

## TÜRK HUKUKUNDA KİŞİSEL SAĞLIK VERİLERİ VE İDARENİN KİŞİSEL SAĞLIK VERİLERİNİ KORUMA YÜKÜMLÜLÜĞÜ

*Personal Health Data in Turkish Law and the Obligation of the Administration to Protect Personal Health Data*

Ayşe Aşlı ALÇIN\*

### Özet

Hassas kişisel veriler kategorisi içinde yer alan kişisel sağlık verileri, “kimliği belirli ya da belirlenebilir gerçek kişiye ilişkin her türlü sağlık bilgisi” olarak tanımlanabilir. Bu tanımın kapsamına kişinin “geçmişi, şimdiki anı ve geleceğine ilişkin fiziksel ve ruhsal sağlığı hakkında her türlü bilgi ile kişiye sunulan sağlık hizmetiyle ilgili bilgiler” dahildir.

Bu çalışmada öncelikle, ulusal ve Türkiye’nin taraf olduğu uluslararası düzenlemeler ışığında, kişisel sağlık verileri kavramı ve bu verilerin işlenmesine ilişkin kurallar ve usuller ele alınacaktır. Türk hukukunda kişisel sağlık verilerinin işlenebileceği hallere ayrıca değinilecektir. Bu bağlamda, veri koruma hukukunda, hassas verilerin işlenmesinin diğer verilere kıyasla daha katı bir denetime tabi tutulması anlamına gelen hassaslık ilkesi ve veri toplama ve işlemenin bağlı olduğu amaç/amaçları gerçekleştirmek için zorunlu olan miktarla sınırlı olacak şekilde veri toplanması gerekliliğini ifade eden minimumluk ilkesine uygunluk değerlendirmesi yapılacaktır. Ardından, idarenin kişisel sağlık verilerinin korunmasına ilişkin yükümlülükleri açıklanacaktır. İdarenin kişisel sağlık verilerine ilişkin aydınlatma, veri güvenliğini sağlama, düzenleme ve denetleme yapma yükümlülüklerinin anlamı ve kapsamı ortaya konulacaktır.

Avrupa İnsan Hakları Mahkemesi ve Danıştay kararları ışığında, idarenin söz konusu yükümlülüklerini yerine getirmemesi durumunun nasıl ortaya çıkabileceği ve ortaya çıkış şekillerine göre sorumluluğunun türünün ve kapsamının ne olacağı ihtimallere göre değerlendirilecektir.

**Anahtar Kelimeler:** Hassas veri, Kişisel veri, Veri güvenliği, Veri işleme, Hasta hakları, Sağlık hakkı

➤ Bu makale Etik Kurul İznine tabi değildir/This article is not subject to Ethics Committee Permission.

➤ Makale Geliş Tarihi/Article Received Date: 15.11.2021

➤ Yayın Kurulu Kabul Tarihi/Editorial Board Acceptance Date: 09.03.2022

\* Dr. Arş. Gör., Bursa Uludağ Üniversitesi Hukuk Fakültesi, İdare Hukuku Anabilim Dalı, ayseasliyucesoy@gmail.com, <https://orcid.org/0000-0003-4788-2234>



## Abstract

Personal health data contained in the category of sensitive personal data can be defined as “any health data related to an identified or identifiable natural person.” The scope of this definition includes “all kinds of data in regard to physical and mental health of a person related to his/her past, present and future, as well as data in regard to the healthcare service provided to such person.”

This study firstly discusses the concept of personal health data in the light of international regulations, to which Turkey is a party and the rules and principles related to the processing of these data. The cases in which personal health data can be processed in Turkish law will also be discussed. In this context, an assessment about conformity to the principle of minimum, which indicates the necessity to collect data in such a way that such data are only limited to the amount that is necessary to perform the objective/objectives that data collection and processing are affiliated to and the principle of sensitivity, which means processing of sensitive data is subjected to a much more audit compared to other data in data protection law. Then, the obligations of the administration regarding the protection of personal health data will be explained. The meaning and the scope of the obligations of the administration for clarification about personal health data, ensuring data safety, performing regulations and audits will be explained.

In the light of the resolutions of the European Court of Human Rights and the Council of State, how the failure of the administration to fulfill such obligations might occur and the type and scope of responsibility based on the form of failure, will be evaluated according to possibilities.

**Keywords:** Sensitive data, Personal data, Data security, Data processing, Patient rights, Right to health

## GİRİŞ

“Belirli ya da belirlenebilir bir gerçek kişiye ilişkin her türlü bilgi” olarak tanımlanabilecek kişisel verilere, hem devlet ve diğer kamu tüzel kişileri hem de özel hukuk tüzel kişileri tarafından çok çeşitli amaçlarla ihtiyaç duyulmaktadır. Bilgi teknolojileri ve internetin yaygın kullanımı ile birlikte giderek daha fazla kişisel veri oluşurken bu verilerin korunması da gün geçtikçe daha da güçleşmektedir. Zira bilgi ve iletişim teknolojileri bu verilerin düzenlenmesini, depolanmasını, işlenmesini, verinin hızlı ve hatta sahibinden bağımsız şekilde yayılmasını kolaylaştırmaktadır.<sup>1</sup>

Nitelikleri gereği daha etkili bir korumaya ihtiyaç duyan hassas kişisel veriler, çeşitli örgütlerce kişisel verilere duyulan gereksinim, verileri giderek daha akışkan hale getiren teknolojiadaki gelişmeler ve bu gelişmelerin bireylerde yarattığı sürekli takip altında olma kaygısı üçgeninde<sup>2</sup> en kritik noktada yer alır.

<sup>1</sup> Orla Lynskey, *The Foundations of EU Data Protection Law*, (Oxford University Press Oxford 2015) 2.

<sup>2</sup> Elif Küzeci, *Kişisel Verilerin Korunması* (3. Bası, Turhan Kitabevi Ankara, 2019 18.

Hassas kişisel veri kategorisindeki sağlık verilerinin toplanması ve kullanılması, sağlık kamu hizmetinin kaliteli ve etkin şekilde sunulmasına, bilimsel araştırmaların geliştirilmesine en genel anlamıyla kamu yararına hizmet eder. Toplumsal sistem içerisinde “en güçlü bilgi tekeline”<sup>3</sup> sahip olan idarenin sağlık kamu hizmeti faaliyetini etkin ve verimli şekilde yerine getirebilmek için bireylere ait verilere, bu verilerin toplanması, kaydedilmesi ve analiz edilmesine ihtiyacı vardır. Fakat bu ihtiyaç, bilişim teknolojilerindeki gelişmeler ve veri işleme hacmindeki büyüme nedeniyle kişisel sağlık verilerin korunamaması riskini de arttırmaktadır.<sup>4</sup> Bu riskin bertaraf edilebilmesi için idarenin, hizmetten yararlananlara ait verileri toplar ve kullanırken en üst düzeyde veri güvenliğini sağlaması ve koruması gerekmektedir.

Bu çalışmada öncelikle ulusal ve Türkiye’nin taraf olduğu uluslararası düzenlemeler ışığında kişisel veri, hassas kişisel veri ve kişisel sağlık verisi kavramları ele alınacak, kişisel sağlık verilerinin işlenmesi meselesine değinilecektir. Ardından idarenin kişisel sağlık verilerini koruma yükümlülüğü ve bu yükümlülüğünün ihlali halinde doğacak olan sorumluluğu üzerinde durulacaktır.

## I. BİR HASSAS KİŞİSEL VERİ TÜRÜ OLARAK KİŞİSEL SAĞLIK VERİLERİ

### A. Ulusal ve Türkiye’nin Taraf Olduğu Uluslararası Düzenlemeler Işığında Kişisel Veri ve Hassas Kişisel Veri Kavramı

Bilişim teknolojilerinin gelişmesi, iletişim kanallarının artması ve internetin yaygınlaşması bilgi alışverişi olanağını arttırırken, kişisel verilerin, bireyin iradesi dışında, üçüncü kişilerce hukuka uygun ya da aykırı yollardan toplanıp işlenmesini oldukça kolaylaştırmıştır. Daha önce yazılı halde bulunan veriler sayısal ortama aktarılabilir ve çok büyük sayıda veriler, çok küçük aygıtlarda depolanabilir hale gelmiştir.<sup>5</sup> Bu nedenle ulusal ve uluslararası zeminde bu alana ilişkin düzenleme yapma ihtiyacı doğmuştur. Bu ihtiyaç ilk olarak 1970’li yıllarda Avrupa’da ortaya çıkmışsa da, günümüzde tüm dünyaya yayılmıştır.<sup>6</sup>

Kişisel verilerin korunmasına ilişkin ilk hukuki düzenleme, federe düzeyde, 7 Ekim 1970 tarihli Almanya’nın Hessen Eyaletine ait Kişisel Verilerin

<sup>3</sup> Küzeci (n 2) 26; “Bir ülkede en güçlü veri tekele idaredir. Bu gücün sınırlandırılması özel yaşamın ve düşünce ve kanaat özgürlüğünün korunması bakımından önemlidir.” AYM, E.2006/167, K.2008/86, K.T. 20.03.2008.

<sup>4</sup> Küzeci (n 2) 477.

<sup>5</sup> Murat Volkan Dülger, ‘Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Bağlamında Kişisel Verilerin Ceza Normlarıyla Korunması’ (2016) 2 İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi 102.

<sup>6</sup> Dülger, ‘İnsan Hakları ve Temel Hak ve Özgürlükler Bağlamında Kişisel Verilerin Korunması’ (2018) 1 İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi 76.

Korunması Kanunudur.<sup>7</sup> Avrupa’da kişisel verilere ulusal düzeyde koruma sağlayan ilk yasal düzenleme ise 1973 İsveç Veri Koruma Kanunudur.<sup>8</sup> Bu süreci, 1974’te ABD Özel Yaşamın Gizliliği Kanunu, 1977’de Federal Alman Veri Koruma Kanunu ve 1978 yılında çıkarılan Fransız Elektronik Veri İşlemesi, Veriler ve Özgürlük Haklarına İlişkin Kanun takip etmiştir.<sup>9</sup>

Uluslararası düzenlemelere bakıldığında, öncelikle ülkemizin de üyesi bulunduğu Ekonomik İşbirliği ve Kalkınma Teşkilatı (OECD) tarafından 1980 yılında kabul edilen Özel Yaşamın Korunması ve Kişisel Verilerin Sınırötesi Akışına İlişkin Rehber İlkeler<sup>10</sup> dikkat çekmektedir.<sup>11</sup> Sekiz maddeden oluşan Rehber İlkelerin<sup>12</sup>, OECD’ye üye ülkeler bakımından herhangi bir bağlayıcılığı bulunmamakta olup ulusal düzeydeki veri koruma yasalarının birbiri ile uyumlulaştırılması amacını taşımaktadır.<sup>13</sup>

Kişisel verilerin korunmasına dair ilk milletlerarası düzenleme olan Özel Yaşamın Korunması ve Kişisel Verilerin Sınırötesi Akışına İlişkin Rehber İlkeler<sup>14</sup> kişisel verileri, “belirli ya da belirlenebilir gerçek kişiye ilişkin tüm bilgiler” olarak tanımlamıştır.

Avrupa Konseyi tarafından hazırlanan 28 Ocak 1981 tarih ve 108 nolu

<sup>7</sup> Mesut Sarder Çekin, *Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kişisel Verilerin Korunması Kanunu* (1. Bası, On İki Levha, İstanbul, 2018) 5; Hüseyin Murat Develioğlu, *Avrupa Birliği Genel Veri Koruma Tüzüğü* (1. Bası, On İki Levha, İstanbul, 2017) 6; Türkay Henkoğlu, *Bilgi Güvenliği ve Kişisel Verilerin Korunması* (1. Bası, Yetkin, Ankara, 2015) 50; Küzeci (n 2) 103.

<sup>8</sup> Metin Turan, *Karşılaştırmalı Hukukta Kişisel Verilerin Korunması* (1. Bası, Adalet Yayınevi, Ankara, 2017) 4; Lynskey (n 1) 47.

<sup>9</sup> Lynskey (n 1) 47; Turan (n8) 4.

<sup>10</sup> Bu sekiz ilke şu şekildedir:

- Veri toplamının sınırlı olması ilkesi (m.7),
- Veri kalitesi ilkesi (m.8),
- Amacın belirli olması gerektiği ilkesi (m.9),
- Sınırlı kullanım ilkesi (m.10),
- Veri güvenliği ilkesi (m.11),
- Açıklık ilkesi (m.12),
- Bireyin katılımı ilkesi (m.13),
- Hesap verme zorunluluğu ilkesi (m.14).

<sup>11</sup> Çekin (n 7) 7; Develioğlu (n 7) 6; Lynskey (n 1) 47; Küzeci (n 2) 115; Gloria Gonzalez Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Springer 2014) 78.

<sup>12</sup> OECD Rehber İlkeleri 2013 yılında revize edilerek yeniden yayınlanmıştır. Bkz. [http://www.oecd.org/sti/ieconomy/oecd\\_privacy\\_framework.pdf](http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf), (26.08.2021).

<sup>13</sup> Hüseyin Can Aksoy, *Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması* (1. Bası Çakmak Yayınevi Ankara 2010) 4; Gonzalez Fuster (n 11) 80.

<sup>14</sup> OECD Özel Yaşamın Korunması ve Kişisel Verilerin Sınırötesi Akışına İlişkin Rehber İlkeler md. 1. Tam metin için bkz. <http://www.oecd.org/sti/ieconomy/oecdguidelinesontheProtectionofPrivacyandTransborderFlowsofPersonalData.htm>, (21.08.2021).

Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi ise kişisel verilerin korunmasına dair ilk bağlayıcı uluslararası hukuk belgesidir.<sup>15</sup> Türkiye açısından, yasama organı tarafından çıkarılan onay kanunu ile<sup>16</sup> bağlayıcı hale gelen Sözleşmenin yürürlüğe konulması ise 1 Eylül 2016 tarihinde mümkün olabilmıştır. Sözleşmede, kişisel verilerin korunmasına ilişkin çerçeve niteliğinde olan asgari standartlar, temel ilkeler belirlenmiş,<sup>17</sup> Avrupa Konseyi bu standartları geliştirmek amacı ile çeşitli alanlara yönelik olarak tavsiye kararları almıştır.<sup>18</sup>

108 nolu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesinde<sup>19</sup> de kişisel veri aynı şekilde “kimliği belirli ya da belirlenebilir bir gerçek kişi hakkındaki tüm bilgiler” olarak tanımlanmaktadır.

Avrupa Birliği düzeyinde ilk düzenleme olan<sup>20</sup> Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin 95/46/EC sayılı ve 24 Ekim 1995 tarihli Avrupa Parlamentosu ve Avrupa Konseyi Direktifi<sup>21</sup> ise mevcut veri koruma hukukunu güçlendirmekle kalmayıp<sup>22</sup> yeni bazı haklarla onu pekiştiren ortak bir çerçeve sunmuştur.<sup>23</sup> Bu Direktif esas olarak Avrupa birliği içinde, üye devletler içerisinde uyumlu bir hukuksal düzenin kurulmasını ve üye devletlerin veri koruma hukuku kurallarının kapsamlı ve boşluksuz bir şekilde uyumlaştırılmasını hedeflemiştir.<sup>24</sup>

<sup>15</sup> Aksoy (n 13) 5; Oğuz Şimşek, *Anayasa Hukukunda Kişisel Verilerin Korunması* (1. Bası Beta Yayınevi İstanbul 2008) 22; Gonzalez Fuster (n 11) 89.

<sup>16</sup> RG. 17.03.2016 – 29656.

<sup>17</sup> Küzeci (n 2) 128; Şimşek (n 15) 22.

<sup>18</sup> 108 nolu Sözleşmeye ek, 181 nolu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesine Ek Denetleyici Makamlar ve Sınıraşan Veri Akışına İlişkin Protokol ile 108 sayılı Sözleşmedeki eksiklik giderilmeye çalışılmıştır. “Bu protokolde, taraf devletler, ülkelerinde uygulanmak üzere kişisel verilerin korunması alanında görevlerini tam bağımsızlıkla yerine getirecek denetleyici makam kurmayı taahhüt etmiştir. Türkiye, bu protokolü 8 Kasım 2001 tarihinde imzalamıştır. Protokol, 5 Mayıs 2016 tarihli 29703 sayılı Resmi Gazete’de yayımlanarak iç hukuka dâhil edilmiştir.” <https://www.kvkk.gov.tr/Icerik/4183/Kisisel-Verilerin-Korunmasi-Alaninda-Uluslararası-ve-Ulusal-Duzenlemeler>, (26.08.2021).

<sup>19</sup> Sözleşmenin tam metni için bkz. <https://rm.coe.int/1680078b37>, (21.08.2021).

<sup>20</sup> Henkoğlu (n 7) 50; Develioğlu (n 7) 10; Çekin, (n 7) 7; Nilgün Başalp, *Kişisel Verilerin Korunması ve Saklanması* (1. Bası Yetkin, Ankara, 2004) 25.

<sup>21</sup> Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Direktifi’nin tam metni için bakınız. <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN>, (21.08.2021).

<sup>22</sup> 108 nolu sözleşme ile kıyaslandığında 95/46/EC daha sıkı bir koruma getirmektedir. Zira direktif kişisel verilerin işlenmesi ile ilgili her türlü işlemi koruması altına alırken 108 nolu sözleşme yalnızca otomatik işleme tabi tutulan kişisel verileri konu alır. Şimşek (n 15) 23.

<sup>23</sup> Küzeci (n 2) 162.

<sup>24</sup> Şimşek (n 15) 42.

Direktifte kişisel veri; “özellikle bir kimlik numarasına veya fiziksel, fizyolojik, zihinsel, ekonomik, kültürel veya toplumsal kimliğine özgü bir veya daha fazla faktöre atıfta bulunularak doğrudan veya dolaylı olarak tanımlanabilen bir gerçek kişiye ilişkin her türlü bilgi” olarak tanımlanmıştır.

Direktifin yürürlüğe girdiği 1995 yılından bu yana teknolojiye meydana gelen gelişmeler, özellikle bulut bilişim, akıllı telefonlar, sosyal medya, e-ticaret uygulamaları ve küreselleşme, kişisel verilerin işlenmesi yöntemlerini ve hızını oldukça değiştirmiş ve bu durumun yarattığı güvenlik açıkları ile kişisel verilerin kolaylıkla ihlal edilebilirliğine ilişkin tehditler AB kurumlarını günün gereksinimlerine uygun, etkili bir reform sürecine yönlendirmiştir.<sup>25</sup> Bu sürecin sonunda, 27 Nisan 2016’da, 2016/679 sayılı Genel Veri Koruma Tüzüğü<sup>26</sup> kabul edilmiştir. Bu Tüzük, 95/46/EC sayılı Veri Koruma Direktifini ilga ederek 25 Mayıs 2018 tarihinde yürürlüğe girmiştir.<sup>27</sup>

Tüzüğün amacı, 95/46/EC sayılı Direktif ile kişisel verilerin korunmasına yönelik belirlenen ilkelerin geliştirilmesi, gelişen teknoloji karşısında bireylerin temel haklarının daha kapsamlı bir şekilde korunması ve AB ülkelerinin veri koruma kurallarının birbirleriyle uyumlu hale getirilmesidir<sup>28</sup>.

95/46/EC sayılı Veri Koruma Direktifinden farklı olarak, 2016/679 sayılı Genel Veri Koruma Tüzüğü, Avrupa Birliği’nin İşleyişi Hakkındaki Antlaşmanın 288’inci maddesi uyarınca<sup>29</sup> genel uygulama alanına sahiptir. Bütünüyle bağlayıcıdır. Yürürlük tarihinden itibaren tüm üye devletlerde doğrudan uygulanır.<sup>30</sup> Üye devletlerin bir düzenleme ile tüzük hükümlerini iç hukuklarına aktarmalarına gerek bulunmamaktadır.<sup>31</sup>

<sup>25</sup> Küzeci (n 2) 193; Nilgün Başalp, ‘Avrupa Birliği Veri Koruması Genel Regülasyonu’nun Temel Yenilikleri’ (2015) 21 Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi 82.

<sup>26</sup> [http://ec.europa.eu/justice/data-protection/reform/files/regulation\\_oj\\_en.pdf](http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf), (21.08.2021).

<sup>27</sup> Çekin (n 7) 7; Develioğlu (n 7)13; Furkan Güven Taştan, *Türk Sözleşme Hukukunda Kişisel Verilerin Korunması* (2. Bası On İki Levha İstanbul 2017) 17.

<sup>28</sup> Paul Voigt, Axel Von dem Bussche, *The EU General Data Protection Regulation (GDPR)* (Springer, 2017) 1.

<sup>29</sup> Avrupa Birliği’nin İşleyişi Hakkındaki Antlaşma:

Madde 288: “Kurumlar, Birliğin yetkilerinin kullanılması için tüzük, direktif, karar, tavsiye ve görüşler kabul eder.

Tüzükler genel uygulama alanına sahiptir. Bütünüyle bağlayıcıdır ve tüm üye devletlerde doğrudan uygulanır.

Direktifler, muhatap alınan her üye devleti, ulaştırılması gerekli sonuçları itibarıyla bağlar, şekil ve yöntem seçimini ise ulusal otoritelere bırakır.

Kararlar bütünüyle bağlayıcıdır. Muhatabı belirtilen bir karar, yalnızca muhatabı için bağlayıcıdır.

Tavsiye ve görüşler bağlayıcı değildir.”

<sup>30</sup> Sanem Baykal, İlke Göçmen, ‘Avrupa Birliği Hukukunun Kaynakları Bakımından Normlar Hiyerarşisi’ Prof. Dr. Erdal Onar’a Armağan, (2013) 325.

<sup>31</sup> Paul B. Lambert, *Understanding the New European Data Protection Rules* (CRC Press New York, 2017) 101; Voigt, Von dem Bussche (n 28) 2.

Düzenlemenin tüzük formunda yapılmasının sebebi, hukuki niteliği itibarıyla doğrudan uygulama niteliğine sahip olmayan 95/46/EC sayılı Direktifinin yürürlükte olduğu dönemde, iç hukuklarında direktifte belirlenen çerçeveye uygun düzenlemeler yapmaları gereken üye devletlerin uygulamalarının ciddi şekilde farklılaşmasıdır.<sup>32</sup>

2016/679 sayılı Genel Veri Koruma Tüzüğünde<sup>33</sup> kişisel veri tanımı, 95/46/EC sayılı Veri Koruma Direktifine benzer şekildedir. Ancak bu tanıma, teknolojik gelişmeler nedeniyle “genetik kimlik”, “konum verileri” ve “çevrimiçi kimlik belirleyiciler” de eklenmiştir.

Ulusal düzeydeki kişisel verilerin korunmasına dair düzenlemelere bakıldığında ise, uzun bir geçmişten söz etmek ne yazık ki mümkün değildir. Kanun düzeyinde ilk kez, 2005 yılında yürürlüğe giren 5237 sayılı Türk Ceza Kanunuyla düzenlenmiştir. Kanunda kişisel verilerin hukuka aykırı şekilde kaydedilmesi (m. 135), hukuka aykırı şekilde verilmesi ya da elde edilmesi (m. 136) ve kanunda belirtilen sürelerin geçmesine rağmen yok edilmemesi (m. 138) hallerinde cezai yaptırımlar öngörülmektedir.

2010 yılında, 5982 sayılı Kanun madde 2 çerçevesinde, Anayasa’nın 20’nci maddesine eklenen üçüncü fıkra ile kişisel verilerin korunması, bir temel hak mertebesine yükseltilmiştir.<sup>34</sup> Anayasa madde 20/3’e göre, “*Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir.*”

Usul ve esasları tespit edecek olan kanun ise, ilgili fıkranın yürürlüğe girmesinden yaklaşık altı yıl sonra çıkarılabilmektedir. 2016 yılında yürürlüğe giren Kişisel Verilerin Korunması Kanunu<sup>35</sup> uluslararası düzenlemelere uygun şekilde kişisel veriyi, “kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi” olarak tanımlamıştır.<sup>36</sup>

<sup>32</sup> Küzeci (n 2) 195.

<sup>33</sup> 2016/679 sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü Madde 4/1, <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN>, (21.08.2021).

<sup>34</sup> Çekin (n 7) 8.

<sup>35</sup> RG. 7.04.2016 – 29677.

<sup>36</sup> Kişisel Verilerin Korunması Kanunu gerekçesi m. 3

“Kişisel veri, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi ifade etmektedir. Bu bağlamda sadece bireyin adı, soyadı, doğum tarihi ve doğum yeri gibi onun kesin teşhisini sağlayan bilgiler değil, aynı zamanda kişinin fiziki, ailevi, ekonomik, sosyal ve sair özelliklerine ilişkin bilgiler de kişisel veridir. Bir kişinin belirli veya belirlenebilir olması, mevcut verilerin herhangi bir şekilde bir gerçek kişiyle ilişkilendirilmesi suretiyle,



Türk Anayasa Mahkemesinin kişisel veriye ilişkin tanımı ise; “adı, soyadı, doğum tarihi ve doğum yeri gibi bireyin sadece kimliğini ortaya koyan bilgiler değil; telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, IP adresi, e-posta adresi, hobiler, tercihler, etkileşimde bulunulan kişiler, grup üyelikleri, aile bilgileri, sağlık bilgileri gibi kişiyi doğrudan veya dolaylı olarak belirlenebilir kılan tüm veriler” şeklindedir.<sup>37</sup>

Tüm bu düzenlemelerden yola çıkarak kişisel verinin üç unsurdan oluştuğu söylenebilir. Kişisel veriden bahsedebilmek için, her şeyden önce bir “veri” bulunmalıdır, bu veri “bir gerçek kişiye ilişkin” olmalı ve “gerçek kişiyi belirli ya da belirlenebilir kılma” niteliğine sahip olmalıdır.<sup>38</sup>

Yukarıda yer verdiğimiz ulusal ve uluslararası düzenlemelerde yapılan tanım/tanımlara uyan ve unsurlarını taşıyan kişisel verilerin bir kısmı nitelikleri gereği, önemi ve hassasiyeti nedeniyle daha fazla korumaya ihtiyaç duyar<sup>39</sup> ve bu nedenle veri koruma düzenlemelerinde özel bir rejime tabi tutulur.<sup>40</sup> Hassas kişisel veriler olarak adlandırılan bu veriler, açıklanması halinde kişinin toplum içinde ayrımcılığa uğramasına neden olabilecek niteliğe sahip, “dini

---

*o kişinin tanımlanabilir hale getirilmesini ifade eder. Yani verilerin; kişinin fiziksel, ekonomik, kültürel, sosyal veya psikolojik kimliğini ifade eden somut bir içerik taşıması veya kimlik, vergi, sigorta numarası gibi herhangi bir kayıtlı ilişkilendirilmesi sonucunda kişinin belirlenmesini sağlayan tüm halleri kapsar. İsim, telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, genetik bilgiler gibi veriler dolaylı da olsa kişiyi belirlenebilir kılabilme özellikleri nedeniyle kişisel verilerdir.”* <https://www.tbmm.gov.tr/sirasayi/donem26/yil01/ss117.pdf>, (21.08.2021).

<sup>37</sup> AyM, E. 2013/122, K. 2014/74, KT. 9.4.2014, RG. 26.7.2014 - 29072; E. 2014/149, K. 2014/151, KT. 2.10.2014, RG. 1.1.2015 - 29223; E. 2013/84, K. 2014/183, KT. 4.12.2014, RG. 13.3.2015 - 29294; E. 2014/74, K. 2014/201, KT. 25.12.2014, RG. 23.5.2015 - 29364; E. 2014/180, K. 2015/30, KT. 19.3.2015, RG. 3.4.2015 - 29315; E. 2015/32, K. 2015/102, KT. 12.11.2015, RG. 02.12.2015 - 29550; E. 2017/180, K. 2018/109, KT. 6/12/2018, RG. 23.1.2019 - 30664; E. 2014/196, K. 2015/103, KT. 12.11.2015, RG. 16.12.2015 - 29564.

<sup>38</sup> Veri Çalışma Grubu’nun 4/2007 Sayılı Kişisel Veri Kavramı Hakkında Görüşü (Opinion 4/2007 On The Concept Of Personal Data, Article 29, Data Protection Working Party), [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf), (21.08.2021).

<sup>39</sup> Doktrinde bazı yazarlar, “her kişisel verinin ayrı ayrı önemli olduğunu; kişisel verileri, korunması daha önemli ya da daha az önemli gibi bir sınıflandırmaya tabi tutmanın yanlış olacağını, başlangıçta tehlike taşımayan bir bilginin üzerinde yapılacak işlemler sonucu önemli hale gelebileceği dolayısıyla her kişisel verinin önem derecesinin somut olayın özelliklerine göre değerlendirilmesi gerektiğini” savunmaktadır. Korkmaz İbrahim, “Kişisel Verilerin Korunması Kanunu Hakkında Bir Değerlendirme”, Türkiye Barolar Birliği Dergisi, 2016, sy.124, ss. 81-152, s. 113, dn. 149; Küzeci (n 2) 244.

<sup>40</sup> Cemil Kaya, ‘Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi’ (2011) 1-2 İÜHF 317.



inanç”, “etnik köken”, “politik görüş”, “sağlık durumu” ve “cinsel hayat” ile ilgili bilgilerdir.<sup>41</sup>

Hassas veri, özel nitelikli veri, “özel kategorili kişisel veriler”, “özel koruma gerektiren veri”, “özel kişisel veri” gibi çeşitli isimlerle<sup>42</sup> tanımlamalar yapılan ve özel koruma mekanizmaları öngörülen bu verilerin ortak paydası kendi bünyelerinde taşıdıkları yüksek risktir.<sup>43</sup> Bu risk faktörü ise, ayrımcılık tehlikesidir. İşte kişisel verilerin bir kısmının hassas veri şeklinde bir sınıflandırmaya tabi tutulmasının ardında bu risk faktörü vardır. Hassas veriler, söz konusu risk faktörünün bertaraf edilmesi amacıyla daha yüksek standartlarla korunmuştur.<sup>44</sup> Diğer kişisel verilere nazaran hassas kişisel verilerin kötü niyetle kullanımı yahut yalnızca üçüncü kişilerle paylaşılmış olması bile birey için ağır ve geri döndürülemez sonuçlara neden olabilecektir. Bu sebeple pek çok ulusal ve uluslararası düzenlemeyle kişisel verilerin bu özel nitelikli grubu ayrı ve daha katı kurallara bağlanmıştır.

108 nolu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesine göre, bireylerin “ırksal kökeni”, “siyasi görüşleri”, “dini ve diğer inançları”, “sağlık bilgileri”, “cinsel hayatı” ve “ceza mahkumiyeti ile alakalı” her türlü veri hassas veri kategorisinde yer alır. 95/46/EC sayılı Veri Koruma Direktifinde ise 108 nolu Sözleşmede sayılan veri türlerine ek olarak “felsefi inanç”, “sendika üyeliği” ve “etnik kökenle bağlantılı veriler” de hassas veri kategorisine dahil edilmiştir.<sup>45</sup> 95/46/EC sayılı Veri Koruma Direktifinin yerini alan 2016/679 sayılı Genel Veri Koruma Tüzüğüyle “biyometrik veriler” ve “genetik veriler” de, teknolojik gelişmelere paralel olarak, bu kategoriye eklenmiştir.<sup>46</sup> 6698 sayılı Kişisel Verilerin Korunması Kanununa bakıldığında ise bireylerin “kılık ve kıyafeti”, “dernek veya vakıf üyeliği” hakkındaki bilgilerin de bu sınıflandırmaya dahil edildiği görülmektedir.<sup>47</sup>

## B. Kişisel Sağlık Verileri Kavramı

Kişisel sağlık verileri, kişisel veri tanımından hareketle “kimliği belirli ya da belirlenebilir gerçek kişiye ilişkin her türlü sağlık bilgisi” olarak tanımlanabilir. 2002 Washington Dünya Hekimler Birliği Genel Kurulunda

<sup>41</sup> Kaya (n 40) 317; Henkoğlu (n 7) 28; Şimşek (n 15) 88; Küzeci (n 2) 243; Lambert (n 31) 112; Başalp (n 20) 43; Aydın Akgül, *Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması* (1. Bası Beta Yayınevi İstanbul 2014) 18.

<sup>42</sup> Kaya (n 40) 318.

<sup>43</sup> Hayrunnisa Özdemir, *Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması* (1. Bası Seçkin Ankara 2009) 126.

<sup>44</sup> Taştan (n 27) 45.

<sup>45</sup> 95/46/EC sayılı Direktif madde 8.

<sup>46</sup> 2016/679 Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR) madde 9.

<sup>47</sup> 6698 sayılı Kişisel Verilerin Korunması Kanunu madde 6.

kabul edilen bildirgeye göre sağlık verileri, “*kişinin bedensel ya da zihinsel sağlığına ilişkin kayıt altına alınmış tüm bilgiler*”dir.<sup>48</sup>

21.06.2019 tarihli ve 30808 sayılı Resmi Gazete’de yayımlanarak yürürlüğe giren, kişisel sağlık verilerine ilişkin özel düzenleme olan Kişisel Sağlık Verileri Hakkında Yönetmelikte<sup>49</sup> kişisel sağlık verisi; “*kimliği belirli ya da belirlenebilir gerçek kişinin fiziksel ve ruhsal sağlığına ilişkin her türlü bilgi ile kişiye sunulan sağlık hizmetiyle ilgili bilgiler*” olarak tanımlanmaktadır.<sup>50</sup>

Sağlık verileri, “tıbbi veri” olarak da adlandırılmaktadır. Bireye ilişkin sağlık verisi, bireyin geçmişi, şimdiki anı ve geleceği, fiziksel veya zihinsel sağlığı ile ilgili olabilir.<sup>51</sup> Hastalığın türü, hastanın kişisel durumu, hastalığın öyküsü, teşhis, tedavi süreci, tahlil ve test sonuçları, hastalığın hasta üzerindeki psikolojik etkileri, hasta dosyası, kullandığı ilaçlar, geçmişteki sağlık kayıtları gibi bireyin sağlığıyla bağlantılı, “*kişiye sunulan sağlık hizmeti ile ilgili*”,<sup>52</sup> fiziki veya elektronik ortamda tutulan her türlü veri bu kapsama girmektedir.

<sup>48</sup> Dünya Hekimler Birliği Sağlıkla İlgili Veritabanlarına İlişkin Bildirge, <http://www.ttb.org.tr/TD/TD109/23.php>, (22.08.2021).

<sup>49</sup> RG. 21.06.2019 – 30808.

<sup>50</sup> Bu yönetmelik kişisel sağlık verilerinin özel olarak düzenlenmesine yönelik ilk girişim değildir. Daha öncesinde bu alana yönelik ilk olarak, Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelik çıkarılmıştır. Bu yönetmelik, Kişisel Verilerin Korunması Kanununun yürürlüğe girmesinden sonra çıkarılan ilk yönetmeliktir. (RG. 20.10.2016-29863) Fakat Kanuna göre, Kişisel Verileri Koruma Kurulu’ndan görüş alınmasının şart iken, Kurulu’nun kontrol ve denetiminden geçirilmeksizin hazırlandığı gerekçesiyle Danıştay kararıyla yürütmesi durdurulmuştur. (D15D, E. 2016/10500, YD. 6.7.2017; D15D, E. 2018/844, YD. 26.6.2018) Yürütmeyi durdurma kararının (D15D, E. 2016/10500, KT. 6.7.2017) hemen ardından Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelikte Değişiklik Yapılmasına Dair Yönetmelik (RG. 24.11.2017-30250) yayınlanarak, yürütmesi durdurulmuş olan yönetmeliğin bazı hükümleri değiştirilmiştir. Oysa düzenlemenin tamamının yürütülmesi durdurulmuşken, bu düzenlemede kısmen değişikliğe yol açacak yeni bir düzenlemenin yapılması, değiştirilmeyen hükümlerin hukuka aykırılık karinesini ortadan kaldırmayacağı gibi, söz konusu değişiklik yapma iradesi de yargı kararını aynen ve gecikmeksizin uygulamaktan kaçınma anlamına gelir. Nitekim Danıştay da bu gerekçelerle, Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelikte Değişiklik Yapılmasına Dair Yönetmeliğin yürütmesini durdurmuştur. (D15D, E.2018/1490, YD. 9.10.2018; D15D, E.2018/251, YD. 9.10.2018) Ardından yukarıda sözünü ettiğimiz “Kişisel Sağlık Verileri Hakkında Yönetmelik” 21.06.2019 tarihli ve 30808 sayılı Resmi Gazete’de yayımlanarak yürürlüğe girmiştir.

<sup>51</sup> Lambert (n 31) 385; Voigt, Von dem Bussche (n 28) 111; Akgül (n 41) 278.

<sup>52</sup> Kişisel Sağlık Verileri Hakkında Yönetmelik, madde 4/1-j, “Kişisel sağlık verisi: Kimliği belirli ya da belirlenebilir gerçek kişinin fiziksel ve ruhsal sağlığına ilişkin her türlü bilgi ile kişiye sunulan sağlık hizmetiyle ilgili bilgileri,”

## C. Kişisel Sağlık Verilerinin İşlenmesi Kavramı

### 1. Genel Hatlarıyla Hassas Kişisel Verilerin İşlenmesi Kavramı

Kişisel verilerin işlenmesi kavramı, “kişisel veriler üzerinde yapılan her türlü işlemin” karşılığıdır.<sup>53</sup>

95/46/EC sayılı Veri Koruma Direktifi 2/b maddesine ve 2016/679 sayılı Genel Veri Koruma Tüzüğü 4/2 maddesine göre, “işleme, otomatik ya da otomatik olmayan araçlarla, kişisel verilerin toplanması, kaydedilmesi, saklanması, organize edilmesi, uyarlanması ya da değiştirilmesi, kullanılması, başkalarına transfer edilmesi, yayılması, kombinasyonu veya ilişkilendirilmesi, bloke edilmesi, silinmesi, yok edilmesi gibi kişisel veriler üzerinde yapılan her türlü faaliyeti” ifade eder.<sup>54</sup> Kişisel verilerin bilgisayar gibi otomasyon sistemleri kullanılarak işlenmesi otomatik işleme, otomasyon sistemleri kullanılmadan belli bir düzen ve sıraya dizilerek erişimin organize edilmesi suretiyle işlenmesi ise otomatik olmayan araçlarla işleme anlamına gelir.<sup>55</sup>

6698 sayılı Kişisel Verilerin Korunması Kanununun “Tanımlar” başlıklı 3’üncü maddesinin 1-e bendine göre kişisel verilerin işlenmesi, “*kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi*” ifade eder.

Anlaşılabacağı üzere kişisel verilerin işlenmesi; “*verilerin elde edilmesi ile başlayan kaydedilme, incelenme, düzenlenme, birleştirilme, açıklanma, birleştirilme gibi bu veri kullanılarak ya da bu veri üzerinde yapılan her türlü işlemi ve bir süreci*” ifade eder.<sup>56</sup>

Kişisel verilerin işlenmesi konuya ilişkin her ulusal ve uluslararası düzenlemede bazı şartlara tabi tutulmuş, belli kurallara bağlanmıştır. Ancak kişisel sağlık verilerinin de içinde bulunduğu hassas kişisel veriler özellikli bir veri kategorisi olduğu için bu türden verilerin işlenmesi kural olarak yasaktır.<sup>57</sup> Bir başka deyişle hassas verilerin işlenmesi kesin işlem yasağına tabidir.<sup>58</sup> Bunlar ancak kanuni temelle ya da ilgilinin rızası ile işlenebilir.<sup>59</sup>

<sup>53</sup> Stewart Room, *Data Protection and Compliance in Context* (British Computer Society, United Kingdom 2006) 41.

<sup>54</sup> 95/46/EC sayılı Direktif madde 4/2.

<sup>55</sup> Başalp (n 20) 33.

<sup>56</sup> Kaya (n 40) 317.

<sup>57</sup> Kaya (n 40) 323.

<sup>58</sup> Özdemir (n 43) 127

<sup>59</sup> Şimşek (n 15) 86.

108 nolu Sözleşmenin özel veri kategorileri başlıklı 6'ncı maddesine göre *"iç hukukta uygun güvenceler sağlanmadıkça bu türden veriler otomatik işleme tabi tutulamaz."* Hassas verilerin işlenmesi istisnai olduğu için işlenebileceği hallerin ayrıca ve açıkça belirtilmesi gerekmektedir. 95/46/EC sayılı Veri Koruma Direktifi madde 8/2 ve 2016/679 sayılı Genel Veri Koruma Tüzüğü madde 9/2'de bu istisnai haller düzenlenmiştir.

1982 Anayasasının kişisel verilerin korunması hakkının düzenlendiği, özel hayatın gizliliği başlığını taşıyan 20'nci maddesinin 3'üncü fıkrasına göre, *"kişisel veriler ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla"* işlenebilir. Anlaşılabacağı üzere Anayasa'da hassas verilerin işlenmesine ilişkin ayrı bir düzenlenme yapılmamış bu görev kanun koyucuya bırakılmıştır.

6698 sayılı Kişisel Verilerin Korunması Kanununda ise, "özel nitelikli kişisel verilerin işlenme şartları" başlıklı 6'ncı maddede hassas verilerin işlenme şartları düzenlenmiştir. Maddenin ikinci fıkrasında genel kural olarak, özel nitelikli (hassas) kişisel verilerin, ilgilinin açık rızası olmaksızın işlenemeyeceği belirtilmiştir. Aynı maddenin 3'üncü fıkrasında ise genel kurala istisna getirilmiş, hassas verilerin açık rıza aranmaksızın işlenebileceği haller düzenlenmiştir. Burada ikili bir ayrıma gidilmiş, sağlık ve cinsel hayata ilişkin veriler için ayrı, sağlık ve cinsel hayata ilişkin veriler haricindeki hassas veriler için ayrı işlenme şartları getirilmiştir.

Düzenlemeye göre, bireyin sağlık ve cinsel hayat dışındaki hassas kişisel verileri yani ırk, etnik köken, siyasi görüş, felsefi inanç, din, mezhep veya diğer inançlar, kılık ve kıyafet, dernek, vakıf ya da sendika üyeliği, ceza mahkûmiyeti ve güvenlik tedbirleri ile ilgili veriler ile biyometrik ve genetik veriler kanunlarda öngörülen hallerde ilgili kişinin açık rızası aranmaksızın işlenebilecektir. Sağlık ve cinsel hayata ilişkin verilerin ise, sadece *"kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla ve yalnızca sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebileceği"* belirtilmiştir.

Kişisel sağlık verileri ve cinsel hayata ilişkin veriler bağlamında, Kişisel Verilerin Korunması Kanununda hassas kişisel verilerin istisnai olarak açık rıza aranmaksızın işlenebileceği hallerin düzenlendiği madde 6/3'ün ayrıca değerlendirilmesi gerekir.

Hassas kişisel veri kategorisi içinde, açıklandığı zaman ayrımcılığa ve kötü muameleye maruz kalma ihtimalinin diğer hassas verilere nazaran daha yüksek olduğu, hassas veriler arasında belki de en güçlü korumaya ihtiyaç duyan bu tür verilerin "kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile

finansmanının planlanması ve yönetimi” gibi oldukça geniş tutulan ve daha da geniş yorumlanabilmeye elverişli amaçlar çerçevesinde, yine sınırları oldukça geniş ve yoruma açık bir kişi grubu tarafından işlenebilmesi hükmün istisnai olma niteliği ile bağdaşmamaktadır. Söz konusu hüküm düzenlenme amacının aksine verilerin güvenliğini ve koruma mekanizmasını zayıflattığı gibi, hassas kişisel verileri daha güçlü bir güvence sistemine bağlamayı amaçlayan Kanun’un genel mantığına da ters düşmektedir.

Belirtmemiz gerekir ki, bu fıkra Anayasa Mahkemesinin önüne gitmiş fakat Mahkeme düzenlemenin Anayasa aykırı olmadığına hükmetmiştir.<sup>60</sup>

Bu başlık altında son olarak kişisel sağlık verilerinin işlenmesi sürecine dahil olan aktörlere, veri sorumlusu ve veri işleyen kavramlarına değinmek gerekmektedir.

Gerek 95/46/EC sayılı Veri Koruma Direktifinde gerekse 2016/679 sayılı Genel Veri Koruma Tüzüğünde “veri kontrolörü (*data controller*)” terimi, “kişisel verilerin işlenmesinin amaçlarını ve araçlarını tek başına veya başkalarıyla birlikte belirleyen gerçek veya tüzel kişi, kamu otoritesi, kamu kurumu ya da diğer bir yapı”nın karşılığıdır. Kişisel Verilerin Korunması Kanununda ise aynı veri işleme aktörleri için “veri sorumlusu” kavramı kullanılmıştır. Kanuna göre veri sorumlusu, “*kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi*” olarak tanımlanmıştır (m. 3/1). Veri işleyen (işleyici)<sup>61</sup> ise, “*veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişiyi ifade eder*” (m. 3/ğ).

Herhangi bir gerçek veya tüzel kişi aynı zamanda hem veri sorumlusu, hem de veri işleyen olabilir.<sup>62</sup> Veri işleyen, teknik olarak veri işleme faaliyetiyle ilgilenirken veri sorumlusu verilerin işlenmesine ilişkin kararların alınması, işleme faaliyetinin amacı ve yöntemini belirleme yetkisine sahiptir.<sup>63</sup> Veri sorumlusu, yasal düzenlemelerde yer alan kişisel verilerin işlenmesine dair bütün kuralların uygulayıcısı, yükümlülüklerin muhatabı ve meydana gelen zararların sorumlusudur.<sup>64</sup>

<sup>60</sup> AyM, E. 2016/125, K. 2017/143, KT. 28.9.2017, R.G. 23.1.2018 – 30310.

<sup>61</sup> 95/46/EC sayılı Veri Koruma Direktifinde ve 2016/679 sayılı Genel Veri Koruma Tüzüğünde işleyici (*processor*) kavramı kullanılmaktadır. Her iki düzenlemede de işleyici, veri sorumlusu (*data controller*) adına kişisel verileri işleyen gerçek veya tüzel kişi, kamu otoritesi, ajans veya diğer bir yapı olarak tanımlanmaktadır.

<sup>62</sup> 6698 s. Kişisel Verilerin Korunması Kanunu gerekçesi madde 3, <https://www.tbmm.gov.tr/sirasayi/donem26/yil01/ss117.pdf>, (23.08.2021)

<sup>63</sup> <https://www.kvkk.gov.tr/Icerik/4195/Veri-Sorumlusu-ve-Veri-Isleyen>, (23.08.2021).

<sup>64</sup> Tekin Memiş, ‘Veri Sorumlusu ve Veri İşleyen Arasındaki İlişkiler ve Sorumluluk Düzeni’ (2017) 6 Beykent Üniversitesi Hukuk Fakültesi Dergisi 11.

## 2. Kişisel Sağlık Verilerinin İşlenmesi

### a. Genel Hatlarıyla Kişisel Sağlık Verilerinin İşlenmesi

10.7.2018 tarihinde Resmi Gazetede yayınlanarak yürürlüğe giren 1 sayılı Cumhurbaşkanlığı Kararnamesinin<sup>65</sup> Sağlık Bakanlığını düzenleyen on ikinci bölümünün “bilgi toplama, işleme ve paylaşma yetkisi” başlığını taşıyan 378’inci maddesinde, bir önceki başlık altında sözünü ettiğimiz, Kişisel Verilerinin Korunması Kanunu’nda kişisel sağlık verilerinin işlenmesi yasağının istisnasını düzenleyen ilgili hükmün (belirsiz) sınırları dahilinde ve ona paralel bir hüküm tesis edilmiştir.

Kararnamenin 378’inci maddesinin 1’inci fıkrasında “sağlık hizmeti almak üzere kamu veya özel sağlık kuruluşları ile sağlık mesleği mensuplarına müracaat edenlerin, sağlık hizmetinin gereği olarak vermek zorunda oldukları veya kendilerine verilen hizmete ilişkin kişisel verilerinin işlenebileceği” ifade edilmiştir. Aynı maddenin 2’nci fıkrasında ise, “sağlık hizmetinin verilmesi, kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi ile sağlık hizmetlerinin planlanması ve maliyetlerin hesaplanması amacıyla Bakanlığın, birinci fıkra kapsamında elde edilen verileri alarak işleyebileceği ve bu verilerin Kişisel Verilerin Korunması Kanununda öngörülen şartlar dışında aktarılamayacağı” hüküm altına alınmıştır.

Hükümden anlaşılabacağı üzere Sağlık Bakanlığının, “sağlık kamu hizmetinin ifası vesilesiyle elde ettiği tüm sağlık verilerini yine sağlık hizmetinin gerekleri için, kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi ile sağlık hizmetlerinin planlanması ve maliyetlerin hesaplanması amacıyla işleme” yetkisi bulunmaktadır.

Esasında burada söz konusu düzenlemenin geçmişinden de söz etmek gerekmektedir. Kişisel sağlık verilerinin toplanması, işlenmesi ve paylaşılması yetkisi ilk olarak 663 sayılı Sağlık Bakanlığı ve Bağlı Kuruluşlarının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararnamenin<sup>66</sup> 47’nci maddesiyle düzenlenmiş idi. Bu madde ile Sağlık Bakanlığında ülke çapında her türlü kişisel sağlık verisini toplama ve işleme konusunda iki kez yetki verilmiş, fakat Anayasa Mahkemesi bu yetkiyi düzenleyen hükümleri Anayasaya aykırı oldukları gerekçesiyle iptal etmiştir. Üçüncü kez yapılan düzenleme ise, 2.7.2018 tarih ve 703 sayılı KHK ile yürürlükten kaldırılmıştır. Düzenlemenin yürürlükten kaldırılmadan önceki son şekli, 10.7.2018 tarihinde yürürlüğe giren Cumhurbaşkanlığı Kararnamesinde aynen korunmuştur.

<sup>65</sup> RG. 10.7.2018 – 30474.

<sup>66</sup> RG. 2.11.2011 – 28103.



Düzenlemenin ilk halinde<sup>67</sup> Sağlık Bakanlığı kişisel sağlık verilerini “her türlü vasıtayla” toplamaya, işlemeye ve paylaşmaya yetkili kılınmıştı. Anayasa Mahkemesi ise bu yetkiyi düzenleyen 47’nci maddenin ilk 3 fıkrasını, Anayasa’nın 20’nci maddesinde düzenlenen ve Kişinin Hakları ve Ödevleri başlıklı ikinci bölümünde yer alan özel hayatın gizliliği ve kişisel verilerin korunması hakkına ilişkin olarak kanun hükmünde kararname ile düzenleme yapılmasını, Anayasa mülga m. 91/1’de yer alan “sıkıyönetim ve olağanüstü haller dışında, Anayasanın ikinci kısmının birinci ve ikinci bölümlerinde yer alan temel hak ve özgürlüklerin kanun hükmünde kararnamelerle düzenlenemeyeceği” kuralına aykırı bularak iptal etmiştir.<sup>68</sup>

İptal kararı üzerine 47’nci madde yeniden düzenlenmiş<sup>69</sup> ve kanun koyucu aynı hükmü 6495 sayılı Kanun<sup>70</sup> ile yine 663 sayılı KHK’nın 47’nci maddesine eklemiştir. Söz konusu 47’nci madde KHK içinde yer almasına rağmen, 6495 sayılı Kanun ile değiştirildiğinden artık yasa niteliğinde bir metin haline

<sup>67</sup> 663 sayılı KHK,

“Bilgi toplama, işleme ve paylaşma yetkisi

Madde 47- (1) Bakanlık ve bağlı kuruluşları, mevzuatla kendilerine verilen görevleri, e-devlet uygulamalarına uygun olarak daha etkin ve hızlı biçimde yerine getirebilmek için, bütün kamu ve özel sağlık kurum ve kuruluşlarından; sağlık hizmeti alanların, aldıkları sağlık hizmetinin gereği olarak ilgili sağlık kurum ve kuruluşuna vermek zorunda oldukları kişisel bilgileri ve bu kimselere verilen hizmete ilişkin bilgileri her türlü vasıtayla toplamaya, işlemeye ve paylaşmaya yetkilidir.

(2) Bakanlık ve bağlı kuruluşları işlediği kişisel sağlık verilerini ilgili üçüncü kişiler ve kamu kurum ve kuruluşları ile ancak bu kişi ve kurumların bu verilere erişebileceği hususunda kanunen yetkili olması halinde ve görevlerini yapmalarına yetecek derecede paylaşabilir.

(3) Bakanlık ve bağlı kuruluşları, mevzuatla kendilerine verilen görevleri yerine getirebilmek için gereken bilgileri, kamu ve özel ilgili bütün kişi ve kuruluşlardan istemeye yetkilidir. İlgili kişi ve kuruluşlar istenilen bilgileri vermekle yükümlüdür.”

<sup>68</sup> AyM, E. 2011/150, K. 2013/30, KT. 14.02.2013, RG. 25.06.2013 – 28688.

<sup>69</sup> “Bilgi toplama, işleme ve paylaşma yetkisi

Madde 47- (1) (Değişik: 12/7/2013-6495/73 md.) Bakanlık ve bağlı kuruluşları, mevzuatla kendilerine verilen görevleri, e-devlet uygulamalarına uygun olarak daha etkin ve daha hızlı biçimde yerine getirebilmek için, bütün kamu ve özel sağlık kurum ve kuruluşlarından; sağlık hizmeti alanların, aldıkları sağlık hizmetinin gereği olarak ilgili sağlık kurum ve kuruluşuna vermek zorunda oldukları kişisel bilgileri ve bu kimselere verilen hizmete ilişkin bilgileri her türlü vasıtayla toplamaya, işlemeye ve paylaşmaya yetkilidir.

(2) (Değişik: 12/7/2013-6495/73 md.) Bakanlık ve bağlı kuruluşları işlediği kişisel sağlık verilerini ilgili üçüncü kişiler ve kamu kurum ve kuruluşları ile ancak bu kişi ve kurumların bu verilere erişebileceği hususunda kanunen yetkili olması hâlinde görevlerini yapmalarına yetecek derecede paylaşabilir.

(3) (Değişik: 12/7/2013-6495/73 md.) Bakanlık ve bağlı kuruluşları, mevzuatla kendilerine verilen görevleri yerine getirebilmek için gereken bilgileri, kamu ve özel ilgili bütün kişi ve kuruluşlardan istemeye yetkilidir. İlgili kişi ve kuruluşlar istenilen bilgileri vermekle yükümlüdür.”

<sup>70</sup> RG. 2.02.2013 – 28726.

gelmiştir. Dolayısıyla Anayasa Mahkemesinin bu maddenin ilk üç fıkrasını iptal etme gerekçesi olan “kanunla düzenlenme” şartı bu şekilde sağlanmıştır. Düzenleme tekrar Anayasa Mahkemesinin önüne getirilmiştir. Anayasa Mahkemesi bu kez, anılan düzenlemenin ölçülülük ilkesine aykırı olduğunu saptamış ve düzenlemeyi tekrar iptal etmiştir.<sup>71</sup>

Mahkemeye göre, “*kişisel bilgilerin ‘her türlü vasıta’yla toplanmasına, işlenmesine ve paylaşılmasına izin verilmesi, sınırlamayı, öngörülme amacının ötesinde kişisel bilgilerin gizliliğinin keyfi şekilde ihlal edilmesi sonucunu doğurabilecek bir araca dönüştürmektedir. Bu ise sınırlama aracıyla sınırlama amacı arasında bulunması gereken makul dengeyi bozmakta, özel hayatın ve kişisel verilerin korunmasını isteme haklarına kuralda belirtilen sınırlama amacı dışında ölçüsüz bir şekilde müdahale edilebilmesine imkân tanımaktadır.*”

Anayasa Mahkemesinin 2014 yılında verdiği bu ikinci iptal kararından sonra 663 s. KHK’nın 47’nci maddesi yeniden formüle edilmiş<sup>72</sup> ve “her türlü vasıta ile işleme, toplama ve paylaşma” yetkisine yer verilmemiştir. Öte yandan 1’inci fıkra da önceki düzenlemeden farklı olarak sadece sağlık kurum ve kuruluşlarına değil, sağlık mesleği mensuplarına müracaat edenlerin verilerinin de işlenmesi düzenlenmiştir.

47’nci maddenin son hali için de Anayasa Mahkemesine gidilmiş fakat Mahkeme, bu düzenlemenin Anayasaya aykırı olmadığına hükmetmiştir.<sup>73</sup> Bu düzenleme de 703 sayılı KHK ile yürürlükten kaldırılmış fakat aynı metin 1 sayılı Cumhurbaşkanlığı Kararnamesinin 378’inci maddesinde aynen korunmuştur.

Her ne kadar Anayasa Mahkemesi kişisel sağlık verilerinin işlenmesine ilişkin bu metni, 663 s. KHK’da yer aldığı dönemde Anayasaya aykırı bulmamış olsa da, 6698 sayılı Kişisel Verilerin Korunması Kanunu m. 6/3’te yer alan sağlık ve cinsel hayata ilişkin verilerin açık rıza aranmaksızın işlenebilmesini

<sup>71</sup> AyM, E. 2013/114, K. 2014/184, KT. 4.12.2014, RG. 16.07.2015 - 29418.

<sup>72</sup> 663 s. KHK,

“*Bilgi toplama, işleme ve paylaşma yetkisi*

*Madde 47- (Değişik: 24/3/2016-6698/30 md.) (1) Sağlık hizmeti almak üzere, kamu veya özel sağlık kuruluşları ile sağlık mesleği mensuplarına müracaat edenlerin, sağlık hizmetinin gereği olarak vermek zorunda oldukları veya kendilerine verilen hizmete ilişkin kişisel verileri işlenebilir.*

*(2) Sağlık hizmetinin verilmesi, kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi ile sağlık hizmetlerinin planlanması ve maliyetlerin hesaplanması amacıyla Bakanlık, birinci fıkra kapsamında elde edilen verileri alarak işleyebilir. Bu veriler, Kişisel Verilerin Korunması Kanununda öngörülen şartlar dışında aktarılamaz.*

*(3) Bakanlık, ikinci fıkra gereğince toplanan ve işlenen kişisel verilere, ilgili kişilerin kendilerinin veya yetki verdikleri üçüncü kişilerin erişimlerini sağlayacak bir sistem kurar. (...)*”

<sup>73</sup> AyM, E. 2016/125, K.2017/143, 23.01.2019, RG. 23.01.2018 – 30310.

meşru kılan amaçlara yönelik yaptığımız eleştiriler bu düzenleme için de geçerlidir. Kişisel sağlık verilerinin, kapsamı ve sınırları genişletilmeye müsait amaçlar çerçevesinde yine sınırlarının belirli olduğunu söylemenin güç olduğu bir kişi grubu tarafından işlenmesi veri koruma hukukunun mantığına aykırıdır. Zira veri koruma hukukunda, hassas verilerin işlenmesinin diğer verilere kıyasla daha katı bir denetime tabi tutulması anlamına gelen hassaslık ilkesi ve veri toplama ve işlemenin bağlı olduğu amaç/amaçları gerçekleştirmek için zorunlu olan miktarla sınırlı olacak şekilde veri toplanması gerekliliğini ifade eden minimumluk ilkesine riayet edilmesi gerekir.<sup>74</sup>

### **b. Kişisel Sağlık Verilerinin Merkezi Veri Kayıt Sistemi Kullanılarak İşlenmesi**

Sağlık Bakanlığının, sağlık hizmeti dolayısıyla elde ettiği kişisel verileri yine sağlık hizmetinin gerekleri doğrultusunda işleme yetkisinin bir uzantısı olarak, ülke çapında elde ettiği kişisel verilerin yer aldığı, sağlık hizmetlerinin daha hızlı ve etkin şekilde yürütülebilmesi amacıyla yönelik bir bilişim sistemi kurma yetkisi vardır. Bu yetki 3359 sayılı Sağlık Hizmetleri Temel Kanunu<sup>75</sup> madde 3/f de düzenlenmiştir. Fıkraya göre; *“Herkesin sağlık durumunun takip edilebilmesi ve sağlık hizmetlerinin daha etkin ve hızlı şekilde yürütülmesi maksadıyla, Sağlık Bakanlığı ve bağlı kuruluşlarınca gerekli kayıt ve bildirim sistemi kurulur. Bu sistem, e-Devlet uygulamalarına uygun olarak elektronik ortamda da oluşturulabilir. Bu amaçla, Sağlık Bakanlığınca, bağlı kuruluşları da kapsayacak şekilde ülke çapında bilişim sistemi kurulabilir.”*

Benzer bir düzenleme 1 sayılı Cumhurbaşkanlığı Kararnamesinde de yer almaktadır. Kararname m. 378/3’e göre Sağlık Bakanlığı, “sağlık hizmetinin ifası sebebiyle topladığı ve işlediği kişisel verilere, ilgili kişilerin kendilerinin veya yetki verdikleri üçüncü kişilerin erişimlerini sağlayacak bir sistem kurmaya” yetkilidir.

Görüldüğü gibi bu düzenlemeler sağlık verilerinin Sağlık Bakanlığı bünyesinde merkezi bir sistemde tutulmasına ilişkindir. Sağlık.net, e-nabız, merkezi hekim randevu sistemi (MHRS) bunun uygulama örnekleridir. Bu türden bir çalışmanın, bireylerin kişisel sağlık verilerinin toplanması, kaydedilmesi ve analiz edilmesinin, sağlık kamu hizmetinin etkin ve verimli şekilde sunulabilmesi için gerekliliği, anlaşılabilir bir gerekçedir. Fakat öncelikle hangi kayıtların toplanacağı, toplanan kayıtlardan hangisi veya hangilerine, kim/kimler tarafından erişilebileceği ve bu kayıtlara erişim sınırlarının ne olacağı, ne kadar süre saklanacağı, silinmesine ve anonimleştirilmesine ilişkin nasıl bir prosedürün uygulanacağı, sistemin güvenliğine dair alınan koruma önlemlerinin ne olduğu sorularının kuşkuya yer bırakmayacak açıklıkta

<sup>74</sup> Kaya (n 40) 324.

<sup>75</sup> RG. 15.5.1987 – 19461.

cevaplanması gerekir. Zira bireyin hak ve özgürlükleri korunmadan, yeterince önlem alınmadan kamu yararına hareket etmek, kamu yararına yönelik bir faaliyeti değil aksine temel hak ve özgürlük ihlalini oluşturur. Kişisel verilerin korunması, bilgi ve veri güvenliğine ilişkin alınacak hukuki önlemler ve düzenlemeler yoluyla sağlanabilir.<sup>76</sup> Ancak ne kanuni düzenlemeler ne de Kişisel Sağlık Verileri Hakkında Yönetmelikteki veri güvenliği ve kişisel sağlık verilerine erişim ile ilgili detaylandırılmış hükümler söz konusu kaygıları ortadan kaldırmaya yetmektedir.

Dolayısıyla sağlık verilerinin tümünün merkezi bir veri tabanında tutulmasının siber saldırı riskine karşı başlı başına bir güvenlik açığı olduğu itirazı,<sup>77</sup> aşırıya kaçan bir yorum olmayacaktır. Zira kişisel sağlık kayıtlarının tek bir merkezde tutulması, merkezi olarak toplanıp işlenmesi, bu bilgilerin, bu verileri işlemeye yetkisi olmayanların eline geçmesi ve dolayısıyla mahremiyetin ihlal edilmesi riskini artırır. Kişisel verilerin işlenmesine merkezi veri kayıt sistemleriyle devam edilse dahi mümkün olduğunca anonimleştirilerek ve belli bir süre ile sınırlı olarak tutulması<sup>78</sup> hem kişisel sağlık verilerinin korunmasına hem de kamu yararına hizmet eden bir yaklaşım olacaktır.

### c. Kişisel Sağlık Verilerinin Biyometrik Yöntemler Kullanılarak İşlenmesi

Biyometrik yöntemler, bireyin tespit edilmesini veya doğrulanmasını sağlayan, kendisine ait parmak izi, ses, yüz, retina, iris, avuç içi, el geometrisi, imza, konuşma, yürüyüş tanıma, tuşlama, DNA bilgisi gibi fiziksel veya davranışsal, otomatik kimlik denetleme teknikleridir.<sup>79</sup>

Biyometrik veriler ise, 2016/679 sayılı Genel Veri Koruma Tüzüğü m. 4/14'te “yüz görüntüleri veya daktiloskopik veriler gibi bireyin özgün bir şekilde teşhis edilmesini sağlayan veya teyit eden fiziksel, fizyolojik veya davranışsal özelliklerine ilişkin olarak spesifik teknik işlemlerden kaynaklanan kişisel veriler” olarak tanımlanmıştır.<sup>80</sup> Avrupa İnsan Hakları Mahkemesi de “S. ve Marper / Birleşik Krallık” davasında; resmi otoritelerin muhafaza ettikleri, parmak izi, DNA, kan ve hücre örneklerinin kişisel veri kapsamında olduğunu kabul etmiştir.<sup>81</sup>

<sup>76</sup> Henkoğlu (n 7) 20.

<sup>77</sup> Küzeci (n 2) 477.

<sup>78</sup> Küzeci (n 2) 477.

<sup>79</sup> Aydın Akgül, ‘Kişisel Verilerin Korunması Bağlamında Biyometrik Yöntemlerin Kullanımı ve Danıştay Yaklaşımı’ (2015) 118 TBB Dergisi, 202; Cüneyd Er, *Biyometrik Yöntemler ve Özel Hayatın Gizliliği Hakkı: Parmak İzi, Göz ve DNA Tarama Gibi Teknolojik Kimlik Denetleme Usullerinin Hukuki Statüsü* (1. Bası Yetkin Yayınları Ankara 2007) 21.

<sup>80</sup> Lambert (n 31) 116; Voigt, Von dem Bussche (n 28) 111-112.

<sup>81</sup> S. ve Marper / Birleşik Krallık, Başvuru No: 30562/04 ve 30566/04, KT. 4.12.2008.

6698 sayılı Kişisel Verilerin Korunması Kanunu m. 6/1’de özel nitelikli (hassas) veri kategorisinin içinde sağlık verileri ile biyometrik veriler ayrı ayrı sayılmış olsa da, biyometrik yöntemlerle elde edilen biyometrik veriler, bireyin sağlığına ilişkin olabilir. Bu durumda biyometrik yöntemler kullanılarak elde edilmiş kişisel sağlık verisi haline gelir ve dolayısıyla biyometrik yöntemler kullanılarak elde edilen kişisel sağlık verilerinin işlenmesi de m. 6/3’teki sınırlamaya tabi olur.

Kişisel Verilerin Korunması Kanunu yürürlüğe girmeden önce, 2012 yılında, 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanununun m. 67/3’e eklenen<sup>82</sup> “biyometrik yöntemlerle kimlik doğrulaması yapılması ve/veya” ibaresi ile “*genel sağlık sigortalısı ve bakmakla yükümlü olduğu kişilerin sağlık hizmetlerinden ve diğer haklardan yararlanabilmeleri için sağlık hizmet sunucularına başvurduklarında acil haller hariç olmak üzere (acil hallerde ise acil halin sona ermesinden sonra); biyometrik yöntemlerle kimlik doğrulamasının yapılması ve/veya nüfus cüzdanı, sürücü belgesi, evlenme cüzdanı, pasaport veya Kurum tarafından verilen resimli sağlık kartı belgelerinden birinin gösterilmesi*”<sup>83</sup> zorunluluğu getirilmiştir.

Bu düzenleme yürürlüğe girdikten sonra Danıştay, genel sağlık sigortalısı ve bakmakla yükümlü olduğu kişilerin sağlık hizmetlerinden ve diğer haklardan yararlanabilmeleri için sağlık hizmet sunucularına başvurduklarında biyometrik yöntemlerle kimlik doğrulaması yapılmasının Avrupa İnsan Hakları Sözleşmesine ve Anayasaya aykırı olduğu gerekçesiyle Anayasa Mahkemesine itiraz yoluna başvurmuştur. Danıştay, anılan düzenlemede, “*biyometrik yöntemlerle yapılacak kimlik doğrulaması sonucu elde edilecek kişisel verilen toplanması ve işlenmesinin kapsamının, bu verilerin korunmasına ilişkin usul ve esasların belirtilmediğini*” vurgulamıştır.<sup>84</sup> Fakat Anayasa Mahkemesi, dava konusu düzenleme ile getirilen sistemin kamu kuruluşlarına yönelik yolsuzluklara karşı etkili ve güvenli olduğunu saptamış ve iptal istemini reddetmiştir.<sup>85</sup> Oysaki henüz Kişisel Verilerin Korunması Kanunu yürürlüğe girmeden önce yapılan bu düzenlemede gerçekten de sağlık verilerinin işlenmesine ilişkin bir hüküm yer almakta olmasına karşın verilerin korunmasına ilişkin bir güvence, kişisel sağlık verilerinin kötüye kullanılmasını önleyici, etkili kontrol mekanizmaları, toplanan verilerin ne kadar süreyle saklanacağına ilişkin bir düzenleme bulunmamaktadır.

2016 yılında, kişisel verilerin korunmasına ilişkin genel kanun niteliğinde olan Kişisel Verilerin Korunması Kanununun yürürlüğe girmesiyle, anılan kanun maddesine, “biyometrik yöntemlerle kimlik doğrulaması yapılması

<sup>82</sup> 01.03.2012 tarih ve 6283 sayılı Kanun madde 1.

<sup>83</sup> 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu m. 67/3.

<sup>84</sup> AyM, E. 2014/180, K. 2015/30, KT. 19.3.2015, RG. 3.4.2015-29315.

<sup>85</sup> AyM, E. 2014/180, K. 2015/30, KT. 19.3.2015, RG. 3.4.2015-29315.

ve/veya” ibaresi eklemesinin kişisel verilerin korunması hakkına aykırılığı hususunda yarattığı tereddütler giderilmiş gibi görünse de esasında aynı hala aynı eleştiriler geçerlidir. Kişisel Verilerin Korunması Kanunu m. 6/3’te yer alan “... Sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî 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 işlenebilir.” hükmüne dair yukarıdaki itirazlarımız unutulmamalıdır.

Öte yandan, Sosyal Sigortalar ve Genel Sağlık Sigortası Kanununun m. 67/3’e eklenen ifade ile birlikte kimlik doğrulaması için kullanılacak yöntemler “ve/veya” bağlacı ile belirlenmiş olmasına karşın, bir başka ifadeyle biyometrik yöntemlerle kimlik doğrulaması yapılması kanuna göre alternatifi olmayan, kullanılabilecek tek yöntem olmamasına karşın, uygulamada Sosyal Güvenlik Kurumu Sağlık Uygulama Tebliği ile biyometrik verilerin paylaşımı zorunlu tutulmuştur.<sup>86</sup>

## II. İDARENİN KİŞİSEL SAĞLIK VERİLERİNİ KORUMA YÜKÜMLÜLÜĞÜ

### A. Kişisel Sağlık Verilerinin Korunması Hakkı

Kişisel verilerin korunması hakkı temel bir insan hakkıdır.<sup>87</sup> Kişisel verilerin korunması hakkı, veri sahibinin verileri üzerindeki hakimiyetini ifade eden<sup>88</sup> anayasal bir haktır. Anayasanın 20’nci maddesinde özel hayatın gizliliği başlığı altında düzenlenmiştir. Anayasadaki düzenlenme şeklinden hareketle kişisel verilerin korunması hakkını özel yaşama saygı hakkı içinde, onun bir uzantısı olarak değerlendirmek mümkünse de, tarihsel süreç içinde gün geçtikçe, teknolojinin ve bilişim sistemlerinin gelişmesine de paralel olarak kişisel verilerin korunması hakkının özel yaşama saygı hakkının özellikli bir türü ve kendine özgü bazı gereklilikleri olan ayrı bir hak alanı olarak görülmeye ve bu şekilde değerlendirilmeye başlanmıştır.<sup>89</sup>

<sup>86</sup> RG. 24.03.2013 – 28597,

Sosyal Güvenlik Kurumu Sağlık Uygulama Tebliği,

“1.6 - Kimlik tespiti: (1)Sağlık kurum ve kuruluşlarınca, kişilerin müracaatı aşamasında, acil hallerde ise acil halin sona ermesinden sonra, nüfus cüzdanı, sürücü belgesi, evlenme cüzdanı, pasaport veya verilmiş ise Kurum sağlık kartı belgelerinden biri ile kimlik tespiti ve biyometrik yöntemlerle kimlik doğrulaması yapılması zorunludur.”

<sup>87</sup> Kişisel verilerin korunması günümüzde, 2016/679 Genel Veri Koruma Tüzüğü, Avrupa Birliğinin 2000 tarihli Temel Haklar Şartı, Lizbon Anlaşması ve Veri Koruma Sözleşmesinde bireyler için temel bir yasal hak olarak kabul edilmektedir. Lambert (n 31) 101.

<sup>88</sup> Dülger (n 6) 74.

<sup>89</sup> Küzeci (n 2) 69.



Kişisel verilerin korunması hakkı bireylerin maddi ve manevi varlıklarının korunmasına hizmet eder.<sup>90</sup> Bireyin, kendisine ait kişisel veriler üzerindeki tasarruf yetkisi insan onurunun ve bununla bağlantılı olarak kişilik hakkının bir gereksinimidir.<sup>91</sup> İnternetteki hareketliliğinden bina girişlerine kadar her türlü hareketi, davranışı ve tercihi çeşitli kontrol biçimleriyle gözetim altında tutulan,<sup>92</sup> bilgileri kaydedilen ve işlenen bireylerin bu süreçten haberdar edilmemesi ve /veya müdahale etme hakkına sahip olmaması, kendi özgür iradesine göre şekillendirebileceği bir özel hayatlarının kalmamasına<sup>93</sup> ve bireyselliklerini koruma olanağının ortadan kalkmasına yol açacaktır. Sürekli kendisi hakkında bilgilerin başkalarının elinde olduğu bilinciyle hareket eden kişinin hür şekilde karar vermesi, kişiliğini geliştirmesi mümkün olmayacaktır.<sup>94</sup>

Esasında bireye ait her türlü bilginin kişisel veri kapsamında olması nedeniyle kişisel verilerin korunması hakkı birçok hakla, özellikle insan onuru, düşünceyi açıklama özgürlüğü, özel haberleşmenin gizliliği ve vicdan, din ve inanç özgürlüğü ve kuşkusuz özel hayatın gizliliği ile iç içe geçmiş durumdadır.<sup>95</sup>

Ulusal ve uluslararası düzenlemelerde yer alan kişisel verilerin korunmasına ilişkin güvenceler başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerinin korunmasına hizmet eder. Hatta bu alanda yapılan düzenlemelerdeki asıl amacın kişisel verilerin korunmasından önce ve onun ötesinde insan onuru, düşünceyi açıklama özgürlüğü, özel haberleşmenin gizliliği ve vicdan, din ve inanç özgürlüğü ve özel hayatın gizliliğinin korunması olduğunu söylemek yanlış olmayacaktır.<sup>96</sup>

Avrupa İnsan Hakları Mahkemesi kararları incelendiğinde, ilk bakışta Mahkemenin kişisel verilerin korunması hakkını, özel hayata saygı hakkı (AİHS m.8) içinde ele aldığı şeklinde bir yorum yapılabilir.<sup>97</sup> Fakat Mahkemenin, önüne gelen davalarda somut olaya özgü yaptığı değerlendirmelere bakıldığında,

<sup>90</sup> Aksoy (n 13) 2.

<sup>91</sup> Çekin, (n 7) 6, 7.

<sup>92</sup> David Lyon, Zygmunt Bauman, *Akışkan Gözetim* (1. Bası Ayrıntı Yayınları 2013) 9.

<sup>93</sup> Şimşek (n 15) 4.

<sup>94</sup> Çekin (n 7) 7.

<sup>95</sup> Dülger (n 6) 76.

<sup>96</sup> Çekin (n 7) 23.

<sup>97</sup> Örnek olarak bkz. Klass ve diğerleri / Almanya, Başvuru No: 5029/71, KT. 06/09/1978; Z. / Finlandiya, Başvuru No: 22009/93, KT. 25/02/1997; L.L. / Fransa, Başvuru No: 7508/02, KT. 10.10.2006; I. / Finlandiya, Başvuru No: 20511/03, KT. 17.07.2008; S. ve Marper / Birleşik Krallık, Başvuru No: 30562/04 ve 30566/04, KT. 04/12/2008; Armonas / Litvanya ve Biriuk / Litvanya, Başvuru No: 36919/02 ve 23373/03, KT. 25/11/2008; Uslu / Türkiye (no:2), Başvuru No: 23815/04, KT. 20.01.2009; K.H. ve diğerleri / Slovakya, Başvuru No: 32881/04, KT. 28/04/2009; Ageyevy / Rusya, Başvuru No: 7075/10, KT. 18/04/2013; Avilkina ve diğerleri / Rusya, Başvuru No: 1585/09, KT. 06/06/2013; Konovalova / Rusya, Başvuru No: 37873/04, KT. 09.10.2014.

kişisel verilere ayrıca yer verdiği anlaşılabılır.<sup>98</sup> Mahkemenin Avrupa İnsan Hakları Sözleşmesi tarafından güvence altına alınmış hakların korunmasını sağlamak üzere kurulduğu göz önünde bulundurulduğunda içtihatlarında 8'inci maddeyi dayanak yaparak karar vermesi hukuka uygun ve sözleşme nezdinde kişisel verilerin korunmasını sağlayan bir yöntemdir. Zira Avrupa İnsan Hakları Sözleşmesinde kişisel verilerin korunmasına yönelik bağımsız bir temel hak bulunmamaktadır.<sup>99</sup>

Anayasa Mahkemesinin de kişisel verilerin korunmasına ilişkin temel değerlendirmesi, kişisel verilerin korunması konusunun her şeyden önce insan onuruna saygı ve kişilik haklarına dayandığı şeklindedir.<sup>100</sup> Mahkemeye göre “*kişisel verilerin korunması hakkı kişinin insan onurunun korunmasının ve kişiliğini serbestçe geliştirebilmesi hakkının özel bir biçimidir ve bireyin hak ve özgürlüklerini kişisel verilerin işlenmesi sırasında korumayı*” amaçlamaktadır.<sup>101</sup>

Kişisel sağlık verileri, kişilere ilişkin tıbbi kayıtların tutulması ve belli amaçlarla işlenmesi de şüphesiz özel hayata saygı hakkının, insan onuru ve kişilik hakkının bir parçasıdır. Önceki bölümde de ifade ettiğimiz gibi, bir hassas veri türü olarak kişisel sağlık verilerinin işlenmesi, bünyesinde taşıdığı ayrımcılık tehlikesi nedeniyle kişisel veri kümesi içinde daha katı kurallara bağlı, daha sıkı bir denetime tabidir. Aynı nedenden ötürü sağlık verileri söz konusu olduğunda kişisel verilerin korunması hakkının çok daha dikkat ve özenle ele alınması gerekir.

Sağlık hizmetinden yararlanan bireye ilişkin sağlık verilerinin kaydedilmesi, düzenlenmesi, aktarılması, açıklanması tıbbi teşhis ve tedavi süreci için gerekli olabilir. Doğru müdahalede bulunabilmek için bu bilgilere ihtiyaç duyulabilir. Ancak diğer taraftan bu veriler kişiseldir ve bireylerin bu bilgilerini gizli tutma hakları vardır. Bireylerin bu bilgilerinin yeterli düzeyde korunmadığına dair kuşkuyla kapılması sağlık hizmetlerinden faydalanmaktan çekinmelerine neden olabilir.<sup>102</sup>

AİHM'nin “Z. / Finlandiya” kararında<sup>103</sup> ifade ettiği gibi, sağlık verilerinin gizliliğine saygı göstermek hayati bir ilkedir. Hastanın mahremiyetine saygı duymanın yanında, tıp mesleğine ve genel olarak sağlık hizmetlerine olan güvenini korumak da çok önemlidir. Kişisel sağlık verilerinin ifşa edilebileceği

<sup>98</sup> Dülger (n 6) 139; Gonzalez Fuster (n 11) 95-102. “Korunması”, s. 139; Gonzalez Fuster, s. 95-102.

<sup>99</sup> Şimşek (n 15) 30.

<sup>100</sup> AyM, E. 2010/40, K. 2012/8, KT. 19.01.2012, RG. 6.3.2013 – 28579.

<sup>101</sup> AyM, E. 2010/40, K. 2012/8, KT. 19.01.2012, RG. 6.3.2013 – 28579; AyM, E. 2013/84, K. 2014/183, KT. 04.12.2014, RG. 13.03.2015 – 29294; AyM, E. 2014/180, K. 2015/30, KT. 19.03.2015, RG. 3.04.2015 – 29315.

<sup>102</sup> Küzeci (n 2) 247.

<sup>103</sup> Z. / Finlandiya, Başvuru No: 22009/93, KT. 25/02/1997, § 95; benzer ifade için bkz. M.S. / İsveç, Başvuru No: 74/1996/693/885, KT. 27.08.1997, § 41.

şüphesi, tıbbi yardıma ihtiyaç duyan bireyleri gerekli tedaviyi görmek ve hatta bu tür bir yardım istemekten caydırabilir ve bu durum bireysel ve toplumsal düzeyde oldukça ağır sonuçlara sebebiyet verebilir.

Bireyin kişisel sağlık verilerinin korunmasına ilişkin hak ve talebi aynı zamanda hasta haklarının da bir parçasıdır. 01.08.1998 tarih ve 23420 sayılı Resmi Gazete’de yayımlanarak yürürlüğe giren Hasta Hakları Yönetmeliğine göre, “hasta hakları temel insan haklarının sağlık hizmetlerine yansımalarıdır. Hasta hakları, sağlık hizmetlerinden faydalanma ihtiyacı bulunan bireylerin, sırf insan olmalarından kaynaklanan, uluslararası<sup>104</sup> ve ulusal<sup>105</sup> düzenlemelerle

<sup>104</sup> Hasta haklarına ilişkin uluslararası düzenlemelere örnek olarak, Dünya Tabipler Birliği Cenevre Bildirgesi’nde yer alan hekimlik andı (“... hastamın bana açtığı sırları, yaşamını yitirdikten sonra bile gizli tutacağıma ...”); Dünya Tabipler Birliği Lizbon Hasta Hakları Bildirgesi (1981);bu bildirgeyi revize eden Bali Bildirgesi (1995) ve 2005 yılında hasta haklarının yeniden ele alındığı, Bali Bildirgesinin geliştirilmesiyle oluşan Santiago Bildirgesi (8. Gizlilik hakkı a. Bir hastanın sağlık durumu, tıbbi durumu, teşhisi, prognozu ve tedavisi ile ilgili tüm tanımlayıcı bilgiler ve kişisel diğer tüm bilgiler, ölümden sonra bile gizli tutulmalıdır. İstisnai olarak, hasta yakınları, kendilerini sağlık riskleri konusunda bilgilendirecek bilgilere erişim hakkına sahip olabilirler. b. Gizli bilgiler ancak hastanın açık rıza göstermesi veya kanunda açıkça öngörülmesi halinde açıklanabilir. Hasta açık bir onay vermediği sürece, bilgiler diğer sağlık hizmeti sağlayıcılarına yalnızca kesin olarak “bilinmesi gerekenler” temelinde açıklanabilir. c. Tüm tanımlanabilir hasta verileri korunmalıdır. Verilerin korunması, usulüne uygun olmalıdır. Tanımlanabilir verilerin elde edilebildiği insan türlerini de aynı şekilde korunmalıdır.) örnek verilebilir.

Ayrıca Avrupa Birliğine üye ülkelerde hasta haklarına ilişkin düzenlemelerde uyumu amaçlayan 2002 tarihli Avrupa Birliği Hasta Hakları Statüsü (6. *Özel ve Gizlilik Hakkı*: Her birey kişisel bilgilerinin; sağlık durumu, yapılan teşhis ve tedavi konularında bilginin yanı sıra teşhis ve tedavi yapılırken veya özel ziyaretlerinin gizliliğinin muhafazası hususunda, gizli tutulmasını talep etme hakkına sahiptir. Bir bireyin sağlık durumuna veya ona uygulanan tıbbi/cerrahi tedaviye ilişkin bilgi ve veriler gizli olmalı ve öyle muhafaza(korunmalıdır) edilmelidir. Tıbbi/cerrahi müdahale sırasında bile kişisel gizliliğe saygı gösterilmeli, yani uygun ortamda yapılmalı ve gerçekten orada bulunması gerekli olan kişiler (hastanın onayı veya özel bir talebi olması durumları hariç) nezdinde yapılmalıdır.); Avrupa Konseyi metni olan, İnsan Hakları ve Biyotıp Sözleşmesi (Madde 10: *Özel yaşam ve bilgilendirme hakkı* 1. Herkes, kendi sağlığıyla ilgili bilgileri bakımından, özel yaşamına saygı gösterilmesini isteme hakkına sahiptir. 2. Herkes, kendi sağlığı hakkında toplanmış herhangi bir bilgiyi öğrenme hakkına sahiptir. Bununla beraber, bireylerin, bilgilendirilmeme istekleri de gözetilecektir. 3. Ayrıksı(istisnai) durumlarda, 2. paragrafta belirtilen hakların kullanılmasında, hastanın yararları bakımından yasa tarafından kısıtlamalar öngörülebilir.) ve Avrupa Hasta Haklarının Geliştirilmesi ya da bilinen adıyla Amsterdam Bildirgesi

(“4.Mahremiyet ve özel hayat

4.1.Hastanın sağlık durumu, tıbbi durumu, tanısı, prognozu, tedavisi hakkındaki ve kişiye özel diğer tüm bilgiler; ölümden sonra bile gizli olarak korunmalıdır.

4.2.Hastaya ait bu bilgiler; yalnızca hastanın açık izni veya mahkemenin kesin isteği üzerine açıklanabilir. Hastanın tedavisi ile ilgili diğer sağlık personeline ihtiyaç söz konusu olduğunda hastanın onayı olduğu varsayılarak davranılır.

4.3.Hastanın kimliğine dair bilgiler korunmalıdır. Bu bilgilerin korunması usulüne uygun yapılmalıdır.

4.4.Hastalar; tanıları, tedavileri ve bakımları ile ilgili kayıtlara, diğer dosyalara, teknik kayıtlara ve tıbbi dosyalarına bakabilme ve kendi dosyalarının ve kayıtlarının kopyasını alabilme hakkına sahiptir. Bu hak üçüncü kişilerin bilgilerine bakabilmeyi içermez.

4.5.Hastalar, kendileriyle ilgili tıbbi ve kişisel bilgilerin uygunsuz, eksik, çift anlamlı, eski olması veya tanı, tedavi ve bakım amacıyla ilgili olmaması durumunda bu bilgileri yenileme, daha açık hale getirme, bazı kısımlarını çıkarma, tamamlama, düzeltme hakkına sahiptir.

4.6.Hastanın tanı, tedavi ve bakımı için gerekli olmadıkça ve ek olarak hasta izin vermedikçe hastanın özel ve aile hayatına girilemez.

teminat altına alınmış bulunan haklarını” ifade eder.

Hasta hakları bireyin sahip olduğu haklarını sağlık hizmetlerinden yararlanırken kullanabilmesi ile ilgili haklardır. Bu haklar bireyin yaşama hakkı, beden bütünlüğü hakkı, özel yaşam hakkı, sağlık hakkı, kişisel verilerin korunması hakkı gibi haklarının ayrılmaz bir parçasıdır.<sup>106</sup> Kanun ile izin verilen haller ile tıbbi zorunluluklar dışında, hastanın özel hayatının ve aile hayatının gizliliğine dokunulamayacağı, Hasta Hakları Yönetmeliğinde yer alan hasta haklarına ilişkin temel ilkelerden biridir.<sup>107</sup> Kayıtlara ulaşma, kayıtları inceleme ve kayıtlarda düzeltme talep etme hakkı, mahremiyete saygı gösterilmesi hakkı, hastaya ait bilgilerin gizliliği; kişisel sağlık verilerinin korunması hakkı ile ilişkilendirilebilecek hasta haklarındandır.

## B. İdarenin Kişisel Sağlık Verilerinin Korunmasına İlişkin Yükümlülükleri

### 1. Aydınlatma Yükümlülüğü

Aydınlatma yükümlülüğü genel olarak, veri sorumlusunun, kişisel verileri işlenen bireylere, bu verilerin ne şekilde toplandığı, kim tarafından hangi amaçlarla ve hukuki sebeplerle işlenebileceği, işlenen kişisel verilerin kimlere hangi amaçlarla aktarılabilir, amaca uygun kullanılıp kullanılmadığı konusunda bilgi verme yükümlülüğü anlamına gelir.

108 nolu Sözleşme<sup>108</sup>, OECD Rehber İlkeleri<sup>109</sup> gibi uluslararası düzenlemelere de konu olan aydınlatma yükümlülüğü, Kişisel Verilerin Korunması Kanununun 10’uncu maddesinde düzenlenmiştir. Bu maddeye göre, “veri sorumlusu (veya yetkilendirdiği kişi), ilgili kişiye,

a) Veri sorumlusunun ve varsa temsilcisinin kimliği,

4.7.Tıbbi girişimler ancak kişinin özel hayatına saygı gösterilmesi durumunda yapılabilir. Bunun anlamı önerilen girişimin hastanın onayı veya isteğine göre ve kişinin ihtiyacı durumunda yapılabileceğidir

4.8.Sağlık kurumlarına başvuran hastalar, özellikle sağlık personelinin kişisel bakımlarını veya muayene ve tedavilerini yapacağı durumda kurumların özel hayatlarının korunmasını sağlayan fiziksel özelliklere sahip olmasını bekleme hakkına sahiptirler.”)

hasta haklarına ilişkin uluslararası düzenlemelerdir.

<sup>105</sup> Hasta haklarına ilişkin ulusal düzenlemelere örnek olarak, Tıbbi Deontoloji Tüzüğü (RG. 19.2.1960 - 10436), Umumi Hıfzıssıhha Kanunu (RG. 6.5.1930 - 1489), Tababet ve Şuabatı Sanatlarının Tarzı İcrasına Dair Kanun (RG. 14.4.1928 - 863), 3359 sayılı Sağlık Hizmetleri Temel Kanunu(RG. 15.5.1987 - 19461) verilebilir.

<sup>106</sup> Özge Yücel (Ed.), Gürkan Sert (Ed.), *Sağlık ve Tıp Hukukunda Sorumluluk ve İnsan Hakları: Sağlık Hizmeti, Sağlık Hakkı ve Hasta Hakları, Medeni Hukuk, Ceza ve İdare Hukuku Yönünden Sorumluluk* (1. Bası Seçkin Ankara 2018) 125.

<sup>107</sup> Hasta Hakları Yönetmeliği, m.5/f, RG. 01.08.1998 – 23420.

<sup>108</sup> Bkz. 108 nolu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi madde 8.

<sup>109</sup> Bkz. OECD Özel Yaşamın Korunması ve Kişisel Verilerin Sınırlanması Akışına İlişkin Rehber İlkeler paragraf 13.

- b) Kişisel verilerin hangi amaçla işleneceği,
- c) İşlenen kişisel verilerin kimlere ve hangi amaçla aktarılabileceği,
- ç) Kişisel veri toplamanın yöntemi ve hukuki sebebi<sup>110</sup>,
- d) 11 inci maddede sayılan diğer hakları<sup>111</sup>, konusunda bilgi vermekle yükümlüdür.”

Kişisel Verileri Koruma Kurumu tarafından yayınlanan Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul Ve Esaslar Hakkında Tebliğde<sup>112</sup> bu yükümlülük hakkında daha ayrıntılı düzenlemelere yer verilmiştir.

Aydınlatma yükümlülüğünün hukuka uygun şekilde yerine getirildiğinden söz edilebilmesi için, Kişisel Verilerin Korunması Kanununun 4’üncü maddesinde yer alan genel ilkelere de uygun olması gerekmektedir. Nitekim bu husus Kişisel Verileri Koruma Kurulu tarafından çıkarılan Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberinde vurgulanmıştır.<sup>113</sup>

Kişisel verilerin işlenmesine bireyin açık rızası olması durumunda da, kişisel verilerin kanunda düzenlenen istisna hükümleri dahilinde açık rıza aranmaksızın işlenmesi halinde de, veri sorumlusunun aydınlatma yükümlülüğü vardır. İlgili kişi, kişisel verisinin işlendiği her durumda bilgi alma hakkına sahiptir.

Açık rıza şartı ve aydınlatma yükümlülüğü birbirlerinden farklı kişisel veri işleme kurallarıdır. Dolayısıyla açık rıza şartının yerine getirildiği durumlarda

<sup>110</sup> “Hukuki sebep”ten kasıt, aydınlatma yükümlülüğü kapsamında kişisel verilerin, Kanunun 5 ve 6’ncı maddelerinde belirtilen işleme şartlarından hangisine dayanılarak işlendiğidir.” Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ, m. 5/h.

<sup>111</sup> 6698 sayılı Kişisel Verilerin Korunması Kanunu,  
“Madde 11/1: Herkes, veri sorumlusuna başvurarak kendisiyle ilgili;  
a) Kişisel veri işlenip işlenmediğini öğrenme,  
b) Kişisel verileri işlenmişse buna ilişkin bilgi talep etme,  
c) Kişisel verilerin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme,  
ç) Yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme,  
d) Kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme,  
e) 7 nci maddede öngörülen şartlar çerçevesinde kişisel verilerin silinmesini veya yok edilmesini isteme,  
f) (d) ve (e) bentleri uyarınca yapılan işlemlerin, kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme,  
g) İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme,  
ğ) Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme, haklarına sahiptir.”

<sup>112</sup> RG. 10.03.2018 – 30356.

<sup>113</sup> Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi, s. 9.

aydınlatma yükümlülüğünün olmadığı ya da aydınlatma yükümlülüğünün yerine getirildiği durumlarda açık rızanın aranmasına gerek olmadığı gibi bir sonuca ulaşamaz. Kişisel verilerin işlenmesine bireyin açık rızasının gerektiği durumlarda, birey önce hangi verisinin hangi amaç/amaçlarla işleneceği hususunda aydınlatılmalı ardından bireyin açık rızası alınmalıdır.<sup>114</sup>

Kişisel veri, veri sahibinden doğrudan elde edilebileceği gibi, dolaylı olarak başka kaynaklardan da ilgili kişinin verisine ulaşılabilir. Kişisel verilerin ilgili kişiden elde edilmemesi halinde de aydınlatma yükümlülüğü yerine getirilmelidir. Bu kurala, 2016/679 sayılı Genel Veri Koruma Tüzüğü<sup>115</sup> ve Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul Ve Esaslar Hakkında Tebliğde<sup>116</sup> ayrıntılı olarak yer verilmiştir.

Aydınlatma yükümlülüğü kişisel sağlık verilerinin işlenmesi faaliyetinde de kuşkusuz geçerlidir. Sağlık Bakanlığı ve sağlık hizmeti sunucuları veri sorumlusu olarak aydınlatma yükümlülüğüne, sağlık verileri işlenen bireyler de bu verilerin işlenme süreci ve yöntemi ile ilgili her türlü bilgi alma hakkına sahiptir.

Tebliğ'in 5'inci maddesinin d ve e bentlerine göre; "aydınlatma yükümlülüğünün yerine getirilmesi, ilgili kişinin talebine bağlı değildir."<sup>117</sup> Bu yükümlülüğünün yerine getirildiğinin ispatı ise veri sorumlusuna aittir.<sup>118</sup>

## 2. Veri Güvenliğini Sağlama Yükümlülüğü

Veri güvenliği kişisel verilerin korunması için gerekli bütün teknik ve idari önlemlerin alınması anlamına gelir. Veri güvenliği, verilerin kaybedilmesi, yetkisiz kişilerin verilere ulaşması, değiştirmesi ve işlemesi gibi olası tehlikelere karşı alınacak uygun güvenlik tedbirleriyle sağlanır.<sup>119</sup>

<sup>114</sup> Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ.

"Madde 5/1-f. "Kişisel veri işleme faaliyetinin açık rıza şartına dayalı olarak gerçekleştirilmesi halinde, aydınlatma yükümlülüğü ve açık rızanın alınması işlemlerinin ayrı ayrı yerine getirilmesi gerekmektedir."

<sup>115</sup> Bkz. Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR) madde 14/3.

<sup>116</sup> Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Rehberi,

"Madde 6: (1) Kişisel verilerin ilgili kişiden elde edilmemesi halinde;

a) Kişisel verilerin elde edilmesinden itibaren makul bir süre içerisinde,

b) Kişisel verilerin ilgili kişi ile iletişim amacıyla kullanılacak olması durumunda, ilk iletişim kurulması esnasında,

c) Kişisel verilerin aktarılabilecek olması halinde, en geç kişisel verilerin ilk kez aktarımının yapılacağı esnada

ilgili kişiyi aydınlatma yükümlülüğünün yerine getirilmesi gerekir."

<sup>117</sup> Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ, madde 5/1-d.

<sup>118</sup> Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ, madde 5/1-e.

<sup>119</sup> Şimşek (n 15) 95.



108 nolu Sözleşmenin 7’nci maddesine göre, “*otomatik dosyalara kaydedilen kişisel verileri korumak için, bunların kaza sonucu veya izinsiz olarak imhasına veya kaza sonucu kaybolmasına veya bunların izinsiz olarak elde edilmesine, değiştirilmesine veya dağıtılmasına karşı uygun güvenlik önlemlerinin*” alınması gerekmektedir.

2016/679 sayılı Genel Veri Koruma Tüzüğü’nün ikinci kısmı da kişisel verilerin güvenliği başlığını taşımaktadır ve bu kısımda veri güvenliği ilkesinin uygulanmasına ilişkin hükümler yer almaktadır.

Kişisel Verilerin Korunması Kanununun 12’nci maddesine göre veri sorumlusu;

- a) Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek,
- b) Kişisel verilere hukuka aykırı olarak erişilmesini önlemek,
- c) Kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır.”

Kişisel Sağlık Verileri Hakkındaki Yönetmelik m.18/1’de de, Kanunun bu maddesinde “*veri güvenliğine ilişkin yükümlülüklere riayet edileceği ve teknik ve idari tedbirlerin alınmasında, Kurum tarafından hazırlanan Kişisel Veri Güvenliği Rehberinin esas alınacağı*” belirtilmiştir.

Kişisel Veri Güvenliği Rehberi esas alınarak, kişisel verilerin güvenliğine ilişkin teknik ve idari tedbirler; kişisel verinin niteliğine göre muhtemel risk ve tehditlerin belirlenmesi, bunların azaltılması ya da ortadan kaldırılmasına yönelik kontrol ve çözüm alternatifleri bulunması, veri güvenliği politikaları oluşturulması, çalışanların eğitimi, siber güvenliği sağlanması, kişisel veri içeren her türlü ortamın güvenliğinin sağlanması ve takibi<sup>120</sup> şeklinde örneklendirilebilir. Fakat hassas kişisel veri kategorisinde yer alan sağlık verilerinin güvenliğinin sağlanmasına ilişkin; veri işleme faaliyetinde bulunanların ve veri sorumlularının yetkilerinin kapsamı ve yetki süreleri bakımından daha katı koruma tedbirleri getirilmesi gerekliliği bir eleştiri olarak savunulabilir.

“*Veri sorumlusu, kişisel verilerin kendi adına başka bir gerçek veya tüzel kişi tarafından işlenmesi hâlinde, gerekli tedbirlerin alınması hususunda bu kişilerle birlikte müştereken sorumludur.*”<sup>121</sup> Dolayısıyla veri işleyenler de veri güvenliğinin sağlanması amacıyla tedbir almak zorundadır. Kanun, veri sorumlusuna ayrıca kendi kurum veya kuruluşunda veri güvenliğine ilişkin

<sup>120</sup> Kişisel Verileri Koruma Kurulu tarafından bu teknik ve idari tedbirlerin ne olduğu konusunda hazırlanan veri güvenliği rehberi için bkz. <https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/7512d0d4-f345-41cb-bc5b-8d5cf125e3a1.pdf>, (29.08.2021).

<sup>121</sup> Kişisel Verilerin Korunması Kanunu, madde 12/2.

ve kanunun uygulanmasına ilişkin denetim yapma/yaptırma yükümlülüğü getirmiştir.<sup>122</sup> Veri sorumluları ile veri işleyenlerin bir başka yükümlülüğü, görevden ayrıldıktan sonra dahi, öğrendikleri kişisel verileri Kanun hükümlerine aykırı olarak başkalarına açıklama ve işleme amacı dışında kullanma yasağıdır.<sup>123</sup> Veri sorumlusunun veri güvenliğine ilişkin son olarak, “işlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, bu durumu en kısa sürede” ilgisine ve Kurula bildirme görevi mevcuttur.<sup>124</sup> Veri sorumlusunun Kurul’a veri güvenliğinin ihlalini bildirme yükümlülüğünde, kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesine kimin icra yahut ihmal yoluyla sebep olduğunun önemi yoktur. Veri sorumlusuna böyle bir ödev yüklenmesinin sebebi, ihlalin kapsamının artmasının ve tekrar etmesinin önüne geçmektir.<sup>125</sup>

Kişisel Verileri Koruma Kurulu da veri güvenliğine ilişkin yükümlülükleri belirlemek amacıyla düzenleyici işlem yapma yetki ve görevine sahiptir.<sup>126</sup> Kişisel sağlık verileri özelinde, 1 sayılı Cumhurbaşkanlığı Kararnamesi m. 378/4’e göre, Sağlık Bakanlığı, “ilgili mevzuat uyarınca elde edilen kişisel sağlık verilerinin güvenliğinin sağlanması için gerekli tedbirleri almakla ve bu amaçla, sistemde kayıtlı bilgilerin hangi görevli tarafından ne amaçla kullanıldığının denetlenmesine imkân tanıyan bir güvenlik sistemi” kurmakla görevlidir.

### 3. Düzenleme ve Denetleme Yapma Yükümlülüğü

Sağlık Hizmetleri Temel Kanunu ek madde 11’e göre, “sağlık hizmeti sunumu ile ilgili tüm iş ve işlemler Sağlık Bakanlığınca denetlenir.” 1 sayılı Cumhurbaşkanlığı Kararnamesinin 355’inci maddesi 1/i bendine göre ise, ilgili mevzuat çerçevesinde kişisel verilerin korunmasına ve veri mahremiyetinin sağlanmasına yönelik düzenleme yapmak Sağlık Bakanlığının hizmet birimlerinden biri olan Sağlık Hizmetleri Genel Müdürlüğünün görevidir. Bu hükümler, kişisel sağlık verilerinin korunmasına ilişkin Sağlık Bakanlığının düzenleme ve denetleme yapma yükümlülüğü olduğunu göstermektedir.

Bir önceki başlık altında da ifade ettiğimiz gibi, Kişisel Verilerin Korunması Kanunu m. 12/3’e göre veri sorumlusunun, kişisel verilerin korunmasını, kanunun uygulanmasını sağlamak amacıyla gerekli denetimleri yapmak/ yaptırmak zorunluluğu vardır. Veri sorumlusunun bir kamu tüzel kişisi olması durumunda da bu kural şüphesiz geçerlidir.

<sup>122</sup> Kişisel Verilerin Korunması Kanunu, madde 12/3.

<sup>123</sup> Kişisel Verilerin Korunması Kanunu, madde 12/4.

<sup>124</sup> Kişisel Verilerin Korunması Kanunu, madde 12/5.

<sup>125</sup> Çekin (n 7) 112.

<sup>126</sup> Kişisel Verilerin Korunması Kanunu, madde 22/f.

Kişisel (sağlık) verilerin(in) korunmasına ilişkin düzenleme ve denetim yapma yükümlülüğü, 5018 sayılı “Kamu Mali Yönetimi ve Kontrol Kanunu”<sup>127</sup> III sayılı Cetvele göre düzenleyici ve denetleyici kurumlar arasında yer alan “Kişisel Verileri Koruma Kurumu”nun asli görevidir.

Kurum, kişisel verilerin korunması gibi kamusal hayatın hassas ve teknik bir alanında faaliyet gösteren, bu sektörde düzenleme, denetleme ve yaptırım uygulama görevi üstlenen, kamu tüzel kişiliğine, icrai karar alma yetkisine sahip, idari ve mali özerkliği bulunan, organik ve fonksiyonel bakımdan bağımsız bir idari otoritedir. Kişisel Verileri Koruma Kurumu, kurul ve başkanlıktan oluşur. Kurumun karar organı Kişisel Verileri Koruma Kuruludur. Kurul, Kişisel Verilerin Korunması Kanunu madde 22’ye göre, düzenleyici işlem yapma, denetleme ve ihlal halinde idari yaptırım uygulama yetkisine sahiptir. Aynı Kanunun 15’inci maddesine göre “Kurul, şikâyet üzerine veya ihlal iddiasını öğrenmesi durumunda resen, görev alanına giren konularda gerekli incelemeyi yapar.” İnceleme sonucunda ihlal tespit ederse, “tespit ettiği hukuka aykırılıkların veri sorumlusu tarafından giderilmesine karar vererek ilgililere tebliğ eder.” Bu kararın tebliğden itibaren gecikmeksizin ve en geç otuz gün içinde yerine getirilmesi zorunludur. 18’inci maddeye göre ise Kişisel Verileri Koruma Kurulu, aydınlatma yükümlülüğünü yerine getirmeyenler, veri güvenliğine ilişkin yükümlülükleri yerine getirmeyenler, Kurul tarafından verilen kararları yerine getirmeyenler, Veri Sorumluları Siciline kayıt ve bildirim yükümlülüğüne aykırı hareket edenler hakkında idari para cezası vermeye yetkilidir.

Kişisel Verilerin Korunması Kanununun 6’ncı maddesinin 4’üncü fıkrasında Kurul’a bir yükümlülük olarak, özel nitelikli kişisel verilerin işlenmesinde yeterli önlemleri alma görevi verilmiştir. Bu doğrultuda Kişisel Verileri Koruma Kurul tarafından, 31.01.2018 tarihli ve 2018/10 sayılı karar ile Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler yayımlanmıştır.<sup>128</sup>

<sup>127</sup> RG. 24.12.2003 – 25326.

<sup>128</sup> RG. 07.03.2018 – 30353, “(...) Bu çerçevede, Kanunun 22 nci maddesinin (1) numaralı fıkrasının (ç) ve (e) bentleri uyarınca özel nitelikli kişisel veri işleyen veri sorumluları tarafından alınması gereken yeterli önlemler Kişisel Verileri Koruma Kurulu tarafından aşağıdaki şekilde belirlenmiştir:

- 1- Özel nitelikli kişisel verilerin güvenliğine yönelik sistemli, kuralları net bir şekilde belli, yönetilebilir ve sürdürülebilir ayrı bir politika ve prosedürün belirlenmesi,
- 2- Özel nitelikli kişisel verilerin işlenmesi süreçlerinde yer alan çalışanlara yönelik,
  - a) Kanun ve buna bağlı yönetmelikler ile özel nitelikli kişisel veri güvenliği konularında düzenli olarak eğitimler verilmesi,
  - b) Gizlilik sözleşmelerinin yapılması,
  - c) Verilere erişim yetkisine sahip kullanıcıların, yetki kapsamlarının ve sürelerinin net olarak tanımlanması,

Kişisel Verileri Koruma Kurulunun kanunda öngörülen denetim yükümlülüğünü hiç veya gereği gibi yerine getirmemesi halinde hizmet kusurundan söz etmek mümkündür. Elbette ki Kurumun idari sorumluluğundan bahsedebilmek için, kişisel verilerin korunması hakkının ihlali halinde ortaya çıkan zararlar Kişisel Verileri Koruma Kurumunun denetim faaliyetini hiç veya gereği gibi yerine getirmemesi şeklindeki ihmali fiili arasında illiyet bağı olmalıdır. Bir başka deyişle denetim yapılsaydı zarar meydana gelmeyecekti ya da daha az zarar görülecekti denilebiliyorsa kurumun bu ihmali faaliyeti kusur olarak tanımlanabilir. Ancak kişisel verilerin korunması hakkının ihlalinde asıl sorumlu veri sorumlusudur. Kişisel Verileri Koruma Kurumu denetim

ç) Periyodik olarak yetki kontrollerinin gerçekleştirilmesi,

d) Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkilerinin derhal kaldırılması. Bu kapsamda, veri sorumlusu tarafından kendisine tahsis edilen envanterin iade alınması,

3- Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği ortamlar; elektronik ortam ise

a) Verilerin kriptografik yöntemler kullanılarak muhafaza edilmesi,

b) Kriptografik anahtarların güvenli ve farklı ortamlarda tutulması,

c) Veriler üzerinde gerçekleştirilen tüm hareketlerin işlem kayıtlarının güvenli olarak loglanması,

ç) Verilerin bulunduğu ortamlara ait güvenlik güncellemelerinin sürekli takip edilmesi, gerekli güvenlik testlerinin düzenli olarak yapılması/yaptırılması, test sonuçlarının kayıt altına alınması,

d) Verilere bir yazılım aracılığı ile erişiliyorsa bu yazılıma ait kullanıcı yetkilendirmelerinin yapılması, bu yazılımların güvenlik testlerinin düzenli olarak yapılması/yaptırılması, test sonuçlarının kayıt altına alınması,

e) Verilere uzaktan erişim gerekiyorsa en az iki kademeli kimlik doğrulama sisteminin sağlanması,

4- Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği ortamlar; fiziksel ortam ise

a) Özel nitelikli kişisel verilerin bulunduğu ortamın niteliğine göre yeterli güvenlik önlemlerinin (elektrik kaçağı, yangın, su baskını, hırsızlık vb. durumlara karşı) alındığından emin olunması,

b) Bu ortamların fiziksel güvenliğinin sağlanarak yetkisiz giriş çıkışların engellenmesi,

5- Özel nitelikli kişisel veriler aktarılacaksa

a) Verilerin e-posta yoluyla aktarılması gerekiyorsa şifreli olarak kurumsal e-posta adresiyle veya Kayıtlı Elektronik Posta (KEP) hesabı kullanılarak aktarılması,

b) Taşınabilir Bellek, CD, DVD gibi ortamlar yoluyla aktarılması gerekiyorsa kriptografik yöntemlerle şifrelenmesi ve kriptografik anahtarın farklı ortamda tutulması,

c) Farklı fiziksel ortamlardaki sunucular arasında aktarma gerçekleştiriliyorsa, sunucular arasında VPN kurularak veya SFTP yöntemiyle veri aktarımının gerçekleştirilmesi,

ç) Verilerin kağıt ortamı yoluyla aktarımı gerekiyorsa evrakın çalınması, kaybolması ya da yetkisiz kişiler tarafından görülmesi gibi risklere karşı gerekli önlemlerin alınması ve evrakın "gizlilik dereceli belgeler" formatında gönderilmesi gerekir."

6- Yukarıda belirtilen önlemlerin yanı sıra Kişisel Verileri Koruma Kurumunun internet sitesinde yayımlanan Kişisel Veri Güvenliği Rehberinde belirtilen uygun güvenlik düzeyini temin etmeye yönelik teknik ve idari tedbirler de dikkate alınmalıdır."

yükümlülüğü yerine getirmediği takdirde veri sorumlusu ile birlikte bu zararı kusuru oranında tazmin etmekle mükelleftir. Öte yandan veri sorumlusu, kurulun gerekli denetimleri yapmadığını gerekçe göstererek sorumluluktan kurtulamaz.

## C. İDARENİN KİŞİSEL SAĞLIK VERİLERİNİ KORUMA YÜKÜMLÜLÜĞÜNÜ YERİNE GETİRMEMESİNDEN KAYNAKLANAN SORUMLULUĞU

### 1. Genel Olarak

Anayasa'nın 125'inci maddesinin son fıkrası, “idare kendi eylem ve işlemlerinden doğan zararı ödemekle yükümlüdür” hükmüyle idarenin kusurlu ya da kusursuz olması şeklinde herhangi bir ayırım yapmaksızın mali sorumluluğunun temelini oluşturur.<sup>129</sup> Bu çalışmada idarenin sorumluluğu ile kastedilen idarenin akit dışı idari sorumluluğudur. Akit dışı idari sorumluluk, idarenin kamu hukuku alanında idare hukukunun özellikleri dikkate alınarak geliştirilen, özel hukuktan farklı, kendine özgü kuralları olan bir sorumluluk türüdür. Kusurlu sorumluluk ve kusursuz sorumluluk olarak iki ayrı esasa dayanır.

Kusurlu sorumluluk diğer adıyla hizmet kusuru genel olarak bir kamu hizmetinin kuruluş, işleyiş ve teşkilatlanmasındaki bozukluk, aksaklık ya da düzensizlik olarak tanımlanabilir.<sup>130</sup>

Bir ülkedeki “en güçlü veri tekeli” olan<sup>131</sup> idare geniş anlamda kamu hizmeti faaliyetini yerine getirirken gereksinim duyduğu kişisel veriler üzerinde toplama, kaydetme, inceleme, kullanma, depolama gibi çeşitli şekillerde işlem yapmaktadır. İdare bu işlemleri yaparken/işleme faaliyetinde bulunurken ve veri işleme faaliyetinden bulunanları denetlerken kendi icrai veya ihmali fiiliyle bir zarara sebebiyet verirse, ortaya çıkan bu zararı tazmin etmekle mükelleftir. Nitekim Kişisel Verilerin Korunması Kanunu m. 11/ğ'ye göre, ilgili kişi, kişisel verilerinin kanuna aykırı olarak işlenmesi sebebiyle zarara uğrarsa bu zararın giderilmesini talep etme hakkına sahiptir.

Kişisel sağlık verileri söz konusu olduğunda da, verilere ilişkin kayıtların eksik ya da yanlış tutulması, kaybedilmesi yahut hiç kayıt altına alınmaması, bireylerin kendi verilerine erişiminin engellenmesi, verilerin amaç dışı kullanılması, gerektiğinden uzun süre saklanması, hukuka aykırı olarak üçüncü kişilerle paylaşımı, veri işleme faaliyetinde bulunan kamu personeli veya (sağlık hizmeti faaliyetinde bulunan) özel hukuk tüzel kişileri üzerinde denetim ve gözetim görevini gereği gibi yerine getirmemesi, kişisel verilerin

<sup>129</sup> Metin Günday, *İdare Hukuku* (10. Bası İmaj Yayıncılık Ankara 2013) 367.

<sup>130</sup> Bahtiyar Akyılmaz, Murat Sezginer, Cemil Kaya, *İdare Hukuku* (9. Bası, Savaş Yayınevi Ankara 2018) 112; Günday (n 129) 369.

<sup>131</sup> AYM, E.2006/167, K.2008/86, K.T. 20.03.2008.

korunmasına ilişkin dikkat ve özen gösterilmemesi durumu hizmet kusuru kapsamında değerlendirilmektedir.

İdarenin, hukuk sınırlarının/kurallarının dışına çıkarak sağlık verilerini işlemesi ya da veri işleme faaliyetinin denetimini görevini gereği gibi yerine getirmemesi bireyin bir zarara uğramasına sebep olursa, bu zararın her şeyden önce hukuk devleti ilkesi gereği idare tarafından tazmin edilmesi gerekir.<sup>132</sup> Bu tazmin borcunun hukuki mekanizması ise, İdari Yargılama Usulü Kanunu madde 2/1-b’de düzenlenmiş olan tam yargı davasıdır.

## 2. Kişisel Sağlık Verilerinin Muhafaza Edilmemesi, Eksik veya Yanlış Tutulması

Tıbbi teşhis ve tedaviye yönelik kayıtlar defaatle açıkladığımız gibi kişisel sağlık verisi olarak kabul edilmektedir. Sağlık kamu hizmetini sunan kamu tüzel kişileri ve kamu tüzel kişilerinin gözetimi ve denetimi altında bu hizmeti sunan özel hukuk tüzel kişileri ve hekimler, tanıtıcı bilgiler, risk faktörleri, hastalık öyküsü, teşhis, tedavi planı gibi tıbbi bilgileri kayıt altına almakla yükümlüdür.

Tıbbi kayıtların tutulması özellikle de bir bilişim sistemi içinde muhafaza edilmesi, tıbbi hataların önüne geçmek, hastanın sağlık durumunu takip edebilmek, sağlık hizmetini daha etkili, kaliteli ve verimli şekilde sunmak gibi pek çok fayda sağlar. Bu verilerin hiç muhafaza edilmemesi de, özenli bir şekilde muhafaza edilmemesi, kaybedilmesi, eksik veya yanlış kayıt altına alınması da idarenin hizmet kusurudur.

Sağlık Bakanlığının, kişisel sağlık verilerini uygun şekilde kayıt altına almayan sağlık hizmeti sunucuları ve diğer veri işleyenler üzerinde denetim ve yaptırım uygulama yetkisi vardır. Sağlık Hizmetleri Temel Kanunu ek madde 11’e göre,<sup>133</sup> “sağlık hizmeti sunumu ile ilgili tüm iş ve işlemler Sağlık

<sup>132</sup> Akgül (n 41) 33.

<sup>133</sup> Ek Madde 11 – (Ek: 2/1/2014-6514/46 md.) “Sağlık hizmeti sunumu ile ilgili tüm iş ve işlemler Sağlık Bakanlığınca denetlenir. Olağanüstü durumlarda mesleğini icraya yetkili kişilerce acil sağlık hizmeti ulaşıma ve sağlık hizmeti devamlılık arz edene kadar verilecek olan sağlık hizmeti hariç, ruhsatsız olarak sağlık hizmeti sunan veya yetkisiz kişilerce sağlık hizmeti verdirenler, bir yıldan üç yıla kadar hapis ve yirmi bin güne kadar adli para cezası ile cezalandırılır. Özel izne tabi hizmet birimlerini Sağlık Bakanlığından izin almaksızın açan veya buralarda verilecek hizmetleri sunan sağlık kurum ve kuruluşları, bir önceki aya ait brüt hizmet gelirinin yarısına kadar idari para cezası ile cezalandırılır. Bakanlıkça belirlenen kayıtları uygun şekilde tutmayan veya bildirim zorunluluğunu yerine getirmeyen sağlık kurum ve kuruluşları iki defa uyarılır. Uyarıya uymayanlara bir önceki aya ait brüt hizmet gelirinin yüzde biri kadar idari para cezası verilir. Sağlık Bakanlığınca belirlenen acil hastaya müdahale esaslarına; personel, tıbbi cihaz ve donanım, bina ve hizmet birimleri, malzeme ile ilaç standartlarına uyulmaması hâllerinde bir önceki aya ait brüt hizmet gelirinin yüzde beşine kadar idari para cezası uygulanır. Bu maddedeki idari para cezasını gerektiren fiillerin bir yıl içinde tekrarı hâlinde idari para cezaları bir kat artırılarak



*Bakanlığınca denetlenir*”. Tıbbi verilerin gereği gibi, hassas kişisel verilerin işlenmesi kurallarına uygun şekilde kayıt altına alınıp alınmadığını denetlemek de şüphesiz Sağlık Bakanlığının yetki ve görev alanı içindedir. Bu denetim sonucunda Bakanlığın, tıbbi kayıtları uygun şekilde muhafaza etmeyen sağlık hizmeti sunucusunu uyarma ve yaptırım uygulama yetkisi mevcuttur.<sup>134</sup>

Danıştay, davacının şiddetli bel ağrısı şikâyetiyle başvurduğu hastanede yapılan enjeksiyon sonucu bacağında his kaybı olduğundan bahisle açtığı davada, hastaya ait tıbbi kayıtların eksik ve özensiz tutulmasından dolayı davacıda oluşan sağlık probleminin açıklanamadığını ve idarenin sorumluluğunun belirlenemediğini, bu durumun hizmetin sağlık hizmetinin kötü işlemesi anlamına geldiğini ifade etmiştir. Sağlık verilerinin eksik olmasının, hastanın hakkında uygulanan tedavileri ve rahatsızlığının nedenini öğrenmesine engel olması nedeniyle idarenin manevi tazmin sorumluluğu olduğuna karar vermiştir.<sup>135</sup> Başka bir olayda, davacının kanser tanısıyla

*uygulanır; üçüncü defa işlenmesinde ise sağlık kurum ve kuruluşunun ilgili bölümünün veya tamamının faaliyeti on güne kadar durdurulur. Aynı isim ve sahipliğe birden fazla sağlık kurum ve kuruluşu bulunması hâlinde idari yaptırımlar sadece ihlalin yapıldığı sağlık kurum ve kuruluşu ile sınırlı olarak uygulanır. Bu maddede belirtilen idari para cezalarını vermeye valiler, faaliyet durdurma cezasını vermeye Sağlık Bakanlığı yetkilidir. Bu maddenin uygulanmasına ilişkin usul ve esaslar, üniversite sağlık uygulama ve araştırma merkezleri yönünden Yükseköğretim Kurulunun görüşü alınarak Sağlık Bakanlığınca düzenlenir.”*

<sup>134</sup> Sağlık Hizmetleri Temel Kanunu,

Ek madde 3/5: “Bakanlıkça belirlenen kayıtları uygun şekilde tutmayan veya bildirim zorunluluğunu yerine getirmeyen sağlık kurum ve kuruluşları iki defa uyarılır. Uyarıya uymayanlara bir önceki aya ait brüt hizmet gelirinin yüzde biri kadar idari para cezası verilir.”

<sup>135</sup> DİDDK, E. 2015/3016, K. 2016/186, T. 8.2.2016, aynı yönde bkz. İstanbul BİM, 8. İDD, E. 2017/5, K. 2017/305, KT. 7.3.2017, “(...) Poliklinik kayıtlarının düzenli şekilde tutulmamasından kaynaklı tıbbi kayıt eksikliğinin hizmet kusurunun belirlenmemesindeki payı dikkate alındığında, davacının hakkında uygulanan tedavileri ve zararlı sonucun sebebinin öğrenecek tıbbi kayıtların noksan olması, dolayısıyla tedavi sürecinde gelişen olaylarla ilgili maddi gerçeğe (rahatsızlığının nedenine) hiçbir zaman ulaşamayacak ve ömür boyu şüphe duyacak olması nedeniyle uğradığı manevi zararının tazmini zorunludur. Başka bir anlatımla; hastanın başvurduğu gün ve saatin, hastaya uygulanan tedavinin, tedaviyi uygulayan doktor ve sağlık personelinin adının, kullanılan ilaç bilgilerinin hasta dosyasında(poliklinik defterinde) yer alması, hasta haklarının da gereği olup; söz konusu kayıtların düzenli ve yeterli tutulmaması-kişinin doğruyu öğrenme hakkına engel olacağından- hizmet kusurunu oluşturmaktadır.”; DİDDK, E. 2015/2939, K. 2016/3522, KT. 21.12.2016, “Davacıların yakınına ilişkin olarak eksik tedavinin uygulanması, hastane kayıtlarının düzgün, yeterli ve güvenilir şekilde tutulmaması, davacılar yakının Mardin Devlet Hastanesi Başhekimliği'nin yazısına göre taburcu edilmesine rağmen bu konuda herhangi bir kaydında bulunmaması,hasta ve hasta yakınlarına hangi tedavilerin uygulandığı veya uygulanması gerektiği yönünde bilgilendirme yapılmamış olması, ayrıca olaya ilişkin olarak dosyada yer alan ifade tutanaklarının da birbirini tutmaması ve çelişkili olması karşısında; dava konusu uyuşmazlıkta davalı idarenin hizmet kusuru bulunduğu sonucuna varılmıştır.” Aynı yönde bir başka davada idarenin teşhis ve tedavide tıbbi eksiklik

ameliyat edildikten sonra başka bir hastanede yapılan tetkik ve tahliller sonucu kanser olmadığı sonucuna ulaşılması üzerine, konulan tanının hatalı ve yanlış olduğu, gereksiz yere cerrahi müdahalede bulunulduğu gerekçesiyle maddi ve manevi tazminat talebiyle açtığı davada Danıştay, sağlık hizmetlerinden yararlananlarla ilgili kayıtların eksikliğini, yapılan tedavilerin kayıt altına alınmamasını, tetkik ve inceleme sonuçlarının muhafaza edilmemesini hizmet kusuru olarak nitelendirmiştir.<sup>136</sup> Tıbbi kayıtların ve dolayısıyla sağlık hizmetinin eksik ve kusurlu işlemesi nedeniyle idarenin manevi tazminat ödemesi gerektiğine hükmetmiştir.<sup>137</sup>

### 3. Kişisel Sağlık Verilerinin Açıklanması ya da Üçüncü Kişilerle Paylaşılması

Kişisel sağlık verilerinin, hukuka aykırı olarak açıklanması ya da üçüncü kişilerle paylaşımı veri güvenliğinin ihlali anlamına gelir. İdare sağlık ve sosyal güvenlik hizmetini yerine getirirken elde ettiği sağlık verilerinin güvenliğini sağlamakla mükelleftir. Öte yandan tüm sağlık çalışanlarının da hasta mahremiyeti ve sır saklama yükümlülüğü çerçevesinde sorumluluğu vardır.<sup>138</sup>

Sır saklama yükümlülüğü, hastanın sağlık durumu ya da onun hakkında sağlık hizmeti vesilesiyle edindiği bilgileri üçüncü kişilere aktarma/açıklama yasağını ifade eden,<sup>139</sup> Hipokrat yemininde,<sup>140</sup> Tıbbi Deontoloji Tüzüğünde,<sup>141</sup> Türk Tabipler Birliği Hekimlik Meslek Etiği Kurallarında<sup>142</sup> ve Hasta Hakları

---

ve ihmali iddiasıyla açılan bir tam yargı davasında, hastaya ait tıbbi kayıtların gerekli şekilde muhafaza edilmemesi ve hasta dosyasının kaybedilmesini ağır hizmet kusuru olarak görmüş ve mahkeme tarafından istenmesine rağmen davalı idarenin tıbbi kayıtları ibraz edememesinin, idarenin sorumluluğu tespit etmeye ve yargısal denetime engel teşkil ettiğini ifade etmiştir. İdarenin tıbbi kayıtları muhafaza etmemesinin manevi tazminat yükümlülüğü doğurduğuna hükmetmiştir. D10D, E. 2007/3301, K. 2008/2939, KT. 29.4.2008, <https://www.lexpera.com.tr/>, (20.08.2021).

<sup>136</sup> D15D, E. 2013/4071 K. 2014/2431, KT. 3.4.2014, <https://www.lexpera.com.tr/>, (20.08.2021).

<sup>137</sup> D15D, E. 2013/4071 K. 2014/2431, KT. 3.4.2014, <https://www.lexpera.com.tr/>, (20.08.2021).

<sup>138</sup> Yücel, Sert (n 106) 184; Murat Volkan Dülger, ‘Sağlık Hukukunda Kişisel Verilerin Korunması ve Hasta Mahremiyeti’, (2014) 2 İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi 60; Sabire Sanem Yılmaz, Tıp Alanında Kişisel Verilerin Açıklanması Suçu (2. Bası Seçkin Ankara 2017) 53.

<sup>139</sup> Dülger (n 138) 59.

<sup>140</sup> Hipokrat yemininde “Gerek sanatımın icrası sırasında gerekse insanlarla gündelik ilişkideyken edindiğim bilgileri ortalığa saçmayacağım, bir sır olarak saklayacağım ve kimseye açmayacağım.” sözü yer alır bu hekimlerin sır saklama yükümlülüğünün etik karşılığıdır.

<sup>141</sup> Madde 4: “Tabip ve dış tabibi, meslek ve sanatının icrası vesilesiyle muttali olduğu sırları, kanuni mecburiyet olmadıkça, ifşa edemez. Tıbbi toplantılarda takdim edilen veya yayınlarda bahis konusu olan vakalarda, hastanın hüviyeti açıklanamaz.”

<sup>142</sup> Madde 9: “Hekim, hastasından mesleğini uygularken öğrendiği sırları açıklayamaz.

Yönetmeliğinde<sup>143</sup> de yer alan bir etik bir görevdir.<sup>144</sup> Hekimlerin ve diğer sağlık çalışanlarının hasta mahremiyetini ve sır saklama yükümlülüğünü ihlal etmeleri Türk Ceza Kanununun 136'ncı maddesinde düzenlenen "verileri hukuka aykırı olarak verme veya ele geçirme" suçunu oluşturabileceği gibi, bu suçun oluşmadığı hallerde dahi, meslek kurallarına aykırılık dolayısıyla bir disiplin yaptırımı veya tazminat sorumluluğuna sebep olabilir.<sup>145</sup>

Belirtmek gerekir ki, veri güvenliğinin en önemli unsuru insan unsurudur. Fakat hekimler ve diğer sağlık çalışanlarının tıbbi verilerin büyük bir kısmının kayıt altına alındığı bilişim teknolojileri konusunda uzman olmaları mesleklerinin bir gereği değildir. Bu yüzden tüm sağlık çalışanlarının kişisel

---

*Hastanın ölmesi ya da o hekimle ilişkisinin sona ermesi, hekimin bu yükümlülüğünü ortadan kaldırmaz. Hastanın onam vermesi ya da sırrın saklanması hasta ya da öteki insanların yaşamını tehlikeye sokması durumunda, hastanın kişilik haklarının zedelenmemesi koşuluyla, hekim bu sırrı saklamakla yükümlü değildir. Yasal zorunluluk durumlarında hekimin rapor düzenlemesi de, meslek sırrının açıklanması anlamına gelmez. Hekim, tanık ya da bilirkişi olarak mahkemeye çağrıldığında olayın meslek sırrı olduğunu ileri sürerek bu görevlerinden çekilebilir."*

<sup>143</sup> Madde 21:

*"Hastanın, mahremiyetine saygı gösterilmesi esastır. Hasta mahremiyetinin korunmasını açıkça talep de edebilir. Her türlü tıbbi müdahale, hastanın mahremiyetine saygı gösterilmek suretiyle icra edilir.*

*Mahremiyete saygı gösterilmesi ve bunu istemek hakkı;*

- a) Hastanın, sağlık durumu ile ilgili tıbbi değerlendirmelerin gizlilik içerisinde yürütülmesini,*
- b) Muayenenin, teşhisin, tedavinin ve hasta ile doğrudan teması gerektiren diğer işlemlerin makul bir gizlilik ortamında gerçekleştirilmesini,*
- c) Tıbben sakınca olmayan hallerde yanında bir yakınının bulunmasına izin verilmesini,*
- d) Tedavisi ile doğrudan ilgili olmayan kimselerin, tıbbi müdahale sırasında bulunmamasını,*
- e) Hastalığın mahiyeti gerektirmedikçe hastanın şahsi ve ailevi hayatına müdahale edilmemesini,*
- f) Sağlık harcamalarının kaynağının gizli tutulmasını, kapsar.*

*Ölüm olayı, mahremiyetin bozulması hakkını vermez.*

*Eğitim verilen sağlık kurum ve kuruluşlarında, hastanın tedavisi ile doğrudan ilgili olmayanların tıbbi müdahale sırasında bulunması gerekli ise; önceden veya tedavi sırasında bunun için hastanın ayrıca rızası alınır."*

Madde 23:

*"Sağlık hizmetinin verilmesi sebebiyle edinilen bilgiler, kanun ile müsaade edilen haller dışında, hiçbir şekilde açıklanamaz. Kişinin rızasına dayansa bile, kişilik haklarından bütünüyle vazgeçilmesi, bu hakların başkalarına devri veya aşırı şekilde sınırlandırılması neticesini doğuran hallerde bilginin açıklanması, bunları açıklayan hukuki sorumluluğunu kaldırmaz. Hukuki ve ahlaki yönden geçerli ve haklı bir sebebe dayanmaksızın hastaya zarar verme ihtimali bulunan bilginin ifşa edilmesi, personelin ve diğer kimselerin hukuki ve cezai sorumluluğunu da gerektirir.*

*Araştırma ve eğitim amacı ile yapılan faaliyetlerde de hastanın kimlik bilgileri, rızası olmaksızın açıklanamaz."*

<sup>144</sup> Küzeci (n 2) 481.

<sup>145</sup> Dülger (n 138) 469.

sağlık verilerinin gizliliği ve hassasiyeti hususunda bilgilendirilmeleri ve buna ilişkin denetim mekanizmalarının kurulması gereklidir.<sup>146</sup>

1 sayılı Cumhurbaşkanlığı Kararnamesinin 378/3'üncü maddesine göre "Sağlık Bakanlığının, toplayıp işlediği kişisel sağlık verilerine ilgili kişilerin erişimini sağlayacak bir sistem kurma" yetkisi ve görevi vardır. Aynı maddenin 4'üncü fıkrasına göre ise Bakanlık, "kurulan sistemlerin ve bu sistemlerde yer alan kişisel sağlık verilerinin güvenliği ve güvenilirliğini sağlamak için gerekli tedbirleri almakla, sistemde kayıtlı kişisel verilerin hangi görevli tarafından ne amaçla kullanıldığını denetlemekle ve buna ilişkin bir güvenlik sistemi kurmakla" yükümlüdür.

Hasta Hakları Yönetmeliğinde de hastanın kişisel sağlık bilgilerinin gizliliğine, hastanın rızası ya da kanuni müsaade olmaksızın hasta bilgilerinin açıklanmamasına ilişkin hükümler mevcuttur. Yönetmeliğin 23'üncü maddesine göre,

*"Sağlık hizmetinin verilmesi sebebiyle edinilen bilgiler, kanun ile müsaade edilen haller dışında, hiçbir şekilde açıklanamaz.*

*Kişinin rızasına dayansa bile, kişilik haklarından bütünüyle vazgeçilmesi, bu hakların başkalarına devri veya aşırı şekilde sınırlandırılması neticesini doğuran hallerde bilginin açıklanması, bunları açıklayanın hukuki sorumluluğunu kaldırmaz.*

*Hukuki ve ahlaki yönden geçerli ve haklı bir sebebe dayanmaksızın hastaya zarar verme ihtimali bulunan bilginin ifşa edilmesi, personelin ve diğer kimselerin hukuki ve cezai sorumluluğunu da gerektirir.*

*Araştırma ve eğitim amacı ile yapılan faaliyetlerde de hastanın kimlik bilgileri, rızası olmaksızın açıklanamaz."*<sup>147</sup>

Yargı kararlarına baktığımızda ise, Danıştay veri güvenliğinin ihlali, kişisel verilerin ilgilinin rızası ya da kanuni gereklilik olmaksızın açıklanması ya da üçüncü kişilerle paylaşılması durumunda idarenin hizmet kusuru bulunduğu yönünde kararlar vermektedir.

Yaptırmış olduğu HIV testi sonucunun pozitif çıktığını laboratuvar teknisyeninin söylemesi ile öğrendikten sonra intihar eden kişinin yakınlarının

<sup>146</sup> Küzeci (n 2) 482.

<sup>147</sup> Hasta Hakları Yönetmeliğinin 20 ve 21'nci maddeleri de kişisel sağlık verilerinin gizliliği kapsamında değerlendirilebilir. Bkz. Hasta Hakları Yönetmeliği madde 20: "İlgili mevzuat hükümleri ve/veya yetkili mercilerce alınacak tedbirlerin gerektirdiği haller dışında; kişi, sağlık durumu hakkında kendisinin, yakınlarının ya da hiç kimsenin bilgilendirilmemesini talep edebilir. Bu durumda kişinin kararı yazılı olarak alınır. Hasta, bilgi verilmemesi talebini istediği zaman değiştirebilir ve bilgi verilmesini talep edebilir." Hasta Hakları Yönetmeliği madde 21 için bkz. dn. 143.

açtığı davada Danıştay, HIV testi sonucunun doğrulama testi yapılmadan ve bu test sonuçlanmadan testi yaptıran kişi dahil hiç kimseyle paylaşılması gerekirken bu aşamadan önce laboratuvar teknisyeni tarafından paylaşılmasının kişinin intiharına sebep olduğunu belirtmiş, kişisel sağlık verisi olduğu konusunda şüphe bulunmayan HIV testi sonucunun laboratuvar teknisyeni tarafından (ve doğrulama testi yapılmadan) açıklanmasını ağır hizmet kusuru olarak nitelendirmiş ve idarenin tazminat ödemesi gerektiğine hükmetmiştir.<sup>148</sup> Bir başka olayda, davacının, hakkında düzenlenen “askerliğe elverişli değildir” şeklindeki sağlık raporunun basın yayın organlarınca elde edilmesi sebebiyle uğradığını ileri sürdüğü zararın tazmini için açtığı davada idare mahkemesi, sağlık raporunun bir kişisel sağlık verisi olduğu, kişisel sağlık verilerinin ulusal ve uluslararası düzenlemeler ışığında hassas kişisel veri kategorisinde olduğunu belirtmiş ve hassas kişisel veri niteliği taşıyan sağlık raporunun muhafazasında idarenin kusuru bulunduğunu gerekçe göstererek manevi tazminata hükmetmiştir. Temyiz incelemesinde Danıştay aynı gerekçelerle idare mahkemesinin kararını onamıştır.<sup>149</sup>

Avrupa İnsan Hakları Mahkemesi, *I. / Finlandiya* davasında tıbbi kayıtların güvenliliğine ilişkin gerekli tedbirlerin alınmamasını, bu bilgilerin üçüncü kişilerin eline geçmesine engel olacak bir sistemin yokluğunu AİHS’nin ihlali olarak değerlendirmiştir. Davaya konu olayda, bir devlet hastanesinde hemşire olarak çalışan başvuru, HIV pozitif olduğuna ve çalıştığı hastanede gördüğü tedaviye ilişkin bilgilerinin iş arkadaşları tarafından öğrenildiğinden şüphe ederek, kişisel sağlık kayıtlarının kimlerle paylaşıldığını öğrenmek amacıyla idari ve yargısal başvuru yollarını kullanmıştır. Fakat bu mekanizmalardan özel hayatının korunmasına elverişli bir sonuç elde edemeyince AİHM’ye başvurmuştur. Mahkeme, hastanenin şikâyet üzerine, sonradan aldığı tedbirleri yeterli görmemiş ve tıbbi kayıtların güvenliğini sağlamak için alınması gereken tedbirlerde geç kalındığını bu nedenle başvuru kişinin özel hayatına saygı hakkının ihlal edildiğine karar vermiştir.<sup>150</sup>

Bir başka olayda, *Avilkina vd. / Rusya* davasında, Yehova Şahitleri tarikatına mensup üç kişi, kan nakli yapılmasını reddetmeleri üzerine sağlık kayıtlarının rızaları dışında ifşa edilmesi ve buna karşı iç hukukta açılan davada yerel mahkemenin bu uygulamayı hukuka uygun bulması üzerine AİHM’ye başvuruda bulunmuşlardır. Mahkeme, bazı durumlarda bir suçun soruşturulması veya yargılamanın aleni olmasıyla elde edilecek faydanın, sağlıkla ilgili kişisel verilerin gizliliğinin korunmasındaki hastanın çıkarından üstün tutulabileceğini belirtmiş fakat somut olayda böyle bir gerekliliğin söz konusu olmadığına karar vermiştir.

<sup>148</sup> D10D, E. 2005/8407, K. 2007/6526, KT. 28.12.2007, <https://www.lexpera.com.tr>, (18.08.2021).

<sup>149</sup> D15D, E. 2015/10101 K. 2016/664 KT. 8.2.2016, <https://www.lexpera.com.tr>, (18.08.2021).

<sup>150</sup> I. / Finlandiya, Başvuru No: 20511/03, KT. 17.07.2008.

Başvurucuların bir ceza soruşturması kapsamında sanık veya şüpheli olmadığı, kan naklinin reddinin başvuru için herhangi bir hayati tehlikeye sebep olmadığı ve bağlı bulundukları tarikatın baskısı sonucu kan naklini reddettikleri yönünde bir bulgunun saptanamadığı ifade edilmiştir. Dolayısıyla başvuranların gizli tıbbi bilgilerinin açıklanmasını gerektirecek acil bir toplumsal gereksinim bulunmadığı halde başvuru rızası alınmaksızın, bilgi verilmeden ve itiraz imkanı tanınmadan kişisel sağlık verilerinin açıklanmasının AİHS'nin 8'inci maddesini ihlal ettiği sonucuna varılmıştır.<sup>151</sup>

#### 4. Kişisel Sağlık Verilerine İlişkin Bilgi Edinme Hakkının ve Erişimin Engellenmesi

4982 sayılı Bilgi Edinme Hakkı Kanununda bilgi, “kurum ve kuruluşların sahip oldukları kayıtlarda yer alan her türlü veri” olarak tanımlanmıştır. Anayasanın bilgi edinme ve kamu denetçisine başvurma hakkını düzenleyen madde 74/3'ü, Bilgi Edinme Kanununu ve “Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar.” şeklindeki Anayasa madde 20/3'ü birlikte yorumlandığında, bireylerin kişisel (sağlık) verilerine erişme ve bilgi edinme hakkına sahip olduğu söylenebilir.

Bu hak, kişisel sağlık verilerinin işlenip işlenmediğini öğrenmeyi de içine alır. Zira bireyin kendisine ilişkin kayıtların işlenip işlenmediği hususunda bilgi edinme özgürlüğüne sahip olması, bireyin kişisel verilerinin işlenmesi karşısında sahip olduğu haklarını kullanabilmesinin bir ön koşuldur.<sup>152</sup>

Bireyin kişisel verilerine erişim hakkı kayıt altına alınan ve işlenen verilerinin doğruluğunu denetleme, düzeltirme, sildirme ve engelleme hakkının da bir gerekliliğidir.<sup>153</sup> 2016/679 sayılı Genel Veri Koruma Tüzüğü'nün 15'inci maddesinde veri sahibinin erişim hakkı, 95/46/EC sayılı Veri Koruma Direktifine benzer şekilde ancak daha kapsamlı olarak düzenlenmiştir.

Kişisel Verilerin Korunması Kanununda ilgili kişinin haklarını düzenleyen madde 11'e göre, “herkes veri sorumlusuna başvurarak kendisiyle ilgili kişisel veri işlenip işlenmediğini öğrenme ve kişisel verileri işlenmişse buna ilişkin bilgi talep etme hakkına sahiptir.” Bu, bireyin hakkı ve dolayısıyla veri sorumlusu olan idarenin de bir yükümlülüğüdür. Nitekim Sağlık Bakanlığının, “sağlık hizmetinin verilmesi, kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis,

<sup>151</sup> Avilkina ve diğerleri / Rusya, Başvuru No: 1585/09, KT. 06/06/2013.

<sup>152</sup> Şimşek (n 15) 145.

<sup>153</sup> Küzeci (n 2) 222; Berrak Yılmaz, ‘Türk Anayasa Mahkemesi ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması’ (Yayımlanmamış Doktora Tezi, Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü 2019) 80, 81.



tedavi ve bakım hizmetlerinin yürütülmesi ile sağlık hizmetlerinin planlanması ve maliyetlerin hesaplanması amacıyla toplayıp işlediği kişisel verilere ilgili kişilerin erişebileceği bir sistem kurma” yetkisi ve görevi bulunmaktadır.<sup>154</sup>

Danıştay, çocukları ölü doğan anne ve baba tarafından doğumun gerçekleştiği hastaneye karşı açılan bir davada, davacılar tarafından birden fazla kez talep edilmesine rağmen, kişisel sağlık verilerinin, “*başta hasta dosyası olmak üzere, epikriz ve ölüm raporlarının davacı tarafa süresinde ve eksiksiz olarak verilmemesinin sağlık hizmetinin geç ve kötü işlediği*” anlamına geldiğini belirtmiştir. Hastanın talep ettiği tıbbi kayıtların yasal süre geçtikten sonra kendisiyle paylaşılmasını hizmetin geç işlemesi, talep ettiği tüm kayıtların kendisiyle paylaşılmamasını ise hizmetin kötü işlemesi olarak görmüştür. Hizmet kusuru teşkil eden bu ihmalin Bilgi Edinme Hakkı Kanununun bilgi ve belgeye erişimi düzenleyen 10’uncu maddesine ve Hasta Hakları Yönetmeliğinin kayıtları inceleme başlıklı 16’ncı maddesine<sup>155</sup> aykırı olduğuna, idarenin hizmet kusuru nedeniyle manevi tazminat ödemesi gerektiğine hükmetmiştir.<sup>156</sup>

Avrupa İnsan Hakları Mahkemesi *K.H. vd./Slovakya* davasında, başvuruçuların vekilleri aracılığıyla kişisel sağlık verilerine ulaşma taleplerinin karşılıksız kalmasını özel hayata saygı hakkının ihlali olarak görmüştür. İki ayrı hastanede sezaryenle doğum yaptıktan sonra bir daha hamile kalamadıklarından doğum sırasında rızaları dışında sterilizasyon operasyonu yapıldığından şüphelenen başvuruçular, vekilleri aracılığıyla kişisel sağlık kayıtlarını incelemek ve hasta dosyalarının fotokopisini almak için hastanelere başvurduklarında olumsuz yanıt almışlardır. Başvuruçular, vekilleri aracılığıyla tıbbi kayıtlarına erişmelerine izin verilmemesinin hukuka aykırı olduğu iddiasıyla iç hukuk yollarını tüketip istedikleri sonucu alamayınca AİHM’ye başvurmuşlardır. AİHM, kişisel sağlık verilerini içeren dosyaya erişmek ve fotokopisini alabilmek için ilgili kişinin haklı bir gerekçe bildirme zorunluluğu olmadığını, aksine bu talebi reddeden makamın bu kararın haklı

<sup>154</sup> 1 sayılı Cumhurbaşkanlığı Kararnamesi,

Madde 378: (2) “Sağlık hizmetinin verilmesi, kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi ile sağlık hizmetlerinin planlanması ve maliyetlerin hesaplanması amacıyla Bakanlık, birinci fıkra kapsamında elde edilen verileri olarak işleyebilir. Bu veriler; Kişisel Verilerin Korunması Kanununda öngörülen şartlar dışında aktarılamaz. (3) Bakanlık, ikinci fıkra gereğince toplanan ve işlenen kişisel verilere, ilgili kişilerin kendilerinin veya yetki verdikleri üçüncü kişilerin erişimlerini sağlayacak bir sistem kurar.”

<sup>155</sup> Madde 16: “Hasta, sağlık durumu ile ilgili bilgiler bulunan dosyayı ve kayıtları, doğrudan veya vekili veya kanuni temsilcisi vasıtası ile inceleyebilir ve bir suretini alabilir. Bu kayıtlar, sadece hastanın tedavisi ile doğrudan ilgili olanlar tarafından görülebilir.”

<sup>156</sup> D15D, E. 2014/5076, K. 2015/2184 KT. 15.4.2015, <https://www.lexpera.com.tr>, (21.08.2021).

gerekçesini bildirmek zorunluluğu olduğunu ifade etmiştir. Ayrıca ulusal mahkemelerin bu bilgilerin fotokopisinin alınmasına izin verilmemesini bu bilgilerin kötüye kullanılmasını önleme amacına dayandığını fakat kişilerin kendi sağlık kayıtlarını nasıl kötüye kullanacakları konusunda inandırıcı bir gerekçe bulunmadığını belirtmiştir. Mahkeme, kişisel sağlık verilerinin üçüncü kişiler tarafından kötüye kullanılmasına engel olmak için bazı önlemler alınmasının gerekli olduğunu ancak bu önlemlerin başvuranların kendi tıbbi kayıtlarının örneğini almalarının engellenmesi şeklinde değil, kişisel sağlık verilerin açıklanma ve üçüncü kişilerle paylaşma şartlarının belirlenmesi ve sınırlandırılması şeklinde olabileceğini belirtmiş ve Sözleşmenin 8'inci maddesinin ihlal edildiğine karar vermiştir.<sup>157</sup>

*Uslu / Türkiye* davasında ise, olay sırasında hükümlü olarak cezaevinde bulunan başvuru, cezaevi revirinde yapılan muayenesinin ardından verilen doktor raporu ve cezaevi reviri kaydının ilgili sayfalarının birer kopyasının kendisine verilmesi talebinde bulunmuştur. Talep cezaevi infaz hakimliği tarafından yerine getirilmiş fakat birkaç gün sonra savcı, “resmi cezaevi dokümanlarının, orijinallerinin veya kopyalarının asayiş ve güvenlik nedeniyle tutuklu veya hükümlülere verilemeyeceği”ne ilişkin hüküm içeren bir genelgeye dayanarak ağır ceza mahkemesine itirazda bulunmuş ve mahkeme kararı ile söz konusu tıbbi kayıtlar geri alınmıştır. Başvurucunun, geri alınma kararına ilişkin itirazı da reddedilmiştir. AİHM, olayda bireyin ve toplumun çatışan çıkarları arasında adil bir denge olup olmadığını değerlendirmiştir. Mahkeme, cezaevi doktoru tarafından verilen rapor ile cezaevi revirine geldiğine dair yapılan kaydın birer kopyasını edinmenin başvuranı ilgilendirdiğini, böylece sağlanacak tedavinin seçiminde uygun bir söz hakkı olacağını belirtmiş ve bireyle toplumun çatışan çıkarları arasında adil bir denge olduğundan söz edebilmek için, tutukluların/hükümlülerin kişisel sağlık verilerinin de içinde bulunduğu resmi dokümanlara erişimine getirilen kısıtlamanın şekli ve hukuki dayanağı konusunda haklı bir gerekçenin olması gerektiğini ifade etmiştir. Sonuç olarak böylesi haklı bir gerekçenin yokluğu bireyle toplumun çatışan çıkarları arasında adil bir dengenin kurulamamasına ve AİHS'nin 8'inci maddesinin, ihlaline sebep olmuştur.<sup>158</sup>

## 5. Kişisel Sağlık Verilerinin Amaç Dışında ve/veya Gereğinden Uzun Süre Tutulması

Kişisel verilerin belli bir amaca bağlı ve bu amaçla sınırlı olarak işlenmesi verilerin toplanmasından başlayarak veri işleme sürecinin her aşamasında aranması gereken temel bir veri koruma hukuku ilkesidir.<sup>159</sup> Bu ilke uyarınca,

<sup>157</sup> K.H. ve diğerleri / Slovakya, Başvuru No: 32881/04, 28.04.2009.

<sup>158</sup> Uslu / Türkiye (no:2), Başvuru No: 23815/04, KT. 20.01.2009.

<sup>159</sup> Başalp (n 20) 37.

veri sorumlusu ve veri işleyen kişisel sağlık verilerini işleme faaliyetini, belirli, açık ve meşru amaçlarla, bu amaçlarla sınırlı olarak ve amacın gerçekleşmesine yetecek kadar veri ile yerine getirmesi gerekir. Aynı zamanda verilerin, amacın gerçekleşmesine yetecek süre kadar muhafaza edilmesi gereklidir.<sup>160</sup>

Amaçla sınırlı olma prensibi, verilerin sadece toplanması aşamasında değil, daha sonra gerçekleştirilen işleme faaliyetlerinde de uygulama alanı bulur. Bir başka ifadeyle verilerin sadece toplanma amacının değil, sonraki işleme amaçlarının da toplanma aşamasında bildirilen amaç ile uyumlu olması aranır.<sup>161</sup>

Amaca bağlı ve sınırlı işleme ile amacın gerçekleşmesine yetecek süre kadar muhafaza etme ilkeleri gereğince, kişisel verilerin toplanma ve kullanma amacının mümkün olduğunca açık şekilde tanımlanması ve belirlenmesi zorunludur.<sup>162</sup> Ayrıca kaydedilen verilerin türü ve kapsamı, kullanma amacı için elverişli ve yeterli derecede olmalı ve gerekli olandan daha fazla kişisel veri toplanmamalı, amaca ulaşıldıktan sonra verinin muhafazasına son verilmelidir.<sup>163</sup> Zira amacın gerektirdiğinden daha uzun süre tutulmaması ilkesinin kabul edilmemesi halinde, bireyler bir kez toplanan bilgilerinin hayat boyu bir yerlerde kayıt altında tutulacağı kaygısına kapılacak ve kişisel verilerin korunması hukukunun dayanağı olan bireyin maddi ve manevi bütünlüğü, özel yaşamın gizliliği gibi temel değerler zarar görecektir.<sup>164</sup>

108 nolu Sözleşmenin 5'inci maddesinde, söz konusu ilkeye uygun şekilde, *“kişisel verilerin belli ve meşru amaçlar için kaydedilebileceği ve bu amaçlara aykırı şekilde kullanılamayacağı ve kaydedilme amaçlarını gerçekleştirmek için gerekli olan süreyi aşmayacak şekilde muhafaza edileceği”* düzenlenmiştir.

2016/679 sayılı Genel Veri Koruma Tüzüğü'nün 5/1-b maddesinde, *“kişisel verilerin belirli, açık ve meşru amaçlara yönelik olarak toplanacağı ve bu amaçlara aykırı bir şekilde işlenmeyeceği”*; 5/1-e maddesinde ise, *“kişisel verilerin işleme amaçlarının gerektirdiğinden daha fazla saklanmaması”* gerektiği belirtilmiştir. Ancak 89/1 maddesi uyarınca, *“kişisel verilerin kamu yararına arşivleme, bilimsel veya tarihi araştırma ya da istatistiki amaçlarla işlenmeleri halinde daha uzun süreler boyunca saklanabileceği”* belirtilmiştir. Tüzük'ün 17. maddesinde ilgili kişilere, toplandığı amaç ile ilgili olarak artık gerekli olmayan kişisel verilerinin silinmesini talep etme hakkı tanınması bu ilkenin en önemli yansıması olarak kabul edilebilir.<sup>165</sup>

6698 sayılı Kişisel Verilerin Korunması Kanununun kişisel verilerin işlenmesine ilişkin genel ilkelerin düzenlendiği 4'üncü maddesinde de, *“belirli,*

<sup>160</sup> Şimşek (n 15) 83; Küzeci (n 2) 215.

<sup>161</sup> Develioğlu (n 7) 46.

<sup>162</sup> Şimşek (n 15) 84.

<sup>163</sup> Şimşek (n 15) 84.

<sup>164</sup> Küzeci (n 2) 215.

<sup>165</sup> Develioğlu (n 7) 50.

açık ve meşru amaçlar için işlenme (4-c)”, “işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma (4-ç)”, “ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme (4-d)” ilkelerine yer verilmiştir. Aynı Kanunun veri sorumluları sicilini düzenleyen 16’ncı maddesinde, “kişisel verileri işleyen gerçek ve tüzel kişilerin veri sorumluları siciline başvuru yaparken diğer kanuni gereklerin yanında, kişisel verilerin hangi amaçla işleneceğini (3-b)” ve “kişisel verilerin işlendikleri amaç için gerekli olan azami süreyi (3-f) bildirme zorunluluğu” bu ilkelerin bir yansımasıdır.

Avrupa İnsan Hakları Mahkemesi, “*S. ve Marper / Birleşik Krallık*” davasında kişisel sağlık verilerinin amacın gerektirdiğinden daha uzun süre tutulmasının özel hayata saygı hakkına aykırı olduğuna karar vermiştir. Dava konusu olay, başvuru S. ve Marper’den bir soruşturma sırasında alınan parmak izi, DNA profili ve hücre örneklerinin soruşturma bittikten sonra da, ulusal veri tabanında belirsiz bir süre boyunca tutulmaya devam edilmesi ile ilgilidir. Başvurucular, delil niteliğinde toplanan bu biyometrik verilerin silinmesini talep etmiş fakat yasaya göre bu verilerin süresiz olarak tutulabileceği gerekçe gösterilerek talepleri reddedilmiştir. Mahkeme beraat eden ya da hakkındaki ceza davası düşen kişilere ait verilerin bir veri tabanında süresiz olarak saklanmasına imkan veren bu uygulamayı özel hayata saygı hakkının ihlali olarak değerlendirmiştir. Söz konusu verilerin toplanması ve tutulmasının suçun işlenmesini önlediği kabul edilse dahi ihlal edilen hukuki değerle arasında adil bir denge olmadığını ve demokratik bir toplumda gerekli kabul edilemeyeceğini belirtmiş, sağlık verilerine ilişkin bu süresiz saklama uygulamasının Sözleşmenin 8’inci maddesini ihlal ettiğine karar vermiştir.<sup>166</sup>

AIHM’nin önüne gelen bir başka dava, başvurunun rızası dahilinde gerçekleşen sezaryenle doğum esnasında rızası alınmaksızın yapılan sterilizasyon operasyonunun üzerinden yedi yıl geçtikten sonra başlatılan idari denetim kapsamında kişisel tıbbi verilerinin elde edilmesi ile ilgilidir. Hastane yönetimi bu işlemten yedi yıl sonra sağlık kuruluşlarındaki sağlık hizmetlerinin kalitesini denetleme yetkisine sahip bir kamu kurumundan (MADEKKI) olay hakkında denetim yapılması talebinde bulunmuştur. MADEKKI yürüttüğü soruşturma kapsamında başvurunun sağlık durumuyla ilgili tüm kişisel verileri (denetim talep eden hastaneden ve hastanın daha önce tıbbi destek aldığı üç farklı sağlık kuruluşundan) herhangi bir ayırım gözetmeksizin toplamıştır. AIHM, topladığı tıbbi kayıtları değerlendirip başvurunun sağlık durumu ile ilgili bir rapor hazırlayan MADEKKI’nin görevlendirilme amacına uygun ve gerekli olup olmadığına bakmaksızın, ilgili kişinin rızası dışında, başvurucuya ait yedi yıl içindeki her tür kişisel sağlık bilgisini toplaması ve işlemesinin AIHS madde 8’in ihlali anlamına geldiğini ifade etmiştir. AIHM, MADEKKI’nin

<sup>166</sup> S. ve Marper / Birleşik Krallık, Başvuru No: 30562/04 ve 30566/04, KT. 4.12.2008.

denetim görevini yerine getirirken hangi kişisel verileri toplayabileceğine ilişkin iç hukukta bir sınırlama getirilmediğini, kuruma tanınan bu yetkinin kapsamı ve sınırlarının belirsiz olduğunu tespit etmiştir. Kurumun olayla doğrudan ilgisi olmayan sağlık verilerini de toplayıp işleyebilmesinin, kanuni düzenlemede keyfiliği önleyecek bir hükmün olmamasına bağlamıştır. Sonuç olarak, Sözleşmenin 8’inci maddesinin ihlal edildiğine karar vermiştir.<sup>167</sup>

## SONUÇ

Açıklandığı, yetkisiz kişilerin eline geçtiği zaman ayrımcılığa ve kötü muameleye maruz kalma riskini bünyesinde barındıran hassas (özel nitelikli) kişisel verilerin elde edilmesi ve işlenmesi, ulusal ve uluslararası düzenlemelerle diğer kişisel verilerden ayrı ve daha katı kurallara bağlanmıştır. Kişisel sağlık verilerinin de, bu kategori içinde yer alan bir veri grubu olarak, işlenme şartlarının, süresinin, yönteminin, amacının işlemeye yetkili kişi/kişi grubunun, geniş yorumlanmaya müsait olmayacak netlikte ve sınırlarının belli olması gerekir. Zira ancak bu şekilde, güçlü bir koruma mekanizmasıyla sağlık verilerinin “hassasiyetleri” gözetilmiş olur. Fakat yürürlükteki Kişisel Verilerin Korunması Kanununda “sağlık ve cinsel hayata ilişkin kişisel verilerin, kamu sağlığının korunması, koruyucu hekimlik, tıbbî 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” şeklindeki düzenleme (m.6/3) ne bu veri grubunun hassas olma niteliğiyle ne de güçlü bir koruma mekanizması oluşturma gerekliliğiyle bağdaşmaktadır. Üstelik söz konusu hüküm hassas kişisel verileri daha güçlü, yüksek standartlarda korumayı amaçlayan Kanun’un genel mantığına da ters düşmektedir. Aynı eleştiriler, 1 sayılı Cumhurbaşkanlığı Kararnamesinin Sağlık Bakanlığının düzenlendiği on ikinci bölümün bilgi toplama, işleme ve paylaşma yetkisi başlıklı 378’inci maddesinin ikinci fıkrası için de geçerlidir. Aynı şekilde kişisel sağlık verilerinin merkezi bir veri kayıt sisteminde toplanması ve işlenmesi bir kamu hizmeti olarak sağlık hizmetinin etkinliği ve verimliliği açısından kabul edilebilir olsa da, bu konuda yapılacak düzenlemelerde yukarıdaki eleştirilerin dikkate alınması gerekir.

Öte yandan bir veri sorumlusu olarak idarenin sağlık verilerini işlerken veri güvenliğini sağlama, kişisel sağlık verileri işlenen bireyleri bu konuda aydınlatma, veri koruma hukukuna uygun hareket edilip edilmediğini denetleme yükümlülüğü vardır. Düzenleme ve denetim yapma Kişisel Verileri Koruma Kurumunun asli görevi olduğu gibi, sağlık verileri özelinde Sağlık Bakanlığının da bir yükümlülüğüdür. İdare bu yükümlülüklerini yerine getirmediği takdirde

<sup>167</sup> L.H. / Letonya, Başvuru No: 52019/07, 29.04.2014.

bir zarar ortaya çıkarsa bu zararı tazmin etmekle mükelleftir. Danıştay ve AİHM içtihatları incelendiğinde kişisel sağlık verileri söz konusu olduğunda, verilerin eksik ya da yanlış kaydedilmesi veya hiç kayıt altına alınmaması, amaç dışı kullanılması, gereğinden uzun süre saklanması, hukuka aykırı olarak üçüncü kişilerle paylaşımı, bireylerin kendi verilerine erişiminin engellenmesi gibi durumların hizmet kusuru kapsamında değerlendirildiği ve idarenin bu yükümlülükleri yerine getirmemesi halinde zararı tazmine hükmedildiği görülmektedir.

## KAYNAKÇA

Akgül A, ‘Kişisel Verilerin Korunması Bağlamında Biyometrik Yöntemlerin Kullanımı ve Danıştay Yaklaşımı’ (2015) 118 TBB Dergisi 199-222.

— —, *Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması* (1. Bası Beta Yayınevi İstanbul 2014).

Aksoy HC, *Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması* (1. Bası Çakmak Yayınevi Ankara 2010).

Akyılmaz B, Sezginer M, Kaya C, *İdare Hukuku* (9. Bası, Savaş Yayınevi Ankara 2018).

Başalp N, ‘Avrupa Birliği Veri Koruması Genel Regülasyonu’nun Temel Yenilikleri’ (2015) 21 Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi 77-106.

— —, *Kişisel Verilerin Korunması ve Saklanması* (1. Bası Yetkin Ankara 2004)

Baykal S, Göçmen İ, ‘Avrupa Birliği Hukukunun Kaynakları Bakımından Normlar Hiyerarşisi’ Prof. Dr. Erdal Onar’a Armağan (2013) 317-365.

Çekin MS, *Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kişisel Verilerin Korunması Kanunu*, (1. Bası On İki Levha İstanbul, 2018).

Develioğlu HM, *Avrupa Birliği Genel Veri Koruma Tüzüğü* (1. Bası On İki Levha İstanbul 2017)

Dülger MV, ‘İnsan Hakları ve Temel Hak ve Özgürlükler Bağlamında Kişisel Verilerin Korunması’ (2018) 1 İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi 71-143.

— —, ‘Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Bağlamında Kişisel Verilerin Ceza Normlarıyla Korunması’ (2016) 2 İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi, 101-167.

— —, ‘Sağlık Hukukunda Kişisel Verilerin Korunması ve Hasta Mahremiyeti’ (2014) 2 İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi 43-80.



Er C, *Biyometrik Yöntemler ve Özel Hayatın Gizliliği Hakkı: Parmak İzi, Göz ve DNA Tarama Gibi Teknolojik Kimlik Denetleme Usullerinin Hukuki Statüsü*, (1. Bası Yetkin Yayınları, Ankara, 2007).

Gonzalez Fuster G, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Springer 2014).

Günday M, *İdare Hukuku* (10. Bası İmaj Yayıncılık Ankara 2013).

Henkoğlu T, *Bilgi Güvenliği ve Kişisel Verilerin Korunması* (1. Bası Yetkin Ankara 2015).

Kaya C, 'Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi' (2011) 1-2 İÜHFM 317-334.

Korkmaz İ, 'Kişisel Verilerin Korunması Kanunu Hakkında Bir Değerlendirme' (2016) 124 Türkiye Barolar Birliği Dergisi 81-152.

Küzeci E, *Kişisel Verilerin Korunması* (3. Bası, Turhan Kitabevi, Ankara, 2019).

Lambert PB, *Understanding the New European Data Protection Rules* (CRC Press New York 2017).

Lynskey O, *The Foundations of EU Data Protection Law* (Oxford University Press 2015).

Lyon D, Bauman Z, *Akışkan Gözetim* (1. Bası Ayrıntı Yayınları 2013).

Memiş T, 'Veri Sorumlusu ve Veri İşleyen Arasındaki İlişkiler ve Sorumluluk Düzeni' (2017) 6 Beykent Üniversitesi Hukuk Fakültesi Dergisi 9-23.

Özdemir H, *Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması* (1. Bası Seçkin Ankara 2009).

Room S, *Data Protection and Compliance in Context* (British Computer Society United Kingdom 2006).

Şimşek O, *Anayasa Hukukunda Kişisel Verilerin Korunması* (1. Bası, Beta Yayınevi İstanbul 2008)

Taştan FG, *Türk Sözleşme Hukukunda Kişisel Verilerin Korunması* (2. Bası On İki Levha İstanbul 2017)

Turan M, *Karşılaştırmalı Hukukta Kişisel Verilerin Korunması* (1. Bası, Adalet Yayınevi Ankara 2017).

Voigt P, Von dem Bussche A, *The EU General Data Protection Regulation (GDPR)* (Springer 2017).

Yılmaz SS, *Tıp Alanında Kişisel Verilerin Açıklanması Suçu* (2. Bası Seçkin Ankara 2017).

Yücel Ö (Ed.), Sert G (Ed.), *Sağlık ve Tıp Hukukunda Sorumluluk ve İnsan Hakları: Sağlık Hizmeti, Sağlık Hakkı ve Hasta Hakları, Medeni Hukuk, Ceza ve İdare Hukuku Yönünden Sorumluluk* (1. Bası Seçkin Ankara 2018).