yükseltiğinin bilincinde olarak yasal düzenlemelerini inşa etmektedir. Türkiye'de bu anlamda disiplinlerarası yaklaşım ve kurumlararası işbirliği eksikliği sağlık verilerinin ikincil amaçlarla kullanımına dair temkinli bir yaklaşımı beraberinde getirmektedir. Ayrıca dijitalleşmenin hız kazandığı günümüzde, sağlık verilerinin korunmasına yönelik yasal düzenlemelerin sürekli olarak gözden geçirilmesi önem kazanmaktadır. Veri anonimleştirme ve dinamik rıza süreçlerine yönelik mekanizmaların geliştirilmesi, veri paylaşımının hem güvenli hem de etkili bir şekilde yapılmasını sağlayabilir. Sonuç olarak sağlık verilerinin yönetiminde her ülke kendi önceliklerini ve risk algılarını yansıtmaktadır. Haliyle bu durum da veri paylaşımı, gizlilik ve güvenlik arasında karmaşık ama yerel dinamiklere uygun çözümlerin yaratılmasına sebep olmaktadır. Sağlık verilerinin hem güvenliğini sağlamak hem de araştırma ve geliştirme alanlarında etkin kullanılabilirliğini artırmak için ülkelerin birbirlerinden öğrenebilecekleri iyi uygulamaların incelenmesi anahtar bir gelişim aracı olabilir. Türkiye için, veri güvenliğini tehlikeye atmadan, araştırmacıların ve kamu kurumlarının erişimine dair daha elverişli çözümler geliştirmek, sağlık hizmetlerinin kalitesini ve sistem performansını artıracak potansiyel bir adım olarak değerlendirilebilir. Bu bağlamda sağlık verilerinin yönetiminde ideal bir denge kurmanın, ulusal şartlara, dinamiklere ve teknolojik gelişmelere uyumlu esnek yaklaşımlarla mümkün olacağı öngörülmektedir.

Kaynaklar

Adeniyi, A. O., Arowoogun, J. O., Okolo, C. A., Chidi, R.,Babawarun, O. *(2024). Ethical Considerations in Healthcare IT: A Review of Data Privacy and Patient Consent Issues. World Journal of Advanced Research and Reviews, 21(2), 1660-1668. https://doi.org/10.30574/wjarr.2024.21.2.0593*

American Institute for Healthcare Management *(2021). Erişim Linki: https://www.amihm.org/healthcare-data-quality/ Erişim Tarihi: 1 Ocak 2025.*

Amsterdam Bildirgesi *(2015). 37th International Privacy Conference of Data Protection and Privacy Commissioners, Closed Session, 27 October, Amsterdam, Netherlands.*

Arora, C. *(2019). Digital Health Fiduciaries: Protecting User Privacy When Sharing Health Data. Ethics and Information Technology, 21(3), 181-196. https://doi.org/10.1007/s10676-019-09499-x*

Cavoukian, A., Alvarez, R.C. *(2012) Embedding Privacy Into The Design of EHRs to Enable Multiple Functionalities - Win/Win.*

Chung, R. J., Lee, J. B., Hackell, J. M., Alderman, E. M. *(2024). Confidentiality in The Care of Adolescents: Technical Report. Pediatrics, 153 (5): e2024066327. https://doi.org/10.1542/peds.2024-066327*

CIHI (Canadian Institute For Health Information) *What are health data standards?, Erişim tarihi: 17.05.2024, Erişim linki: https://www.cihi.ca/en/submit-data-and-view-standards/data-standards/what-are-health-data-standards*

Data Protection Act *(2018) Erişim Tarihi: 17.05.2024, Erişim Linki: https://www.legislation.gov.uk/ukpga/2018/12/section/1/enacted*

Deveci, A., Esen, M.F. *(2022). Medikal Sentetik Veri Üretimiyle Veri Dengelemesi. İstatistik ve Uygulamalı Bilimler Dergisi, (5):17-27. https://doi.org/10.52693/jsas.1105599*

Fernández-Alemán, J. L., Señor, I. C., Lozoya, P. Á. O., Toval, A. *(2013) Security and Privacy in Electronic Health Records: A Systematic Literature Review. Journal of Biomedical Informatics, 46(3): 541-562. https://doi.org/10.1016/j.jbi.2012.12.003*

Goldberg, L., Lide, B., Lowry, S., Massett, H. A., O'Connell, T., Preece, J., Quesenbery, W., Shneiderman, B. *(2011). Usability and Accessibility in Consumer Health Informatics: Current Trends and Future challenges. American Journal of Preventive Medicine, 40(5):187-197. https://doi.org/10.1016/j.amepre.2011.01.009*

Greenhalgh, T., Hinder, S., Stramer, K., Bratan, T., Russell, J. *(2010) Adoption, Non-Adoption, And Abandonment of A Personal Electronic Health Record: Case Study of Healthspace. Bmj, 2010. 341: C5814. https://doi.org/10.1136/bmj.c5814*

Haas, M. A., Teare, H., Prictor, M., Ceregra, G., Vidgen, M. E., Bunker, D., Kaye, J., Boughtwood, T. *(2021). 'CTRL': An Online, Dynamic Consent And Participant Engagement Platform Working Towards Solving The Complexities Of Consent İn Genomic Research. European Journal of Human Genetics, 29(4), 687-698. https://doi.org/10.1038/s41431-020-00782-w*

Health System Use Technical Advisory Committee *(2010). "Best Practice" Guidelines For Managing The Disclosure Of De-Identified Health Information.*

Farayola, O. A., Olorunfemi, O. L., Shoetan, P. O. *(2024). Data Privacy And Security in IT: A Review Of Techniques And Challenges. Computer Science & IT Research Journal, 5(3): 606-615. https://doi.org/10.51594/csitrj.v5i3.909*

ICO - Information Commissioner's Office official web page *Erişim tarihi: 16.05.2024 Erişim linki: https://ico.org.uk/*

ISO / TS 13606-4 *(2009)* ***ISO 22857*** *(2013) Health Informatics — Guidelines on Data Protection To Facilitate Trans-Border Flows of Personal Health Data. Erişim Tarihi: 16.05.2024, Erişim Linki: https://www.iso.org/obp/ui/#iso:std:iso:22857:en*

İleri, Y.Y., Uludağ, A. *(2017). E-Nabız Uygulamasının Yönetim Bilişim Sistemleri ve Hasta Mahremiyeti Açısından Değerlendirilmesi. Uluslararası Sağlık Yönetimi ve Stratejileri Araştırma Dergisi, 3(3):318-325.*

Kaplan, B. *(2015) Selling Health Data De-Identification, Privacy, And Speech. Cambridge Q. Healthcare Ethics, 24: 256.*

Karaca, M. *(2023). Türkiye, İspanya ve Kanada Sağlık Sistemi ve Göstergelerinin Karşılaştırmalı Analizi. Anadolu Akademi Sosyal Bilimler Dergisi, 5(1):125-151.*

Keshta, I., Odeh, A. *(2021). Security And Privacy Of Electronic Health Records: Concerns And Challenges. Egyptian Informatics Journal, 22 (2): 177–183. https://doi.org/10.1016/j.eij.2020.07.003*

Leonard, K.J., Casselman, M., Wiljer, D. *(2008) Who Will Demand Access To Their Personal Health Record. A Focus on The Users of Health Services And What They Want. Healthcare Quarterly, 11(1): 92-6.*

Nickelsen, T. *(2001) Data Validity And Coverage In The Danish National Health Registry: A Literature Review. Ugeskrift For Laeger, 164(1): 33-37.*

Nowrozy, R., Ahmed, K., Kayes, A. S. M., Wang, H., McIntosh, T. R. *(2024). Privacy Preservation Of Electronic Health Records İn The Modern Era: A Systematic Survey. ACM Computing Surveys, 56(8): 1-37.*

OECD *(2015). Health Data Governance: Privacy, Monitoring And Research. OECD Publishing.*

Olaniyi, O.O., Okunleye, O.J., Olabanji, S.O., Asonze, C.U. *(2023). IoT security in The Era of Ubiquitous Computing: A Multidisciplinary Approach To Addressing Vulnerabilities And Promoting Resilience. Asian Journal of Research in Computer Science, 16(4): 354-371. DOI: 10.9734/ajrcos/2023/v16i4397*

Par, Ö. E., Soysal, E. *(2010). Kişisel Sağlık Bilgilerinin Güvenliği Açısından Medula'da Kullanılan Yasa ve Standartların HIPAA ile Karşılaştırılması. MIE.*

Quach, S., Thaichon, P., Martin, K.D., Weaven, S., Palmatier, R.W. *(2022). Digital Technologies: Tensions in Privacy And Data. Journal of The Academy of Marketing Science, 50(6): 1299-1323.*

Rosenfeld, L., Torous, J., Vahia, I.V. *(2017) Data Security And Privacy In Apps For Dementia: An Analysis Of Existing Privacy Policies. The American Journal Of Geriatric Psychiatry, 25(8): 873-877. https://doi.org/10.1016/j.jagp.2017.04.009*

Shojaei, P., Vlahu-Gjorgievska, E., Chow, Y. W. *(2024). Security and Privacy of Technologies in Health Information Systems: A Systematic Literature Review. Computers, 13(2): 41. https://doi.org/10.3390/computers13020041*

Swartz, N. *(2004) Canada's Privacy Law Faces Legal Challenge: If Canadian Courts Rule PIPEDA Unconstitutional And Strike It Down, The Ramifications For Canadian And Worldwide Businesses Will Be Profound. Information Management Journal, 38(2): 20-24.*

Scott, R.E., Jennett, P., Yeo, M. *(2004) Access And Authorisation In A Glocal E-Health Policy Context. International Journal Of Medical Informatics, 73(3): 259-266. https://doi.org/10.1016/j.ijmedinf.2003.11.020*

Söyler, S., Averbek, G.S. *(2022). Sağlık Teknolojileri ve Metaverse: Potansiyel Uygulama Alanları ve Mevcut Engeller. International Anatolia Academic Online Journal Health Sciences, 8(2):138-166.*

T.C. Cumhurbaşkanlığı Mevzuat Bilgi Sistemi *(2019) Erişim tarihi: 20.05.2024, Erişim linki: https://www.resmigazete.gov.tr/eskiler/2019/06/20190621-3.htm*

The World Medical Association *(2008) Declaration of Helsinki, WMA General Assembly, Seoul, Korea, October.*

Thoroddsen, A., Sigurjónsdóttir, G., Ehnfors, M., Ehrenberg, A. *(2013). Accuracy, Completeness and Comprehensiveness of Information on Pressure Ulcers Recorded in the Patient Record. Scandinavian Journal of Caring Sciences, 27(1):84-91. https://doi.org/10.1111/j.1471-6712.2012.01004.x*

Türk Tabipler Birliği Web Sayfası *(2009) Erişim tarihi: 20.05.2020, Hasta Hakları Bildirgesi. Erişim linki: https://www.ttb.org.tr/etik_bildirge.php*

Türk Tabipler Birliği Web Sayfası *(2019) Erişim tarihi: 02.01.2025, Mahremiyet Hakkının Korunmasına İlişkin Bildirge. Erişim linki: https://www.ttb.org.tr/etik_bildirge.php*

Wadmann, S., Hartlev, M., Hoeyer, K. *(2023). The Life and Death of Confidentiality: A Historical Analysis of The Flows of Patient information. BioSocieties, 18(2), 282-307.*

Williamson, S. M., Prybutok, V. *(2024). Balancing Privacy and Progress: A Review of Privacy Challenges, Systemic Oversight and Patient Perceptions in AI-Driven Healthcare. Applied Sciences, 14(2), 675.*

Wiljer, D., Urowitz, S., Apatu, E., DeLenardo, C., Eysenbach, G., Harth, T., Pai, H., Leonard, K. *(2008) Patient Accessible Electronic Health Records: Exploring Recommendations For Successful Implementation Strategies. Journal of Medical Internet Research, 10(4): e34. doi:10.2196/jmir.1061*

Vinsensia, D., Amri, S., Sihotang, J., Sihotang, H.T. *(2024). New Method for Identification and Response to Infectious Disease Patterns Based on Comprehensive Health Service Data. MATRIK: Jurnal Manajemen, Teknik Informatika dan Rekayasa Komputer, 23(3):583-592. https://doi.org/10.30812/matrik.v23i3.4000*