JOURNAL OF ACADEMIC PERSPECTIVE ON SOCIAL STUDIES (JAPSS)

SOSYAL ÇALIŞMALAR ÜZERİNE AKADEMİK PERSPEKTİF DERGİSİ

E-ISSN: 2667-5889	https://dergipark.org.tr/tr/pub/japss	**Paper Type:** Review Paper, **Makale Türü:** Derleme
Sayı:1, Nisan 2021	**Issue:**1, April 2021	**Received Date / Geliş Tarihi:** 27/08/2020 **Accepted Date / Kabul Tarihi**:10/09/2020

MAHREMİYET KAPSAMINDA KİŞİSEL SAĞLIK VERİLERİNİN KORUNMASI VE DEPOLANMASI

♦♦♦

PROTECTION AND STORAGE OF PERSONAL HEALTH DATA IN THE SCOPE OF PRIVACY

Atıf/ to Cite (APA): Atalay, H. (2021). Mahremiyet Kapsamında Kişisel Sağlık Verilerinin Korunması ve Depolanması. Journal of Academic Perspective on Social Studies, (1), 01-20.

Havva Nur ATALAY[1]

DOI: https://doi.org/10.35344/japss.786353

ÖZ

Kişiye özgü, kişisel bilgiler şeklinde tanımlanan kişisel veriler, ilerleyen teknolojiler doğrultusunda siber saldırıların bulunması ve kötü niyetli bireylerin/şirketlerin rekabet avantajı sağlamak amacıyla bu verileri elde etmeye çalışması sebebiyle mahremiyetinin sağlanması ve korunması noktasında günümüzde gittikçe daha da önemli hale gelmiştir. Mahremiyet kavramı sağlık alanında yalnızca bedensel mahremiyet olarak hasta mahremiyeti şeklinde değil bilgi mahremiyeti veya bilişsel mahremiyet olarak da ele alınmaktadır. Kişisel verilerin korunması ve depolanması konusunda da bilgi mahremiyetinin sağlanması oldukça önem arz etmektedir. Kişisel sağlık verileri bireyin hastane kapısından girdiği andan çıktığı ana kadar paylaştığı bilgiler ve hekim tarafından yapılan tahlil, tetkik sonuçlarını da kapsayan bilgiler bütünüdür. 6698 Sayılı Kişisel Verileri Koruma Kanunu'nda özel nitelikli kişisel veriler olarak yer alan kişisel sağlık verilerinin korunması ve depolanması da ayrıca hassasiyet gerekmektedir. Bu doğrultuda Tıbbi Arşiv Yönetmeliği ve dijital veri koruma standartları göz önünde bulundurulmaktadır. Ulusal ve uluslararası birçok sözleşmede kişisel verilerin korunması hususu dikkatle ele alınmıştır. 108 Sayılı sözleşme ile başlayan ve 2016-2019 yıllarında yayımlanan yönetmeliklerle ulusal alanda gündeme gelen kişisel verilerin korunmasının hukuken işleyiş açısından sekteye uğramadığı görülmektedir. Fakat uygulama açısından henüz yeterli önem verilmediği için mahremiyet ihlalleri mevcuttur. E-nabız, Minimum Veri Modeli gibi yöntemlerle kişisel sağlık verileri kriptolu şekilde korunarak mahremiyet ihlali en aza indirilmeye çalışılmaktadır. Literatüre bakıldığı zaman kişisel verilerin korunması noktasında birçok hukuki bakış açısı kazandırılmıştır fakat kişisel verileri sağlık alanında inceleyen ve mahremiyet boyutuyla ele alan çalışma sayısı oldukça azdır. Literatürdeki bu açığa karşılık çalışmanın amacı kişisel sağlık verilerinin korunması ve depolanması konusunu mahremiyet bakış açısıyla değerlendirmektir.

Anahtar Kelimeler: Mahremiyet, Kişisel Veri, Kişisel Sağlık Verisi

ABSTRACT

Personal data, which is defined as personal, personal information, has become more and more important today in terms of ensuring and protecting its privacy due to the presence of cyber attacks in line with advancing technologies and malicious individuals / companies trying to obtain this data in order to gain competitive advantage. In the field of health, the concept of privacy is considered not only as physical privacy but also as patient privacy, but also as information privacy or cognitive privacy. It is very important to ensure information privacy in the protection and storage of personal data. Personal health data is generally a set of information that an individual shares from the moment he enters the hospital door to the moment he leaves, and includes the results of the analysis and examination. Protection and storage of personal health data, which is included as special personal data in the Personal Data Protection Law No. 6698, also requires sensitivity. Accordingly, the Medical Archive Regulation and digital data protection

[1] Yüksek Lisans Öğrencisi, Selçuk Üniversitesi Sağlık Bilimleri Fakültesi, Sağlık Yönetimi Bölümü, nur.atlyy@gmail.com, ORCID ID: https://orcid.org/0000-0002-2805-1921

standards are taken into consideration. The protection of personal data has been carefully considered in many national and international conventions. It is seen that the protection of personal data, which came to the agenda in the national field with the regulations that started with the contract number 108 and published in 2016-2019, is not interrupted in terms of legal functioning. However, there are privacy violations due to the lack of sufficient attention in terms of implementation. With methods such as E-pulse, Minimum Data Model, personal health data are protected in an encrypted manner and privacy violations are tried to be minimized. When we look at the literature, many legal perspectives have been gained regarding the protection of personal data, but the number of studies examining personal data in the field of health and dealing with privacy is very few. Despite this gap in the literature, the aim of the study is to evaluate the protection and storage of personal health data from a privacy perspective.

Keywords: Privacy, Personal Data, Personal Health Data

1.GİRİŞ

Ulusal ve uluslararası düzenlemelerde sağlık alanında mahremiyetin sağlanması hakkının sıklıkla yer aldığı görülmektedir. Mahremiyet kavramı, yasaklı olan ve yapılması konusunda bir sorumluluk bulunduran anlamına gelen Arapça 'da kullanılan haram (yasaklanmış) kelimesinden gelen bir sözcük olmakta ve bir kişiye ait diğer kişilere mahrem olan gizli tutulması gereken bilgileri içermektedir (Şen,2015). Sağlık hizmetlerinde mahremiyet sadece hizmet alındığı an ile sınırlı olmayıp bu süreçteki kişiye ait tüm sağlık verilerini de kapsamaktadır.

Kişisel veri kavramı, kişinin tüm yaşamıyla bağlantılı her türlü özel ya da kamusal bilgiyi içerir(Altundiş,2016). Kişisel sağlık verileri, kişiyi direkt olarak tanımlayan mental ve fiziksel sağlığına ilişkin bütün veriler olarak tanımlanmaktadır (Avaner,2018). Hasta mahremiyeti, hastaya ait bütün bilgilerin gizli olma durumunu ifade etmektedir(Arslan ve Demir,2016). Dolayısıyla kişisel sağlık verilerinin korunması ve depolanması konusunda mahremiyeti sağlamada hem bireyin kendisine hem de bu verileri elinde bulunduran kişi, kurum ve kuruluşlara büyük görev düşmektedir. Kişisel veriler bireylerin mahrem alanını kapsadığından kişisel verilerin ihlali mahremiyet ihlali olarak görülmekte ve böyle bir durum; bireylerin hem kurum kuruluşlara hem de devlete olan güvenini ciddi bir şekilde sarsmakta ve toplumu politik, ekonomik ve sosyal yönden etkilemektedir.

Hastane sayıları ve başvuran hasta sayıları göz önüne alındığında ciddi şekilde kişisel veri havuzu oluşmaktadır. Sağlık kurum ve kuruluşlarında hasta mahremiyetinin korunması ve sağlık verilerinin güvenliğinin sağlanması için, sağlıklı bir dokümantasyon altyapısının oluşturulması gerekir. Fakat bu alt yapıyı oluşturmak da sağlık kurumlarının sorumluluğundadır. Gittikçe artan teknoloji kullanımı doğrultusunda bu alt yapı yalnızca fiziki arşiv ile sınırlı kalmayıp, kişisel verilerin işlendiği ve depolandığı e-nabız, bulut bilişim, hastane bilgi yönetim sistemleri(HBYS) gibi dijital ortamları da kapsamaktadır. Bu sebeple hastane yöneticileri tarafından uyulması zorunlu dijital veri koruma standartları mutlaka göz önünde bulundurulmalıdır (Özkan,2018).

Bu çalışmada kişisel sağlık verilerinin korunması ve depolanmasına ait bir literatür araştırması yapılması ve mahremiyet boyutuyla değerlendirilmesi amaçlanmıştır. Bu bağlamda ilk bölümde mahremiyet ve hasta mahremiyeti kavramları tanımlanacak, ikinci bölümde sağlık işletmelerinde kişisel sağlık verilerinin korunması ve depolanması konusu ele alınacak ve üçüncü bölümde literatürden örnekler verilerek kişisel sağlık verilerinin korunması ve depolanmasına mahremiyet boyutuyla eleştirel bir bakış açısı geliştirilecektir.

2. MAHREMİYET

Mahremiyet kavramının çoğu birey için farklı anlam taşıması yani çok anlamlılığı ve özel yaşam sınırları dâhilinde bulunan konuların zamandan zamana, bireyden bireye veya kültürden kültüre farklılık göstermesi, kavramın açıklanmasını ve sınırlarının çizilmesini zorlaştırmaktadır(Korkmaz,2013; Yüksel,2009). Köken olarak incelendiği zaman mahremiyet kavramını tanımlamak daha kolay hale gelmektedir. Mahremiyet kavramı, yasaklı olan ve yapılması durumunda sorumluluk oluşturan eylemler anlamını taşıyan Arapça bir kavram olan haram kelimesinden türetilmiş olup; bir bireye özgü, özel, diğer kişilere karşı gizli tutulması gereken bilgiler bütününü kapsamaktadır(Şen,2015). Bireyin kişilik hakları, diğer kişilerle iletişim özgürlüğü ve aynı zamanda özel hayata saygı kavramlarıyla ilişki içinde olan mahremiyeti, gizlilik, dokunulmazlık, sır alanı vb. gibi kişinin kendisine ait olan ve onamı alınmadan kendisi dışında kimse ile paylaşılmayan her şeyi kapsayan bir kavram olarak tanımlamak mümkündür(Arslan ve Demir,2017; Korkmaz,2013). Bir anlamda mahremiyetin bu yönü bireyin dokunulmazlığı şeklinde isimlendirilebilir(Diler,2014). Dolayısıyla mahremiyet, özgürlük, demokrasi, psikolojik refah, bireysellik ve yaratıcılık için gerekli olan temel bir haktır(Solove,2008).

Mahremiyet, bireyin diğer insanlar tarafından ne kadar tanındığı ve bilindiği, başkalarının fiziki şekilde bireye ne kadar ulaşabilir olduğu aynı zamanda bireyin diğer insanların ilgi ve dikkatinin ne kadar odağında olduğu konularıyla yakından ilişkili bir kavram olarak ele alınır(Yüksel,2009). Bu noktada mahremiyet kavramı özel hayatın gizliliği olarak tanımlanmaktadır. Temel olarak bireyin hayatının diğer kişiler tarafından öğrenilmesini ve ulaşılmasını istemediği, başkalarından gizlediği kısmı özel hayat olarak ele alınmaktadır(Can,2020). Avrupa İnsan Hakları Sözleşmesi(AİHS)'nin 8. maddesinde, kişinin yalnızca kendine ait bu hayatını, özel hayatı, ailesi ile olan hayatı ve haberleşme özgürlüğü şeklinde ifade etmiştir. Anayasa'da bireylerin özel hayatı ile aile hayatının korunması ve kendi özel hayatına saygı duyulması hakkına sahip olduğu ayrıca bu söz konusu özel hayatın gizliliğine dokunulmaması gerektiği yer almaktadır(Hafızoğulları ve Özen,2009). Fakat yaşamın veya yaşama ilişkin bir veri bütününün her zaman gizlemek için ötekinden saklanmadığı, ötekinin istenmeyen yaklaşımlarından korunmak için de paylaşılmadığı dikkate alınırsa gizliliğin yalnızca mahremiyetin sağlanabilmesinin aracı olduğu açıkça fark edilmektedir(İzgi,2014).

2.1. Hasta Mahremiyeti

Hasta Hakları Yönetmeliği(HHY)'ne göre mahremiyet; hastaneye başvuran bireyin mevcut sağlık görünümü ile ilgili olan tüm tıbbi müdahaleler, süreçler ve değerlendirmelerin tamamen gizlilik esaslı devam ettirilmesi, tedavi aşamasında bir sorun teşkil etmediği sürece yakının refakat etmesine izin verilmesi, direkt olarak ilgisi olmayan bireylerin ise tedavi ortamında olmaması olarak tanımlanmaktadır(Candan ve Bilgili,2018).

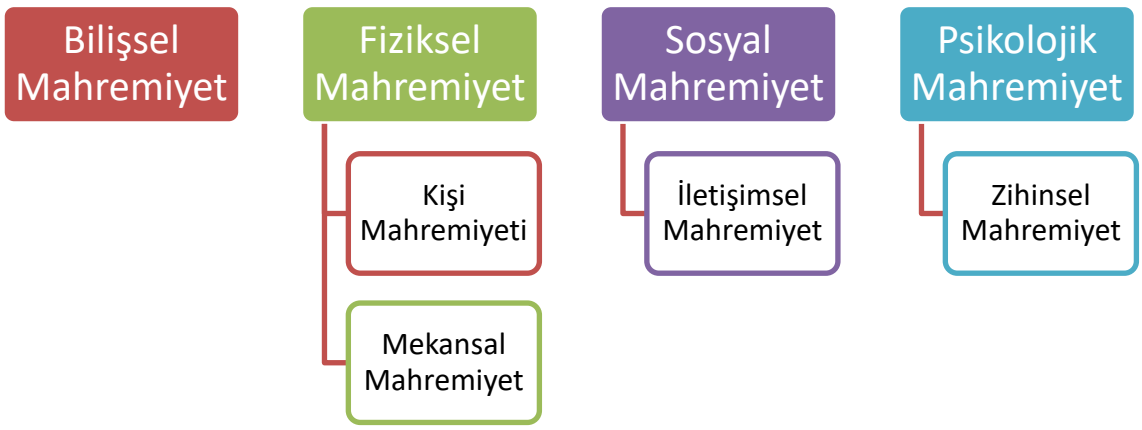
Sağlık çalışanları hastaların mahremiyetini en üst düzeyde korumakla sorumludur (Şenyürek,2017). Hipokrat Yemini'nin 17.maddesinde mahremiyet ile ilgili hastanın tedavi sırasında işitilen bilgilerin diğer kişiler tasavvurunda konuşulmaması gerektiği konusuna değinilmiştir(Altuner,2015). Bununla birlikte Hasta Hakları Yönetmeliğinin 21.maddesi mahremiyet ile ilgilidir ve ilgili maddede *"Hastanın, mahremiyetine saygı gösterilmesi esastır. Hasta mahremiyetinin korunmasını açıkça talep de edebilir. Her türlü tıbbi müdahale, hastanın mahremiyetine saygı gösterilmek suretiyle icra edilir*…" ifadeleri yer almaktadır(Dülger,2015).

Hastanın tedavi görmesi, yaşam hakkına bağlı olan sağlık hakkının bir gereğidir. Bu tedavideki mahremiyet, bireyin bedeninde uygulanan tedavi girişimleri ve bunların özel bilgilerini oluşturur(Şen,2015). Bireyin bakım ve tedavi için veya başka sebeple paylaşmak mecburiyetinde olduğu, fakat toplumdaki diğer bireylerden saklamak istediği bireysel yaşamı gibi özel alanlar hasta mahremiyeti konusu içinde değerlendirilebilir(Özer,2015). Kişi bir sağlık sorunu yaşadığı zaman, sağlık hizmetlerine erişim, tanı ve tedavi süreci esnasında kendisi ile ilgili verileri sağlık hizmet sunucularına güvenerek verir ve bu paylaşım esnasında bilgilerin gizli tutulacağına inanır(Şenyürek,2017). Gizlilik, hekim-hasta ilişkisi gibi belirli ilişkilerin karakteristik bir bilgi mahremiyeti biçimidir. Bu ilişki esnasında elde edilen kişisel bilgiler, hasta bilgilerin paylaşımı durumundan haberdar olmadıkça başkalarına ifşa edilmemelidir(Than Win,2005).

2.2.Mahremiyetin Boyutları

Mahremiyet kavramını 1890 yılında Amerikalı Yargıç Brandeis *"yalnız bırakılma hakkı; hakların en kapsamlısı ve özgür insanlar tarafından en çok değer verileni"* şeklinde tanımlamıştır. Zamanla mahremiyet kavramının bedensel-fiziksel mahremiyet, zihinsel-iletişimsel mahremiyet ve bilgi mahremiyeti şeklinde farklı boyutları oluşmaya başlamıştır(Dülger,2015). Sağlık alanında da mahremiyet; fiziksel, sosyal, psikolojik ve bilgi boyutlarıyla ele alınabilmektedir(Bekmezci ve Özkan,2015). Clarke(2009) tarafından yapılan sınıflandırmaya göre ise mahremiyetin kişisel, kişisel iletişim, kişisel bilgi ve kişisel davranış mahremiyeti şeklinde 4 boyutu bulunmaktadır. Mahremiyet kavramı ve boyutları Sağlıkta Kalite Standartları(SKS)'nda ayrıntılı bir şekilde tanımlanmaktadır. SKS'ye göre mahremiyet bilişsel, fiziksel, sosyal ve psikolojik mahremiyet olarak 4 boyutta ele alınmaktadır.

Görüldüğü üzere literatürde mahremiyet kavramı üzerine yapılan çalışmalarda mahremiyetin ana ve alt boyutları ile ilgili farklı sınıflandırmalar bulunmaktadır. Bu sınıflandırmaların bir bileşimi şekil 2.1'de gösterilmiştir(Akten,2017; Bekmezci ve Özkan,2015; Avaner,2018; Varol,2018).



Şekil 2.1: Mahremiyetin Ana ve Alt Boyutları
(Kaynak: SKS,2020; Akten,2017; Bekmezci ve Özkan,2015; Avaner,2018; Varol,2018'dan esinlenerek geliştirilmiştir.)

Bilişsel mahremiyet ile son zamanlarda devletlerin kişisel verileri ve kişisel sağlık verilerini işlediği elektronik ve internet gibi sanal ortamlarda mevcut olan verilerin mahremiyeti ele

alınır(Akar ve ark, 2019). Bilgi mahremiyeti veya bilişsel mahremiyet, hastaya ait olan bilgi mahiyetindeki dokümanların yetkisiz kişiler tarafından ulaşılmasının engellenmesi şeklinde de tanımlanabilmektedir(Şen,2015). Bilgi mahremiyeti kişisel verilerin işlenme, toplanma, depolanma ve iletiminin yapılma süreçlerinin kontrol edilmesini gerektirir (Korkmaz,2013). Tıbbi müdahale sırasında hangi sağlık personellerinin bulunacağı beden mahremiyetinde önem taşıyan bir konudur. Hasta Hakları Yönetmeliği(HHY)'nin mahremiyete saygı hakkını ele aldığı md.21/d' ye göre; *"Tedavisi ile doğrudan ilgili olmayan kimselerin, tıbbi müdahale sırasında bulunmamasını"* ifadesiyle beden mahremiyeti hususu açıkça belirtilmiştir(Kandilli, 2019). Mekânsal mahremiyet literatürde çoğu çalışmada bedensel-fiziksel mahremiyet ile birlikte kullanılmaktadır. Mekân mahremiyeti bireyin kendine özel olan olayları yaşadığı herhangi bir ortamın bireye özel olmasını gerektirir. İçinde yaşanılan olaylar kadar, bu olayların yaşandığı mekân da önemli ve kişiye özeldir(İpek, 2020). Mekânsal mahremiyete hastanede her odanın kapısı olması ve poliklinik odalarındaki paravanlar örnek olarak düşünülebilir(Avaner, 2018). Bireyin beden mahremiyeti hakkının sonucu olarak; bireyin izninin bulunmadığı tıbbi ve medikal işlemlere tabi tutulmaması, gerekli bilgilendirmeler yapıldıktan sonra onam alınan ve bireyin talep ettiği işlemlere(bir sakınca bulunmadığı sürece) başlanması örnek verilebilir(Bekmezci ve Özkan, 2015). Psikolojik mahremiyet ise bilişsel ve bireyin duygusu ile ilgili aşamaların kontrol edilmesi, değerlere yön verilmesi ve birey olarak varlığını(kimliğini) sürdürmesi şeklinde tanımlanabilmektedir. Ayrıca bireyin oluşacak her bir durum ile ilgili kendi kararlarını vermesi şeklinde de ifade edilmektedir(Öztürk ve ark, 2014). Psikolojik mahremiyet türü sağlık hizmetlerinde en az mahremiyetin diğer boyutları kadar önemlidir. Herhangi bir sağlık kuruluşunda tedavi görmekte olan hastanın psikolojik mahremiyet hakkının ihlal edilmesi sonucu kişide diğer mahremiyet türleri kadar kolay ve kısa süreli ortaya çıkmamasına rağmen daha büyük izler taşıyan problemler oluşturmaktadır(Akten,2017).

3. KİŞİSEL SAĞLIK VERİLERİNİN KORUNMASI VE DEPOLANMASI

3.1.Kişisel Veri

Kişisel kavramı Türk Dil Kurumu (TDK)'na göre "kişiye ilişkin, kişi ile ilgili" şeklinde; veri kavramı ise "data, bilgi" şeklinde tanımlanmaktadır. Veri kavramı; gözlemlerin, oluşumların veya çeşitli durumların her türlü gösterimidir(Kılınç,2012). Kişisel veriden bahsedebilmek için, gerçek bir kişiye ait olan bir veri olmalı ve bu gerçek kişinin de bu veri ile nitelenebilir ve tanımlanabilir olması gerekmektedir(Kişisel verileri Koruma Kurumu,2018). Bir bilgiyi kişisel veri şeklinde tanımlayabilmek için, verinin, bireyin özel hayatına, iş hayatına veya kamuya açık hayatına yönelik olup olmaması arasında bir ayrım yoktur. Verinin türüne ilişkin yapılacak isimlendirme önem teşkil eden bir konu değildir. Bununla ilişkili olarak bilginin, gizli bir bilgi olması mecburi olmamakla birlikte bireyin kamusal hayatına ait, kendi tarafından paylaşılan açık bir bilgi de kişisel bir veridir(Kandilli,2019).

Bayındır(2019)'a göre kişisel veri; bireyin hem şahsi hem ailevi niteliklerini belirten, bireyi toplumdaki diğer kişilerden ayırıp özelliklerini tanımlamayı sağlayan her türlü bilgidir. Bu bağlamda, kişisel verileri kişisel nitelikte olmayan diğer verilerden ayırmak için esas olarak iki kriterin kullanıldığı söylenebilir. Buna göre, edinilen herhangi bir bilginin kişisel veri şeklinde tanımlanması için mevcut verinin bir bireyle ilişkilendirilmesi birinci kriter, o bireyin direkt olarak tanımlanması veya tanımlanabilir olması ise ikinci kriter olarak ele alınmaktadır. İsim, fotoğraf, Whatsapp, Facebook, Twitter, İnstagram gibi sosyal medya iletileri, parmak izi, e-posta adresi, biyometrik ve tıbbi bilgiler bu kapsama girmektedir(Altundiş,2016). Sağlık hukukunda

kişisel veriler, paylaşım noktasında belirli kişilerin bulunduğu yalnızca seçilen kişilerle paylaşıldığı, paylaşılmaması gereken durumlarda hastanın makul bir nedeninin ve bu doğrultuda korunmaya değer bir faydanın olduğu bütün veri türleridir. 6698 sayılı Kişisel Verilerin Korunması Kanunu'nda kişisel veri kavramı *"Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi"* olarak tanımlanmıştır. (Dülger,2015).

3.2.Kişisel Sağlık Verisi

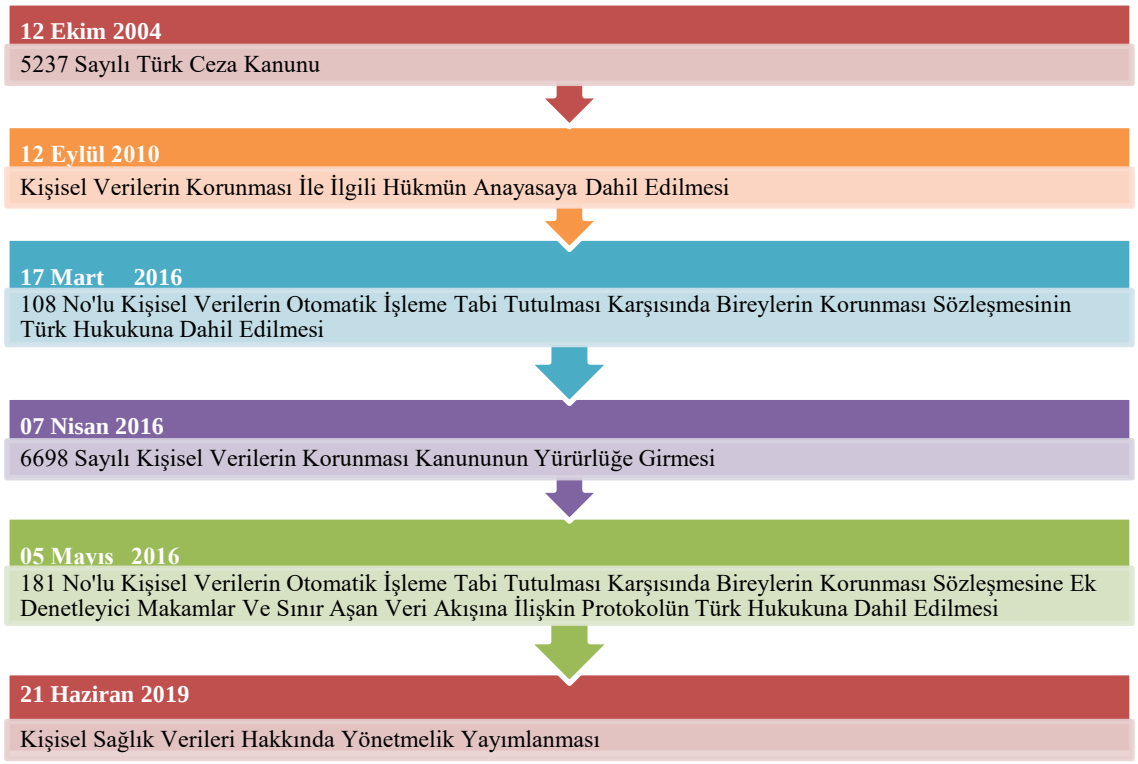
Kişisel sağlık verileri Kişisel Verilerin Korunması Kanunu'nda özel nitelikli kişisel veriler olarak ele alınmıştır. İlgili Kanunun'un md.6/1'de özel nitelikli kişisel veriler "*kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri*" şeklinde belirtilmiştir(Bayındır,2019).

Kişisel sağlık verileri en net tanımıyla Kişisel Sağlık Verileri Hakkında Yönetmelik md.4/1'de yer almıştır. Kişisel sağlık verisi söz konusu Yönetmelik'te, kişisel sağlık verilerinin fiziksel ve ruhsal sağlıkla ilgili veriler, alınan sağlık hizmetleriyle ilgili oluşturulan bilgiler bütünü şeklinde ele alınmıştır. Bu doğrultuda aslında bireyin sağlık durumuyla alakalı açık ve yakın ilişkiye sahip olan bütün veriler, kişisel sağlık verisi olarak kabul edilmelidir(İmançlı,2019). Örneğin; kişinin geçirdiği hastalıklar, yapılan tahlil sonuçları, bireyin kullandığı ilaçlar gibi veriler kişisel sağlık verilerini oluşturmaktadır(Kişisel verileri Koruma Kurumu,2018).

Dünya Tabipler Birliği(DTB) kişisel sağlık verisini "Sağlık Veri Tabanları ile İlgili Etik Düşünceler Bildirgesi"nde, kişinin kimliğini oluşturan mental ve fiziksel sağlığı ile ilişkili olan kayıt altına alınan tüm bilgi şeklinde açıklamaktadır(Avaner,2018). Özetle; kişinin doğum anından başlayan ve ölüm ile sonuçlanan yaşamı boyunca tutulan ve sağlığı ile ilgili olan bütün verilere kişisel sağlık verileri denilmektedir(Olca ve Can,2014).

3.3. Kişisel Sağlık Verileri ile İlgili Türkiye'deki Düzenlemeler

Sağlık verisi ile ilgili ele geçirme, yanlış işleme, amaç dışı kullanım gibi olumsuz durumların varlığı nedeniyle ulusal bilgi güvenliği bakımından ciddi tehlike oluşturabilecek bu riskler için, uluslararası yönetmeliklerle ve kanunlarla uygulamaya geçirilen düzenlemeler göz önüne alınmalıdır(Olca ve Can,2014). Bu doğrultuda kişisel veriler ile ilgili yaptırıma sahip ilk düzenleme olan ve Avrupa Konseyi tarafından, hudut dışı veri akışı prensiplerinin belirlenmesi ve üyeliği bulunan bütün ülkelerde kişisel verilerin özdeş standartlarda korunması amacı ile düzenlenen 108 sayılı "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi", 1981 yılı Ocak ayında imzaya açılmış ve Türkiye tarafından da imzalanmıştır(Altundiş,2016; Hatipoğlu,2019). İlgili Sözleşme, 29656 sayılı ve 17 Mart 2016 tarihinde iç hukuka eklenmiştir(Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi,2018). Genel olarak bakılacak olursa kişisel verilerin korunması ile ilgili yapılan ulusal düzenlemeler Şekil 3.1'de yer almaktadır (Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi, 2018):



Şekil 3.1: Ulusal Düzenlemeler

Kaynak: Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi, 2018.

Türkiye Cumhuriyeti Devleti, kişisel verilerin korunmasına yönelik olarak kanun tasarısı hazırlığı ile 1989 yılında ilk çalışmasına başlamıştır. 2006 yılına kadar yapılan tasarı çalışmaları devam etmiş ve 2008'de Türkiye Büyük Millet Meclisi(TBMM)'ne gönderilmiş ancak yasalaşma aşamasına geçmeden geçersiz sayılmıştır. Kamu kurumlarının kullandığı bilgi iletişim teknolojileri doğrultusunda oluşabilecek mahremiyet ihlallerini konu edinen en kapsamlı yasalara bağlı düzenleme olarak bu tasarıyı söylemek mümkündür (Tataroğlu,2009). 2012 yılında tasarı başbakanlığa tekrar gönderilmiş ve 6698 sayılı Kişisel Verilerin Korunması Kanunu 7 Nisan 2016 tarihinde yayımlanmıştır(Çetin,2014; Dülger,2019).

6698 sayılı Kanun'un yayımlanmasından birkaç ay sonra 20 Ekim 2016'da "Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelik" yayımlanmıştır. Bu yönetmelik yayımlandığında 6698 sayılı Kanun'un yeni yasalaşmış olması, henüz fazla bilgi birikimi oluşturulmamış ve konuyla ilgili çalışma yapan yetkili bireylerin görüşleri alınmamış olması sebebiyle mevzuata uygun olarak düzenlenmediği esasıyla eleştirilere konu olmuştur(Dülger,2019). Açılan davalar sonucunda Danıştay kararı ile Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelik'in yürütmesi 6 Temmuz 2017 tarihinde durdurulmuştur(https://www.lexpera.com.tr/mevzuat/yonetmelikler/kisisel-saglik-verilerinin-islenmesi-ve-mahremiyetinin-saglanmasi-hakkinda-yonetmelik Erişim Tarihi:18.05.2020). 24 Kasım 2017 tarihinde yapılan eleştiriler ve eksiklikler göz önüne alınarak 30250 sayılı Resmi Gazete'de Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelikte Değişiklik Yapılmasına Dair Yönetmelik yayımlanmıştır(Dülger,2015). Yapılan değişiklikler önceki yönetmeliğe nazaran Kanun'a uygun olarak ve eleştiriler göz önüne alınarak yapılmış olsa da yürütmesi daha önceden durdurulmuş

olan yönetmelik üzerinde değişiklik yapılamayacağı ve yürütmesi durdurulmuş olan yönetmeliği tekrar yürürlüğe koyma amacı taşıdığı için hukuka aykırı olduğu ifade edilerek söz konusu Yönetmelik, Türk Diş Hekimleri Birliği ve Türk Tabipleri Birliği tarafından yargıya taşınmıştır(Dülger,2019; İmançlı,2019). 9 Ekim 2018 tarihinde söz konusu Yönetmelik hakkında yürütmenin durdurulması kararı alınmıştır. Son olarak 21 Haziran 2019 tarihinde 30808 sayılı Resmî Gazete'de Kişisel Sağlık Verileri Hakkında Yönetmelik yayımlanmış ve önceki Yönetmelik yürürlükten kaldırılmıştır(Dülger,2019).

4.MAHREMİYET AÇISINDAN KİŞİSEL SAĞLIK VERİLERİNİN KORUNMASI VE DEPOLANMASI

Hastanın durumunun kronolojik takibi, hastaya daha iyi bir sağlık hizmeti verebilme, hekimin yükümlülüğü ve sorumluğunun sınırlarını belirleme, işlemlerin hızlı ve pratik olması gibi yararlı sebepler tıbbi kayıtların gerekliliğini ortaya koymaktadır. Diğer yandan bu kadar çok verinin fiziki arşiv veya elektronik ortam gibi belli yerlerde kaydedilmesi, bireylerin verilerinin, güvenlik ve mahremiyet sorununu doğurmaktadır(Kandilli,2019). Bu çerçevede kişisel verilerin güvenli bir şekilde korunması ve depolanması zorunlu hale gelmiş ve bireylerin, özel hayatının gizliliğini sağlayabilmek için üçüncü kişilerin eline geçmesinde sakınca bulunan verilerinin hukuken korunmasını gerekli kılmıştır(Ağıralan,2015; Hatipoğlu,2019). Bu nedenle, kişisel verilerin korunma ve depolanma yöntemlerine ilişkin bir harita belirlenirken bilginin paylaşımı ve depolanması arasında, bilgiyi ileten kişi ve bu bilginin paylaşımı sonucunda toplumda oluşturacağı faydayı maksimum düzeyde tutacak bir dengeyi göz önüne almak gerekmektedir(Derinözlü,2017).

Sağlık hizmeti gibi güven değerinin esas olduğu alanlarda verilerin güvenliğinin sağlanması, hakkın elde edilebilmesi bakımından önemlidir. Uluslararası tüm belgelerde önemi dolayısıyla veri güvenliğinin sağlanmasına vurgu yapılmaktadır(İzgi,2014). Örneğin Amsterdam Bildirgesi'nin 4.maddesinde hastanın tüm tedavi süreçlerinde vermiş olduğu bilgilerin yalnızca yaşarken değil ölümden sonra bile korunması gerekliliği ve hastanın izni olmadan diğer kişilerle paylaşılmaması gerektiği ele alınmıştır(Dülger,2019). Kişisel verilerin korunması konusu; mahremiyet, özel hayatın gizliliği ve korunması kavramları ile doğrudan ilişki içerisindedir. Mahremiyet kavramının bir görünümü olan özel hayatın gizliliği, bir hak olarak görülmektedir. Özel yaşamın gizliliği, İnsan Hakları Evrensel Bildirgesi'nin 12.maddesinde ve Türkiye Cumhuriyeti Anayasası'nın 20.maddesinde korunmaya değer bir hak olarak yer almakta ve bu başlıkta ele alınan kişisel verilerin korunması konusu mahremiyetin sağlanması ile yakından ilişki içerisinde bulunmaktadır(Dülger,2015; Erdinç,2017).

Kişisel verilerin tanımının da içerdiği üzere bireyi direkt olarak tanımlayabilen veriler olması dolayısıyla bireyler bu bilgilerin korunmasını açıkça talep edebilir ayrıca mahremiyet ihlali sonucunda hukuksal süreçlere başvurabilmektedir. Son yıllarda bazı kişisel verilerin paylaşılmaması veya kişisel verilerin korunması konusunda hassasiyet düzeyi artmıştır. Günümüzde kişisel verilerin korunması veya verilerin üçüncü kişilerle paylaşılmaması konusunda hem mahkemeler hem idari kuruluşlar birçok talep almaya başlamıştır(Altundiş,2016). Yapılan herhangi bir kişisel veri ihlali sonucunda Kişisel Verileri Koruma Kanunu'nda yer alan koruma mekanizması idari ve cezai yaptırım, tazminat şeklindedir. Tazminat hakkı ilgili yasanın md.11/ğ ve 14/3' te belirtilmiştir. İdari yaptırım cezası kanunun 18. maddesi Kabahatler başlığında düzenlenmiştir. Cezai yaptırım ise 17. maddesinde, Türk Ceza Kanunu(TCK)'nun ilgili maddelerine atıfla hüküm altına alınmıştır(Kandilli,2019).

Avrupa Birliği(AB) Tüzüğü'nün 23.maddesinde veri sorumlusu kavramı tanımlanmış ve bu tanıma göre veri sorumlusu; kişisel verilerin korunmasına ilişkin belirlenen ilkelerin uygulanabilmesi için gereken, organizasyonel ve teknik tedbirleri almak mecburiyetinde olan kişidir(Çekin,2016). Veri sorumlusu kavramı Kişisel Sağlık Verileri Hakkında Yönetmelik(2019)'te, mevcut kişisel verilerin işlenmesi ve verileri kaydetmek için bir sistem oluşturup bu sistemin yönetilmesinden sorumlu kişi olarak tanımlanmaktadır. Ayrıca veri sorumlusu, sağlık verilerini işleme operasyonunun "nasıl" ve "neden" yapılması gerektiğini açıklayan kişidir(Kişisel Verileri Koruma Kurumu,2018). Sorumlu, kayıtlı verilerin bir araştırmada kullanılması gerektiği zaman verilerin anonimleştirilmiş bir sürümünü, veri analistleri için yararlı olan ve veri tabanındaki bireylerin gizliliğini koruyan bir sürümünü yayınlamalıdır(Dankar,2012). Anonimleştirme süreçleri, özel alan gizliliğinin ve kişisel verilerin korunması konusunda, mevzuatlar gözetiminde güvenilir süreçlerden biri olarak nitelendirilmekte ve hem kamu hem de özel sektör kuruluşları bu süreçlerle veri paylaşımına teşvik edilmektedir(Gözüküçük,2014). Anonimleştirme aşamasında veri sorumlusu ilk olarak, isim, soy isim ve sosyal güvenlik numaraları gibi kişisel tanımlayıcıları silmekte, ikinci olarak ise belirli bir bağlamda tanımlayıcılar gibi görünen dolaylı yoldan kişiyi tanımlayabilen diğer bilgi kategorilerini değiştirmektedir. Anonimleşen verileri analistler bu haliyle de yararlı bulmaktadır. Aynı zamanda kötü niyetli pazarlamacıların ve kimlik hırsızlarının, veriler doğrultusunda gözetlenen bireylerin bilgilerini tanımlaması imkânsız hale gelmektedir. Dolayısıyla anonimleştirme bu aşamalar sayesinde gizliliği sağlamaktadır(Ohm,2009).

Kişisel verilerin çoğu günümüzde teknolojik araçlarla otomatik olarak işlenmektedir. Hatta fiziki arşivlerde bulunan ve otomatik olmayan yollarla işlenmiş veriler otomatik ortamlara aktarılmaktadır. Dolayısıyla, "tamamen veya kısmen otomatik yollarla işlenen" ve "veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen" veriler 6698 sayılı Kanun kapsamında korunmaktadır(Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi,2018). Elektronik sistemlerin sağlık hizmetlerinde kullanılması ile birlikte sağlık verilerinin korunması günden güne daha önemli hale gelmiştir. Bu doğrultuda 6 Temmuz 2019 tarihinde *verilerin güvenliği ve risklerin azaltılması amacıyla* 2019/12 Sayılı Bilgi Güvenliği Tedbirleri Cumhurbaşkanlığı Genelgesi yayımlanmıştır(T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi,2019).

Kişisel sağlık verilerinin korunma ve depolanma zorunluluğu yalnızca kamu ve üniversite hastaneleri için geçerli olmayıp özel hastaneleri de kapsamaktadır. Bu doğrultuda Özel Hastaneler Yönetmeliği md.49/4'te özel hastanelerin 6698 sayılı Kanun'a göre işlediği ve kayıt altına aldığı verileri Bakanlığın belirlediği standartlara göre veri sistemine göndermesi zorunluluğu ele alınmıştır. Kısacası bu hüküm ile özel hastanelerin Sağlık Bakanlığına veri gönderme zorunluluğu ve sağlık verilerinin 6689 sayılı Kanuna uygun olarak işlenmesi gerektiği vurgulanmıştır(Yüksel,2019). Ayrıca bireylerin ve sağlık hizmet sunucularının kişisel sağlık kayıtlarına ulaşımı Sağlık Bakanlığı tarafından belirlenen ilke ve esaslara göre düzenlenmekte ve erişim geçmişi kayıt altına alınmaktadır(Nalbantoğlu,2018). Bu sayede ulaşan bireylerin kullandıkları amaç ve veri seti denetlenebilmekte herhangi bir bilgi sızıntısında sorumlu kişiler tespit edilebilmektedir. Özel sağlık kurumları tarafından SGK(Sosyal Güvenlik Kurumu)'ya Medula aracılığıyla kişisel sağlık verilerinin gönderilmesinde yurt içindeki üçüncü kişiye gönderme söz konusudur. KVKK md.8/b.1 uyarınca ilgili kişinin açık rızası bulunuyorsa, özel sağlık kurumları tarafından SGK'ya Medula aracılığıyla kişisel sağlık verilerinin

gönderilebileceği gibi KVKK md.8/b.2-b veya md.8/b.3 uyarınca da açık rıza aranmaksızın da aktarma gerçekleştirilebilir(Bayındır,2019).

4.1. Elektronik Sağlık Kayıtları ve E-Nabız

Tıbbi kayıtlar gerek sanal olarak elektronik ortamda, gerek fiziki olarak arşivde saklanmaktadırlar(Bezirgan Gözmener, 2019). Elektronik sağlık kaydı, ilgili verilere sadece konu ile ilgili yetkili kişilerin erişimine izin verdiği için kişisel sağlık verilerinin mahremiyetinin ve güvenliğinin sağlanması noktasında önem arz etmektedir(Altundiş,2016). Günümüzde elektronik sağlık kaydı denildiğinde akla ilk olarak sağlık bilgi sistemleri(yardımcı olarak medula, sağlık-net, e-reçete) ve e-nabız sistemi gelmektedir. Sağlık bilgi sistemleri, verileri işleyen ve sağlık ortamlarında bilgi ve bilgi akışını sağlayan, yönetimsel açıdan karar vericilerin ihtiyaçlarını karşılayan ve her sistem gibi birbiriyle ilişkili parçalardan oluşan bir sistem olarak tanımlanmaktadır(Sur ve Palteki, 2013; Almunawar ve Anshari, 2012).

Kişilerin geçmişten günümüze ve günümüzden geleceğe tüm sağlık verilerinin ve hastalık öykülerinin bilgi teknolojileri kullanılarak işlenmesi, kaydedilmesi ve sınıflandırılması sonucunda oluşturulan tüm veriler Elektronik Sağlık Kaydı(ESK) olarak adlandırılmaktadır(Karakethüdaoğlu, 2019). ESK, kişilere ait sağlık veya hastalık öyküsünün tanı, tedavi ve bakım sonuçlarını içeren belgelerin kayıt altına alındığı bir sistemdir(Ay,2008). Bu sistem sayesinde herhangi bir araştırma ve denetim durumunda depolanan kayıtları geri çağırmak mümkündür(Sağlık Bakanlığı Dijital Hastane, 2020).

Kişisel sağlık kayıtlarının elektronik ortamlarda tutulması kapsamında günümüzde, Google Health ve Microsoft HealthVault gibi sistemler geliştirilmiş ve bu alanlara ciddi yatırımlar yapılmıştır(İnal ve Ercil Cagiltay, 2019). Gökay ve Ark(2015) "Kişisel Sağlık Kaydı Sistemleri Kullanılabilirlik Durum Çalışması" isimli araştırmada Microsoft HealthVault sisteminin ülkemizde uygulanabilirliğini araştırmışlardır. Çalışmaya 40 yaşın üzerinde 13 kişi katılmıştır ve bu kişilere belirli görevler verilmiştir. Çalışmanın sonucunda bireylerin çoğunun(%88 üzeri) görevleri başarı ile yerine getirdiği fakat memnuniyet düzeylerinin yeteri kadar yüksek olmadığı tespit edilmiştir. Memnuniyetsizlik sebepleri ise sistemin kullanım açısından karmaşık olması olarak belirtilmiştir. Bu çalışmadan da yola çıkarak elektronik sağlık kayıt sistemlerinin; bireylerin teknolojiyi kullanma ve algılama düzeyleri göz önüne alınarak geliştirilmesi gerektiği sonucuna varılmaktadır. Ülkemizde bu tip bir uygulama olan kişisel sağlık kaydı olarak e-nabız sistemi kullanılmaktadır.

E-nabız, sağlık kurumlarında işlenen ve elde edilen sağlık verilerine hem bireylerin hem sağlık profesyonellerinin internet ve mobil cihazlar üzerinden istenildiği anda ulaşabilecekleri bir uygulamadır (Demir,2017). Aynı zamanda e-Nabız uygulaması ile bireyler kullandıkları akıllı cihazlardan aldıkları şeker, tansiyon gibi ölçüm verileriyle adım sayısı ve nabız gibi verileri sağlık profillerine aktarabilmekte ve bu bilgileri karşılaştırmalı olarak görüntüleyebilmektedirler(İleri ve Uludağ, 2017).

Hekimlerin, sağlık hizmet sunucularının hastaya ait teşhis, tanı ve tedavi süreçlerinde kayıt altına alınan görüntüleme, tahlil, laboratuvar sonuçlarını girmesi ile e-nabızdaki kişisel veriler oluşmaktadır(E-Nabız Kılavuzu, 2018). Tüm bu tanı, teşhis ve tedavi sürecinde elde edilen bilgilerin tek bir ortamda depolanması bireylerin bilgilerinin güvende olup olmadığı sorusunu sormalarına sebep olmaktadır. E-nabız sisteminde bulunan kişisel sağlık bilgileri yalnızca, sistem sahibi kişinin "Paylaş" butonunu aktifleştirerek erişime izin verdiği kullanıcılar tarafından

görülmektedir (E-Nabız Kılavuzu, 2018). Paylaşım yetkisini veren kişilere ait sağlık öyküsüne kolaylıkla ulaşabilen sağlık hizmet sunucuları hastalardan kısa süreler içerisinde tekrardan tahlil, tıbbî görüntü veya tetkik istememektedir. Bu doğrultuda hem tetkik için bir kez daha vakit zayiatı yaşanması engellenmekte hem kişilerin iktisadi çıkarları korunmakta hem de radyasyona maruz kalma oranları azalmaktadır (Yeşiltaş,2018). Kişisel Sağlık Verileri Hakkında Yönetmeliğe göre ise bu uygulamada hesabı olan bireylerin gizlilik koşulları ile bilgilendirmeler yapıldığı ve kendi rızaları sonucu erişim izni verdikleri için oluşabilecek zararlardan Bakanlık sorumlu tutulmamaktadır (Ergüden,2019). Dolayısıyla birey paylaş yetkisini verdiği durumda oluşan kişisel verilerin mahremiyeti ihlali doğrultusunda Kanun yetkiyi veren bireyi sorumlu tutmaktadır.

4.2. Büyük Veri (Big Data) ve Bulut Bilişim

Sağlıktaki büyük veriler, sağlık hizmeti sağlayıcılarının mevcut araçları işlemesi ve yorumlaması için çok büyük, çok hızlı ve çok karmaşık anlamlı veri kümeleriyle ilgilidir(Andreu-Perez ve ark,2015).

Tablo 3.1: Yıllara Göre Toplam Hastane Sayısı

Yıllar	Türkiye Geneli	Sağlık Bakanlığı	Üniversite	Özel	Diğer
2014	1528	866	69	556	37
2015	1533	865	70	562	36
2016	1510	876	69	562	3
2017	1518	879	68	569	2
2018	1534	889	68	575	2

(Kaynak: Türkiye İstatistik Kurumu, 2020.)

Tablo 3.1'de 2014-2018 yılları arasında Türkiye'de mevcut hastane sayıları verilmiştir. 04/03/2020 tarihinde güncellenen Türkiye İstatistik Kurumu tarafından yayınlanan Hastane Sayılarının İllere Göre Dağılımı İstatistiği'ne göre Türkiye'de mevcut hastane sayısı 2018 yılında 2017 yılına göre 16 artış göstererek 1534 olmuştur. Sağlık Bakanlığı tarafından 2018'de yayımlanan Sağlık İstatistik Yıllığı'na göre ise bireylerin 2018 yılı içerisinde bu mevcut hastanelere ve hekime toplam müracaat sayısı 782.515.204'tür. Bu rakamların yalnızca başvuru sayısı olduğu ve yapılan tetkikler, tahliller, hastaneye yatan birey sayısı gibi verileri kapsamadığı da göz önüne alınırsa geniş hacimli kişisel sağlık verilerinden söz etmek mümkündür. Söz konusu bu kişisel sağlık verilerinin tek bir sistem altında toplanması büyük veri kavramını oluşturmaktadır.

Büyük veri, tanımı itibariyle yalnızca *"diskte çok fazla yer kaplayan veri"* olarak değil, aynı zamanda geleneksel araçlar ve yöntemlerle işlenemeyen veri olarak da ele alınmaktadır(Karaca,2015). Yani büyük verilerin söz konusu olduğu durumda, hızlı veri birikimi için yüksek hacim, çeşitlilik ve potansiyelden ayrıca veri kalıplarının keşfi ve iletişimi olan analitikten bahsedilmektedir (Bates ve ark,2014). Büyük veri teknolojilerinin kullanımı sonucunda, farklı kaynaklardan gelen tek başına önemli olmayan veriler birleştirilip paylaşılmamış kişisel verilere erişilebilmektedir (Derinözlü,2017). Büyük veri teknolojileri devletler açısından kamu hizmetlerini geliştirmede, suç ile mücadelede ve terör faaliyetlerinin takibinde fayda sağlamaktadır (Derinözlü,2017).

Fiziki olarak depolanması ve korunması gün geçtikçe zorlaşan bu büyük verilerin iletişimi ve aktarımını kolaylaştırmak, depolanmasını sağlamak için sağlık alanında bulut bilişim teknolojileri kullanılmaya başlanmıştır. Bulut bilişim; sigorta şirketleri, hastaneler, tıbbi uygulamalar ve araştırma tesisleri için başlangıç maliyetleri düşük olan gelişmiş bilgi işlem kaynaklarına erişilmesini sağlar. Bunun yanı sıra bulut bilişim sistemleri, sağlıkta kullanılan bilgi sistemlerinin daha yenilikçi ve modern olması konusundaki engelleri de azaltmaktadır(Bayın ve ark, 2016). Sağlık Bakanlığı tarafından geliştirilen SBNet Sağlıkta Bilişim Ağı, bulut bilişim oluşturmak için en önemli adımdır. İnternet aracılığıyla paylaşılan bilgiler şifrelenmeden gönderildiği için siber saldırılara açıktır. Yeni gelişmeler ışığında sağlık şirketlerinde güvenli bilgi teknolojileri günümüzde çok daha fazla etkinlik kazanmıştır. (Marşap ve ark,2010). Bu doğrultuda Sağlık Bilişim ağı güvenli bilişim teknolojilerinin başında gelmektedir. Çünkü Sağlık Özel Ağı internete kapalı olarak faaliyet göstermekte ve oluşabilecek bilgi güvenliği tehditlerinin %81'i ile hiç karşılaşmamaktadır (Bağ S,2018).

4.3. VEM- SBYS Minimum Veri Modeli

Hastanelerde bilgi teknolojilerinin kullanılması sonucunda tartışmasız en önemli veri tabanı hastane bilgi yönetim sistemleri (HBYS) olmuştur. HBYS, klinik yönetimi, hasta bakımı, finansman, kurumsal performans ölçümü ve araştırmanın sorunsuz devam etmesi için gereklidir (Yılmaz ve Demirkan,2012). 4735 sayılı Kamu İhaleleri Sözleşmeleri Kanunu'na göre HBYS firmaları ve hastaneler arasında bir sözleşme imzalanmakta ve bu sözleşmenin süresi bittiğinde hastaneler farklı HBYS firması ile çalışmasını sürdürebilmektedir. Bu durumda hastanenin anlaştığı yeni HBYS firmasının bir önceki firmadan hastaneye ait kayıtlı tüm verileri alması gerekmektedir (Sağlık Bakanlığı Sağlık Bilgi Sistemleri Genel Müdürlüğü, 2015). Veri aktarımının en az sürede ve hatasız şekilde gerçekleştirilmesi, kayıtlı olan sağlık verilerinin arşiv sorumluluğu doğrultusunda güvenlik ve geçmiş kayıtlara istenildiğinde erişim açısından büyük önem taşımaktadır (Ülgü ve Arkadaşları,2018).

Veri aktarımı gerçekleştirilirken herhangi bir veri kaybının olmaması ve doğru şekilde aktarılması sağlık kayıtlarının güvenilirliği bakımından önem arz etmektedir. Fakat Sağlık Bilgi Yönetim Sistemleri'nin düzgün ve doğru şekilde tasarlanmış olmalarının bile bu veri aktarımı sürecinde sağlık kayıtlarında kayıpların oluşmasını engelleyemediği ve bu aktarım işleminin uzun zaman aldığı bilinmektedir (Sağlık Bakanlığı Sağlık Bilgi Sistemleri Genel Müdürlüğü, 2020). Bu kayıpların en aza indirilmesi hatta hiç olmaması amacıyla SBYS Minimum Veri Modeli (VEM) geliştirilmiştir. VEM, sağlık işletmelerinde işlenen, korunması ve depolanması gereken verilerden oluşmaktadır. Yayımlanan ilk sürümü sonrasında eksiklikler noktasında getirilen eleştirilere uygun olarak VEM (V:1.2) yayımlanmıştır (Ülgü ve Arkadaşları,2018). VEM modelinin en güncel ve şu an kullanılmakta olan sürümü 2.0'dır.

4.4. Örnekler ile Türkiye'de Kişisel Sağlık Verilerinin Korunması ve Depolanması

Yasaların büyük çoğunluğu mahremiyetle ilgili olsa da şimdiye kadar gizlilik sorunlarının çözümünde çok sayıda başarısızlık ve zorluk yaşanmıştır (Solove,2008).

Akgül (2013) kişisel sağlık verileri ile ilgili Danıştay kararlarını incelemiştir. Örneklerin birinde doğumsal kalça çıkıklığı teşhisi konulan ve ameliyat sırasında oluşan deformasyon sonucunda idare mahkemesine açılan davada Adli Tıp Kurumu'nun raporu da göz önüne alınarak herhangi bir hizmet eksikliği veya kusuru bulunmadığı sonucuna varılarak dava reddedilmiştir. Fakat daha sonra Danıştay, verilen raporda bireye ait röntgen görüntülerinin hasta dosyasında bulunmadığı

ve bu yapılan müdahalenin sorgulanmasına yol açan istatistik ve grafiklerin depolanmamasının da bir hizmet kusuru olarak görülmesi üzerine manevi tazminat ödenmesi gerektiği gerekçesi ile bu kararı bozmuştur. Bu örnek doğrultusunda kişisel sağlık verilerinin yalnızca bireyin bilgi alma hakkı çerçevesinde değil gerekli durumlarda üçüncü şahıslarla ve mahkeme dosyasına eklenme suretiyle paylaşılması gerektiği için de korunması ve depolanması gerekmekte olduğu sonucuna ulaşılabilmektedir.

Firmalar rekabet piyasasında üstün olma, daha fazla kâr elde etme gibi sebeplerle kişisel verilere ulaşma isteği ile yasal olmayan birçok yola başvurmaktadır. Bu durum, birçok zarara neden olabilir: gizlilik ihlali, kişisel ve profesyonel zarar, işgücü piyasalarına sınırlı erişim, en iyi değer fiyatlandırmasına kısıtlı erişim vb. (Chaudhry ve ark,2015). Kişisel sağlık verileri söz konusu olduğu zaman en yüksek rekabet içerisinde olan paydaşlardan biri ilaç firmalarıdır. 2017 yılında CNN TÜRK tarafından yapılan bir haberde yabancı ilaç firmalarının yasak olmasına rağmen hastalara ait bilgileri almadan ilaç vermedikleri öne sürülmüştür. İlgili haber Kişisel Sağlık Verileri Çalışma Grubu tarafından da ele alınmış ve ilgili *yazıda "İddiaya göre firmaların amacı kendilerine bir hasta veri tabanı oluşturmak. Çünkü bazı ilaçların fiyatı çok yüksek. Hasta bilgilerine ulaşan firma hem Türkiye'deki hastalara uygun ilaç seçimini yapıyor hem de o ilacı satacak hedef kitleye doğrudan ulaşabiliyor"* şeklinde aslında kişisel sağlık verilerinin korunması noktasındaki hayati önemi belirtmiştir.

Veri güvenliğinin sağlanması, veri işleyen bireylere birçok yetki ve sorumluluk getirmiştir. Bu sorumlulukların en önemlisi tartışmasız kişisel verilerin yetkisiz bireylerin eline geçmesinin engellenmesi ve bu doğrultuda tedbirlerin alınmasıdır. Buna ilişkin tedbirlerin özelliği kişisel verinin işlenme amaçları ve kişisel verilerin türü ile doğrudan ilişkilidir (Ketizmen ve Ülküderner, 2007). Özcan (2018) tarafından yapılan "Sigorta Hukuku Bağlamında Kişisel Sağlık Verilerinin Korunması" adlı çalışmada kişisel sağlık verilerinin açıklanması yani korunmaması ile ilgili Danıştay kararı incelenmiştir. İlgili olayda davacıya AIDS teşhisi konulmuş fakat henüz teşhis gerçekleştirilmeden basına yansımıştır. Basına yansıması sonucu işten çıkarılan birey maddi ve manevi zararın tazmini istemiyle dava açmıştır. İdare Mahkemesince; davalı idarenin sağlık verilerini korumama gibi bir hizmet kusuru bulunduğu dolayısıyla davacının bu olay neticesiyle işini kaybetmesi sonucu oluşan maddi zararın ve sonucunda bireyin duyduğu üzüntü sebebiyle uğradığı manevi zararın tazmininin gerekliliğine karar verilmiş ve bu karar Danıştay tarafından da onaylanmıştır. Bu olayda bireyin hem verilerinin sağlık kayıtlarına uygun olarak işlenmeden ve onamı alınmadan 3.kişilerle paylaşılarak mahremiyeti ihlal edilmiş hem de idare tarafından kişisel sağlık verilerinin korunması konusunda büyük açık oluşturmuştur.

Küzeci(2015)'den alıntılanan örnekte; hasta HIV olabilme düşüncesiyle korku ve endişe içerisinde hastaneye başvurmuş, test yaptırmış ve bir süre sonra test sonuçlarını almak için gittiğinde doktorunu bulamamıştır. Bunun üzerine laboranttan test sonuçlarını isteyince HIV pozitif olduğu söyleniyor ve daha sonrasında birey bunun ağırlığını kaldıramayıp intihar ediyor fakat daha sonra anlaşılıyor ki henüz test yapılmamış yapılan test sonucu gerçekte negatif çıkıyor. Bu örnekte baskın olan kısım bilgilerin korunması kısmında o bilgilere kimlerin erişmesi gerektiği ile ilgilidir. Veriler işlendikten ve veri tabanlarına aktarıldıktan sonra bir mahremiyet türü olan bilişsel mahremiyet kavramının daha da önemli olduğu görülmektedir. Aksi takdirde en ufak bir mahremiyet ihlali can kaybı, psikolojik sorunlar doğurabilmektedir.

Aslında kişisel sağlık verilerinin korunmadığını gösteren en net örnek Sosyal Güvenlik Kurumu(SGK)'nun kişisel sağlık verilerini satış konusu etmesi ile ilgili davanın sonuçlanmasıdır.

Dülger(2019) tarafından Sgk'nın Kişisel Sağlık Verilerini Satış Konusu Haline Getirmiş Olmasına İlişkin Mahkeme Kararının Kesinleşmesi Üzerine: Kişisel Sağlık Verileri Satılabilir Mi? isimli çalışmada söz konusu olay incelenmiştir. CHP milletvekili Ö.Ö.'nün iddialarına göre SGK, bireylerin kişisel sağlık verilerini eski bir milletvekiline ait olan Datamed isimli bir şirkete satmıştır. Datamed isimli şirketin sahibi B.İ. isminin karalandığı yönünde tazminat davası açmış ve dava Ö.Ö. lehine sonuçlanmış. İlk derece mahkemesi ve Yargıtay'ın kararıyla da Ö.Ö.'nün iddiaları doğrulanmıştır. Kişisel verilerin korunması ve depolanması konusunda mahremiyet ihlalinin tüm kişisel sağlık verilerini elinde bulunduran ve devlete ait bir kurum tarafından gerçekleştirilmesi oldukça vahim ve irdelenmesi gereken bir konudur.

5. SONUÇ

Kişisel verilerin korunması ve depolanması konusunda etik ve mahremiyet ihlali belki de en çok sağlık alanında ortaya çıkmaktadır. Mahremiyet, kişisel sağlık verileri açısından bireyin sağlık hizmeti almak için hastaneye başvurduğu andan itibaren korunması gereken bir hak olarak değerlendirilmektedir (Candan ve Bilgili,2018). Bu süreçte herhangi bir mahremiyet ihlali olma ihtimali sağlık hizmetini sunan tüm paydaşların ahlaki ilkelere uymalarını zorunlu hale getirmektedir. Ancak bu kişisel sağlık verilerinin korunması hususunda yalnızca sağlık hizmetini sunan kişiler değil devlet de büyük paya sahiptir. Hizmetin sunum sürecinde mahremiyetin sağlanmasının hekimin sorumluluğunda olduğu gibi hizmet sonrasında verilerin güvenli şekilde korunması için gerekli önlemleri almak da devletin sorumluluğundadır (Derinözlü,2017).

Kişisel verilerin korunması konusunda bireyin mahremiyetinin zaman içerisinde kişisel verilere erişimin kolaylaşması ile gerek ulusal gerekse uluslararası düzenlemelere konu olduğu görülmektedir. Anayasa'nın 20.maddesi de özel hayatın gizliliği ve kişisel veriler ile ilgilidir. Ayrıca 2016 yılında Kişisel Verileri Koruma Kanunu çıkarılmış, 2019 yılında da Kişisel Sağlık Verilerinin Korunması Hakkında Yönetmelik yayınlanmıştır. Uluslararası düzenlemelerde ilk adım 108 Sayılı sözleşme ile atılmış olup Türkiye'nin de imzaladığı bu sözleşme ülkelerin kişisel sağlık verileri koruması ile ilgili kapsamlı düzenlemeler içermektedir.

Gittikçe artan teknolojik gelişmeler ile kişisel sağlık verilerinin korunması ve depolanması hususu daha çok önem kazanmaktadır. Teknolojik ilerlemeleri durdurmak neredeyse olanaksız olduğu için her alanda bu ilerlemelere adapte olunması gerekmektedir. Türkiye'de 2003 yılında gerçekleştirilen Sağlıkta Dönüşüm Programı (SDP)'nın bileşenlerinden biri olan Sağlıkta e-Dönüşüm: Ulusal Sağlık Bilgi Sistemi kapsamında kişisel sağlık verilerinin işlenmesi, iletilmesi, depolanması ve korunması amacıyla birçok uygulama geliştirilmiştir. Bu uygulamalardan olan elektronik sağlık kayıtları ve e-nabız kişisel sağlık verilerinin korunması ve depolanması anlamında dikkat çekmektedir. ESK doğrultusunda bireylerin de kendi verilerine erişebilecekleri; tansiyon, şeker, nabız gibi ölçümleri ekleyebilecekleri; kişisel sağlık verilerini izin verdikleri kişilerle paylaşabilecekleri e-nabız sistemi oluşturulmuştur. Bu sistemin en önemli özelliği bireylerin kendilerine ait kimlik numarası ve şifreleri ile girerek yalnızca kendilerine ait olmasıdır. Ayrıca uygulamadaki bilgiler kriptolu olarak şifreli korumaya sahiptir(İleri ve Uludağ,2017). Her ne kadar şifreli olması ve izin verilen kişilerin erişmesinin sağlanması gibi mahremiyet önlemleri alınsa da tüm kişisel verilerin bu alanda depolanması hem günümüz hem gelecek için en ufak güvenlik açığında kişisel verilerin üçüncü kişilerin eline geçmesi konusunda endişe oluşturmaktadır. Dolayısıyla bireylerin bu tür uygulamaları kullanma noktasındaki tutumları da olumsuz olmaktadır.

Sağlık alanındaki teknolojik ilerlemelerde e-sağlık sistemlerinin yer alması kişisel veri kayıtlarını elektronik ortama taşımıştır. Yeni oluşan veri setlerinin yanı sıra artık sağlık kuruluşları daha önceden fiziki arşivlerinde depolanan verileri de elektronik ortama geçirmeye başlamıştır. Bu gelişim başlamadan önce gerek fiziki arşivlerde gerekse o dönemin teknolojik imkânlarının el verdiği ölçüde depolanırken verilere erişimin kolaylığı, düzenli veri depolama, dosyalama sistemleri, verilerin paylaşılması gibi konularda ciddi sıkıntılar yaşanmaktadır. Bu sorunların giderilmesi hususunda elektronik sağlık kayıtları ve sağlığın dijitalleşmesi olumlu bir rol oynamaktadır. Fakat bilgilere erişimin kolaylığı, siber güvenlik duvarının aşılması, kötü niyetli yazılımcılar gibi etkenler göz önüne alındığı zaman teknolojik gelişmeler kişisel sağlık verilerinin mahremiyet ihlali konusunda ciddi sorunlara yol açmıştır(Derinözlü,2017). Bu olumsuzlukların ve siber saldırıların giderilmesi için birçok güvenlik duvarı oluşturulmakta ve her sağlık kurum ve kuruluşu gerekli önlemleri almaktadır. Ayrıca sağlık sektöründe bilgi güvenliği yönetiminin oluşturulmasında ISO kalite standartlarından olan ISO/IEC 27002 kullanılarak gerekli düzenlenmeler gerçekleştirilmektedir.

Hastane Bilgi Yönetim Sistemleri (HBYS) her hastanenin belirli bir sözleşme doğrultusunda anlaşmalı olduğu şirketler tarafından yürütülmektedir. Teknik şartname doğrultusunda hastane bu şartları taşıyan firma ile anlaşmakta ve sözleşme süresi bitene kadar o firma ile faaliyet göstermektedir. Hastaneler sözleşmesi biten firma ile yollarını ayırıp başka bir firma ile çalışmaya devam edebilmektedir. Bu doğrultuda kişisel sağlık verilerinde herhangi bir kayıp oluşmaması ve tek tip veri elde edilebilmesi için Sağlık Bakanlığı Minimum Veri Modeli oluşturulmuştur. Bu modelde HBYS içerisinde yer alan sağlık verileri tek tip olarak depolanmakta ve bir sonraki firmaya aktarılmaktadır. Bu durum verilerin aktarımında mahremiyet ihlalini en aza indirmektedir. Veri aktarımı ve erişimi söz konusu olduğu durumlarda tamamen teknolojik veya tamamen kağıda dayalı yöntemlerin kullanılması göz önüne alındığında kesin bir mahremiyet çözümü bulunmamaktadır. Standartların oluşturulması ve denetlenmesi bu durumu en aza indirmeyi amaçlamaktadır.

KAYNAKLAR

Ağıralan E, (2015). Bilgi Güvenliği, Kişisel Verilerin Korunması Ve Mahremiyet Etki Değerlendirmesi. Yüksek Lisans Tezi, Polis Akademisi Güvenlik Bilimleri Enstitüsü, Ankara.

Akar Y, Özyurt E, Erduran S, Uğurlu D, Aydın İ, (2019). Hasta mahremiyetinin değerlendirilmesi. Sağlık Akademisyenleri Dergisi, 6(1), 63-69.

Akgül A, (2013). Kişisel Verilerin Korunması Açısından İdarenin Hukuki Sorumluluğu ve Yargısal Denetimi. Doktora Tezi, Kocaeli Üniversitesi Sosyal Bilimler Enstitüsü, Kocaeli.

Akten R, (2017). Hastanelerde Hasta Mahremiyetine Gösterilen Özenin Hasta Bakış Açısıyla Değerlendirilmesi (Antalya Örneği). Yüksek Lisans Tezi, Selçuk Üniversitesi Sağlık Bilimleri Enstitüsü, Konya.

Almunawar MN, and Anshari M, (2012). Health Information Systems (HIS): Concept and Technology.
International Conference Informatics Development.

Altundiş M, (2016). Tıbbi Kişisel Verilerin Tutulması ve Korunması Yükümlülüğü Ve İdarenin Bu Yükümlülüğünü Yerine Getirmemesinden Doğan Sorumluluğu. Türkiye Adalet Akademisi Dergisi.7(28), 313-351.

Altuner İ, (2015). Hipokrat Yemini. Iğdır Üniversitesi Sosyal Bilimler Dergisi. 7, 01-07.

Andreu-Perez J, Poon CCY, Merrifield RD, Wong STC, YAang GZ, (2015). Big Data for Health. IEEE J Biomed Health Inform, 19(4), 1193-1208.

Arslan ET, Demir H, (2016). Sağlık Çalışanlarının Hasta Mahremiyetine İlişkin Tutumu: Nitel Bir Araştırma. AİBÜ Sosyal Bilimler Enstitüsü Dergisi. 17(4), 191-220.

Avaner E, (2018). Mahremiyet Nedir? Mahremiyetin Sağlık Hizmetleri Penceresinden Görünürlüğü Nasıldır? Türkiye Biyoetik Dergisi. 5(3), 110-116.

Avcı Y, (2019). Kişisel Verilerin Korunması. Yüksek Lisans Tezi, Selçuk Üniversitesi Sosyal Bilimler Enstitüsü, Konya.

Ay F, (2008). Elektronik Hasta Kayıtları: Güvenlik, Etik ve Yasal Sorunlar. Anadolu Üniversitesi Bilim ve Teknoloji Dergisi, 9(2), 165-175.

Bates DW, Saria S, Ohno-Machado L, Shah A, Escobar G, (2014). Big Data in Health Care: Using Analytics to Identify and Manage High-Risk and High-Cost Patients. Health AFF(Millwood), 33(7), 1123-1131.

Bayın G, Yeşilaydın G, Özkan O, (2016). Bulut Bilişimin Sağlık Hizmetlerinde Kullanımı. Dumlupınar Üniversitesi Sosyal Bilimler Dergisi, 48, 233-253.

Bayındır H, (2019). Özel Sağlık Kurumları Kapsamında Kişisel Sağlık Verilerinin İşlenmesi Ve Korunması. Yüksek Lisans Tezi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü. İstanbul.

Bekmezci H, Özkan H, (2015). Ebelik Uygulamalarında Mahremiyetin Önemi. HSP, 2(1), 113-124.

Bezirgan Gözmener S, (2019). Kişisel Sağlık Verilerinin Kayıt Ve Korunmasında Hemşirelerin Cezai Sorumluluğu. Yüksek Lisans Tezi. Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü, İzmir.

Bezirgan Gözmener S, Şenol S, ve Seren İntepeler Ş, (2019). Hemşirelik Öğrencileri İçin Kişisel Sağlık Verilerinin Kayıt ve Korunması Tutum Ölçeği Geçerlik ve Güvenirlik Çalışması. Dokuz Eylül Üniversitesi Hemşirelik Fakültesi Elektronik Dergisi (DEUHFED). 12(1), 21-30.

Can N, 2020. Hasta Mahremiyeti Hakkı. Türkiye Barolar Birliği Dergisi, 147, 183-219.

Candan M, Bilgili N, (2018). Hemşire ve Ebelerin Hasta Mahremiyetine İlişkin Görüşlerinin Değerlendirilmesi. Gazi Sağlık Bilimleri Dergisi. 3(3), 34-43.

Chaudry A, Crowcroft J, Howard H, Madhavapeddy A, Mortier R, Haddadi H, and McAuley D, (2015). Personal Data: Thinking Inside the Box. Aarhus Series on Human Centered Computing, 1(1), 29-32.

Clarke R, (2009). Privacy Impact Assessment: Its Origins and Development. Computer Law and Security Review, 25(2), 123–135.

CNN Türk. İlaç Firmaları Hastaların Kişisel Bilgilerini Topluyor İddiası. Erişim Tarihi 12 Haziran 2020. https://www.cnnturk.com/video/turkiye/ilac-firmalari-hastalarin-kisisel-bilgilerini-depoluyor-iddiasi.

Çekin MS,(2016). 6698 Sayılı Kişisel Verilerin Korunması Hakkında Kanun'un Big Data (Büyük Veri) ve İrade Serbestisi Açısından Değerlendirilmesi, İÜHFM, 74(2), 629-644.

Çetin H, (2014). Kişisel Veri Güvenliği Ve Kullanıcıların Farkındalık Düzeylerinin İncelenmesi. Akdeniz İ.İ.B.F. Dergisi. (29), 86 – 105. Gözüküçük M, Veri İşleme Süreçlerinde Tartışmalı Bir Çözüm: Veri Anonimleştirmesi. Yüksek Lisans Tezi, İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.

Çobansoy G, 2020. İnsan Hakları Açısından Kişisel Verilerin Korunması Sorunu. Yüksek Lisans Tezi, Maltepe Üniversitesi Lisansüstü Eğitim Enstitüsü, İstanbul.

Dankar FK, El Emam K, (2012). The Application of Differential Privacy to Health Data. ACM International Conference Proceeding Series. 12,158-166.

Derinözlü C. Büyük veri ve Mahremiyet. 1.Ulusal Bulut Bilişim ve Büyük veri Sempozyumu, 25-30, 19-20 Ekim (2017), Antalya.

Diler R, (2014). Mahremiyet Eğitimi ve Önemi. Gaziosmanpaşa Üniversitesi İlahiyat Fakültesi Dergisi. 2(1), 69-98. Erdinç GH, (2017). Bilgi Güvenliği, Kişisel Verilerin Korunması Ve Biyometrik Verilerin İşlenmesine İlişkin Öneriler. Yüksek Lisans Tezi, İstanbul Teknik Üniversitesi Bilişim Enstitüsü, İstanbul.

Dülger MV, (2015). Sağlık Hukukunda Kişisel Verilerin Korunması ve Hasta Mahremiyeti. İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi. 1(2), 43-80.

Dülger MV, (2019). Kişisel Sağlık Verileri Hakkında Yönetmelik'e İlişkin Değerlendirme. Hukuki Haber, 1-11.

Dülger Mv, (2019). Sgk'nın Kişisel Sağlık Verilerini Satış Konusu Haline Getirmiş Olmasına İlişkin Mahkeme Kararının Kesinleşmesi Üzerine: Kişisel Sağlık Verileri Satılabilir Mi?. Erişim Tarihi 10 Eylül 2020, https://www.hukukihaber.net/kisisel-saglik-verileri-satilabilir-mi-makale,5723.html.

Ergüden Ç, (2019). Kişisel Sağlık Verilerinin İşlenmesi. https://www.academia.edu/40904181/k%c4%b0%c5%9e%c4%b0sel_sa%c4%9elık_ver%c4%b0ler%c4%b0n%c4%b0n_%c4%b0%c5%9elenmes%c4%b0 Erişim Tarihi 11 Haziran 2020.

Hafızoğulları Z, ve Özen M, (2009). Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar. Ankara Barosu Dergisi, 67(4), 9-22.

İleri YY, ve Uludağ A, (2017). e-Nabız Uygulamasının Yönetim Bilişim Sistemleri Ve Hasta Mahremiyeti Açısından Değerlendirilmesi. Uluslararası Sağlık Yönetimi Ve Stratejileri Araştırma Dergisi (USAYSAD), 3(3), 318-325.

İmançlı C, (2019). Kişisel Sağlık Verilerinin Korunamamasından Doğan Özel Hukuk Sorumluluğu. Yüksek lisans Tezi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.

İnal Y, Ercil Cagiltay N, E-Nabız Mobil Sağlık Uygulamasına Yönelik Kullanıcı Değerlendirmesi. Hacettepe Sağlık İdaresi Dergisi, 22(2), 375-388.

İpek N, 2020. İslam'ın Mahremiyet Algısı Işığında Mahremiyet Eğitiminin Çocuk Cinsel İstismarını Önlemedeki Rolü. Yüksek Lisans Tezi, Erzincan Binali Yıldırım Üniversitesi Sosyal Bilimler Enstitüsü, Erzincan.

İzgi MC, (2014). Mahremiyet Kavramı Bağlamında Kişisel Sağlık Verileri. Türkiye Biyoetik Dergisi, 1(1), 25-37.

Kandilli E, (2019). Sağlık Hukukunda Etik Açısından Kişisel Veriler Ve Mahremiyet Hakkı. Yüksek Lisans Tezi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.

Karakethüdaoğlu M, (2019). Sistemlerin Geliştirilmesinde Mobil Uygulamalarda Kullanıcı Geri Bildirimlerinin Önemi: Türkiye E-Nabız Örneği. Yüksek Lisans Tezi, Sakarya Üniversitesi İşletme Enstitüsü, Sakarya.

Ketizmen M, ve Ülküderner Ç. E-devlet Uygulamalarında Kişisel Verilerin Korun(ma)ması. XII. Türkiye'de İnternet Konferansı, 189-193, 8-10 Kasım (2007), Bilkent Üniversitesi, Ankara.

Kılınç D, (2012). Anayasal Bir Hak Olarak Kişisel Verilerin Korunması. Ankara Üniversitesi Hukuk Fakültesi Dergisi. 61(3): 1089-1172.

Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelik. Erişim Tarihi, 18 Mayıs 2020. https://www.lexpera.com.tr/mevzuat/yonetmelikler/kisisel-saglik-verilerinin-islenmesi-ve-mahremiyetinin-saglanmasi-hakkinda-yonetmelik.

Kişisel Verileri Koruma Kurumu, (2018). 100 Soruda Kişisel Verileri Koruma Kanunu, KVKK Yayınları, Ankara.

Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi, (2018). Kişisel Verileri Koruma Kurumu, KVKK Yayınları, Ankara.

Korkmaz İ, (2013). Facebook ve Mahremiyet: Görmek Ve Gözetle(n)mek. Yalova Sosyal Bilimler Dergisi, 5, 107-122.

Küzeci E, Türkiye'de Sağlık Verilerinin Korunması: Hukuksal Çerçeve. Kişisel Sağlık Verileri Ulusal Kongresi, 14-20, 19-20 Aralık (2015), İstanbul.

Marşap A, Akalp G, ve Yeniman E, (2010). Sağlık İşletmelerinde İnsan Kaynağının Kurumsal Bilgi Güvenliği Kültürü Gelişimi. Bilişim Teknolojileri Dergisi, 3(1), 31-40.

Nalbantoğlu L, (2018). Kişisel Sağlık Verilerinin İşlenmesi Ve Mahremiyetinin Sağlanması Hakkında Yönetmelikte Yapılan Değişiklikler. The Deloitte Times, 64-67.

Ohm P, (2009). Broken Promises Of Privacy: Responding To The Surprising Failure Of Anonymization. UCLA Law Rewiev, 57, 1701-(2010).

Olca E, ve Can Ö. Ulusal ve uluslararası yönetmeliklerde kişisel sağlık verisi mahremiyetinin korunması. 7.Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı, 71-76, 17-18 Ekim (2014), İstanbul.

Özcan S, (2018). Sigorta Hukuku Bağlamında Kişisel Sağlık Verilerinin Korunması. Yüksek Lisans Tezi, Kadir Has Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.

Özer K, (2015). Sağlık Kuruluşlarında Hasta Mahremiyeti Uygulamalarının ve Sağlık Çalışanlarının Hasta Mahremiyetine Yönelik Tutumlarının İncelenmesi (Konya Örneği). Yüksek Lisans Tezi, Selçuk Üniversitesi Sağlık Bilimleri Enstitüsü, Konya.

Özkan F, (2018). Kişisel Sağlık Verilerinin Korunmasının Pozitif Temelleri ve AİHM Kararlarından Örnekler. Yüksek Lisans Tezi, Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü, İzmir.

Öztürk H, Özçelik SK ve Bahçecik N, (2014). Hemşirelerin Hasta Mahremiyetine Özen Gösterme Durumu. Ege Üniversitesi Hemşirelik Fakültesi Dergisi, 30 (3), 19-31.

Ropiak DJ, (2019). Commentary on Ethics and Morality. Erişim Tarihi, 24 Nisan 2020. Erişim adresi, https://www.researchgate.net/publication/279685427_Commentary_on_Ethics_and_Morality.

Sağlık Bakanlığı Sağlık Bilgi Sistemleri Genel Müdürlüğü, (2015). Hastane Bilgi Yönetim Sistemi Minimum Veri Modeli Sürüm 1.0.

Sağlık Bakanlığı Sağlık Bilgi Sistemleri Genel Müdürlüğü, 2020. Sağlık Bilgi Yönetim Sistemi Veri Modeli (VEM) Sürüm 2.0.

Sağlık Bakanlığı, Dijital Hastane, https://dijitalhastane.saglik.gov.tr/TR,4874/ehr-electronic-health-record---esk-elektronik-saglik-kaydi.html, erişim tarihi 28 Mayıs 2020.

Sağlık Hizmetleri Genel Müdürlüğü; Sağlıkta Kalite, Akreditasyon ve Çalışan Hakları Dairesi Başkanlığı, 2020. Sağlıkta Kalite Standartları(Hastane). 1.Baskı, Ankara. Erişim Tarihi 5 Eylül 2020. https://kalite.saglik.gov.tr/TR,52460/guncel-standartlar.html.

Solove D, (2008). Understanding Privacy. The George Washıngton Unıversıty Law School Publıc Law And Legal Theory Workıng, Harvard University Press.

Sur H, Palteki T, (2013). Hastane Yönetimi, 1.Baskı, İstanbul, Nobel Matbaacılık, s.835.

Şen Y. (2015). İslâm Hukukuna Göre Sağlık Hizmetlerinde Mahremiyet Hakkı. Ekev Akademi Dergisi. 19(61), 403-428.

Şenyürek G. Etik açıdan kişisel sağlık verileri ve korunması. Kişisel Sağlık Verileri Iı. Ulusal Kongresi Kitabı, 151-157, 03-04 Haziran (2017), İstanbul.

Tataroğlu M, (2009). E-Devlet'te Kullanılan Gözetim ve Kayıt Teknolojilerinin Mahremiyet Üzerinde Etkileri. Abant İzzet Baysal Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 18, 95-120.

Than Win K, (2005). A review of security of electronic health records. Health Information Management, 34(1),13.

Türkiye Cumhuriyeti Anayasası, 1982. T.C. Resmî Gazete. 17863, 9 Kasım 1982.

Türkiye Cumhuriyeti Dijital Dönüşüm Ofisi, (2019)/12 Sayılı Genelge, Erişim Tarihi 31 Mayıs 2020, https://cbddo.gov.tr/mevzuat/(2019)-12-sayili-bilgi-guvenligi-tedbirleri-cumhurbaskanligi-genelgesi/.

Türkiye Cumhuriyeti Sağlık Bakanlığı, (2018). e-Nabız V.2.0 Kişisel Sağlık Kaydı Sistemi Kullanma Kılavuzu.

Türkiye Cumhuriyeti Sağlık Bakanlığı, Diğital Hastane, Erişim Tarihi 28 Mayıs 2020,https://dijitalhastane.saglik.gov.tr/TR,4874/ehr-electronic-health-record---esk-elektronik-saglik-kaydi.html.

Türkiye İstatistik Kurumu, Hastane Sayılarının İllere Göre Dağılımı, Erişim Tarihi 5 Temmuz 2020, http://www.tuik.gov.tr/PreTablo.do?alt_id=1095.

Usta A, (2011). Kuramdan Uygulamaya Kamu Yönetiminde Etik ve Ahlâk. Kahramanmaraş Sütçü İmam Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi. 1(2), 39-50.

Ülgü M, Muş E, ve İşleyen F, (2018). Sağlık Bilişimi Standartları. Sağlık Düşüncesi ve Tıp Kültürü Platformu, 46, 14-17.

Varol E, (2018). Hemşirelerin Mahremiyet Hakkındaki Tutumları ve Bakım Uygulamalarının Hasta Mahremiyetine Olan Etkileri. Yüksek Lisans Tezi, Balıkesir Üniversitesi Sağlık Bilimleri Enstitüsü, Balıkesir.

Yeşiltaş A, (2018). E-Nabız Uygulamasının Kullanımını Etkileyen Faktörler. Sağlık Akademisyenleri Dergisi, 5(4), 290-295.

Yılmaz M. ve Demirkan AE, (2012). Hastane Yönetim ve Bilgi Sisteminin Kullanılabilirliğinin Değerlendirilmesi. Bilişim Teknolojileri Dergisi, 5(3), 19-28.

Yüksel M, (2009). Mahremiyet Hakkına ve Bireysel Özgürlüklere Felsefi Yaklaşımlar. Ankara Üniversitesi Sağlık Bilimleri Fakültesi Dergisi, 64 (01), 275-298.