SAĞLIK BİLİŞİM TEKNOLOJİLERİ VE YENİ HUKUKSAL SORU(N)LAR

EHEALTH AND NEW LEGAL PROBLEMS

DOI: 10.21492/inuhfd.410571

Elif KÜZECİ[*]

ÖZET

Elektronik Sağlık ya da kısaca e-Sağlık olarak da nitelenebilecek sağlık bilişim teknolojileri, yeni iletişim teknolojilerinin (Information Communication Technologies-ICTs) sağlık amacıyla kullanılmasını ifade eder. Sağlık bilişim teknolojilerindeki hızlı gelişim geleneksel sağlık hizmeti sunumunda ve hasta-hekim ilişkisinde dönüşüm yaratmaktadır. Bu gelişmenin daha uzun ve daha sağlıklı bir yaşam için pek çok olanak sunduğu açıktır. Ancak bazı yan etkileri olduğu da belirtilmelidir. Nitekim sağlık bilişim teknolojilerindeki hızlı gelişim kişisel verilerin işlenme süreçleri ile ilgili yeni sorular ve sorunlar gündeme getirmektedir. Bu soruların yetkin bir şekilde yanıtlanması, yürürlükteki hukuk kurallarını yorumlarken ve gelecekteki hukuk kurallarını tasarlarken teknolojinin kendine özgü yapısını dikkate almayı gerektirir. Bu çalışma kapsamında öncelikle e-sağlık uygulamalarının getirdiği yenilikler karşısında ortaya çıkan hukuksal sorular değerlendirilmiştir. Ardından ise bu sorunlara çözüm olacağı umulan bazı öneriler geliştirilmiştir. Kanımızca bu sorunların çözülebilmesi, veri öznesinin kendine ilişkin bilgiler üzerindeki denetimini güçlendiren, sürecin şeffaflığını destekleyen ve teknolojinin kendine özgü unsurlarını dikkate alan bir bakış açısı ile olanaklıdır. Bu bakış açısının mevcut hukuk kurallarının yorumuna ve yeni kuralların tasarımına yansıtılması, hak ve özgürlükler ile teknolojik gelişmeler arasında dengenin kurulması açısından yararlı sonuçlar verebilir. Ayrıca teknolojinin önüne bariyerler koymadan bireyin haklarını korumak için hukuk kurallarının yanında bu bakış açısını sistemleştiren etik kurallara da başvurulması daha sağlıklı bir gelecek kurmakta yardımcı olacaktır.

Anahtar Kelimeler: Sağlık hukuku, sağlık bilişim teknolojileri, e-Sağlık, enformasyon ve iletişim teknolojileri, kişisel sağlık verilerinin korunması.

ABSTRACT

Electronic health, shortly eHealth mainly refers to health informatics and means usage of Information Communication Technologies (ICTs) for health purposes. The rapid evolution of eHealth applications causes a transformation not only in healthcare, but also in the relationship between health professionals and patients. On the one hand, these developments can enable longer and healthier life for human beings. On the other hand, they present some side effects. Indeed, the rapid development of health informatics raises new problems related to personal data protection. To solve these problems, the role of the intrinsic structure of the technology should be recognised. From this point of view, this

[*] Dr. Öğretim Üyesi, Bahçeşehir Üniversitesi, Hukuk Fakültesi. (E-mail. elifkuzeci@gmail.com; elif.kuzeci@law.bau.edu.tr)

Makale Gönderilme Tarihi: 28.03.2018
Makale Kabul Tarihi: 27.06.2018

article begins with describing new developments related to eHealth. In the light of these instances, the study tries to evaluate the legal problems in the field and to propose some new solutions. In this sense, there needs to be a perspective which strengthens the control of data subject on her personal health related data, supports transparency of the process and takes into consideration different components of technology. Projecting this perspective to the interpretation of both the current regulations and the construction of new ones can be helpful to create a balance between fundamental rights and technological developments. To protect the rights of individuals without setting barriers to technology as well as applying ethical principles that systematise this perspective will foster a healthier future.

Keywords: Health law, health informatics technologies, eHealth, information-communication technologies (ICTs), health related data protection.

GİRİŞ

Kişisel sağlık verilerinin korunması gerekliliği, pek çok başka bilgi türüne kıyasla, oldukça eskiye dayanır. Bir ilke olarak hasta-hekim gizliliğini Antik Yunan'a, Hipokrat Yeminine kadar götürebilmek olanaklıdır. Günümüzde halen atıf yapılan, dünyanın pek çok yerinde tıp fakültesini bitiren hekimlerin mesleğe başlamadan önce okuyarak uyacaklarını beyan ettikleri bu metnin farklı uyarlamaları bulunur. Hekimin mesleği sırasında öğrendiği bilgileri gizli tutmasına yönelik bir ilke ise bütün örneklerde yer alır. Eski kaynaklarda ilkenin "duyduklarını ve gördüklerini" başkaları ile paylaşmama üzerine kurgulanması[1] şaşırtıcı değildir. Sıradan bir örnekte, hekim ev ziyaretinde bulunur, hastasını muayene eder, sağlığına ilişkin bilgiler edinir ve uygun bir tedavi önerir. Hastayı ve hasta yakınlarını dikkate almazsak, sağlık hizmeti sunulması boyutunda bilgilerin kayıtlı olduğu donanım hekimin kendisi, yazılım ise onun zihnidir. Hekimin meslek etiği kurallarına uyarak bu bilgileri başkaları ile paylaşmadığı durumda gizlilik sağlanmaktadır. Bilgilerin, günümüz bilişim teknolojilerinde olduğu gibi belirsiz bir geleceğe kadar saklanması söz konusu değildir. Her şeyden önce, eskilerin dediği gibi, *"hafiza-i beşer nisyan ile maluldür"*(insan hafızası unutma ile sakattır). Bir insan olan hekim de edindiği bilginin en azından bir kısmını unutacaktır. Burada sistem, veri tabanlarının tam aksi yönde işler: Bilişim sistemlerinde kayıtlı bilgi saklanır, silinmesi isteniyorsa bunun için aktif bir hareket yapılmalıdır. İnsan açısından ise esas olan unutmadır[2].

[1] Hippocrates, Loeb Classical Library, çev. W. H. S. Jones, Harvard University Press, ABD1923, s. 298-300.

[2] BURKELL, Jacquelyn Ann: "Remembering me: big data, individual identity, and the psychological necessity of forgetting", Ethics and Information Technology, 18(1), 2016, s. 17-23.

Modernleşme ile birlikte pek çok alanda olduğu gibi, sağlık hizmetleri açısından da gelişim ve hatta dönüşüm gözlenir. Hastanelerin kurumsallaşmasıyla birlikte hasta kayıtlarının ortaya çıkması gecikmemiştir[3]. Bu kapsamda hastaların sağlık bilgileri sistemli olarak sağlık kuruluşlarında dosyalanmaya başlar. Bu gelişim çizgisi içinde hasta bilgileri, hekimin zihninden ya da kişisel notlarından hastanenin tozlu arşiv raflarına taşınır. Bu noktada hasta bilgilerine erişim fiziksel olarak bu dosyalara erişim ile ilgilidir. Reçete gibi nispeten yeni ve farklı uygulamalarda ise hastanın alması gereken ilacı hekimi dışında belki de gören tek kişi eczacıdır[4]. Bazı örneklerde ise reçetenin, ya da hastanın sağlık durumuna ilişkin notların, hekimin el yazısı ile şifrelendiği bile söylenebilir[5]. Bu durum zamanla değişmiştir. 1960'larda bilgisayarın ortaya çıkması ile hasta bilgileri önce yavaş, daha sonra hızlanarak sayısallaştırılmış, 1990'larda İnternet'in sahnedeki yerini almasıyla farklı kaynaklardaki bilgiler ilişkilendirilebilir duruma gelmiştir[6]. Bu dönemde sağlık bilişim teknolojilerinin hızla geliştiği gözlemlenebilir. Bu alanı e-Sağlık uygulamaları olarak ifade etmek de olanaklıdır.

Yurttaşlara, hastalara, sağlık görevlilerine, sağlık kurumlarına ve kamu kurumlarına pek çok yarar sağlayacağı düşünülen[7] e-Sağlık, Alman Federal Sağlık Bakanlığı tarafından, modern enformasyon ve iletişim

[3] Hastanelerin erken dönem örnekleri oldukça eskiye götürülebilse de bugün bildiğimiz şekliyle bir kurum olarak hastanenin gelişimi oldukça yenidir. Tarihsel gelişime ilişkin ayrıntılı bilgi için bkz. RISSE, Guenter B.: Mending Bodies, Saving Souls, A History of Hospitals, Oxford University Press, Birleşik Krallık 1999. 20. Yüzyılın başında hasta bakımı evlerden, bu işe tahsis edilmiş bir yapı olan hastanelere taşınırken hastanelerde dikkate alınması gereken gereksinimlerden biri de gizlilik olmuştur. THOMPSON, John D./ GOLDIN, Grace: The hospital; a social and architectural history, Yale University Press, ABD 1975.

[4] Modern reçeteler hekim ile eczacının rollerinin ayrılmasından sonra gelişmiştir. Bkz. Making Medicines, A Brief History of Pharmacy and Pharmaceuticals, Anderson, Stuart (ed.), Pharmaceutical Press, Birleşik Krallık, 2005, s. 77 vd.

[5] Çeşitli çalışmalarda hekimin el yazısının okunmasındaki güçlük ile pek çok örnekte karşılaşıldığına ve bunun kimi zaman hasta açısından olumsuz sonuçlara neden olabildiğine işaret edilmektedir. SOKOL, Daniel K./ HETTIGE, Samantha: "Poor handwriting remains a significant problem in medicine", Journal of the Royal Society of Medicine, 12 (99), 2006, s. 645-646; CAPLAN, Jeremy: "Cause of death. Sloppy doctors", Time, 15 Ocak 2007.

[6] FOLLEN, Morris C.: Computer Medical Databases, The First Six Decades (1950-2010), Springer, Birleşik Krallık 2012, s. 33-55.

[7] European Commission: eHealth Action Plan 2012-2020 - Innovative healthcare for the 21st century, Communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee and The Committee of the Regions, , COM(2012) 736 final, Brüksel, 6 Aralık 2012, s. 4.

teknolojilerinin hasta bakımı ve tedavisi için sunduğu olanakları kullanan uygulamaları kapsayan bir kavram olarak tanımlanmıştır[8]. Dünya Sağlık Örgütü (World Health Organization-WHO)[9] ise e-Sağlık'ı daha kapsayıcı bir şekilde enformasyon ve iletişim teknolojilerinin sağlık amacıyla kullanılması olarak nitelemektedir[10]. Daha da geniş bir bakış açısı ile e-Sağlık'ın yalnızca teknik bir gelişme olmadığı; enformasyon ve iletişim teknolojileri kullanılarak ağ dünyasına bağlanmaya, sağlık hizmetlerini yerel, bölgesel ve küresel düzeyde geliştirmeye yönelik bir düşünce ve bakış açısı olarak da nitelenebilir[11]. E-Sağlık çerçevesinde oldukça gelişmiş uygulamalar bulunmaktadır[12]. Yakın zamana kadar bilimkurgu eserlerinde karşılaşılan pek çok sağlık uygulaması, bugün denenmiş ve kullanılmaya başlanmış yöntemlerdir. Bunlar, tanı, önleme ve tedavi kapasitesinin geliştirilmesi için önemli olanaklar sunmaktadır. Öte yandan bu uygulamalar bazı olumsuz sonuçlara da neden olur. Kişisel sağlık verilerinin daha önce görülmeyen oranda işlenmesi bu bağlamda değerlendirilebilir. Bu çalışma kapsamında e-Sağlık uygulamalarının getirdiği olumlu sonuçlardansa, bunların, başta kişisel sağlık verilerinin

[8] BAUER, Christoph: "Grundprinzipien des Datenschutzes bei E-Health", in Bauer,Christoph/ Eickmeier, Frank/ Eckard, Michael (ed.), E-Health, Datenschutz, Datensicherheit, Herausforderungen und Lösungen im IoT-Zeitalter,Springer, Almanya 2018, s. 33.

[9] Dünya Sağlık Örgütü Anayasası, 19 Haziran-22 Temmuz 1946 tarihleri arasında New York-ABD'de gerçekleştirilen Uluslararası Sağlık Konferansında kabul edilmiş, 22 Temmuz 1946'da 61 devlet temsilcisi tarafından imzalanmış ve 7 Nisan 1948'de yürürlüğe girmiştir. Bugün Dünya Sağlık Örgütü'nün, Türkiye de dâhil olmak üzere, 150 üyesi bulunmaktadır. Dünya Sağlık Örgütü bundan böyle, *WHO* olarak anılacaktır.

[10] World Health Organisation: "eHealth at WHO", http://www.who.int/ehealth/about/en (Erişim Tarihi: 19 Mart 2018). AB üyesi devletlerin hukuk sistemlerindeki e-Sağlık tanımlarına ilişkin karşılaştırmalı bir değerlendirme için bkz. Overview of the national laws on electronic health records in the EU Member States and their interaction with the provision of cross-border eHealth services, Final report and recommendations, Belçika 2014, s. 23 https://ec.europa.eu/health/sites/health/files/ehealth/docs/laws_report_recommendations_en.pdf (Erişim Tarihi: 20 Mart 2018).

[11] WANDHWA, Kush/ WRIGHT, David, "eHealth: Frameworks for Assesing Ethical Impacts", in George, Carlisle/ Whitehouse, Diane/ Duquenoy,,Penny (ed.), eHealth: Legal, Ethical and Governance Challenges, Springer, Almanya 2013, s. 184.

[12] Avrupa Komisyonu'na göre e-Sağlık pazarı birbiri ile ilişkili dört büyük kategori uygulama içermektedir. Bunlar; (i) klinik enformasyon sistemleri, (ii) Tele-sağlık ve ev bakımı, kişiselleştirilmiş sağlık hizmetleri, (iii) birleştirilmiş bölgesel ya da ulusal sağlık enformasyon ağları, dağıtık elektronik sağlık kayıtları ve e-reçete, e-sevk gibi ilişkilendirilmiş hizmetler; (iv) klinik dışı sistemlerin ikincil kullanımları. Bkz. European Commission:Accelerating the Development of the eHealth Market in Europe, eHealth Taskforce report 2007, Lüksemburg 2007, s. 10.

korunması olmak üzere, çeşitli alanlarda yarattığı sorunlara ve bu sorunları çözmeye yönelik önerilere odaklanılmıştır. Kanımızca ortaya çıkan yeni hukuksal sorunların saptanması ve öneri geliştirebilmesi için öncelikle yeni teknolojinin özellikleri anlaşılmalıdır. Bu doğrultuda çalışmamız içerisinde ilk olarak sağlık bilişim teknolojilerindeki gelişmeler, ortaya çıkan yeni sorunlar dikkate alınarak örneklendirilmiştir. Ardından yeni teknolojilerin ortaya çıkardığı yeni soru(n)lar hukuksal açıdan irdelenmeye çalışılmıştır. Burada amaçlanan kuramsal düzeyde bir tartışma ortaya koyabilmektedir. Ancak hâlihazırda yürürlükte olan bazı düzenlemelere de konunun anlaşılmasını kolaylaştırılacağı düşünülen yerlerde atıf yapılmıştır. Bu noktada 6698 sayılı Kişisel Verilerin Korunması Kanunu ile Avrupa Birliği'nde Mayıs 2018'de yürürlüğe girecek olan Genel Veri Koruma Tüzüğü, ilki Türkiye'de yürürlükte olan konuya ilişkin temel düzenleme olması, diğeri ise karşılaştırmalı hukuk açısından en gelişkin metin olarak görülmesi nedeniyle, örnek olarak seçilmiştir[13].

I. SAĞLIK BİLİŞİM TEKNOLOJİLERİ VE YENİ SORUNLAR

Sağlık teknolojilerindeki gelişmeler kanımızca bireyin kişisel verilerinin korunması alanını çeşitli açılardan etkilemektedir. Nitekim sağlık verilerinin kapsamı, değeri, edinildiği kaynaklar ve işlenme kapasitesi ile bu bilgiye erişebilen kişiler açısından önemli bir farklılaşma dikkat çekmektedir. Bu süreçler birbirinden kopuk değildir ve birbirini etkileyerek gelişmektedir. Bu değişimi biraz daha yakından incelemek hukuksal süreçlerin değerlendirilmesinde yardımcı olacaktır.

A. Kişisel sağlık verilerini işleme kapasitesindeki artış, kapsamındaki genişleme ve toplandığı kaynaklarda çeşitlenme

Çağımızda pek çok sektörün hızla sayısallaştığı görülmektedir. Tanınmış yatırımcı Marc Andreessen 2011 yılında bu durumu "yazılım dünyayı yiyor" ("Software is eating the World") sözüyle özetlemişti[14]. Sağlık teknolojilerindeki kapsam ve yaygınlaşma hızı düşünüldüğünde bu

[13] 6698 sayılı 24 Mart 2016 tarihli Kişisel Verilerin Korunması Kanunu (Bundan böyle *KVKK* olarak anılacaktır); Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Bundan böyle *AB Genel Veri Koruma Tüzüğü* ya da *GVKT* olarak anılacaktır).

[14] ANDREESSEN, Marc, "Why Software Is Eating the World?", The Wall Street Journal, 20 Ağustos 2011.

alanın da **sayısallaşma** eğiliminin dışında kalmadığı, kişisel sağlık verilerinin artan oranda bilgisayarlarda ve veri tabanlarında tutulduğu, görülebilir. Bu gelişimin ilk aşamada hasta dosyalarının sayısal ortama taşınması ile başladığı söylenebilir[15]. Sayısallaşma, bilgilerin daha kolay ilişkilendirilmesini ve aktarılmasını olanaklı kılar. Örneğin elektronik sağlık kayıtları (electronic health records-EHR) ile bireyin sağlık durumuna ilişkin olarak geçmişi ve bugünü içeren kapsamlı bilgilerin sunulması hedeflenmektedir[16].

İşleme, hukuksal anlamda, bilgi üzerinde gerçekleştirilen her türlü eylemi ifade eder. Kaydetme, kullanma, aktarma, muhafaza etme, silme ve yok etme gibi birbirinden farklı pek çok hareket bu kapsamdadır[17]. Günümüzde sağlık verilerinin işlenme kapasitesi, geçmiş dönemlere kıyasla, çok daha geniş çaplıdır. Sağlık bilgilerini sayısal ortamda tutan yalnızca hekimler ya da sağlık çalışanları değildir. Bireyin, kendisine ilişkin sağlık bilgilerini kayıt ve takip edebileceği araçlar da gittikçe artmaktadır. Örneğin kişinin kullandığı ilaçları, gebelik durumunu, alerjilerini kaydettiği cep telefonu uygulamaları artmaktadır.

İnternet'in yaygınlaşması ise sağlık verilerine **uzaktan erişim**i olanaklı kılmıştır. Hekimlerin hasta dosyalarına evlerinden ulaşmaları yanında, hastalar da örneğin test sonuçlarını ilgili sağlık kuruluşunun İnternet sayfasından öğrenebilmekte, hekim ile e-posta üzerinden haberleşebilmektedir. Bu şekilde teknolojideki gelişim, hasta-hekim ilişkisindeki değişimi de beraberinde getirmektedir[18]. Uzaktan danışma, tanı ve hatta kimi zaman tedavi alımında e-hekim gibi uygulamalara daha sık başvurulmaktadır. Cep telefonları ve başka bazı cihazlar aracılığıyla hasta sağlık verileri düzenli olarak hekime iletilebilmektedir. Bu ise, hastanın sağlık kurumunda fiziksel olarak bulunmadan hekimine

[15] Hasta dosyalarının kâğıt ortamında tutulması ile sayısal ortama aktarılmasına ilişkin bazı değerlendirmeler için bkz. DICK, Richard S./STEEN, Elaine B./ DETMER, Don E.: The Computer Based Patient Report, National Academy Press, ABD 1997, s.56 vd.

[16] Article 29 Data Protection Working Party: Working Document on the processing of personal data relating to health in electronic health records (EHR), WP 131, 15 Şubat 2007.

[17] Aralarında bazı ufak farklılıklar olmakla birlikte pek çok hukuksal düzenlemede veri işlemenin bu temelde tanımlandığı görülmektedir. Örneğin bkz. KVKK, m. 3/1, e; GVKT, m. 4/2.

[18] Bu konuda kapsamlı bir inceleme için bkz. WACHTER, Robert: The Digital Doctor: Hope, Hype, and Harm at the Dawn of Medicine's Computer Age, Mc Graw-Hill, ABD 2017.

danışmasını olanaklı kılar[19]. Bu noktada önemli bir gelişme de "mobil sağlık"tır. Klinik uygulamaları ve kamu sağlığını desteklemek için kablosuz cihazların kullanımı olarak tanımlanan mobil sağlık (m-Sağlık), e-Sağlığın önemli bir bileşeni olarak değerlendirilmektedir[20]. M-Sağlık'ın önleyici tedavi, sağlık hizmetlerinin daha etkin ve sürdürebilir kılınması, nitelikli sağlık hizmetine erişim, hastaların tedavi sürecinde daha katılımcı olması gibi konularda büyük bir potansiyel taşıdığı ifade edilmektedir[21].

Sağlık bilgilerinin hızla sayısallaşması ve bağlanabilir kılınması, toplandığı **kaynakları**n çeşitlenmesini de sağlamaktadır. Bu husus, birkaç başlık altında değerlendirilebilir. İlk olarak ilgili **kişinin kendisi**nin sağlık verisi edindiği kaynaklarda artış gözlenmektedir. Pek çok kişi, günlük yaşamında kullandığı bazı basit cihazlar ile sağlık verilerini kaydetmekte ve incelemektedir. Kullanımı yaygınlaşan giyilebilir teknolojiler, uyku düzeninden, adım sayısına, pek çok konuda bilgi sunar. Giyilebilir teknolojinin sağlık durumunun izlenmesinde, sağlık verilerine erişimde ve tıp eğitiminde önemli bir yarar sağlayacağı düşünülmektedir[22]. İkinci olarak, günümüzde daha önceden bilinmeyen **yeni kaynaklar**a erişilebilmektedir. Genetik testlerin kapsamındaki genişleme ve bu testlere erişim kolaylığı bu açıdan değerlendirilebilir. Tükürük gibi kolay elde edilebilir bir vücut sıvısından kapsamlı ve hassas verilerin edinilmesi 20. Yüzyılda karşılaştığımız heyecan verici buluşlardan biridir. Bazı ülkelerde-*23andMe* gibi bilinen ve popüler bir örnekte olduğu gibi-birey, soy bağına ve sağlık durumuna ilişkin genetik bilgilere doğrudan

[19] Bu noktadaki uygulamaların on seneyi aşkın bir geçmişi bulunmaktadır. Örnek olarak The New York Times'da 2006 yılında yayınlanan şu araştırma haberi değerlendirilebilir: FEDER, Barnaby J.:"Remote Control for Health Care", The New York Times, 9 Eylül 2006, http://www.nytimes.com/2006/09/09/business/09node.html (Erişim Tarihi: 19 Mart 2018).

[20] EXTER,André den: "eHealth Law: The Final Frontier", in Hervey Tamara K./ Young, Calum Alasdair/ Bishop, Louise E., Research Handbook on Health Law and Policy, Edward Elgar Publishing, Birleşik Krallık 2017, s. 254; World Health Organisation: mHealth, New horizons for health through mobile technologies, Global Observatory for eHealth series-Volume 3, İsviçre 2011, s. 5 http://www.who.int/goe/publications/goe_mhealth_web.pdf, (Erişim Tarihi: 19 Mart 2018).

[21] European Commission: Green Paper on mobile health ("mHealth"), COM(2014) 219 final, 10 Nisan 2014, Belçika, s. 4 vd; World Health Organization, Executive Board: mHealth: use of mobile wireless technologies for public health (Report by the Secretariat), 139th session, Provisional agenda item 6.6, EB 139/8, 27 Mayıs 2016.

[22] SULTAN, Nabil "Reflective thoughts on the potential and challenges of wearable technology for healthcare provision and medical education", International Journal of Information Management, 35, 2015, s. 523-525.

tüketiciye sunulan ürünler aracılığıyla ulaşılabilmektedir. Bunun yanında insan bedeninden sürekli veri aktaran yeni teknoloji ürünlerinin geliştiği de görülmektedir. Amerika Birleşik Devletleri Yiyecek ve İlaç İdaresi'nin (FDA) ilk elektronik hapı onayladığı 2012 yılından[23] bu yana bu alanda ciddi bir gelişme gözlenmektedir. Nitekim aynı kurum Kasım 2017'de yutulmasının ardından sayısal takip sağlayan bir hapın bazı ruhsal rahatsızlıkların tedavisinde kullanılmasını onaylamıştır[24]. Soğuk algınlığını henüz başlangıç aşamasında saptayan burun implantlarından, kişinin düşmesi durumunda cep telefonuna gönderdiği sinyal ile vakit kaybetmeden acil servisi aramayı sağlayan kalça protezlerine kadar pek çok **Nesnelerin İnterneti** (Internet of Things-IoT) uygulaması geliştirilmektedir[25]. Nesneler her geçen gün birbirlerine daha bağlı hale gelmekte, bu ise sürekli bilgi akışını olanaklı kılmaktadır.

Büyük Veri (Big Data) ile ilişkili olarak da çeşitli örneklerle karşılaşılmaktadır. Büyük Veri'nin çok farklı tanımları bulunmaktadır ve bunların birçoğu büyük miktardaki çok çeşitli verinin son derece hızlı bir şekilde işlenerek yeni ve öngörü içeren bilgiye ulaşma olanağı sunan yeni bir teknolojiye vurgu yapmaktadır[26]. Julia Cohen Büyük Veri'yi teknoloji ve süreç (process) kesişiminin kısaltması olarak nitelemektedir. Bu kapsamda teknoloji, büyük miktardaki verinin çok kısa sürede incelenmesi, sıralanması ve sorgulanmasını olanaklı kılan enformasyon işleme yapısı iken; süreç, verinin örüntü için araştırılması, örüntünün öngörü analitiği için ayrıştırılması ve analizlerin yeni verilere uygulanmasını kapsar. Her ikisi birlikte, veri akışının belirli ve veri merkezli bir bilgiye dönüştürülmesini sağlayan bir teknik sunar[27]. Büyük

[23] SCHMIDT, Eric/ COHEN, Jared: The New Digital Age, Transforming Nations, Businesses, and Our Lives, Vintage, ABD 2014, s. 26.

[24] US Food and Drug Administration: "FDA approves pill with sensor that digitally tracks if patients have ingested their medication", 13 Kasım 2017, https://fda.gov/NewsEvents/Newsroom/PressAnnouncement/ucm584933.htm (Erişim Tarihi: 20 Mart 2018).

[25] Sağlık alanında *Nesnelerin İnterneti* kullanımına ilişkin olarak bkz. MAKSIMOVIĆ, Mirjana/ VUJOVIĆ, Vladimir: "Internet of Things Based E-health Systems: Ideas, Expectations and Concerns", in Khan, Samee U./Zomaya, Albert Y./ Abbas, Assad (ed.), Handbook of Large-Scale Distributed Computing in Smart Healthcare, Springer, Almanya 2017.

[26] Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (T-PD): Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data, T-PD (2017)01, 23 Ocak 2017, s. 2.

[27] COHEN,Julie E.: "What Privacy Is For", Harvard Law Review, 126, 2013, s. 1920.

Veri analizleri ile "küçük" ve dağınık verilerden sağlık bilgileri ortaya çıkarılabilmektedir. Bu yöntem ile sağlık alanında ulaşılabilecek olumlu sonuçlar çeşitli çalışmalarda ileri sürülmektedir[28]. Ancak Büyük Veri analizlerinin yalnızca sağlık hizmeti sunmak amacıyla kullanılmadığı da bir gerçektir. ABD'de büyük bir perakendeci firma olan Target'ın hangi müşterilerinin hamile olduğunu, henüz onlar aileleri ve arkadaşları ile paylaşmadan öğrenmesi ve buna yönelik reklamlar paylaşması bu kapsamda dikkat çekici bir örnektir[29].

B. Sağlık bilgilerine erişebilen kişilerde artış

Sağlık hizmeti hasta, hekim ve sağlık çalışanları çemberinden çıkarak artan oranda başka aktörlerin de yer aldığı bir alana dönüşmektedir. Sağlık bilişim teknolojilerindeki gelişmeler ise sağlık bilgilerine eriş(ebil)en kişilerin artmasına neden olmaktadır. Bu kapsamda yetkili kişilerin, yetkisiz kişilerin ve bir de belki yeni kişilerin sağlık verilerine erişimi değerlendirilebilir.

İlk olarak, sağlık bilişim teknolojilerindeki gelişmeler sonucunda kişisel sağlık verilerine erişebilecek **yetkili kişi** kümesi genişlemektedir. Doğru tanı ve tedavi amacıyla tek bir vakıada çok daha fazla sayıda kişi hasta bilgilerine erişmektedir. Ayrıca sağlık bilişim teknolojilerindeki gelişme ile bilgi işlem uzmanları, biyomedikal mühendisleri, teknisyenler gibi kişilerin de sürece dâhil olması söz konusu olabilmektedir. Bir başka anlatımla, geleneksel olarak sağlık hizmeti alımında yer almayan kişilerin kişisel sağlık verilerine erişimi bazı durumlarda olanaklı ve hatta gerekli olabilmektedir. Öte yandan özellikle tıbbi araştırmalar kapsamında açık kaynak politikaları gibi nedenlerle büyük çaplı veri paylaşımının arttığı görülmektedir[30]. Avrupa'daki pek çok uygulama, tıbbi araştırmalarda veri yoğunlaşmış etkinliklerin arttığını göstermektedir. Bu kapsamda sağlıkla ilgili, genomik ya da başka türdeki veriler geniş kapsamlı olarak toplanmakta, tekrar kullanılmakta ve aralarında bağlantı kurulmaktadır[31].

---

[28] Örneğin bkz. CHAWLA, Nitesh/ DAVIS, V. Darcy A.: "Bringin Big Data to Personalized Healthcare: A Paient-Centered Framework", Journal of General Internal Medicine, 28, 2013, s. 660-665; RAGHUPATHI, Wullianallur/ RAGHUPATHI, Viju "Big data analytics in healthcare: promise and potential", Health Information Science and Systems, 2(3), 2014, s. 1-10.

[29] DUHIGG, Charles: "How companies learn your secrets", The New York Times, 16 Şubat 2012.

[30] PEREIRA,Stacey/ GIBBS, Richarda/ McGUIRE, A. Amy L.: "Open Access Data Sharing in Genomic Research", Genes, 5(3), 2014, s. 739-747.

[31] MOSTERT, Menno/ BREDENOORD,Annelien L./ CIH BIESAART, Monique/ DELDEN, Johannes JM van: "Big Data in Medical Research and EU Data Protection

Kişisel sağlık verilerine erişebilen **yetkisiz kişiler** açısından da artış gözlemlenebilir. Yukarıda işaret edildiği üzere modern sağlık hizmetleri öncesinde, hekim-hasta ilişkilerinin geleneksel biçimde kurulduğu dönemde, sağlık bilgilerine yetkisiz kişilerin erişimi, hekimin böyle bir paylaşımda bulunup bulunmamasına bağlıydı. Sağlık hizmetinin kurumsallaşarak hasta dosyalarının oluşturulmasından sonra ise yetkisiz erişim fiziksel olarak bu dosyalara ulaşabilmeyi gerektiriyordu. Oysa bilgilerin veri tabanlarına aktarılması ve artan oranda sayısallaşması ile uzaktan erişim olanakları gelişti. Bu ise bir anda oldukça kapsamlı bilginin mekânsal olarak uzakta bulunan kişilerce de elde edilmesini olanaklı kıldı. Ayrıca veri depolama araçlarının hızla ucuzlaması, küçülmesi ve hızlanması kurum içinden yetkisiz erişimlerde de eskiye oranla çok daha kapsamlı bilginin kısa süreden aktarılmasına neden olabilmektedir. Veri güvenliğinin öneminin pek çok alanda artan oranda hissedilmesi de bu gibi tehlikelerden kaynaklanmaktadır. Bu noktada sağlık bilişim teknolojilerinin sunduğu önemli olanak, gereken önlemler alınmadığında, onun aşil topuğu da olabilmektedir. Sağlık alanında artan veri sızıntıları bunun bir örneği olarak değerlendirilebilir[32]. Günümüzde adeta bir sağlık verileri piyasası oluşmuştur[33]. Çalışmalar, sağlık bilgilerinin kredi kartı bilgisinden on kat daha değerli olduğunu ortaya koymaktadır[34]. Nitekim kredi kartının aksine, sağlık bilgileri değiştirilemez niteliktedir.

Son olarak, bilişim teknolojilerindeki hızlı gelişim dikkate alındığında yakın zamanda yeni bir "kişilik" kategorisinin de değerlendirme kapsamına alınabileceği düşünülebilir. Nitekim sağlık alanında yapay zekâ kullanımına yönelik uygulamalar ve çalışmalar dikkat çekicidir[35]. Yapay zekânın özellikle sağlık durumu izleme, sağlık hizmetini geliştirme, siber saldırılarının saptanması, müşteri hizmetlerinin

Law: Challenges of the Consent or Anonymise Approach", European Journal of Human Genetics, 24, 2016, s. 957.

[32] Yakın tarihli birkaç örnek için bkz. "Largest Healthcare Data Breaches of 2017", HIPAA Journal, 4 Ocak 2018, https://www.hipaajournal.com/largest-healthcare-data-breaches-2017/ (Erişim Tarihi: 5 Mart 2018).

[33] Bu konuda kapsamlı bir çalışma için bkz. TANNER, Adam: Our Bodies, Our Data, How Companies Make Millions Selling Our Medical Records, Beacon Press, ABD 2017.

[34] HUMER, Caroline/ FINKLE, Jim: "Your medical record is worth more to hackers than your credit card", Reuters, 4 Eylül 2014, https://www.reuters.com/article/us-cybersecurity-hospitals/your-medical-record-is-worth-more-to-hackers-than-your-credit-card-idUSKCN0HJ21I20140924 (Erişim Tarihi: 4 Mart 2018).

[35] HAMET, Pavel/ TREMBLAY, Johanne: "Artificial Intelligence in Medicine", Metabolism Clinical and Experimental, 9, 2017, s. 536-540.

iyileştirilmesi, hastane yönetiminde verimliliğinin arttırılması gibi alanlarda kullanılması düşünülmektedir[36]. Bu durum gelecekte yeni bir kişilik türü olarak tanınma olasılığı bulunan yapay zekânın[37] sağlık verileri işlemesine ilişkin özel bir değerlendirmeyi gerekli kılabilir[38].

II. HUKUKSAL DEĞERLENDİRME

Sağlık bilişim teknolojileri sağlık hizmetinin geliştirilmesi ile daha uzun ve sağlıklı bir yaşam idealine yaklaşılması yönünde çeşitli olanaklar sunmaktadır. Ancak bu sistemler, yukarıda işaret edildiği üzere, kişisel sağlık verilerinin önceki döneme kıyasla daha kapsamlı işlenmesi sonucunu da beraberinde getirmektedir. Bu durum, kişisel sağlık verilerinin korunmasını, yeni teknolojileri dikkate alarak yeniden düşünmeyi zorunlu kılar. Nitekim sağlık alanında yaşasan dönüşüm karşısında, veri öznesinin haklarını yeni bir bakış açısı ile değerlendirmek gerekecektir. Kanımızca bu değerlendirmenin doğru bir şekilde yapılabilmesi için öncelikle sağlık verilerinin korunması gereksiniminin üzerinde durulmalıdır. Nitekim kişisel sağlık verilerinin korunmasının hukuksal kaynağı da burada yatar. Kanımızca bu hak alanının dayandığı temel değeri doğru değerlendirmemiz uygulamayı ve düzenlemeleri yeni gelişmeler ile uyumlu kılabilmemiz açısından son derece önemlidir. Etkin korumanın geliştirilmesine yönelik öneriler de ancak bu temelin üzerine inşa edilebilir.

I. Sağlık bilişim teknolojileri ve kişisel sağlık verilerinin korunması

Sağlık verilerinin korunması gereksiniminin biyolojik, psikolojik, sosyal ve siyasal nedenlerden kaynaklandığı söylenebilir. Öncelikle insan, paylaşımını kimlerle, ne oranda yapacağına kendisinin karar verdiği bir özel alana gereksinim duyar. Biyologlar bunun doğal bir gereksinim olduğuna, hatta yalnızca insanlarda değil, başka memelilerde de görüldüğüne işaret etmektedir[39]. Psikoloji alanındaki araştırmalar, insanın farklı ilişki grupları içerisinde değişen kimliklerle bulunduğunu belirtmektedir[40]. Bu psikolojik bir soruna işaret etmediği gibi, duygu

[36] "Data doctors: How AI is changing healthcare", The Guardian (International Edition), 26 Ocak 2018.
[37] Erken dönem bir tartışma için bkz. SOLUM, Lawrence B.: "Legal Personhood for Artificial Intelligences", North Carolina Law Review, 7(4) 1992, s. 1231-1287.
[38] CHUNG, Jason: "What Should We Do About Artificial Intelligence in Health Care?", NYSBA Health Law Journal, 22(3), 2017, s. 37-40.
[39] SCHENEIER, Bruce: Data and Goliath, W.W.Norton & Company, ABD 2015, s. 126.
[40] *Ibid.*

durumu açısından sağlıklı da görülmektedir[41]. Bu gereksinimin karşılanmadığı kişilerde ise fiziksel ve ruhsal sıkıntılar görülmektedir[42]. Bu açıdan insanın kendine ilişkin bilgiler üzerindeki denetimini kaybettiği bir ortamda özel alanına bir müdahale oluştuğunu hissetmesi beklenir. Bu durum, bireyin kendi alanını belirleme gücünü ve ilişkilerindeki seçim hakkını kaybettiği düşüncesi ile baskı ve kaygı hissetmesine neden olabilir.

WHO'nun tanımı uyarınca sağlık "fiziksel, zihinsel ve sosyal olarak tam bir refah halidir ve salt hastalık ve güçsüzlüğün bulunmaması" değildir[43]. Bu tanım dikkate alınarak bireylerin sağlıklı olabilmeleri için belirli oranda özel yaşam alanına gereksinim duydukları belirtilebilir. Bireysel sağlığı etkileyebilecek bu durumun yanında kişisel sağlık verilerinin korunmaması, genel sağlığı da olumsuz yönde etkileyebilir. Nitekim Avrupa İnsan Hakları Mahkemesi (AİHM) bir kararında sağlık verilerinin korunmamasının hastaların tanı ve tedaviden kaçınmasına neden olabileceğine işaret etmiştir. Bu ise özellikle bulaşıcı hastalıklarla mücadeleyi olumsuz yönde etkileyecektir[44]. WHO da bu türdeki hastalıklara ilişkin olarak, kamu otoritelerinin gizliliğin sağlanmasını açıkça güvencelemediği durumlarda hastaların çoğunlukla tedavi arayışında isteksiz olduğuna dikkat çekmektedir[45]. Bu durum, sosyal damgalanmaya neden olabilen hastalıklar açısından daha da büyük bir tehlike oluşturur. Ayrıca yeterli korumanın olmadığı bir durumda, izlenenlerin izleyenlerin beklentilerine göre davranacağı düşüncesinden hareketle kurulan *panoptik* yapıların[46] toplumsal farklılıkları törpüleyerek, demokratik süreçlere zarar verebileceği unutulmamalıdır. Böyle bir ortamda kişiler maddi ve manevi zararlar ile karşılaşabilir. Ancak bu zararların ötesinde kişinin sağlık bilgilerinin korunmasının bir insan hakkı olduğu ve herhangi bir zarar oluşmadığı durumda da korunması gerektiği belirtilmelidir.

---

[41] JOURARD, Sidney M.: "Some Psychological Aspects of Privacy", Law and Contemporary Problems, 2(31), 1966, s. 307-318.

[42] SCHENEIER, s. 126.

[43] WHO Anayasası, Başlangıç. Anayasa, yukarıda da belirtildiği üzere, 1946 yılında kabul edilmiştir ve bu tarihten günümüze sağlık kavramının tanımı hiç değiştirilmemiştir.

[44] AİHM, Z, Finlandiya kararı, 22009/93, 25 Şubat 1997.

[45] World Health Organisation: Global diffusion of eHealth: Making universal health coverage, Report of the third global survey on eHealth, Global Observatory for eHealth, İsviçre 2016, s. 109.

[46] FOUCAULT, Michael Hapishanenin Doğuşu, çev. Mehmet Ali Kılıçbay, 3. Baskı, İmge, Ankara 2006, s. 289 vd.

Kanımızca, bu gereklilikleri karşılayan etkin bir sistem için konuya ilişkin hukuk kurallarını, yukarıda örneklendirilen yeni sağlık teknolojilerini dikkate alarak değerlendirmek ve yeni kurallar üzerinde düşünmek gerekir. Bu kapsamda karşılaşılabilecek soru(n)lardan biri, hangi verilerin kişisel sağlık verisi olduğunu saptamaya ilişkindir. Gerçekten sağlık teknolojilerindeki gelişmeler sağlığa ilişkin bilgilerin farklı yöntemlerle ve çeşitli araçlarla toplanmasını sağlamaktadır. Bu ise bazı durumlarda bir bilginin kişisel sağlık verisi olup olmadığını saptamayı güçleştirir.

Kişisel veri ulusal ve uluslararası hukuksal metinlerde tanımlanmıştır. Konuya ilişkin yargısal içtihatlar ve öğretinin yorumları da oldukça gelişkindir. Belirtmek gerekir ki dünyada yüzün üzerinde devlette kişisel verilerin korunmasına ilişkin hukuksal düzenlemeler kabul edilmiş[47], pek çok uluslararası kuruluş ve ulusüstü bir yapı olan AB bu alanı koruyan düzenlemeler benimsemiştir[48]. Bu nedenle kavramsal tartışmalarda yararlanılabilecek kaynaklar, ulusal sınırların ötesindedir. Hukuksal düzenleme örneklerinin büyük bir kısmında sağlık bilgilerinin özel nitelikli kişisel veriler kapsamında yer aldığı görülür. Pek çok yerde hassas kişisel veriler olarak da adlandırılan bu kategoride yer alan bilgiler, daha güçlü bir koruma sistemine tabi tutulmaktadır[49].

Kişisel veriler genel olarak "belirli ya da belirlenebilir bir gerçek kişiye ilişkin her türlü bilgi"yi niteler[50]. Karşılaştırmalı hukuk açısından değerlendirildiğinde tanımlamalarda bazı farklılıklar görülse de temel olarak benzer bir yapının kabul edildiği söylenebilir[51]. Kişisel veri niteliğinde olmayan bilgiler açısından kişisel verilerin korunmasına yönelik düzenlemelerin uygulanmayacağı açıktır. Bu durumda hangi verilerin bu kapsama girdiği saptanmalıdır. Öte yandan bu verinin kişisel sağlık verisi niteliğinde olup olmadığı da belirlenmelidir. Nitekim bu durumda özel kategorideki verilerin işlenmesine yönelik ilkeler uygulanacaktır[52].

---

[47] GREENLEAF,Graham: "Sheherezade and the 101 Data Privacy Laws: Origins, Significance and Global Trajectories", Journal of Law, Information and Science, 1(23), 2014, s.4-49.

[48] Örneğin bkz. OECD Guidelines on the Protecion of Privacy and Transborder Flows of Personal Data, 23 Eylül 1980; United Nations guidelines concerning computerized personal data files, 14 Aralık 1990; APEC Privacy Framework, 29 Ekim 2004; AB Veri Koruma Yönergesi; GVKT.

[49] Örneğin bkz. KVKK, m. 6; GVKT, m. 9.

[50] KVKK'da bu tanım benimsenmiştir. KVKK m. 3/1,d.

[51] Örneğin bkz. AB Veri Koruma Yönergesi, m. 2/a; GVKT, m. 4/1.

[52] KVKK, m. 6; GVKT, m. 9.

Yukarıda verilen örneklerde de görüleceği üzere, farklı kaynaklardan toplanan bilgilerin ilişkilendirilmesi sonucunda kişisel sağlık verisine ulaşılabilmektedir. İnternet üzerinden alışveriş yapılan bir sitedeki hareketlerden bir kişinin hamile olduğu bilgisinin çıkarılması, ya da klavye tuşlama ritmindeki değişiklikten sağlık durumuna işaret eden bilgilere ulaşılması[53] bu kapsamda sayılabilir. Kısacası sağlık bilişim teknolojilerindeki gelişmeler, kişisel sağlık verilerine ilişkin yeni bir değerlendirmeyi gerektirir.

AB Genel Veri Koruma Tüzüğünde (GVKT) sağlıkla ilgili veriler "bir gerçek kişinin, sağlık durumuna ilişkin bilgileri açığa çıkaran sağlık hizmetlerinin sağlanması da dâhil olmak üzere, fiziksel ve zihinsel sağlığıyla ilgili veriler" olarak tanımlanmıştır[54]. Kişinin önceki, şimdiki ve sonraki sağlık durumuna ilişkin bilgiler bu kapsamdadır. Bilginin edinildiği kaynağın ise önemi yoktur. Hekim, sağlık çalışanı, tıbbi cihaz ya da teşhis için kullanılan laboratuvar kaynak olabilir[55]. AB Veri Koruma Yönergesinin 29. Maddesi uyarınca kurulan ve bağımsız bir kuruluş olan 29. Madde Veri Koruma Grubu sağlık bilgilerinin yalnızca tıbbi kaynaklardan edinilen bilgileri kapsamadığına işaret etmiştir. Kişisel sağlık verileri arasında veri öznesinin fiziksel ve ruhsal sağlık durumuna ilişkin ve tıbbi kaynaklardan edinilen bilgiler-bir başka ifade ile açıkça sağlık verisi olanlar-yer aldığı gibi, kendi başına ya da başka bilgilerle birleştirilerek bir kişinin gerçek sağlık durumuna ya da sağlık riskine ilişkin sonuç çıkarılabilen veriler de bulunur. Ayrıca bu verilerin ortaya çıkardığı sonuçların doğru, meşru ya da yeterli olup olmadığına bakılmaksızın, kişinin sağlık durumuna ya da riskine ilişkin sonuçlara ulaşıldığında sağlık bilgisi olarak kabul edileceği söylenebilir[56].

Mason Marks ise, ilk aşamada sağlıkla ilgili görünmeyen ancak sonradan bu bağlantının kurulduğu bilgileri "Müstakbel Sağlık Verisi" (Emergent Medical Data-EMD) olarak adlandırmaktadır. Sosyal medya üzerindeki beğenilerden, ziyaret edilen İnternet sitelerinden, elektronik

[53] "How your electronic DNA could be the secure login of the future", The Guardian, 18 Temmuz 2014, http://www.theguardian.com/technology/2014/jul/18/how-your-electronic-dna-could-be-the-secure-login-of-the-future (Erişim Tarihi: 5 Mart 2018).

[54] GVKT, m. 4/15. KVKK'da ise sağlık verileri tanımlanmamıştır.

[55] GVKT, Başlangıç par. 35.

[56] Article 29 Working Party: "Health Data in Apps and Devices" (Annex), Avrupa Komisyonu'nun m-Sağlık uygulamalarının ne zaman kişisel veri düzenlemelerinin kapsamına gireceğine ilişkin 29. Madde Veri Koruma Grubuna ilettiği mektuba cevaben, ekli belge, 5 Şubat 2015, s. 5 (https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/20150205_letter_art29wp_ec_health_data_after_plenary_annex_en.pdf) (Erişim Tarihi: 20 Mart 2018).

ortamda yapılan alışverişlerden derlenen bilgiler bir yapbozun parçaları gibi birleştirilerek sağlık verisine ulaşılabilmektedir[57]. Bu türdeki veriler, adım ölçer olarak da çalışan kalça protezinden ya da bir hastanın çevrimiçi bir forumda benzer sağlık sorunlarından dertli kişilerle karşılıklı bilgi alışverişinde bulunmasından farklıdır. Nitekim bu örneklerde kişi, sağlık bilgisini gönüllü olarak paylaşır. Eğer bu kaynaklardan hareketle başka sağlık bilgilerine de ulaşılıyorsa bu durumda dolaylı bir bağlantıdan söz edilebilir. Örneğin akıllı telefon ya da saat ile izlenen uyku durumundaki değişiklik bir sağlık sorununa işaret edebilir. Bu noktada tutulan bilgi geleneksel sağlık bilgisinden farklı olsa da sağlıkla bir bağlantı taşımaktadır. Müstakbel Sağlık Verileri ise sağlıkla ilgisi bulunmayan ya da ilişkisini öngörmenin oldukça zor olduğu durumlar için geçerlidir. Bağlantının çoğu zaman karmaşık veri analizleri ile kurulduğu görülmektedir[58].

Verinin hangi noktada sağlık bilgisi olarak kabul edileceğinin saptanması önemlidir. Nitekim bu an, konuya ilişkin hukuksal düzenlemelerin de uygulanmaya başlayacağı zamandır. Ancak Müstakbel Sağlık Verileri ya da sağlık durumuna ilişkin sonuç çıkarılabilen verilerin bu hassas kategoride olduğunu ilk aşamada saptayabilmek kolay değildir. Bu noktada dar yorum korumanın zayıflamasına ve hatta bazı durumlarda ortadan kalkmasına neden olabilir. Genişletici yorum ise, özellikle Büyük Veri'deki gelişmeler düşünüldüğünde, hemen hemen her tür bilgiyi bu kapsamda sayma gibi bir sonuca götürebilir. Bu ise konuya ilişkin ilkelerin uygulanabilirliği açısından sorun yaratabilir. Bir verinin kişisel sağlık verisi olup olmadığı sonraki süreçleri etkileyen temel sorudur. Nitekim kişisel sağlık verisi olduğuna karar verildikten sonra işlemenin hukuka uygun olup olmadığı incelenecektir. Bu anlamda işlemenin hukuksal dayanağı ve veri öznesinin aydınlatılmasına yönelik süreçler belirlenecektir.

Veri öznesinin kendisine ilişkin bilgiler ile arasındaki hukuksal bağın kurulmasında en önemli dayanaklardan biri rıza alımıdır. Veri öznesinin rızası hukuksal açıdan da meşru işleme nedenleri arasındadır[59]. Hatta örneğin Kişisel Verilerin Korunması Kanunu (KVKK) açısından açık rızanın veri işlemenin temel meşruiyet koşulu, yani kural olarak

[57] MARKS,Mason: "Emergent Medical Data", 11 Ekim 2017, http://blogs.harvard.edu/billofhealth/2017/10/11/emergent-medical-data/ (Erişim Tarihi: 3 Mart 2018).
[58] *Ibid.*
[59] AB Veri Koruma Yönergesi, m. 7/a, 8/2,a; GVKT, m. 6,9.

başvurulması gereken kaynak, olduğu görülür[60]. Sağlık teknolojilerindeki gelişmeler ise rıza alım süreçlerine ilişkin çeşitli soruları gündeme getirir. Bu noktada öncelikle rıza alımının hangi aşamada gerçekleştirileceği ve içeriğinin ne olacağı değerlendirilmelidir. Yukarıda da işaret edildiği gibi, sağlıkla ilgisi bulunmadığı düşünülen verilerden hareketle sağlık bilgisine ulaşılabilmektedir. Başlangıçta masum görülen bilgilerin ilk işleme amacından farklı amaçlarla ya da başka kişilerce işlenmesi veyahut çeşitli bilgilerle birleştirilmesi bu sonucu getirebilir. Bu durumda yalnızca verinin karakteristik yapısı üzerinden karar vermek yanıltıcı olacaktır, ilk ve sonraki kullanım amaçlarına da bakılmalıdır[61]. Bu hususun rıza beyanının içeriğine yansıtılması beklenir. Nitekim rızanın, veri öznesinin kendine ilişkin bilgiler üzerindeki denetimini sağlayabilmesi için belirli bir konuya ilişkin olması, bilgilendirilmeye dayanması ve özgür irade ile açıklanması beklenmektedir. Bu ölçütler farklı hukuksal düzenlemelerde benimsenmiştir[62].

Veri öznesi, sağlık bilgisi üzerinde denetimi bulunması için, neyi kabul ya da reddettiğini bilmelidir. Nitekim kendisine ilişkin bilginin sonraki kullanım alanlarını bilmesi veri işleme süreçlerinin şeffaflığı açısından gereklidir. Veri öznesinin kişisel sağlık verilerinin işleme süreçlerine ilişkin aydınlatılmasına yönelik hükümlerin[63] varlığı da mantıksal kaynağını burada bulur. Ancak uygulamada-özellikle Büyük Veri ve Nesnelerin İnterneti açısından düşünüldüğünde-verilerin sonuçlarının öngörülebilmesi pek de kolay olmayabilir[64]. Bu ise bilgilendirme ve aydınlatma yükümlülüklerinin içeriği konusunda duraksamaya neden olabilir. Bir diğer husus, özellikle bu verilerin tıbbi araştırmalarda kullanılması durumunda karşımıza çıkar. Tıbbi araştırmalarda, verilerin elde edilmesi sırasında rıza alımı sonraki kullanımlar farklılaşacağı için elverişli olmayabilir. Bu durumda gündeme gelebilen ve verinin ileriki kullanım alanlarını genişçe belirleyen "kapsamlı rıza" (broad consent) gibi yöntemler ise açık, özgülenmiş, bilgilendirmeye ve özgür iradeye dayanan rıza koşullarını karşılamamaktadır[65].

[60] KVKK, m. 5, 6.
[61] Article 29 Working Party:"Health Data in Apps and Devices" (Annex), s. 4.
[62] Örneğin KVKK, m. 3/1,a; GVKT, m. 4/11.
[63] Örneğin, KVKK, m. 10, GVKT, m. 13-14.
[64] CRAWFORD, Kate/ SCHULTZ, Jason: "Big Data And Due Process: Toward A Framework To Redress Predictive Privacy Harms", Boston College Law Review, 5, 2014, s. 93 vd.
[65] MOSTERT ve diğ.: s. 958.

Sağlık teknolojilerinin gelişmesi ile tekrar değerlendirme gereksinimi oluşan başka bir husus ise, kişisel sağlık verilerinin aktarımına ilişkindir. Uzaktan tanı ve tedavi, e-hekimlik, e-ilaç gibi pek çok örnekte bilgi aktarımı teknolojinin bir parçası hatta sunduğu olanağın temel koşuludur. Bu ise veri aktarımını sınırlayan hukuksal düzenlemeleri incelemeyi gerekli kılar. Nitekim kişisel sağlık verilerinin korunmasına yönelik hukuksal düzenlemelerde verilerin aktarılmasına ilişkin kurallar özel olarak belirlenmektedir[66]. Bu durumda veri öznesinin açık rızası ya da diğer hukuka uygunluk nedenleri mutlaka aranmalıdır. Bazı uygulamalarda ise aktarım ya da sonraki işleme etkinlikleri bulunmayabilir. Örneğin akıllı saat gibi giyilebilir teknolojiler açısından, tutulan veriler kimseye aktarılmıyorsa, yalnızca bu cihazın içinde tutuluyorsa veri korumaya ilişkin ilkelerin uygulanmayacağı düşünülebilir. 29. Madde Veri Koruma Grubu da görüşünü bu yönde açıklamıştır[67]. KVKK açısından bu durum, yasa hükümlerinin uygulanmayacağı durumlardan biri olan "[k]işisel verilerin (…) gerçek kişiler tarafından tamamen kendisiyle (…) ilgili faaliyetler kapsamında işlenmesi" istisnası[68] kapsamında değerlendirilebilir.

Bunun yanında teknolojideki gelişme, veri güvenliğine ilişkin hukuksal düzenlemelerin önemini de arttırmaktadır. Veri güvenliği uyarınca riske uygun teknik ve örgütsel güvenlik önlemleri alınmalıdır[69]. Bu önlemler alınırken veri işlenen araçların kendine özgü nitelikleri göz önünde tutulmalıdır. Bu açıdan sağlık teknolojilerindeki gelişmeler, yalnızca sayısallaştırılmış hasta dosyalarının korunmasının ötesinde bazı önlemleri gerektirir. Nitekim kalp pili, kalça protezi gibi vücut içine yerleştirilen parçalar, giyilebilen sağlık teknolojileri gibi ürünler çeşitlenmektedir. Nesnelerin İnternet'i ise hızla gelişmekte ve daha çok sayıda nesneyi birbiri ile "konuşur" kılmaktadır. Bu, siber atakları da daha olası kılar[70]. Sağlık teknolojileri söz konusu olduğunda ise oldukça ciddi risklerle karşılaşılabilir. Bu kapsamda, kişilerin sağlık bilgilerine yetkisiz kişilerce erişilebilmesi, yukarıda açıklandığı üzere, kişinin kendi bilgileri üzerindeki denetimini kaybetmesi, maddi ve manevi zarara uğraması gibi olumsuz sonuçlar yaratabilir. Bunun yanında yeni teknoloji ürünlerine yönelik saldırıların kişilerin sağlığı üzerinde doğrudan etki yaratabilmesi

[66] KVKK, m. 8,9; GVKT, m. 44 vd.
[67] Article 29 Working Party:"Health Data in Apps and Devices" (Annex), s. 5.
[68] KVKK, m. 28/1,a.
[69] GVKT, m. 32/1.
[70] GOODMAN, Marc:"An Internet of Hackable Things", The Wired World of 2016, Ocak 2016, s. 94-95.

de söz konusudur[71]. Bir siber saldırı sonrasında kalp pilinin çalışmamaya başlaması ya da şeker ölçüm cihazının kişiyi yanlış yönlendirecek bir konuma gelmesi olası tehlikelere örnek olarak gösterilebilir.

Rıza alım süreçleri, üçüncü kişilere aktarım ya da veri güvenliği konularında ortaya çıkan bazı sorunların çözümünde anonimleştirme bir yöntem olarak dikkate alınabilir. Belirli ya da belirlenebilir bir gerçek kişi ile ilişkili olmayan ya da artık veri öznesi ile ilişkilendirilmesi olanaklı bulunmayan bilgileri nitelemek için anonimlik kavramı kullanılmaktadır. Bu nedenle anonim bilgilere kişisel verilerin korunmasına ilişkin ilkelerin uygulanmayacağı kimi düzenlemelerde yer almaktadır[72]. Sağlık teknolojilerinin kullanımında ve tıbbi araştırmalar sırasında, bilgilerin yalnızca kümelenmiş biçimde paylaşılması ya da kimlik belirteçlerinin çıkarılması gizliliğin sağlanması için yeterli görülebilmektedir. Ancak çalışmalar gerçek anlamda anonimliğin sağlanmasındaki zorluğu ortaya koymaktadır[73]. Bu durum özellikle sağlıkla ilgili verilerin yeniden kullanımında ya da genomik veriler söz konusu olduğunda açıkça görülür[74]. Bu açıdan bilgilerin anonimleştirilerek paylaşılması, olası sakıncaların giderilmesinde elverişli bir yol gibi gözükse de tam anonimlik oluşmadığında sorunun çözümünü sağlamadığı, aksine sorunun üzerini örterek sağlık bilgisinin işlendiği bir durumu denetim alanının dışına çıkarabileceği belirtilmelidir.

II. Öneriler

Sağlık bilişim teknolojilerindeki yeniliklerin getirdiği yeni soru(n)ların çözümünde, risklerin bertaraf edilmesi ya da en aza indirgenmesinde hukuk kurallarının önemli bir yeri olacaktır. Nitekim bu gereksinimden hareketle son yıllarda konuya ilişkin hukuksal

[71] E-Sağlık alanında güvenlik risklerini değerlendiren bir araştırma için bkz. LIVEI, Dimitri/ SARRI, Anna/Christina SKOULOUDI, Security and Resilince in eHealth, Security Challenges and Risks, ENISA 2015.

[72] GVKT, Baş. Par. 58. KVKK'da ise anonim hale getirme, "Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesini" ifade eder (m. 3/1,b). Bu durumda anonim hale getirilen veriler için kişisel verilerin korunmasına yönelik ilkeler uygulanmayacaktır. Çünkü belirtilen nitelikteki bilgiler artık kişisel veri niteliğinde değildir.

[73] HEENEY, J./ HAWKINS, N./ VRIES, J. De/ BODDINGTON, P./ KAYE, J.: "Assessing the Privacy Risks of Data Sharing in Genomics", Public Health Genomics, 14, 2011, s. 17-25.

[74] MOSTERT ve diğ., s. 958; GYMREK Melissa/ McGUIRE, Amy L./ GOLAN, David/ HALPERIN, Eran/ ERLICH, Yaniv: "Identifying Personal Genomes by Surname Inference", Science, 339 (6117), 2013, s. 321-324.

düzenlemelerde artış görülmektedir. WHO verileri uyarınca elektronik sağlık kayıtlarında hastaların gizliliğini koruyan hukuksal düzenlemelerin küresel düzeyde oranı 2010 yılında %31 iken, 2015 yılında %55'e yükselmiştir. Ancak veri korumaya yönelik gelişkin düzenlemelerin olduğu bazı yerlerde de özel olarak sağlık verilerinin korunmasını düzenleyen kurallar bulunmayabilir. Bazı Avrupa devletlerinde bu durum görülmektedir[75]. Bu nedenle esasında düzenleme bulunan devletler belirtilenin üzerinde olabilir. Öte yandan şuna da işaret edilmelidir: Bu oran konunun hukuksal alana aktarımında bir artış olduğunu ortaya koysa da sağlık bilgilerinin korunmasına yönelik güvencenin düzeyi hakkında bir bilgi içermemektedir. Dolayısıyla bazı yerlerde konuya ilişkin hukuksal düzenlemeler bulunsa da bunlar etkin koruma açısından yetersiz kalabilir. Kapsamlı düzenlemelerin kabul edildiği yerlerde ise bunların yeni teknolojilere uyumluluğu ve uygulanma yöntemine ilişkin tartışmalar sürmektedir[76]. Bu durumda sağlık teknolojilerinin yarattığı yan etkilere karşın güvence sisteminin nasıl olması gerektiği konusunda öneri ve görüş geliştirmek anlamlıdır. Kanımızca sorunun çözümünde sağlık teknolojilerindeki dönüşümü dikkate alan bir bakış açısı yardımcı olacaktır. Bu değerlendirme noktasından hareketle yürürlükte bulunan ve ileriki dönemde kabul edilecek hukuksal düzenlemeler ile hukuk dışı güvenceler üzerinde durulabilir.

İlk olarak **mevcut hukuksal düzenlemeler** yeni bir bakış açısı ile değerlendirilmelidir. Bu açıdan elektronik sağlık alanında sınırlı düzenleme bulunan devletlerin daha avantajlı bir konumda olduğu dahi söylenebilir. Elektronik sağlık hizmetleri öncesinde kabul edilmiş kuralları değiştirme ve uyarlama çabasındansa, bu alana özgü yeni kurallar belirlemek daha kolay olabilir[77]. Ancak her hâlükârda, yani elektronik sağlık hizmetlerinin uygulamaya başlamasından sonra kabul edilmiş bir düzenleme bile olsa, hukuksal kurallar yeni teknolojilerin kendine has özellikleri ile uyumlu yorum geliştirmeye elverişli olmalıdır. Nitekim sağlık değişim hızlanarak devam etmektedir. Şu husus dikkate

[75] World Health Organisation: Global diffusion of eHealth: Making universal health coverage , s. 114.

[76] Örneğin bkz. DUMORTIER, Jos/VERHENNEMAN: "Legal Regulation of Electronic Health Records: A Comparative Analysis of Europe and the US", in George, Carlisle/ Whitehouse, Diane/ Duquenoy, Penny (ed.),eHealth: Legal, Ethical and Governance Challenges, Springer, Almanya 2013, s. 25-56.

[77] Bu yönde bir görüş için bkz. World Health Organisation: Global diffusion of eHealth: Making universal health coverage, s. 123.

alınabilir: Günümüzde verilerin %1'den azı incelenmiş ve kullanılmıştır[78]. Veri hacmi ise her geçen gün artmaktadır. İleriki dönemde özellikle Büyük Veri alanındaki gelişmeler sonunda daha büyük oranda bilginin işleneceği açıktır. Bunun sonucunda hâlihazırda son derece etkileyici olan veri analizlerinden ileride neler çıkarılabileceğini kestirmek güçtür.

Hukuk kurallarının teknoloji ile aynı hızda gelişmesi ve değişmesi beklenemez. Ancak teknolojik gelişmelerin dinamiğini ve dinamizmini dikkate alarak, teknoloji geçirmez (technology-proof) bir yapıda hukuksal kurallar benimsenirse, yeni bir ürün ile karşılaşıldığında bu bakış açısı ile uyumlu uygulama ve yorum geliştirilmesi olanaklı olabilir. Buna koşut olarak süreçlerde **şeffaflı**ğın arttırılması ve bunun ortaya konulan bakış açısının bir bileşeni olması gerektiği kanaatindeyiz. Bu husus, kişisel verilerin korunması açısından genel olarak geçerlidir. Kişisel sağlık verileri açısından ise, hassas niteliği dolayısıyla, daha da önemlidir. Kişinin kendi ruhsal ve bedensel durumuna ilişkin bilgilerinin üzerinde denetimi olmalıdır. Bu, yukarıda açıklandığı üzere, aynı zamanda psikolojik bir gereksinimdir. Bunun sağlanabilmesi için ise bireyin kendisi değil, bilgilerin işlenme süreçleri şeffaflaşmalıdır. Mevcut düzenlemeler bu konuda hükümler içerse de yeni gelişen teknolojiler karşısında bireyin bunları kullanabilme olanakları gerilemektedir. Konu, küresel düzeyde düşünüldüğünde daha da çarpıcı bir sorun olarak karşımıza çıkar. Örneğin WHO'ya üye devletlerin yalnızca %29'u hastalara elektronik ortamda kişisel sağlık verilerine ulaşmaya yönelik hukuksal düzenlemeleri kabul etmiştir[79].

Mevcut hukuksal düzenlemelerin bazı hükümleri, veri işleme süreçlerinde şeffaflığı geliştirmeye yönelik bir bakış açısı ile yorumlandığında etkili olabilir. Kanımızca bu zemini sağlayan hükümlerin gelecekte daha fazla uygulanacağını beklemek de makuldür. Nitekim özellikle pek çok yeni teknolojinin ayrıntılı veri analizlerine dayandığı düşünüldüğünde veri öznesinin sürece müdahale yeteneği, geliştirilmesi gereken bir unsur olarak karşımızca çıkar. Bu noktada bireysel karar alma süreçlerine ilişkin sınırlamalar geliştirilebilecek hükümlere örnek olarak verilebilir. Örneğin GVKT uyarınca tamamen

[78] Antonio REGALADO, bu oranı 2013 yılında %0,5 olarak vermiştir. REGALADO, Antonio: "The Data Made ME Do It", MIT Technology Review, 3 Mayıs 2013, https://www.technologyreview.com/s/514346/the-data-made-me-do-it/ (Erişim Tarihi: 4 Mart 2018).

[79] World Health Organisation: Global diffusion of eHealth: Making universal health coverage, s. 119.

otomatik veri işleme ile kişinin kendisi hakkında hukuksal sonuç doğuran veya onu etkileyen bir karara konu olmama hakkı bulunmaktadır[80].

Kişisel verilerin aktarımına ilişkin yürürlükteki hükümlerin de önümüzdeki dönemde daha sık uygulanacağı beklenebilir. Nitekim sayısallaşma kişisel sağlık verilerinin aktarımının yaygınlaşmasını da beraberinde getirmektedir. Yukarıda açıklandığı üzere bunun olumlu sonuçları olduğu gibi, bazı risklere de neden olmaktadır. Ulusal ya da uluslararası alanda olsun veri öznesinin kural olarak kişisel sağlık verilerinin aktarılacağı kişiler üzerinde denetimi olmalıdır. Çeşitli araştırmalar ilgili kişilerin kişisel sağlık verilerini hekimler ve sağlık görevlileri dışındaki kişilerle paylaşmada istekli olmadıklarını ortaya koymaktadır[81]. Ayrıca küresel düzeyde sağlık hizmetlerinin geliştirilmesi için uluslararası bilgi paylaşımının önemi her geçen gün biraz daha anlaşılmaktadır. Ancak bu paylaşımın kuralları belirlenmiş olmalıdır. Kişisel verilerin korunmasına ilişkin düzenlemelerin bulunduğu yerlerde genellikle bilginin aktarılacağı hedef devlette yeterli düzeyde koruma olması koşulu aranmaktadır[82]. Belirtmek gerekir ki tedavi ve bakım amacıyla, elektronik sağlık bilgilerinin uluslararası aktarımının kurallarını belirleyen düzenlemeler dünyanın sınırlı bir bölümünde bulunmaktadır. Bu düzenlemeler daha çok gelişmiş devletlerde kabul edilmiştir. Aynı şekilde bu bilgilerin ülke içinde ve farklı araştırma kuruluşları arasındaki paylaşımlarına ilişkin kuralların da özellikle az gelişmiş ve gelişmekte olan sınırlı sayıda devlette hukuksal düzenlemelere konu olduğu görülmektedir[83]. Buna ek olarak, sağlık hizmetlerindeki aktörlerin ulus devletlerin sınırlarını aşan çeşitliliği de kişisel sağlık verilerinin işlenmesine ilişkin kuralların küresel düzeyde uyumlaştırılması gerekliliğini arttırır[84].

---

[80] GVKT, m. 22. KVKK uyarınca ise veri öznesinin "[i]şlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme" hakkı bulunmaktadır. KVKK, m. 11/1, g.

[81] Örneğin bkz. European Commission: Attitudes towards the impact of digitisation and automation on daily life, Special Eurobarometer 460 (Summary), Avrupa Birliği 2017, s. 17 (http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm), (Erişim Tarihi: 20 Mart 2018).

[82] Örneğin bkz. KVKK, m. 9, GVKT, m. 44 vd.

[83] World Health Organisation: Global diffusion of eHealth: Making universal health coverage, s. 116-117.

[84] CALLENS, Stefaan "The EU Legal Framework on e-Health", in Mossialos, Elias/ Permanand, Govin/ Baeten, Rita/ Hervey, Tamara K. (ed.), Health Systems Governance in Europe, The Role of European Union Law and Policy, Cambridge University Press, Birleşik Krallık 2010, s. 579.

Yürürlükteki hukuksal kuralların sağlık teknolojilerinin gelişmesinden kaynaklı çıkarlar ile yukarıda işaret edilen değerler arasında dengeyi sağlamada elverişsiz kaldığı durumlar olabilir. Bu noktada **yeni geliştirilecek hukuksal düzenlemeler** üzerine düşünülmelidir. Kanımızca teknolojiyi bir bütün olarak dikkate alan ve denge sağlamaya yönelen bakış açısının bu süreçte büyük önemi bulunacaktır. Nitekim teknolojinin gelişim hızı dikkate alındığında yeni kuralların hızla eskimesi söz konusu olabilir. Düzenlemelerde teknoloji geçirmez yaklaşımın yanında teknolojik çözümleri hukuksal süreçlere katma, hedef olan hak korumasının gerçekleştirilmesinde olumlu etki yaratabilir. Bu yaklaşımın bazı örneklerini GVKT'de bulmak olanaklıdır. GVKT'nin "tasarım ve varsayılan yoluyla verilerin korunması" kenar başlığını taşıyan hükmü altında veri koruma ilkelerinin sağlanmasına destek olarak başvurulabilecek bazı teknik ve yönetsel önlemler düzenlenmiştir[85].

Teknoloji ile hukukun kesiştiği bir diğer alanın veri güvenliği olduğu söylenebilir. Veri koruma mevzuatında veri güvenliğine ilişkin ilkeler önemli bir yer tutmaktadır. Ancak bu ilkeler kişisel veri işleyen sistemler için öngörülmüştür. Oysaki yukarıda değerlendirildiği üzere, özellikle Büyük Veri uygulamalarında çoğu zaman ilk aşamada elde edilen verilerden çıkartılabilecek sonuçlar anlaşılamayabilir. Bu durum veri güvenliğinin yaygın uygulaması gerekliliğini de ortaya koymaktadır. Ancak belirtmek gerekir ki sağlık teknolojilerinin geliştirilmesine büyük yatırımlar yapılırken, veri güvenliğine ilişkin yatırımların çoğu zaman ilk aşamada gerçekleştirilmediği, sistem çalışmaya başladıktan sonra yapıldığı görülmektedir.

E-Sağlık hizmetlerinden güvenle yararlanılmasının sağlanması için bu sistemlere büyük yatırımlar yapılırken, veri güvenliği ihmal edilmemeli ve sistem henüz kuruluş aşamasında güçlü bir veri güvenliği sistemi ile desteklenmelidir. Bu husus elbette, teknik önlemlerin yanında örgütsel önlemlerin alınmasını da gerekli kılar. Veri güvenliğine ilişkin ilkenin yer aldığı çeşitli hukuksal düzenlemelerde bu husus "teknik ve idari önlemler" olarak nitelenmektedir[86]. Örneğin hasta kayıt sistemlerine erişim yetkisi bulunanların sınırlandırılması ve derecelendirilmesi bu kapsamda değerlendirilebilir. Bir başka anlatımla, veri güvenliğinin sağlanmasında kimlerin sağlık bilgilerine erişebileceğinin belirlenmesi yanında, kimlerin hangi bilgilere erişebileceği de belirlenmelidir.

[85] GVKT, m. 25.
[86] Örneğin bkz. KVKK, m. 12/1, GVKT, m. 32/1.

Yürürlükteki çeşitli düzenlemelerde yer alan bu ilkenin etkin uygulamasına yönelik olarak yeniden değerlendirilmesi yararlı olabilir. Bu noktada erişim yetkisi bulunanların kimlik denetimlerinin uygun bir usul ile yapılması da sağlanmalıdır. Elektronik imza, akıllı kartlar gibi kimlik tanımlama uygulamalarının bazı devletlerde tercih edildiği görülmektedir[87]. Bu uygulamaların yaygınlaştırılması veri güvenliğinin sağlanmasına yönelik olumlu etki yaratacaktır. Öte yandan veri güvenliğinin daha güçlü bir şekilde sağlanması da sağlık bilişim teknolojilerinin beklentileri gerçekleştirebilmesi için önemlidir. Bu husus, m-Sağlık uygulamaları üzerinden örneklendirilebilir. M-Sağlık kapsamında cep telefonu uygulamaları gibi gelişmekte olan alanların, gelecekte etkin ve erişilebilir sağlık hizmeti sunumuna önemli bir katkı sağlayacağı düşünülmektedir. Bu uygulamalar, hekime ve sağlık kuruluşuna ulaşamayan kişilere bu olanağı sunabileceği gibi, damgalanma endişesi ile sağlık hizmeti almaktan çekinen hastaya da yardımcı olabilir[88]. Ancak bu olumlu etkinin gerçekleşebilmesi için sürecin her aşamasında veri güvenliğinin sağlanması elzemdir. Unutulmamalıdır ki pek çok farklı aktörün yer aldığı bir zincir en zayıf halka kadar güçlüdür[89].

Teknoloji ile hukuksal kuralları kaynaştıran başka düzenlemeler üzerine de düşünülebilir. Örneğin rıza alım süreçlerinde yaşanan sorunların aşımında, teknoloji ile desteklenen farklı rıza alım yöntemlerine başvurulabilir. Bu noktada verilerin sonraki kullanımlarını hukuka uygun kılmaya yönelik bir öneri "dinamik rıza"dır (dynamic consent). Temel olarak dinamik rıza, enformasyon teknolojileri kullanımına ve bireylerin katılımını etkinleştirmeye dayanır. Böylelikle veri özneleri bilgilendirilebilecek ve gerektiğinde rızaları kolaylıkla alınabilecektir. Bu yönteme yöneltilen bir eleştiri ise veri öznesinin üzerinde bir bilgi yığımı yaratabilecek olmasıdır[90]. Bu haklı eleştirinin aşılabilmesi için bu alana ilişkin toplumda farkındalık düzeyini arttıracak

[87] European Commission: Overview of the national laws on electronic health records…, s. 36.

[88] European Commission: Green paper on mobile Health, s. 4.

[89] Article 29 Working Party: Opinion 02/2013 on apps on smart devices, 00461/13/EN WP 202, 27 Şubat 2013, s. 5 vd.

[90] MOSTERT ve diğ., s. 957; KAE, Jane/ WHITLEY, Edgar A./ LUND, David, MORRISON, Michael/ TEARE, Harriet/ MELHAM,Karen: "Dynamic Consent: A Patient Interface for Twenty-First Century Research Networks", European Journal of Human Genetics, 23, 2015, s. 141-146; STEINSBEKK, Kristin/ MYSKJA, Solum Bjørn Kåe/ SOLBERG, Berge:"Broad Consent versus Dynamic Consent in Biobank Research: Is Passive Participation a Ethical Problem?", European Journal of Human Genetics, 21, 2013, s. 897-902.

çalışmalar yapılması yararlı olabilir. Farkındalık eksikliklerinin yalnızca bireysel haklar açısından değil, e-Sağlık hizmetlerine yönelik düşük güven dolayısıyla bu teknolojilerin gelişmesinin önünde de engel oluşturduğu dile getirilmektedir[91]. Hâlihazırda farkındalığı arttırmaya yönelik bazı çalışmalar saptanabilse de[92] bunların sınırlı kaldığı görülmektedir. Farkındalık çalışmaları ile haklarını öğrenen kişi, daha bilinçli tercihlerde bulunabilir. Ancak her halükârda rıza metinlerinin ortalama bir kişinin anlayabileceği bir dille kaleme alınmasına ve makul bir uzunlukta olmasına dikkat edilmelidir.

Dinamik rıza yanında veri öznesinin sürece katılımını arttıran başka uygulamalar da benimsenebilir. Nitekim kişisel sağlık verilerini işlemeyi meşru kılan tek yasal dayanak olarak rızanın görülmesi, korumayı eksik kılar. Rızanın bulundu durumlarda da ilgiliye çeşitli haklar tanınmalıdır. Örneğin veri öznesinin kişisel sağlık verilerinin ne zaman ve nasıl kullanıldığını öğrenmesine ve bu konuda belirlemede bulunmasına yönelik güvenceler tanınabilir[93]. Bu kapsamda veri öznesinin, kişisel sağlık verilerinin yayınlanmasını önleme, kimlere aktarıldığını bilme, bu bilgilere kimlerin eriştiğini öğrenme gibi haklarını[94] kolay ve hızlı bir şekilde kullanımı teknolojik alt yapı ile de desteklenmelidir. Veri öznesinin kimlerin verilerine eriştiğini öğrenme olanağını arttıracak uygulamaların geliştirilmesi veri güvenliği açısından da olumlu sonuç yaratacaktır.

Kanımızca sağlık teknolojilerinin geliştirilmesi sırasında, bir başka anlatımla henüz sistem tasarım aşamasındayken, veri öznesinin haklarını gözeten bir yaklaşımın benimsenmesi çeşitli sorunların aşılmasına yardımcı olacaktır. Bu noktada hukuksal düzenlemelerin önemi büyüktür. Ancak hukuk dışı güvencelerin de veri öznesinin haklarının korunması açısından yararlı sonuçlar getirebileceği dikkatten kaçmamalıdır. Hukuksal düzenlemeleri destekleyen etik kuralların ve denetim sisteminin geliştirilmesinin yararlı olacağı kanısındayız. Nitekim e-Sağlık hizmetlerinin genişleyen uygulama alanı, dikkatlice değerlendirilmesi

[91] European Commission: eHealth Action Plan 2012-2020 - Innovative healthcare for the 21st century, s. 5.

[92] Örnek olarak WHO'nun Birleşmiş Milletler'in enformasyon ve iletişim teknolojilerine özgülenmiş birimi olan ITU ile ortaklaşa gerçekleştirdiği farkındalık çalışmaları gösterilebilir. Bkz. mHealth: use of mobile wireless technologies for public health, s. 3.

[93] Article 29 Working Party: Working Document on the processing of personal data relating to health in electronic health records (EHR), s. 13.

[94] Bu hakların bir kısmı yürürlükteki hukuksal düzenlemeler ile de tanınmıştır. Örneğin bkz. KVKK, m. 11, GVKT, m. 12 vd.

gereken pek çok etik soruyu gündeme getirmektedir[95]. Bu noktada önemli bir husus, sağlık bilişim teknolojileri ile ilişkili olarak, etik kuralların yalnızca sağlık görevlileri açısından düşünülmemesidir. Bu çalışmanın başında da işaret edildiği üzere hasta-hekim gizliliği ve buradan türeyen şekliyle sağlık personelinin sır tutma yükümlülüğünün eskiye dayanan bir geçmişi bulunmaktadır. Buradaki temel değerleri gözeterek ancak sağlık personeli ile sınırlı kalmayacak şekilde etik kuralların geliştirilmesi önerilebilir. Yukarıdaki örneklerde de görüldüğü üzere, sağlık teknolojilerinin seyri sağlık çalışanı olmayan başka aktörlerin de sürece eklendiğine işaret etmektedir. Belirtmek gerekir ki teknoloji ve değerler ilişkisi de uzunca sayılabilecek bir zamandır tartışılmakta ve her ikisini kaynaştırmaya yönelik değerlendirmeler yapılmaktadır[96]. Ayrıca tıbbi araştırmalar sırasında sağlık verilerinin yeniden kullanımının bir etik komitesi tarafından yetkilendirilme gerektirmesi[97] ya da yeni bir teknolojinin pazardaki yerini almadan önce etik değerlendirmeden geçirilmesi[98] önerilen yöntemler arasındadır.

SONUÇ

İçinde yaşadığımız 21. yüzyılın henüz ilk çeyreğinde çağımıza bilişim teknolojilerindeki gelişmelerin damga vuracağına yönelik pek çok işaret saptanabilir. Sağlık alanındaki dönüşüm de bu kapsamda değerlendirilebilir. Geleneksel sağlık hizmetini farklı bir boyuta taşıyacak yeni ürünler teknolojinin baş döndürücü bir hızla geliştiğini göstermektedir. Yukarıda bazı örnekler üzerinden değerlendirilen e-Sağlık uygulamaları da daha başarılı, ucuz ve hızlı önleme-tanı-tedavi süreçleri için pek çok olanak sunmaktadır. Ancak sağlık bilişim teknolojilerinin bizlere daha sağlıklı bir yaşam sunması olası yan etkilerinin en alt düzeyde tutulması ile olanaklı olabilir. Kanımızca bunun sağlanması için ise bireyin denetimine, sürecin şeffaflığına dayanan bir bakış açısının geliştirilmesi gerekir. Bu, yürürlükteki kuralların yorumuna ve geleceğin hukuk kurallarının tasarımına yansıtılabilmelidir. Teknolojinin yalnızca

[95] WANDHWA, WRIGHT, s. 185.

[96] Örneğin bkz. FLANAGAN, Mary/ HOWE, Daniel C./NISSENBAUM, Helen: "Embodying Values in Technology", in OVEN, Jeroen van den/ WECKERT, John (ed.), Information Technology and Moral Philosophy, Cambridge University Press, Birleşik Krallık 2008, s. 322-353.

[97] SETHI, Nayta/ LAURIE, Graeme T.: "Delivering proportionate governance in the era of eHealth: Making linkage and privacy work together", Medical Law International, 13, 2013, s. 168-204.

[98] WANDHWA, WRIGHT, s. 197.

hızla değil, aynı zamanda hızlanarak geliştiği ve yaygınlaştığı dikkate alınmalıdır. Ayrıca yasa koyucuların ve uygulayıcıların yeni teknolojilerin kendine özgü yapısını tanımalarının önemli olduğu düşüncesindeyiz. Bu, yalnızca sorunların daha doğru bir şekilde değerlendirilmesini değil, sorunların çözümünde teknolojiden daha fazla yararlanılmasını sağlayacaktır. Önümüzdeki yıllarda hukuk ile teknolojinin kaynaştığı alanları daha sık görebiliriz. Teknolojinin önünde bariyerler koymadan bireyin haklarını korumak için hukuk kurallarının yanında belirtilen bakış açısını sistemleştiren etik kurallara da daha sık başvurulması geleceğe daha güçlü, daha sağlıklı adımlarla ilerlememize yardımcı olacaktır.

KAYNAKÇA

ANDREESSEN, Marc, "Why Software Is Eating the World?", The Wall Street Journal, 20 Ağustos 2011.

Article 29 Data Protection Working Party: Working Document on the processing of personal data relating to health in electronic health records (EHR), WP 131, 15 Şubat 2007.

Article 29 Working Party: "Health Data in Apps and Devices" (Annex), Avrupa Komisyonu'nun m-Sağlık uygulamalarının ne zaman kişisel veri düzenlemelerinin kapsamına gireceğine ilişkin 29. Madde Veri Koruma Grubuna ilettiği mektuba cevaben, ekli belge, 5 Şubat 2015, (https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/20150205_letter_art29wp_ec_health_data_after_plenary_annex_en.pdf) (Erişim Tarihi: 20 Mart 2018).

Article 29 Working Party: Opinion 02/2013 on apps on smart devices, 00461/13/EN WP 202, 27 Şubat 2013, s. 5 vd.

BAUER, Christoph: "Grundprinzipien des Datenschutzes bei E-Health", in Bauer,Christoph/ Eickmeier, Frank/ Eckard, Michael (ed.), E-Health, Datenschutz, Datensicherheit, Herausforderungen und Lösungen im IoT-Zeitalter,Springer, Almanya 2018,s. 33.

BURKELL, Jacquelyn Ann: "Remembering me: big data, individual identity, and the psychological necessity of forgetting", Ethics and Information Technology, 18(1), 2016, s. 17-23.

CALLENS, Stefaan "The EU Legal Framework on e-Health", in Mossialos, Elias/ Permanand, Govin/ Baeten, Rita/ Hervey, Tamara K. (ed.), Health Systems Governance in Europe, The Role of European Union Law and Policy, Cambridge University Press, Birleşik Krallık 2010.

CAPLAN, Jeremy: "Cause of death. Sloppy doctors", Time, 15 Ocak 2007.

CHAWLA, Nitesh/ DAVIS, V. Darcy A.: "Bringin Big Data to Personalized Healthcare: A Paient-Centered Framework", Journal of General Internal Medicine, 28, 2013, s. 660-665.

CHUNG, Jason: "What Should We Do About Artificial Intelligence in Health Care?", NYSBA Health Law Journal, 22(3), 2017, s. 37-40.

COHEN,Julie E.: "What Privacy Is For", Harvard Law Review, 126, 2013, s. 1904-1933.

Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (T-PD): Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data, T-PD(2017)01, 23 Ocak 2017.

CRAWFORD, Kate/ SCHULTZ, Jason: "Big Data And Due Process: Toward A Framework To Redress Predictive Privacy Harms", Boston College Law Review, 5, 2014, s. 93-128.

Data doctors: How AI is changing healthcare, The Guardian (International Edition), 26 Ocak 2018.

DICK, Richard S./STEEN, Elaine B./ DETMER, Don E.: The Computer Based Patient Report, National Academy Press, ABD 1997.

DUHIGG, Charles: "How companies learn your secrets", The New York Times, 16 Şubat 2012.

DUMORTIER, Jos/VERHENNEMAN: "Legal Regulation of Electronic Health ecords: A Comparative Analysis of Europe and the US", in George, Carlisle/ Whitehouse, Diane/ Duquenoy, Penny (ed.),eHealth: Legal, Ethical and Governance Challenges, Springer, Almanya 2013, s. 25-56.

European Commission: Attitudes towards the impact of digitisation and automation on daily life, Special Eurobarometer 460 (Summary), Avrupa Birliği 2017, s. 17 (http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm), (Erişim Tarihi: 20 Mart 2018).

European Commission: eHealth Action Plan 2012-2020 - Innovative healthcare for the 21st century, Communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee and The Committee of the Regions, , COM(2012) 736 final, Brüksel, 6 Aralık 2012, s. 4.

European Commission: Green Paper on mobile health ("mHealth"), COM(2014) 219 final, Belçika 10 Nisan 2014.

European Commission:Accelerating the Development of the eHealth Market in Europe, eHealth Taskforce report 2007, Luxemburg 2007, s. 10.

EXTER,André den: "eHealth Law: The Final Frontier", in Hervey Tamara K./ Young, Calum Alasdair/ Bishop, Louise E., Research Handbook on Health Law and Policy, Edward Elgar Publishing, Birleşik Krallık 2017.

FEDER, Barnaby J.:"Remote Control for Health Care", The New York Times, 9 Eylül 2006, http://www.nytimes.com/2006/09/09/business/09node.html (Erişim Tarihi: 19 Mart 2018).

FLANAGAN, Mary/ HOWE, Daniel C./NISSENBAUM, Helen: "Embodying Values in Technology", in OVEN, Jeroen van den/ WECKERT, John (ed.), Information Technology and Moral Philosophy, Cambridge University Press, Birleşik Krallık 2008, s. 322-353.

FOLLEN, Morris C.: Computer Medical Databases, The First Six Decades (1950-2010), Springer, Birleşik Krallık 2012, s. 33-55.

FOUCAULT, Michael Hapishanenin Doğuşu, çev. Mehmet Ali Kılıçbay, 3. Baskı, İmge, Ankara 2006.

GOODMAN, Marc: "An Internet of Hackable Things", The Wired World of 2016, Ocak 2016, s. 94-95.

GREENLEAF, Graham: "Sheherezade and the 101 Data Privacy Laws: Origins, Significance and Global Trajectories", Journal of Law, Information and Science, 1(23), 2014, s.4-49.

GYMREK Melissa/ McGUIRE, Amy L./ GOLAN, David/ HALPERIN, Eran/ ERLICH, Yaniv: "Identifying Personal Genomes by Surname Inference", Science, 339 (6117), 2013, s. 321-324.

HAMET, Pavel/ TREMBLAY, Johanne: "Artificial Intelligence in Medicine", Metabolism Clinical and Experimental, 9, 2017, s. 536-540.

HEENEY, J./ HAWKINS, N./ VRIES, J. De/ BODDINGTON, P./ KAYE, J.: "Assessing the Privacy Risks of Data Sharing in Genomics", Public Health Genomics, 14, 2011, s. 17-25.

Hippocrates, Loeb Classical Library, çev. W. H. S. Jones, Harvard University Press, ABD 1923.

How your electronic DNA could be the secure login of the future, The Guardian, 18 Temmuz 2014, http://www.theguardian.com/technology/2014/jul/18/how-your-electronic-dna-could-be-the-secure-login-of-the-future (Erişim Tarihi: 5 Mart 2018).

HUMER, Caroline/ FINKLE, Jim: "Your medical record is worth more to hackers than your credit card", Reuters, 4 Eylül 2014, https://www.reuters.com/article/us-cybersecurity-hospitals/your-medical-record-is-worth-more-to-hackers-than-your-credit-card-idUSKCN0HJ21I20140924 (Erişim Tarihi: 4 Mart 2018).

JOURARD, Sidney M.: "Some Psychological Aspects of Privacy", Law and Contemporary Problems, 2 (31), 1966, s. 307-318.

KAE, Jane/ WHITLEY, Edgar A./ LUND, David, MORRISON, Michael/ TEARE, Harriet/ MELHAM, Karen: "Dynamic Consent: A Patient Interface for Twenty-First Century Research Networks", European Journal of Human Genetics, 23, 2015, s. 141-146.

Largest Healthcare Data Breaches of 2017, HIPAA Journal, 4 Ocak 2018, https://www.hipaajournal.com/largest-healthcare-data-breaches-2017/ (Erişim Tarihi: 5 Mart 2018).

LIVEI, Dimitri/ SARRI, Anna/Christina SKOULOUDI, Security and Resilince in eHealth, Security Challenges and Risks, ENISA 2015.

Making Medicines, A Brief History of Pharmacy and Pharmaceuticals, Anderson, Stuart (ed.), Pharmaceutical Press, Birleşik Krallık 2005.

MAKSIMOVIĆ, Mirjana/ VUJOVIĆ, Vladimir: "Internet of Things Based E-health Systems: Ideas, Expectations and Concerns", in Khan, Samee U./Zomaya, Albert Y./ Abbas, Assad (ed.), Handbook of Large-Scale Distributed Computing in Smart Healthcare, Springer, Almanya 2017.

MARKS, Mason: "Emergent Medical Data", 11 Ekim 2017, http://blogs.harvard.edu/billofhealth/2017/10/11/emergent-medical-data/ (Erişim Tarihi: 3 Mart 2018).

MOSTERT, Menno/ BREDENOORD, Annelien L./ CIH BIESAART, Monique/ DELDEN, Johannes JM van: "Big Data in Medical Research and EU Data Protection Law: Challenges o the Consent or Anonymise Approach", European Journal of Human Genetics, 24, 2016, s. 956-960.

Overview of the national laws on electronic health records in the EU Member States and their interaction with the provision of cross-border eHealth services, Final report and recommendations, Belçika 2014, s. 23 https://ec.europa.eu/health/sites/health/files/ehealth/docs/laws_report_recommendations_en.pdf (Erişim Tarihi: 20 Mart 2018).

PEREIRA, Stacey/ GIBBS, Richarda/ McGUIRE, A. Amy L.: "Open Access Data Sharing in Genomic Research", Genes, 5(3), 2014, s. 739-747.

RAGHUPATHI, Wullianallur/ RAGHUPATHI, Viju "Big data analytics in healthcare: promise and potential", Health Information Science and Systems, 2(3), 2014, s. 1-10.

REGALADO, Antonio: "The Data Made ME Do It", MIT Technology Review, 3 Mayıs 2013, https://www.technologyreview.com/s/514346/the-data-made-me-do-it/ (Erişim Tarihi: 4 Mart 2018).

RISSE, Guenter B.: Mending Bodies, Saving Souls, A History of Hospitals, Oxford University Press, Birleşik Krallık 1999.

SCHENEIER, Bruce: Data and Goliath, W.W. Norton & Company, ABD 2015.

SCHMIDT, Eric/ COHEN, Jared: The New Digital Age, Transforming Nations, Businesses, and Our Lives, Vintage, ABD 2014.

SETHI, Nayta/ LAURIE, Graeme T.: "Delivering proportionate governance in the era of eHealth: Making linkage and privacy work together", Medical Law International, 13, 2013, s. 168-204.

SOKOL, Daniel K./ HETTIGE, Samantha: "Poor handwriting remains a significant problem in medicine", Journal of the Royal Society of Medicine, 12 (99), 2006, s. 645-646.

SOLUM, Lawrence B.: "Legal Personhood for Artificial Intelligences", North Carolina Law Review, 7(4) 1992, s. 1231-1287.

STEINSBEKK, Kristin/ MYSKJA, Solum Bjørn Kåe/ SOLBERG, Berge:"Broad Consent versus Dynamic Consent in Biobank Research: Is Passive Participation a Ethical Problem?", European Journal of Human Genetics, 21, 2013, s. 897-902.

SULTAN, Nabil "Reflective thoughts on the potential and challenges of wearable technology for healthcare provision and medical education", International Journal of Information Management, 35, 2015, s. 523-525.

TANNER, Adam: Our Bodies, Our Data, How Companies Make Millions Selling Our Medical Records, Beacon Press, ABD 2017.

THOMPSON, John D./ GOLDIN, Grace: The hospital; a social and architectural history, Yale University Press, ABD 1975.

US Food and Drug Admnistration: "FDA approves pill with sensor that digitally tracks if patients have ingested their medication", 13 Kasım 2017, https://fda.gov/NewsEvents/Newsroom/PressAnnouncement/ucm584933.htm (Erişim Tarihi: 20 Mart 2018).

WACHTER, Robert: The Digital Doctor: Hope, Hype, and Harm at the Dawn of Medicine's Computer Age, Mc Graw-Hill, ABD 2017.

WANDHWA, Kush/ WRIGHT, David, "eHealth: Frameworks for Assesing Ethical Impacts", in George, Carlisle/ Whitehouse, Diane/ Duquenoy,,Penny (ed.), eHealth: Legal, Ethical and Governance Challenges, Springer, Almanya 2013, s. 184.

World Health Organisation: "eHealth at WHO", http://www.who.int/ehealth/about/en (Erişim Tarihi: 19 Mart 2018).

World Health Organisation: Global diffusion of eHealth: Making universal health coverage, Report of the third global survey on eHealth, Global Observatory for eHealth, İsviçre 2016.

World Health Organisation: mHealth, New horizons for health through mobile technologies, Global Observatory for eHealth series-Volume 3, İsviçre 2011, s. 5 http://www.who.int/goe/publications/goe_mhealth_web.pdf, (Erişim Tarihi: 19 Mart 2018).

World Health Organization, Executive Board: mHealth: use of mobile wireless technologies for public health (Report by the Secretariat), 139th session, Provisional agenda item 6.6, EB 139/8, 27 Mayıs 2016.