

ELEKTRONİK SAĞLIK KAYITLARINDA FARKINDALIK *

Denizhan YILMAZ **
Esmâ ERGÜNER ÖZKOÇ ***
Gizem ÖGÜTÇÜ ULAŞ ****

ÖZ

Elektronik Sağlık Kayıtları (ESK) sistemleri, kişilerin, geçmiş ve şimdiki fiziksel ve ruhsal sağlık durumlarıyla ilgili tüm bilgilerin bilgisayar ortamında kayıt altına alınmasını, saklanması, iletilmesini, erişilmesini, ilişkilendirilmesini, işlenmesini ve gerektiğinde kullanılmasını sağlayan sistemlerdir. İnsanların en mahrem bilgilerini ihtiva eden, özel nitelikli hassas veri olarak adlandırılan sağlık verilerinin hukuka aykırı bir biçimde ele geçirilmesi, işlenmesi veya paylaşılması ayrımcılık başta olmak üzere ilgili kişinin ciddi zararlara uğramasına sebep olabilmektedir. Bu bilgilerin paylaşılması kişinin özel hayatının gizliliğine, hastanın mahremiyet hakkının korunmasına ve doktorun hastasına karşı sır saklama yükümlülüğünün ihlal edilmesine sebep olmaktadır. Kişisel sağlık verilerinin çalınması veya yanlış şekilde anonimleştirilmesi de bir güvenlik zafiyeti olarak değerlendirilmektedir. Oluşabilecek tüm bu zafiyetler konusunda gerek bireysel ve gerekse toplumsal hassasiyetler artmakta, tartışmalar ve çalışmalar kamuoyunun gündeminde gittikçe artan bir şekilde yer almaktadır. Bu çalışmada, Türkiye’de yaşayan farklı demografik özelliklere sahip bireylerin kişisel sağlık verileri ile ilgili farkındalık ve beklentilerinin ölçümü ve istatistiksel olarak değerlendirilmesi amaçlanmaktadır. Elde edilen sonuçlara göre genel olarak katılımcıların elektronik sağlık kayıtları konusunda farkındalıklarının yüksek olduğu ve fakat dijital ortamda kayıt altına alınan sağlık verilerinin güvenliği ve gizliliği konusunda endişeleri olduğu yönünde sonuçlar elde edilmiştir.

Anahtar Kelimeler: Kişisel sağlık verileri, tıp bilişimi, elektronik sağlık kaydı, kişisel veri güvenliği

MAKALE HAKKINDA

* Bu çalışma, Denizhan Yılmaz’ın Başkent Üniversitesi, Yönetim Bilişim Sistemleri Yüksek Lisans Programında hazırladığı “Sayısal Sağlık Verilerinde Farkındalık” isimli tezinden üretilmiştir.

** Yazılım Uzman Yard., Hacettepe Teknokent Safir C blok, denizhanyilmaz@yandex.com

 <https://orcid.org/0000-0001-5843-1426>

*** Dr. Öğr. Üyesi., Başkent Üniversitesi, Yönetim Bilişim Sistemleri Bölümü, Ankara, eozkoc@baskent.edu.tr

 <https://orcid.org/0000-0003-1728-5930>

**** Öğr. Gör., Başkent Üniversitesi, Yönetim Bilişim Sistemleri Bölümü, Ankara ogutcu@baskent.edu.tr

 <https://orcid.org/0000-0001-6386-0911>

Gönderim Tarihi: 17.04.2021

Kabul Tarihi: 07.09.2021

Atıfta Bulunmak İçin:

Yılmaz, D., Ergüner Özkoç, E., Ögütçü Ulaş, G.. (2021). Elektronik sağlık kayıtlarında farkındalık. Hacettepe Sağlık İdaresi Dergisi, 24(4): 777-792

ELECTRONIC HEALTH RECORDS AWARENESS *

Denizhan YILMAZ **
Esma ERGÜNER ÖZKOÇ ***
Gizem ÖĞÜTÇÜ ULAŞ****

ABSTRACT


Electronic Health Records (EHR) Systems are allow people to collect, record, store, transmit, access, relate, process and use all information about their past and present physical and mental health conditions in computer environment. The illegal acquisition, processing or sharing of health data, which includes the most private information of people and called sensitive data, may cause serious harm to the person concerned, especially discrimination. Sharing this information causes the privacy of the individuals' private life, the protection of the patient's right to privacy, and the violation of the doctor's obligation to keep the patient's secret. The theft, loss or incorrect anonymization of personal health data is also considered as a security weakness. Both individuals and social sensitivity about all these vulnerabilities increase, and discussions and studies are increasingly on the agenda of the public. In this study, we aimed to evaluate statistically the awareness and expectations of individuals who has different demographic characteristics of people living in Turkey, regarding personal digital health data. According to the results, the awareness of the participants about electronic health record was high in general, but it was concluded that they had concerns about the security and confidentiality of health data recorded in digital environment.

Keywords: Personal health data, medical informatics, electronic health record, personal data security

ARTICLE INFO

* This study was produced from Denizhan Yılmaz's thesis titled "Awareness in Digital Health Data", which is prepared at Başkent University, Management Information Systems Master's Program.

** Assist. Software Specialist., Hacettepe Teknokent Safir C blok, denizhanyilmaz@yandex.com

 <https://orcid.org/0000-0001-5843-1426>

*** Assist.Prof., Başkent University, Management Information System Department, Ankara, eozkoc@baskent.edu.tr

 <https://orcid.org/0000-0003-1728-5930>

**** Lecturer, Başkent University, Management Information System Department, Ankara ogutcu@baskent.edu.tr

 <https://orcid.org/0000-0001-6386-0911>

Received: 17.04.2021

Accepted: 07.09.2021

Cite This Paper:

Yılmaz, D., Ergüner Özkoç, E., Öğütçü Ulaş, G.. (2021). Elektronik sağlık kayıtlarında farkındalık. Hacettepe Sağlık İdaresi Dergisi, 24(4): 777-792

I. GİRİŞ

Hızla gelişen bilgi ve iletişim teknolojilerindeki dönüşüm, tüm alanlarda olduğu gibi sağlık sektörünü de önemli derecede etkilemektedir. Bilişim teknolojilerindeki gelişmelerle birlikte sağlık alanında da önemli değişimler ve dönüşümler yaşanmıştır. Özellikle 2019 pandemisi ile dokümantasyon ve veri paylaşımı konusundaki gelişmelerin sağlık uygulamalarındaki etkisi bütün ülkelerde öne çıkmaktadır. Bilişim teknolojileri, sağlık verilerinin ve bilgi birikiminin yayınlanmasını, paylaşılmasını ve veriye ulaşmayı kolaylaştırmakta, klinik karar verme aşamalarında sağlık çalışanlarına destek sağlamaktadır. Aynı zamanda hekimlerin diğer sağlık profesyonelleri ile olan çalışmalarını destekleyip veri paylaşımını hızlandırmaktadır. Bu nedenle, sağlık hizmetlerinde kişisel verilerin toplanması, korunması ve değerlendirilmesi gittikçe önem kazanmaktadır.

Kişisel veri, bir bilginin kimliği belirli gerçek kişi ile ilişkili veya ilişkilendirilebilir her türlü veri olarak kabul edilmektedir. Kişisel verilerin en önemlileri kanunlar ve ilgili mevzuatlar ile güvence altına alınmış kişilerin özlük bilgisi ve sağlık bilgisi gibi mahremiyet içeren verileridir. Kişisel verilerin dijital ortamlarda kayıt altına alınıp işlenmesiyle kişisel verilerin güvenliği ve korunması tüm dünyada tartışma konusu olmuştur (Knight, 2017). Verilerin dijital ortamlarda kaydedilmesi ile birlikte en önemli tartışma konularından birisi de kişisel verilerin gizliliği ve güvenliği olmuştur. Bu konu için tüm devletler ulusal ve uluslararası çalışmalar gerçekleştirmiş ve gerçekleştirmeye devam etmektedirler (Chik, 2013). OECD (Ekonomik Kalkınma ve İşbirliği Örgütü) ülkeleri gizlilik ihlalleri konusunda özel yönergeler ve araştırmalar yayınlamıştır. Bu araştırmalarda kişisel veriler ile ilgili hukuk sistemleri ve kısıtlamalar üzerinde durulmuştur. Kişisel veriler ve bu verilerin korunması, gizliliği ve güvenliği devletler açısından ekonomik olarak da büyük bir öneme sahiptir (O'Leary vd., 1995). Kişisel olarak tanımlanan her türlü veri gizlilik ilkeleri kapsamında değerlendirilmektedir (Schwartz ve Solove, 2014).

Sağlık alanında kişisel verilerin her geçen gün artması ve işlenmesi riskleri de beraberinde getirmektedir. Dijital dünya her saniye veri üretmektedir. Sağlık verilerini dijital ortama taşımak ve bu ortamlarda kaydetmek için sadece bireylerin sağlık kuruluşlarına gitmesine ve verilerin bu kuruluşlarda kayıt altına alınmasına gerek yoktur. Günümüzde akıllı cihazlar (tablet, saat, telefon), giyilebilir teknolojinin kullanımı kişisel sağlık verilerinin dijital ortamlarda artmasını sağlamaktadır. Dolayısıyla günümüzde bu cihazların her biri gizlilik ve güvenlik yasalarından sorumlu tutulmaktadır. Kullanıcılar cihazları kullanmaya başlamadan önce kullanım risklerine ait sözleşmeleri onaylamaktadırlar (Calvaresi vd., 2020).

Özel ya da kamu sağlık kuruluşlarında hastaların sağlık geçmişine ilişkin bilgiler, tahlil sonuçları, kendilerine konulan tanımlar, tedaviler ve bunların süreleri sayısal ortamda yer almaktadır (Dülger, 2015). Hastaların geçmişteki tanı ve tedavilerine hekimlerin ulaşabilmesi yeni tanımların doğru bir şekilde konulmasını, müdahalenin daha çabuk ve daha az riskli gerçekleştirilmesini sağlayabilmektedir. Sağlık alanında yapılan araştırmalarda da ifade edildiği gibi hasta bilgilerinin ulaşılabilir olması önemli yararlar sağlamaktadır (Küzeci, 2019). Sisteme kayıt edilen kişisel sağlık verileri, farklı kurumlar arasında da paylaşılmakta, hastalara ait bilgilere birçok kişi erişebilmektedir. Bu erişimler ile ilgili izin ve yetkiler düzenlenirken verinin gizliliği ve güvenliğine önem verilerek gerekli düzenlemeler yapılmalıdır. Özellikle "özel nitelikli hassas veri" olarak adlandırılan sağlık verilerinin hukuka aykırı bir biçimde ele geçirilmesi, işlenmesi veya paylaşılması ayrımcılık başta olmak üzere ilgili kişi için ciddi zararlara yol açmasına sebep olabilmektedir. Bunun beraberinde bu bilgilerin paylaşılması kişinin özel hayatının gizliliği, hastanın mahremiyet hakkının korunmasına ve doktorun hastasına karşı sır saklama yükümlülüğünün ihlal edilmesine sebep olmaktadır. Mahremiyet kavramının içinde bulunan kişisel sağlık verileri ile veri sahibi olan kişiler tehdide maruz kalabilmekte, sevdikleri tarafından terk edilebilmekte, işlerinden kovulabilmekte, sosyal ayrımcılığa uğrayabilmektedir (Başalp, 2015). İşverenlerin bu bilgiler sayesinde personel seçim kararlarını değiştirebilmeleri, bankaların sağlık sorunları olduğunu gördükleri müşterilerine kredi hizmeti vermek istememeleri, sigorta şirketlerinin sağlık sorunları bulunan bireylere yüksek primli sigorta poliçeleri sunabilmeleri de bu olumsuzluklara eklenebilir. Bu sebeplerle mahremiyet içeren kişisel veriler,

kanunlar ve mevzuatlar kapsamında korunmak durumundadır (Schwartz, 2003). Öte yandan, sağlık verileri gibi bilimsel, ekonomik, politik çalışmalara konu olabilecek kişisel veriler anonimleştirilerek, yani kişisel verinin, kişi kimliğinden ayrıştırılarak anonim hale getirilerek bu araştırmalar için veri olarak kullanılabilir (Bayardo, 2005).

Türkiye’de, Elektronik Sağlık Kayıtları (ESK) ve Kişisel Elektronik Sağlık Kayıtları (KESK) ile ilgili ilk çalışmalar, 2003 yılı başında T.C. Sağlık Bakanlığı tarafından kamuoyuna duyurulan Sağlıkta Dönüşüm Programı kapsamında başlamıştır (Türkiye Cumhuriyeti Sağlık Bakanlığı [SB], 2007). ESK sistemi, kişilerin, geçmiş ve şimdiki fiziksel ve ruhsal sağlık durumlarıyla ilgili tüm bilgilerin bilgisayar ortamında toplanmasını, kayıt altına alınmasını, saklanmasını, iletilmesini, erişilmesini, ilişkilendirilmesini, işlenmesini ve gerektiğinde kullanılmasını sağlayan sistemdir. ESK, hastalara ait KESK’ni, etik ve yasal kurallara uygun, zaman içerisinde elde edilen tüm kayıtların bütünlüğünü sağlayabilen, gizliliğini koruyan bir sistem olmalıdır. Sağlıkta gizliliği korumanın en temel yöntemi hasta mahremiyeti ve gizliliğini bir hasta hakkı olarak gören sağlık kurumu çalışanlarının olmasıdır. Bütün seviyelerdeki sağlık çalışanları bu hususta sorumluluk taşımaktadırlar (Arslan ve Demir, 2017). Hastalarla ilgili sağlık kayıtlarını ancak doğrudan ilgili kişiler görebilmeli; harici sağlık personelleri de dâhil olmak üzere başka kişilerin görmesinin, bu bilgilere ulaşmasının mümkün olmaması sağlanmalıdır (Dülger, 2015).

Bu çalışmada, Türkiye Cumhuriyeti vatandaşlarının ESK hakkında bilgi düzeylerinin, beklentilerinin ve farkındalıklarının belirlenmesi için anket yöntemi ile nicel bir araştırma yapılmıştır.

II. LİTERATÜR TARAMASI

Sağlık bilişim sistemlerinde güvenliği şu şekilde tanımlayabiliriz: Kişilerin, kurumların, devletlerin maddi ve manevi sahip olduğu her şeye karşı yapılan ve yapılmaya çalışılan saldırı ve tehditler için alınacak önlemlerdir (Yılmaz vd., 2015). Siber güvenlik ise; sayısal ortamlardan yapılan çeşitli saldırı ve tehditlere karşı bilgi teknolojilerinin gizliliğini, bütünlüğünü, kullanılabilirliğini ve erişimini koruyan stratejiler ve çalışmaların bütünüdür. Gizlilik, bilgilerin ve belgelerin erişim izni olmayan bireyler ve sistemlere karşı ulaşılmaz konuma getirilmesidir (Jang-Jackard ve Nepal, 2014). Siber güvenliğin ihlalinde ortaya çıkan tüm tehdit ve saldırılar ise siber saldırı kapsamına alınmaktadır (Hathaway vd., 2012). Siber saldırıların kaynağına ilişkin yapılan bir çalışmada; sağlık organizasyonlarına yönelik yapılan siber saldırıların %38’inin çevrimiçi dolandırıcılardan, %21’inin örgüt içi bireylerden ve %21’inin ise hackerlardan kaynaklandığı belirtilmiştir (Healthcare Information and Management Systems Society [HIMSS] North America, 2018). Bir başka çalışmada ise siber saldırılara uğrayan sistemlere erişimin kolay olmasının nedeninin; medikal amaçlı kullanılan teknolojik cihazlar üretilirken sistemlerinde güvenlik yazılımlarının bulunmasına gerek duyulmaması olduğu belirtilmiştir (Ayala, 2016). Bu açıkların oluşmasının temelinde ise ülke sağlık politikaları ve sağlık bilişimi yazılım gereksinimleri hazırlanırken değerlendirilme ve planlama aşamalarında siber güvenlik konusunun göz ardı edilmesi yatmaktadır (Kruse vd., 2017).

Safran ve arkadaşları tarafından 2007 yılında yapılan çalışmada kişisel sağlık verilerinin ikincil kullanımından yani sağlık verilerinin hastalık tedavisi dışında kullanıldığı alanlardan bahsedilmiştir. Bu alanlar; bilimsel araştırmalar, kalite ve güvenlik ölçümleri, halk sağlığı ödemeleri, pazarlama ve ticaret faaliyetleri gibi çeşitli alanlardır. Veriler anonimleştirildikten sonra bu alanlarda kullanılmasında hukuki bir engel bulunmamaktadır. Yapılan araştırmalar sonucunda kişisel sağlık verilerinin ticari değerinin milyonlarca dolarlarla ifade edilebileceği ortaya çıkmaktadır. Sağlık verilerinin ikincil kullanımı ile ilgili bu çalışmada, veri sahipliğinden ziyade veriyi yönetmeye ve veriyi işlemeye odaklanmanın doğru olduğu, kişisel sağlık verilerinin güvenliği ile ilgili kamu bilinci ve güveni oluşturma gerekliliğine vurgu yapılmıştır (Safran vd., 2007).

Archer ve arkadaşlarının 2011 yılında, Amerika ve Kanada merkezli kişisel sağlık kayıtları kapsamının belirlenip incelenmesi ile ilgili yaptıkları bir çalışma sonucunda dijital sağlık kayıtlarının doktor merkezli tutuldukları ve takibe alındığı ortaya konulmuştur. Bu verilerin hastaların sağlıklarının olumlu yönden etkilenmesi ve doktorların işlerinin kolaylaşması için güvenliği sağlanmış portallar

üzerinden sürekli güncellenerek daha doğru kişisel ve toplumsal sağlık verilerine ulaşılabileceği savunulmuştur.

Spencer ve arkadaşları tarafından 2016 yılında yapılan bir çalışmada dijital sağlık kayıtlarının anonimleştirilerek kullanılmasının her geçen gün arttığı ve çeşitli araştırmalarda kullanılmak için büyük bir fırsat olarak görüldüğü söylenmiştir. Bununla birlikte verilerin uygunsuz kullanımına ilişkin kamuoyu endişelerinin göz önünde bulundurulması gerektiğine dikkat çekmişlerdir. Hastaların dijital sağlık kayıtlarına kimlerin ulaşacağına kendilerinin karar vermesini daha etik ve güvenilir olduğunu savunmuşlardır.

Entzeridou ve arkadaşları tarafından 2018 yılında yapılan çalışmada elektronik sağlık kayıtlarının etik kaygıları üzerinde durulmuştur ve elektronik sağlık kayıtlarının risklerinin, faydalarından daha ağır bastığı savunulmuştur. Çalışmada hekimlerin ve sağlık kayıtları oluşturan hastaların elektronik sağlık kayıtlarının etik endişeleri ile ilgili beklenti ve farkındalıkları araştırılması planlanmış ve bunun ile ilgili bir anket çalışması yapılmıştır. Demografik soruların yanında sağlık kayıtlarının etki, algılanan riskler ve etik sorunları ile ilgili kapalı uçlu sorular sorulmuştur. Yapılan anket çalışmasının sonucunda halkın %46'sı hekimlerin ise %91'i ESK risklerinin farkında olduğu ortaya konmuştur. Katılımcıların büyük bir çoğunluğu kişisel sağlık verilerinin üçüncü şahısların eline geçtiği takdirde büyük endişe duyacaklarını belirtmişlerdir. Hastaların ve hekimlerin, kişisel sağlık kayıtlarının gizliliği ve güvenliğinin sağlanması koşuluyla elektronik sağlık kayıtlarının faydasını kabul ettikleri ve destekledikleri görülmüştür.

Häikiö ve arkadaşları tarafından 2020 yılında yapılan çalışmada sağlık sektörünün şu anda ESK ile daha aktif bir hizmet sağladığı savunulmuştur. Çalışmada kişisel veriler ile ilgili beklentiler ve değerler hizmet sağlayıcıları ve bireysel kullanıcılar açısından incelemiştir. Çalışma görüşme yolu ile toplanan ampirik materyal analizine dayanmaktadır. Kişisel sağlık verileri ile ilgili güvenlik endişeleri olduğu görülse de hizmet sağlayıcı yani verilerin saklanması ve kayıt edilmesinde rol oynayan kurumlar yapılan araştırmada güvenilir bulunmuştur. Çalışma sonucunda kişisel sağlık verilerinin potansiyel faydalarına erişmek için güvenilirliği arttırmak ve veri güvenlik endişelerinin giderilmesi gerektiği ortaya çıkmıştır.

Türkiye'de ise Öğütçü ve arkadaşları tarafından 2011 yılında yapılan elektronik sağlık kayıtlarının içeriği, hassasiyeti ve erişim kontrollerine yönelik farkındalık ve beklentilerinin değerlendirilmesi adlı çalışmada, elektronik sağlık kayıtlarına ilişkin bilincin tam olarak oluşmadığı, elektronik sağlık kayıtlarına ilişkin en büyük endişenin bu kayıtlara erişim konusunda duyulduğu ortaya çıkmıştır. Çalışma sonucunda ortaya çıkan bir başka sonuç ise hasta ve doktorların sağlık alanında teknolojinin kullanımı konusundaki beklentilerinin oldukça yüksek olmasıdır. Özkan tarafından 2011 yılında yapılan çalışmada ise elektronik sağlık bilgilerinin gizliliği ve mahremiyeti konusu ele alınmıştır. Çalışma sonucunda, çalışmaya katılan bireylerin, sağlık hizmetlerinde bilgisayar kullanımı ile ilgili bir endişelerinin olmadığı, fakat bilgilerinin güvenliğinin sağlanıp, sağlanmadığı konusunda kararsız oldukları ortaya çıkmıştır. Çalışmada ortaya çıkan bir başka sonuç ise katılımcıların doktorlarına, hemşirelerine, eczacılarına ve diğer sağlık çalışanlarına güvendiklerini ancak sigorta şirketleri, devlet, özel sektör sağlık araştırmacılarına, bilgisayar sistemlerini yöneten uzmanlara güvenmediklerini ortaya koymuştur.

2011 yılından itibaren dijitalleşmenin büyük ivme kazandığı günümüzde, kullanıcıların bilgi ve farkındalık seviyelerinin ve beklentilerinin ne düzeyde değiştiğini ortaya koymak amacı ile de bu çalışma gerçekleştirilmiştir.

III. GEREÇ VE YÖNTEM

Araştırmada, sayısal veri güvenliği perspektifinden Türkiye Cumhuriyeti vatandaşlarının elektronik sağlık kayıtlarının güvenliğine yönelik farkındalık ve beklentilerini değerlendirilmesi amaçlanmıştır. Bu kapsamda elektronik sağlık kayıtları farkındalık ve beklentileri ölçeği ifadelerinden oluşan, Google Forms üzerinden elektronik anket formu oluşturulmuştur. Araştırmanın evreni 18 yaş üzeri Türkiye

Cumhuriyeti vatandaşlarıdır. 2019 pandemisi döneminde ulaşım kolaylığı gözetilerek basit rasgele örnekleme yöntemi kullanılarak çevrimiçi anket uygulaması yapılmıştır. Örneklemimiz teknoloji okuryazarı ve internet erişimi olan reşit T.C. vatandaşlarıdır. Çalışma kapsamında yaşları 18-70 arasında değişen, Türkiye'nin farklı illerinde ikamet eden 444 katılımcıya ulaşılmıştır. Araştırma kapsamında yapılan anket çalışmasının yönteminin çevrimiçi anket yöntemi olarak belirlenmesi nedeniyle araştırmacı ve katılımcının yüz yüze görüşme yaparak elde edilebilecek verilere ulaşamamasının yanında teknoloji okuryazarı olmayan ve internet erişimi olmayan bireylerle ulaşamaması da çalışmanın kısıtları olarak kabul edilmiştir. Çalışmanın, Başkent Üniversitesi Sosyal ve Beşeri Bilimler Sanat Araştırma Kurulu tarafından 9.03.2021 tarihli 17162298.600-68 sayılı Etik Kurul onayı mevcuttur.

Araştırmada 5'li Likert tipi ölçek kullanılmış, seçenekler "Kesinlikle Katılıyorum"dan "Kesinlikle Katılmıyorum"a kadar değişmektedir. Çalışmada Öğütçü tarafından 2011 yılında yapılan Elektronik Sağlık Kayıtlarının İçeriği, Hassasiyeti ve Erişim Kontrollerine Yönelik Farkındalık ve Beklentilerin Değerlendirilmesi çalışmasında kullanılan anket sorularına 3 soru eklenerek kullanılmıştır (Öğütçü vd., 2011). Eklenen üç sorunun iki temel amacı vardır. Bunlardan ilki ilgili çalışmanın yayınlandığı tarihte henüz taslak olarak mevcut olduğu halde yürürlüğe girmemiş olan 6698 Sayısı Kişisel Verilerin Korunması Kanunu (KVKK)'nun bu çalışmanın yapıldığı tarihte yürürlüğe girmiş olmasıdır. İkinci amaç ise yine benzer şekilde ilgili çalışmanın yapıldığı tarihte henüz kullanımda olmayan, sağlık kayıtlarına erişimlerin mümkün olduğu E-Nabız uygulamasının bu çalışmanın yapıldığı tarihte aktif olarak E-Devlet'in bir parçası olarak kullanılabilir olmasıdır. Bu bağlamda ölçeğe KVKK ve E-Nabız uygulaması hakkında 3 soru eklenmiştir. Ölçekte yapısal hiçbir değişiklik yapılmamıştır. Yeni eklenen soruların anlaşılabilirliğini anlamak amacı ile ölçek sorularına ilişkin uzman görüşü alınmış ve buna göre ölçek uygulanabilir kabul edilmiştir. Ölçeğe ilişkin güvenilirlik sonuçları aşağıdaki paragraflarda paylaşılmıştır. Uygulanan anket formu yedi alt bölümden oluşmaktadır. Katılımcılara;

1. Sosyo-demografik özelliklerine yönelik
2. Elektronik ortamlarda kayıt altına alınan verileri ne derece kişisel bulduklarını ölçmeye yönelik
3. Verilerin dijital ortam ve uygulamalarda kayıt altına alındığının farkındalığına yönelik
4. Sağlık bilgilerinin gizliliği ile ilgili görüşlere yönelik
5. Sağlık bilgilerinin dijital ortamlarda saklanması ile ilgili gizlilik ve güvenliğe dair farkındalık ve beklentileri ölçmeye yönelik
6. Dijital ortamda saklanan sağlık bilgilerinin kullanımı ile ilgili farkındalık ve beklentilerini ölçmeye yönelik
7. Dijital ortamda saklanan sağlık bilgilerinin güvenlik sorumluları ile ilgili farkındalık ve beklentilerini ölçmeye yönelik sorular yöneltilmiştir.

Bu çalışmada anket sorularından herhangi birine cevap verme oranı 0,5 olarak alınmış ve heterojen bir dağılım gösterdiği varsayımı altında varyans $\sigma^2=0,25$ olarak alınmıştır. Anketteki bir sorudan tahmin edilecek bir oran tahmini ile gerçek oran değeri arasındaki farkı ortaya çıkarmada (d) 0,05'lik bir hata hoş görüldüğünde, %95 güven olasılığı ile yapılan parametre tahminleri için başlangıç örneklem büyüklüğü aşağıdaki gibi;

$$n_0 = \frac{z_{\alpha/2}^2 PQ}{d^2} = \frac{(1,96)^2 (0,5)(0,5)}{(0,05)^2} = 384,16 \text{ hesaplanmıştır.}$$

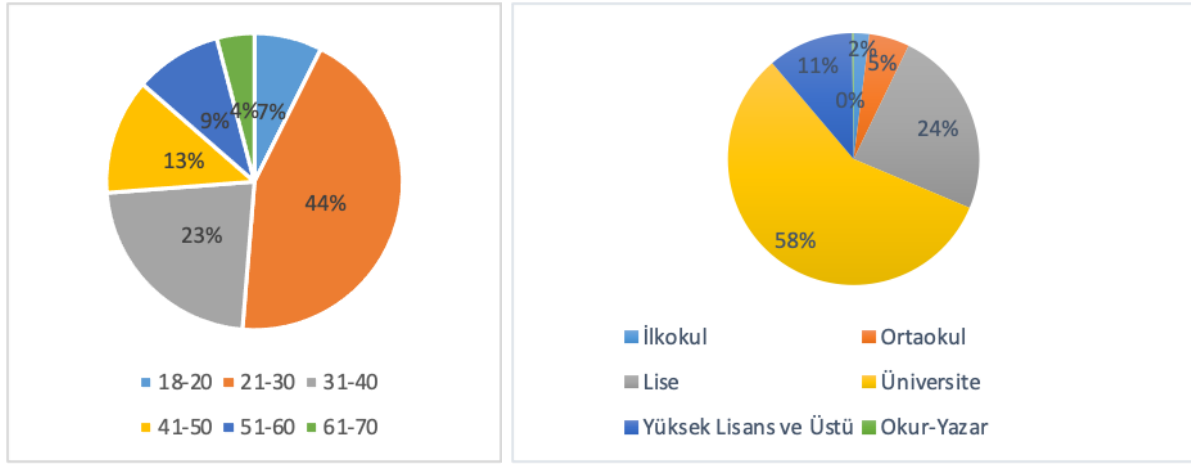
Araştırma sonucunda elde edilen verilerin analizi için Statistical Package for the Social Sciences (SPSS) 22.0 kullanılmıştır. Katılımcıların demografik bilgileri (yaş, eğitim) tablolar ile düzenlenmiştir. Araştırmada veriler, 'n' ve '%' olarak verilmiştir. Verilerin sonuçlarını aktarmak için yüzde, standart sapma, güven derecesi, sayı gibi istatistik verileri kullanılmıştır. Araştırmada elde edilen verilerin istatistiksel anlamlılık düzeyi $p<0,5$ olarak kabul edilmiştir. Araştırmada ölçeğin güvenilirliği için hesaplanan Cronbach's Alpha değeri analiz edilmiştir. Cronbach's Alpha değerinin $>0,70$ olduğu çalışmalar literatürde güvenilir olarak kabul edilmiştir (Özdamar, 1999) ve bu çalışmada, Cronbach's

Alpha değeri 0,900 Cronbach's Alpha Based on Standardized Items değeri (Güvenirlik katsayısı) ise 0,911 olarak hesaplanmıştır.

VI. ANALİZ VE BULGULAR

Araştırmaya katılan katılımcıların yaşları, %43,9'u 21-30 yaş arası, %22,5'i 31-40 yaş arası, %12,6'sı 41-50 yaş arası, %9,5'i 51-60 yaş arası, %7,4'ü 18-20 yaş arası %4,1'i 18-20 olarak dağılım göstermiştir. Araştırmaya katılan katılımcıların %66'sı 21-40 yaş arasındadır. Katılımcıların, eğitim düzeyleri, %57,4'ü üniversite mezunu, %24,1'i, lise mezunu, %11,0'ı yüksek lisans ve üstü mezunu, %5,2'si ortaokul mezunu, %2,0'ı ilkokul mezunu, %0,2'si ise okur-yazar bireylerden oluşmaktadır. Katılımcıların %93'ü lise ve daha yüksek eğitim düzeyine sahiptir. (Şekil 1)

Şekil 1. Katılımcıların Demografik Bilgileri



(a) Katılımcıların Yaş Dağılımı

(b) Katılımcıların Eğitim Durumu

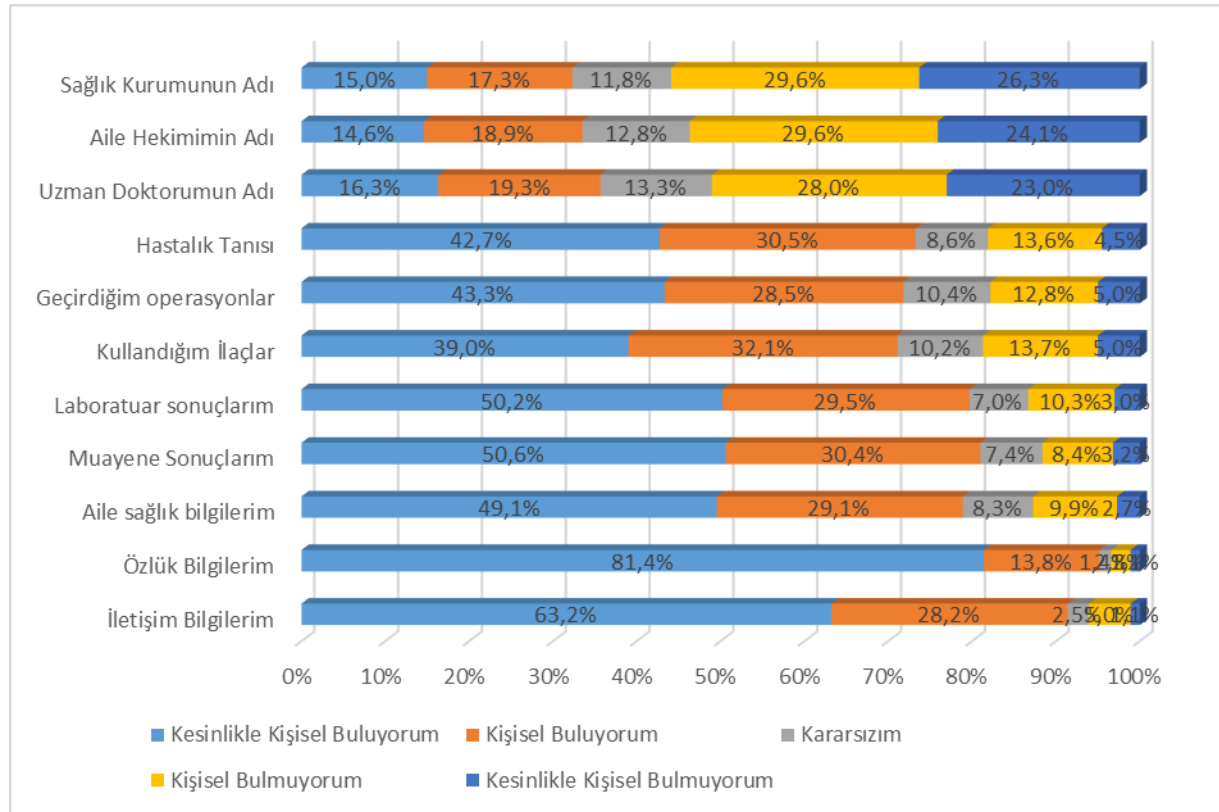
Katılımcıların, %79,3'ünün herhangi bir bilinen rahatsızlığı bulunmamaktayken, %20'sinin bilinen bir rahatsızlığı vardır (%0,7 katılımcı ise bu soruya iki yanıtı seçerek cevap vermiş ve değerlendirmede bu cevaplar geçersiz sayılmıştır). Katılımcıların, %51,4'ü son 1 yıl içerisinde 1-3 arası kez sağlık kurumuna başvururken, %12,8'i 4-6 arası kez sağlık kurumuna başvurmuştur. %2,9 katılımcı ise son 1 yıl içerisinde 6 ve üzeri defa sağlık kurumuna başvururken, %32,7 katılımcı hiç sağlık kurumuna başvurmamıştır. Katılımcıların %66'sı son 1 yıl içerisinde en az bir kez sağlık kurumuna başvurmuştur. Katılımcıların sosyal güvenceleri %73'ü SGK (SSK, Emekli Sandığı, BAĞ-KUR) gibi devlet tarafından sağlanan sosyal güvenceye sahip bireylerden oluşmaktadır. %12,4'ünü oluşturan katılımcı ise SGK güvencesinin yanına ek olarak özel sağlık sigortası yaptırmış bireylerdir. %5,2 katılımcının ise sadece özel sağlık sigortası vardır. Katılımcıların, %2,5'i ise kurum sigortası ile sosyal güvencelerini sağlamaktadırlar. Katılımcıların %0,9'u ise Türkiye Cumhuriyeti tarafından engelli vatandaşlara sağlanan 60/c1-c3-c9 kapsamında sosyal güvenceye sahipken, %5,3 katılımcı herhangi bir sosyal güvenceye sahip değildir.

Katılımcıların, %78,6'sı sürekli ilaç kullanmazken, %20,5'i sürekli ilaç kullanan bireylerden oluşmaktadır. %0,9 katılımcı ise bu soruya cevap vermemiştir. Ayrıca katılımcıların, %82,9'u farklı sektörlerde çalışırken, %16,9'u sağlık sektöründe çalışmaktadır (%0,2 geçersiz).

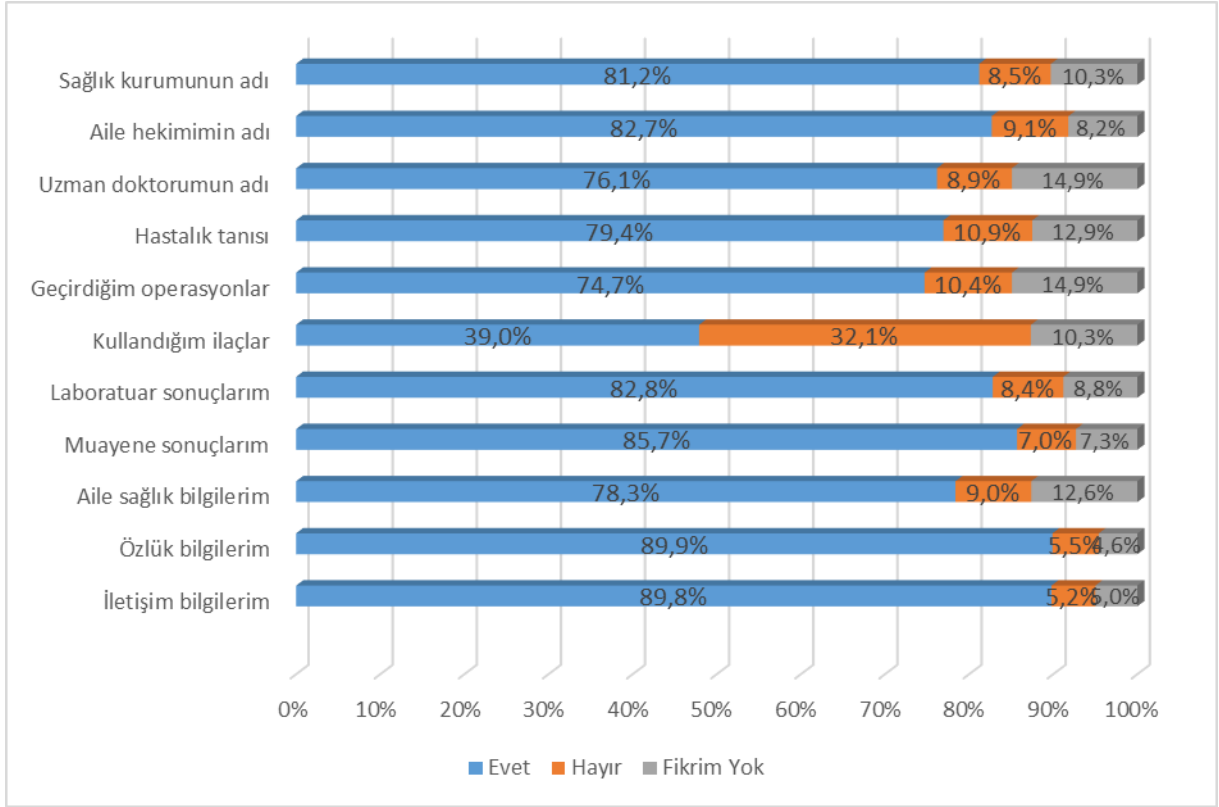
Çalışmaya katılan, katılımcılara kayıt altına alınan dijital sağlık verilerini kişisel bulup bulmadıkları ile ilgili sorular yöneltilmiştir. Bu veriler, iletişim bilgileri (adres, telefon, vb.), özlük bilgileri (TC kimlik no, doğum tarihi, vb.), aile sağlık bilgileri (kalıtsal hastalıklar, genetik bilgiler, vb.), muayene sonuçları (şikâyetler, doktor bulguları, vb.), laboratuvar sonuçları (kan/idrar tahlilleri, röntgen, MR sonuçları, vb.), kullandığı ilaçlar, geçirdiği operasyonlar, hastalık tanıları, uzman doktorlarının adı, aile hekimlerinin adı, başvurdukları sağlık kurumunun adı (hastane, eczane, vb.) gibi

elektronik ortamlarda kayıt altına alınan verilerdir. Katılımcıların %91,4'ü iletişim bilgilerini kişisel bulurken, geri kalan kısım ise kararsız veya bu veriyi kişisel bulmadıklarını belirtmişlerdir. Özlük bilgilerini ise katılımcıların, %95,2'si kişisel bulurken kalan kısım kararsız ve kişisel bulmadıklarını belirtmişlerdir. Aile sağlık bilgilerinde ise katılımcıların %78,2'si kişisel bulduklarını ifade ederken kalan kısım kararsız ve kişisel bulmadıklarını belirtmişlerdir. Muayene sonuçlarını kişisel bulan katılımcı oranı %81 iken kalan kısım kişisel bulmayan ve kararsız kalan katılımcılardan oluşmaktadır. Laboratuvar sonuçlarını kişisel bulan katılımcı oranı %79,7'dir. Kullandığı ilaçları kişisel bulan katılımcı oranı ise %71,1'dir. Geçirdiği operasyonları kişisel bulan katılımcı oranı %71,8'dir. Hastalık tanılarını ise kişisel bulan katılımcı oranı %73,2'dir. Katılımcıların %35,6'sı uzman doktorlarının adını kişisel bulduklarını belirtmişlerdir. Aile hekiminin adlarını kişisel bulan katılımcıların oranı %33,5 sağlık kurumlarının adlarını kişisel bulan katılımcı oranı %32,3'tür. (Şekil 2)

Şekil 2. Sayısal Verileri Kişisel Bulma Durumu

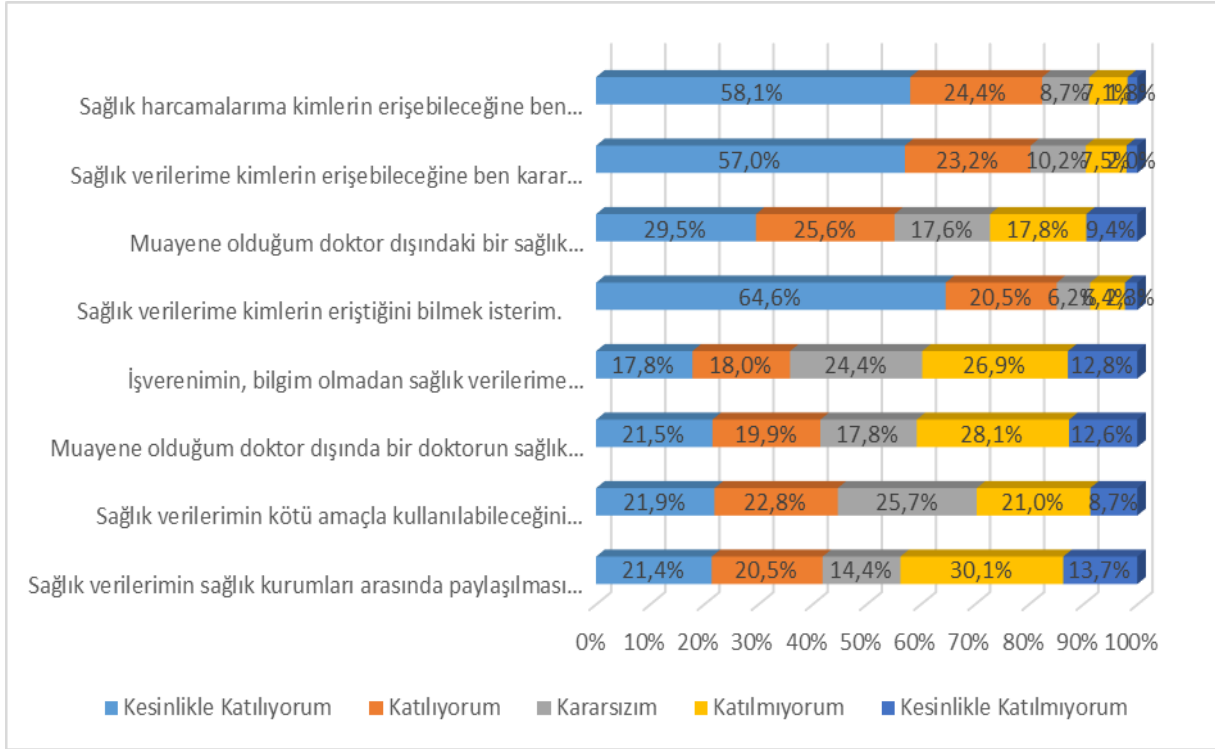


Çalışmaya katılanlara sağlık verilerinin, dijital ortamlarda kayıt altına alındığının ve saklandığının farkındalığını ölçmek için sorular yönetilmiştir. Araştırmaya katılan 444 katılımcıdan, iletişim bilgilerinin dijital ortamda kayıt altına alındığını bilenlerin oranı %89,8'dir. Özlük bilgilerinin kayıt altına alınıp, saklandığının farkında olan katılımcı oranı ise %89,9'dur. Katılımcıların, Aile sağlık bilgilerinin dijital ortamlarda saklandığının farkında olanlarının oranı ise %78,3'tür. Muayene sonuçlarının dijital ortamlarda saklandığının farkında olan katılımcı oranı ise %85,7'dir. Katılımcıların %82,8'i laboratuvar sonuçlarının dijital ortamlarda saklandığını bilmektedir. Kullandığı ilaçların dijital ortamlarda saklandığını bilen katılımcı oranı ise %74,7'dir. Geçirdiği operasyonların dijital ortamlarda saklandığını bilen katılımcı oranı %76,2'dir. Hastalık tanılarının dijital ortamlarda kaydedildiğini bilen katılımcı oranı ise %79,4'dür. Uzman doktorunun adlarının dijital ortamlarda kayıt altına alındığını ise katılımcıların %76,1'i bilmektedir. Aile hekiminin adının dijital ortamlarda saklandığını bilen katılımcı oranı %82,7'dir. Sağlık kurumunun adının dijital ortamlarda kayıt altına alındığını bilen katılımcı oranı ise %81,2'dir. (Şekil 3)

Şekil 3. Verilerin Dijital Ortamda Kayıt Altına Alınmasına Yönelik Farkındalık

Katılımcılara sağlık bilgilerinin gizliliği ile ilgili birtakım ifadelere katılma derecelerini belirleyen sorular sorulmuştur. Katılımcıların %41,9'u kayıt altına alınan sağlık verilerinin sağlık kurumları arasında paylaşılmasından endişe duyacaklarını belirtmiştir. Katılımcıların %44,7'si mevcut sağlık verilerinin kötü amaçla kullanılabileceğini düşünmektedir. Muayene olduğu doktor dışında başka bir doktorun sağlık verilerini görmesinden rahatsız olacağını ifade eden katılımcı yüzdesi ise %41,4'tür. İşverenlerinin sağlık verilerine izinsiz bir şekilde ulaşabileceklerini düşünen katılımcı oranı ise %35,8'dir. Sağlık verilerini kimlerin erişeceğini bilmek isteyen katılımcı oranı %85,1'dir. Muayene olduğu doktor dışında herhangi bir sağlık personelinin sağlık verilerini görmesinden rahatsız olacağını belirten katılımcı oranı ise %55,1'dir. Sağlık verilerine kimlerin erişeceğini yetkilendirmesini yapmak isteyen katılımcı oranı ise %80,2'dir. Sağlık harcamalarına kimlerin erişebileceğini kendisinin karar vermesini isteyen katılımcı oranı %82,5'tir. (Şekil 4)

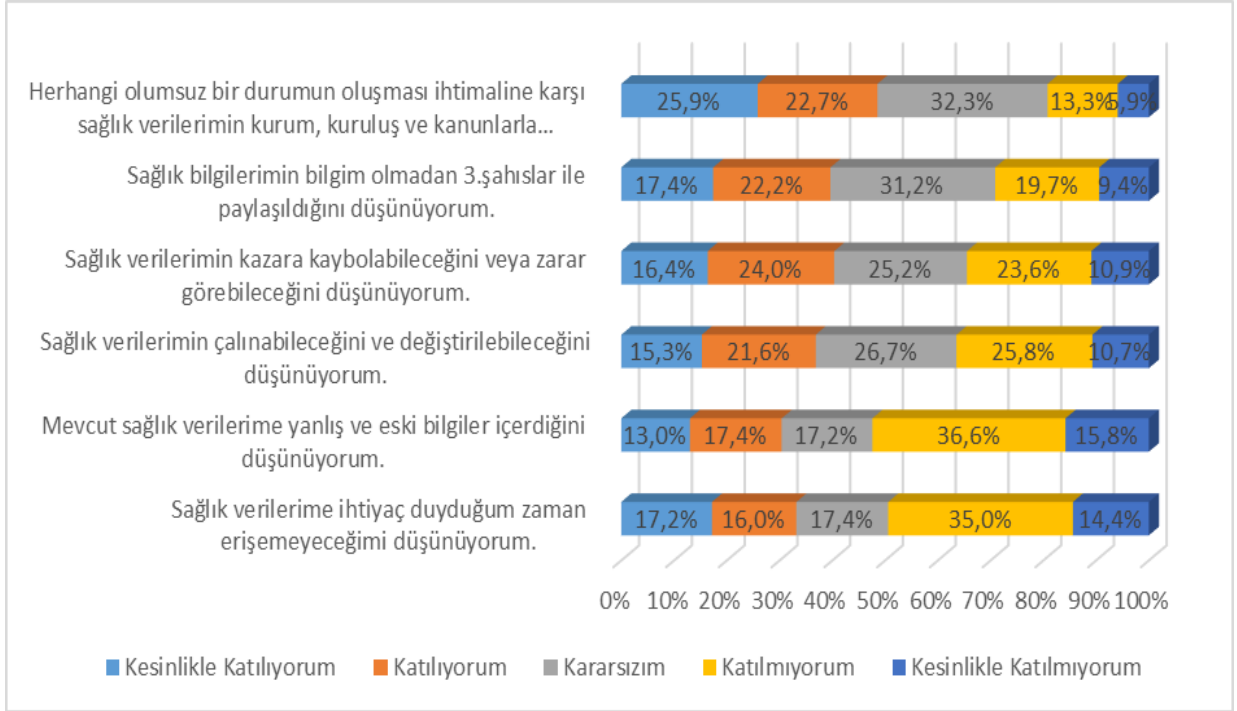
Şekil 4. Sağlık Bilgilerinin Gizliliği ile İlgili İfadelere Katılma Durumu



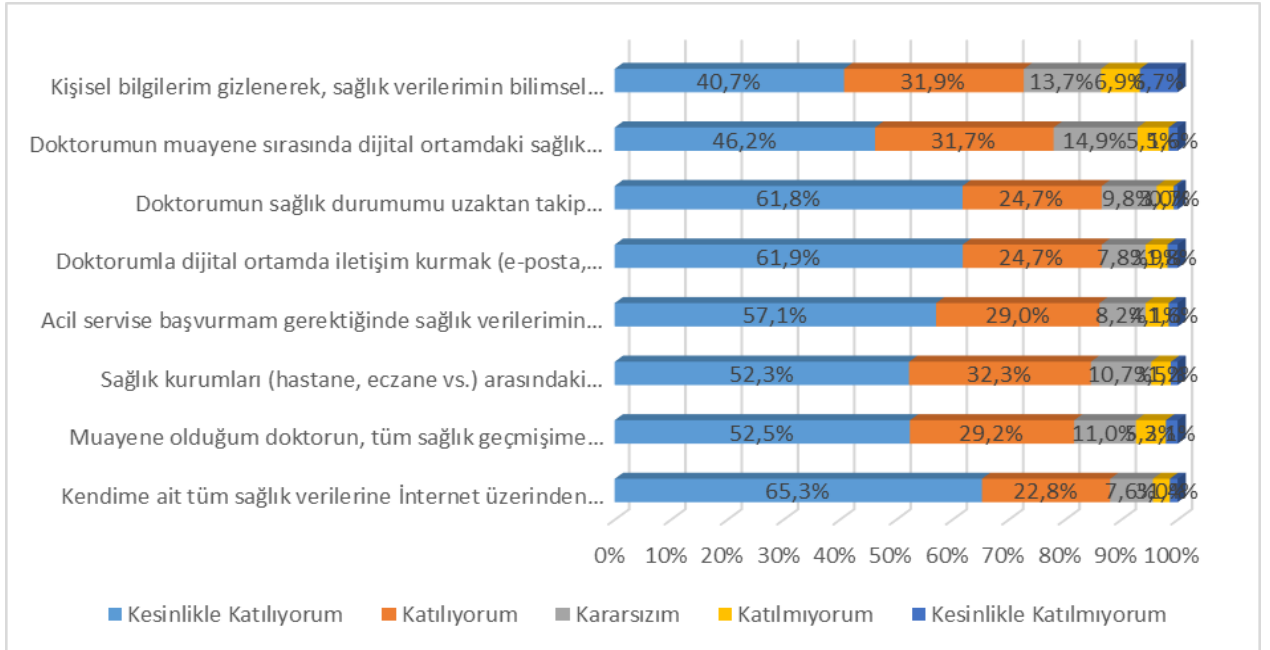
Katılımcılara, sağlık bilgilerinin dijital ortamlarda saklanması ile ilgili gizlilik ve güvenliğe dair farkındalık ve beklentileri ölçmek amacıyla bazı sorular sorulmuştur. Katılımcıların verdikleri cevaplara göre, sağlık verilerine ihtiyaç duydukları anda erişemeyeceğini düşünen katılımcı oranı %33,2'dir. Katılımcıların %30,4'ü mevcut sağlık verilerinin yanlış ve eski bilgiler içerdiğini, %36,9 sağlık verilerinin çalınabilip, değiştirilebileceğini düşünmektedir. Sağlık verilerinin kazara kaybolabileceğini düşünen katılımcı oranı ise %40,4'tür. Sağlık bilgilerinin, bilgileri olmadan üçüncü şahıslar ile paylaşıldığını düşünen katılımcı oranı %39,7'dir. Sağlık verilerinin çalınması, kötüye kullanılması gibi durumlarda kamu kurum, kuruluş ve kanunlarla korunduğunu düşünen katılımcı oranı ise %48,6'dır. (Şekil 5)

Dijital ortamlarda saklanan sağlık bilgilerinin kullanımı ile ilgili katılımcılara belirtilen ifadelerle katılım derecelerini belirlemek için sorular sorulmuştur, katılımcıların verdikleri yanıtlara göre, tüm sağlık verilerine internet üzerinden ulaşmak isteyen katılımcıların oranı %88,1'dir. Katılımcıların %81,7'si muayene oldukları doktorlarının, sağlık geçmişlerine erişebilmelerini istediklerini belirtmişlerdir. Katılımcıların, %84,6'sı ise sağlık kurumları (hastane, eczane vs.) arasındaki işbirliğinin tedavileri için önemli ve yararlı olduklarını düşünmektedirler. Katılımcıların %86,1'i acil servise başvurmaları gerektiğinde başvurdukları acil servislerin sağlık verilerinin tamamına ulaşabilmelerini istemektedirler. Doktoru ile dijital ortamda (e-posta, anında mesajlaşma programları, vb.) iletişim kurmak isteyen katılımcı oranı ise %86,6'dır. Katılımcıların, %86,5'i ise doktorlarının, sağlık durumlarını uzaktan takip etmesini istemektedir. Muayene oldukları doktorlarının dijital ortamdaki sağlık verilerinden yararlandığını düşünen katılımcı oranı ise %77,9'dur. Kişisel sağlık bilgilerinin anonimleştirilerek, bilimsel araştırmalarda kullanılmasından rahatsız olmayacak katılımcı oranı ise %72,6'dır. (Şekil 6)

Şekil 5. Sağlık Bilgilerinin Dijital Ortamlarda Saklanması İle İlgili Gizlilik ve Güvenliğe Dair Farkındalık Durumu



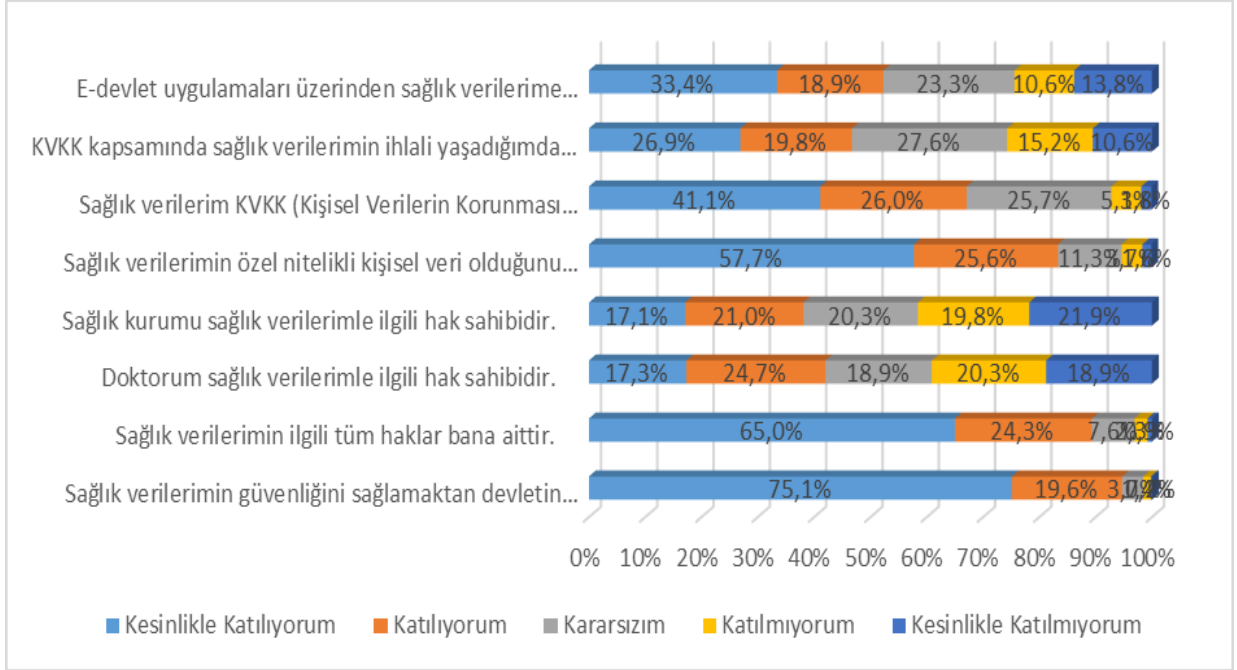
Şekil 6. Dijital Ortamda Saklanan Sağlık Bilgilerinin Kullanımı ile İlgili İfadelere Katılım Durumları



Dijital ortamlarda saklanan sağlık bilgilerinin güvenlik sorumlulukları ile ilgili bazı sorular yöneltilmiştir. Katılımcıların %94,7'si sağlık verilerinin güvenliğini sağlamaktan devletin sorumlu olması gerektiğini düşünmektedir. Kişisel sağlık verileri ile ilgili tüm hakların kendisine ait olduğunu düşünen katılımcı oranı %89,3'tür. Doktorlarının, sağlık verileri ilgili hak sahibi olduğunu düşünen katılımcı oranı %42'dir. Başvurdukları sağlık kurumlarının sağlık verileri ile ilgili hak sahibi olduğunu düşünen katılımcıların oranı ise %38,1'dir. Sağlık verilerinin özel nitelikli kişisel veri olduğunun farkında olan katılımcı oranı %83,3'tür. Katılımcıların %67,1'i sağlık verilerinin Kişisel

Verilerin Korunması Kanunu (KVKK) kapsamında korunduğunun farkında olduklarını belirtmişlerdir. KVKK kapsamında, sağlık verileri ihlale uğradığında ne yapmaları gerektiğini bildiklerini belirten katılımcıların oranı %46,7'dir. E-devlet üzerinden sağlık verilerine kimlerin erişebileceği konusunda yetkilendirme yapabileceğini bilen kullanıcıların oranı ise %52,3'tür (Şekil-7)

Şekil 7. Dijital ortamlarda saklanan sağlık bilgilerinin güvenlik sorumluları ile ilgili İfadelere Katılım Durumu



V. DEĞERLENDİRME

Farklı demografik özelliklere sahip katılımcılar ile gerçekleştirilen ESK'nın güvenliğine yönelik farkındalığın ve beklentilerin araştırıldığı çalışma sonucunda ortaya çıkan veriler; katılımcıların büyük çoğunluğunun, özlük bilgilerini, iletişim bilgilerini, aile sağlık bilgilerini, kullandığı ilaçları, hastalık tanımlarını, laboratuvar sonuçlarını, geçirdikleri operasyonlar gibi kendilerine ait bilgileri kişisel bulduklarını göstermiştir. Ancak katılımcıların yine büyük bir kısmı aile hekimlerinin isimlerini, sağlık kuruluşlarının ve uzman doktorlarının isimlerini kişisel bulmadıklarını ifade etmişlerdir. Bu durumda katılımcılar, doktorlarını ve başvurdukları sağlık kurumlarını kişiye ait özel bir bilgi olarak görmemektedirler sonucunu doğurmaktadır.

Katılımcıların büyük bir bölümü bu bilgilerinin dijital ortamda kayıt altında olduğunun farkında olduğunu belirtmişlerdir. Katılımcıların anlamlı bir kısmı sağlık verilerinin sağlık kurumları arasında paylaşılmasından, muayene olduğu doktor haricinde bir doktorun veya sağlık çalışanının sağlık verilerini görmesinden, işverenlerinin kendilerinin bilgisi olmadan sağlık verilerine erişebileceği konusunda endişe duyduklarını belirtmiştir. Büyük bir kısmı ise sağlık verilerinin kötü amaçla kullanılabileceğini düşünmekte ve sağlık verilerine, sağlık harcamalarına kimlerin erişeceğine kendileri karar vermek istemektedir. Bu sonuçlar göstermiştir ki katılımcılar dijital ortamda kayıt altına alınan sağlık verilerinin güvenliği ve gizliliği konusunda endişelilerdir.

Katılımcıların büyük çoğunluğu sağlık verilerinin dijital ortamlarda kayıt altına alındığını bilmelerine rağmen anlamlı bir kısmı sağlık verilerine ihtiyaç duyulduğu takdirde erişemeyeceklerini ve mevcut sağlık verilerinin yanlış ve eksik bilgiler içerdiğini, sağlık verilerinin çalınıp, değiştirileceğine, kaybolabileceğine, kendilerinin bilgisi olmadan üçüncü şahıslar ile paylaşılacağını düşünmektedirler. Bunun yanı sıra bu sorular için kararsız olan katılımcı sayısı da dikkat çekmektedir. Bu sonuçlar göstermiştir ki dijital ortamlarda kayıt altına alınan sağlık verilerine güven konusunda

endişeyle yaklaşan katılımcıların %48'si yine de kişisel sağlık verilerinin devlet tarafından kanunlar kapsamında korunduğuna inanmaktadır.

Katılımcılar her ne kadar elektronik sağlık kayıtları hakkında endişe duysalar da kendilerine ait tüm verilere internet üzerinden kendilerinin ve doktorlarının erişebilmesini istediklerini belirtmişlerdir. Bu sonuca göre katılımcılar, kendilerinin ya da doktorlarının dijital ortamlar sayesinde verilerine ulaştıkları takdirde, zaman kazanacaklarını, tanı ve teşhislerinin erken bir şekilde sonuçlanabileceğinin farkında olduklarını ve sağlık verilerinin sağlık kurumları arasında paylaşılmasının, büyük bir kolaylık sağlayacağını düşünmektedirler. Katılımcıların büyük çoğunluğu zaman tasarrufu, ekonomik tasarruf ve hızlı tanı tedavi için ve daha sağlıklı bir yaşam için doktorlarının kendilerini uzaktan takip etmelerinde bir sakınca görmediklerini ve doktorlarıyla dijital ortamlardan iletişim kurmak istediklerini belirtmişlerdir.

Yine anket sonuçları gösteriyor ki katılımcılar, kayıt altına alınan sağlık verilerinden, hekimlerin yararlandığını farkındadır ve kimlikleri gizlenip, verileri anonimleştirildiği takdirde, sağlık verilerinin bilimsel araştırmalar için kullanılmasından rahatsız değillerdir. Her ne kadar dijital ortamlarda verilerin kaydedilmesi hakkında tam güven oluşmasa da katılımcılar dijital sağlık verilerinin her anlamda hayatlarını kolaylaştıracaklarını düşünmektedirler. Kişisel sağlık verilerinin devlet tarafından korunması gerektiğine inanan ve sağlık verileri ile ilgili tüm hakların kendilerine ait olduğunu düşünen katılımcılar çoğunluktadır. Bu da katılımcıların sağlık verilerinin önemini farkında olduklarını ve devletin bu verilerden sorumlu olmasının farkında olduklarını göstermiştir. Devlet tarafından sağlık verilerinin korunması gerektiğini düşünen katılımcılar, sağlık verilerinin KVKK tarafından korunduğunu bildiklerini belirtmişlerdir. Ancak büyük bir çoğunluk sağlık veri ihlali yaşadıklarında KVKK kapsamında ne yapacaklarını bilip bilmediklerini konusunda kararsız olduklarını veya ne yapacaklarını bilmediklerini dile getirmişlerdir. Limon'un (2019) çalışmasında da ifade ettiği gibi sağlık çalışanları yanında, halkın da bu konuda eğitilmesi ve bilgi güvenliği okuryazarlığının yüksek seviyelere getirilerek bireylerin de kendi sağlık kayıtlarının güvenliği hakkında sorumluluk almalarını sağlanmalıdır (Limon, 2019).

Günümüzde verilerin artık teknolojiyle entegre olup, dijitalleştirilmeden saklanması imkânı olmadığı aşikârdır. Çalışma bulgularımız Ögütçü ve diğerleri tarafından 2011 de yapılan benzer çalışma ile kıyaslandığında Türkiye'de yaşayan hasta ve potansiyel hastaların elektronik sağlık kayıtlarının içeriği, hassasiyeti ve elektronik sağlık kayıtlarına erişim yetkilendirmeleri konusuna yönelik farkındalıklarının geçen 10 yılda arttığı gözlemlenmiştir. 10 yıl önce katılımcıların hangi verilerin, bu kayıtlara dâhil olduğuna yönelik ve sağlık sisteminde yer alan bilgi sistemlerinin birbirleri ile entegre çalıştığına yönelik farkındalık seviyeleri oldukça düşükken günümüzde bu seviye oldukça yüksektir (Ögütçü vd., 2011). Çetin ve Çevik'in 2021 yılında bu çalışmadan farklı olarak hemşirelik öğrencileri üzerine yaptıkları çalışmada da hemşirelik öğrencilerinin kişisel verilerin kaydı ve korunmasına ilişkin tutumlarının olumlu olduğu ve farkındalıklarının yüksek olduğu saptanmıştır (Çetin ve Çevik, 2021). Filik ve Ünalın'ın tıbbi sekreterlerde bilgi güvenliği farkındalık düzeyine ilişkin yaptıkları çalışmada özellikle kadın çalışanların bilgi güvenliği farkındalığının yüksek seviyede olduğu ifade edilmiştir (Filik ve Ünalın, 2021). Bu durum katılımcıların geçen on yılda gelişen teknolojilere adaptasyonunun arttığı, dijital sağlık uygulamalarının (e-nabız vb.) yaygınlaşması ve buna paralel olarak da insanların bilgi düzeyinin artması şeklinde açıklanabilir.

VI. SONUÇ VE ÖNERİLER

İçinde bulunduğumuz bilişim çağında, 2019 pandemisinin de yadsınamaz itici kuvveti ile dijitalleşme süreci öngörülemeyen bir hıza ulaşmıştır. Hem kamu kurumlarında hem de özel sektörde özellikle tıp, eğitim, pazarlama gibi alanlarda dijitalleşmeye olan ilgi artmıştır. Bu süreçte geliştirilen web tabanlı ve mobil uygulamalar ile sağlanan hizmetin kalitesi, erişim kolaylığı ve dolayısıyla kullanıcı memnuniyeti artmıştır. Sağlanan birçok avantajının yanı sıra verilerin dijital ortamlarda kaydedilmesi ve farklı amaçlarla kullanılması bireyleri sistemi kullanmaya ve geliştiricilere olan güvenini sorgulamaya sevk etmektedir. Bu araştırma kişi mahremiyetinin en yüksek seviyede olduğu

sağlık sektöründe, bireylerin elektronik sağlık kayıtlarının farkındalığını belirlemek amacıyla yapılmıştır.

Araştırmada katılımcılara; elektronik ortamlarda kayıt altına alınan verileri ne derece kişisel buldukları, verilerin dijital ortam ve uygulamalarda kayıt altına alındığının farkındalığı, sağlık bilgilerinin gizliliği, elektronik ortamlarda saklanması, kullanımı ve güvenlik sorumluları ile ilgili farkındalık ve beklentilerine yönelik sorular yöneltilmiştir. Araştırmada, Türkiye’de yaşayan hasta ve potansiyel hastaların elektronik sağlık kayıtlarının içeriği, hassasiyeti ve elektronik sağlık kayıtlarına erişim yetkilendirmeleri konusuna yönelik farkındalıklarının yüksek olduğu ve fakat dijital ortamda kayıt altına alınan sağlık verilerinin güvenliği ve gizliliği, herhangi bir ihlal karşısında izlenecek yol konusunda endişeleri olduğu yönünde sonuçlar elde edilmiştir.

Dijital ortamlarda tutulan sağlık verileri ile ilgili kaygılı ve kararsız olan bireylere: (i) dijital ortamların güvenlik ve gizlilik ilkeleri hakkında (ii) kişisel veri ihlali yaşadıklarında, hangi kamu kurum, kuruluşlar ve kanunlar ile korundukları ve yasal hakları hakkında (iii) herhangi bir mağduriyet durumunda hangi kuruma başvurmaları nasıl bir yol haritası izlemeleri konusunda bilgilendirilme yapılması gerekmektedir. Bu bilgilendirme neticesinde kamu kurum, kuruluş ve kanunlara güvenin daha da artacağı ve dijital ortamlar ile ilgili gizlilik ve güvenlik endişelerinin giderileceği öngörülmektedir. Çünkü araştırma sonucunda sağlık sektöründe çalışan bireylerin elektronik sağlık kayıtları ile ilgili farkındalıklarının daha yüksek olduğu saptanmıştır. Bu da sağlık sektörünün içinde yer alan bireylerin sistem ile ilgili yeterince bilgi sahibi olduğu ve bu bilgiler sonucunda ortaya çıkabilecek durumların farkında olduğunu göstermektedir. Diğer yandan katılımcılar eğitim seviyelerine göre değerlendirildiğinde, eğitim seviyesinin yükselmesi ile birlikte farkındalığın da arttığı saptanmıştır. Bu sebeplerle, öncelikli yayınlar ve kamu spotları ile yazılı ve görsel basında, sosyal medya platformlarında tüm vatandaşların erişebileceği düzeyde Kişisel Verileri Koruma Kurumu ve T.C. Sağlık Bakanlığı tarafından bilgilendirici eğitimler, kampanyalar düzenlenmesi önerilmektedir.

Etik Kurul İzni: Çalışmanın, Başkent Üniversitesi Sosyal ve Beşeri Bilimler Sanat Araştırma Kurulu tarafından 9.03.2021 tarihli 17162298.600-68 sayılı Etik Kurul onayı mevcuttur.

KAYNAKLAR

- Archer, N., Fevrier-Thomas U., Lokker C., McKibbin K.A., & Straus S.E. (2011). Personal health records: a scoping review. *Journal of the American Medical Informatics Association*, 18(4), 515-522.
- Arslan, E. T., & Demir, H. (2017). Sağlık çalışanlarının hasta mahremiyetine ilişkin tutumu: nitel bir araştırma. *Bolu Abant İzzet Baysal Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 17(4), 191-220.
- Ayala, L. (2016). Cyber-physical attack recovery procedures. In *Cyber-Physical Attack Recovery Procedures* Apress, Berkeley, CA, 1-14.
- Başalp, N. (2015). Avrupa Birliği veri koruması genel regülasyonu'nun temel yenilikleri. *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi*, 21(1), 77-106.
- Bayardo, R. J., & Agrawal, R (2005, April). Data privacy through optimal k-anonymization. In *21st International conference on data engineering (ICDE'05)* (pp. 217-228). IEEE.
- Calvaresi, D., Schumacher, M., & Calbimonte, J. P. (2020, October). Personal data privacy semantics in multi-agent systems interactions. In *International Conference on Practical Applications of Agents and Multi-Agent Systems* (pp. 55-67). Springer, Cham.

- Chik, W. B. (2013). The singapore personal data protection act and an assessment of future trends in data privacy reform. *Computer Law & Security Review*, 29(5), 554-575.
- Çetin, S. P., & Çevik, K. (2021). Hemşirelik öğrencilerinin hastaların kişisel sağlık verilerinin kayıt ve korunmasına ilişkin tutumları. *Dokuz Eylül Üniversitesi Hemşirelik Fakültesi Elektronik Dergisi*, 14(3), 199-206.
- Dülger, M. V. (2015). Sağlık hukukunda kişisel verilerin korunması ve hasta mahremiyeti. *İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi*, 1(2), 43-80.
- Entzeridou, E., Markopoulou, E., & Mollaki, V. (2018). Public and physician's expectations and ethical concerns about electronic health record: Benefits outweigh risks except for information security. *International Journal of Medical Informatics*, 110, 98-107.
- Filik, T., & Ünalın, D. (2021). The evaluation of the effect of the information security awareness level in medical secretaries on the security and privacy implementations of electronic health records. *Hacettepe Sağlık İdaresi Dergisi*, 24(1), 183-202.
- Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., & Spiegel, J. (2012). The law of cyber-attack. *California Law Review*, 817-885.
- Häikiö, J., Yli-Kauhaluoma, S., Pikkarainen, M., Iivari, M., & Koivumäki, T. (2020). Expectations to data: Perspectives of service providers and users of future health and wellness services. *Health and Technology*, 1-16.
- HIMSS, Healthcare Information and Management Systems Society North America (2018). *2018 HIMSS cybersecurity survey*. https://www.himss.org/sites/himssorg/files/u132196/2018_HIMSS_Cybersecurity_Survey_Final_Report.pdf
- Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, 80(5), 973-993.
- Knight, A. (2017). Towards a new approach to the legal definition of personal data and a jurisdictional model of data protection law: surpassing the requirement for an assessment of identifiability from data with an effects-based approach. Doctoral Dissertation, University of Southampton.
- Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology and Health Care*, 25(1), 1-10.
- Küzeci, E. (2019). *Kişisel verilerin korunması*, 3.Baskı, Seçkin Yayıncılık, Ankara.
- Limon, S. (2019). Hastanelerdeki tıbbi dokümanların geleneksel ortamdan elektronik ortama dönüşümü. *Uygulamalı Sosyal Bilimler ve Güzel Sanatlar Dergisi*, 1(1), 30-39.
- O'Leary, D. E., Bonorris, S., Klosgen, W., Khaw, Y. T., Lee, H. Y., & Ziarko, W. (1995). Some privacy issues in knowledge discovery: the OECD personal privacy guidelines. *IEEE Expert*, 10(2), 48-59.
- Öğütçü, G., Köybaşı, N. A. G., & Cula, S. (2011). Elektronik Sağlık Kayıtlarının İçeriği, Hassasiyeti ve Erişim Kontrollerine Yönelik Farkındalık ve Beklentilerin Değerlendirilmesi. *Tıp Bilişim Derneği*, 88-97.
- Özdamar, K. (1999). *Paket programlar ile istatistiksel veri analizi-1: SPSS-MINITAB*. Kaan Kitabevi, İstanbul.

- Özkan, Ö. (2011). *Attitudes and opinions of people who use medical services about privacy and confidentiality of health information in electronic environment*. Master's thesis, Middle East Technical University.
- Safran, C., Bloomrosen, M., Hammond, W. E., Labkoff, S., Markel-Fox, S., Tang, P. C., & Detmer, D. E. (2007). Toward a national framework for the secondary use of health data: an American Medical Informatics Association White Paper. *Journal of the American Medical Informatics Association*, 14(1), 1-9.
- Schwartz, P. M. (2003). Property, privacy, and personal data. *Harvard Law Review*, 117, 2056.
- Schwartz, P. M., & Solove, D. J. (2014). Reconciling personal information in the United States and European Union. *California Law Review*, 102, 877.
- Spencer, K., Sanders, C., Whitley, E. A., Lund, D., Kaye, J., & Dixon, W. G. (2016). Patient perspectives on sharing anonymized personal health data using a digital system for dynamic consent and research feedback: a qualitative study. *Journal of medical Internet research*, 18(4), 66.
- SB., Türkiye Cumhuriyeti Sağlık Bakanlığı (2007, Ocak 13). *Sağlıkta dönüşüm programı* <https://www.saglik.gov.tr/TR,11415/saglikta-donusum-programi.html>.
- Yılmaz, E., Ulus, H., & Gönen, S. (2015). Bilgi toplumuna geçiş ve siber güvenlik. *Bilişim Teknolojileri Dergisi*, 8(3), 133.