**HASTA VERİLERİNİN GİZLİLİĞİ**

**VE**

**BÜYÜK VERİ İLE GÜVENLİĞİN SAĞLANMASI**

Fatma zehra atak

Kırıkkale üniversitesi, bilgisayar mühendisliği

Gazi üniversitesi sağlık bilişimi tezli yüksek lisans program öğrencisi

atakfatmazehra@gmail.com

ÖZET

Bu çalışmada sağlık sektöründe meydana gelen kişisel veri gizliliği ve hasta veri mahremiyeti sorunu ele alınmıştır. Hasta - hekim ilişkisi incelenmiş ve hastanın kişisel veri güvenliğine odaklanılmıştır. Veri gizliliği ve güvenilirliğinin arttırılması için büyük veri konusu araştırılmıştır. Büyük verinin tanımı yapılmış ve olumlu olumsuz yönlerinden bahsedilmiştir.

Anahtar Sözcükler: Mahremiyet, gizlilik, kişisel veriler, kişisel veri güvenliği, hassas veriler, büyük veri, kişisel verilerin işlenmesi

ABSTRACT

Personal data privacy and patient data privacy issues in the healthcare industry have been addressed in this study. The patient - physician relationship was examined and focused on personal data security. The subject of big data has been investigated, in order to increase data privacy and reliability. Big data is defined and its positive aspects are mentioned.

Keywords: Privacy, secrecy, personal data, personal data security, sensitive content data, big data, processing personal data

1. GİRİŞ

Genel konu başlığımız olan hasta verileri ve hasta veri gizliliği farklı alanlar gibi anlaşılsa da aslında birbiriyle tamamen iç içe konulardır. Bu çalışmada kişisel veri gizliliği ve hasta mahremiyeti birbiriyle ilişkili şekilde ele alınmıştır.

Hekimler tıp fakultesinden mezun olurken hipokrat yemini ederler.hipokrat yemini’nde hekimler hastaların mahrem bilgilerinin açıklamayacaklarına, bu bilgileri sır olarak saklayacaklarına dair şu ifadeleri söylerler “*...insan hayatına mutlak surette saygı göstereceğime,mesleğim dolayısıyla öğrendiğim küçük sırları saklayacağıma..*.”[1]. Bu yemin ile meslek hayatlarına başlarlar. Hastalar kişisel bilgilerin hatta çoğu zaman özel hayat sırlarını bile hekimleri veya sağlık çalışanları ile paylaştıkları için yemin etmeleri önemlidir. Hasta mahremiyetine önem verilmediği durumlarda, hasta ve herhangi bir sağlık çalışanı arasındaki ilişkilerde güven azalımı yaşanmaktadır. Güven bağı sarsıldığında artık hasta özel bilgilerini sağlık çalışanları ile paylaşmaktan kaçınır.

Hekim hasta ilişkisi kutsaldır. Hekim hasta arasındaki ilişkinin mahremiyeti, tedavi için önemli bir koşuldur. Tedavi de üçüncü kişinin müdahalesinden kaçınılması gerekmektedir. Lakin bazı zamanlarda birden çok bölümün ortak tedavi uygulaması gerektiği durumlarda üçüncü veya daha fazla hekim ile beraber tedavi süreci yönetilir. Bu duruma sağlık çalışanları açısından bakdığımızda hasta mahremiyetini korumak kolay bir konu değildir.

Kişi sağlık bilgilerinin elde edilmesi, korunması, saklanması birer hassas veridir. Hassas verilerin güvenliği çok önemldir. Hassas veriler kişişel verilere göre daha özele indirgenmiş olup kişinin daha özenli saklamak istediği verilerdir. Hassas veriler, kişinin temel haklarını, sağlık yaşamını, özel hayatını ve cinsellik gibi konularını kapsamaktadır.

Hassas kişisel veriler kötüye kullanıldıklarında temel hak ve özgürlüklere yönelik önemli riskler taşıdıklarından dolayı daha özenli bir korumaya tabi tutulmalıdır. Bu veriler hastanın öğrenmesini istemediği yakınlarından birine ya da kötü amaç için kullanacak birinin eline geçtiğinde hasta toplumdan dışlanma, itibar kaybetme veya ayrımcılığa uğrama sorunlarıyla karşılaşabilir. Bu ihtimallerin gerçekleşmemesi için oldukça dikkatli davranmak gerekir.

1. GİZLİLİK , MAHREMİYET, KİŞİSEL VERİ, KRİPTOGRAFİ VE ŞİFRELEME, ANONİMLEŞTİRME KAVRAMLARI[10]

* Gizlilik (confidentiality), sözlükte “gizli olma durumu, mahremiyet” Olarak tanımlanmaktadır. Bu anlamının yanı sıra detaylı sözlükte ise “hekimin mesleğini ve sanatını uygularken öğrendiği bilgileri, hayvan sahibinin onamı ve yasal zorunluluk gibi durumlar dışında, saklı tutma yükümlülüğü, sır saklamak ilkesi” olarak geçmektedir.
* Mahremiyet (privacy), zamana göre kültüre göre hatta bazen bireye göre bile değişkenlik göstermektedir. Bu değişkenliği genel olarak tanımlamak gerekir. Mahremiyet kelimesi ise mahrem kökü ile arapçadan gelmektedir. Türkçe sözlükte “gizlilik, mahrem olma durumu” olarak tanımlanırken arapça sözlükte anlamı “ birisinin hususi hâllerine ait gizli sır. Gizli olan,herkese söylenmeyen, gizli sır.” olarak geçmektedir[2].
* Kişisel veri(personel data), kanunda “*kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi*” olarak tanımlanmıştır. Ilk öncelik kişinin gerçek olmasıdır. Daha sonra kişinin her alanda kendine ait özel hissettiği her veri veya bilgi o kişinin sahsi verileridir. Örneğin kimlik numarası, cep telefon numarası, e-posta adresi, parmak izi, kişisel özel veriler ve benzeri bilgiler bir kişinin kişisel verileridir.
* Kriptografi, veriyi gizleme bilimidir. Kriptografi ile saklanması istenen veri şifrelenir (encryption) ve üçüncü sahışlar tarafından görüntülenemez. Şifreli veriyi sadece hedeflenen kişi okuyabilir. Güvenlik sistemidir.
* Anonimleştirme (anonymization), veriler kriptografi bilimi ile şifrelenirken gönderici ve alıcının kimliklerini saklamaya yarayan bir yöntemdir. Burada ki amaç kişilerin mahremiyetini korumaktır.

1. MAHREMİYET BOYUTU (PRICVACY SIZE)

Sağlıkta kalite standartları (sks)’ın da ise hasta mahremiyetinin boyutları şu şekilde sıralanmıştır[2]:

* Bilişsel mahremiyet: “bireyin kişisel bilgilerine başkaları tarafından ulaşılma durumunu kontrol edebilmesidir. Bireyin kendisiyle ilgili bilgileri nasıl, ne zaman ve ne ölçüde açığa vurabileceğine karar verme hakkıdır.”
* Fiziksel mahremiyet: “bedensel mahremiyetin de ele alındığı, bireyin kendi çevresindeki fiziksel alan üzerindeki kontrolü ile ilişkilidir. Diğer bireylerle fiziksel teması, bu temastaki yakınlığı içerir. Ayrıca, bireyin vücudunu çevreleyen, başkaları tarafından görünmeyen gizli alanları ve evi, iş yeri gibi fiziksel alanları üzerindeki kontrolünü, yani kişisel egemenlik alanını kapsar.”
* Psikolojik mahremiyet: “bireyin değerleri, inançları ve onu etkileyen diğer konulardaki bilgileri kontrol etme, düşünce ve duygularını, hangi koşullar altında ve kiminle paylaşacağına karar verme hakkını kapsar.”
* Sosyal mahremiyet: “bireyin, sosyal ilişkilerinin yönetimi, yani ilişkinin tarafları, sıklığı ve etkileşimine ilişkin kontrolünün olmasıdır. İnsanları bireysel ve grup olarak değerlendirmeyi, kültürel özellikleri göz önünde bulundurmayı gerektirir. Çeşitli kültürlerde bu nedenle mahremiyet kapsamı, önemi ve mahremiyeti sağlama yöntemleri farklılık göstermektedir. Batı ve doğu toplumlarının, çeşitli dinsel grupların, modern ve geleneksel toplumların mahremiyete ilişkin değerleri, inançları ve beklentileri arasında farklılıklar bulunmaktadır” (sağlık bakanlığı 2015).

1. KİŞİSEL VERİ TARIHÇESI (PERSONEL DATA HISTORY)

Gerçek bir kişinin, dünyada kişilik gizlilik hakları ile ilk beyanneme İnsan hakları evrensel bildirgesinde 10 aralık 1948 tarihinde gündeme gelmiştir.bildirgenin 12.maddesi ile kamu oyuna duyrulmuştur. Madde 12 “hiç kimsenin özel yaşamına, ailesine, evine ya da yazışmasına keyfi olarak karışılamaz, onuruna ve adına saldırılamaz. Herkesin, bu gibi müdahale ya da saldırılara karşı yasa tarafından korunma hakkı vardır.” dir.

Dünya sağlık örgütü, 1964 yılında yayımlanan helsinki deklerasyonunda hasta haklarını daha da geliştirmiştir. 21.madde ye göre ; “*araştırmaya katılan hastanın/deneğin kendi bütünlüğünü koruma hakkına her daim saygı gösterilmelidir. Hastanın/deneğin gizliliğini ve bilgi mahremiyetini sağlamak için ve hastanın fiziksel ve ruhsal bütünlüğü ve kişiliği üzerine yapacağı etkiyi en az düzeye indirmek için her türlü önlem alınmalıdır.*” İfadesi yer almaktadır.

Birleşmiş Milletler’in Kişisel ve Siyasal Haklar Sözleşmesi’nde kişisel veri haklarından bahsedilmiştir. Sözleşmenin “Mahremiyet Hakkı” başlıklı 17. maddesi şöyledir[3]:

*“1. Hiç kimsenin özel ve aile yaşamına, konutuna veya haberleşmesine keyfi veya hukuka aykırı olarak müdahale edilemez; onuru veya itibarı hukuka aykırı saldırılara maruz bırakılamaz.*

*2. Herkes bu tür saldırılara veya müdahalelere karşı hukuk tarafından korunma hakkına sahiptir*”.

Hasta hakları kavramı ilk olarak 1070li yılların basında dünyada ses getirmiştir. 1990 lı yıllarda ise bildiriler yayımlanmaya baslamıstır. Türkiye de ise 2000li yıllarda konuşulmaya baslandı. 2016 yılında ise kişisel verilerin korunma kanunu ile hayatımıza girmiştir.

1. KİŞİSEL VERİLERİN İŞLENMESİ (PROCESSING PERSONEL DATA)

Kvkk’nin tanımlar başlıklı 3 üncü maddesinde kişisel verilerin işlenmesi şu şekilde tanımlanmaktadır; “*kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem*” Olarak tanımlanmıştır.

Avrupa konseyi’nin 108 nolu sözleşmesi’nde kişisel verilerin işlenmesi şu şekilde tanımlanmaktadır:

“*otomatik işleme, bir bütün veya parçalar halinde otomatik araçlarla gerçekleştirilmesi halinde aşağıdaki işlemleri içerir; verileri saklama, bu veriler üzerinde mantıksal ve/veya aritmetik işlemlerin gerçekleştirilmesi, verilerin değiştirilmesi, silinmesi, verilerin saklama yerlerinden geri alınarak/kurtarılarak yeniden kullanılması veya yayınlanması*.” Olarak tanımlanmıştır.

Telekomünikasyon sektöründe kişisel bilgilerin İşlenmesi ve gizliliğin korunması hakkında yönetmeliğin 3. Maddesinde ise kişisel bilgilerin işlenmesi,[3]

“*otomatik olsun olmasın, toplama, kaydetme, hazırlama, yükleme, uyarlama, değiştirme, geri çağırma, danışma, kullanma, aktarma yoluyla açığa vurma, yayma ya da bunların dışında erişilebilir hale getirme, düzenleme, birleştirme, engelleme, silme gibi yollardan, kişisel bilgiler üzerinden yürütülmekte olan herhangi bir işlem ya da işlemler bütünü*” Olarak tanımlanmıştır.

Sağlık sektöründe ise veri sahibi kişilerinde bu konuda aydınlatılması öncelikle gereklidir. Aydınlatma metinlerinde bu konuların ayrı bölümde açıkça belirtilmesi lazımdır. Eğer hizmet onlie olacakca farklı bilgilendirme hazırlanmalıdır. İşlenecek veriler sağlık verisi olduğundan açık rıza onam formu ve aydınlatma metni farklı olarak hazırlanıp veri sahibi kişilere sunulmalıdır.

Sağlık sektöründe kişisel veri işlemeyi nasıl yapıyoruz?[3]

1. Birincil işleme: Sağlık yada sosyal hizmet sunumu cercevesi. Verinin doğrudan hastadan toplanan yada sonradan hastadan alınan verilerle işlenen veri
2. Ikincil işleme: Daha geniş kapsamda işlenir. Sağlık bakanlıgı veya sgk tarafından sağlık hizmetlerinin planlanması, yönetimi geliştirilmesi. Sağlık verisinin tekrar kullanımını amaçlıyor
3. Üçüncül: Bilimsel veya tarihsel, arşivleme amaclarla kamu yada özel sektör kurulusları tarafından veri işleme karşımıza cıkabilir.sağlık verisinin tekrar kullanımını amaçlıyor.
4. KİŞİSEL VERİ GÜVENLİĞİ (PERSONEL DATA SECURITY)

Sağlık sektöründe son zamanlarda kişisel verilerin güvenli saklanamaması, çalınan verilerin kötüye kullanımı ve teknolojinin gelişmesiyle birlikte yapılan siber saldırılar kişisel veri güvenliğine daha tedbirli yaklaşılması gerektiğini göstermiştir. Sağlık sektöründe ihtiyaç duyulan güvenlik önlemleri git gide daha da artmıştır. Güvenlik üst seviyeye çıkmalı ve verilerin daha korunaklı saklanması elzemdir. Güvenlik tedbirlerinin yanı sıra sağlık çalışanlarına da büyük sorumluluklar düşmektedir. Mesela bu konuda bilinçlenmeleri ve daha duyarlı olmaları gerekmektedir.

1. BÜYÜK VERI (BIG DATA):

Büyük veri nedir?

Çok büyük veri kaynakları ve çok daha fazla karmaşık veri kümeleridir. Bu veri kümelerinin hacimleri o kadar fazladır ki normal veritabanı sistemleri ile yönetilmesi, depolanması veya işlenmesi, analiz edilmesi çokta mümkün olmayan verilerdir. Büyük verinin boyutu ve verimliliği ters orantılır. Diğer sistemlerde çözülemeyecek işler bu sistem ile çözülebilir. Diğer sistemlerin bir süre sonra güvenlik ve gizlilik tedbirleri yeytersiz kaldıgı için büyük veri ortaya cıkmıstır lakin veri arttıkça büyük veri sisteminde de güvenliği ve gizliliği sağlamak zorlaşır. Bu aşamada da yüksek tedbirli kriptografik şifreleme uygulamaları kullanılır.

Büyük veri sağlık alanında, hastalıkların erken teşhisi veya tedavi için ilaç geliştirilmesi gibi benzeri konularda kullanılmaktadır. Büyük veri toplayan kurumlar arasında Sağlık Bakanlığı birinci sırada gözükmektedir. Büyük veri uygulamalarının ortaya çıkmasıyla birey mahremiyetini korumak daha güvenceli hale gelmiştir. Geleneksel yollar malesef yeni çıkan uygulamalar ile güvenliliğini kaybetmeye başlamıştır. Sağlık sektörü büyüdükçe ve içinde bulunduğumuz covid-19 dönemi itibari ile online görüşmeler, tedaviler, muayeneler gün geçtikçe artmaktadır. Teknolojinin gelişmesiyle ve bu artışın gerçekleşmesiyle verilerin güvenliği tehlike arz etmektedir. Tam da bu aşamada büyük veri uygulamaları hayataımızda büyük bir yere sahip olmaya başladı. Elektronik sağlık kayıtları, tele-tıp, e-nabız ve uygulamalar gibi platformlar ile hayatımıza entegre olmaya başladı.[4] Içinde bulunduğumuz bu durumu büyük verinin beş özelliği bu durumu gayet iyi anlatmaktadır.

Literatürde büyük veri için beş özellikten 5v bahsedilir. Araştırmalar 3V olarakta bahseder ama genelde 5V olarak geçer. 3V olarak; çok büyük hacimli (volume) olması, çok çeşitli (variety) olması ve çok hızlı (velocity) olmasıdır. 5Vden bahsedilirken geriye kalan 2V ise; verinin değerli olması (value) ve doğru olmasıdır (veracity). Beş özelliği açıklamak gerekirse[4,9],

1. Variety çeşitlilik: Toplanan verilerin aynı yerde analiz edilebilmesi ve farklı formattaki verilerin birbirine dönüştürülebilmesidir
2. Volum hacim: Gün geçtikçe üretilen veri miktarında büyük bir artış olmaktadır. Bu verilerin işlenmesi, kullanılabilir hale gelmesi ve bilgiye dönüştürülmesi gerekmektedir
3. Velocity hız: Gitgide büyüyen verinin devamlılıgı için hem yazılımsam hemde donanımsal altyapının yeterli hıza ulaşması lazımdır
4. Value deger: Katmanların en önemlisi değer katmanıdır. Anlık karar verme süreçleri buradan yürütülür.
5. Doğru veracity: Verilerin güvenilir olması gerekmektedir. Doğru bilgi içermelidir

Olarak tanımlanmaktadır.

1. BÜYÜK VERİ GÜVENLİĞİ (BIG DATA SECURITY):

Büyük veri güvenliğini sağlamak için geleneksel güvenlik yöntemleri yerine bu platform için yapılmış, uygulanmış sistemleri kullanmak gerekir. Geleneksel yöntemlerin kullanılmamasının sebebi yeni tehditler oluşturmasıdır. Büyük veri sistemlerinde güvenliği maksimum seviyede koruyabilmek için merkezi güvenliğinde kriptografiyi zorunlu kılabilir, veri madenciliği ile korunabilir veya güvenilir veri depolama kullanılabilir.[9]

Büyük veride güvenliği sağlarken bazı zorluklarla karşılaşılabilir. Bunlar en başta gizlilik ve mahremiyet konusudur. Daha sonra güçlü kripto uygulamaları, nitelikli eleman eksikliği, analiz yetersizliği gibi konulardır. Güvenlik tedbirlerinde bu konular yeri geldiğinde yetersiz kalabilmektedir.

1. SONUÇ

Yapılan bu çalışmada hasta mahremiyetinin yeteri kadar korunmaması sonucunda açığa çıkan veri zafiyeti anlatılmıştır. Bu durum karşısında hekim - hasta ilişkisi arasında oluşabilecek güvensizlikten bahsedilmiştir. Bu güvensizlik verilerin yeteri kadar korunmamasından ortaya çıkmaktadır. Verileri daha iyi koruyabilmek için büyük veri uygulamaları konusu incelenmiştir. Büyük veri ile daha önce gizliliği sağlamakta yetemeyen geleneksel çalışma yöntemleri rafa kaldırılmaya başlanmıştır. Büyük veri çalışmaları anlatılmış, en iyi güvenlik sistemlerinden bahsedilmiştir. Bu şekilde hasta mahremiyetine verilen önem gerçekçi olabilecek ve hekim - hasta arasındaki ilişki daha az zarar görerek ilerleme kaydedilebilecektir.

KAYNAKLAR

[1]. Hipokrat yemini

[2]. Özata, Musa / Özer, Kubilay; “ Sağlık Çalışanlarının Hasta Mahremiyeti Konusundaki Tutumlarının İncelenmesi”,Hacettepe Sağlık İdaresi Dergisi,2017;20(1):1-21

[3]. Dülger,Murat Volkan; “Sağlık Hukukunda Kişisel Verilerin Korunması ve Hasta Mahremiyeti”, İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi 1 (2), 2015; 43-80

[4]. Ünsal, Çağrı Zeybek / Büken, Nüket Örnek; “Biyotıp Araştırmaları ile ilgili Olarak, “Kişisel Verilerin Korunması Kanunu” ve “Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelik” Ne Diyor?”, Turkiye Klinikleri J Med Ethics Law Hist-Special Topics 2018;4(1):82-90

[5]. Karaaslan, Enis / Ergin, Ali Murat / Turgut, Nalin / Kılıç, Özgür; “Elektronik Sağlık Kayıtlarının Gizlilik ve Mahremiyeti”

[6]. Kişisel verilerin korunması kanunu

[7]. Sağlık bakanlığı web servisleri veri paketleri

[8]. T.C. Sağlık Bakanlığı Ulusal Sağlık Veri Sözlüğü

[9]. Eyüpoğlu, Can / Aydın, Muhammed Ali / Sertbaş, Ahmet / Zaim, Abdül Halim / Öneş, Onur; “Büyük Veride Mahremiyetin Korunması”, BİLİŞİM TEKNOLOJİLERİ DERGİSİ, CİLT: 10, SAYI: 2, NİSAN 2017

[10]. Türk Dil Kurumu Sözlükleri