Ulusal ve Uluslararası Yönetmeliklerde Kişisel Sağlık Verisi Mahremiyetinin Korunması

E. Olca ve Ö. Can

***Özet*— Bilgisayar ve internet kullanımı; hayatı kolaylaştırma, verimliliği artırma ve maliyetleri düşürme gibi katma değerlerle birlikte günlük hayatın en önemli parçalarından biri olmuştur. Ancak, bilgi sistemlerinde yer alan verilerin hangi amaçlarla, hangi durumlarda ve nasıl kullanılacakları konusunda yeterli kontrollerin ve yaptırımların bulunmaması, kişinin kendi verisi üzerindeki erişimleri kontrol edebilmesini zorlaştırmakta ve kişisel mahremiyetini korumasına yönelik endişelerin ortaya çıkmasına neden olmaktadır. Teknolojinin hızla gelişmesi ve bunun sonucunda meydana gelen elektronik dönüşümler çerçevesinde, kişisel sağlık bilgilerinin dijital ortama geçirilmesi kişisel haklar yönünden ciddi riskler ortaya çıkarmaktadır. Bu dönüşümle birlikte, e-sağlık alanında oluşan riskleri yönetmek, kişisel verilerin gizliliğini ve güvenliğini sağlamak için ulusal ve uluslararası alanlarda standartlar belirlenmesine ve yasal düzenlemeler yapılmasına başlanmıştır. Bu çalışmada; mahremiyeti korunması gereken bir e-varlık şeklini alan kişisel veri, kişisel sağlık verisi ve dijital ortamda tutulan Elektronik Sağlık Kaydı (ESK) olarak incelenmekte, bu e-varlıkların mahremiyetinin korunması için oluşturulan yönetmelikler ve standartlar bazında yapılan çalışmalar anlatılmaktadır.**

***Anahtar Kelimeler*—Elektronik sağlık kaydı, kişisel veri, mahremiyet, veri güvenliği.**

***Abstract*— Computers and internet usage have become one of the most important parts of daily life with the added values such as making life easier, increasing productivity and reducing costs. However, the absence of sufficient control and sanctions over the purposes, situations and ways of data usage in the information systems makes it difficult for a person to control access on her/his own data, and causes concerns to emerge about personal privacy. As a result of the rapid technological development and the electronic transformation it brings with, transition of personal health information to the digital environment poses serious risks in terms of personal rights. In order to manage risks in e-health domain and to secure privacy and security of personal data, new attempts have emerged to set standards and legal regulations both in national and international fields. In this study; personal data which has become an e-entity whose privacy needs to be protected, is analyzed as personal health data and Electronic Health Record (EHR) in digital platform, and the study also reviews studies carried out in the form of regulations and standards to protect the privacy e-entity.**

Manuscript received July 19, 2004.

Emre Olca, İzmir Üniversitesi Mühendislik Fakültesi Yazılım Mühendisliği Bölümü, 35350, Üçkuyular, İzmir, Türkiye (İlgili yazar telefon: +90-232-4464949; faks: +90-232-2240909; e-posta: emre.olca@izmir.edu.tr).

Özgü Can, Ege Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü, 35100, Bornova, İzmir, Türkiye (e-posta: ozgu.can@ege.edu.tr).

***Index Terms*—Electronic health record, personal data, privacy, data security.**

I. Giriş

Teknolojinin hızla gelişmesi sonucunda, e-sağlık sistemlerinde yer alan hasta ve tedavi verileri, kayıtların elektronikleşme süreci içerisinde dijital ortama taşınmıştır. Bu taşınma öncesinde, hasta ve tedavi verilerinin saklanması için o dönemin teknolojik imkânları kullanılırken, sağlık verilerinin düzgün alınması, düzenli saklanması, gerektiğinde hızlı bir şekilde erişilmesi, paylaşılması ve arşivlenmesi konularında ciddi sıkıntılar yaşanmıştır. Elektronik ortama geçiş ile bu sıkıntılar aşılmış, istenildiği zaman ve yerden ulaşılabilir bir hale gelmiştir. Fakat bu erişim kolaylığının yanında veri güvenliği riskleri, veri istismarları ve ekonomik tehditler ortaya çıkmıştır. Bu tehditlerin en önemlilerinden birisi, kişiler üzerinde maddi ve manevi büyük zararlara yol açabilecek kişisel sağlık veri mahremiyetinin ihlal edilmesidir. Elektronik sağlık kayıtları, sağlık alanında yer alan bütün kullanıcılar için önemli avantajlar sağlamış olmasına rağmen, teknolojinin kötü amaçlı kullanımı sonucu verilerin gizliliği ve güvenliği konusunda ciddi sıkıntıların ortaya çıkmasına neden olmaktadır.

Sağlık verisi üzerinde oluşan risklerin sonucu olarak, yasal düzenlemeler yapılmaktadır. Ulusal bilgi güvenliği açısından tehlike yaratabilecek bu riskler için, kanunlarla ve uluslararası yönetmeliklerle yapılan düzenlemeler uygulanmalıdır. Yapılan tüm düzenlemelere rağmen, kişinin kendi haklarının farkında olması ve mahremiyetinin korunması için yasal mevzuatlar doğrultusunda işlem yapıldığından emin olması gerekmektedir. Çünkü bilgi güvenliğinin en zayıf halkası tehdide doğrudan veya dolaylı olarak maruz kalan eğitimsiz ya da bilinç eksikliği olan bireylerdir. Bu nedenle kişi, sağlık sistemindeki bir aktör olarak, kişisel verisinin mahremiyetini ve güvenlik önlemlerini tamamen diğer paydaşlara bırakmamalı ve sürecin yönetmelikler doğrultusunda ilerlediğinin takibini yapabilmelidir.

Bu çalışmada; kişisel veriler, kişisel sağlık verileri ve bunların kanunlarla ve uluslararası yönetmeliklerle yapılan düzenlemelerinden bahsedilmekte, e-sağlık dâhilinde kişisel sağlık verileri için gizlilik ve güvenlik kavramlarının önemine değinilmektedir. Sağlık etki alanında, potansiyel mahremiyet riskleri ve mahremiyetin hasta hakları açısından önemi anlatılmaktadır. Bu çalışmanın organizasyonu aşağıdaki şekilde düzenlenmiştir: İkinci bölümde kişisel veri ve kişisel sağlık verisi kavramları açıklanmakta ve hukuki zeminleri

aktarılmaktadır. Üçüncü bölümde, genel bir değerlendirme yapılmakta ve dördüncü bölümde sonuç yer almaktadır.

II. KİŞİSEL VERİ VE YÖNETMELİKLER

Veriden ya da bu verinin ilgili olduğu diğer veriler ile birleştirilmesi sonucunda oluşan veri kümesinden, veri sahibinin kimliği elde edilebiliyorsa bu veri kişisel veridir. Örneğin, bir veri tabanında yer alan kullanıcı isimleri ve adresleri kişisel verilerdir. 1995 yılında yayınlanmış olan 95/46/EC numaralı Avrupa Birliği direktifi [1], kişisel veri tanımını, kim olduğu belli veya belirlenebilen bir gerçek kişiye ait tüm bilgilerdir şeklinde ifade etmektedir. Bu direktife göre, kimliği belirlenebilir gerçek kişi; "*Özellikle bir kimlik numarası referans alınarak doğrudan ya da dolaylı belirlenebilen ya da fiziksel, psikolojik, akli, ekonomik, kültürel veya sosyal kimliğine özgü bir veya birden çok faktörle tanımlanabilen kişidir*". Bu tek bir bilgi olabileceği gibi, birbiriyle ilişkili çok sayıda bilgi de olabilmektedir. Kişinin adı, adresi, kimlik numarası, doğum tarihi, banka hesap numarası, kredi kartı numarası, parmak izi, IP adresi, sağlık raporları, kişisel veri örnekleridir. Anayasanın 20. Maddesi "*Özel Hayatın Gizliliği*" [2] başlığı altında yer alan "*Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz*" ifadesiyle kişisel veriler bir hak olarak tanımlanmakta ve koruma altına alınmaktadır. Avrupa İnsan Hakları Sözleşmesinde, kişisel veri tanımı için açık bir ifade bulunmamaktadır. Ancak, "*özel ve aile hayatına saygı hakkı*" başlıklı 8. maddesinin 1. fıkrasına göre; "*Herkes, özel ve aile hayatına, konutuna ve yazışmalarına saygı gösterilmesi hakkına sahiptir*" hükmünde geçen "*özel hayata saygı hakkı*" kişisel verileri de kapsamaktadır [3]. Kişisel Verilerin Korunması Kanun Tasarısı'nda [4], kişisel veri tanımının içine tüzel kişiler de dâhil edilmekte ve kişisel veri "*Belirli veya kimliği belirlenebilir gerçek ve tüzel kişilere ilişkin bilgilerin tamamı*" olarak tanımlanmaktadır. 108 Numaralı Avrupa Konseyi Sözleşmesinde [5] ise; "*Kişisel veri, kimliği belirtilen ya da belirtilebilen gerçek kişiyle ilgili tüm bilgileri ifade eder*" şeklinde bir tanım yer almaktadır. Ekonomik Kalkınma ve İşbirliği Örgütü (The Organisation for Economic Co-operation and Development, OECD)'nün Rehber İlkelerinde [6] ise "*Belirli veya belirlenebilir bir gerçek kişiye ilişkin tüm bilgiler*" olarak bir tanım bulunmaktadır.

A. Kişisel Veri, Erişimi, Kullanımı ve Korunması

Amerika ve birçok gelişmiş Avrupa ülkesinde, elektronik ortama ve bilgisayar kullanımına ülkemizden daha önce geçilmiş olması nedeniyle, son çeyrek yüzyılda kişisel verilerin güvenliğine ilişkin tehlikelerin farkına varılmış ve bu alanda ülke mevzuatlarında çeşitli düzenlemeler yapılmıştır. Katı yaptırımları olan gizlilik düzenlemeleri nedeniyle, kişisel bilgiler kritik kurumsal veriler arasında en önemli bilgiler olarak kabul edilir bir duruma gelmiştir. Bu nedenle, kişisel verilere sahip olan kurumlar, bu verilerin erişimi ve kullanımı için kritik kurumsal verilerinin güvenliğine ilişkin bir program yürütmektedirler [7].

Yine kişisel verinin erişimi ve kullanımı için, Türkiye Cumhuriyeti Anayasasının 20. Maddesinde [2] özel hayatın gizliliğinin dokunulamaz olduğu belirtilmekte ve kişisel veriye erişim için "*Millî güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlâkın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak, usulüne göre verilmiş hâkim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; kimsenin üstü, özel kâğıtları ve eşyası aranamaz ve bunlara el konulamaz. Yetkili merciin kararı yirmi dört saat içinde görevli hâkimin onayına sunulur. Hâkim, kararını el koymadan itibaren kırk sekiz saat içinde açıklar; aksi halde, el koyma kendiliğinden kalkar*" tanımı yapılmaktadır. Sonradan eklenen ek fıkra ile de "*kişinin açık rızası*" terimi kullanılmakta, kişisel verinin ancak kanunda öngörülen durumlarda ve/veya kişinin açık izniyle erişilip işlenebileceği vurgulanmaktadır. Kişisel verinin korunması kapsamında, 2010 yılında yapılan bir düzenleme ile 20. Maddeye ek bir fıkra eklenmiştir. Bu ek fıkrada [2], "*Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir*" ifadesi yer almaktadır. Bu fıkrada, hüküm açık bir şekilde ifade edilmekte, kişisel verilerin ancak kanunla öngörülen durumlar ve kanuna dayalı düzenlemelerle işlenebileceği vurgulanmakta ve kişisel verilerin korunması öngörülmektedir. Ayrıca, bu maddede, kişisel verilerin ancak kişinin açık izni ile işlenebileceği, kişisel verilerin nasıl korunacağına dair esas ve usullerin kanunla düzenleneceği ifade edilmekte [8] ve kişisel verilerin mahremiyeti ve korunması hakkının varlığı tanınmaktadır.

Avrupa İnsan Hakları Sözleşmesinin 8. maddesinin 2. fıkrasında, kişisel veriye erişim hakkı için "*Bu hakkın kullanılmasına bir kamu otoritesinin müdahalesi, ancak ulusal güvenlik, kamu emniyeti, ülkenin ekonomik refahı, dirlik ve düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için, demokratik bir toplumda, zorunlu olan ölçüde ve yasayla öngörülmüş olmak koşuluyla söz konusu olabilir*" tanımı yapılmakta, ayrıca kişisel veri gizliliğinin ve güvenliğinin nasıl uygulanabileceği ifade edilmektedir [3]. 8. maddenin ihlal edilmesi ve yasal yaptırımlar ile ilgili de çeşitli adli örnekler mevcuttur. Avrupa İnsan Hakları Mahkemesi'nin 02.12.2008 tarih ve 2872/02 başvuru numaralı K.U. v. FİNLANDİYA davasında [9], 12 yaşında bir erkek çocuğu adına yayınlanan bir ilanda; çocuğun yaşı ve fiziksel özellikleri belirtilerek "kendisine yol gösterecek" kendi yaşında veya daha büyük bir erkekle yakın ilişki kurmak istediği ifadelerine yer verilmiştir. İnternet servis sağlayıcısının bu reklamı veren kişinin kimliğini gizlilik kurallarını ihlal edeceği gerekçesiyle açıklamayı reddetmiştir. Finlandiya mahkemeleri de servis sağlayıcının yasal olarak söz konusu bilgiyi açıklamaya mecbur olmadığı hükmüne varmışlardır. Bunun üzerine, Avrupa İnsan Hakları Mahkemesi bunun ceza gerektiren bir eylem olduğuna ve

Avrupa İnsan Hakları Sözleşmesinin 8. maddesinin ihlal edildiğine karar vermiştir [10]. 25.02.1997 tarih ve 22009/93 başvuru numaralı Z v. FİNLANDİYA davasında [11], bir ceza davası kapsamında kişinin HIV durumunu da içeren tıbbî bilgilerin açıklanmasından dolayı özel hayatına saygı gösterilmesi hakkının ihlal edildiği gerekçesiyle açılan davada, mahkeme ilgili kişinin tıbbî kayıtlarının ifşasının, Avrupa İnsan Hakları Sözleşmesi 8. madde 2. fıkra kapsamında gerekli olduğuna karar vermiştir. Ancak mahkeme, temyiz mahkemesi kararında kişinin adının ve HIV statüsünün açıklanmasının herhangi bir meşru amaç için gerekli olmadığına ve özel hayata saygı hakkının ihlal edildiğine karar vermiştir. Çünkü kişinin yaşadığı sağlık problemleri, doktoru ile arasındaki ilişkisi, teşhis, tedavi ve tetkik bilgileri, verilen ilaçlar ve görüntüleme sonuçları tümüyle özel hayatının gizliliği ve korunması hakkı kapsamına girmektedir. 27.08.1997 tarihli M.S. v. İSVEÇ davasında ise [12], başvurana ait kürtaj hakkında bilgileri de içeren tıbbî verilerin, tedavi gördüğü sağlık kurumu tarafından sosyal güvenlik kurumuna verilmesinin Avrupa İnsan Hakları Sözleşmesinin 8. maddesini ihlal ettiği iddiası değerlendirilmiştir. Bu davada, diğer dava sonuçlarının aksine, sosyal güvenlik kurumunun ilgili sağlık kurumundan bilgileri isteme yükümlülüğünün kanun dâhilinde olduğuna ve Avrupa İnsan Hakları Sözleşmenin 8. maddesinde güvence altına alınan özel hayata saygı hakkının ihlal edilmediğine karar vermiştir. Avrupa Birliği Direktifi 2b maddesinde ise [13], verinin işlenmesi çok geniş bir şekilde tanımlanmaktadır. Buna göre verinin işlenmesi; verinin toplanması, kaydedilmesi, organizasyonu, depolanması, değiştirilmesi, geri alınması, kullanımı, iletimi, yayma veya yayını ve hatta engellenmesi, silinmesi veya imhası dâhil olmak üzere kişisel veriler üzerinde manüel veya otomatik müdahaleyi kapsamaktadır.

Kişisel verilerin korunması konusu, gerçek anlamda ilk defa 1980 yılında Ekonomik Kalkınma ve İşbirliği Örgütü (OECD) tarafından ele alınmaktadır. Burada kabul edilen ilkeler diğer çalışmalara da rehber niteliğinde olmuştur. Bu çalışmaya göre, kişisel veri toplanması ve işlenmesi ilkesinde, kişisel veri kullanımının sınırları olması gerektiği belirtilmekte ve yine kişisel verilerin yasal mevzuatlara uygun, meşru yollarla ve mümkün olduğunca bireyin bilgisi veya izni dâhilinde elde edilmesi gerektiği vurgulanmaktadır [14]. 5237 sayılı Türk Ceza Kanunu, kişisel verilerin korunmasına yönelik suçları düzenleyen 134., 135., 136., 137. ve 138. maddelerinde manüel olarak yapılan veri işleme faaliyetleri de suç kapsamına alınmaktadır [15]. Türk Ceza Kanunu 138. maddesinde, kişisel verilerin korunmasında temel ilkeler arasında bulunan "süre sınırı" karşılanmaktadır [15]. Bununla birlikte, Türk Medeni Kanunu'nda "Kişilik Haklarının Korunması"nı düzenleyen 23. ve 24. maddeleri uyarınca da, kişisel veriler koruma altına alınmaktadır [16]. Avrupa Birliği Temel Haklar Şartı'nın 8. maddesinde kişisel verilerin korunması başlığı altında "*Herkes, kendisini ilgilendiren kişisel verilerin korunması hakkına sahiptir. Bu veriler, adil bir şekilde, belirli amaçlar için ve ilgili kişinin rızasına veya yasa ile öngörülmüş diğer meşru bir temele dayanarak tutulur. Herkes, kendisi hakkında toplanmış verilere erişme ve bunları düzelttirme hakkına sahiptir. Bu kurallara uyulması, bağımsız bir makam tarafından denetlenir*" ifadesi bulunmaktadır [17].

Kişisel verilerin korunmasına yönelik dünyada yapılan çalışmaların tarihsel sürecine bakıldığında, 1970 yılında Almanya'da *Verilerin Korunması Kanunu* çıkarılmış [18], 1970 yılının sonunda Lüksemburg'da kişisel verilerin korunmasına yönelik bir düzenleme yapılmıştır. 1973 yılında İsveç'te verilerin korunmasına ilişkin kanun çıkartılmış, 1974'te Amerika'da özel alanın korunmasına ilişkin kanun kabul edilmiştir. Bu kanunlara ek olarak, 1977 yılında Kanada'da *İnsan Hakları Kanunu* ve 1978 yılında Fransa'da *Elektronik Veri İşlenmesi, Veriler ve Özgürlük Hakları*na ilişkin kanun çıkarılmıştır. Aynı süreçte; İsviçre, Danimarka ve Norveç'te de verilerin korunmasına ilişkin yasal düzenlemeler yapılmıştır [19]. 1980 yılında OECD tarafından kişisel veri toplanması ve işlenmesi [6] ile ilgili sözleşme kabul edilmiş, 1981 yılında da Avrupa Konseyi, verilerin korunmasına yönelik olan 108 numaralı sözleşmeyi [20] kabul etmiştir. Bu sözleşmeler birçok sözleşmeye rehber olmuş, birçoğu yeniden gözden geçirilmiştir. Avrupa Birliği; AB 95/46/EC numaralı direktifi, 108 Numaralı Sözleşme, OECD Rehber ilkeleri gibi çalışmalar ile kişisel verilerin mahremiyetinin korunması alanında temel alınacak çeşitli çalışmalar ortaya çıkarmıştır [21].

B. Kişisel Sağlık Verisi, Erişimi, Kullanımı ve Korunması

Kişisel sağlık verisi kavramı, kişisel veri kavramı içinde yer almaktadır. Tedavinin sürekliliğinin sağlanmasında önemli bir payı olan kişisel sağlık verisi, toplum sağlığına da önemli katkılarda bulunmaktadır. Ayrıca, bilimsel araştırmalara kaynak olmakta ve hukuki durumlar için belge niteliği taşımaktadır. Kabul edilen kanunlar, mevzuatlar, sözleşmeler dâhilinde kişinin, kişisel sağlık verileri ile ilgili hakları; özel yaşama ve aile yaşamına saygı hakkı, sağlık hizmetinden faydalanma hakkı, yaşam hakkı, ifade özgürlüğü, düşünce vicdan ve din özgürlüğü, adil yargılanma hakkı, hakların kötüye kullanılmasının yasaklanması hakkı, hakların kısıtlanmasının sınırlanması hakkı, özgürlük ve güvenlik hakkı ile doğrudan bağlantılıdır [22].

Kişisel sağlık verisinin sahibi durumundaki hastanın hakları, uluslararası alanda ilk olarak 1981 yılında Lizbon'da imzalanan Dünya Hekimler Birliği (DHB) Hasta Hakları Bildirgesinde ele alınmıştır. Bu bildirge, 1995'te Bali'de yenilenmiş, son olarak ta 2005 Santiago Bildirgesi'yle geliştirilmiştir. Washington'da 2002 yılında yapılan Dünya Hekimler Birliği (DHB) [23] Genel Kurulu'nda kabul edilen bildirgede kişisel sağlık bilgileri; "*Kişinin bedensel ya da zihinsel sağlığına ilişkin kayıt edilmiş tüm bilgilerdir*" olarak tanımlanmaktadır. Kişisel veri olarak, kişinin kimlik ve sağlık bilgileri yanı sıra hücre, uzuv, kan ve DNA gibi bilgileri de önemlidir. Kasım 2002 tarihli Avrupa Birliği Hasta Haklarına İlişkin Avrupa Statüsü Ana Sözleşmesi Temel Dokümanı 6. Maddesinde [24] "*Özel ve Gizlilik Hakkı*" başlığı altında; "*Her birey kişisel bilgilerinin; sağlık durumu, yapılan teşhis ve tedavi konularında bilginin yanı sıra teşhis ve tedavi yapılırken veya özel ziyaretlerinin gizliliğinin muhafazası hususunda, gizli tutulmasını talep etme hakkına sahiptir*" tanımı yer almaktadır.

Türkiye Cumhuriyeti Sağlık Bakanlığı Hasta Hakları Yönetmeliği "*Mahremiyete Saygı Gösterilmesi*" başlıklı Madde 21'e bakıldığında [25], kişisel sağlık bilgileri ile ilgili olarak: "*Hastanın, mahremiyetine saygı gösterilmesi esastır. Her türlü tıbbi müdahale, hastanın mahremiyetine saygı gösterilmek suretiyle icra edilir. Mahremiyete saygı gösterilmesi ve bunu isteme hakkı;*

1) *Hastanın, sağlık durumu ile ilgili tıbbi değerlendirmelerin gizlilik içerisinde yürütülmesini,*
2) *Muayenenin, teşhisin, tedavinin ve hasta ile doğrudan teması gerektiren diğer işlemlerin makul bir gizlilik ortamında gerçekleştirilmesini kapsar"* tanımı yer almaktadır.

Sağlık Bakanlığı tarafından hazırlanan, kamuoyunun bilgisine ve görüşüne sunulan "Kişisel Sağlık Verilerinin İşlenmesi ve Veri Mahremiyetinin Sağlanması Hakkında Yönetmelik Taslağı [26]"nın amacı; kişisel sağlık verilerinin kayıt altına alınabilmesi, veri mahremiyetinin sağlanması, işlenmesi ve işleyecek gerçek ve tüzel kişilerin uyacakları esas ve usulleri belirlemektir. Ancak, Sağlık Bakanlığı'nın kişisel sağlık verilerini hangi şartlarda tutacağı belirtilmemiştir. Bu taslak kapsamında, Sağlık Bakanlığı en büyük veri toplayan kurum olarak görülmektedir. Bu durumda, kişisel sağlık verilerinin gereğinden uzun saklanmasının önüne geçmek ve suiistimalleri önlemek için gerekli düzenlemelerin yapılması ve sınırların belirlenmesi gerekmektedir.

Bilgi güvenliği konusunda ki diğer bir önemli çalışma olan ISO 27000 ailesi, oldukça kapsamlı süreçleri içermektedir [27]. ISO/IEC 27001:2005, *Bilgi Güvenliği Yönetim Sistemi* için özellikleri belirlerken ISO/IEC 27002:2005 *Bilgi Güvenliği Yönetimi* için uygulama kodu niteliğindedir. ISO 27799:2008 standardı ise, sağlık bilişimi için bir standarttır. Sağlık sektöründe bilgi güvenliği yönetiminin gerçekleştiriminde ISO/IEC 27002 kullanılarak düzenlenmeler gerçekleştirilmektedir [28].

Amerika Birleşik Devletleri'nde sağlık sektöründeki bilgi ve bilgi akışının güvenliğini oluşturmak ve devamlılığını sağlamak için 1996 yılında kabul edilen ve uygulanmaya başlanan HIPAA'ya (Health Insurance Portability and Accountability Act) göre sağlık bilgisi, sağlık hizmeti servisleri, halk sağlığı otoriteleri, sigorta firmaları, sağlık hizmetinde bulunan profesyoneller tarafından üretilen ya da elde edilen ve hayatın tüm dönemi için fiziksel veya ruhsal sağlık ile ilişkili olan herhangi bir bilgidir [29]. Özetle; kişisel sağlık bilgileri, kişinin doğumundan ölümüne kadar geçen süreyi kapsayan sağlık bilgilerinin tümüdür.

Kişisel veriler açısından sağlık sektöründe uygulanan prensipler genel prensiplere paraleldir. Sağlık uzmanları için Sağlık Hizmetlerinde Mahremiyet ve Gizlilik Üzerine Avrupa Rehberi'nde (European Guidance for Healthcare Professionals on Confidentiality and Privacy in Healthcare) kişisel sağlık verileriyle ilgili olarak hastanın bilgilendirilmesi, rıza/onam alınması, seçim hakkı, hasta kimliğinin gizlenmesi ve anonimleştirme, bilgi açıklamasını gerektiren durumlar, güvenlik, erişim ve düzeltme maddeleri tanımlanmaktadır [30].

Kişisel sağlık verisi, kişinin tedavisinin sürekliliği için ne kadar gerekli ise, istatistiksel ve bilimsel amaçlar için de aynı derecede gereklidir. Bu doğrultuda sağlık verisine, veri örneklerine ve laboratuar sonuçlarına erişim isteği gerekliliği ve bu veriler üzerinde araştırma yapma ihtiyacı da her geçen gün artmaktadır. Kaynaklara erişim denetiminin gerçekleştirimi, kişisel hakların korunmasının sağlanmasında önemli ve gerekli bir denetimdir. Araştırma ve geliştirme için kullanılan veri kümeleri ne kadar fazla veri içerirse, elde edilen sonuçların geçerliliği ve genelleştirilmesi de etkili olacaktır. Bu nedenle, hasta verilerinde kişisel mahremiyetin korunması ve veri güvenliğinin sağlanması hakkı dâhilinde araştırmalar için kullanılacak sağlık verisinin kullanımının maksimizasyonu ile gizlilik ve güvenlik dengesinin kurulması önemlidir.

Türkiye'de tüm sağlık kurumları, tek bir çatı altında toplanmış olup, 2006 yılından itibaren Sosyal Güvenlik Kurumu (SGK) güvencesiyle hizmet alan kişilerin bilgileri elektronik ortamda (MEDULA) [31] tutulmaya başlanmıştır. 2012 yılı itibariyle, e-reçete sistemine geçilmiş ve kişilerin ilaç bilgileri de saklanmaya başlanmıştır. SGK, anlaşmasız kurumlar/muayenehanelerden hasta verilerini almak için, ayrı bir sistem tasarlamıştır (Sağlık2NET) [32]. Bu sistem 2013 Ağustos'ta yasalaşmış ve uygulamaya alınmayı beklemektedir.

Türkiye'de sağlık hizmetinin özelleştirilmesine bağlı olarak Sosyal Güvenlik Kurumu'na MEDULA sistemi kapsamında gönderilen veriler incelendiğinde, özel sağlık sektörü de kişisel sağlık verilerine en az %35 oranında sahip bulunmaktadır [33]. Ulusal özel sağlık sektörünün uluslararası sermaye ile ortaklıklarının artması ve yönetimlerinin uluslararası sermaye lehine değişmesi sonucu, bu bilgiler tümü ile uluslararası sermayenin de kontrol ve kullanımına geçmiş bulunmaktadır.

Türkiye'de, kişilerin sağlık hakkıyla ilgili pek çok dava Avrupa İnsan Hakları Mahkemesine taşınmış ve Türkiye, kişinin yaşam hakkını korumak için gerekli sistemi oluşturamadığı gerekçesiyle mahkûm olmuştur [34]. Hasta haklarının korunması kapsamında kişisel sağlık verilerinin gizliliği ve güvenliğinin sağlanması ile hasta güveni ve memnuniyeti ile başlayan ve sonrasında sağlık kurumuna ulaşacak olan olumlu etki, ülke çıkarları bağlamında zaman tasarrufu ve ekonomik kazanımlar sağlayacaktır.

Kişisel sağlık verileri kapsamında olan kişinin sağlık durumuna ilişkin genel veriler, kişiye uygulanan tedaviye ilişkin veriler ve tedavi sonrasını kapsayan süreç için öngörülen durumlar gizli olmalı ve korunmalıdır. Sağlık Bakanlığının 2005 yılında yayınladığı "Veri Güvenliği Genelgesi" adlı genelgede [35] verilerin kullanımıyla ilgili "*verilerin hastanın izni olmadan başka kurumlara/şahıslara verilmemesi*" gibi esaslar getirilmiş ve bu esasların uygulanmasına yönelik olarak da "*Kurumda kimin hangi yetkilerle hangi verilere ulaşacağı çok iyi tanımlanmalıdır. Rol tabanlı yetkilendirme yapılmalıdır ve yetkisiz kişilerin hastanın sağlık kayıtlarına erişmesi mümkün olmamalıdır.*" maddesiyle açıklama yapılmıştır. HIPAA güvenlik kurallarına göre [36]; kişisel sağlık bilgilerinin gizliliği, bütünlüğü ve erişilebilirliği garanti altına alınmalıdır. Bu nedenle, kişisel sağlık bilgilerinin bütünlüğünü tehdit edici ve/veya mahremiyetini tehlikeye sokacak her türlü izinsiz erişime karşı önlemler alınmalıdır.

Kişisel sağlık verileri açısından evrensel ilke her zaman kişinin hak ve özgürlüklerinin korunmasının ön planda

olmasının gerektiğidir. Dünya standartlarında kişisel sağlık verileri, kişisel veri kategorisi içinde kritik ve özel niteliği olan veriler kategorisinde yer bulmaktadır.

III. DEĞERLENDİRME

E-dönüşüm sürecinde kritik önem taşıyan sağlık verilerinin dijital ortama taşınması ile hasta ve tedavi bilgileri kâğıt tabanlı formattan çıkarak dünyanın her noktasından kolayca ulaşılabilir olmuş, elektronik sağlık kayıtları da tıp bilişimi alanında ön plana çıkan önemli konular arasına girmiştir. Dijital ortama geçiş ile birlikte kalite ve verimin artması, iş akışının otomatize olması, hasta tedavi ve bakımının iyileştirilmesi, acil durumlarda hasta bilgilerine hızlı ulaşım, daha iyi bir dokümantasyon, yasal bilgi ve belge oluşturmada kolaylık, sağlık hizmetinin daha iyi planlanabilmesini gibi birçok kazanım sağlanmıştır. Ancak, bu kazanımların karşısında da hasta mahremiyetinin ihlali ve kişilerin maddi, manevi ve sosyal yönden zarar görmesi, kişisel bilgilerin kişilerin haberi olmaksızın çeşitli ortamlarda ifşa edilebilmesi, sisteme güven duygusunda ki azalmaya bağlı hastanın bilgilerini saklaması ve tedavinin bu durumdan etkilenmesi, toplanan verilerin metalaştırılarak alınıp, satılabilir bir duruma gelmesi ve verilerin amaç dışı kullanımı gibi çok kritik riskler ortaya çıkmaktadır. Temel hak ve hürriyetlerin öneminin giderek arttığı ve kişilerin bilinçlendiği günümüzde de, kişisel bilgilerin gizliliği dâhilinde bu riskleri minimize etmek için ülke ve sağlık kurumları bazında ve uluslararası çapta tanımlar yapılmakta, standartlar belirlenmekte, çözümler önerilmektedir.

Bu tanımlamaların en başında, Sağlık Bilgi ve Yönetim Sistemleri Topluluğu (Healthcare Information and Management Systems Society, HIMSS) Elektronik Sağlık Kaydı (ESK) tanımını [37]: "*Hasta sağlık bilgilerinin herhangi bir sağlık kuruluşunda bir veya birden çok kuruluş tarafından oluşturulmuş boylamsal (dikey) elektronik kayıtlardır. Bu bilgiler kapsamında hastanın cinsiyeti, ilerleme notları, sorunları, tedavileri, yaşam belirtileri, geçmiş tıbbi bilgileri, bağışıklıkları, laboratuar verileri ve radyoloji raporları girmektedir*" olarak vermektedir. Sağlık Bakanlığı tarafından duyurulan bir sertifikada [38], ESK' nın dijital çağ ile birlikte yaşamımıza giren kavramlardan biri ve de en önemlisi olduğundan bahsedilmektedir.

Her türlü kayıtta olduğu gibi, elektronik sağlık kaydında da kişisel sağlık verilerinin gerçek sahibi kişidir. Kişinin sağlık hizmeti aldığı kurumlar açısından sağlık hizmetini veren kurum ya da kişi (hekim) olma durumu kişisel sağlık verilerinin üzerinde "sahip olma" hakkını oluşturmamaktadır. Sağlık hizmeti gerek kişinin doğrudan kendi ödemesi sonucu, gerekse de vergilendirme yöntemi ile almış olduğu bir hizmettir. Her iki durumda da kurumsal haklar kişisel hakların önüne geçmemelidir. Tüm sağlık kurumlarının ve ilgili personellerin kişisel hakları tanıma ve destekleme ve hatta kişilerin mahremiyetini sağlama konusunda sorumlulukları bulunmaktadır. Santiago'da 2005 yılında yapılan Dünya Hekimler Birliğinde ortaya çıkan Hasta Hakları Bildirgesinin gizlilikle ilgili 8. Maddesi [39] "Hastanın sağlık durumu, tıbbi durumu, tanısı, hastalığın seyri ile ilgili tahmini, tedavisi ve kişiye özel diğer tüm bilgiler ölümden sonra bile gizli olarak korunmalıdır" ifadesine yer vermektedir. 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanununa [40] göre, Sosyal Güvenlik Kurumu (SGK) MEDULA [31] sistemi ile hizmet alımı sonucu ödeme kapsamı dâhilindeki kişilerin kişisel sağlık bilgilerini elektronik ortamda kayıt altına almaktadır. Sağlık Bakanlığı kendine bağlı ya da denetiminde bulunan sağlık kurumlarından GEBLİZ, AşıNet, 15-49 Yaş Kadın İzlem gibi formlar ile hastaların sağlık verilerine ek olarak kişisel bilgileri de toplamaktadır. Kamu ve özel sağlık kuruluşlarından da SağlıkNET [32] kapsamında bilgiler bakanlığa gönderilmektedir. Tutulan tüm kişisel sağlık verileri, Sağlık Bakanlığı, SGK, hekimler, eczaneler, laboratuvarlar ve çalışanları, adli süreç kapsamında adli makamlar tarafından da kolaylıkla izlenebilmektedir. Veri miktarı hızlı bir şekilde artarken, veriye erişim imkânı da yoğun ve kolay bir şekilde gerçekleşmektedir. *Kişisel Verilerin Korunması Kanun Tasarısı* [4], halen kanunlaşmayı beklemektedir. Türkiye Cumhuriyeti hukuk sisteminde tek genel düzenleme Türkiye Cumhuriyeti Anayasası olup, Türk Ceza Kanunu ve Medeni Kanun ile de kişisel verilerin korunmasına aykırı davranışlara ilişkin genel hükümler belirtilmektedir. Günümüzde, genel olarak düzenlenen bir "Kişisel Verilerin Korunması Hakkında Kanun" mevcut değildir ve AB mevzuatına uyum içinde genel bir kanuni düzenlemeye acil olarak ihtiyaç duyulmaktadır.

IV. SONUÇ

Verilerin elektronikleşmesi sürecinin olumlu yanlarının yanında, olumsuzlukları da aynı derecede önem taşımaktadır. Sürecin hukuki bağlamda kurallara bağlanması, gizliliğinin ve güvenliğinin sağlanması ve kontrol edilebilmesi konusunda yönetmeliklerin oluşturulması ve teknolojik düzenlemelerin gerçekleştirilmesi ihtiyacı doğmaktadır. Ancak, yaşanan bazı olaylara ve alınan tüm tedbirlere rağmen olumsuzlukların tümüyle ortadan kalkmasının mümkün olmadığı tartışmaları da sürmektedir. Hukuk alanındaki gelişmeler ve düzenlemeler, bilim ve teknolojideki kadar hızlı olamamaktadır. Bu durum, elektronik ortamda tutulan kişisel sağlık verilerinin gizliliği, güvenliği, güvenilirliği, işlenmesi ve saklanması konularında çeşitli aksaklıkları beraberinde getirmektedir.

Türkiye Cumhuriyeti Sağlık Bakanlığı, hasta mahremiyeti konusunda MEDULA sistemi ile sağlık verisi toplayan diğer birçok sağlık kurumuna göre daha hassas davranmaktadır. Sağlık Bakanlığı tarafından, 2005 yılında yayınlanan Veri Güvenliği Genelgesi [41] son yıllarda detaylandırılarak güncellenmiştir. Hukuk ve tıp bilişimi alanlarında yürürlükte olan kanunlar ve Avrupa Birliği kriterleri ile birlikte yapılan çalışmalar sınırları belirlemekte, yasallaştırmakta ve pratiğe geçirilmesi için yönlendirmelerde bulunmaktadırlar. Teorik anlamda yapılan bu çalışmaların uygulamaya geçmesiyle birlikte bireylerin, kişisel verilerin gizliliği ve güvenliği konusunda bilinçlenip sistemi desteklemeleri bu sürece ivme kazandıracaktır.

KAYNAKLAR

[1] Directive 95/46/EC of The European Parliement and of The Council, Available: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1995:281:0031:0050:EN:PDF
[2] Türkiye Cumhuriyeti Anayasası, Available: http://global.tbmm.gov.tr/docs/constitution_en.pdf
[3] Avrupa İnsan Hakları Sözleşmesi, Avrupa Antlaşmaları Serisi, no. 5, Available: http://www.echr.coe.int/Documents/Convention_2014_1_TUR.pdf
[4] Kişisel Verilerin Korunması Hakkında Yasa Tasarısı md.3/ç., Available: http://www2.tbmm.gov.tr/d23/1/1-0576.pdf
[5] Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair 108 Numaralı Avrupa Konseyi Sözleşmesi, Available: http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm
[6] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Available: http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm
[7] E. McCallister, T. Grance, and K. Scarfone, "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)", Recommendations of the National Institute of Standards and Technology, *NIST Special Publication 800-122*, April 2010.
[8] Kişisel Sağlık Verilerinin Korunması Bir Haktır, Available: http://www.ttb.org.tr/index.php/Haberler/ksv-4171.html
[9] AHİM, K.U. v. FINLANDIYA DAVASI (Başvuru no: 2872/02), Available: http://hudoc.echr.coe.int/sites/eng/pages/search.%20aspx?i=001-89964
[10] Avrupa İnsan Hakları Mahkemesi, Küçüklerin Korunması, Available: http://www.inhak.adalet.gov.tr/tematik/cocuklar/kucuklerin_korunmasi.pdf
[11] AHİM, Z v. FİNLANDİYA (Başvuru no. 22009/93), Available: http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-58033
[12] Protection of personal data, Available: http://www.echr.coe.int/Documents/FS_Data_ENG.pdf
[13] D. Elgesem, "The structure of rights in Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and the free movement of such data," Ethics and Information Technology, vol. 1, no. 4, pp. 283-293, 1999.
[14] Sağlık Hizmetlerinde Kişisel Veri Toplanması Hakkında TPD Hasta Mahremiyeti Görev Grubu Raporu, Available: http://78.189.53.61/-/49UPK/Sunu/huseyin_soysal.pdf
[15] 5237 sayılı Türk Ceza Kanunu md. 135 vd., Available: http://www.tbmm.gov.tr/kanunlar/k5237.html
[16] Türk Medeni Kanunu, Available: http://www.tbmm.gov.tr/kanunlar/k4721.html
[17] Avrupa Birliği Temel Haklar Şartı md. 8, Available: http://www.europarl.europa.eu/charter/pdf/text_en.pdf
[18] M. D. Birnhack, "The EU Data Protection Directive: An Engine of a global regime", in *Elsevier Computer Law and Security Report*, 2008, vol. 24, pp. 511.
[19] Ç.Z. Ünsal, "Google'ın Yeni Gizlilik Politikası Google Inc. Tarafından 1 Mart 2012 Tarihinde Yayımlanan Politikasının Kişisel Verilerin Korunması İlkeleri İle Uyumluluğu Ve Avrupa Birliği'nin 95/46/Ec Sayılı Veri Koruma Direktifi Açısından Değerlendirilmesi", *Hacettepe Hukuk Fakültesi Dergisi*, 3(1) 2013, 99–124.
[20] Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşme, Available: http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm
[21] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 1981, Available: http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm
[22] Sağlık Hizmetlerinde Kişisel Veri Toplanması, Korunması Ve Değerlendirilmesi, Available: http://www.kisiselsaglikverileri.org/hakkinda.php?id=32
[23] WMA General Assembly, Washington, DC, USA, October 2002.
[24] European Charter of Patients' Rights Basis Document*, Rome, November 2002.
[25] Hasta Hakları Yönetmeliği, Available: http://www.haksay.org/?q=node/18
[26] "Kişisel Sağlık Verilerinin İşlenmesi ve Veri Mahremiyetinin Sağlanması Hakkında Yönetmelik Taslağı", *T.C. Sağlık Bakanlığı*, Available: http://www.saglik.gov.tr/TR/belge/1-17634/kisisel-saglik-verilerinin-islenmesi-ve-veri-mahremiyet-.html
[27] An Introduction To ISO 27799 (ISO27799), Available: http://www.27000.org/iso-27799.htm
[28] Kişisel sağlık verilerinin Elektronik İletişim Yöntemleriyle İletimi, standartları ve çözüm yolları, Available: http://www.saglikbilisimdernegi.org/makaleler.php?mak_id=20
[29] Protected Health Information: What Does PHI Include?, *HIPAA*, Available: http://www.hipaa.com/2009/09/hipaa-protected-health-information-what-does-phi-include/
[30] R. McClelland ve C.M. Harper, "European Guidance for Healthcare Professionals on Confidentiality and Privacy in Healthcare".
[31] Medula, Available: http://www.saglik.gov.tr/TR/belge/1-29730/medula.html?vurgu=medula
[32] SağlıkNET, Available: http://www.e-saglik.gov.tr/SaglikNet/SaglikNetHakkinda.aspx
[33] A. Altay, "Sağlık Hizmetlerinin Sunumunda Yeni Açılımlar Ve Türkiye Açısından Değerlendirilmesi", *Sayıştay Dergisi*, Sayı 64.
[34] I.Sağlık Hukuku Sempozyumu İzmir Üniversitesi'nde, Available: http://sbe.izmir.edu.tr/haberler/item/253-i-sa%C4%9Fl%C4%B1k-hukuku-sempozyumu-izmir-%C3%BCniversitesi-nde-d%C3%BCzenlendi.html
[35] Veri Güvenliği Hakkında Genelge 2005/153, Available: http://sbsgm.saglik.gov.tr/belge/1-24386/veri-guvenligi-hakkinda-genelge-2005153.html
[36] "An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountabilit Act (HIPAA) Security Rule", *National Institiue of Standarts and Technology*, USA, 2008.
[37] Health Care Information and Management System Society (HIMSS), Available: http://www.himss.org/library/ehr/?navItemNumber=13261
[38] G. Öğütçü, N. A. G. Köybaşı, ve S. Cula, "Elektronik Sağlık Kayıtlarının İçeriği, Hassasiyeti ve Erişim Kontrollerine Yönelik Farkındalık ve Beklentilerin Değerlendirilmesi", 2011.
[39] World Medical Association Declaration of Lisbon on The Rights of The Patient, *The World Medical Association*, INC, Santiago, 2005, Available: http://dl.med.or.jp/dl-med/wma/lisbon2005e.pdf
[40] Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu, 31.05.2006, Available: http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5510.pdf
[41] Veri Güvenliği Hakkında Genelge 2005/153, Available: http://sbsgm.saglik.gov.tr/belge/1-24386/veri-guvenligi-hakkinda-genelge-2005153.html

Emre OLCA 2013 yılından itibaren İzmir Üniversitesi Yazılım Mühendisliği Bölümünde Araştırma Görevlisi olarak çalışmaktadır. Yüksek Lisansını Dokuz Eylül Üniversitesi Bilgisayar Mühendisliği Bölümünde, "An e-Sign Tool For Document Delivery" isimli tez ile tamamlamıştır. Doktorası Ege Üniversitesi Bilgisayar Mühendisliği Bölümünde devam etmektedir.Veri Mahremiyeti ve Güvenliği, Anlamsal Web, Ontoloji, Yazılım Geliştirme Süreçleri alanlarında çalışmalarını sürdürmektedir.

Özgü CAN 2011 yılından itibaren Ege Üniversitesi Bilgisayar Mühendisliği Bölümü Yazılım Ana Bilim dalında Yardımcı Doçent olarak çalışmaktadır. Doktorasını aynı bölümde, "Anlamsal Web için Kişiselleştirilebilir Ontoloji Tabanlı Erişim Denetimi ve Politika Yönetimi" isimli tez ile tamamlamıştır. Yüksek Lisansını "Asal Sayı Örüntüleri ve Goldbach Sanısı Üzerine Bir Çalışma" isimli tez ile 2002 yılında Ege Üniversitesi Uluslararası Bilgisayar Enstitüsü'nde yapmıştır. Anlamsal Web, Politika Yönetimi, Erişim Denetimi, Bilgi Güvenliği, Veri Anonimleştirme ve Kişiselleştirme konularında akademik ilgi alanına sahiptir.