Mobil Ortamda Kişisel Verilere Yönelik Gizlilik ve Güvenlik Yaklaşımları: Mobil Sağlık Uygulamaları Üzerine Bir Değerlendirme[1]

Şahika Eroğlu
Hacettepe Üniversitesi, Edebiyat Fakültesi, Bilgi ve Belge Yönetimi Bölümü, sahikaeroglu@hacettepe.edu.tr

Tolga Çakmak
Hacettepe Üniversitesi, Edebiyat Fakültesi, Bilgi ve Belge Yönetimi Bölümü, tcakmak@hacettepe.edu.tr

Öz: *Mobil uygulama pazarında büyük bir paya sahip olan mobil sağlık uygulamaları da kişisel verilerin yoğun kullanımı ile öne çıkmaktadır. Mobil sağlık uygulamalarının yaygın kullanımı ise kişisel verilerin gizliliği ve güvenliğine yönelik kaygıları beraberinde getirmektedir. Mobil sağlık uygulamaları temelinde sıklıkla kullanılan özel nitelikli kişisel veriler olarak ele alabileceğimiz sağlık verilerinin, bu uygulamalarda yetkisiz kullanımı, üçüncü kişilerle paylaşımı, hukuka aykırı olarak ele geçirilmesi, işlenmesi ayrımcılık başta olmak üzere bireylerin farklı kapsamlarda zarara uğramasına neden olmaktadır. Bu çalışmada, mobil sağlık uygulamalarında kişisel verilerin gizliliği ve güvenliğine yönelik yaklaşımların literatür kapsamında betimlenmesi amaçlanmıştır. Bu doğrultuda çalışma, mobil ortamda kişisel verilerin gizlilik ve güvenliğini mobil sağlık uygulamaları özelinde değerlendirerek konuya yönelik yaklaşımları sunmaktadır. Değerlendirilen literatür kapsamında, mobil sağlık uygulamalarında yaşanan kişisel verilerin gizliliği ve güvenliğine yönelik sorunlar vurgulanmış ve konuya yönelik önerilere yer verilmiştir. Bu çerçevede mobil sağlık uygulamalarının geliştirilmesinde kişisel verilerin gizliliği ve güvenliğine, konuyla ilgili risklere ve yasal düzenlemelere yönelik farkındalıkla hareket edilmesi önerilmiştir. Diğer yandan çalışmada vurgulanan bir diğer öneri ise kullanıcıların mobil sağlık uygulamalarını kullanımlarında veri paylaşım izinlerine dikkat etmeleridir.*
Anahtar Kelimeler: *Kişisel veri, kişisel veri gizliliği, kişisel veri güvenliği, mobil sağlık uygulamaları.*

Giriş

Günümüzde kişisel veri olarak adlandırabileceğimiz çoğu verinin mobil cihazlar aracılığı ile oluşturulduğunu, paylaşıldığını ve depolandığını söylemek mümkündür. Kullanıcıların veri erişim, üretim ve toplama olanaklarını artıran mobil teknolojiler, anlık olarak da üretilebilen içerikleri kaydeden bir depolama alanı olarak da kullanılmaktadır. Özellikle 2008 yılında Apple tarafından ilk uygulama mağazasının lanse edilmesinden bu yana, bilgisayarlarca yapılabilecek çoğu işlem mekân ve cihazdan bağımsız olarak yapılabilir bir hale gelmeye başlamıştır. Neredeyse hepsi kişiselleştirilebilir ve çoğunlukla bireysel olarak sahip olunan akıllı telefonlar ve uygulamalar günlük hayattaki ihtiyaçlarımızın önemli bir bölümünü gidermemize de olanak tanımaktadır. Fotoğraf çekmekten, haber okumaya, bankacılık hizmetlerinden çevrimiçi alışverişe kadar geniş bir yelpazede geliştirilen bu uygulamalar sektörel hizmetlerin tasarlanmasında da kullanılmaya başlanmıştır. Kullanımı gittikçe yaygınlaşan ve çoğunlukla kişisel verilere erişimi olan uygulamaların söz konusu verilerin gizliliği ve güvenliğine yönelik sundukları çerçeve çeşitli kaygıları da beraberinde getirmektedir. Mobil uygulamaların çoğu zaman işlevleri dışında fazladan kişisel veri talep etmeleri, kullanıcıların izni ve rızası dışındaki verileri toplaması, izlemesi ve işlemesi bu kaygıların temelini oluşturmaktadır (Hong, Liu, Cheng, Ren ve Chen, 2017; Zhang ve diğerleri, 2018).

Mobil teknolojiler, hemen hemen bütün sektörlerde olduğu gibi sağlık sektöründe de yoğun bir kullanıma sahiptir. Her yere taşınabilen ve her an kullanılabilen mobil teknolojiler, iletişimi sağlamanın yanı sıra kullanıcıların hayatlarını iyileştirmek adına farklı olanaklar da sunmaktadır. Bu bağlamda mobil teknolojilerin geliştirilen uygulamalarla birlikte sağlık hizmetlerine erişim sağlama noktasında olumlu katkılarının olduğunu söylemek mümkündür. Mobil sağlık uygulamaları olarak da adlandırılan bu uygulamalar, sağlıklı ve iyi yaşam hedeflerinin yanı sıra, medikal uzman eğitimi, hasta eğitimleri ve kişiselleştirilmiş sağlık bilgi sistemlerine erişimi de

[1] Bu çalışma, Prof. Dr. Nazan Özenç Uçak'a Armağan olarak hazırlanan kitap için yazılmış ve değerlendirmeler sonucunda yayına kabul alan bölümün yayın öncesi kopyasıdır.

amaçlamaktadır (Sunyaev, Dehling, Taylor ve Mandl, 2014). Bu alandaki uygulamaların en temel işlevi, kullanıcıların verilerini toplayarak onların sağlığına özgü teşhiste bulunabilmesi ya da aktivitelere (yürüyüş, koşu, uyku gibi) bağlı olarak değişen (adım sayısı, nabız gibi) yönelik verileri görselleştirerek sunabilmesidir. Bu işlevde de söz konusu uygulamayı kullananların özel ve hassas nitelikteki tıbbi bilgilerini paylaşmaları önem taşımaktadır.

Mevcut mobil sağlık uygulamalarının sayılarının çokluğu ve çeşitliliği nedeniyle, bilgi güvenliği ve gizliliği üzerindeki etkilerin belirsiz ve karmaşık olduğu söylenebilir. Kişisel verilerin gizliliği ve güvenliğine yönelik ihlal yaşayan kullanıcılar mal kaybı, sosyal sigorta sorunları, işyeri ayrımcılığı, genetik ayrımcılık ve itibar kayıplarına uğrayabilmektedir (Parker ve diğerleri, 2017; "Privacy and Mobile Apps", 2019). Konuyla ilgili olarak Avancha, Baxi ve Kotz (2012) bilgi güvenliği ve gizliliğin ihlalinin yalnızca özel, hassas bilgilerin sızmasına veya manipüle edilmesine neden olmakla kalmayıp, aynı zamanda sağlığa zarar verme ve hatta ölüme bile yol açabileceğini belirtmektedir (Avancha, Baxi ve Kotz, 2012). Bu ihlallerle açığa çıkan bilgilerin kötüye kullanımıyla kullanıcıları sağlıklarını olumsuz etkileyecek davranışlarda bulunmaya yönlendirmenin de mümkün olduğunu söyleyebiliriz.

Literatürde mobil uygulamalara yönelik olarak kişisel ve hassas verilerin kullanım ihlallerine, mahremiyet risklerine, alınabilecek önlemlere, geliştirilebilecek sistem, model ve düzenlemelere yönelik birçok çalışmanın yapıldığı görülmektedir. Söz konusu çalışmaların konuyu teknik, yasal ve kullanıcı algıları/kültür bağlamında değerlendirdiği gözlenmektedir. Bu doğrultuda literatürde mobil uygulama sistemlerinin teknik gereklilik ve yeterlilikleri (Al Ameen, Liu ve Kwak, 2012), gizlilik ve güvenlik sistem değerlendirmeleri ve modellemeleri (Al Ameen, Liu ve Kwak, 2012; Avancha, Baxi ve Kotz, 2012; Enck ve diğerleri, 2010; Yan, Chen ve Shen, 2014), kötü amaçlı yazılım kodu algılaması ve bunlara yönelik ara yazılım geliştirme (Dagon, Martin ve Starner, 2004; Enck, Ongtang ve McDaniel, 2009; Luo, Hao, Du, Wang ve Yin, 2011; Zhou, Zhang, Jiang ve Freeh, 2011), kullanıcı odaklılık (Giannetsos, Dimitriou ve Prasad, 2011), mobil uygulama üreticilerin uygulama geliştirme süreçlerinde yararlanabilecekleri gizlilik ve güvenlik kriterlerinin belirlenmesi ve politikaların değerlendirilmesi (Rowan ve Dehlinger, 2014) gibi konuyu farklı açılardan ele alan çalışmalar yayımlanmıştır.

Günümüzde birçok mobil uygulama kişisel verileri kullanmaktadır. Bu uygulamalar kapsamında yer alan mobil sağlık uygulamaları ise topladığı kişisel verinin boyutu ve niteliği bakımından birçok mobil uygulamanın topladığı kişisel veriden farklılık göstermektedir. Bu uygulamalar genellikle kullanıcıların özel nitelikli hassas verilerini depolama, bu verileri kullanarak tanı koyma, tedavi önerilerinde veya yönlendirmelerde bulunma gibi özelliklere sahip olmalarıyla diğer uygulamalardan ayrılmaktadır. Sunduğu özelliklerin neredeyse tamamı kişisel ve hassas nitelikte verilere dayanan bu uygulamalardaki gizlilik ve güvenliğe yönelik çalışmalar, sağlık verilerine yönelik ihlallerin oluşmaması, ilgili risklerin belirlenmesi ve kötüye kullanım gibi durumların ortaya çıkmaması ya da bu tür durumlara yönelik tedbirlerin alınması açısından önem taşımaktadır.

Bu çalışmada kullanımı gittikçe artan mobil sağlık uygulamalarının özel ve hassas nitelikli kişisel veri kullanımına dayanan yapılarının kişisel verilerin gizliliği ve güvenliği kapsamında değerlendirilmesi amaçlanmaktadır. Belirlenen amaç doğrultusunda çalışmada öncelikle mobil ortamda kişisel veri paylaşımı kapsamında gizlilik ve güvenlik konusu ele alınmaktadır. Bu bölümün ardından Mobil Sağlık Uygulamaları başlığı altında mobil uygulamaların bir türü olarak nitelendirilen bu uygulamaların özellikleri literatürdeki çalışmalara dayanarak sunulmuştur. Mobil Sağlık Uygulamalarında Kişisel Verilerin Güvenliği ve Yasal Düzenlemeler başlığı altında ise söz konusu uygulamalardaki kişisel veri güvenliğiyle ilgili riskler anlatılırken bu konuya yönelik yasal düzenlemeler detaylandırılmıştır. Değerlendirme ve Sonuç başlığında ise mobil sağlık uygulamalarında yaşanan, kişisel verilerin gizlilik ve güvenliği sorunlarına değinilmekte ve bu sorunlara yönelik değerlendirme ve önerilere yer verilmiştir.

Mobil Ortamda Kişisel Veri Paylaşımı Kapsamında Gizlilik ve Güvenlik

Kimliği belirtilen veya belirtilebilen gerçek kişi ile ilgili tüm bilgiler olarak tanımlanan kişisel veri kavramına yönelik (Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi, 1981) literatürde yapılmış benzer tanımlara rastlansa da nelerin kişisel veri kapsamında değerlendirileceği veya tamamlanabileceği ile ilgili halen belirsizlikler yaşanmaktadır. Kişisel verilerin gizliliğinin ihlalinin suç teşkil

ettiği göz önüne alındığında kişisel veri tanımını karşılayan verilerin net bir şekilde ortaya konulması önem taşımaktadır. Bu bağlamda yapılan bir çalışmada kişinin tüm yaşamına ilişkin verilerin kişisel veri olarak kabul edilmesi gerekliliği vurgulanmıştır. Kişinin hizmet aldığı sağlık birimindeki verilerinden, fiziksel özelliklerini barındıran tüm veriler, sosyo-ekonomik durumuna ilişkin verilerin hepsi kişisel veri olarak örneklendirilmiştir (Yılmaz, 2016). Konu ile ilgili Türkiye'deki mevzuat incelendiğinde kişisel verinin Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi (1981) ile benzer şekilde tanımlandığı görülürken ilgili Kanunda da kişisel veri kapsamının net olarak çizilmediği görülmektedir. (Kişisel Verilerin Korunması Kanunu, 2016).

İlgili mevzuat incelendiğinde kişisel verinin "Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi" temsil ettiği vurgulanırken kişisel veri kapsamının net olarak ortaya konulmadığı görülmektedir (Kişisel Verilerin Korunması Kanunu, 2016). Diğer yandan, aynı Kanunda özel nitelikli kişisel veriler tanımlanırken "Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri" olarak tanımlanmıştır. Özel nitelikli kişisel verilerin ayrı tanımlanmasında ilgili verilerin öğrenilmesi halinde kişi hakkında ayrımcılık yapılmasına veya mağduriyete neden olabilecekleri nedeniyle ayrıntılandığı vurgulanmaktadır (KVKK, t.y). Genel olarak değerlendirildiğinde, ilgili mevzuatlarda kişisel veri tanımlamalarında net belirtilebilen kişisel verilerin (kişinin adı, adresi, doğum tarihi, telefon numarası vb.) sınırlığı olduğu görülmektedir. Bu noktada kavram sınırlarının tam bir netlik gösterememesinin konuya yönelik belirsizlik yarattığı söylenebilir. Konuya yönelik yapılan bir çalışmada kişisel verinin tanımlanmasında dört başlıktan yararlanılabileceği belirtilmektedir. Buna göre kişisel veriler:

- Hakkınızdakiler : Ad, soyad, adres, cinsiyet, e-posta vb.
- Sizin tarafınızdan sağlanan veriler: Durum güncellemesi, fotoğraf, video vb.
- Hareketler vasıtasıyla yaratılan ve dijital sistemlerin gözlenmesi ile elde edilen veriler: Akış verileri, coğrafi konum logları, satın alma işlemleri vb.
- Hakkınızdaki çıkarımlar ile elde edilen veriler: Diğer verilerin analizi ile elde edilebilen kişisel veriler olarak tanımlanabilmektedir (Introduction to the Personal Data Ecosystem, 2019)

Internetin yoğun kullanımı ile neredeyse hayatımızın her anında kullandığımız mobil teknolojiler kişisel verilerin açığa çıkmasını kolaylaştırmaktadır. Çevrimiçi ortamlarda bireyler, kişisel verilerini, bazen bilerek bazen de bilmeden, mal ve hizmet satın alma, oyun oynama, e-öğrenme veya vergi ödeme gibi birçok farklı amaç için sunmaktadırlar. Elektronik ayak izleri olarak da adlandırabileceğimiz kullanıcı eylemleri sonucunda ortaya çıkan kişisel veriler birçok alanda ilgi uyandırmaktadır.

Söz konusu veriler tahminsel analitik yöntemler aracılığı ile bilgi ekonomisinde alınıp satılabilen bir meta haline gelmiştir. Değeri gittikçe artan bu verilerin toplanması, kullanıcıların mahremiyetine yönelik tehdit ve tehlikeleri de beraberinde getirmektedir. Kişisel veriler birçok yönden kötüye kullanılabilmektedir. Çevrimiçi ortamlarda açığa çıkan, toplanan ve farklı tekniklerle anlamlandırılabilen veriler, bireylerin özel yaşamları, siyasal düşünceleri, sosyal statüleri, arkadaşlık ilişkileri, politik yönelimleri gibi bilgilerini ortaya çıkarırken, bu durum, bireylerin özel hayatlarının gizliliğini de ihlal edebilmektedir (Boyd ve Ellison, 2007). Google, Facebook gibi hizmet sağlayıcıların aynı zamanda kişisel verileri de toplaması ve bu verilerin paylaşımının farklı sektörler açısından rekabet ve güç kaynağı olarak kullanılabilmesi bu kaygıların açığa çıkmasını tetiklemektedir (Hong ve diğerleri, 2017; Lutz ve Strathoff, 2014; Zhang ve diğerleri, 2018). Bu doğrultuda literatürde de konu stalking, siber zorbalık ve diğer gizlilik ihlalleri başlıkları kapsamında yoğun bir şekilde ele alınmaktadır (Lutz ve Strathoff, 2014).

Günlük yaşamda her alanda kullanılmaya başlanan mobil cihazlar ve mobil uygulamalar ile kullanıcılar, rutin hayat süreçlerinde gerekli olan birçok işlemi yapabilmektedir. Kullanılan mobil uygulamaların zaman zaman işlevleri dışında fazla kişisel veri talep etmeleri, kullanıcıların farkında olmadan gereksiz verilerinin toplanması ve işlenmesi kullanıcı mahremiyetini etkileyebilmektedir (Hong ve diğerleri, 2017; Zhang ve diğerleri, 2018). Bu noktada kullanıcılar, kullanımı gittikçe yoğunlaşan, çok sayıda ve benzer özelliklerde olan çoğu uygulamanın güvenliği konusunda kaygılar duymaktadır. Kişisel verilerin farklı araç ve tekniklerle işlenmesi, kullanıcıların

güvenliği ve gizliliği için önemli riskler oluşturmaktadır. Bu riskler çoğunlukla kişisel verilerin üçüncü taraf hizmetlerin ve yazılımların kullanımları için paylaşılması ile ilişkilendirilmektedir. Bunun yanı sıra riskler, mobil cihazlarda tutulan veri ve sensör çeşitleri ile kullanıcıların izlenmesi olasılığının artması, karmaşık mobil uygulama ekosistemi gibi nedenlere de dayandırılmaktadır (ENISA, 2017). Uygulamaların dinamik yapısı nedeniyle nasıl çalıştığının anlaşılmasının karmaşık olması, farklı ağlar ve sistemlerle iletişim halinde olmaları gibi özellikleri de gizlilik ve güvenlik değerlendirmelerini zorlaştırmaktadır. Mobil cihazlarda hassas kaynaklara (veya verilere) haksız erişimden kaynaklanan mahremiyet riskleri bulunmaktadır. Bu bağlamda kullanılan mobil uygulamalarda gizlilik kaygılarının azaltılması ve sistemlerin seçimleri üzerine farklı modeller üretildiği ve çalışmalar yapıldığı görülmektedir. Genel olarak değerlendirildiğinde mobil uygulamaların güvenirliğinin önemine vurgu yapılan çalışmalarda, güvenilirlik sağlanması üzerine modellerin önerildiği görülmektedir (Dadhich, Dutta ve Govil, 2011; Lin ve Varadharajan, 2010; Yan ve diğerleri, 2014).

Milyonlarca uygulama üreticisi ve akıllı telefon kullanıcısını kapsayan ve dünyanın büyük endüstrilerinden birisi haline gelen mobil uygulama ekosistemi 2017 yılında yapılan bir istatistiğe göre yaklaşık 197 milyar uygulama üretmiştir. Bu uygulamalarda az sayıda uygulama geliştiricisinin veri koruma zorunluluklarını sağladığı belirtilmektedir (ENISA, 2017). Bu çerçevede değerlendirildiğinde, uygulama geliştiricilerin gizlilik ve güvenlik gereksinimlerini uygulamada nasıl düzenleyebilecekleri ve araçlarına nasıl uygulayacakları konularına yönelik farkındalık ve bilgi eksikliklerinin olduğu veya konunun yaptırımları konusunda yaşanan eksikliklerin geliştiricileri gizlilik ve güvenlik uygulamalarını geri planda tutmalarına neden olduğu anlaşılmaktadır.

Mobil Sağlık Uygulamaları

Mobil sağlık uygulamaları, sağlıkla ilgili bilgilerin mobil teknolojilerle bütünleştirilmesine dayanmaktadır. Bu uygulamaların sağlıkla ilgili neredeyse tüm yeniliklerden daha hızlı çoğaldığı, 2020 yılı itibariyle 300.000'in üzerinde mobil sağlık uygulamasının olduğu; bu sayının da 2015 yılındaki mobil sağlık uygulaması sayısının iki katı olduğu belirtilmektedir (levine, nature makalesi, bates, landman, levin). Literatürde mobil sağlık uygulamalarının potansiyel faydaları üzerine değerlendirmelerin yapıldığı dikkati çekmektedir. Bu çerçevede söz konusu uygulamaların; sağlık kurumlarının kullanılabilirliğini ve teknoloji kullanımına yatkın sağlık personelinin verimliliğini artırması, hasta ve yakınlarının sağlık bilgi düzeyinin gelişimine etki etmesi, sağlık maliyetlerinin azalması gibi yararlarının olacağı belirtilmektedir (Patrick, Griswold, Raab ve Intille, 2008).

Mobil sağlık uygulamaları ile ilgili çalışmalar yapan Research2Guidance tarafından 2017 yılında yayımlanan bir raporda da sağlık sektöründe mobil uygulama sayısının 325.000 civarında olduğu ifade edilmektedir (Research2Guidance). Ayrıca 2017 yılında yapılan bir çalışmaya göre yaklaşık olarak yılda 3.2 milyar indirme sayısına sahip olduğu belirtilmektedir (Karandeep, 2017). Bununla birlikte sağlık sektöründe hükümetlerin ve sağlık uzmanlarının aktif olarak uygulama geliştirmeye ve vatandaşların kullanımını teşvik etmeye destek verdiği bilinmektedir (eHealth, 2011; Parker ve diğerleri, 2017). Gelişen teknoloji çerçevesinde sayılarındaki artışa karşın bu uygulamaların doğrudan olmasa da zararlı olabilecek nitelikte ve kullanıcıların farketmeyebilecekleri riskler (güvenlik, karşılıklı işlerlik ve içerik ile ilgili standartlara uyumsuzluk gibi) içerebildiği dile getirilmektedir (levine). Literatürde de 2015 yılında yoğun kullanımı olan 600 uygulama üzerinde yapılmış bir çalışmada söz konusu uygulamaların yalnızca %30,5'inin gizlilik politikasına sahip olduğu vurgulanmıştır (atıf verilcek). Bu doğrultuda mobil sağlık uygulamalarındaki güvenlik ve gizlilik konularına değinmeden önce bu uygulamaların işlevlerinin ve karakteristiklerinin anlaşılması gerektiği düşünülmektedir.

Mobil sağlık uygulamaları, sağlık hizmeti sunan sağlayıcıların, kullanıcıların sağlık verilerini üretmeleri, depolamaları, aktarmaları, paylaşmaları veya bu verilere erişmeleri için geliştirdikleri etkileşime dayalı uygulamalar olarak tanımlanmaktadır (Helm ve Georgatos, 2014, s. 134). Literatürdeki çalışmalarda ayrıca, mobil sağlık uygulamalarının işlevlerine göre kategorilere ayrılarak değerlendirildiği dikkati çekmektedir. Bu çalışmalardan birinde mobil sağlık uygulamaları işlev olarak iki gruba ayrılmıştır. Bunlardan biri kişisel düzeyde sağlıkla ilgili aktivite takibi yapan, bu aktiviteleri analiz eden ve sosyal medya paylaşımı gibi özellikler taşıyan kullanıcı uygulamalarıdır. Diğer grupta ise sağlık kuruluşları ve çalışanları için geliştirilmiş olan belirli bir konuda bilgi sağlayan, tanı koyma ve tedavi önerme gibi klinik kararları destekleyici nitelikte içerik sunan, elektronik sağlık kayıtlarına erişim sağlayan veya hastaları uzaktan takip etme özelliğine sahip uygulamalar bulunmaktadır

(Helm ve Georgatos, 2014). Benzer bir diğer çalışmada da mobil sağlık uygulamalarının sunduğu hizmete göre gruplandırdığı görülmektedir. Boulos, Brewer, Karimkhani, Buller ve Dellavalle (2014) tarafından yapılan çalışmada tıbbi hizmet sağlayıcılar için geliştirilen uygulamaların bu alana yönelik terminoloji içerdiğini ve daha çok uzmanlık gerektiren bir kullanıma hitap ettiği belirtilmiştir. Bu çalışmada önceki çalışmadan farklı olarak mobil sağlık uygulamalarının belirli bir hastalığa ya da uzmanlık alanına odaklanan uygulamalar ile tıbbi eğitim ve öğrenim uygulamalarını da içerdiği ifade edilmiştir. Kotz, Gunter, Kumar ve Weiner (2016) ise mobil sağlık uygulamalarını topladıkları ve sundukları veriler çerçevesinde sınıflandırmıştır. Buna göre mobil sağlık uygulamalarının kalp atışı, kan basıncı gibi fizyolojik parametreleri izleyen uygulamalar, belirli bir hareketin, fiziksel ya da sosyal aktivitenin veya sağlıkla ilgili davranışları raporlayan, kaydeden ve ölçümleyen uygulamalar, sağlık kayıtlarına ve kullanıcıların diğer verilerine erişim sağlayan uygulamalar ile hastalarla sağlık hizmeti sunanlar arasında iletişim kurmada kullanılan teletıp uygulamaları olarak dört grupta değerlendirildiği görülmektedir. Bir diğer çalışmada ise literatürde yer alan sistematik değerlendirmelerden ve meta-analizlerden hareketle mobil sağlık uygulamalarının işlevleri belirlenmiştir (Rowland, Fitzgerald, Holme, Powell ve McGregor, 2020). Buna göre mobil sağlık uygulamaları klinik karar verme ve tanı koyma, tedaviye uyum sağlamada kullanıcıları davranış değişikliğine yönlendiren uygulamalar, dijital terapi uygulamaları ve hastalıkla ilgili eğitim veren uygulamalar olarak gruplanmıştır. Bu çalışmaları genel olarak değerlendirdiğimizde mobil sağlık uygulamalarının kullanıcı grubuna göre, topladığı veriye göre ve sağlıkla ilgili odaklandığı konulara göre gruplandığı anlaşılmaktadır. Yukarıda verilen çalışmalarda da belirtilen işlevler güvenlik ve gizlilik açısından ele alındığında bu uygulamaların kullanıcıların hassas nitelikli kişisel verilerinin yanı sıra belirli bir aktiviteye yönelik davranışlarını, tanı koyma ve tedavi belirleme sürecindeki kararları da kayıt altına alabilecek altyapıya sahip olduklarını söyleyebiliriz. Ayrıca belirtilen işlevler mobil sağlık uygulamalarında oluşabilecek gizlilik ve güvenlik ihlallerinin kapsamı hakkında da fikir vermektedir.

Mobil sağlık uygulamalarının işlevlerine yönelik kategorizasyona dayanan çalışmalara ek olarak bu uygulamaların güvenliğini ve etkinliğini artırmak için rehberlerin de yayınlandığı görülmektedir. Bu kapsamda Birleşik Devletler Sağlık Bakanlığına bağlı Gıda ve İlaç Ürünleri Bürosu (United States Food and Drug Administration) tarafından yayımlanan Mobil Tıbbi Uygulamalar (Mobile Medical Applications) başlıklı raporda mobil uygulamaların şu özellikleri taşıması beklenmektedir (FDA, 2015):

- Hastaların ya da kullanıcıların kendi hastalık veya durumlarını spesifik bir tedavi ya da iyileştirme önerisi almadan yönetebilmelerine imkân tanıma,
- Hasta ya da kullanıcıların sağlıkla ilgili bilgilerini basit araçlarla düzenleyebilmelerine katkıda bulunma,
- Hastaların ya da kullanıcıların sağlık koşulları ya da tedavileriyle ilgili bilgilere kolaylıkla erişim sağlama,
- Hastaların ya da kullanıcıların potansiyel sağlık durumları ile ilgili yerlerle iletişim kurmalarına, sağlık durumlarıyla ilgili bilgileri göstermelerine ve bir doküman olarak kaydetmelerine fırsat yaratma,
- Sağlık alanında hizmet verenler için basit görevleri otomatize etme,
- Hastaların ya da kullanıcıların elektronik ortamda tutulan sağlık kayıtlarına erişmeleri ve bu kayıtlarla etkileşimde bulunabilmelerine yönelik platformları oluşturma.

Yukarıda sıralanan özellikler, mobil sağlık uygulamalarının kişisel ve özel nitelikli veriler ile olan bağlantısının daha açık olarak anlaşılmasını sağlamaktadır. İlk maddede belirtilen kullanıcıların kendi hastalık ya da durumlarını yönetebilmeleri, bu uygulamaların sağlıkla ilgili kişisel verilerin kayıt altına alınmasını ve bu verilerin bir arayüz üzerinden sunulmasını gerektirmektedir. Bu yönüyle mobil sağlık uygulamalarının, kayıt altına aldığı kişisel ve özel nitelikli sağlık verilere yönelik süreçler (bu verileri düzenleme, paylaşma, görselleştirme gibi) üzerine kurgulanmış bir mimariye sahip olduğunu söylemek mümkündür. Söz konusu durum diğer maddeler açısından değerlendirildiğinde ise bu uygulamaların yalnızca veriyi depolama değil ayrıca kullanıcılara verilerini düzenlemelerine, kullanmalarına, paylaşım ve erişim koşullarını belirlemelerine, bu verilerden doküman üretmelerine de imkân tanıması gerektiğini göstermektedir. Bu noktada mobil sağlık uygulamalarında oluşabilecek güvenlik ve gizlilik ihlallerinde teknik altyapının yanı sıra kullanıcıların konuyla ilgili bilgi ve farkındalık düzeylerinin de etkisinin olacağını ifade edebiliriz.

Mobil Sağlık Uygulamalarında Kişisel Verilerin Güvenliği ve Yasal Düzenlemeler

Bütün mobil uygulamalarda olduğu gibi mobil sağlık uygulamalarında da üretilen herhangi bir veri bir başka mobil uygulama, cihaz ya da üçüncü parti kişilerle paylaşılabilmektedir. Bu noktada uygulamalarda sunulan gizlilik bildirimleri (politikaları, sözleşmeleri) ilgili uygulamanın veri paylaşımı ve kullanımında ne kadar risk taşıdığı konusunda önemli bir kılavuz olarak nitelendirilmektedir. Getirdikleri birçok avantaja karşın uygulamalar, gizlilik ve mahremiyet gibi konularda çeşitli riskler de taşıyabilmektedir. Bu çerçevede, her an internete bağlanarak veri aktarabilme ve coğrafi konum verisini işleyebilme gibi özellikler, mobil uygulamaları ideal bir izleme aracı haline getirebilmektedir. Ayrıca, konuyla ilgili çeşitli çalışmalarda, güncel mobil uygulama sağlayıcı platformların gerekli doğrulama (örn: ikili doğrulama) mekanizmalarını yapılandırmada eksikliklerinin olduğu, bu platformlardaki mobil uygulamaların bir bölümünün kullanıcıların kişisel verilerinin çalınması potansiyelini taşıdığı, bazı uygulamaların ise diğer uygulamaların reklam gelirlerini çalma amacıyla tasarlandığı vurgulanmaktadır (Su, 2014). Herhangi bir kategori gözetmeksizin birçok mobil uygulama için geçerli olan bu risklerin yanı sıra, mobil sağlık uygulamaları için de bazı spesifik risklerin bulunduğunu söylemek mümkündür. Bu riskler genel olarak şu şekilde özetlenebilir (Privacy Rights Clearinghouse, 2016):

- Birçok mobil sağlık uygulaması birçok kişisel veri (fotoğraf, ad, soyad, e-posta gibi verilerin dışında günlük yemek tüketiminden egzersiz davranışlarına kadar geniş bir yelpazede) tutmaktadır.
- Mobil sağlık uygulaması olarak kullanılan uygulamaların önemli bir bölümü reklam uygulamalarıyla gelir sağlamaktadır. Bindirme (piggybacking) olarak da adlandırılan bu tür uygulamalarda özgün uygulama, reklam ya da zararlı içerik barındırabilen kodları da taşıyabilmektedir. Bu tür uygulamalarda kişisel bilgiler kolaylıkla aktarılabilmektedir.
- Birçok mobil sağlık uygulaması bir gizlilik politikasına sahip olmasına karşın kişisel bilgilerin korunması ve gizliliğinin sağlanması konusunda şifresiz ve güvenilir olmayan ağ bağlantılarını kullanmaktadır.

Mobil sağlık uygulamalarının bilginin gizliliği ve güvenliği açısından taşıdığı riskler bu uygulamaların kullanımına yönelik karar verme süreçlerini de etkileyebilmektedir. Yapılan bir çalışmada mobil sağlık uygulamalarının kullanımına karar verme ve bu uygulamalara güven duyma konusunda da kullanıcılara yardımcı olabilecek bilgilerin (bkz. Tablo 1) standart ve şeffaf bir yapıda sunulması önerilmektedir (Albrecht, 2013).

Tablo 1. Sağlık uygulamaları ve medikal uygulamalar için değerlendirme kriterleri (Albrecht, 2013)

Ölçüt	**İçerik**	**İşlev**
Dağıtıcı/Uygulama Sahibi	Uygulamayı geliştiren veya dağıtımını sağlayan kurum ve kuruluş hakkındaki bilgiler	İletişim kurmak Sponsor ve diğer bütün paydaşlar arasındaki çıkar çatışmalarını belirlemek.
	Uygulama üstverisi	Uygulamanın genel işleyişi ile ilgili temel bilgi edinimi
Geliştirilme Gerekçeleri	Uygulama ile nelerin ve kimlerin hedeflendiğinin açıklanması ve uygulamanın sağlık kategorisinde olup olmadığının açıklanması	Uygulamanın temel işlevini, profesyonel boyutta hangi kategoride yer aldığını ve kullanım alanını anlamak.
İşlevselik	Uygulamanın sınırlarının ve özelliklerinin belirtilmesi	Uygulama ile hedeflenen amaçlara ulaşmak için geliştirilen özellikleri ve uygulamanın kullanım güvenliğine yönelik limit ve riskleri belirlemek.
	Uygulamanın kullanılabilirliği ile ilgili ne tür ölçümlerin yapıldığına dair ayrıntılar	Uygulama geliştirme süreci hakkında bilgi sahibi olmak.

Güvenilirlik ve Geçerlilik	Uygulamanın temel aldığı bilgi kaynaklarının güvenilirliği ve açıklaması	Uygulama özelliklerinin geçerli ve güvenilir bilgi kaynaklarına dayanıp dayanmadığını analiz etmek
	Kalite güvence yöntemlerinin açıklanması	Uygulamanın üretim aşamasındaki kalite düzeyini tahmin etmek
Veri Talebi ve Yönetimi	Toplanan ve işlenen veri türleri ile miktarının açıklanması	Uygulamanın veri toplama ve işleme adımlarının uygulama amaçlarıyla örtüşüp örtüşmediğini saptamak
Veri Koruma ve Gizliliği	Uygulama sağlayıcının veri koruma ve gizliliği ile ilgili yasal düzenlemelere uygun hareket ettiği ve bağlı olduğu yasal düzenlemeler hakkında bilgi	Uygulama sağlayıcının geliştirilen uygulamanın amaç ve kapsamına uygun bir veri koruma ve gizlilik açıklaması sunup sunmadığının belirlenmesi
Veri Aktarımı ve Depolama	Uygulamada kullanılan tüm verilerin korunmasına yönelik önlemlerin belirlenmesi	Veri aktarım ve depolama süreçlerinin yeterli düzeyde korunup korunmadığının analiz edilmesi

Tablo 1'de, mobil sağlık uygulamalarının kullanımına karar vermek ya da uygulamanın güvenilirliğini değerlendirebilmek ile ilgili fikir sağlayacak kriterler yedi başlıkta sıralanmaktadır. Bu başlıklar incelendiğinde, genel olarak uygulamanın özelliklerinin sıralandığı görülürken ölçütlerin önemli bir bölümünün veri ile ilgili süreçler hakkındaki açıklamaları içerdiği dikkati çekmektedir. Bilgi gizliliği ve güvenliğine yönelik unsurların temelinde insan faktörünün bulunduğu düşünüldüğünde uygulama kullanmadan önce kullanıcıların bu ölçütlere yönelik farkındalıklarının olması ve bu doğrultuda karar vermeleri önemlidir.

Mobil sağlık uygulamalarındaki gizlilik ve güvenlik uygulamalarında öne çıkan bir diğer nokta ise yasal düzenlemelerdir. Bu bağlamda özellikle mobil sağlık uygulamasının geliştirildiği konum ile verilerin depolandığı yerin bölgesel olarak farklılık göstermesi dahi veri aktarımı ve dolaşımı ile ilgili hukuki açıdan sakıncalı durumların ortaya çıkmasına neden olabilmektedir. Nitekim konuyla ilgili yasal düzenlemelerin hem ülkeler bazında hem de uluslararası boyutta oluştuğu bilinmektedir. Ayrıca mobil sağlık uygulamaları ile ilgili yasal düzenlemelerin sağlık bilgisi, veri depolama koşulları ve bilgi iletişim teknolojileri ile ilgili konuları kapsadığı belirtilmektedir (Helm ve Georgatos, 2014). Geçmişi Hipokrat yeminine kadar dayandırılabilen sağlık bilgisinin gizliliği ve güvenliği ile ilgili uygulamaların gelişen teknoloji ile birlikte farklı bir boyuta geldiği görülmektedir. Bu çerçevede sunulan ulusal ve uluslararası düzenlemelerin çoğunluğunun hasta mahremiyeti kavramından yola çıkılarak geliştirildiği söylenebilir. Bu bağlamda yapılan düzenlemelere bakıldığında, hasta hakları ve sağlık verilerinin korunması ile ilgili ilk çalışmanın 1981 yılında Lizbon'da ilan edilen Dünya Hekimler Birliği Hasta Hakları Bildirgesi olduğu görülmektedir. Bu bildirge, 1995 ve 2005 yıllarında geliştirilmiştir ("Hasta Hakları Kılavuzu", 2013). Avrupa Konseyi'nin 97(5) sayılı tavsiye kararında sağlık verilerinin toplanmasında ve işlenmesinde mahremiyet hakkına yönelik ifadelere yer verildiği görülmektedir (Yılmaz, 2016). 1983 yılında düzenlenen Dünya Tabipler Birliği 35. Genel Kurulu'nda tıbbi verilerin paylaşımına ve bu verilerin bilgisayarlarda kullanımına yönelik yönlendirmelerde bulunulmuştur (Yılmaz, 2016). 1994 yılında Amsterdam'da yayımlanan Avrupa'da Hasta Haklarının Geliştirilmesi Bildirgesi ile de hasta hakları arasında mahremiyet ve gizlilik ile ilgili konular yer almış; kişisel sağlık verisi sahibi olarak hastaların bu verilerinin ölüm sonrasında dahi gizli tutulması gereği vurgulanmıştır (Amsterdam Bildirgesi, 1994). Belirtilen bu bildirgelere ek olarak 2002 yılında Washington'da Dünya Hekimler Birliği tarafından kabul edilen bildirgede ve yine 2002 tarihli Avrupa Birliği Hasta Haklarına İlişkin Avrupa Statüsü Ana Sözleşmesinde kişisel sağlık verilerinin tanımına ve gizliliğine yönelik açıklamaların bulunduğu anlaşılmaktadır (Olca ve Can, 2014). Genel olarak ilgili düzenlemeler

incelendiğinde hasta mahremiyetinin ön plana çıkarıldığı ve 80'li yıllardan itibaren konunun yasal düzenlemelere yansıdığı görülmektedir.

Konuyla ilgili Türkiye'de mevzuat incelendiğinde Anayasanın "Özel Hayatın Gizliliği" başlığını taşıyan 20. Maddesinde, kişisel verilerinin gizliliğinin sağlanmasının anayasal bir hak olarak vurgulandığı görülür. Söz konusu maddeye 2010 yılında yapılan "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"(T.C, Anayasası, 1982) eklemesi ile kişisel verilerin işlenmesi, elde edilmesi ve kullanımının denetlenmesine yönelik düzenlemeler yapılmıştır. Bu maddeyle kişisel verilerin korunmasını hakkı Anayasa kapsamında koruma altına alınmıştır. Türk Medeni Kanunu'nun 24. Maddesi yine kişilik haklarının korunması bağlamında kişisel verilerin korunması ile hukuksal olarak ilişkilendirilen hükümler içermektedir (Türk Medeni Kanunu, 2001). Türk Ceza Kanunu'nun 134, 135 ve 136. Maddelerinde de özel hayatın gizliliği ve kişisel verilerin toplanması ve korunmasıyla ilgili çeşitli konuların düzenlendiği görülür (Türk Ceza Kanunu, 2004). Anayasa ve çeşitli kanunlar düzleminde değinilen kişisel verilerin korunması konusu 2016 yılında 6698 sayılı Kişisel Verilerin Korunması Kanunu ile ayrıntılandırılmıştır. İlgili kanunda sağlık verilerinin de içerisinde yer aldığı "Özel nitelikli kişisel verilerin işlenme şartları" 6. Madde kapsamında ele alınmıştır (Kişisel Verilerin Korunması Kanunu, 2016). Bununla birlikte 6698 Sayılı Kişisel Verilerin Korunması Kanununa istinaden ve Avrupa Komisyonunun 108 sayılı Sözleşmesi ve Avrupa Birliğinin 95/46/EC sayılı Direktifine uygun olarak Kişisel Verileri Koruma Kurumu (KVKK) oluşturulmuştur. Bu sayede kişisel verilerin korunmasına ilişkin ilk defa bir kurum yapılandırılmasına gidilmiştir (Kutlu ve Kahraman, 2017).

Temel Kanunların yanı sıra kişisel sağlık verilerinin korunmasında aşağıdaki yönetmelik ve yönergeler Türkiye'deki kurumsal uygulamalarda belirleyici olmaktadır (Kişisel…, 2016; 2017; Yataklı…, 2001; 2016; Hasta Hakları Yönetmeliği, 1998):

- Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelik,
- Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelikte Değişiklik Yapılmasına İlişkin Yönetmelik,
- Yataklı Tedavi Kurumları Tıbbî Kayıt ve Arşiv Hizmetleri Yönergesi,
- Yataklı Tedavi Kurumları Tıbbî Kayıt ve Arşiv Hizmetleri Yönergesinde Değişiklik Yapılmasına Dair Yönerge,
- Hasta Hakları Yönetmeliği.

Türkiye'de 2011 yılında çıkarılan 663 sayılı Kanun Hükmünde Kararnamenin 47. Maddesinde yer alan kişisel sağlık verilerinin toplanmasına, işlenmesine ve paylaşımına yönelik düzenlemeler bu maddenin uygulanmasından doğacak zarar ve olanaksız durumlar nedeniyle iptal edilmiştir (Sağlık…, 2011). Diğer taraftan Sağlık Bakanlığının Sağlık Bilgi Sistemleri Uygulamalarına yönelik 2015/17 Sayılı Genelgesi bilgi sistemlerinde verilerin tutulması ve güvenliği ile ilgili süreçleri içermektedir (Sağlık…, 2015). Ek olarak e-devlet ile bütünleşik bir şekilde hizmet veren Ulusal Sağlık Sistemi ve bir mobil sağlık uygulaması olan e-Nabız'daki kişisel sağlık verilerinin yönetimi ile ilgili konular 2016/6 Sayılı genelge ile ele alınmıştır (Sağlık.Net…, 2016). Genel olarak değerlendirdiğimizde kişisel sağlık verilerinin, hukuki açıdan hem kişisel verilerin korunması hem de sağlık ile ilgili mevzuat düzenlemelerinden etkilenen bir veri özelliği taşıdığı anlaşılmaktadır. Bu bağlamda sıralanan yönetmelik ve yönergeler incelendiğinde Türkiye'deki düzenlemelerin kişisel sağlık verilerinin işlenmesi, mahremiyetinin sağlanması, hasta hakları ve tıbbî kayıtların arşivlenmesi ekseninde şekillendiği dikkati çekmektedir. Bu bağlamda kişisel sağlık verilerinin gizliliği ve korunmasına ilişkin şartların daha ayrıntılı mevzuatlarda düzenlenmediği bilgi sistemlerine veya mobil sağlık uygulamalarına yönelik kapsamlı bir yapının olmadığı dikkati çekmektedir.

Değerlendirme ve Sonuç

Hayatın her alanında farklı amaçlarla kullanılabilen mobil uygulamaların etki ettiği önemli sektörlerden bir tanesi de sağlık sektörüdür. Mobil sağlık uygulamaları kullanıcıların hayatlarını iyileştirmek bağlamında farklı olanaklar sunmaktadır. Bunun yanı sıra medikal uzmanların eğitimi, hasta eğitimleri, sağlık hizmetlerinin iyileştirilmesi ve

etkinliğinin artırılması, sağlık bilgi sistemlerine erişim gibi olanakları da sunmaktadır. Mobil cihazların sağlık sektöründe kullanılması birçok avantaj sağlamasına rağmen, bu uygulamaların işlevlerini gerçekleştirirken yoğunlukla özel ve hassas nitelikli kişisel veri kullanımını gerektirmesi, söz konusu verilerin gizlilik ve güvenliğine yönelik kaygıları da beraberinde getirmektedir. Bu kaygıların, kullanıcıların kişisel verilerinin güvenliği, gizliliği ve söz konusu verilerin etik kullanımı üzerine yoğunlaştığını söylemek mümkündür. Mobil cihazlarda kişisel sağlık verilerinin tutulması, bu verilerin üçüncü şahıslar tarafından uygunsuz kullanımı, sağlık verileri güvenliği ve gizliliği konusundaki endişeleri artırmaktadır.

Mobil sağlık uygulamalarının yapısı, kullanıcıların verilerini toplayarak onların sağlığına özgü teşhis ya da aktivite takibi sağlayabilmeye dayanmaktadır. Bu durum kullanıcıların söz konusu uygulamalardan yararlanmak adına onların özel ve hassas tıbbi bilgilerini paylaşmalarını gerektirmektedir. Bu kapsamda değerlendirildiğinde, kişisel verilerin gizliliği ve güvenliğinin ihlalinin, kullanıcıların, mal ve itibar kaybına uğramaları, genetik ayrımcılık, işyeri ayrımcılığı, sigorta problemleri gibi sorunlarla karşı karşıya kalmalarına neden olduğu anlaşılmaktadır. Sağlık alanında kişisel verilerin ve hasta mahremiyetin güvence altına alınması Anayasa'da da "Özel Yaşamın Gizliliğinin Korunması" ilkesinin önemli bir ayağını oluşturmaktadır. Kişisel verilerin gizliliği ve güvenliğinin korunmamasının önceki bölümlerde de genel hatlarıyla açıklandığı gibi özel ve hassas nitelikli verilerin manipülasyonu, üçüncü partilerle paylaşımı, yanlış tedavi ve yönlendirmelere neden olacağı göz önüne alındığında konuya yönelik yapılacak çalışmaların ve alınacak önlemlerin ne denli önemli olacağı açıktır.

Mobil sağlık uygulamalarında, kişisel verilerin güvenliği ve gizliliğinin korunmasının üç bileşen (düzenlemeler, teknik ve kullanıcı) çerçevesinde değerlendirebileceğini söyleyebiliriz. Bu bileşenlerden ilki kişisel verilerin korunması ve gizliliği kapsamında sunulacak yasal ve politik düzenlemeler olarak sayılabilir. Bu bağlamda, ulusal ve uluslararası alanda düzenlemelerin varlığı bilinmektedir. Günümüzde birçok ülkede yürürlüğe konan Kişisel Verilerin Korunması Kanunu'nun sağlık verilerinin gizliliğinin korunması üzerine ayrıntılandırılmış hükümler içermesi ve bu hükümlerin kişisel verilerin işlenme koşullarını, veri depolama ve paylaşım koşullarını netleştirmesi önemlidir. Sağlık verilerinin işlenmesi, korunması ve gizliliğine yönelik Kişisel Verileri Koruma Kanunu'nun yanı sıra direkt sağlık alanını konu alan ayrıntı destekleyici kanunların oluşturulması gerekmektedir. Bu çerçevede mobil uygulama üreticilerinin ulusal ve uluslararası hükümler çerçevesinde hizmetlerini sağlamaya yönlendirilmelerinin önemi vurgulanabilir. Bu durum ilgili hizmetlerin kullanıcıların kişisel verilerinin korunması ve gizliliğinin korunması konularının hukuksal zeminlere oturtulmasını destekleyecektir. Mobil sağlık uygulamaların işledikleri veriler nedeniyle söz konusu uygulamalarda yasal altyapının yanı sıra, uygulama geliştiricilerine ve uygulama kullanıcılarına yönelik rehberler ve standartlar geliştirilmesi gerekmektedir. Nitekim, bu uygulamaların uluslararası kullanım nitelikleri göz önüne alındığında konuya yönelik otorite kurumların (Örn: KVKK) geliştireceği standart ve rehberlerin, gizliliğin korunmasına yönelik katkılarının olacağı açıktır.

Diğer tüm sistemlerde ve düzenlemelerde olduğu gibi kullanıcı faktörünün mobil sağlık uygulamalarında kişisel verilerin güvenliği ve gizliliği konusunda da önemli bir bileşen olduğunu söylemek mümkündür. Bu uygulamalardaki gizlilik ve güvenlik sistem ve düzenlemelerinin etkin olarak sürdürülebilirliği son kullanıcı eğitimleri verilmesi ve konuyla ilgili farkındalıklarının geliştirilmesi ile bağlantılıdır. Bu çerçevede, kişisel verilerin gizliliği ve güvenliğine yönelik farkındalığın artırılması, kişisel veri ve mahremiyet algılarının geliştirilmesine yönelik çalışmaların yapılması gerekmektedir. Günümüzde mobil ortamdaki servis sağlayıcılar (Google Play, App Store) farklı yeteneklerde mobil sağlık uygulamasını kullanıcıların hizmetine sunmaktadır. Neredeyse hayatın her anında kullanılabilen mobil teknolojilere mobil sağlık uygulamaları yüklenirken, kullanıcıların uygulama tarafından istenen izinleri değerlendirebilmesi önemli görülmektedir.

Kaynakça

Al Ameen, M., Liu, J. ve Kwak, K. (2012). Security and privacy issues in wireless sensor networks for healthcare applications. *Journal of Medical Systems, 36*(1), 93-101. doi:10.1007/s10916-010-9449-4

Albrecht, U.V. (2013). Transparency of health-apps for trust and decision making. *Journal of Medical Internet Research, 15*(12). doi:10.2196/jmir.2981

Amsterdam Bildirgesi. (1994). https://sbu.saglik.gov.tr/hastahaklari/amsterdam.htm adresinden erişildi.

Avancha, S., Baxi, A. ve Kotz, D. (2012). Privacy in mobile technology for personal healthcare. *ACM Computing Surveys*, *45*(1), 1-54. doi:10.1145/2379776.2379779

Boulos, M. N. K., Brewer, A. C., Karimkhani, C., Buller, D. B. ve Dellavalle, R. P. (2014). Mobile medical and health apps: state of the art, concerns, regulatory control and certification. *Online Journal of Public Health Informatics*, *5*(3), 229. doi:10.5210/ojphi.v5i3.4814

boyd, d. m. ve Ellison, N. B. (2007). Social network sites: definition, history, and scholarship. *Journal of Computer-Mediated Communication*, *13*(1), 210-230. doi:10.1111/j.1083-6101.2007.00393.x

Dadhich, P., Dutta, K. ve Govil, M. C. (2011). Trust enhanced authorization for distrubuted systems. *International Journal of Scientific & Engineering Research*, *2*(3), 1-7.

Dagon, D., Martin, T. ve Starner, T. (2004). Mobile phones as computing devices: The viruses are coming! *IEEE Pervasive Computing*, *3*(4), 11–15. doi:10.1109/MPRV.2004.21

eHealth, W. G. O. for. (2011). *mHealth: new horizons for health through mobile technologies: second global survey on eHealth*. Geneva : World Health Organization. https://apps.who.int/iris/handle/10665/44607 adresinden erişildi.

Enck, W., Gilbert, P., Chun, B.-G., Cox, L. P., Jung, J., McDaniel, P. ve Sheth, A. N. (2010). TaintDroid: An information-flow tracking system for realtime privacy monitoring on smartphones. *Proceedings of the 9th USENIX Conference on Operating Systems Design and Implementation* içinde (s. 393–407). Berkeley, CA, USA: USENIX Association. http://dl.acm.org/citation.cfm?id=1924943.1924971 adresinden erişildi.

Enck, W., Ongtang, M. ve McDaniel, P. (2009). On Lightweight mobile phone application certification. *Proceedings of the 16th ACM Conference on Computer and Communications Security* içinde(s. 235–245). New York, NY, USA: ACM. doi:10.1145/1653662.1653691

ENISA. (2017). *Privacy and data protection in mobile applications: a study on the app development ecosystem and the technical implementation of GDPR*. https://publications.europa.eu/en/publication-detail/-/publication/5d1a8d45-0af0-11e8-966a-01aa75ed71a1 adresinden erişildi.

FDA. (2015). *Mobile medical applications*. Rockville, MD: FDA. https://www.fda.gov/medicaldevices/digitalhealth/mobilemedicalapplications/default.htm adresinden erişildi.

Franco, M. ve Tursunbayeva, A. (2014). Mobile technology and public health organisational system. *Symphonya. Emerging Issues in Management*, 80-89. doi:10.4468/2014.1.06franco.tusrsunbayeva

Giannetsos, T., Dimitriou, T. ve Prasad, N. R. (2011). People-centric sensing in assistive healthcare: Privacy challenges and directions. *Security and Communication Networks*, *4*(11), 1295-1307. doi:10.1002/sec.313

Hasta Hakları Kılavuzu. (2013). *Hekimler ve Tabip Odası Yöneticileri için Mevzuat*. 6 Mayıs 2019 tarihinde http://www.ttb.org.tr/mevzuat/index.php?option=com_content&view=article&id=984:hasta&catid=26:etik&Itemid=65 adresinden erişildi.

Hasta Hakları Yönetmeliği (1998, 1 Ağustos). *Resmi Gazete* (Sayı: 23420) http://www.mevzuat.gov.tr/Metin.Aspx?MevzuatKod=7.5.4847&MevzuatIliski=0&sourceXmlSearch=hasta%20haklar%C4%B1 adresinden erişildi.

Helm, A. M. ve Georgatos, D. (2014). Privacy and MHealth: How mobile health apps fit into a privacy framework not limited to HIPAA. *Syracuse Law Review*, *64*, 131-170.

Hong, S., Liu, C., Cheng, B., Ren, B. ve Chen, J. (2017). MobiGemini: sensitive-based data and resource protection framework for mobile device. *China Communications*, *14*(7), 1-11. doi:10.1109/CC.2017.8010979

Introduction to the Personal Data Ecosystem (2019). http://pde.cc/introduction-to-the-personal-data-ecosystem/ adresinden erişildi.

Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelik (2016, 20 Ekim). *Resmi Gazete* (Sayı: 29863) http://www.resmigazete.gov.tr/eskiler/2016/10/20161020-1.htm adresinden erişildi.

Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelikte Değişiklik Yapılmasına İlişkin Yönetmelik (2017, 24 Kasım). *Resmi Gazete* (Sayı: 30250) http://www.resmigazete.gov.tr/eskiler/2017/11/20171124-1.htm adresinden erişildi.

Kişisel Verilerin Korunması Kanunu (2016, 7 Nisan). *Resmi Gazete* (Sayı: 29677) https://www.mevzuat.gov.tr/MevzuatMetin/1.5.6698.pdf adresinden erişildi.

Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi, 28 Ocak 1981, 108 Avrupa Konseyi Antlaşma Serileri 33. https://humanrightscenter.bilgi.edu.tr/media/uploads/2016/03/29/KisiselVerilerinOtomatikIslemeTabiTutulmasiKarsisindaBireylerinKorunmasiSozlesmesi.pdf adresinden erişildi.

Kotz, D., Gunter, C. A., Kumar, S. ve Weiner, J. P. (2016). Privacy and security in mobile health: A research agenda. *Computer*, *49*(6), 22-30. doi:10.1109/MC.2016.185

KVKK. (t.y.). *Özel nitelikli kişisel verilerin işlenme şartları.* https://www.kvkk.gov.tr/Icerik/5238/Ozel-Nitelikli-Kisisel Verilerin-Islenme-Sartlari adresinden erişildi

Kutlu, Ö., ve Kahraman, S. (2017). Türkiye'de kişisel verilerin korunması politikasının analizi. *Siyaset, Ekonomi ve Yönetim Araştırmaları Dergisi*, *5*(4), 45-62.

Lin, C. ve Varadharajan, V. (2010). MobileTrust: a trust enhanced security architecture for mobile agent systems. *International Journal of Information Security*, *9*(3), 153-178. doi:10.1007/s10207-009-0098-x

Luo, T., Hao, H., Du, W., Wang, Y. ve Yin, H. (2011). Attacks on WebView in the Android system. *Proceedings of the 27th Annual Computer Security Applications Conference* içinde (s. 343–352). New York, NY, USA: ACM. doi:10.1145/2076732.2076781

Lutz, C. ve Strathoff, P. (2014). *Privacy concerns and online behavior – not so paradoxical after all? viewing the privacy paradox through different theoretical lenses* (SSRN Scholarly Paper No: ID 2425132). Rochester, NY: Social Science Research Network. https://papers.ssrn.com/abstract=2425132 adresinden erişildi.

Olca, E. ve Can, Ö. (2014). Ulusal ve uluslararası yönetmeliklerde kişisel sağlık verisi mahremiyetinin korunması. https://www.researchgate.net/publication/328782662_Ulusal_ve_Uluslararasi_Yonetmeliklerde_Kisisel_Saglik_Verisi_Mahremiyetinin_Korunmasi adresinden erişildi.

Ozdalga, E., Ozdalga, A. ve Ahuja, N. (2012). The smartphone in medicine: a review of current and potential use among physicians and students. *Journal of Medical Internet Research, 14*(5), e128. doi:10.2196/jmir.1994

Parker, L., Karliychuk, T., Gillies, D., Mintzes, B., Raven, M. ve Grundy, Q. (2017). A health app developer's guide to law and policy: a multi-sector policy analysis. *BMC Medical Informatics and Decision Making, 17*. doi:10.1186/s12911-017-0535-0

Patrick, K., Griswold, W. G., Raab, F. ve Intille, S. S. (2008). Health and the mobile phone. *American journal of preventive medicine*, *35*(2), 177-181. doi:10.1016/j.amepre.2008.05.001

Privacy and Mobile Apps. (2019, 28 Mart).*Office of the Information Commissioner Queensland*. 28 Mart 2019 tarihinde https://www.oic.qld.gov.au/guidelines/for-government/guidelines-privacy-principles/applying-the-privacy-principles/privacy-and-mobile-apps adresinden erişildi.

Privacy Rights Clearinghouse. (2016). Mobile health and fitness apps: what are the privacy risks?, https://www.privacyrights.org/consumer-guides/mobile-health-and-fitness-apps-what-are-privacy-risks adresinden erişildi.

Rowan, M. ve Dehlinger, J. (2014). A privacy policy comparison of health and fitness related mobile applications. *Procedia Computer Science*, *37*, 348–355. doi:10.1016/j.procs.2014.08.051

Sağlık Alanında Bazı Düzenlemeler Hakkında Kanun Hükmünde Kararname (2011, 2 Kasım). *Resmi Gazete* (Sayı: 28103 Mükerrer) http://www.mevzuat.gov.tr/MevzuatMetin/4.5.663.pdf adresinden erişildi.

Sağlık Bilgi Sistemleri Uygulamaları Hakkında 2015/17 Sayılı Genelge (2015). *T.C. Sağlık Bakanlığı* https://www.saglik.gov.tr/TR,11183/saglik-bilgi-sistemleri-uygulamalari-hakkinda-201517-sayili-genelge.html adresinden erişildi.

Sağlık.Net Online ve e-Nabız Hakkında 2016/6 Sayılı Genelge (2016). *T.C. Sağlık Bakanlığı* https://dosyasb.saglik.gov.tr/Eklenti/820,genelge20166pdf.pdf?0 adresinden erişildi.

Su, W.C. (2014). A preliminary survey of knowledge discovery on smartphone applications (apps): Principles, techniques and research directions for e-health. *ICME International Conference on Complex Medical Engineering* içinde (s. 369-374). Taipei: IEEE.

Sunyaev, A., Dehling, T., Taylor, P. ve Mandl, K. (2014). Availability and quality of mobile health app privacy policies. *Journal of the American Medical Informatics Association*, 1–4. doi:10.1136/amiajnl-2013-002605

T.C. Anayasası. (1982). *T. C. Resmi Gazete, 17863 (Mükerrer)*, 9 Kasım 1982.

Türk Ceza Kanunu (2004, 12 Ekim). *Resmi Gazete* (Sayı: 25611) http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5237.pdf adresinden erişildi.

Türk Medeni Kanunu (2001, 8 Aralık). *Resmi Gazete* (Sayı: 24607) https://www.mevzuat.gov.tr/MevzuatMetin/1.5.4721.pdf adresinden erişildi.

Yataklı Tedavi Kurumları Tıbbî Kayıt ve Arşiv Hizmetleri Yönergesi (2001). *Hekimler ve Tabip Odası Yöneticileri için Mevzuat.* http://www.ttb.org.tr/mevzuat/index.php?option=com_content&view=article&id=228:yatakli-tedavkurumlari-tibbkayit-ve-arv-hmetleryerges&catid=8:ygeler&Itemid=34 adresinden erişildi.

Yataklı Tedavi Kurumları Tıbbi Kayıt ve Arşiv Hizmetleri Yönergesinde Değişiklik Yapılmasına Dair Yönerge (2016). *T.C. Sağlık Bakanlığı* https://www.saglik.gov.tr/TR,11242/yatakli-tedavi-kurumlari-tibbi-kayit-ve-arsiv-hizmetleri-yonergesinde-degisiklik-yapilmasina-dair-yonergesi.html adresinden erişildi.

Yan, Z., Chen, Y. ve Shen, Y. (2014). PerContRep: a practical reputation system for pervasive content services. *The Journal of Supercomputing*, *70*(3), 1051-1074. doi:10.1007/s11227-014-1116-y

Yılmaz, S. S. (2016). Tıp alanında kişisel verilerin açıklanması suçu. *Terazi Hukuk Dergisi*, *11*(119), 272-283.

Zhang, L. L., Liang, C. M., Li, Z. L., Liu, Y., Zhao, F. ve Chen, E. (2018). Characterizing privacy risks of mobile apps with sensitivity analysis. *IEEE Transactions on Mobile Computing*, *17*(2), 279–292. doi:10.1109/TMC.2017.2708716

Zhou, Y., Zhang, X., Jiang, X. ve Freeh, V. W. (2011). Taming ınformation-stealing smartphone applications (on Android). *Proceedings of the 4th International Conference on Trust and Trustworthy Computing* içinde (s. 93–107). Berlin, Heidelberg: Springer-Verlag. http://dl.acm.org/citation.cfm?id=2022245.2022255 adresinden erişildi.