Kişisel sağlık verilerinin mahremiyeti

Ahmet Esad Berktaş

1987 yılında Karşıyaka'da doğdu. 2010 yılında Başkent Üniversitesi Hukuk Fakültesinden mezun oldu. Avukatlık stajını tamamlayarak mesleki çalışmalarda bulunmak üzere Londra'ya gitti. Yüksek lisansını İngiltere Southampton Üniversitesinde Bilişim Hukuku alanında "Kişisel Verilerin Korunması: AB ve Türkiye" konulu tez çalışması ile 2013'te tamamladı. Halen Medipol Üniversitesi Sosyal Bilimler Enstitüsünde Özel Hukuk doktora programına devam etmektedir. Sağlık Bakanlığı Sağlık Bilgi Sistemleri Genel Müdürlüğünde, Sağlık Bilişimi Hukuku Danışmanı olarak görev yapmaktadır. Türkiye Sağlık Enstitüleri Başkanlığı, Türkiye Biyoteknoloji Enstitüsü tarafından yürütülen Türkiye Genom Projesi Bilim Kurulu'nda yer almakta ve kişisel sağlık verilerinin korunması konusu özelinde çalışmaları bulunmaktadır. Berktaş, evlidir ve bir çocuk babasıdır.

Ülkemizde yakın bir döneme kadar yalnızca etik ilke ve kurallar kapsamında incelenmekte olan kişisel sağlık verilerinin mahremiyeti, bir süredir mevzuat hükümleri ile de düzenlenmektedir. Bu makalede konunun yalnızca hukuki boyutu değerlendirilecektir. Amerika'da ünlü bir söz vardır: "Bedavaya öğle yemeği yoktur." *Western* filmlerinde görmeye alışık olduğumuz salonlarda, içki isteyenlere ilave bir bedel ödemeksizin sınırsız yemek imkânı sunulmaktadır. Bu yemekler genellikle çok tuzlu ve su ihtiyacı doğuran gıdalardan oluşmaktadır. Ücretsiz olduğu için çokça tüketilen bu yemekler kişinin susamasına sebebiyet vermekte, bu da daha fazla içki talebine ve dolayısı ile daha yüklü bir faturaya yol açmaktadır. Yani bu veciz söz, herhangi bir kişi veya toplumun "hiçbir şey karşılığında herhangi bir şeyi" elde edemeyeceğini, bir ürün veya hizmetin ücretsiz sunulduğu düşünülse dahi bunun gizli bir bedeli olduğunu anlatmak için kullanılmaktadır. Herhangi bir bedel ödemeksizin kullanıldığı düşünülen, yıllık geliri 10,2 milyon dolar olan bir anlık mesajlaşma uygulamasının, 2014 yılında 22 milyar dolar karşılığında bir sosyal medya platformu tarafından satın alınmış olması, verinin değerini ortaya koyması bakımından önemli bir örnek teşkil etmektedir.

Günümüzün en değerli kaynağının artık petrol değil kaliteli veri olduğu kabul edilmektedir. Bunun gerekçesi de veri analitiği sistemleri sayesinde iş ve süreç etkinliğinin çok yüksek oranlarda geliştirilmesi, çok daha az harcama ile çok daha yüksek faydaların elde edilebilmesi imkânıdır. Yapılan bir araştırmada yalnızca büyük veriye (*big data*) bağlı ekonominin önümüzdeki yıl 43,7 milyar avro olacağı öngörülmekte (1), kötü verinin ABD ekonomisine maliyetinin ise yıllık 3.1 trilyon dolar olduğu ifade edilmektedir (2). İşte günümüzde verinin ulaştığı bu değer, mahremiyet problemlerini de beraberinde getirmekte, temel insan hak ve özgürlükleri arasında kabul edilen kişisel verilerinin korunmasını isteme hakkının daha etkin kullanılmasının önemini ve kişi mahremiyetinin sağlanması için alınması gereken hukuki, idari ve teknik önlemlerin önemini ortaya koymaktadır.

Siber korsanların, diğer verilere oranla sağlık verilerine daha fazla ilgi gösterdikleri görülmektedir. Yapılan araştırmalarda her 100 veri ihlâlinden 23'ünün sağlık sektöründe yaşandığı (3), 2012-2016 yılları arasında 140 milyon Amerika Birleşik Devletleri (ABD) vatandaşının sağlık verilerinin mahremiyetinin ihlâl edildiği (4), veri ihlâllerinde maliyetin kişi başına ortalama 158 dolar olmasına karşın sağlık sektörünün 355 dolar ile bu konuda zirvede olduğu (5), ABD'de siber güvenliği yeterince önemsemeyen sağlık hizmeti sunucularının 2015-2019 yılları arasında yaşayacakları veri ihlâlleri nedeniyle yaklaşık 305 milyar dolar kümülatif maliyete katlanmak zorunda kalacakları (6) ve veri mahremiyeti ile nesnelerin internetine ilişkin tehditlerin sağlık sektörüne yönelik en önemli tehditler arasında yer aldığı raporlanmaktadır (7).

Tarihsel Gelişim

Özel hayatın gizliliği ve mahremiyet hakkı kapsamında ele alınmakta olan kişisel verilerin korunması konusunda yaklaşık 50 yıl kadar önce dünya genelinde bir kanunlaştırma hareketi başlamıştır. Konuya ilişkin AB'deki ilk genel düzenleme olan ve 1995 yılında yürürlüğe giren 95/46/EC sayılı AB Direktifi ile konuya ilişkin çerçeve belirlenmiş ve üye ülkeler bu çerçeveye uygun olarak iç hukuklarında gerekli düzenlemeleri yapmıştır. Avrupa Komisyonu, teknolojinin ve haberleşme imkânlarının ilerlemesi, çok daha farklı ve büyük boyutlarda veri işleme tekniklerinin gelişmesi ve kişisel verilerin etkin bir şekilde korunması konusunda yaşanan zorluklar nedeniyle, 2012 yılında Genel Veri Koruma Tüzüğü (GDPR) taslağını hazırlamıştır. 27.04.2016 tarihinde kabul edilen ve iki yıllık bir geçiş süreci öngörülen GDPR, 25.05.2018 itibarıyla yürürlüğe girecek.

Ülkemizde ise 2010 yılında yapılan

Anayasa referandumunda, "Özel hayatın gizliliği" başlıklı 20'nci maddeye yeni bir hüküm ilave edilmiştir. Eklenen hüküm ile herkese kişisel verilerinin korunmasını isteme hakkı verilmiş ve kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenleneceği belirtilmiştir. İşte burada işaret edilen 6698 sayılı Kişisel Verilerin Korunması Kanunu, 07.04.2016 tarihli ve 29677 sayılı Resmî Gazete'de yayımlanarak yürürlüğe girmiştir.

Kişisel Sağlık Verileri

6698 sayılı Kanun'un hazırlanmasında 95/46/EC sayılı AB Direktifi esas alınmış olup, bu düzenlemelerin hükümleri arasında çok büyük bir benzerliğin bulunduğunu söylemek mümkündür. 6698 sayılı Kanun'da kişisel veriler; kişisel veri ve özel nitelikli kişisel veri olarak ikiye ayrılmakta, özel nitelikli kişisel veriler için daha sıkı bir koruma rejimi öngörülmektedir. 6698 sayılı Kanun'un 6'ncı maddesinin birinci fıkrasında özel nitelikli kişisel verilerin neler olduğu tahdidi olarak zikredilmekte, ikinci fıkrasında bu verilerin kural olarak açık rıza olmaksızın işlenemeyeceği ifade edilmekte, üçüncü fıkrasında ise bu kuralın istisnalarına yer verilmektedir.

Sağlığa ve cinsel hayata ilişkin veriler dışındaki özel nitelikli kişisel verilerin kanunlarda açıkça belirtilen hallerde ilgili kişinin açık rızası olmaksızın işlenebileceği öngörülmekte; buna karşın sağlığa ve cinsel hayata ilişkin kişisel verilerin ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebileceği düzenlenmektedir. 6698 sayılı Kanun'un gerekçesinde yetkili kurum ve kuruluşların, Sağlık Bakanlığı ve sağlık kuruluşları ile Sosyal Güvenlik Kurumu olduğundan bahsedilmektedir.

Dolayısı ile 6698 sayılı Kanun'da özel nitelikli kişisel veri olarak düzenlenen sağlık verilerine daha da özel bir konum atfedilmekte, bu verilerin kanunda açıkça öngörülmüş olma şartının sağlanmış olması hâlinde bile ilgili kişinin açık rızası olmaksızın işlenemeyeceği belirtilmekte, ancak madde hükmünde yer verilen istisnai amaçlarla ve istisnai taraflarca açık rıza olmaksızın işlenebileceği hüküm altına alınmaktadır.

6698 sayılı Kanun'un 6'ncı maddesinin dördüncü fıkrasında ise özel nitelikli kişisel verilerin işlenmesinde Kişisel Verileri Koruma Kurulu (Kurul) tarafından belirlenen yeterli önlemlerin alınması şart koşulmaktadır. Madde hükmünde ifade edilen yeterli önlemler 31.01.2018 tarihli ve 2018/10 sayılı Kurul Kararı ile

Ülkemizde 2010 yılında yapılan Anayasa referandumunda, "Özel hayatın gizliliği" başlıklı 20'nci maddeye yeni bir hüküm ilave edilmiştir. Eklenen hüküm ile herkese kişisel verilerinin korunmasını isteme hakkı verilmiş ve kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenleneceği belirtilmiştir. İşte burada işaret edilen 6698 sayılı Kişisel Verilerin Korunması Kanunu, 07.04.2016 tarihli ve 29677 Resmi Gazete'de yayımlanarak yürürlüğe girmiştir.

belirlenmiş ve 07.03.2018 tarihli Resmî Gazete'de yayımlanmıştır. 6698 sayılı Kanun sonrasında hazırlanan ve ilk sektörel düzenleme niteliğindeki Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelik (Kişisel Sağlık Verileri Yönetmeliği) ise 20.10.2016 tarihinde yürürlüğe girmiştir.

6698 sayılı Kanun'da tanımlanmayan '*kişisel sağlık verisi*' ifadesi, Kişisel Sağlık Verileri Yönetmeliğinde, "*Kimliği belirli ya da belirlenebilir gerçek kişinin fiziksel ve ruhsal sağlığına ilişkin her türlü bilgi ile kişiye sunulan sağlık hizmetiyle ilgili bilgi*" olarak tanımlanmaktadır. Bu tanım, önümüzdeki günlerde AB'de yürürlüğe girecek olan Tüzük'ten alınmış olup, veri mahremiyeti açısından ifadeyi doğruya en yakın şekilde tarif etmektedir.

Kişisel Sağlık Verileri Yönetmeliği'nin kapsamına kişisel sağlık verisi işleyen tüm kamu hukuku ve özel hukuk tüzel kişileri ile gerçek kişiler girmekle birlikte; ilgili maddelerin metninden anlaşılacağı üzere bazı hükümleri yalnızca sağlık hizmeti sunucuları bakımından bağlayıcıdır. Sağlık hizmeti sunucusu ise "*Ülke genelinde birinci, ikinci ve üçüncü basamakta faaliyet gösteren ve sağlık hizmeti sunmakta olan bütün sağlık tesisleri*" olarak tanımlanmaktadır. Yürürlüğe girdiği tarihte üyeleri henüz belirlenmemiş olduğu için görüşü alınamayan Kurul'un yapılanma süreçleri tamamlandıktan sonra Yönetmelik hakkında iki kere görüşü alınmış ve bu görüş çerçevesinde hazırlanan değişiklikler, 24.11.2017 tarihli Resmi Gazete'de yayımlanarak yürürlüğe girmiştir.

Merkezi Sağlık Veri Sistemi ve Kişisel Sağlık Kaydı Sistemi

3359 sayılı Sağlık Hizmetleri Temel Kanunu'nun 3'üncü maddesinin (f) fıkrasında, herkesin sağlık durumunun takip edilebilmesi ve sağlık hizmetlerinin daha etkin ve hızlı şekilde yürütülmesi maksadıyla, Sağlık Bakanlığınca ülke çapında kayıt ve bildirim sistemi kurulacağı öngörülmektedir. Bu kapsamda Bakanlık, merkezi sağlık veri sistemi olarak da ifade edilen Ulusal Sağlık Sistemi'ni (USS) kurmuştur.

663 sayılı Sağlık Bakanlığı ve Bağlı Kuruluşlarının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname'nin (663 sayılı KHK) 47'nci maddesinin ikinci fıkrası uyarınca Bakanlık, sağlık hizmeti almak üzere sağlık hizmeti sunucularına müracaat edenlerin verilerini alarak işleyebilmektedir.

Kişisel Sağlık Verileri Yönetmeliğinin beşinci maddesinin sekizinci fıkrası uyarınca sağlık hizmeti sunucuları, Kanun'un emredici hükümleri ile Kurul ve Bakanlık tarafından belirlenen usul ve esaslara uygun bir şekilde kişisel sağlık verilerini merkezi sağlık veri sistemine aktarmakla yükümlüdür. Yönetmelik'te yapılan sağlık hizmeti sunucusu tanımı nedeniyle üniversite hastanelerinin de USS'ye veri göndermekle yükümlü olduğunu söylemek mümkündür. Yine geçtiğimiz yıl yapılan değişiklikle Özel Hastaneler Yönetmeliği'nin 49'uncu maddesinin dördüncü fıkrasına da benzer bir hüküm ilave edilmiş, özel sağlık tesislerinin USS'ye veri gönderme yükümlülüğüne ilişkin yeni bir düzenleme yapılmıştır.

663 sayılı KHK'nın 47'nci maddesinin üçüncü fıkrasında, sağlık verisi işlenen kişilerin kendilerinin veya yetki verdikleri üçüncü kişilerin erişimlerini sağlayacak bir sistemin kurulması öngörülmektedir. Bu hüküm uyarınca hazırlanan e-Nabız Kişisel Sağlık Kaydı Sistemi'nde (e-Nabız) hesap oluşturan vatandaşlar, sağlık verilerine kimlerin erişebileceklerini istedikleri şekilde belirleyebilmekte, aile hekimleri de dâhil olmak üzere kendi sağlık verilerine başkalarının erişimini kısıtlayabilmektedirler. e-Nabız hesabı bulunmayan vatandaşların sağlık verileri ise yalnızca aile hekimleri tarafından görüntülenebilmekte, ayrıca randevu alınan hekim tarafından sağlık verilerine 24 saat süre ile sınırlı olmak kaydıyla erişilebilmektedir.

Taraflar

Kişisel verinin işlenmesi sürecinde taraflar; ilgili kişi (veri sahibi), veri sorumlusu ve varsa veri işleyenden oluşmaktadır. Bu tarafların kim olduğuna ilişkin tartışmalarda karışıklık yaşandığı gözlemlenmektedir. 6698 sayılı Kanun'da ilgili kişi, kişisel verisi işlenen gerçek kişiyi; veri sorumlusu, kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi; veri işleyen ise veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişiyi ifade etmektedir. Sağlık hizmeti almak üzere bir kamu hastanesini ziyaret eden hasta örneği üzerinden tarafları somutlaştırmak gerekirse veri sahibi hastadır. Veri sorumlusu, hastanenin ayrı bir tüzel kişiliği bulunmadığı gerekçesi ile hastanenin bağlı bulunduğu Sağlık Bakanlığının; veri işleyen ise kamu hastanesinde, Bakanlığın verdiği yetkiye dayanarak Bakanlık adına kişisel verileri işleyen Hastane Bilgi Yönetim Sistemi firmasının tüzel kişiliğidir.

Bununla birlikte, veri sorumlusunun tespiti her zaman kolay olmayabilmektedir. Özellikle şehir hastanelerinde durumun biraz daha karışık olduğunu söylemek mümkündür. Nitekim veri sorumlusunun tanımında yer alan unsurlar farklı kişilere işaret etmektedir. Şehir hastanelerinde kişisel sağlık verilerinin işlenme amaçla-

rını ve vasıtalarını Bakanlık belirlemekte; buna karşın veri kayıt sisteminin kurulmasından ve yönetilmesinden ise sözleşme gereği yüklenici sorumludur. Bu konuda yaşanması muhtemel uyuşmazlıkların önüne geçmek için Kurul tarafından gerekli düzenleyici işlemlerin yapılması gerektiği değerlendirilmektedir.

Yaptırımlar

Kişisel sağlık verileri hukuka aykırı olarak işlenen, üçüncü kişilere aktarılan veya verilerin işlenmesini gerektiren sebepler ortadan kalkmış olmasına karşın verileri yok etmeyenler ya da 6698 sayılı Kanun'da yer alan kabahatler hakkında farklı yollara başvurulabilir. Kişisel sağlık verilerinin işlenmesinde yasal düzenlemelere aykırı davrananlar hakkında takip edilebilecek yollar üç farklı başlık altında incelenebilir.

İlk olarak Türk Medeni Kanunu'nun 24'üncü maddesi uyarınca herkes, hukuka aykırı olarak kişilik haklarına saldırıda bulunanlara karşı korunmayı isteyebilir. Kişiliğin korunması kapsamında değerlendirilen kişisel verilerinin korunmasını isteme hakkı uyarınca hukuk mahkemelerinde maddi ve manevi tazminat davası açılabilir.

İkinci olarak kişisel sağlık verisi hukuka aykırı olarak işlenenler hakkında Türk Ceza Kanunu'nun (TCK) 135 ila 140'ıncı madde hükümleri uygulanabilir. Kişisel sağlık verisi hukuka aykırı olarak kaydedenler hakkında 1 yıldan 3 yıla kadar hapis cezasının öngörüldüğü TCK m. 135, kişisel sağlık verisini hukuka aykırı olarak bir başkasına veren, yayan veya ele geçirenler hakkında 2 yıldan 4 yıla kadar hapis cezasının öngörüldüğü TCK m. 136, kişisel sağlık verisini hukuka uygun bir şekilde işledikten sonra veri işlemeyi gerektiren sebep ortadan kalkmış olmasına rağmen verileri sistem içerisinde yok etmeyenler hakkında ise 1 yıldan 2 yıla kadar hapis cezasının öngörüldüğü TCK m. 138 uyarınca suç duyurusunda bulunulabilir. Kişisel verinin sağlığa ilişkin olması halinde veya suçların kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle ya da belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle işlenmesi durumunda verilecek olan cezanın yarı oranda artırılacağı hüküm altına alınmıştır.

Üçüncü ve son olarak, kişisel sağlık verisi hukuka aykırı olarak işlenen kişi, 6698 sayılı Kanun'un 13'üncü maddesi uyarınca veri sorumlusuna başvurabilir. Başvurunun reddedilmesi veya verilen cevabın yetersiz bulunması ya da başvurunun otuz gün içerisinde cevaplandırılmaması hâlinde ilgili kişi, Kurula şikâyet başvurusunda bulunabilir. Kurul, yapacağı inceleme sonucunda kişisel sağlık verilerinin işlenmesinde 6698 sayılı Kanun'un emredici hükümlerine uymayan veri sorumluları hakkında, Kanun'un 18'inci maddesinde öngörülen 5 bin ile 1 milyon lira arasında idari para cezasına hükmedebilir.

Uygulamadaki Yanlışlar

6698 sayılı Kanun'da açık rıza için herhangi bir şekilde şartı belirlenmemiş olsa da, Hasta Hakları Yönetmeliği'nin 34'üncü maddesi uyarınca tıbbi araştırmalarda rıza yazılı şekil şartına tabidir. Kişisel verilerinin bilimsel araştırmalarda kullanılmasına onam vermeyen hastaların verileri bu çalışmalarda hiçbir şekilde kullanılmamalıdır. Özellikle retrospektif çalışmalar bakımından bu sürecin yeterince işletilmediği, sağlık hizmeti sunucusunu tıbbî teşhis ve tedavi amacıyla ziyaret eden hastaların onamı olmaksızın, verilerinin bilimsel çalışmalarda da kullanıldığı görülmektedir.

Bazı hekimler tarafından yapılan bir diğer hata da farklı gerekçelerle hastaya, gerçekte bulunmayan bir tanının girilmesidir. Hastaya gerçekte var olmayan bir tanının girilmesi veya gerçekte var olan bir tanının silinmesi, bir diğer ifade ile verileri mevzuata aykırı olarak değiştirme işlemleri, hekimin sorumluluğunu gerektirmektedir. Bu durum henüz ciddi bir risk olarak görülmese de özellikle veri koruma mevzuatına ilişkin farkındalığın artmasıyla birlikte malpraktis benzeri bir tablonun yaşanabileceği değerlendirilmektedir.

Mevzuat Eleştirileri

Biyometrik verilerin ve genetik verilerin tekil tanımlayıcı özellikte oldukları, bunun da ötesinde genetik verilerin yalnızca ait olduğu kişinin kendisini değil; aynı zamanda kişinin biyolojik yakınlarını da tanımlayıcı nitelikte olduğu bilinmekte ve bu nedenle söz konusu verilerin, sağlığa ve cinsel hayata ilişkin verilere kıyasla çok daha mahrem oldukları düşünülmektedir. Buna karşın biyometrik veriler ile genetik veriler, sağlığa ve cinsel hayata ilişkin verilerin aksine, kanunlarda açıkça öngörülmüş olma hâlinin sağlandığı durumlarda ilgili kişilerin açık rızası olmaksızın işlenebilmekte ve dolayısıyla aktarılabilmektedir. Kişiselleştirilmiş tıp uygulamalarının giderek önem kazandığı günümüzde, özellikle genetik veriler için daha özel bir koruma rejiminin öngörülmesi gerekmektedir. 6698 sayılı Kanun'da öngörülen idari para cezalarının üst limitinin, trilyon dolarlık sağlık sektörünün milyar dolarlık aktörleri üzerinde caydırıcılıktan son derece uzak olduğu, bu nedenle cezaların GDPR'da düzenlendiği şekilde revize edilmesi ve ciddi oranda artırılması düşünülmelidir.

Kişiselleştirilmiş tıp uygulamalarının giderek önem kazandığı günümüzde, özellikle genetik veriler için daha özel bir koruma rejiminin öngörülmesi gerekmektedir. 6698 sayılı Kanun'da öngörülen idari para cezalarının üst limitinin, trilyon dolarlık sağlık sektörünün milyar dolarlık aktörleri üzerinde caydırıcılıktan son derece uzak olduğu, bu nedenle cezaların GDPR'da düzenlendiği şekilde revize edilmesi ve ciddi oranda artırılması düşünülmelidir.

Kaynaklar

1) Avrupa Komisyonu (2017) – https://ec.europa.eu/epsc/sites/epsc/files/strategic_note_issue_21.pdf (Erişim Tarihi: 10.01.2019)

2) Harvard Business Review (2016) – https://hbr.org/2016/09/bad-data-costs-the-u-s-3-trillion-per-year (Erişim Tarihi: 09.01.2018)

3) Baker Hostetler (2016) - http://f.datasrvr.com/fr1/516/11618/BakerHostetler_2016_Data_Security_Incident_Response_Report.pdf (Erişim Tarihi: 11.02.2018)

4) U.S. Department of Health & Human Services-Office for Civil Rights – https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (Erişim Tarihi: 09.01.2018)

5) Ponemon (2016) - https://public.dhe.ibm.com/common/ssi/ecm/se/en/sel03094wwen/SEL03094WWEN.PDF (Erişim Tarihi: 09.01.2018)

6) Accenture (2015) - https://www.accenture.com/t20150723T115443__w__/us-en/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Dualpub_19/Accenture-Provider-Cyber-Security-The-$300-Billion-Attack.pdf (Erişim Tarihi: 09.01.2018)

7) PwC (2018) – https://www.pwc.com/us/en/health-industries/assets/pwc-health-research-institute-top-health-industry-issues-of-2018-report.pdf (Erişim Tarihi: 25.02.2018)