

HASTANIN KİŞİSEL VERİLERİNİN KORUNMASI VE İDARENİN YÜKÜMLÜLÜKLERİ

*Arş. Gör. Altı YEŞİLYURT**

ÖZET:

Kişisel verilerin korunması ulusal ve uluslararası birçok hukuki metinde kendine yer bulmuş güncelliğini koruyan bir kavramdır. Kişisel sağlık verileri, özellikli koruma gerektiren veri kategorileri arasında sayılmış, bu verilerin işlenmesi özel şartlara bağlanmıştır. Mevzuatımızda, hastanın kişisel verilerinin toplanması, kaydı, saklanması, korunması ile ilgili birtakım düzenlemeler mevcuttur. Çalışmamızda veri koruma hukuku çerçevesinde mevcut düzenlemeler değerlendirilmiş ve etkin koruma için idarenin yükümlülükleri tespit edilmiştir.

Anahtar Kelimeler: Kişisel Veri, Hassas Kişisel Veri, Kişisel Sağlık Verisi, Sağlık Verilerinin Korunması, İdarenin Yükümlülükleri

ABSTRACT:

The protection of personal data is a concept that preserves the actuality found itself in many national and international legal texts. Personal health data have been counted among the categories of data which require special protection, the processing of this data is connected to specific conditions. The patient's personal data collection, registration, number of regulations related to the preservation and protection is available in Turkish Law System. In this context, these notions/ duties has been interpreted and designated within the framework of data protection law and designated requirements for effective protection.

Keywords: Personal Data, Sensitive Personal Data, Personal Health Data, Protection of Health Data, Obligations of Administration

* Erciyes Üniversitesi Hukuk Fakültesi İdare Hukuku Anabilim Dalı.

GİRİŞ

Teknolojinin ve hukukun gelişmesine bağlı olarak daha önce tartışılmayan yeni kavramlar hukuk terminolojisine girmektedir. Kişisel verilerin korunması da bu kavramlardan biridir.

Hukuk sistemlerinde kişilik en yüksek ve saldırılara en açık değer olarak kabul edilmektedir. Bu bakımdan hukuk sistemleri, kişiliğe saygı ile kişilik hakkının saldırı öncesi ve sonrası korunması için gerekli tedbirleri almak zorundadır¹. “Belirli veya kimliği belirlenebilir olmak şartıyla bir kişiye ilişkin bütün bilgileri”² ifade eden kişisel veri kavramının da gerek kişiliğin korunması gerek özel hayat kapsamında saldırılara karşı korunması gerekmektedir.

Anayasamızın 65. maddesi devlete; bireylere sağlık hizmetlerinin sunulması ve bireylerin sağlığının korunması bakımından büyük bir mükellefiyet yüklemiştir. İdarenin bu yükümlülüğü yerine getirmekten imtina etmesi düşünülemez³. Söz konusu sağlık hizmetinin sunumu sırasında birey hakkında birçok bilgi toplanmakta ve işlenmektedir. Toplanan bu bilgiler kişisel veri niteliğinde bilgilerdir. Kişisel verilerden bir kısmı diğer kişisel veri türlerine göre daha etkin koruma gerektirmektedir. Bu veri türüne “hassas kişisel veri”⁴ denilmektedir. Kişinin sağlık verileri de hassas veri kapsamında değerlendirilmektedir. Bu nedenle sağlık verilerinin diğer veri türlerine göre daha özel ve etkin şekilde korunması gerekmektedir.

Her ne kadar mevzuatımızda kişisel sağlık verilerin korunması konusunda idareye etkin tedbirler alma ödevi yükleyen pozitif hukuk kuralları yürürlükte olmasa da Anayasa m.20’de ve uluslararası belgelerde yer alan düzenlemeler, çeşitli kanunlarda yer alan özel hükümler ve etik kuralları gereği idare sağlık hizmetinin sunumu nedeniyle kayıt altına alınan kişisel verilerin mahremiyetini,

¹ **Mustafa Dural/Tufan Ögüz**, Türk Özel Hukuku C.II Kişiler Hukuku, İstanbul 2009, s.93.

² 24 Temmuz 2012 tarihli ve 28363 sayılı Resmi Gazete’de yayımlanan Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmeliğin 3. maddesinde, Avrupa Birliği tarafından çıkarılan 95/46/EC sayılı “Bireylerin Kişisel Verilerinin İşlenmesi ve Serbestçe Dolaşımı Karşısında Korunmasına İlişkin Direktif”in 2/a maddesinde, “Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair 108 sayılı Avrupa Konseyi Sözleşmesi”nin 2(a) maddesinde, OECD tarafından 1980 yılında yayımlanan Rehber İlkelerin 1/b maddesinde kişisel veri yukarıda belirtilen şekilde tanımlanmıştır.

³ **Fatih Birtek**, “Sağlık Hizmetlerinin Yürütülmesinde İdarenin Kusura Dayanan Sorumluluğu”, Erciyes Üniversitesi Hukuk Fakültesi Dergisi, C. 2, S. 3-4, Y. 2007, s.123.

⁴ Bu adlandırma Avrupa Birliği uygulamasında görülmektedir. Avrupa Birliği Direktifi’nin 8. maddesi, “Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşme”nin 6. maddesi ve “Kişisel Verilerin İşlenmesi ve Bu Verilerin Transferi Konusunda Bireylerin Korunması Hakkında Avrupa Birliği Direktifi”nin 8. maddesi hassas kişisel veri kategorisine yer veren düzenlemelerdir.

gizliliğini ve güvenliğini sağlamalı, hukuka aykırı olarak kullanımını engelleyecek denetimleri yapmalı, gerekli tedbirleri almalıdır.

I. KİŞİSEL VERİ

Ulusal ve uluslararası birçok hukuki metinde tanımlandığı şekliyle kişisel veri; “*belirli veya belirlenebilir nitelikteki bir kişiye ilişkin her türlü bilgi*”yi ifade etmektedir⁵. Avrupa Birliği’nde kişisel verilerle ilgili ilk düzenleme olan 1995/46 sayılı Direktif’in 2. maddesinde kişisel veri; “*Kimliği belirtilen veya belirlenebilen bir kişiyle ilgili bilgi*” olarak tanımlanmıştır. 2008 yılında Bakanlar Kurulu tarafından kararlaştırılıp Meclise sunulan ancak hala görüşülmeyi bekleyen Kişisel Verilerin Korunması Kanunu Tasarısı⁶ m.3’te kişisel veri; “*belirli veya kimliği belirlenebilir gerçek ve tüzel kişilere ilişkin bütün bilgiler*” şeklinde tanımlanmışken; 26.12.2014 tarihinde meclise sunulan Tasarının⁷ 3. maddesinde kişisel veri; “*kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi*” şeklinde tanımlanmıştır⁸.

A. Kişisel Verinin Unsurları

Ulusal ve uluslararası metinlerde genel olarak tanımlandığı şekliyle kişisel verinin üç temel unsuru vardır; veri, kimliği belirli veya belirlenebilir kişi ve verinin kişiye ait olması. Uluslararası belgelerde kişisel veri, “*personal data*” olarak ifade edilmiştir. Burada yer alan “*data*” ifadesi Türkçe’ye kimi araştırmacılar tarafından “*veri*” kimileri tarafından ise “*bilgi*” olarak çevrilmiştir. Collins terimler sözlüğünde “*data*”, Türkçe’ye “*veri*” olarak çevrilmiştir⁹. Veri

⁵ 24 Temmuz 2012 tarihli ve 28363 sayılı Resmi Gazete’de yayımlanan Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmeliğin 3. maddesinde, “Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair 108 sayılı Avrupa Konseyi Sözleşmesi”nin 2(a) maddesinde, OECD tarafından 1980 yılında yayımlanan Rehber İlkelerin 1/b maddesinde kişisel veri yukarıda belirtilen şekilde tanımlanmıştır.

⁶ Adalet Bakanlığı tarafından hazırlanan, Bakanlar Kurulunca 7.04.2008 tarihinde kararlaştırılan, 22.04.2008 tarihinde meclise sunulan Kişisel Verilerin Korunması Kanunu Tasarısı, <http://www2.tbmm.gov.tr/d23/1/1-0576.pdf>, E.T. 25.09.2014.

⁷ Adalet Bakanlığı tarafından hazırlanan, Bakanlar Kurulunca 3.11.2014 tarihinde kararlaştırılan, 26.12.2014 tarihinde meclise sunulan Kişisel Verilerin Korunması Kanunu Tasarısı, <http://www2.tbmm.gov.tr/d24/1/1-1009.pdf>, E.T. 25.01.2015.

⁸ Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik’te kişisel veri şu şekilde tanımlanmıştır; “*Kişisel veri: Belirli veya kimliği belirlenebilir gerçek ve tüzel kişilere ilişkin bütün bilgileri*” ifade eder. <http://www.mevzuat.gov.tr/Metin.Aspx?MevzuatKod=7.5.16405&MevzuatIliski=0&sourceXMLSearch=E.T.25.09.2014>.

⁹ Collins Terimler Sözlüğü, <http://www.collinsdictionary.com/dictionary/english/data?showCookiePolicy=true> E.T. 25.09.2014.

kavramı hem bilgiyi hem de birtakım sayısal değerleri kapsar. Sayısal değerler de kişiyi tanımlamaya yaramaktadır. Mesela telefon numarası, IP adresi sayısal bir değerdir ve kişiyi tanımlamaya elverişlidir. Bilgiyle birlikte kişiyi tanımlayan sayısal değerlerin de koruma altına alınması gerektiği için kanaatimizce de “bilgi” yerine “veri” kavramının kullanılması daha uygundur.

1. Veri ve Bilgi Kavramları

Kişisel veri kavramının temel unsurunu oluşturan veri kavramının anlamını ve bilgi ile enformasyon kavramları arasındaki farkı ortaya koymak gerekmektedir. Bu nedenle enformasyon ve bilgi kavramını tanımlayacak olursak; anlamının geniş kapsamlı ve çok yönlü olması sebebiyle bilgi kavramı üzerinde genel bir tanım olmamakla birlikte¹⁰ Türk Dil Kurumu Güncel Sözlükte bilgi; “bilgi işlemde kullanılan uzlaşım kurallarından yararlanarak kişinin veriye yönelttiği anlam” şeklinde tanımlanmıştır¹¹. Enformasyon; “danışma, tanıtma, haber alma, haber verme, haberleşme”¹², veri ise “olgu kavram ya da komutların iletişim, yorum ve işlem için elverişli biçimsel ve uzlaşım bir gösterimi” olarak tanımlanmıştır¹³. Enformasyon ve bilgiye temel teşkil eden veri, tek başına bir anlam ifade etmese de belirli bir hedef doğrultusunda işlem den geçirildikten sonra işlevsel hale gelmektedir¹⁴.

Veri; “bireyin şahsi, mesleki ve ailevi özelliklerini gösteren, o bireyi diğer bireylerden ayırmaya ve niteliklerini ortaya koymaya elverişli her türlü bilgi” anlamına gelmektedir¹⁵. Kişisel veri tanımındaki her türlü bilgi kavramı oldukça geniş kapsamlı bir ifadedir. 2008 tarihli Kişisel Verilerin Korunması Kanunu Tasarısı 3. madde gerekçesinde¹⁶; kanun kapsamına giren kişisel verilerin yalnızca

¹⁰ **Atıla Erkal**, “Genel Olarak Bilgi ve Bilgi Teorisi Çerçevesinde Bilginin Hukuktaki Anlamı”, Selçuk Üniversitesi Hukuk Fakültesi Dergisi, C. 17, S. 2, Y. 2009, s.26.

¹¹ TDK Bilim ve Sanat Terimleri Ana Sözlüğü, http://tdk.gov.tr/index.php?option=com_bilimsanat&view=bilimsanat&kategoriget=terim&kelimeget=bilgi&hngget=md E.T. 26.09.2014.

¹² TDK Güncel Türkçe Sözlük, http://tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.54d34ee8a6f215.54002657 E.T. 26.09.2014.

¹³ TDK Bilim ve Sanat Terimleri Ana Sözlüğü, http://tdk.gov.tr/index.php?option=com_bilimsanat&arama=kelime&guid=TDK.GTS.54d34e33320787.42806138 E.T. 26.09.2014.

¹⁴ **Ahmet Boz**, “Kişisel Verilerin Korunması: Türkiye ABD ve AB Önemleri”, Polis Akademisi Güvenlik Bilimleri Enstitüsü Güvenlik Stratejileri ve Yönetimi Anabilim Dalı, (Yüksek Lisans Tezi), Ankara 2014, s.6-7.

¹⁵ **Ersan Şen**, “Kişisel Verilerin Korunması Kanunu Tasarısı’nın Anayasa ve Türk Ceza Kanunu Hükümleri Çerçevesinde Değerlendirilmesi”, İstanbul Barosu Dergisi, C. 83, S. 3, Y. 2009, s.1197.

¹⁶ Adalet Bakanlığı tarafından hazırlanan, Bakanlar Kurulunca 7.04.2008 tarihinde kararlaştırılan, 22.04.2008 tarihinde meclise sunulan Kişisel Verilerin Korunması Kanunu Tasarısı Madde Gerekçesi, <http://www2.tbmm.gov.tr/d23/1/1-0576.pdf>, E.T. 26.09.2014.

bireyin adı, soyadı, doğum tarihi ve doğum yeri gibi onun kesin teşhisini sağlayan bilgileri değil, aynı zamanda kişinin akli, psikolojik, fiziki, kültürel, sosyal ve sair özelliklerine ilişkin bilgileri de kapsadığı belirtilmiştir. Yani bir kimsenin özel hayatı ve aile yaşamına ilişkin bilgiler kişisel veri niteliği taşıdığı gibi bu kimsenin iş ilişkileri ile ekonomik ve sosyal yaşamına ilişkin bilgiler de kişisel veri olarak kabul edilmelidir¹⁷. Mesela kişinin öğrenimine, işine, görevine, gelirin, borçlarına, mallarına, eserlerine, görüşlerine, düşüncelerine, inançlarına vb. ilişkin bilgiler kişisel veri kavramına dâhildir. Yine telefon numarası¹⁸, elektronik posta adresi, parmak izi, DNA, adres, sosyal güvenlik numarası, hesap numarası¹⁹, fotoğrafı²⁰, banka bilgileri, sosyal ağ web sitelerindeki mesajları²¹, IP numarası²² kişisel veri kapsamındadır²³. Bu bilgilerden kişinin etnik kökeni, dini, inancı, sağlığı, cinsel yaşamı, siyasal görüşleri özel nitelikleri dolayısıyla duyarlı bilgiler

¹⁷ **Hüseyin Can Aksoy**, Medeni Hukuk ve Özellikle Kişiler Hukuku Yönünden Kişisel Verilerin Korunması, Ankara 2010, s.13.

¹⁸ Yargıtay 12. CD.'nin 10.06.2013 tarihli kararına göre "...sanağın, eşiyle ilişkisi olduğunu düşündüğü, katılan adına arkadaşlık sitelerinde üyelik işlemleri yaparak, elektronik posta adresi oluşturduğu sitelerde, katılanın bilgisi ve rızası dışında, ona ait cep telefonu ve evde kurulu telefon numaraları ile msn adresini yazıp, katılanın fotoğraflarını koyduğunun iddia edilmesi karşısında, kanıtlanması halinde eylemin, 5237 Sayılı TCK'nın 136/1. maddesinde tanımlanan verileri hukuka aykırı olarak verme veya ele geçirme suçunu oluşturacağı..." belirtilmiştir. Yargıtay 12. CD. E. 2012/19748, K. 2013/15776, T. 10.06.2013, (Kazancı İçtihat Bilgi Bankası, <http://www.kazanci.com/kho2/ibb/giris.htm> E.T. 26.09.2014).

¹⁹ **Doğan Kılınç**, "Anayasal Bir Hak Olarak Kişisel Verilerin Korunması", AÜHFD, 61 (3) 2012, s.1094.

²⁰ Yargıtay 12. CD. 11.9.2012 tarihli kararında kişinin görüntüsünü kişisel veri saymıştır ve kararda şu şekilde ifade edilmiştir: "...bir özel hayat görüntüsü ya da sesinin, kişisel veri olduğunda kuşku bulunmamaktadır...". Yargıtay 12. CD. E. 2012/17703, K.2012/18222, T.11.09.2012, (Kazancı İçtihat Bilgi Bankası, <http://www.kazanci.com/kho2/ibb/giris.htm> E.T. 26.09.2014).

²¹ **Aydın Akgül**, "Danıştay Kararları Işığında Kişisel Sağlık Verilerin Korunması", Danıştay Dergisi, Sayı:133, Yıl: 2013, s.24.

²² Avrupa Adalet Divanı'nın Promusicae kararına göre, "bilgisayar IP numarası" da kişisel veri kapsamındadır. Açıklama için bkz. **Aydın Akgül**, Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması, İstanbul 2014, s.41.

²³ Yargıtay 12. CD.'nin 10.06.2013 tarihli kararında "kişisel veri" kavramı açık bir biçimde tanımlanmıştır. Karara göre "*kişisel veri*" kavramından, kişinin, yetkisiz üçüncü kişilerin bilgisine sunmadığı, istediğinde başka kişilere açıklayarak ancak sınırlı bir çevreyle paylaştığı nüfus bilgileri (TC kimlik numarası, adı, soyadı, doğum yeri ve tarihi, anne ve baba adı gibi), adli sicil kaydı, yerleşim yeri, eğitim durumu, mesleği, banka hesap bilgileri, telefon numarası, elektronik posta adresi, kan grubu, medeni hali, parmak izi, DNA'sı, saç, tükürük, tırnak gibi biyolojik örnekleri, cinsel ve ahlaki eğilimi, sağlık bilgileri, etnik kökeni, siyasi, felsefi ve dini görüşü, sendikal bağlantıları gibi kişinin kimliğini belirleyen veya belirlenebilir kılan, kişiyi toplumda yer alan diğer bireylerden ayıran ve onun niteliklerini ortaya koymaya elverişli, gerçek kişiye ait her türlü bilginin anlaşılması gerekir)." Yargıtay 12. CD. E. 2013/10672, K. 2013/15772, T. 10.06.2013, (Kazancı İçtihat Bilgi Bankası, <http://www.kazanci.com/kho2/ibb/giris.htm>, E.T. 26.09.2014).

sayılır ve daha katı koruma önlemlerine tabi tutulur²⁴. Bir “veri”nin “kişisel veri” olarak kabul edilebilmesi için, “bir kişiyi tanımlaması, onu diğerlerinden ayırması ve bir kimsenin kendine has bazı özelliklerini ortaya koyması” gerekmektedir²⁵. Bu bağlamda kişisel veriler, özünde bireyin kimliğini ortaya çıkartan, bir kişiyi belirli kılan ve onu karakterize eden verilerdir²⁶.

Bilginin nesnel veya öznel nitelikte olması, o bilginin kişisel veri niteliği taşıyıp taşıyamaması açısından önemli olmadığı gibi herhangi bir bilginin kişisel veri niteliği taşıması için gerçeklik veya doğruluğunun kanıtlanmış olması koşulu da aranmamaktadır²⁷.

Değinilmesi gereken bir husus da verilerin işlenmesi konusudur. Tasarıda kişisel verilerin işlenmesi: “*Kişisel verilerin tamamen veya kısmen, otomatik olan veya olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, elde edilebilir hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi ifade eder*” şeklinde tanımlanmıştır²⁸.

Tasarının 3. madde gerekçesinde belirtildiği gibi kişisel verilerin işlenmesi kavramı geniş bir alanı kapsamaktadır, buna göre kişisel verilerin toplanmasından başlayarak tüm işlem türleri tanım kapsamına girmekte ve kişisel verilerin korunması yalnızca dijital ortamda bulunanları değil, elle tutulan bilgileri de kapsamaktadır²⁹.

2. Kimliği Belirli veya Belirlenebilir Bir Kişi

a. Kişi Kavramı

Kişisel verilerin korunması kapsamında kişi kavramına kimlerin gireceğine ilişkin olarak uluslararası doktrinde ve mevzuatta görüş birliği bulunmamaktadır³⁰. Nitekim Avrupa Birliği ülkelerinin kişisel verilere ilişkin kanunlarındaki kişisel veri tanımlarında bilginin kiminle ilişkili olduğuna yönelik kişi kavramı birbirinden farklılık göstermektedir³¹.

²⁴ Adalet Bakanlığı tarafından hazırlanan, Bakanlar Kurulunca 3.11.2014 tarihinde kararlaştırılan, 26.12.2014 tarihinde meclise sunulan Kişisel Verilerin Korunması Kanunu Tasarısı 6. madde Gerekçesi, <http://web.tbmm.gov.tr/gelenkagitlar/metinler/362939.pdf> E.T. 10.01.2015.

²⁵ Hale Akdağ, Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması, Ankara 2013, s.6.

²⁶ Akgül, Kişisel Sağlık Verileri, s.24.

²⁷ Aksoy, s.16.

²⁸ Adalet Bakanlığı tarafından hazırlanan, Bakanlar Kurulunca 3.11.2014 tarihinde kararlaştırılan, 26.12.2014 tarihinde meclise sunulan Kişisel Verilerin Korunması Kanunu Tasarısı m.3.

²⁹ Adalet Bakanlığı tarafından hazırlanan, Bakanlar Kurulunca 3.11.2014 tarihinde kararlaştırılan, 26.12.2014 tarihinde meclise sunulan Kişisel Verilerin Korunması Kanunu Tasarısı Madde Gerekçesi.

³⁰ Bu konudaki tartışmalar ve görüşler hakkında bakınız, Aksoy, s.18.

³¹ Akgül, Kişisel Verilerin Korunması, s.14.

Kişisel veriler gerçek kişilerle ilgili olabileceği gibi tüzel kişilerle de ilgili olabilir. Ancak gerçek ve tüzel kişilerin aynı hukuki korumaya tabi tutulup tutulmaması konusu tartışmalıdır³². Bu durum veri koruma yasalarında ilgili kişi konusundaki düzenleme farklılıklarının altında yatan sebeptir. Bazı yazarlar, verilerin işlenmesinden etkilenen menfaatlerin yalnızca gerçek kişilerin menfaatleriyle sınırlı olmadığını tüzel kişilerin de koruma kapsamına alınması gerektiğini savunmaktadır³³. Aksi görüşe göre ise özel hayat yalnızca gerçek kişilerle ilgilidir, tüzel kişiler içinse ticari gizliliğin korunması söz konusudur. Bu nedenle sadece gerçek kişilerin bu korumadan yararlanması gerekmektedir³⁴. Kanaatimizce şirket, banka gibi tüzel kişilerin verileri ticari sır kapsamında korunmaktadır. Bu nedenle kişisel verilerin korunmasına kapsamında “kişi” kavramına dahil edilmemelidir. Ancak dernek, vakıf gibi kar amacı gütmeyen tüzel kişiler kişisel verilerin korunması kapsamında korumaya tabi tutulmalıdır. Mesela bir derneğin üyelerinin kim olduğu, kimlerin bağış yaptığı bilgisi derneğin kimliğini belirli kılıp, karakterize edebilecek niteliktedir. Bu nedenle dernek, vakıf gibi kar amacı gütmeyen tüzel kişilerin korumadan yararlanması gereklidir.

Hastanın kişisel verileri başlığı altında hastanın ancak gerçek kişi olabileceği bilgisinden yola çıkarsak veri koruması kapsamına tüzel kişilerin dahil olup olmaması gerektiği konusunu tartışmaya gerek yoktur.

Son olarak değinilmesi gereken konu kişisel verilerin korunması kapsamına ölmüş kişilerin dahil olup olmadığı hususudur. Direktif kişisel verilerin yalnızca gerçek kişilerle ilgili olduğunu kabul etmişse de ülkeler iç hukuklarında direktifi genişletici düzenleme yapabilirler. Nitekim bu konuda birçok ülke farklı düzenlemeler getirmiştir³⁵. Hasta hakları yönetmeliği mahremiyet ölümle bitmez demektir(m.21/3). Kanaatimizce ölmüş kimseler de koruma kapsamında olmalıdır.

b. Kimliği Belirli veya Belirlenebilir Olmak

Bir kişinin belirli veya belirlenebilir olması, mevcut verilerin herhangi bir şekilde bir gerçek kişiyle ilişkilendirilmesi suretiyle, o kişinin tanımlanabilir hale getirilmesini ifade eder. Yani verilerin kişinin fiziksel, ekonomik, kültürel,

³² **Durmuş Tezcan**, “Bilgisayar Karşısında Özel Hayatın Korunması”, Anayasa Yargısı Dergisi, C.8, Y. 1991, s.389.

³³ **Douwe Korff**, “Study on The Protection of The Rights and Interests of Legal Persons With Regard to the Processing of Personal Data Relating to Such Persons”, Final Report, Commission of the European Communities, http://ec.europa.eu/justice/data-protection/document/studies/files/20000202_rights_interests_legal_en.pdf, s.43, E.T. 30.09.2014.

³⁴ **Tezcan**, s.389.

³⁵ **Aksoy**, s.20.

sosyal veya psikolojik kimliğini ifade eden somut bir içerik taşıması veya kimlik, vergi, sigorta numarası gibi herhangi bir kayıtle 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 verilerdir³⁶.

Kişinin kimliğini belirlemede temel nokta isminin bilinip bilinmemesi değil, grup içinde diğerlerinden ayırt edilebilmesidir. Herhangi bir ölçütün bir kimseyi diğerlerinden ayırt edilebilir kılıp kılmayacağı her somut olayın özellikleri çerçevesinde ele alınmalıdır. Örneğin yaygın bir soyadı bir kişiyi sınıftaki diğer öğrenciler arasında belirlenebilir kılmaya yeterliyken bütün ülke çapında belirlenebilir kılmada yeterli değildir. Hatta siyah giyinmiş adam ifadesi gibi belirsiz bir bilgi kimliği belirlenebilir kılma niteliğinde olmamakta birlikte, trafikte bekleyenler arasında bir kişiyi belirlenebilir kılacaktır³⁷. Aynı şekilde kişinin ayakkabı numarası, eşinin mesleği tüm ülkede kişiyi belirli kılmaya yeterli değilken³⁸, belli bir grup içinde kişiyi belirlenebilir kılmaya yeterlidir. Bu yüzden herhangi bir bilginin kişiyi belirlenebilir kılıp kılmayacağı meselesi her somut olay bakımından ayrıca değerlendirilmelidir.

Belirlenebilir olma konusunda isimsiz (anonymous), isimsizleştirilmiş (anonymised) ve takma isimli (pseudonymised) verilere de değinilmesi gerekmektedir. İsimsiz verilerle bir kişinin kimliğini belirli kılmak mümkün değildir. İsimsizleştirilmiş veriler belirli bir kişiyle ilgilidir, bilginin kimle ilgili olduğu belli değildir ancak kişinin kimliği tespit edilebilir. Takma isimli verilerde bilginin kime ait olduğu yalnızca ilgili kod çözümlenerek belirlenebilir³⁹. İsimsiz verilerde kişiye direkt ve dolaylı erişim alanlarını tümüyle yok edilmiştir. Bu açık bir şekilde isim, vatandaşlık numarası, telefon numarasını, posta kodunu, semti yok etme şeklinde olabilir. İsimsizleştirilmiş ve takma isimli verilerde ise, kişi bağlantısı yok edilmiştir. Kişi bağlantısını yok etme kişiye direkt ve dolaylı erişim alanlarını tümüyle yok etmeyip, ana veri tabanından başka bir yerde saklamadır; yani veri tabanı ikiye bölünür. Fakat aslında yok etme değil, verilerin

³⁶ Adalet Bakanlığı tarafından hazırlanan, Bakanlar Kurulunca 7.04.2008 tarihinde kararlaştırılan, 22.04.2008 tarihinde meclise sunulan Kişisel Verilerin Korunması Kanunu Tasarısı 3. madde Gerekçesi.

³⁷ **Douwe Korff**, "Comparative Study on Different Approaches to New Privacy Challenges in Particular in the Light of Technological Developments", Working Paper no:2, Commission of the European Communities, http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_working_paper_2_en.pdf s.45-46, E.T. 01.10.2014.

³⁸ Bazı meslekler kişinin eşini tüm ülke çapına belirli kılabilir. Cumhurbaşkanlığı, Başbakanlık, Bakanlık gibi.

³⁹ **Korff**, New Privacy Challenges, s.48.

başka bir yerde saklanması söz konusudur⁴⁰. Yani isimsiz verilerde kimliği belirlemek mümkün değildir. İsimlendirilmiş verilerde kimlik belirlenebilir, takma isimli veriler ise kodlar aracılığıyla çözülebilir⁴¹. Bu nedenle isimsiz verilerin koruma altına alınması gerekmemekle birlikte isimlendirilmiş ve takma isimli veriler koruma altına alınmalıdır.

II. HASSAS KİŞİSEL VERİLER

Bazı veriler başkalarınca öğrenilmeleri halinde özellikleri gereği ilgili kişinin mağduriyetine yol açabilecek ve ayrımcılık tehlikesi oluşturacak nitelikte hassas verilerdir. Kişisel Verilerin Korunması Kanunu Tasarısı 6. maddede özel niteliği olan kişisel veriler sayılmakta ve genel kural olarak bu verilerin işlenmeyeceği düzenlenmektedir. Buna göre kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, dernek, vakıf veya sendika üyeliği, sağlığı veya cinsel hayatıyla ilgili veriler özel niteliği olan veri olarak kabul edilmektedir. Özel nitelikteki verilere dolaylı da olsa erişim imkanı veren veriler de madde kapsamındadır⁴².

Avrupa Birliği Direktifi 8. maddesinde de genellikle hassas veri olarak tabir edilen genel durumun çok üstünde hukuki korumaya tabi tutulan veriler olduğundan bahsedilmektedir. Bu veriler; ırk veya etnik köken, politik görüş, din, felsefi düşünce, sendikal üyelik, sağlık verileri, cinsel sorunlardır⁴³.

Avrupa Konseyi'nin düzenlemelerinden "Biyoloji ve Tıbbın Uygulanması Bakımından İnsan Hakları ve İnsan Haysiyetinin Korunması Sözleşmesi"⁴⁴ ve "Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şa-

⁴⁰ **Melih Kırılıdoğ**, "Elektronik Sağlık Kayıtlarında Teknolojik Gelişmeler, Kullanım Alanları, Amaç ve Yasa Dışı Kullanımlar", Kişisel Sağlık Verilerine Mesleki Yaklaşımlar Çalıştayı, İstanbul 2013, s.65.

⁴¹ **Korff**, New Privacy Challenges, s.48.

⁴² Adalet Bakanlığı tarafından hazırlanan, Bakanlar Kurulunca 3.11.2014 tarihinde kararlaştırılan, 26.12.2014 tarihinde meclise sunulan Kişisel Verilerin Korunması Kanunu Tasarısı 6. madde gerekçesi.

⁴³ **Korff**, New Privacy Challenges, s.73.

⁴⁴ Madde 10. (Özel yaşam ve bilgilendirilme hakkı)

"1. Herkes, kendi sağlığıyla ilgili bilgiler 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. İstisnai durumlarda, 2'nci paragrafta belirtilen hakların kullanılmasında hastanın yararları bakımından kanun tarafından kısıtlamalar öngörülebilir."

hısların Korunmasına Dair Sözleşme"⁴⁵ tıbbi veriler açısından koruma sağlayan ve hastanın verilerini özellikli veri kategorisinde sayan düzenlemelerdir.

Yargıtay 12. Ceza Dairesi'nin 15.5.2012 tarihli kararında sağlıkla ilgili verilerin hassas veri olduğu ifade edilmiştir⁴⁶.

Kişisel sağlık verileri nitelikleri itibarıyla hassas kişisel veri kategorisinde yer almaktadır. Hassas veri kategorisinde yer alan veriler, diğer verilere göre daha sıkı koruma tedbirleriyle korunmaktadır. Bu nedenle hastanın hangi verilerinin kişisel veri kapsamına dâhil olduğunun saptanması korumadan yararlanacak verilerin tespiti bakımından önemlidir.

A. Hassas Veri Olarak Hastanın Kişisel Verileri

Hastanın⁴⁷ kişisel verileri, hastaya ait olup da sağlık meslek mensubuna aktarılan veya herhangi bir şekilde bu kişiler tarafından hukuka uygun olarak öğrenilen ve hastanın başkaları tarafından duyulmasını istemeyeceği bilgileri şeklinde ifade edilebilir⁴⁸.

2002 yılında Washington'da yapılan Dünya Hekimler Birliği (DHB) Genel Kurulu'nda kabul edilen bildirmede kişisel sağlık bilgileri, "*kişinin bedensel ya da zihinsel sağlığına ilişkin kayıtlı edilmiş tüm bilgiler*" olarak tanımlanmıştır⁴⁹.

Mahremiyet kurallarının koruduğu sağlık bilgileri, bireye ilişkin bilinebilir sağlık verileri olarak ifade edilmekte ve bu kapsamda cinsiyete ilişkin bilgiler de dâhil de olmak üzere bireyin geçmiş, mevcut ve gelecekteki fiziksel veya

⁴⁵ Madde 6 (Özellikli veri kategorileri)

"İç hukukta uygun güvenceler sağlanmadıkça, ırk menşesini, politik düşünceleri, dini veya diğer inançları ortaya koyan kişisel nitelikteki verilerle sağlık veya cinsel yaşamla ilgili kişisel nitelikteki veriler ve ceza mahkumiyetleri, otomatik bilgi işlemine tâbi tutulamazlar.

⁴⁶ Yargıtay 12. Ceza Dairesi, 15.05.2012 tarihli karar; "*sağlık verileri kişilerin iş güvenliğini, toplum içindeki statüsünü ve sigorta kapsamını etkileyen hassas bilgilerdir. Ayrıca sağlık verileri kişilerin sosyal yaşantısı ve psikolojik durumları hakkında bilgi edinilmesine neden olabilir. Biyometrik (Kişinin kendine özgü fiziksel veya biyolojik niteliklerine dayalı olarak insanların kimliğini tespit için dijital teknolojiye dayalı olarak kullanılan veriler de kişisel veriler arasındadır...*". Yargıtay 12. CD. E. 2011/20072, K. 2012/12126, T. 15.05.2012, (Kazancı İçtihat Bilgi Bankası, <http://www.kazanci.com/kho2/ibb/giris.htm> E.T. 02.10.2014).

⁴⁷ "Hasta" kavramı, Hasta Hakları Yönetmeliği 4/1-b bendinde tanımlanmıştır. Buna göre; "*Hasta: Sağlık hizmetlerinden faydalanma ihtiyacı bulunan kimseyi*" ifade eder. Hasta kavramı yalnızca tedavi olan kişileri ifade etmez. Bu kişiler yanında teşhis ve tanı için sağlık kurumlarına başvuranları da kapsar. Bu bağlamda

6331 sayılı İş Sağlığı ve Güvenliği Kanunu 15. maddesi uyarınca sağlık raporu almak için sağlık kurumuna başvuran kişi de hasta kapsamında değerlendirilmelidir.

⁴⁸ **Hakan Hakeri**, Tıp Hukuku, Ankara 2013, s.798.

⁴⁹ Dünya Hekimler Birliği Sağlıkla İlgili Veri Tabanına İlişkin Bildirge, <http://www.ttb.org.tr/TD/TD109/23.php>, E.T. 02.10.2014.

ruhsal sağlık durumu, bireye sağlık hizmeti sağlanması veya bireye sağlanan sağlık hizmeti için geçmişte, hâlihazırda ya da gelecekte yapılacak ödemeleri kapsadığı gibi birçok genel tanıtıcıları da kapsamaktadır (ad, adres, doğum tarihi, sosyal sigorta numarası gibi)⁵⁰.

Healthcare Information and Management Systems Society (HIMSS) tarafından yapılan tanıma göre kişisel veri kapsamına kişinin kimlik bilgileri yanı sıra hastanın cinsiyeti, progres notları, sorunlar, tedaviler, yaşam belirtileri (hayati bulgular, uyarılar), tıbbi özgeçmiş, bağışıklamalar, laboratuvar verileri ve radyoloji raporları ile bedenine ilişkin biyolojik-genetik bilgileri (hücre, uzuv, kan ve DNA) girmektedir⁵¹.

Tüm bunların yanında tanımda belirtildiği gibi zihinsel sağlık kapsamında elde edilmiş verilerde kişisel sağlık verileridir. Bir psikiyatrisin hastasıyla görüşmesi sonucu edindiği bilgiler de kişisel veri kapsamına girdiğinden koruma kapsamında olmalıdır.

Sonuç olarak sağlık alanında kişisel veri, sağlık personeli tarafından edinilen her türlü bilgi olarak tanımlanabilir. Kişisel veri, sadece sağlık personeline aktarılan bilgileri değil, kişinin bir hekimi, hastaneyi ziyaret etmesinden kaynaklanan kayıtları da kapsamaktadır⁵². Nitekim kişisel veri kavramının geniş yorumlanması gerektiği savunulmakta ve hastanın muayene olduğu bilgisi de bu kapsamda değerlendirilmektedir. Bu nedenle suç işlendiği yönünde belirti olmadığı müddetçe hekim, hastayı muayene ettiği bilgisini paylaşmamalıdır⁵³.

III. KİŞİSEL VERİLERİN KORUNMASI VE İDARENİN YÜKÜMLÜLÜKLERİ

A. Kişisel Verilerin Korunması

İnsanın kendisi hakkında, özel yaşamı ile aile mahremiyeti konusunda başkalarının değer yargıları oluşturmalarına esas teşkil edebilecek nitelikte bilgilerin, kendisinden habersiz veya yanlış biçimde toplanması ve bunların düzeltilmesi olanağına sahip bulunmaması zayıfın kuvvetli tarafından ezilmesi sonucunu yaratır⁵⁴. Hukuk düzeni buna müsaade etmemeli, zayıfı kuvvetlinin ihlalleri karşısında koruyacak düzenlemeleri yürürlüğe koymalıdır.

⁵⁰ Leyla Keser Berber/ Mahir M. Ülgü/ Cüneyd Er, Elektronik Sağlık Kayıtları ve Özel Hayatın Gizliliği, İstanbul 2009, s.81.

⁵¹ Kişisel Sağlık Verileri Çalışma Grubu, “Sağlık Hizmetlerinde Kişisel Veri Toplanması, Korunması ve Değerlendirilmesi” <http://www.kisiselsaglikverileri.org/32-saglik-hizmetlerinde-kisisel-veri-toplanmasi-korunmasi-ve-degerlendirilmesi.html> E.T. 12.10.2014.

⁵² Hakeri, s.798.

⁵³ Hakeri, s.799.

⁵⁴ Tezcan, s.386.

Hubmann'a göre kişinin hayat alanı üç kısımdan oluşmaktadır. Bunlar kişinin güven duyduğu kimselerle paylaştığı, bunun dışındaki kişilere kapalı olmasını istediği "giz alanı", kişinin gizli hayatına dahil olmayan fakat ailesi, yakınları ve arkadaşları gibi sıkı ilişkiler içinde olduğu sınırlı sayıda kişilerle paylaşmak istediği "özel alanı" ve kişinin başkalarının bilmesinden rahatsız olmadığı kamuya açık "ortak alanı"dır⁵⁵.

İşte burada mahremiyet kavramı ile özel yaşamın gizliliği arasındaki ayırım daha belirgin olarak ortaya çıkmaktadır: Mahremiyet kişinin gizli ve özel alanını kapsamakta iken, özel yaşam mahremiyeti de içine alan bir üst kavramı ifade etmektedir ve özel yaşamın gizliliği hakkı kişinin mahrem alanının dışındaki kamuya açık alanını da koruma altına almaktadır⁵⁶. Hukuk düzeni özel yaşamın gizliliğini koruma altına alarak, kişilerin hem mahrem alanlarını hem kamuya açık alanlarını korumaktadır.

Kişisel verilere yönelik saldırılar temelde üç gruptan gelebilir: bireyler ve kişi toplulukları, çeşitli gruplar ve özel teşebbüsler ile devletler. Bireylerden gelebilecek saldırılara baktığımız zaman sağlık alanında kişisel verilere yönelik saldırılar sağlık meslek mensuplarından gelebilir⁵⁷. Bireylere başka bireylerden gelen saldırılar temelde medeni hukuk kapsamında kişilik haklarıyla ilişkilidir. Bu saldırıların suç niteliğinde olması durumunda ise ceza hukuku devreye girecektir. Çeşitli gruplar ve özel teşebbüsler, piyasada güçlerini ve işlem hacimleri arttırmak, müşterilerine daha iyi hizmet vermek ve hepsinin temelinde kârlılıklarını yükseltmek amacıyla geniş oranda kişisel veriler toplamakta ve bunları işlemektedir. Son olarak devletlerin, suçluluğu önleme, terörle mücadele, vatandaşlarına daha iyi hizmet sunma gibi nedenlerle, tuttuğu verilerin yarattığı hukuksal sorunlar bulunmaktadır⁵⁸.

⁵⁵ **Serap Helvacı**, Türk ve İsviçre Hukuklarında Kişilik Hakkını Konuyucu Davalar, İstanbul 2001, s.62.

⁵⁶ **Uğur Ersoy**, Bir İnsan Hakları Kavramı Olarak Kişisel Verilerin Korunması, Gazi Üniversitesi Sosyal Bilimler Enstitüsü, (Yüksek Lisans Tezi), Ankara 2009, s.10-11.

⁵⁷ Sağlık meslek mensubu olanlar Tababet ve Şuabatı Sanatlarının Tarzı İcrasına Dair Kanunu Ek madde 13'te tespit edilmiştir. Bunlar; tabipler, diş hekimleri, sünnetçiler, ebeler, hastabakıcı hemşireler, klinik psikolog, fizyoterapist, odyolog, diyetisyen, dil ve konuşma terapisti, pedogog, sağlık fizikçisi, anestezi teknisyeni/teknikeri, tıbbi laboratuvar ve patoloji teknikeri, tıbbi görüntüleme teknisyeni/teknikeri, ağız diş sağlığı teknikeri, diş protez teknikeri, tıbbi protez ve oryöz teknisyeni/teknikeri, ameliyathane teknikeri, adli tıp teknikeri, diyaliz teknikeri, fizyoterapi teknikeri, perfüzyonist, radyoterapi teknikeri, eczane teknikeri, iş ve uğraşı terapisti, iş ve uğraşı teknikeri (ergoterapi teknikeri), elektronörofizyoloji teknikeri, mamografi teknikeri, acil tıp teknikeri, hemşire yardımcısı, ebe yardımcısı, sağlık bakım teknisyenidir.

⁵⁸ **Elif Küzeci**, Kişisel Verilerin Korunması, Ankara Üniversitesi Sosyal Bilimler Enstitüsü, (Doktora Tezi), Ankara 2010, s.6.

Hastanın kişisel verilerine saldırı genel olarak devlet, sağlık meslek mensubu ve üçüncü kişilerden gelebilir.

Ülkemizde bel ağrısı yakınmasıyla sağlık kurumuna başvuran hastayı aynı gün medikal malzeme satan firmanın telefonla arayıp korse pazarlaması, gazete- lere yansıyan habere göre; ev telefonu aranan aileye bekâr kızlarının TC kimlik numarası söylenerek hamilelik takibi için aile hekimine gitmesi gerektiği bildirilmesi sıradan olaylardandır. Kolay erişilen bu veriler nedeniyle kişilerin sigortacılık, sağlık, ticaret ve iş hayatında haksız işlemlere tabi tutulabilmesi mümkündür. SGK'nın toplanan verileri Data-Med adlı şirkete sattığı iddialarının⁵⁹ basına yansması üzerine verilerin anonimleştirilerek satıldığına ilişkin açıklama kamuoyunu ve hekimleri tatmin etmemiştir⁶⁰.

Türk hukukunda kişisel verilerin korunmasına hizmet edebilecek kişisel verilerin korunması kanunu yürürlükte olmasa bile Anayasanın bazı hükümleri, özel kanunlarda yer alan hükümler ile Türkiye'nin taraf olduğu ve insan haklarının korunmasına ilişkin birtakım uluslararası sözleşmeler yoluyla kişisel verilerin belli bir ölçüde korunması söz konusu olabilmektedir.

1. Anayasa

Anayasanın “Temel Hak ve Ödevler” başlıklı ikinci kısmı oldukça geniş bir temel haklar listesi içermektedir (Anayasa m.12-74). Herkesin kişiliğine bağlı dokunulmaz devredilmez vazgeçilmez temel hak ve özgürlüklere sahip olduğunu belirten Anayasa, temel hak ve özgürlüklere bir anayasa normu niteliği kazandırmıştır⁶¹. Kişisel verilerin korunması anayasal bir normdur.

Anayasanın “özel hayatın gizliliği” başlıklı 20. maddesine 2010 yılında eklenen üçüncü fıkrasında⁶², kişisel verilerin korunması anayasal bir hak olarak kabul edilmiş ve kişisel verilerin korunmasını isteme hakkının kapsamı da düzenlenmiştir⁶³. Maddeye göre kişisel verilerin korunması hakkı

⁵⁹ <http://www.sgk.com.tr/1090-Haber1-75-milyonun-saglik-verilerinin-satisi-tam-gaz--devam-ediyor.html> E.T. 13.10.2014.

⁶⁰ **Hüseyin Soysal**, “Sağlık Hizmetlerinde Kişisel Veri Toplanması”, Türkiye Psikiyatri Derneği Bülteni, C. 16 S. 3, Y.2013, s.10.

⁶¹ **Aksoy**, s.93.

⁶² “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.” Anayasa m.20/3.

⁶³ Her ne kadar kişisel verilerin korunması Anayasaya 2010 yılında girse de bu tarihten önce de kişisel veriler korunmaktaydı. Mesela TCK 2005 yılı itibarıyla m.135 vd. maddeleri uyarınca kişisel verileri korumaktaydı. Bu durum kanun koyucunun asli düzenleme yetkisine dayanmaktadır. Kanun koyucu anayasaya aykırı olmamak üzere ilk elden düzenleme yapabilir.

kişisel verilerle ilgili bilgilendirilme, erişim, düzeltme ve sildirme hakkı ile kişisel verilerin amacı doğrultusunda kullanılıp kullanılmadığını öğrenme haklarını kapsar.

Kişi manevi varlığını korumak için kural olarak kişisel verilerini işleyen herkese karşı kişiliğinin korumasını isteyebilecektir. Kişi ancak çevresinin kendisi hakkında sahip olduğu bilgilerin bilincinde olarak manevi varlığını koruyabilecektir. Bu sebeple de hangi kişisel verilerinin kime veya kimlere iletileceğini kontrol edebilme hakkına sahip olmalıdır. Yani veri koruması hakkı kişiye hangi kişisel verilerinin kim tarafından ve kimin için hangi amaçla elde edildiğini öğrenme hakkı verecektir. Kişinin rızası ve hukuka uygun bir amaç olmaksızın elde edilen verilerin işlenmesi kişilik hakkını ihlal edecektir⁶⁴.

Anayasa'nın 20. maddesinin son cümlesinde kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenleneceği belirtilmiştir. Yasama yetkisinin devredilmezliği ilkesi gereğince, Anayasa'nın açıkça kanun ile düzenlenmesini öngördüğü konularda yürütme organı doğrudan ve ilk elden düzenleme yapamaz. Anayasa Mahkemesi'nin 5809 sayılı Elektronik Haberleşme Kanunu'nun, "Kurum, elektronik haberleşme sektörüyle ilgili kişisel verilerin işlenmesi ve gizliliğinin korunmasına yönelik usul ve esasları belirlemeye yetkilidir" hükmünü içeren 51. maddesinin iptaline ilişkin olarak vermiş olduğu, 9.4.2014 tarih, E. 2013/122 ve K. 2014/74 sayılı kararında⁶⁵; Anayasa'nın 20. maddesinin son fıkrası ile kişisel verilerin güvence altına alınmış olduğunu, kişisel verilerin kaydedilmesi, işlenmesi ve silinmesi gibi hususların mutlak surette "kanun" ile düzenlenmesi gerektiğini belirtmiştir.

⁶⁴ Başalp, s.100-101.

⁶⁵ 26.7.2014 tarih ve 29072 sayılı Resmi Gazete'de yayınlanmıştır. Kararda "kişisel veri kavramı, belirli veya kimliği belirlenebilir olmak şartıyla, bir kişiye ilişkin bütün bilgilerini ifade etmektedir. Bu bağlamda, adı, soyadı...telefon numarası...görüntü ve ses kayıtları...gibi kişiyi doğrudan veya dolaylı olarak belirlenebilir kılan tüm veriler kişisel veri kapsamındadır. Kişisel verilerin korunması hakkı, kişinin insan onurunun korunmasının ve kişiliğinin serbestçe geliştirebilmesi hakkının özel bir biçimi olarak, bireyin hak ve özgürlüklerini kişisel verilerin işlenmesi sırasında korumayı amaçlamaktadır. Bilişim teknolojilerindeki gelişmeler sonucunda, geleneksel yöntemlerle mümkün olmayan çok sayıda verinin toplanabilmesi, daha önce birbirinden ilişiksiz şekilde tutulan pek çok verinin merkezi olarak bir araya getirilebilmesi; verilerin, veri eşleştirme ve veri madenciliği gibi ileri teknolojik imkanlarla analize tabi tutulmak suretiyle, veriden yeni veriler üretme kapasitesinin artması, verilere erişim ve veri transferinin kolaylaşması... gibi etkenler günümüzde kişisel verilerin en üst seviyede korunmasını zorunlu kılmaktadır. Bu bağlamda Anayasa'nın 20. maddesinin üçüncü fıkrasının son cümlesinde, kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenleri" hükmüne yer verilerek kişisel verilerin korunması hakkı anayasal güvenceye bağlanmış ve bu şekilde kamu makamlarının keyfi müdahalelerine karşı koruma altına alınmıştır." denilmektedir.

2. Kişisel Verilerin Korunması Kanunu Tasarısı

Bir temel hak ve özgürlük olarak Anayasa ile güvence altına alınan kişisel verilerin korunması hakkına ve bu hakkın içerisinde yer alan kişisel sağlık verilerinin korunmasına yönelik yapılacak düzenlemelerin ancak ve ancak kanunla yapılabileceği⁶⁶ belirtilmiş olmasına rağmen Türk Hukuku'nda kişisel verilerin korunmasına ilişkin özel bir kanun bulunmamaktadır. Meclise sunulan kişisel verilerin korunmasına ilişkin kanunu tasarısı yasallaşmayı beklemektedir.^{67, 68}

Kişisel Verilerin Korunması Kanunu Tasarısı üzerinde 1990'lı yıllardan beri çalışılmaktadır⁶⁹. En son olarak Adalet Bakanlığı tarafından hazırlanan, Bakanlar Kurulunca 3.11.2014 tarihinde kararlaştırılan, Kişisel Verilerin Korunması Kanunu Tasarısı 26.12.2014 tarihinde meclise sunulmuştur.

Tasarı'nın 6. maddesi 2/e bendinde özel nitelikli veri olan sağlık verilerinin; *"kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi ile sağlık hizmetlerinin yönetimi ve finansmanı*

⁶⁶ **Akgül**, Kişisel Sağlık Verileri, s.28.

⁶⁷ Kişisel Verilerin Korunması Kanunu Tasarısı, http://www.tbmm.gov.tr/develop/owa/tasari_teklif_sd.sorgu_yonlendirme,e.t 05.02.2015.

⁶⁸ Kişisel Verilerin Korunması Kanunu Tasarısı ile ilgili ilk çalışmalar 1989 yılında başlamış ve 2000'li yıllara kadar çeşitli tasarılar hazırlanmış ancak çalışmalar sonuçlandırılmamıştır. 2000 yılında kurulan komisyonun da tasarı çalışmalarını tamamlayamaması üzerine 30/03/2004 tarihli Bakan oluru ile Prof. Dr. Bahri Öztürk başkanlığında yeni bir Komisyon oluşturularak Tasarı hazırlık çalışmalarına devam edilmiştir.

Bu Komisyon tarafından hazırlanan Tasarı, kamu kurumları, üniversiteler ve sivil toplum örgütleri de dahil olmak üzere toplam 53 kuruluşa görüşe gönderilmiş, Başbakanlık aşamasında da tekrar görüş alınmıştır. Gelen görüşler üzerinde çalışmalarını tamamlayan Adalet Bakanlığı, Tasarıyı 28/07/2006 tarihinde Başbakanlığa göndermiştir. Tasarı, Başbakanlık tarafından 22/4/2008 tarihinde Türkiye Büyük Millet Meclisi'ne sevk edilmiştir. Tasarı, 02/05/2008 tarihinde esas komisyon olarak Adalet Komisyonuna gönderilmiştir. Tasarı, 07/05/2008 tarihinde Meclis Adalet Komisyonu tarafından alt komisyona havale edilmiştir. Alt Komisyon tasarı ile ilgili birkaç toplantı yaptıktan sonra yoğun gündem nedeniyle çalışmalarına ara vermiş ve Adalet Alt Komisyonunda bulunan tasarı, araya TBMM Seçimlerinin girmesi nedeniyle yasalasamayınca İçtüzüğü'nün 77. maddesi gereğince hükümsüz sayılmıştır. Bunun üzerine, Adalet Bakanlığı tarafından 15/09/2011 tarihinde Başbakanlığa yazılan yazıyla Tasarının yenilenmesinin uygun olacağı bildirilmiştir. Bu sırada, Bakanlık bünyesinde bir çalışma grubu oluşturulmuş, bu çalışma grubu mevcut Tasarıyı getirilen eleştiri ve öneriler doğrultusunda yeniden kaleme almış ve yeni Tasarı 08.06.2012 tarihinde Başbakanlığa gönderilmiştir.(Kişisel Verilerin Korunması Kanunu Tasarısı Hakkında Bilgi Notu, http://www.tbmm.gov.tr/arastirma_komisyonlari/bilisim_internet/docs/sunumlar/Adalet%20Bakanl%C4%B1%C4%9F%C4%B1%20Kanunlar%20Genel%20M%C3%BCd%C3%BCrl%C3%BC%C4%9F%C3%BC29-05-2012.pdf s.2-3, E.T. 15.01.2015.)

⁶⁹ **Elif Küzeci**, *"Kişisel Sağlık Verileri ve Hukuki Haklar"*, Kişisel Sağlık Verilerine Mesleki Yaklaşımlar Çalıştayı, İstanbul 2013, s.22.

amacıyla, sır saklama yükümlülüğü altında bulunan kişiler tarafından işlenmesi” kabul edilmiştir⁷⁰.

Hüküm Anayasa 20. maddesinde yer alan “kişisel veriler ancak kanunda öngörülen hallerde işlenebilir” hükmüne uygun olarak kişisel verilerin hangi amaçla toplanacağını belirtmiş, amacı sınırlandırmıştır. Sadece kanunda sayılan amaçlar için veri toplanıp, işlenebilecektir. Aynı şekilde veri işleyebilecek kişiler de sınırlı sayıda kanunda sayılmıştır. Maddeye göre sır saklama yükümlülüğü altında bulunmayan kişiler veri toplayıp işleyemez.

Tasarının 7. maddesinde kanuna uygun olarak işlenmiş verilerin, işlenmesini gerektiren sebep ortadan kalkmış ise veriler resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından⁷¹ silinir, yok edilir veya anonim hâle getirilir. Maddede verilerin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin usul ve esasların yönetmelikte gösterileceği belirtilmiştir. Veri koruma hukuku açısından önemli ve gerekli bir düzenlemedir. Toplanan veriler süresiz şekilde saklanmamalıdır. Tasarıda süre sınırı getirilmemiş, işlenmesini gerektiren sebebin ortadan kalktığı durumlarda verilerin silineceği, yok edileceği veya anonim hale getirileceği düzenlenmiştir. Tasarıya azami süre sınırı getirilmesi uygulama açısından maddenin etkinliğini artıracaktır.

Anayasanın 20. maddesinin son fıkrası gereği Tasarının yasalaşması gerekmektedir. Çünkü yürürlükte bulunan ve kişisel verilere ilişkin hüküm ihtiva eden pek çok yönetmelik hukuka aykırı⁷² ve asli düzenleme yetkisinin yasama

⁷⁰ Adalet Bakanlığı tarafından hazırlanan, Bakanlar Kurulunca 7.04.2008 tarihinde kararlaştırılan, 22.04.2008 tarihinde meclise sunulan Kişisel Verilerin Korunması Kanunu Tasarısı 7. maddesi 2/f bendinde “*koruyucu hekimlik, tıbbî teşhis, tedavi, bakım veya sağlık hizmetlerinin yürütülmesi amacıyla kişisel verilerin; sağlık kurumları, sigorta şirketleri, sosyal güvenlik kurumları, işyeri sağlık birimi oluşturmakla yükümlü işverenler, sağlıkla ilgili okul ve üniversiteler tarafından ilgili kanunlara uygun olarak, hukuken veya meslek kurallarına göre sır saklama yükümlülüğü altında bulunan sağlık personeli veya eşdeğer seviyede sır saklama yükümlülüğü altındaki bir başka kişinin gözetimi altında işlenmesi*” kabul edilmişti.

⁷¹ Veri sorumlusu “*birim, kurum veya kuruluşlarda veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi*” ifade eder. Kişisel Verilerin Korunması Kanunu Tasarısı, m.3.

⁷² Danıştay İdari Dava Daireleri Genel Kurulu’nun 06.03.2014 tarih ve YD itiraz No. 2013/819 sayılı kararına göre: “*İdarelerce, gelişen teknolojinin kamu hizmetlerinin etkin ve verimli yürütülmesini kolaylaştırıcı etki sağlaması amacıyla, kamu kesiminde kullanılmaya başlanması mümkün olmakla birlikte, teknoloji kullanılarak kişisel verilerin kayıt altına alınması ve uygulamasının ilgili Anayasal düzenleme uyarınca belirli bir yasal çerçeve içine oturtulması, konuya ilişkin usul ve esasların yasa hükmü ile tespit edilmesi ve yine Anayasa’daki ve uluslararası metinlerdeki temel hak ve özgürlüklere ilişkin hükümlere uygun olması gerektiği kuşkusuzdur. Pozitif hukukumuzda kişisel verilerin işlenmesine ilişkin olarak Anayasanın 20. Maddesi hükmü çerçevesinde yürürlüğe konulmuş yasal bir düzenleme bulunmadığı gi-*

organına ait olduğu temel kuralını ihlal etmektedir. Veri korumasına ilişkin çerçeve yasanın bir an evvel yasalaşması önemli ve gereklidir.

3. Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu

5510 sayılı Kanun'un, "Sağlık hizmeti sunucularının kayıt ve bildirim zorunluluğu ve kontrol yetkisi"⁷³ başlıklı 78. maddesinin birinci fıkrasında; Sosyal Güvenlik Kurumu Başkanlığı ile sözleşmesi olan, tüm sağlık hizmeti sunucularının, sağlık hizmeti sunduğu tüm kişilere ait sözleşme hükümlerinde yer verilen bilgileri, belirlenen yöntemlere ve süreye uygun biçimde elektronik ortamda veya yazılı olarak Sosyal Güvenlik Kurumu Başkanlığı'na göndermek zorunda olduğu; ikinci fıkrasında genel sağlık sigortalısı ve bakmakla yükümlü olduğu kişinin sağlık bilgilerinin gizliliğinin esas olacağı hükmü yer almaktadır.

Sağlık bilgilerinin ne şekilde korunacağı, ulusal güvenlik nedeniyle sağlık bilgisi paylaşımına açılmayacak kişilerin tespiti ilgili Bakanlıkların önerisi üzerine Çalışma ve Sosyal Güvenlik Bakanlığı tarafından tespit edilir. Bu kişi ve grupların sağlık bilgilerinin nasıl tutulacağı ilgili kuruluşların görüşleri alınarak hazırlanacak yönetmelik⁷³ ile düzenlenir hükmüne yer vermiştir.

Maddede sağlık hizmetinden yararlanan kişilerinin sözleşmede yer alan bilgilerinin Sosyal Güvenlik Kurumu Başkanlığı'na gönderilmesi gerektiği, ikinci fıkrada ise sağlık bilgilerinin gizliliğinin esas olduğu belirtilmiş, bilgilerin ne şekilde korunacağı Çalışma ve Sosyal Güvenlik Bakanlığı tarafından tespit edilir denmiştir. Ayrıca bilgilerin nasıl tutulacağı hazırlanacak yönetmelikle belirlenir denilerek oldukça geniş düzenleme yetkisi idareye bırakılmıştır. Anayasa m.20/son fıkrası hükmüne göre, kişisel verilerin korunmasına ilişkin usul ve esaslar kanunla düzenlenmelidir. Kanun hükmünün konuyu yönetmeliğin düzenleme alanına bırakması Anayasa m.20/son fıkrası hükmüne aykırıdır. Anayasanın açıkça kanunla düzenlenmesini belirttiği alanda yürütme organı doğrudan ve ilk elden düzenleme yapmamalıdır.

bi...kanunda davalı kuruma yetki veren bir düzenleme yer almamaktadır. Bu bağlamda, Anayasa'nın yukarıda alıntısı yapılan hükümleri ve uluslararası metinler uyarınca güvence altına alınan ve kanunla düzenlenmesi gereken kişisel verilerin işlenmesine ilişkin olarak uygulanmanın sınırlarını, kişisel verinin nasıl depolanıp kullanılacağını tespit eden usul ve esasları gösteren bir düzenleme olmadan çıkarılan dava konusu Yönetmelik hükmünde hukuka aykırılık bulunmamaktadır." denilmektedir. (Kazancı İçtihat Bilgi Bankası, <http://www.kazanci.com/kho2/ibb/giris.htm> E.T.14.10.2014).

⁷³ Genel Sağlık Sigortası Verilerinin Güvenliği ve Paylaşımına İlişkin Yönetmelik, RG, T. 11.07.2012, S. 28350.

Sosyal Güvenlik Kurumunun avuçiçi kimlik tarama uygulamasının⁷⁴ Anayasaya uygunluğuna değinmek gerekmektedir. 5510 sayılı Sosyal Güvenlik Kurumu Kanunu 67/3 şu şekildedir; “Ayrıca 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 zorunludur.” 1/3/2012 tarihli ve 6283 sayılı Kanunun 1. maddesiyle, bu fıkrada yer alan “nüfus cüzdanı” ibaresinden önce gelmek üzere “biyometrik yöntemlerle kimlik doğrulamasının yapılması ve/veya” ibaresi eklenmiştir. Kanun maddesi bu şekildeyken Sosyal Güvenlik Kurumu Sağlık Uygulama Tebliği “...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.” diyerek kimlik doğrulama için hem resmi belge ibrazını hem biyometrik kimlik doğrulaması yapılmasını zorunlu kılmıştır.

Avuçiçi kimlik tarama uygulaması biyometrik kimlik doğrulama yöntemleri arasında yer almaktadır. Biyometrik yöntemler, ölçülebilir fizyolojik ve bireysel özellikleri aracılığıyla gerçekleştirilen ve otomatik şekilde doğrulanabilen kimlik denetleme tekniklerini ifade etmektedir. Bu yöntemler arasında par-

⁷⁴ Sosyal Güvenlik Kurumu (SGK) tarafından hastanelerde ve sağlık merkezlerinde zorunlu hale getirilen ve Biyometrik Kimlik Doğrulama Sistemi adı verilen uygulamadır.

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. Kimlik tespiti, biyometrik kayıt işlemi veya biyometrik kimlik doğrulama işlemi usulüne uygun yapmayan ve bu nedenle bir başka kişiye sağlık hizmeti sunulması nedeniyle Kurumun zarara uğramasına sebebiyet veren sağlık hizmeti sunucularından ödenen tutar geri alınır.

(2) 2828 sayılı Sosyal Hizmetler Kanunu kapsamında sağlanan yardımlardan ücretsiz faydalananların, sağlık kurum ve kuruluşlarına birinci fıkrada belirtilen belgeleri ibraz edememeleri halinde 2828 sayılı Kanun kapsamında bulduklarını gösterir belgeye göre gerekli işlemler yürütülecek sonrasında söz konusu belgelerin ibrazı ilgili Kurumdan istenecektir.

(3) Kapsamdaki kişilerin kendi adına bir başkasının sağlık hizmeti almasını veya Kurumdan haksız bir menfaat temin etmesini sağlaması yasaktır. Bu fiilleri işleyenlerden Kurumun uğradığı zararın iki katı kanuni faiziyle birlikte müştereken ve müteselsilen tahsil edilir ve ilgililer hakkında 5237 sayılı Türk Ceza Kanunu hükümleri doğrultusunda suç duyurusunda bulunulur.” http://www.sgk.gov.tr/wps/portal/tr/mevzuat/yururlukteki_mevzuat/tebligler E.T. 10.01.2015.

mak izi tanıma, avuç içi tarama, el geometrisi tanıma, iris tanıma, yüz tanıma, retina tanıma, DNA tanıma gibi yöntemler bulunmaktadır. Tüm bu yöntemler kullanılarak bireyin kimliği tespit edilebilmekte, kendine has özellikleri, kişisel verileri kayıt altına alınabilmektedir.

Parmak izi, avuç içi damar izi, retina gibi biyometrik verilerin kişisel veri kapsamında korunan verilerdir. Kişisel veriler Anayasa'nın 20. maddesiyle güvence altına alınmıştır. Anayasa m.20'de kişisel verilerin ancak kanunda öngörülen hallerde işlenebileceği hüküm altına alınmıştır. Anayasa Mahkemesi içtihatlarında, yasama yetkisinin devredilmezliği ilkesi gereğince, Anayasa'nın açıkça kanunla düzenlenmesini öngördüğü konularda yürütme organına doğrudan ve ilk elden düzenleyici işlem yapma yetkisi verilemeyeceği kabul edilmektedir. Dolayısıyla kişisel verinin işleyişi ile ilgili olarak, genel hatlarıyla da olsa, usul ve esasların kanunla belirlenmesi Anayasal bir zorunluluk bulunmaktadır. Bu nedenle, mevcut düzenleme hukuka aykırıdır.

Nitekim Danıştay 15. Dairesi Sağlık Uygulama Tebliğinin 1.6- Kimlik Tespiti başlıklı bölümünün 1. paragrafının 1. cümlesinde geçen "*ve Biyometrik yöntemlerle kimlik doğrulaması yapılması zorunludur*" ibaresi ile 2. cümlesinin tamamının ve 1.6.1- Biyometrik Kimlik Doğrulama İşlemi başlıklı bölümünün 1 ve 2 no.lu paragraflarının iptali istemiyle açılan davada yürütmeyi durdurma kararı vermiş⁷⁵ ve 5510 sayılı Sosyal Güvenlik Kurumu Kanunu 67. maddesinin 3. fıkrasında yer alan "... Biyometrik yöntemlerle kimlik doğrulaması yapılması ve/veya..." ibaresinin iptali için Anayasa Mahkemesine başvurmuştur. Mahkeme henüz karar vermemiştir⁷⁶.

"Bilgi ve belge isteme hakkı, bilgi ve belgelerin Kuruma verilme usulü" başlıklı 100. maddede kanunda sayılan kurumların Devletin güvenliği ve temel dış yararlarına karşı ağır sonuçlar doğuracak hâller ile özel hayat ve aile hayatının gizliliği ve savunma hakkına ilişkin hükümler saklı kalmak kaydıyla özel kanunlardaki yasaklayıcı ve sınırlayıcı hükümler dikkate alınmaksızın gizli dahi olsa Kurum tarafından kişilerin sosyal güvenliğinin sağlanması, 6183 sayılı Kanuna göre Kurum alacaklarının takip ve tahsili ile bu Kanun kapsamında verilen diğer görevler ile sınırlı olmak üzere istenecek her türlü bilgi ve belgeyi sürekli ve/veya belli aralıklarla vermeye mecbur oldukları düzenlenmiştir. Maddenin devamında bilgi ve belgelerin kuruma verilme usulü düzenlenmiştir.

⁷⁵ Danıştay 15. Dairesi ise 2014/4562E sayılı ve 11.09.2014 tarihli kararı, (Kazancı İçtihat Bilgi Bankası, <http://www.kazanci.com/kho2/ibb/giris.htm> E.T. 12.01.2015).

⁷⁶ Anayasa Mahkemesi, E. 2014/180, Danıştay 15. Daire.

4. Türk Ceza Kanunu

5237 sayılı Türk Ceza Kanunu'nda kişisel verilerin korunması ve veri güvenliğinin ihlali halinde sorumluların cezalandırılması amacıyla bazı düzenlemeler yapılmıştır. “Kişisel verilerin kaydedilmesi” başlıklı 135. maddede “*hukuka aykırı olarak kişisel verileri kaydeden kimseye bir yıldan üç yıla kadar hapis cezası verileceği*” hüküm altına alınmıştır⁷⁷. İkinci fıkrada ise “*kişilerin siyasî, felsefî veya dinî görüşlerine, ırkî kökenlerine; hukuka aykırı olarak ahlâkî eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgileri kişisel veri olarak kaydeden kimse, yukarıdaki fıkra hükmüne göre cezalandırılır*” hükmüne yer verilmiştir. Bu fıkrada uluslararası hukuki metinlerde düzenlenen hassas kişisel verilere benzer şekilde hassas kişisel veriler sayılmış ve hassas veri olan sağlık durumlarına ilişkin bilgilere de ikinci fıkrada yer verilmiştir.

Her türlü özel veya resmi kuruluşlarca kişisel veriler kaydedilmektedir ancak bu kişisel verilerin ilgili kurumlar dışında başka kişi ve kurumlarca ele geçirilmesi ya da kaydedilmesi halinde bu suç oluşacaktır. Kişilerin rızası alınarak kaydedilen bilgilerin amaçları dışında kullanılması da suç oluşturacaktır. Bu suç Avrupa Konseyi kapsamında hazırlanan ve 28 Ocak 1981 tarihinde Türkiye tarafından imzalanan Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşme'nin iç hukukumuzdaki yansımadır⁷⁸.

136. madde uyarınca kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, iki yıldan dört yıla kadar hapis cezası ile cezalandırılır⁷⁹. 136. madde hükmü ile hukuka uygun olarak kaydedilmiş olsun veya olmasın kişisel verileri hukuka aykırı olarak başkalarına vermek, yaymak veya ele geçirmek bağımsız bir suç olarak tanımlanmıştır. Kanun gereği, mağdurun rızası veya meslek icabı kayıt altına alınan veri, hangi hukuka uygun amaçla kaydedilmişse sadece o amaç çerçevesinde kullanılabilir. Bunun dışında hangi nedenle olursa olsun veriyi hukuka aykırı olarak ele geçiren kişi 136. maddede tanımlanan suçu işlemiş sayılacaktır⁸⁰.

⁷⁷ Kanunun ilk halinde yer alan “*altı aydan üç yıla kadar hapis cezası verilir*” hükmü, 21.02.2014 tarih ve 6526 sayılı Terörle Mücadele Kanunu ve Ceza Muhakemesi ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun'un(RG, T.06.04.2014, S. 28933) 3. maddesiyle “*altı aydan*” ibaresi “*bir yıldan*” şeklinde değiştirilmiştir.

⁷⁸ **Gökhan Taneri**, *Hasta Hakları*, Ankara 2014, s.318.

⁷⁹ Kanunun ilk halinde yer alan “*bir yıldan dört yıla kadar hapis cezası verilir*” hükmü, 21.02.2014 tarih ve 6526 sayılı Terörle Mücadele Kanunu ve Ceza Muhakemesi ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun'un(RG, T.06.04.2014, S. 28933) 4. maddesiyle “*bir yıldan*” ibaresi “*iki yıldan*” şeklinde değiştirilmiştir.

⁸⁰ **Şen**, s.1209.

Nitelikli hallerin sayıldığı 137. maddede kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle, belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle kişisel verilerin kaydedilmesi, verileri hukuka aykırı olarak verme veya ele geçirme suçlarının işlenmesi hâlinde, verilecek ceza yarı oranında artırılır şeklinde düzenlenmiştir. Burada geçen meslek ve sanatın kamusal ya da özel olmasının suçun oluşumuna etkisi yoktur⁸¹. Hükme göre hekimler, psikiyatristler, eczacılar ve diğer sağlık meslek mensupları, mesleklerinin icrası sırasında öğrendikleri kişisel verileri hukuka aykırı olarak kaydeder, başkalarına verir veya yayarlarsa ceza yarı oranda artırılabacaktır.

“Verileri yok etmeme” başlıklı 138. maddenin birinci fıkrasında Kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediğinde bir yıldan iki yıla kadar hapis cezası verilir hükmüne yer verilmiştir⁸². İkinci fıkrasında suçun konusunun Ceza Muhakemesi Kanunu hükümlerine göre ortadan kaldırılması veya yok edilmesi gereken veri olması hâlinde verilecek ceza bir kat artırılır hükmüne yer verilmiştir⁸³.

Türk Ceza Kanunu'nun sayılan hükümleri kişisel veriler konusunda ortaya çıkarabilecek suiistimal ve hukuka aykırılıkların önüne geçilmesi bakımından önemlidir. Hatta TCK'nın 135. ve 136. maddelerinde düzenlenen kişisel verilerin kayda alınması ve hukuka aykırı olarak bir başkasına verilmesi ya da ele geçirilmesi suçlarına ilişkin belirlenen cezaların artırılması, kişisel verilere yönelik bilinci ve saygıyı artıracak, bu verilerin korunması açısından caydırıcılık işlevi görecektir.

5. Ceza Muhakemesi Kanunu

CMK'nın “moleküler genetik incelemeler” başlıklı 78. maddesinin birinci fıkrasında “75 ve 76'ncı maddelerde öngörülen işlemlerle elde edilen örnekler üzerinde, soybağının veya elde edilen bulgunun şüpheli veya sanığa ya da mağdura ait olup olmadığının tespiti için zorunlu olması halinde moleküler genetik incelemeler yapılabilir. Alınan örnekler üzerinde bu amaçlar dışında tespitler yapılmasına yönelik incelemeler yasaktır” hükmü yer almaktadır. CMK'nın 75. ve 76. maddeleri beden muayenesi ve vücuttan örnek alınmasını düzenler. Bu

⁸¹ **Yavuz Erdoğan**, “Kişisel Verilerin Korunması Bakımından Türk Ceza Kanunu Hükümlerinin Değerlendirilmesi(m.135, 136, 137, 138)”, Erciyes Üniversitesi Hukuk Fakültesi Dergisi, C. VIII, S. 2, Y. 2013, s.590.

⁸² Kanunun ilk halinde yer alan “altı aydan bir yıla kadar hapis cezası verilir” hükmü, 21.02.2014 tarih ve 6526 sayılı Terörle Mücadele Kanunu ve Ceza Muhakemesi ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun'un(RG, T.06.04.2014, S. 28933) 5. maddesiyle “altı aydan” ibaresi “bir yıldan” şeklinde değiştirilmiştir.

⁸³ Bu fıkra kanuna, 21.02.2014 tarih ve 6526 sayılı Terörle Mücadele Kanunu ve Ceza Muhakemesi ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun'un(RG, T.06.04.2014, S. 28933) 5. maddesiyle eklenmiştir.

maddeye göre, elde edilen örnekler üzerinde moleküler genetik inceleme yapılabilmesi için, inceleme yapmanın bir suç sebebiyle zorunlu olması gerektiği düzenlenmiştir. Bunun dışında elde edilen örnekler üzerinde amaç dışında tespit yapılması yasaklanmıştır.

“Genetik inceleme sonuçlarının gizliliği” başlıklı 80. maddede; “75, 76 ve 78. madde hükümlerine göre alınan örnekler üzerinde yapılan inceleme sonuçları, kişisel veri niteliğinde olup, başka bir amaçla kullanılamaz; dosya içeriğini öğrenme yetkisine sahip bulunan kişiler tarafından bir başkasına verilemez. Bu bilgiler, kovuşturmayaya yer olmadığı kararına itiraz süresinin dolması, itirazın reddi, beraat veya ceza verilmesine yer olmadığı kararı verilip kesinleşmesi hallerinde Cumhuriyet savcısının huzurunda derhal yok edilir ve bu husus dosyasında muhafaza edilmek üzere tutanağa geçirilir” hükmü yer almaktadır. Maddeyle inceleme sonuçlarının kişisel veri niteliğinde olduğu vurgulanmıştır. Elde edilen verilerin kullanım amacı sınırlandırılmış, gizliliğinin esas olduğu ve ihtiyaç kalmayan verilerin yok edilmesi hususu düzenlenmiştir.

“Fizik kimliğin tespiti” başlıklı 81. maddede “üst sınırı iki yıl veya daha fazla hapis cezasını gerektiren bir suçtan dolayı şüpheli veya sanığın, kimliğinin tespiti için gerekli olması halinde, Cumhuriyet savcısının emriyle fotoğrafı, beden ölçüleri, parmak ve avuç içi izi, bedeninde yer almış olup teşhisini kolaylaştıracak diğer özellikleri ile sesi ve görüntüleri kayda alınarak, soruşturma ve kovuşturma işlemlerine ilişkin dosyaya konulur. Kovuşturmayaya yer olmadığı kararına itiraz süresinin dolması, itirazın reddi, beraat veya ceza verilmesine yer olmadığı kararı verilip kesinleşmesi hallerinde söz konusu kayıtlar Cumhuriyet savcısının huzurunda derhal yok edilir ve bu husus tutanağa geçirilir” hükmü yer almaktadır. Bu maddeye göre elde edilip dosyaya konulanlar kişisel veri kapsamındadır. İhtiyaç kalmayan verilerin derhal yok edileceğinin düzenlenmesi veri koruma hukukuna uygundur.

CMK'nın 82. maddesinde; 75-81. maddelerde öngörülen işlemlerin yapılması ile ilgili usullerin yönetmelikle gösterileceği belirtilmiş ve bu maddeye dayanarak Adalet Bakanlığı tarafından 01.06.2005 tarihli ve 25832 sayılı Resmi Gazete 'de yayımlanan Ceza Muhakemesinde Beden Muayenesi Genetik İncelemeler ve Fiziki Kimliğin Tespiti Hakkında Yönetmelik çıkarılmıştır.

6. Sağlık Bakanlığı ve Bağlı Kuruluşlarının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname

663 sayılı KHK'nin bilgi toplama işleme ve paylaşma yetkisi adlı 47. maddesinin birinci fıkrası şu şekildedir; “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 vasıta ile toplama, işleme ve paylaşmaya yetkilidir.”

İkinci fıkrasında; “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” hükmü yer almaktadır.

KHK'nin 47. maddesinin özellikle birinci fıkrasında Sağlık Bakanlığı'na verilmiş paylaşma yetkisi sınırlandırılmamıştır. Söz konusu fıkra da yer alan düzenlemeye göre Bakanlık topladığı bütün verileri özel kişiler ve kamu kurum ve kuruluşlarıyla paylaşabilir. Bu durum ölçülülük ilkesine aykırıdır. İkinci fıkraya göre; üçüncü kişilerin ve kamu kurum ve kuruluşlarının verilere erişebileceği kanun ile düzenlenmişse, Bakanlık görevlerini yapmalarına yetecek derecede veriyi paylaşılabilir. İkinci fıkra da düzenleme birinci fıkraya nispeten daha iyidir. Ancak yine de veri koruma ilkelerine aykırı ve veri koruma mevzuatının gerisindedir⁸⁴.

Söz konusu KHK'nin “bilgi toplama işleme ve paylaşma yetkisi” başlıklı 47. maddesinin Anayasaya aykırılığı gerekçesiyle Anayasa Mahkemesi'ne başvurulmuştur. Anayasa Mahkemesi, 14.02.2013 tarihli ve E:2011/150, K.2013/30 sayılı kararıyla; Anayasa'nın ikinci kısmının “Kişinin Hakları ve Ödevleri” başlıklı ikinci bölümünde yer alan 20. maddesiyle güvenceye bağlanan özel hayatın gizliliği ve kişisel verilerin korunması hakkına ilişkin düzenlemeler içeren dava konusu kuralların Anayasa'nın 91. maddesinin birinci fıkrasına aykırılığı gerekçesiyle iptaline karar vermiştir⁸⁵.

Anayasa Mahkemesi verdiği kararda, Bakanlığa verilen paylaşma yetkisinin genişliğinden, bu şekilde veri paylaşımının ölçülülük ilkesine aykırı olduğundan bahsetmemiştir. Mahkeme, temel hakların KHK ile düzenlenemeyeceği gerekçesiyle hükmü iptal etmiştir. Kişisel verileri yönelik bilinci ve saygıyı artırmak adına paylaşma yetkisinin genişliğine ve ölçülülük ilkesine aykırılığa da değinilmesi gerekmektedir. Ancak 12.07.2013 tarihinde kabul edilen ve 02.08.2013 tarihli ve 28726 sayılı Resmi Gazete' de yayımlanan 6495 sayılı Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun'un 73/h-3'üncü maddesi ile 663 sayılı KHK'nin 47. maddesine iptal edilen hükümler aynı şekilde yeniden eklenmiştir. Anayasa Mahkemesi'nin, temel hakların KHK ile düzenlenemeyeceği gerekçesiyle iptal ettiği hüküm kanunla aynı şekilde yeniden eklenecek Mahkeme kararında belirtilen hukuka aykırılık bertaraf edilmiştir. Şekli

⁸⁴ Konuya “Kişisel Verilerin Paylaşılması” başlığı altında değinilecektir.

⁸⁵ Anayasa mahkemesi, 14.03.2013, E:2011/150, K.2013/30, R.G, T. 25.06.2013, S. 28688.

anlamda hukuka uygun hale getirilen bu hüküm, maddi anlamda Anayasaya ve veri koruma hukukuna aykırılık teşkil etmektedir.

Sağlık Bakanlığı ve Bağlı Kuruluşlarının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Karamamenin 8. maddesi Sağlık Bakanlığı teşkilatında yer alan Sağlık Hizmetleri Genel Müdürlüğü'ne ilgili mevzuat çerçevesinde kişisel verilerin korunması ve mahremiyetin sağlanması için düzenleme yapma görevi vermiştir⁸⁶. KHK'nin 11. maddesi Sağlık Bilgi Sistemleri Genel Müdürlüğü'ne, sağlık alanında kullanılan bilişim sistemleri ve iletişim teknolojileri ile ilgili ülke çapında politika, strateji ve standartları belirleme, uluslararası gelişmeleri izleme, veri ve bilgi akışını içeren her türden bilgi sistemleri ve projelerini yapmak ve yaptırmak görevini vermiştir⁸⁷.

7. Tıbbi Deontoloji Nizamnamesi

Nizamnamenin⁸⁸ 4. Maddesinde “*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*” hükmü yer almaktadır. 1960 tarihli Nizamnamenin bu hükmünde hekim ve dış hekimlerinin sır saklama yükümlülüğüne işaret edilmiştir. Kanuni zorunluluk olmadıkça meslek ve sanatın icrası suretiyle öğrenilen sırların paylaşılması gerektiği düzenlenmiştir. Hekim, hastayı tedavi ederken hastayla ilgili kişisel veri niteliğinde birçok bilgiye vakıf olmaktadır. Nizamnamenin çıkarıldığı dönemde kişisel verilerin korunması kavramı ülkemizde gündemde olmadığı için sadece hekimin sır saklama yükümlülüğünden bahsedilmiş, veri toplanması, korunması, paylaşılmasına ilişkin hükümlere yer verilmemiştir.

8. Türk Eczacılar Deontoloji Tüzüğü

Hasta tedavisine bağlı olarak ilaçlarını temin ederken ilişki kurmak mecburiyetinde bulunduğu eczacı ya da sağlık alanında hizmet veren diğer kişi ya da kurumlara bilgi vermek zorunda olabilir⁸⁹. Mahremiyet her zaman ve her yerde saklanmalı ve garanti edilmelidir. Eczanedeki üçüncü şahıslara ne tedaviyi ne

⁸⁶ Sağlık Hizmetleri Genel Müdürlüğü tarafından Kişisel Sağlık Verilerinin İşlenmesi ve Veri Mahremiyetinin Sağlanması Hakkında Yönetmelik Taslağı hazırlanmıştır, <http://www.sb.gov.tr/TR/belge/1-17634/kisisel-saglik-verilerinin-islenmesi-ve-veri-mahremiyet-.html>. E.T. 14.10.2014.

⁸⁷ Sağlık Bilgi Sistemleri Genel Müdürlüğü tarafından Bilgi Güvenliği Politikaları Yönergesi ve Bilgi Güvenliği Politikaları Kılavuzu hazırlanmıştır. <https://bilgiguvenligi.saglik.gov.tr/Home/Yonerge> E.T. 14.10.2014.

⁸⁸ 13.01.1960 tarih ve 4/12578 sayılı Bakanlar Kurulu Kararı, RG, T. 19.02.1960, S. 10436.

⁸⁹ Cahid Doğan, “Sağlık Haklarından Hekimlerin Sır (Kişisel Veri) Saklama Mükellefiyeti”, Sağlık Hukuku Kurultayı, 1-3 Kasım 2007, Ankara, s.141.

de hastayı ilgilendiren konular açıklanmamalıdır⁹⁰. Nitekim Türk Eczacılar Deontoloji Tüzüğü'nün⁹¹ 4. maddesi şu şekildedir; “eczacı, meslek ve sanatının icrası sırasında öğrendiği sırları, kanuni zorunluluk olmadıkça, ifşa edemez.”

Eczacılar da sır saklama yükümü altında olup, SGK bilgilerini gizli tutmak zorundadırlar. Nitekim CMK 46/1-b bendi eczacılara da hastanın kişisel verilerini korumak amacıyla tanıklıktan çekinme hakkı tanımıştır. Eczacıların yanı sıra yanlarında çalışan kalfalar, eczanede bulunan ziyaretçiler, özel şahıslar, diğer servis elemanları, ilaç mümessilleri ve eczane ile ilgili olmayan şahıslarda sır saklama yükümlüsüdürler⁹².

9. Hasta Hakları Yönetmeliği

Hasta Hakları Yönetmeliği'nin⁹³ ilkeler başlığını taşıyan 5. maddesinde “Kanun ile müsaade edilen haller ile tıbbi zorunluluklar dışında, hastanın özel hayatının ve aile hayatının gizliliğine dokunulamaz” hükmü yer almaktadır. “Mahremiyete Saygı Gösterilmesi” başlıklı 21. maddede hastanın, mahremiyetine saygı gösterilmesinin esas olduğu düzenlenmiştir.

“Bilgilerin gizli tutulması” başlıklı 23. madde şu şekildedir, “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 kişilerin hukuki ve cezai sorumluluğunu da gerektirir.

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

İlk cümlede sağlık hizmeti sunumu nedeniyle edinilecek bilgilerin kanunun izin verdiği hallerde açıklanacağı; maddenin devamında ise, verilerin açıklanmasında kişinin rızasının bulunması sağlık personeline sınırsız açıklama yetkisi vermeyeceği düzenlenmiştir. Kişinin rızası bulunmadığı ve kanunun öngörme-

⁹⁰ **Mebrure Değer**, “Hastane Eczacılığında Sır”, Türkiye Klinikleri Tıp Etiği-Hukuku-Tarihi Dergisi C. 5, S. 3, Y. 1997, s.135.

⁹¹ 9.7.1968 tarih ve 6/10314 sayılı Bakanlar Kurulu Kararı, RG, T. 27.7.1968, S. 12961.

⁹² **Değer**, s.135.

⁹³ Hasta Hakları Yönetmeliği, RG, T. 01.08.1998, S. 23420.

diği hallerde kişiye zarar verebilecek bilgilerin açıklanması halinde hukuki ve cezai sorumluluğun gerekeceği belirtilmiştir.

“Hastayla ilgili bilgilerin hastaya verilmesi ve kullanımı” başlıklı 31. maddedeki düzenlemeye göre hasta dosyalarındaki bilgilerin geniş bir özeti ile bilgi ve belgelerin örnekleri, isteği durumunda hastaya verilir. Hekim, yasal zorunluluk olmadıkça, bu bilgileri başkasına veremez. Hekim, hastanın kimlik bilgilerini saklı tutmak koşuluyla, bu bilgileri dosya üzerinden yapacağı araştırmalarda kullanabilir. Hasta dosyalarında hastanın birçok verisi bulunmaktadır. Bunlardan bir kısmı hassas kişisel veri kategorisinde yer alan verilerdir. Düzenleme dosya mahremiyetini sağlamayı, verileri yetkisiz üçüncü kişilerden korumayı amaçlamaktadır. Ayrıca hekimin yapacağı araştırmalarda kişinin kimlik bilgilerini saklı tutması yönündeki düzenleme önemlidir.

10. Yataklı Tedavi Kurumları İşletme Yönetmeliği

Yataklı Tedavi Kurumları İşletme Yönetmeliği⁹⁴ nin “poliklinik hizmetleri” başlıklı 7. maddesi şu şekildedir; “*Poliklinik muayenelerinde gizlik prensiplerine riayet esastır. Burada, halkın gelenek ve ahlak kuralına saygı gösterilir. Hastalar teker teker muayene edilir. Muayene esnasında poliklinik odasında tıp ve yardımcı tıp meslekleri personelinden başka kimsenin bulunmaması gerekir. Ancak hasta isterse ailesinden biri veya bir yakını bulunabilir.*”

Polikliniklerde her gün yüzlerce hasta muayene edilmektedir. Bu hastaların belli bir sıra içinde fakat hızlı bir şekilde muayene edilmesi gerektiğinden her bir hastaya çok kısa süre ayrılmakta, hem de hastalar birbiri yanında giyinip soyunmak zorunda kalmaktadır. Hastalar gruplar halinde muayeneye alınmaktadırlar ki bu durum mahremiyet hakkının ve özel yaşamın ağır bir ihlalidir⁹⁵. Aynı şekilde koğuş sistemi geçerli olan odalarda yapılan teşhis ve tedavi çoğunlukla kamuya açıktır ve bu durum mahremiyet ilkesini ihlal etmektedir⁹⁶. Bunun yanı sıra koğuş sistemi uygulanan hastanelerde, hastaların teşhis ve tedavisi sırasında kişinin sağlık durumuna ilişkin bilgileri üçüncü kişiler de duymaktadır.

Uygulamada hasta dosyaları genellikle hasta odalarında yer almaktadır. Bu durum koğuş sistemi uygulanan hastanelerde kişilerin sağlık bilgilerine, üçüncü kişilerin erişimi konusunda özellikle ziyaretçi saatlerinde daha büyük tehdit oluşturmaktadır. Kişisel sağlık verilerinin hassas veri kategorisinde olduğu göz önüne alındığında bilgilerin bu şekilde yetkisiz üçüncü kişilerin erişimine açık halde bulundurulması veri korumasından uzak bir uygulamadır.

⁹⁴ 10.9.1982 Tarih ve 8/5319 sayılı Bakanlar Kurulu Kararı, RG, T. 13.1.1983, S. 17927 Mük.

⁹⁵ **Yahya Deryal**, “Hasta Hakları Bağlamında Mahremiyet ve Özel Hayata Saygı”, Sağlık Hukuku Kurultayı, 1-3 Kasım 2007, Ankara, s.83.

⁹⁶ **Gökhan Taneri**, Uygulamadan Örnek Hükümlerle Türk Hukukunda Hekim Ceza Sorumluluğu, Ankara 2014, s.317.

11. Hekimlik Meslek Etiği Kuralları

Hekimlik Meslek Etiği Kuralları'nın⁹⁷ “sır saklama yükümlülüğü” başlıklı 9. maddesi şu şekildedir:

“Hekim, hastasından mesleğini uygularken öğrendiği sırları açıklayamaz. 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”.

Hekimlerin mesleklerini icra ederken hastalarından öğrendikleri sırrı açıklamamaları etik ilke olarak kabul edilmiştir. Burada hastanın ölümünün sır saklama yükümünü ortadan kaldırmayacağı belirtilerek ölmüş kişilerin de korunması gerektiği düşüncesi benimsenmiştir. Kişinin rızası veya sırrın saklanması hasta veya üçüncü kişilerin hayatını tehlikeye sokacak ise hekim, hasta ile ilgili bilgileri açıklayacaktır. Ancak bu durumda hekim sınırsız şekilde bilgileri açıklayamaz, hastanın kişilik haklarını zedelemeyecek derecede bilgi açıklayabilir.

Yasal zorunluluk durumunda hekimin düzenlediği raporların sır saklama yükümünü ihlal etmediği ve hekimin tanıklık ve bilirkişilikten çekinebileceği düzenlenmiştir. Hüküm, hekimin sır saklama yükümü açısından gerekli etik ilkeleri ihtiva etmektedir.

12. Ruh Hekimliği (Psikiyatri) Meslek Etiği Kuralları

Sağlık kavramı içine bedensel sağlıkla beraber ruhsal sağlık da girmektedir⁹⁸. Ruh sağlığını iyi hissetmeyen şahıs, hekime korkusuzca başvurabilmeli ve anlatacağı sırların aralarında kalacağına ilişkin herhangi bir tereddüt yaşamamalıdır⁹⁹. Türkiye Psikiyatri Derneği'nin hazırladığı Ruh Hekimliği Meslek Etiği Kuralları'nın¹⁰⁰ “sır saklama yükümü” başlıklı 6. maddesinde herhangi bir psikiyatrik muayene ve sağaltım altındaki kişiyle ilgili bütün bilgilerin hasta-hekim ilişkisi çerçevesinde saklı tutulması gerektiği kabul edilmiştir.

⁹⁷ Hekimlik Meslek Etiği Kuralları, http://www.ttb.org.tr/mevzuat/index.php?option=com_content&view=article&id=65:hekl-meslek-etkurallari&catid=4:t&Itemid=31, E.T. 17.10.2014.

⁹⁸ Aydın Zevkliler, “Tedavi Amaçlı Müdahalelerle Kişilik Hakkına Saldırının Sonuçları”, Dicle Üniversitesi Hukuk Fakültesi Dergisi, S. 1, Y. 1983, s.9.

⁹⁹ Doğan (Cahid), s.139.

¹⁰⁰ Ruh Hekimliği Meslek Etiği Kuralları, <http://www.psikiyatri.org.tr/upload.aspx?upload=311>, E.T. 21.10.2014.

“Kitle iletişim araçları ve sır saklama yükümü” başlıklı 7. maddede ruh hekiminin, klinik ortamında hastaların kimliğini tespit edecek şekilde görüntü alınmasına, kitle iletişim aracında yayınlanmak amacıyla hastayla konuşma yapılmasına aracı olmaması, müsaade etmemesi gerektiği düzenlenmiştir. Bir kişinin psikiyatri kliniğinde muayene olduğu bilgisi dahi kişisel veridir. Muayene olma bilgisi, kişinin sağlık durumuna ilişkin bir bilgi olduğu için hassas veriler arasında yer almaktadır. Ruh Hekimliği(psikiyatri) Meslek Etiği Kurallarının 7. maddesi kişisel verileri koruma amacına hizmet etmektedir.

13. Hekimin Sır Saklama Borcu

Hipokrat Andı’nda, “*Tedavi sırasında ya da hatta tedavi dışında, insanların yaşamlarına ilişkin, dışarıya yayılmaması gereken şeyler görür ya da işitirsem, bunları kendime saklayacağım ve sözünü etmeyi ayıp sayacağım.*” sözü yer alır¹⁰¹. Hipokrat Andı’nda yer alan bu söz hekimin sır saklama yükümünü açıklamaktadır.

Hekimin sır saklama yükümlülüğünün sınırları hakkında sağlıklı bir fikir edinebilmek için, öncelikle “sır” kavramından ne anlaşılması gerektiği ortaya konulmalıdır. Aksi durumda, hekimlerin hastalarıyla ilgili yaptığı her açıklamanın sır saklama yükümlülüğünün ihlali anlamına gelir. Sır; hukuki, etik ve ahlaki, deontolojik yönü olan disiplinler arası bir kavramı teşkil etmektedir¹⁰². Bu nedenle, bütün disiplinler açısından kabul görecektir ortak bir sır kavramının ortaya konması güçtür. Doktrinde sır kavramı farklı şekillerde tanımlanmıştır; ancak biz genel olarak “*açıklanmamasında hastanın menfaati bulunan her şey*”¹⁰³ olarak tanımlayabiliriz.

Hastaya ait sır dediğimizde sadece hastanın sağlığı ile ilgili özel bilgiler değil, buna ilaveten kişisel, ailevi, mesleki, ekonomik ve mali durumunu içeren bilgiler dahi sır kapsamında anlaşılmalıdır¹⁰⁴. Sır kapsamında yer alan bu bilgiler kişisel veridir ve bunlardan bir kısmı hassas veri kategorisinde yer almaktadır. Bu nedenle hekimin sır saklama yükümü kişisel verilerin korunması amacıyla hizmet etmektedir.

Hekimin mesleğin icrası sırasında hastanın kendinden veya hısımlarından doğrudan doğruya veya dolayısıyla öğrendiği, gerek tıbbi gerek tıbbi olmayan

¹⁰¹ Vikipedi, Hipokrat Andı, http://tr.wikipedia.org/wiki/Hipokrat_Yemini, E.T. 11.10.2014.

¹⁰² Maral Törenli Çakıroğlu, “*Hekimin Borçlarından Özel Olarak Sır Saklama Borcu*”, DEÜHFD, C. 12, S. 2, Y. 2010, s.170.

¹⁰³ Murat Doğan, “*Hekimin Hukuki Sorumluluğu*”, Tıbbi Müdahaleden Kaynaklanan Hukuki Sorumluluk Sempozyumu (Mersin 2009), s.41.

¹⁰⁴ Törenli Çakıroğlu, s.171.

hususlar sır sayılır¹⁰⁵. Hastanın herkese anlattığı veya doğası gereği açık olan bilgiler mesela hastanın bir bacağının olmaması felçli olması gibi bilgiler sır saklama yükümlülüğü kapsamında değerlendirilmemelidir¹⁰⁶. Ya da mahkeme bir şahsın belirli bir hastalığından dolayı kısıtlanmasına karar vermiş ve bu karar da ilan edilmiş ise, hekimin bu bilgiyi başkalarına söylemesi sır saklama yükümlülüğüne aykırı olarak değerlendirilmemelidir¹⁰⁷. Hekimin özel hayatında elde ettiği bilgiler, ayrıca resmi bir hasta hekim ilişkisi olmaksızın örneğin komşunun hekime asansörde karşılaştığında şikâyetlerini belirtmek üzere aktardığı bilgiler de sır saklama kapsamında değildir¹⁰⁸.

Hekimin sır saklama yükümlülüğü hasta ile aralarında yapmış oldukları sözleşme gereği olabileceği gibi bu yükümlülük aynı zamanda şahsiyet haklarına saygılı davranmanın da doğal neticesidir. Bireyin olduğu kadar hekimin ailenin ve de toplumun korunan menfaatleri söz konusu olabilmektedir¹⁰⁹. Hastanın özel bir hastaneye başvurması durumunda, hasta ile hekim arasında herhangi bir sözleşme ilişkisi doğmayacaktır. Bu ihtimalde hasta ile hastane arasında hastaneye kabul sözleşmesi adı verilen karma nitelikli bir sözleşme oluşacaktır. Bu sözleşmenin tarafı doktor değil hastanedir. Eğer tıbbi müdahale kamuya ait bir sağlık kuruluşunda özellikle bir kamu hastanesinde meydana gelmesi durumunda hasta bir kamu hizmeti almış olur ve devletin sorumluluğuna gidilir¹¹⁰.

Tıbbi sorumluluk hukukunda tıpkı hekimin sır saklama yükümü gibi hastane işletmecisi ve hastanede çalışan tüm personelin de, bakım ve tedavi hizmetlerinin ifası sürecinde hasta ile ilgili olarak edinilen ve gizlilik niteliği bulunan her türlü bilgiyi üçüncü kişilere aktarmama yükümü vardır¹¹¹. Tedaviyi bizzat yürüten hekim sır saklama yükümü altında olmakla birlikte bilgisine müracaat edilen hekimler, maiyetinde çalışan asistanlar, ebe, hemşire, hasta bakıcı ve idari memurlar da bu yükümlülük altındadırlar. Örneğin doğum için hastaneye müracaat eden bekar bir kadın için sır saklama yükümlülüğü bütün bu kimseler için söz konusu olmalıdır¹¹².

¹⁰⁵ **Hans Langmack**, “*Ceza Hukuku Açısından Hekimin Sır Saklama Yükümü*”, çeviren; **Erdener Yurtcan**, İÜHFİM, C.39, S.1-4, Y. 1974, s.455.

¹⁰⁶ **Hakeri**, s.800.

¹⁰⁷ **Yusuf Büyükay**, “*Hekimin Sır Saklama Yükümlülüğü*”, Atatürk Üniversitesi Erzincan Hukuk Fakültesi Dergisi, C. VIII, S.1-2 (2004), s.387.

¹⁰⁸ **Hakeri**, s.801.

¹⁰⁹ **Büyükay**, s.383-384.

¹¹⁰ **Doğan**(Murat), s.42.

¹¹¹ **Mehmet Demir**, *Tıbbi Organizasyon Kusuru Açısından Hastanelerin Hukuksal Sorumluluğu*, Ankara 2010, s.236.

¹¹² **Büyükay**, s.387-388.

Sır saklama, hekimlerin en önemli ödevlerinden birisi olsa da; istisnaları bulunmaktadır. Hekimin sır saklama yükümlülüğü mutlak bir kural değildir. Kimi durumlarda hekimin sır saklama yükümlülüğü tamamen kalkar, kimi durumlarda ise sınırlanır. Hukuka uygun sır açıklamaları şu şekildedir;

İlk olarak sır sahibi hastanın kendisine ait sırların açıklanmasına rıza göstermesi en temel hukuka uygunluk hallerinden biridir¹¹³. Ancak kişinin rızasının bulunması hekime kişinin bilgilerini sınırsız olarak açıklama hakkı vermez. Nitekim Hasta Hakları Yönetmeliği'nin 23. maddesinde, bilginin açıklanması kişilik haklarından bütünüyle vazgeçilmesi, bu hakların başkalarına devri veya aşırı şekilde sınırlanması neticesini doğurması halinde, hastanın rızasının bunları açıklayanın hukuki sorumluluğunu kaldırmayacağı düzenlenmiştir. Rızaya dayalı bilgi açıklaması kişilik hakkının sınırları dâhilinde ölçülü bir şekilde kullanılmalıdır.

İkincisi ise Umumi Hıfzıssıhha Kanunu'ndan kaynaklanmaktadır. Hekimler halk sağlığını yakından ilgilendiren durumlarla karşılaştıklarında söz konusu durumu ilgili yetkili makama bildirmekle yükümlüdürler. Umumi Hıfzıssıhha Kanunu'nun 57, 97, 107, 114. maddelerinde yer alan bazı bulaşıcı tehlikeli hastalıkların duyurulması gerekmektedir^{114, 115}.

Üçüncüsü zorunluluk halidir. Hekimin mesleğini icra ederken öğrendiği hastaya ait bir sır, üçüncü kişilerin hayatları ya da sağlıkları için ciddi bir tehdit

¹¹³ Törenli Çakıroğlu, s.174.

¹¹⁴ Hayrunnisa Özdemir, “Hadım Etme ve Hekimin Sır Saklama Yükümlülüğü”, Gazi Üniversitesi Hukuk Fakültesi Dergisi, C. XIV, S.1, Y. 2010, s.158.

¹¹⁵ UHK m.57'ye göre “Kolera, veba (Bübön veya zatürree şekli), lekeli humma, karahumma (hummayi tiroidi) daimi surette basil çıkaran mikrop hamilleri dahi - paratifoit humması veya her nevi gıda maddeleri tessemmümatı, çiçek, difteri (Kuşpalazı) - bütün tevkiatı dahi sari beyin humması (İltihabı sahayai dimağii şevkii müstevli), uyku hastalığı (İltihabı dimağii sari), dizanteri (Basilli ve amipli), lohusa humması (Hummai nifası) ruam, kızıl, şarbon, felci tifli (İltihabı nuhai kuddamii sincabii haddi tifli), kızamık, cüzam (Miskin), hummai racia ve malta humması hastalıklarından biri zuhur eder veya bunların birinden şüpheli veyahut bu hastalıklardan vefiyat vuku bulur veya mevtin bu hastalıklardan biri sebebiyle husule geldiğinden şüpheli olursa aşağıdaki maddelerde zikredilen kimseler vak'ayı haber vermeğe mecburdurlar. Kudurmuş veya kuduz şüpheli bir hayvan tarafından ısırılmaları, kuduz müptela hastaların veya kuduzdan ölenlerin ihbarı da mecburidir”. Aynı Kanun 97. maddesinde sıtmalı hastaların, 104. maddesinde frengi hastalarının, 107. maddesinde zührevi hastalığa sahip olanların, 114. maddede veremli hastaların ilgili birimlere bildirilmesi gerektiği düzenlenmiştir. UHK m.57 ve ilgili diğer düzenlemelerde AIDS ile ilgili her hangi bir açıklamaya yer verilmemiştir. Bu durumda, kendisine gelen hastanın AIDS olduğunu anlayan hekimin bunu ilgili makamlara ve hastanın yakınlarına (örneğin hastanın eşine) bildirmek zorunda olup olmadığı ortaya konulmalıdır. 1985 yılında bildirilen ilk HIV(+) olgunun ardından, Sağlık Bakanlığı Genelgesi ile HIV/AIDS bildirimini zorunlu hastalıklar listesine alınmıştır. 1986 yılında tüm kan ve kan ürünlerinin HIV yönünden taranmasına ilişkin genelge yürürlüğe girmiş ve 1987'de serolojik testler yapılmaya başlanmıştır. 1994 yılında ise HIV/AIDS bildirimleri, kodlu hale getirilmiştir.

oluşturursa hekimin durumu yetkili mercilere ve ilgili şahıslara bildirmesi gerektiği ifade edilmektedir¹¹⁶.

Dördüncü hal bilirkişiliktir. Hekim, bilirkişi olarak tayin edilmişse hastayı muayene edip tespit ettiği hususları düzenlemiş olduğu bir raporla mahkemeye sunmak zorundadır. Bu durumda sır saklama yükümlülüğü söz konusu olmayacaktır¹¹⁷. Hekim, bilirkişi olarak atanması durumunda hasta ile alakalı tüm tetkikleri, hastanın kendisine anlattığı tıbbi sırları objektif olarak mahkemeye sunmak zorundadır, bu durumda meslek sırrını açıklama suçu oluşmayacaktır¹¹⁸.

Hasta tarafından hekime karşı açılan davada, hekimin kendisi savunmak amacıyla hasta hakkındaki bilgileri açıklayıp açıklayamayacağı¹¹⁹ ve tedavi ücretini tahsil edemeyen hekimin bu amaçla açtığı davada hastaya ait bilgileri açıklayıp açıklayamayacağı konusu tartışmalıdır¹²⁰. Kanaatimizce hekim, ölçülü olmak kaydıyla ispata yetecek bir kısım verileri açıklamalıdır.

5271 sayılı CMK m.46/1-b hükmünde de, hekimlerin sır saklama yükümlülüğüne işlerlik sağlama adına, hekimlerin tanıklıktan çekinebileceği düzenlenmiştir; yine aynı maddenin ikinci fıkrasında hastanın rızasının bulunması durumunda hekimin tanıklık yapmasının zorunlu olduğu belirtilmiştir. Tanıklıktan çekinme 6100 sayılı Hukuk Muhakemeleri Kanunu'nun 249. maddesinde de CMK m.46/1-b hükmüne benzer şekilde düzenlenmiştir. Hüküm şu şekildedir; *“Kanun gereği sır olarak korunması gereken bilgiler hakkında tanıklığına başvurulacak kimseler, bu hususlar hakkında tanıklıktan çekinebilirler. Ancak, 19/3/1969 tarihli ve 1136 sayılı Avukatlık Kanunu hükmü saklı kalmak üzere sır sahibi tarafından sırrın açıklanmasına izin verildiği takdirde, bu kimseler tanıklıktan çekinemezler”*.

Hekimin ihbar yükümlülüğü de (TCK m.280) sır saklama yükümlülüğünün bir istisnası olarak kabul edilmektedir. Yaralanmış, zehirlenmiş veya saldırıya uğramış bir kimseyi tedavi eden hekimin olayı adalete bildirmesi mağdura ait bir sırrı açıklama anlamına gelmez. Çünkü sır mağdura ait olmayıp saldırıyı yapan kişi için önemlidir¹²¹.

¹¹⁶ **Büyükcay**, s.390.

¹¹⁷ **Törenli Çakıroğlu**, s.178.

¹¹⁸ **Doğan**(Cahid), s.127.

¹¹⁹ Hasta tarafından hekime karşı açılan davada, hekimin kendisi savunmak amacıyla hasta hakkındaki bilgileri açıklayabileceği yönünde bkz. **Doğan** (Murat), s.53.

¹²⁰ **Büyükcay**, s.390.

¹²¹ **Cemal Öztürkler**, Hukuk Uygulamasında Tıbbi Sorumluluk, Teşhis, Tedavi ve Tıbbi Müdahaleden Doğan Tazminat Davaları, Ankara 2006, s.293-294.

Son olarak ferdileştirme yapılmaksızın yapılan açıklamalar şayet şartlara göre ferdileştirme mümkün değilse; mesela bilimsel eserlerde olduğu gibi isim zikretmeksizin yapılan bildirmelerin de hukuka uygun olduğu kabul edilmelidir¹²².

14. Hasta Mahremiyeti

Özel yaşam ya da mahremiyet genel olarak kişilerin yalnız başına kalabildikleri istedikleri gibi düşünüp davranabildikleri başkalarıyla hangi yer zaman ve koşullarda ne ölçüde ilişki ve iletişim kuracaklarına bizzat kendilerinin karar verebildikleri bir alanı ve bu alan üzerinde sahip olunan hakkı ifade eder¹²³. Mahremiyet sosyal ilişkilerde bireyler ve kurumlar arasında bir mekanizma olarak anlaşılmakta ve modern anlamıyla yalnız bırakılma hakkı olarak tanımlanmaktadır¹²⁴.

Mahremiyet, tıpta hastanın kişisel ve gizlilik düşüncesine saygının gelişmesine ve tıbbın temel bir amacı olan hastanın sağlık bakımından geliştirilmesi üzere iki amaca hizmet eder. Kişisel ve gizlilik düşüncesine saygının bir sonucu olarak, hastanın en özel fiziksel ve psikolojik sırları mahcubiyetini ve hassasiyetini azaltmak için gizli tutulur¹²⁵.

Hasta Hakları Yönetmeliği'nin "mahremiyete saygı gösterilmesi" başlıklı 21. maddesinde hastanın, mahremiyetine saygı gösterilmesinin esas olduğu, her türlü tıbbi müdahalenin hastanın mahremiyetine saygı gösterilmek suretiyle icra edileceği, 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 alınacağı düzenlenmiştir.

Bu hastaların muayeneleri sırasında bir yakınlarının yanlarında bulunması ve tedavi ile doğrudan ilgisiz kişilerin odada bulunmaması düzenlenmiştir. Hatta araştırma hastanelerinde stajyer veya öğrencilerin bulunmasını reddetmesi bir hasta hakkı olarak tanınmış olmasına rağmen uygulamada buna pek fazla riayet edilmediği gözlenmektedir¹²⁶.

¹²² Langmack, s.462.

¹²³ Mehmet Yüksel, "Mahremiyet Hakkı ve Sosyo-Tarihsel Gelişimi", Ankara Üniversitesi SBF Dergisi, C. 58, S. 1, Y.2003, s.182.

¹²⁴ Gürsoy Akça/ Doğa Beşer, "Karanlığın Yok Oluşu" Gelişen Teknolojinin Gizlilik ve Mahremiyet Üzerindeki Etkileri", Muğla Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, Bahar 2011 S; 26, s.24.

¹²⁵ M. Cumhuri İzgi, "Mahremiyet Kavramı Bağlamında Kişisel Sağlık Verileri", Türkiye Biyoetik Dergisi, C.1, S.1, Y. 2014, s.33.

¹²⁶ Deryal, s.83.

15. Avrupa İnsan Hakları Sözleşmesi'nde ve Avrupa İnsan Hakları Mahkemesi Kararlarında Kişisel Veriler

4 Kasım 1950 yılında Roma'da imzalanan ve Türkiye tarafından da 18 Mayıs 1954 tarihinde onaylanmış bulunan Avrupa İnsan Hakları Sözleşmesi olarak bilinen, İnsan Haklarının ve Temel Özgürlüklerin Korunmasına Dair Avrupa Sözleşmesi'nin 8. maddesi özel hayata ve aile hayatına saygı başlığını taşımaktadır. Bu maddenin birinci fıkra hükmüne göre “herkes özel hayatına, aile hayatına, konutuna ve haberleşmesine saygı gösterilmesi hakkına sahiptir”¹²⁷. Sözleşmede kişisel verilerle ilgili bir hüküm yoktur ancak mahkeme konuyla ilgili ilk kararlarından itibaren bireyin özel yaşamıyla ilgili bilgilerin toplanmasını ve gizli bilgi kütüğünde saklanmasını ve bu tür bilgilerin ilgililere verilmesini sözleşmenin 8. maddesi kapsamında değerlendirmiştir¹²⁸.

25.02.1997 tarihli Z-Finlandiya kararı kişisel ve tıbbi bilgilerin 8. maddenin koruması altında olduğuna hükmedilmesi bakımından önem taşımaktadır¹²⁹. Dava konusu olay HIV hastası olan başvuran hakkındaki tıbbi bilgilerin cinsel saldırıyla ilgili dava sırasında ifşa edilmesidir¹³⁰.

Mahkeme'ye göre, sağlık verilerinin gizliliğine saygı gösterilmesi, Sözleşme'ye taraf devletlerin yasal sistemlerinde temel bir prensiptir. Bu konunun önemi sadece bireyin mahremiyet hakkıyla değil, aynı zamanda tıp mesleğine ve genel olarak sağlık hizmetlerine güveniyle de ilgilidir. Böylece gizliliği korumamak tıbbi yardıma ihtiyaç duyan kişilerin, uygun tedaviyi görmeleri için gerekli olan kişisel bilgileri açıklamalarını veya işin başından tıbbi yardıma başvurmalarını caydıran sonuçlar doğurabilir. Mahkeme, bu durumun sadece söz konusu kişilerin sağlığını tehlikeye atmakla kalmayacağını, aynı zamanda bulaşıcı hastalıklar söz konusu olduğunda toplum sağlığını da tehlikeye atacağını belirtmiştir. Tıbbi verilerin korunması konusunda bir hastanın ve genel olarak toplumun hakları, bir suçun soruşturulması ve yargılanmasında ve yargılamanın kamuya açık olmasının yararından daha az ağırlıklı olabilir. Her bir dava, özel içeriğine göre değerlendirilmeli ve devletin bu konudaki takdir hakkı göz önünde bulundurulmalıdır¹³¹.

¹²⁷ Gilles Dutertre, Avrupa İnsan Hakları Mahkemesi Kararlarından Örnekler, Almanya 2003, s.199.

¹²⁸ Osman Doğru/ Atilla Nalbant, İnsan Hakları Avrupa Sözleşmesi Açıklama ve Önemli Kararlar, 2. Cilt, Ankara 2013, s.6.

¹²⁹ Berber/ Ülgü/ Er, s.108.

¹³⁰ Avrupa İnsan Hakları Mahkemesi, Kişisel Verilerin Korunması Bilgilendirme Notu, Temmuz 2012 http://www.inhak.adalet.gov.tr/tematik/bilgi/kisisel_veriler.pdf, E.T. 13.11.2014.

¹³¹ Dutertre, s.216-217-218.

Z-Finlandiya davasında Mahkeme, şahidin tıbbi kayıtlarının ifşasının, 8. maddenin 2. fıkrasındaki anlamıyla¹³², mahkeme açısından “gerekli” olduğuna karar vermiştir. Ancak Mahkeme, temyiz mahkemesi kararında şahidin adının ve HIV statüsünün yayınlanmasının herhangi bir meşru amaç için gerekli olmadığına karar vermiştir. Davacının tıbbi kayıtlarının detaylarını (HIV statüsü) içeren dava dosyalarının, 10 yıl sonra kamuya açık hale gelmesinden ve 10 yıl sonra söz konusu kişinin hala hayatta olma olasılığı olmasından yola çıkarak da Sözleşme’nin 8. maddesinin ihlal edildiği sonucuna ulaşmıştır¹³³.

Avrupa İnsan Hakları Mahkemesi 04.12.2008 tarihli S. ve Marper - Birleşik Krallık Davası’nda başvuruların haklarında açılan dava sürecinde alınan parmak izlerinin, hücre örneklerinin ve DNA profillerinin, beraat etmelerine ve başka bir davada ceza kovuşturmasına yer olmadığına karar verilmesine rağmen süresiz biçimde tutulmasına devam edilmesi yüzünden 8. maddenin ihlal edildiğine karar vermiştir¹³⁴.

Mahkeme, kişilerin parmak izleri, biyolojik örnekleri ve DNA profilleri gibi kişisel verilerinin saklanmasıyla ilişkin ayrıntılı hukuksal incelemeler ve karşılaştırmalar yaptıktan sonra, başvuranlar gibi suçlu olduğundan şüphelenilen fakat mahkûm edilmemiş kişilerin parmak izleri, biyolojik örnekleri ve DNA profillerinin muhafaza edilmesinde kamu çıkarları ve özel çıkarlar arasında adil bir denge sağlanamadığını, savunmacı devletin kabul edilebilecek takdir marjını aşmış olduğunu, uygulamanın demokratik bir toplumda gerekli görülemeyeceğini ve başvuruların özel yaşamlarına saygı gösterilmesi haklarına orantısız şekilde saldırı oluşturduğunu kabul ederek savunmacı devletin AIHS’nin 8. maddesine aykırı hareket ettiğine karar vermiştir¹³⁵.

Avrupa İnsan Hakları Mahkemesi 27.08.1997 yılında M.S. - İsveç Davası’nda başvuranın geçirdiği kürtaj hakkında bilgi içeren tıbbi kayıtların sosyal güvenlik kurumuna iletilmesinde 8. maddenin ihlalinin söz konusu olmadığı: söz

¹³² 8. maddenin 2. fıkrası şu şekildedir: “*Bu hakkın kullanılmasına bir kamu otoritesinin müdahalesi, ancak ulusal güvenlik, kamu emniyeti, ülkenin ekonomik refahı, dirlik ve düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için, demokratik bir toplumda zorunlu olan ölçüde ve yasayla öngörülmesi olmak koşuluyla söz konusu olabilir*”. Dutertre, s.239.

¹³³ **Ursula Kilkelly**, Özel Hayata ve Aile Hayatına Saygı Gösterilmesi Hakkı, (Avrupa İnsan Hakları Sözleşmesinin 8. Maddesinin Uygulanmasına İlişkin Kılavuz), Almanya 2001, s.68-69.

¹³⁴ Avrupa İnsan Hakları Mahkemesi, Kişisel Verilerin Korunması Bilgilendirme Notu, Temmuz 2012.

¹³⁵ **Mehmet Can Akyol**, Avrupa İnsan Hakları Mahkemesi S. ve Marper Birleşik Krallık Davası Kararı(Başvuru no: (Başvuru no.30562/04 ve 30566/04) Strazburg 4 Aralık 2008, <http://www.fap.hsyk.gov.tr/dosyalar/aihm-karar-inceleme/m8/sveMarperBirlesikKrallik.pdf> s.30-31, E.T. 13.11.2014.

konusu kurum, başvuranın sırf yararlanmasına yönelik tazminat talebini incelemekten sorumlu olduğu için ilgili kliniğin başvuranın tıbbi kayıtlarını iletmek için ilgili ve yeterli nedeni olduğu belirtilmiştir¹³⁶. Mahkeme davada, hak talebinde bulunan bir kişinin sigortadan yararlanması için tıbbi geçmişine ait bilgilerin Devletin tıbbi kurumları tarafından sosyal sigorta yetkililerine verilmesinin meşru olduğuna karar vermiştir. İfşa edilen bilgilerin sigorta talebiyle ilgili olduğu, bir gizlilik yükümlülüğü olduğu ve bilgilerin istismanı durumunda personele özel ve/veya ceza davası açılabileceği için Mahkeme bu önlemi orantılı bulmuştur¹³⁷.

16. Biyotıp Sözleşmesi

TBMM tarafından 5013 sayılı kanun numarasıyla 03.12.2003 tarihinde, İnsan Hakları ve Biyotıp Sözleşmesinin Onaylanmasının Uygun Bulduğuna Dair Kanunla kabul edilen Biyotıp Sözleşmesinin “özel yaşam ve bilgilendirilme hakkı” başlıklı 10. maddesi şu şekildedir:

“1. Herkes, kendi sağlığıyla ilgili bilgiler 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. İstisnai durumlarda, 2'nci paragrafta belirtilen hakların kullanılmasında hastanın yararları bakımından kanun tarafından kısıtlamalar öngörülebilir.”

Anayasamızın 20. maddesi son fıkrasında yer alan düzenlemeyle Sözleşmenin düzenlemesi benzer hükümler içermektedir.

17. Kişisel Verilerin Otomatik İşlenmesi Karşısında Bireylerin Korunmasına Dair Sözleşme

108 numaralı Kişisel Verilerin Otomatik İşlenmesi Karşısında Bireylerin Korunmasına Dair Sözleşme, Avrupa Konseyi tarafından 29 Ocak 1981 yılında Strasbourg'ta imzalanmıştır.

Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair Avrupa Sözleşmesi'nin, m.5/b ve e bentlerine göre, kişisel veriler:

“b- Belli ve meşru amaçlar için kaydedilmeli ve kaydedilme amacına aykırı şekilde kullanılmamalıdır;

¹³⁶ Avrupa İnsan Hakları Mahkemesi Kişisel Verilerin Korunmasına İlişkin Bilgi Notu, Temmuz 2012, http://www.inhak.adalet.gov.tr/tematik/bilgi/kisisel_veriler.pdf, E.T. 13.11.2014.

¹³⁷ Kilkelly, s.69-70.

e- İlgili kişilerin kimliklerini belirtecek bir biçim altında ve kaydedildikleri kaydedilme amacı için gerekli görülen süreyi aşmayacak bir süre için muhafaza edilmelidir.”

Sözleşmenin amacı *her biri tarafın ülkesinde uyrukluğ u veya ikametgâhı ne olursa olun her bir gerçek kişinin temel hak ve özgürlüklerini ve özellikle kendisiyle ilgili kişisel verilerin otomatik işleme tabi tutulması karşısında özel hayata saygı hakkını güvence altına almaktır*¹³⁸.

Sözleşme yalnızca otomatik işleme tabi tutulan verileri kapsamakta ve en önemlisi taraf devletler bakımından bağlayıcı nitelik taşımaktadır¹³⁹.

Bakanlar Kurulunca 21.07.2014 tarihinde kararlaştırılan “Kişisel Verilerin Otomatik İşlenmesi Karşısında Bireylerin Korunması Sözleşmesinin Onaylanmasının Uygun Bulunduğ una Dair Kanun Tasarısı” 01.08.2014 tarihinde meclise sunulmuştur. Tasarı şu anda meclis komisyonundadır¹⁴⁰.

Sözleşme 1981 yılında imzalanmıştır ancak Türkiye henüz sözleşmeyi uygun bulmamıştır. Sözleşmeyi imzaladığı halde kanunu çıkarmayan tek Avrupa Konseyi üyesi ülke Türkiye’dir. Kanun tasarısı 2014 yılında Meclise sunulmuş hala komisyonda beklemektedir. Sözleşmenin uygun bulunup yürürlüğe konulması otomatik işleme tabi tutulan verilerin korunması bakımından önemlidir.

18. Ekonomik İşbirliği ve Kalkınma Örgütü İlkeleri

Ekonomik İşbirliği ve Kalkınma Örgütü (OECD), 1980 yılında özel yaşamın korunması ve kişisel verilerin sınır ötesi akışına ilişkin yönlendirici ilkeleri yayınlamıştır. OECD üyeleri bakımından herhangi bir bağlayıcılık taşımayan bu ilkeler ulusal düzeydeki veri koruma yasalarının birbiri ile uyumlaştırılmasını amaçlamaktadır¹⁴¹.

19. Birleşmiş Milletler Genel Kurulu İlkeleri

Birleşmiş Milletler teknolojideki ilerlemeye bağlı olarak 1990 yılında bağlayıcı olmayan bir tavsiye yayımlayarak kişisel veri dosyalarının bilgisayar aracılığıyla işlenmesinde genel ilkeler öngörmüştür. Düzenleme üye devletlerin asgari bir standartta buluşmasını hedeflemektedir¹⁴².

¹³⁸ <http://www2.tbmm.gov.tr/d24/1/1-0966.pdf>, m. I, E.T. 22.10.2014.

¹³⁹ Aksoy, s.5.

¹⁴⁰ http://www.tbmm.gov.tr/develop/owa/tasari_teklif_sd.sorgu_yonlendirme E.T. 22.10.2014.

¹⁴¹ Aksoy, s.4

¹⁴² Başalp, s.24-25

20. Avrupa Birliği Direktifleri

Kişisel verilerin korunması konusunda çıkarılan en etkili özel koruma düzenlemesinin 24 Ekim 1995 tarih ve 95/46/EC sayılı, “Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Direktifi” olduğu söylenebilir¹⁴³. Avrupa Birliği’nin 1995 yılında yayınladığı 95/46/EC sayılı direktifin ardından söz konusu direktifi tamamlayıcı nitelikte başka direktifler de yayınlanmıştır. Tamamlayıcı olarak 15 Aralık 1997 tarih ve 97/66/EC sayılı “Haberleşmenin Gizliliği Direktifi”ni çıkarmıştır¹⁴⁴. Benzer bir düzenleme 12.07.2002 tarih ve 2002/58/EC sayılı “Özel Yaşamın Gizliliği ve Elektronik Haberleşme Direktifi” ile yapılmıştır. Bu direktifin, 95/46/EC sayılı Direktifi elektronik iletişim alanında tamamlayıcı özelliği bulunmaktadır¹⁴⁵. Ayrıca 15 Mart 2006 tarih ve 2006/24/EC sayılı “Kamuya Açık Haberleşme Hizmetleri veya Kamu Haberleşme Şebekesi ile Bağlantılı Olarak Üretilen veya İşlenen Verilerin Saklanması İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Direktifi” de 2002/58/EC sayılı direktifin bir tamamlayıcısı olarak kabul edilmiştir¹⁴⁶.

Bunun yanında 15 Şubat 2007 tarihinde Avrupa Birliği ulusal veri korunması görevlilerinden oluşan Article 29 Çalışma Grubu “Elektronik Sağlık Kayıtlarında Yer Alan Sağlığa İlişkin Verilerin İşlenmesine İlişkin Çalışma Dokümanı”ni yayınlamıştır. Çalışma Grubu elektronik sağlık kayıt sistemleri bakımından uygulanacak veri korunması yasal çerçevesinin yorumuna ilişkin olarak rehberlik etmekte ve bazı genel ilkeleri açıklamaktadır. Doküman ayrıca elektronik sağlık sistemlerinin kurulmasında göz önünde bulundurulması gereken veri korunması istekleri ile aynı şekilde ilgili koruma önlemlerine de işaret etmektedir¹⁴⁷.

21. Avrupa Konseyi’nin Tavsiye Kararları

Avrupa konseyinin birçok tavsiye kararı yayınlamıştır. Bunlardan bazıları şunlardır; 13 Şubat 1997 tarihli Tıbbi Verilerin Korunmasına İlişkin R(97) 5 No.lu Tavsiye Kararı, Telekomünikasyonda Veri Korunması Hakkındaki Ulusla-

¹⁴³ Akgül, Kişisel Verilerin Korunması, s.212.

¹⁴⁴ Akgül, Kişisel Verilerin Korunması, s.215.

¹⁴⁵ Başalp, s.24.

¹⁴⁶ Avrupa Adalet Divanı, Avrupa Parlamentosu’nun, Kişisel Verilerin Tutulmasına İlişkin 15 Mart 2006 tarih ve 2006/24/EC sayılı Veri Tutulmasına İlişkin Direktif’i (Data Retention Directive) 8 Nisan 2014 tarihinde yürürlükten kaldırmıştır. Avrupa Adalet Divanı, 8 Nisan 2014 tarihli kararı ile, Direktif hükümlerinin Avrupa Temel Hakları Şartı’nın 7. maddesi ve Avrupa İnsan Hakları Sözleşmesi’nin 8. maddesine aykırı olduğu ve kişisel veri mahremiyetini ihlal ettiği kanaatine ulaşarak Direktifi yürürlükten kaldırmıştır (par. 34-36). Karar metni için bkz. **Grand Chamber**, Digital Rights Ireland Ltd. (C-293/12) v. Minister for Communications, Marine and Natural Resources, <http://eur-lex.europa.eu/legalcontent/EN/TXT/HTML/?uri=CELEX:62012CJ0293&rid=1> E.T. 13.01.2015.

¹⁴⁷ Berber/ Ülgü/ Er, s.137.

rarası Çalışma Grubu'nun "Elektronik Sağlık Kayıtlarının Online Kullanılabilirliğine İlişkin Çalışma Tablosu", AB Komisyonunun bilimde ve yeni teknolojilerde etişe ilişkin Avrupa Grubunun görüşü: Bilgi Toplumunda Sağlığa İlişkin Etik Sorunlar, Avrupa Konseyi Bakanlar Komitesinin üye devletlere yönelik Sigorta Amaçlarıyla Kişisel Verilerin Toplanması ve İşlenmesi Hakkında Tavsiye Kararı Rec (2002)9, Avrupa Konseyi Bakanlar Komitesinin üye devletlere yönelik Ödeme ve İlişkili Diğer İşlemlerde Kullanılan Kişisel Verilerin Korunması Hakkındaki R(90) 19 No.lu Tavsiye Kararı'dır.

B. Kişisel Sağlık Verilerinin Korunmasında İdarenin Yükümlülükleri

1. Kişisel Verileri Koruma Kurulu

Veri koruma otoriteleri kişisel verilerin korunması açısından güvence sağlayan en önemli unsurlardandır. Veri koruma kanunu bulunan 99 ülkeden 85'inde veri koruma otoritesi oluşturulmuştur. Uluslararası düzenlemelerde bu otoritelerin üzerlerine düşen görevi gerektiği şekilde yerine getirebilmeleri için bağımsız (independent), tarafsız (impartial) ve teknik kapasite açısından yetkin ve yeterli (technically competent) yapıda oluşturulmalarına vurgu yapılmıştır¹⁴⁸.

Kişisel verilerin etkin şekilde korunması için ülke düzeyinde teşkilata ihtiyaç vardır. Adalet Bakanlığı tarafından 08.06.2012 tarihinde Başbakanlığa gönderilen, Kişisel Verilerin Korunması Kanunu Tasarısı'nda bağımsız bir kişisel verileri koruma kurulu kurulacağı belirtilmiştir.

Tasarının 18. maddesinde bu kanunla verilen görevleri yapmak üzere, bağımsız bir Kişisel Verileri Koruma Kurulu oluşturulacağı, 19. maddesinde Kurul'un görev ve yetkileri düzenlenmiştir. Görevleri şunlardır; kişilik hakları ihlâl edilenlerin başvuruları hakkında karar vermek, kişisel verilerin işlenmesine ilişkin konularda düzenleyici işlemleri hazırlamak, veri koruma hukuku alanındaki gelişmeleri takip etmek ve bunların uygulanması için gerekli önlemleri almaktır.

Tasarının 15. maddesine göre Kişisel Verileri Koruma Kurulu Genel Sekreterliği'nin veri kütüğü sicili tutması gerekmektedir. Kişisel verileri işleyen gerçek ve tüzel kişilerin veri kütüğü kurmadan önce sicile kaydolmak zorunda olduğu düzenlenmiştir. Bu düzenleme sayesinde kişisel veri işleyen gerçek ve tüzel kişiler kayıt altında tutulacaktır.

Adalet Bakanlığı tarafından hazırlanan, Bakanlar Kurulunca 7.04.2008 tarihinde kararlaştırılan, 22.04.2008 tarihinde meclise sunulan Kişisel Verilerin

¹⁴⁸ Cumhurbaşkanlığı Devlet Denetleme Kurulu'nun 27.01.2013 tarih ve 2013/3 sayılı Kişisel Verilerin Korunmasına İlişkin Ulusal ve Uluslararası Durum Değerlendirmesi ile Bilgi Güvenliği ve Kişisel Verilerin Korunması Kapsamında Gerçekleştirilen Denetim Çalışmaları Raporu.; <http://www.tccb.gov.tr/ddk/ddk56.pdf>, s.791, E.T. 03.11.2014.

Korunması Kanunu Tasarınının 19. maddesinde kişisel verileri koruma kuruluna ön inceleme yapma görevi verilmişti. Şu an mecliste bulunan tasarıda ön incelemeye yer verilmemiştir. Hükme göre kurul, gerçek ve tüzel kişiler veri işleme başlamadan önce bir ön inceleme yapar, ön inceleme sonuçlanmadan veri işlemesi yapılamaz. Bu düzenleme verisi işlenecek kişilerin, kişiliklerine, temel hak ve özgürlüklerine yönelik risk taşıma ihtimali olan ve kişisel verilerin işlenmesine ilişkin ilkelere uygun olmayan ve sağlık verileri için gerekli koşulları taşımayan veri işlemlerini tespit etmek bakımından gerekli olduğu için şu an mecliste bulunan tasarıda ön incelemeye yer verilmemesi eksikliklerdir.

2. Veri İşleme Yetkisi Kanunla Tanınmış Olmalıdır

Kamu hizmeti sunan idarelere, kişisel verilerin kaydedilmesine ve işlenmesine olanak tanıyan (yetki veren) açık bir yasal düzenleme bulunmalıdır¹⁴⁹. Yasal dayanak olmadan kişisel verilerin kaydedilmesi ve işlenmesi hukuka aykırıdır¹⁵⁰.

Kişisel verilerin işlenebilmesi için, esas olarak hukuksal bir temelin bulunması (şekli izin kaydı) zorunludur ve bu yasal düzenlemenin ilgilinin kişisel verilerinin korunması hakkına müdahaleyi içerik olarak haklı kılması gerekmektedir¹⁵¹. Kişisel verilerin kaydedilmesi ancak bu kaydetme veri toplamının yasal amacı için gerekli ise söz konusu olmalıdır¹⁵².

¹⁴⁹ Yapılan işlemlerin kayıtlarının tutulması gerektiği Tababet ve Şuabatı Sanatlarının Tarzı İcrasına Dair Kanunda (R.G.'de yayın 14.04.1928) 72. maddede belirtilmiştir. Buna göre hastaların isim ve hüviyetlerini kayda zorunludur. Özel Hastaneler Yönetmeliği (R.G.'de yayın 27.03.2002), m.48, m.34 ve 50'inci maddelerinde kayıt zorunluluğu öngörülmüştür. Yataklı Tedavi Kurumları İşletme Yönetmeliği'nde (13.1.1983 tarihli ve 1927 sayılı R.G. ve değişiklik 05.05.2005 tarihli ve 25806 sayılı R.G.) m.66-70, m.71-76 ve 81-87'inci maddelerde kayıt zorunluluğu öngörülmüştür.

¹⁵⁰ "İdarelerce, gelişen teknolojinin kamu hizmetlerinin etkin ve verimli yürütülmesini kolaylaştırıcı etki sağlaması amacıyla, kamu kesiminde kullanılmaya başlanması mümkün olmakla birlikte, teknoloji kullanılarak kişisel verilerin kayıt altına alınması ve uygulamasının ilgili Anayasal düzenleme uyarınca belirli bir yasal çerçeve içine oturtulması, konuya ilişkin usul ve esasların yasa hükmü ile tespit edilmesi ve yine Anayasa'daki ve uluslararası metinlerdeki temel hak ve özgürlüklere ilişkin hükümlere uygun olması gerektiği kuşkusuzdur. Pozitif hukukumuzda kişisel verilerin işlenmesine ilişkin olarak Anayasanın 20. Maddesi hükmü çerçevesinde yürürlüğe konulmuş yasal bir düzenleme bulunmadığı gibi... kanunda davalı kuruma yetki veren bir düzenleme yer almamaktadır.

Bu bağlamda, Anayasa'nın yukarıda alıntısı yapılan hükümleri ve uluslararası metinler uyarınca güvence altına alınan ve kanunla düzenlenmesi gereken kişisel verilerin işlenmesine ilişkin olarak uygulamanın sınırlarını, kişisel verinin nasıl depolanıp kullanılacağını tespit eden usul ve esasları gösteren bir düzenleme olmadan çıkarılan dava konusu Yönetmelik hükmünde hukuka ayarlık bulunmamaktadır." denilmektedir. Danıştay İdari Dava Daireleri Genel Kurulu'nun 06.03.2014 tarih ve YD itiraz No. 2013/819 sayılı kararı, (Kazancı İçtihat Bilgi Bankası, <http://www.kazanci.com/kho2/ibb/giris.htm> E.T. 13.10.2014).

¹⁵¹ **Oğuz Şimşek**, Anayasa Hukukunda Kişisel Verilerin Korunması, İstanbul 2008, s.99.

¹⁵² **Şimşek**, s.99.

Veri toplama amacı dışında, meşru bir amaçla kaydetme ancak bu tür bir kaydetmenin toplama amacına izin veren yasal düzenleme tarafından öngörülmesiyle söz konusu olabilir. Amaca aykırı ya da yasal amaca dayanmayan kaydetmeler hukuka aykırıdır¹⁵³.

Temel hak ve hürriyetlere ilişkin olarak, açık kanun hükmüyle herhangi bir düzenleme bulunmadığı müddetçe, kişisel verilerin kaydedilemeyeceği açıktır. Anayasamızın 13. maddesine göre; özgürlük asıl, sınırlama ise istisnadır¹⁵⁴. Bu nedenle, bir temel hak ve hürriyeti sınırlayan kanun hükmü bulunmadığı müddetçe özgürlüğe müdahale edilmesi hukuka aykırıdır. Bir temel hak, kanun ile açıkça sınırlanmadıkça, bu hakkın kullanılması engellenemeyeceği gibi, bu hakka kamu otoriteleri tarafından müdahale de edilemez.

Kişisel sağlık verisi toplayacak kişi ve kurumlar tespit edilmeli, bu kişi ve kurumlar dışındaki kişi ve kurumların veri toplamasına engel olunmalıdır. Nitekim Kişisel Verilerin Korunması Kanunu Tasarısı 6. maddesinde kişisel sağlık verilerinin sır saklama yükümü altında bulunan kişiler tarafından işlenebileceği düzenlenmiştir. Kanuni dayanak olmaksızın yetkisiz kişilerce veri toplanması Anayasa'ya aykırıdır. İdare gerekli denetimleri yaparak kanuni dayanak olmaksızın yetkisiz kişilerce veri toplanmasına ve işlenmesine engel olmalıdır.

3. Kişisel Verilerin Toplanmasında Amaç, Asgarilik ve Verilerin İmhası

Öncelikle hastanın verilerinin toplanmasındaki amaç dikkate alınarak amaçla bağdaşmayan veri toplamalarına engel olunmalıdır. Yani toplanan veriler ancak anılan amaç için önemli olmaları sebebiyle işlenmelidir. Toplanacak kişisel veri miktarının sınırlı tutulması yani asgarilik ilkesi açısından amacın belirlenmesi önemlidir.

Sağlık Bakanlığı'nın sağlıkta dönüşüm programı kapsamında hazırladığı Sağlık.NET, sağlık kurumlarında elektronik ortamda üretilen verileri, doğrudan üretildikleri yerden, standartlara uygun şekilde toplamayı, toplanan verilerden tüm paydaşlar için uygun bilgiler üreterek birinci, ikinci ve üçüncü basamak sağlık hizmetlerinde verim ve kaliteyi arttırmayı hedefleyen, entegre, güvenli, hızlı ve genişleyebilen bir bilgi ve iletişim platformu¹⁵⁵ olarak tanımlanmaktadır.

¹⁵³ Şimşek, s.99.

¹⁵⁴ Nihat Bulut, "4709 Sayılı Kanunla Yapılan Anayasa Değişikliği Çerçevesinde Hak ve Özgürlüklerin Sınırlanması Rejiminin Birey Devlet İlişkisi Açısından Değerlendirilmesi", AÜEHFD, C. V, S. 1-4, Y. 2001, s.41; İbrahim Kaboğlu, Özgürlükler Hukuku, İstanbul 1994, s.68.

¹⁵⁵ 25 Soruda 'Sağlık NET 2' Sistemi <http://www.istabip.org.tr/icerik/net2sorucevap.pdf>, E.T. 13.10.2014.

Sağlık.Net'in sağlık sektöründe sorunların ve önceliklerin belirlenmesinde, önlemlerin alınmasında, sektör kaynaklarının, çalışma ve yatırımların planlanmasında, sunulan sağlık hizmetlerinin kalitesinin değerlendirilmesinde aldığı rolün yanı sıra bilimsel araştırma ve çalışmalarda kullanılmak üzere yeterli düzeyde veri toplayacak ve işleyecek bir fonksiyon üstlendiği belirtilmiştir¹⁵⁶.

Sağlık.NET 2 sistemi, kamu ve özel bütün sağlık kuruluşlarını hastayla ilgili birçok bilgi toplayıp merkezi sisteme göndermekle yükümlü tutmaktadır. Sistemin toplayıp merkezi sisteme göndermekle yükümlü tuttuğu bilgiler yalnızca bildirim zorunlu hastalıklara ilişkin değildir. Bunların yanı sıra istenen bilgiler içinde; kimlik, adres, iletişim bilgileri, hamilelik testleri, sağlık geçmişi, özrürlük durumu, medeni hal, alkol-madde-sigara kullanımı, iş, meslek, öğrenim durumu, eğitim kurumuna devam etme durumu, gelir durumu, ailesinde intihar girişimi, cinsel partner bilgileri, kişisel bakım, kişisel hijyen, mahkumiyet/tutukluluk durumu, hastalık şikayetleri, hastanın öyküsü (anemnezi), bütün tetkik sonuçları, tetkik istenen kurumlar, 15-49 yaş arası kadınların, doğum, düşük türü ve sayıları, kadın sağlığı işlemleri, kullanılan aile planlaması yöntemi, gebelik tespiti sonuçları, son adet tarihi, babanın kan grubu, gebe olduğu tespit edilmiş olsun ya da olmasın, doğum ya da düşükle sonuçlanan tüm gebelikler, ağız ve diş sağlığı ile ilgili tüm koruyucu hekimlik, teşhis ve tedavi işlemleri ve daha pek çok bilgi yer almaktadır¹⁵⁷. Bu bilgiler arasında alkol-madde-sigara kullanımı, sağlık geçmişi gibi kişinin sağlığıyla ilgili olup, hassas kişisel veri kategorisinde yer alan bilgiler de bulunmaktadır.

Sağlık Bakanlığı tarafından hastaların bütün sağlık verilerinin kişilerin kimlikleri anlaşılabilir biçimde ve sınırlandırılmadan toplanması uluslararası ve ulusal alandaki kişisel verileri koruyucu düzenlemelere aykırıdır. Nitekim Danıştay bir kararında kamu kurum ve kuruluşlarının yürüttükleri kamu hizmeti sırasında, hizmetten yararlanan kişilerin bazı kişisel verilerine ulaşmalarının hizmetin yürütülebilmesi için zorunluluk taşıdığını belirtmiştir. Ancak, ulaşılan bu kişisel verilerin hiçbir ayırım gözetilmeksizin, tümünün yazılı bir şekilde kayıt altına alınmasının, Anayasa'nın 20. maddesine aykırılık oluşturacağını, sadece hizmetin yürütülebilmesi için gerekli olan bilgilerin kayıt altına alınması gerektiğini belirtmiştir¹⁵⁸.

¹⁵⁶ <http://www.e-saglik.gov.tr/belge/1-33811/sagliknet-hakkinda.html>, E.T. 13.10.2014

¹⁵⁷ İstanbul Tabip Odası Hukuk Bürosu, "25 Soruda Sağlık.NET 2 Sistemi", <http://www.istabip.org.tr/icerik/net2sorucevap.pdf>, E.T. 13.10.2014.

¹⁵⁸ "Anayasanın 20. maddesinde, herkesin, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahip olduğu, özel hayatın ve aile hayatının gizliliğine dokunulamayacağı; herkesin, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahip olduğu, bu hakkın; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsadığı, kişisel verilerin, ancak kanunda öngörülen hallerde veya

Ayıklanmadan veri toplanması yanında Sağlık.NET 2 sistemi verileri merkezi olarak tek bir bilgisayar ortamında, tek bir fiziksel veri tabanında tutmaktır. Bu durum iki yönden sorunludur. Birincisi sistemin merkezi olmasıdır. Sistem merkezi olduğu için bir noktadan tüm verilere ulaşmak mümkündür. Bu nedenle bütün veriler kopya edilmeye müsait hale gelmektedir. İkinci sorun da hem doktor hem de hasta açısından sistemin zorunlu olmasıdır¹⁵⁹.

Mevcut durumda bilgilerin bu şekilde kayıt altına alınmasının, demokratik bir toplumda gerekli bir müdahale olarak kabul edilmesi mümkün değildir ve Sağlık.NET 2 uygulaması başta Anayasa'nın 20. maddesi olmak üzere hukuka aykırı bir uygulamadır. Bilgi içeriklerinin sınırlandırılması, azaltılması ve ayıklanmasının yanı sıra, ad ve soyadın kodlanması, sadece hasta ve hekimin göreceği şekilde şifrelenmesi, bilgilerin korumalı başka bir veri tabanına kaydedilmesi gibi pek çok araç kullanılarak amaca elverişli şekilde hasta verileri işlenebilir.

Veri toplanması yanında toplanan verilerden kullanım dışı kalan kişisel veriler imha edilmelidir. Cumhurbaşkanlığı Devlet Denetleme Kurulu'nun 27.01.2013 tarih ve 2013/3 sayılı Kişisel Verilerin Korunmasına İlişkin Ulusal ve Uluslararası Durum Değerlendirmesi ile Bilgi Güvenliği ve Kişisel Verilerin Korunması Kapsamında Gerçekleştirilen Denetim Çalışmaları Raporu'nda bu hususa değinilmiş ve şu şekilde ifade edilmiştir; *“kişisel verilerin üçüncü kişilerin eline geçmemesi için, kullanım dışı kalan veya mülkiyeti devredilen üzerine kişisel veri kaydedilmiş donanımların güvenli şekilde imhası veya bu donanımlar üzerindeki verilerin güvenli şekilde silinmesi gerekmektedir. Denetim kapsamındaki kurumlardan sadece birinde kullanım dışı kalan elektronik kayıt ortamlarının güvenli imhası ile ilgili yazılı politikanın bulunduğu, ancak bu kurumda da imha işlemi yerine getirmesi gereken personelin politikadan habersiz olduğu ve politikayı uygulamadığı tespit edilmiştir”*¹⁶⁰.

kişinin açık rızasıyla işlenebileceği, kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenleneceği kurala bağlanmıştır. ... Kamu kurum ve kuruluşlarının yürüttükleri kamu hizmeti sırasında, hizmetten yararlanan kişilerin bazı kişisel verilerine ulaşmaları hizmetin yürütülebilmesi için zorunluluk taşımaktadır. Ancak, ulaşılan bu kişisel verilerin hiçbir ayırım gözetilmeksizin, tümünün yazılı bir şekilde aylık periyotlarla kayıt altına alınması, Anayasa'nın 20. maddesi ile korunan özel hayatın gizliliğine aykırılık oluşturacağı gibi; tüm kişisel bilgilerin, her zaman, yürütülen hizmet için gerekli olduğundan söz edilemeyeceği açıktır. Bu durumda, sadece hizmetin yürütülebilmesi için gerekli olan bilgilerle ilgili olarak bir sınırlama getirilmeksizin, özel hayat ve aile hayatına ilişkin bilgilerin kartekse işlenemeyeceği belirtilmeksizin görüşmelere ait tüm kişisel verilerin kartekslere işlenmesini düzenleyen Yönerge'nin 8. maddesinin ikinci fıkrasında hukuka uygunluk bulunmamaktadır.” Danıştay 10. Dairesi E. 2011/7001, T.14.10.2011, (Kazancı İçtihat Bilgi Bankası, <http://www.kazanci.com/kho2/ibb/giris.htm>, E.T. 13.11.2014).

¹⁵⁹ Kırıldoğ, s.69.

¹⁶⁰ Devlet Denetleme Kurulu Raporu, s.809.

Avrupa İnsan Hakları Mahkemesi 04.12.2008 tarihli S. ve Marper - Birleşik Krallık Davası'nda başvuruların haklarında açılan dava sürecinde alınan parmak izlerinin, hücre örneklerinin ve DNA profillerinin, beraat etmelerine ve başka bir davada ceza kovuşturmasına yer olmadığına karar verilmesine rağmen süresiz biçimde tutulmasına devam edilmesi yüzünden 8. maddenin ihlal edildiğine karar vermiştir¹⁶¹. Mahkeme, kişilerin parmak izleri, biyolojik örnekleri ve DNA profilleri gibi kişisel verilerinin saklanmasına ilişkin ayrıntılı hukuksal incelemeler ve karşılaştırmalar yaptıktan sonra, başvuranlar gibi suçlu olduğundan şüphelenilen fakat mahkûm edilmemiş kişilerin parmak izleri, biyolojik örnekleri ve DNA profillerinin muhafaza edilmesinde kamu çıkarları ve özel çıkarlar arasında adil bir denge sağlanamadığını, savunmacı devletin kabul edilebilecek takdir marjını aşmış olduğunu, uygulamanın demokratik bir toplumda gerekli görülemeyeceğini ve başvuruların özel yaşamlarına saygı gösterilmesi haklarına orantısız şekilde saldırı oluşturduğunu kabul ederek savunmacı devletin AİHS'in 8. maddesine aykırı hareket ettiğine karar vermiştir¹⁶².

3473 sayılı Muhafazasına Lüzum Kalmayan Evrak ve Malzemenin Yok Edilmesi Hakkında Kanun Hükmünde Karamamenin Değiştirilerek Kabulü Hakkında Kanun¹⁶³ kapsamına giren kurum ve kuruluşların¹⁶⁴, ellerinde bulundukları arşiv malzemesi ile arşivlik malzemeyi korumak, tasnif edip saklamak, yönetmelikte belirtilecek bekletme ve saklama süreleri sonunda Devlet Arşivleri Genel Müdürlüğü'ne teslim etmek ve muhafazasına lüzum kalmayan evrak ve malzemeyi yok etmekle mükellef oldukları hükmü yer almaktadır. Ayrıca arşiv malzemesi ile arşivlik malzemenin temlik tasarruflar amacıyla kullanılmayacağı, tahrip ve tahrif edilemeyeceği ve yurt dışına çıkartılamayacağı hüküm altına alınmıştır(m.1 ve m.3). Kanunun 4. maddesinde kanun kapsamına giren kurum ve kuruluşların kurum arşivlerinde yapılacak ayıklama ve imha işlemleri için, bünyelerinde ayıklama ve imha komisyonları teşkil edeceği belirtilmiştir.

Söz konusu düzenlemenin kapsamına bazı kamu kurum ve kuruluşları, kamu iktisadi teşebbüsleri ile özel kanunlarla kurulan kamu bankaları ve teşekkülleri girmektedir. Sağlık alanında özel hastaneler de kişisel veri toplamaktadır. Özel hastaneler 3473 sayılı Kanun kapsamına alınmamıştır. Kişilerin verilerinin süresiz

¹⁶¹ Avrupa İnsan Hakları Mahkemesi, Kişisel Verilerin Korunması Bilgilendirme Notu, Temmuz 2012.

¹⁶² **Akyol**, s.30-31.

¹⁶³ 3473 sayılı Kanun, Kabul Tarihi: 28.9.1988, RG, T. 4.10.1988, S. 19949.

¹⁶⁴ "Genel ve katma bütçeli dairelerle (saklama, ayıklama ve imha işlemleri kendi mevzuatına tabi olmak kaydıyla Cumhurbaşkanlığı, Türkiye Büyük Millet Meclisi, Genelkurmay Başkanlığı, Milli Savunma Bakanlığı, İçişleri Bakanlığı, Dışişleri Bakanlığı ve Milli İstihbarat Teşkilatı hariç) mahalli idareler, üniversiteler ve bunlara bağlı sabit ve döner sermayeli kuruluşlar, kamu iktisadi teşebbüsleri, özel kanunlarla kurulan kamu bankaları ve teşekküllerden, elinde arşiv malzemesi ve arşivlik malzeme bulunduran kurum ve kuruluşların..."

şekilde depolanması kişilik hakkına saldırı niteliğindedir. Hassas veri kategorisinde yer alan kişisel sağlık verilerinin uzun süre saklanmaması, amaç hasıl olduktan sonra bu verilerin imhası gerekmektedir. Hasta verilerini toplayıp işleyen tüm kamu kurum ve kuruluşlarıyla özel kuruluşlar için geçerli olmak üzere belirli süreler geçtikten sonra toplanan verilerin imhası standarda bağlanmalıdır.

4. Kişisel Verilerin Paylaşılması

Kişisel verilerin korunması sadece kurum içi tedbirlerin alınması ile sağlanamamaktadır. Kişisel verilerin kurumlar arası paylaşımı da, verilerin korunması açısından önemli bir konuyu teşkil etmektedir. Kurumlar arası paylaşımın niteliği ve şekli kişisel verilerin korunması açısından önemlidir.

Devlet Denetleme Kurulu raporunda; diğer kamu kurumları ve özel kesim ile veri paylaşımında, hukuki dayanağın bulunup bulunmadığı, verilerin talep eden kurum için gerekliliği, talep edilen verinin ilgili kurumun hizmet gerekleri ile orantılı düzeyde olup olmadığı gibi hususlarda yeterli analiz yapılmadan ve etkin karar mekanizmaları oluşturulmadan veri paylaşıldığı yer almaktadır¹⁶⁵. Bazı kamu kurumlarının sahip olduğu verileri çevrimiçi (online) olarak kamu ve özel kesim kurum ve kuruluşları ile paylaştıkları belirtilmiştir. Ancak veri paylaşım talebinde bulunan kurum ve kuruluşların, çevrimiçi olarak ilgili kurumdan alacağı kişisel verilerin güvenliğini sağlama konusundaki yeterliliğinin araştırılmadığı, bu hususun veri paylaşım protokollerine de ya hiç, ya da yeterince yansıtılmadığı, paylaşılan verileri alan kurumdaki güvenlik düzeyi ile ilgili olarak, genellikle herhangi bir çalışma ve araştırmanın yapılmadığı belirtilmiştir¹⁶⁶.

Sağlık Bakanlığı ve Bağlı Kuruluşlarının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname'nin "bilgi toplama, işleme ve paylaşma yetkisi" başlıklı 47. maddesi şu şekildedir;

“(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 vasıta ile 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.

¹⁶⁵ Devlet Denetleme Kurulu Raporu, s.796.

¹⁶⁶ Devlet Denetleme Kurulu Raporu, s.796.

(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 vermeye yükümlüdür.

(4) Sağlık personeli istihdam eden kamu kurum ve kuruluşları ile özel hukuk tüzel kişileri ve gerçek kişiler, istihdam ettiği personeli ve personel hareketlerini Bakanlığa bildirmekle yükümlüdür.

(5) Bu maddenin uygulanmasına ilişkin hususlar Bakanlıkça çıkarılacak yönetmelikle düzenlenir”.

Maddeye göre Bakanlık ve bağlı kuruluşları bütün özel ve kamu sağlık kurum ve kuruluşlarından sağlık hizmeti alanların, kişisel bilgilerini ve bu kimselere verilen hizmete ilişkin bilgileri her türlü vasıtayla toplamaya, işlemeye ve paylaşmaya yetkilidir. Maddenin ikinci fıkrasında Bakanlık ve Bağlı Kuruluşlarının işlediği kişisel sağlık verilerini ilgili üçüncü kişiler ve kamu kurum ve kuruluşları ile görevlerinin gereği olarak ve görevlerini yapmalarına yetecek derecede paylaşabileceği belirtilmiştir. Maddede düzenlendiği şekliyle Bakanlığın paylaşma yetkisinin sınırı yoktur. Bakanlığın topladığı kişisel sağlık verilerini diğer kamu kurum ve kuruluşlarıyla ve özel kişi ve kurumlarla paylaşması gereksiz ve veri koruma ilkelerine aykırıdır.

Sağlık Bakanlığı ve bağlı kuruluşları, verilere erişiminde yarar bulunan kurumlarla verileri paylaşabilmelidir. Nitekim Avrupa İnsan Hakları Mahkemesi 27.08.1997 yılında M.S. - İsveç Davası'nda başvuranın geçirdiği kurtaj hakkında bilgi içeren tıbbi kayıtların sosyal güvenlik kurumuna iletilmesinde 8. maddenin ihlalinin söz konusu olmadığı; söz konusu kurum, başvuranın sırf yaralanmasına yönelik tazminat talebini incelemekten sorumlu olduğu için ilgili kliniğin başvuranın tıbbi kayıtlarını iletmek için ilgili ve yeterli nedeni olduğu belirtilmiştir¹⁶⁷. Mahkeme davada, hak talebinde bulunan bir kişinin sigortadan yararlanması için tıbbi geçmişine ait bilgilerin devletin tıbbi kurumları tarafından sosyal sigorta yetkililerine verilmesinin meşru olduğuna karar vermiştir. İfşa edilen bilgilerin sigorta talebiyle ilgili olduğu, bir gizlilik yükümlülüğü olduğu ve bilgilerin istismarı durumunda personele özel ve/veya ceza davası açılabileceği için Mahkeme bu önlemi orantılı bulmuştur¹⁶⁸.

Sosyal Güvenlik Kurumu'nun hastaların kişisel verilerine erişmesi gerekli ve yararlıdır. Ancak kararda da belirtildiği gibi Sosyal Güvenlik Kurumu bu verilerin gizlilik ve güvenliğini sağlamalı, başka kişi ve kurumlarla

¹⁶⁷ Avrupa İnsan Hakları Mahkemesi Kişisel Verilerin Korunmasına İlişkin Bilgi Notu, Temmuz 2012, http://www.inhak.adalet.gov.tr/tematik/bilgi/kisisel_veriler.pdf, E.T. 13.11.2014.

¹⁶⁸ Kil Kelly, s.69-70.

paylaşmamalıdır. Sosyal Güvenlik Kurumu dışındaki diğer sigorta şirketleri ile sağlık kurumları arasındaki bilgi akışı da kişisel veriler açısından önem arz etmektedir. Hastaların kişisel sağlık verileri, hastaların sigorta şirketleri ile paylaşılmaktadır. Burada sorun sigorta şirketleri tarafından hasta dosyalarının bir düzenleme olmadan, altyapısı olmadan, sınırlaması olmadan incelenmesidir¹⁶⁹.

Kişisel verileri koruma hukukunun temel mantığı bakımından Bakanlığın paylaşma yetkisi yasal sınırlamalarla daha da güvenceli hale getirilmelidir. Kişinin, sağlık hizmeti almak amacıyla verdiği bilgilerinin başka amaç için kullanılmaması esas olmakla birlikte KHK'nin bu hükmü¹⁷⁰ yürürlükte olduğu sürece en azından paylaşılacak bilgiler sınırlandırılmalıdır. Hangi amaç için veri talep ediliyorsa o amacı gerçekleştirmeye yetecek ölçüde verinin iletilmesi esas olmalıdır. Bu da kurumlar arası paylaşımında asgarilik anlamına gelir.

Bunun yanında bilgiler paylaşılmadan önce ilgili kişiden izin alınmalı ve kişi bilgilerinin hangi kurumla paylaşıldığını bilmelidir. Başbakanlık tarafından yayınlanan Birlikte Çalışılabilirlik Esasları Genelgesinde; *“kişisel verilerin, bilgiyi temin eden kurum dışında diğer kurumlarca kullanılmasında bilgiyi veren kullanıcının izni esastır. Bilgilerin korunmasından ve amacı dışında kullanılmamasından bilgiyi temin eden ve kullanan tüm kurum ve kuruluşlar ortak şekilde sorumludur. Teknoloji seçimlerinde, bu yönde mahremiyeti sağlayıcı çözümlere gidilmelidir”* şeklinde düzenlemeye gidilmiştir (m.1.3.5.2.)¹⁷¹.

Genelgede de ifade edildiği gibi verilerin kişinin izniyle paylaşılması veri koruması hukukunun amacına daha uygun olacaktır. Ayrıca verilerin paylaşıldığı kurum veya kuruluşların da aynı derecede bilgi güvenliği sağlayabilecek nitelikte olması gerekmektedir. Aksi halde veriyi asıl olarak işleyen kurumun almış olduğu güvenlik önlemlerinin önemi kalmayacaktır. Kurumlar arası paylaşımında güvenliği sağlamak için kurumlar arasında ortak bir gizlilik ve güvenlik

¹⁶⁹ **Gürkan Sert**, *“Kişisel Sağlık Verilerine Mesleki, Etik Yaklaşımlar”*, Kişisel Sağlık Verilerine Mesleki Yaklaşımlar Çalıştayı, İstanbul, 2013, s.13.

¹⁷⁰ Söz konusu kararnamenin bilgi toplama işleme ve paylaşma yetkisi başlıklı 47. maddesinin Anayasaya aykırılığı gerekçesiyle Anayasa Mahkemesi'ne başvurulmuştur. Anayasa Mahkemesi verdiği kararda, Bakanlığa verilen paylaşma yetkisinin genişliğinden, bu şekilde veri paylaşımının ölçülülük ilkesine aykırı olduğundan bahsetmemiştir. Mahkeme, temel hakların KHK ile düzenlenemeyeceği gerekçesiyle hükmü iptal etmiştir. Ancak 12.07.2013 tarihinde kabul edilen ve 02.08.2013 tarihli ve 28726 sayılı Resmi Gazete' de yayımlanan 6495 sayılı Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun'un 73/h-3'üncü maddesi ile 663 sayılı KHK'nin 47. maddesine iptal edilen hükümler aynı şekilde yeniden eklenmiştir.

¹⁷¹ E-Dönüşüm Türkiye Projesi Birlikte Çalışılabilirlik Esasları Rehberi, Sürüm 2.1, http://www.bilgitoplumu.gov.tr/wpcontent/uploads/2014/04/Birlikte_Calisabilirlik_Esaslari_Rehberi_2.1.pdf s.6, E.T. 28.10.2014.

politikasının belirlenmesi, güvenlik standardı sağlayamayan kurumlarla verilerin paylaşılmaması gerekmektedir¹⁷².

Bunun yanında paylaşılan verilerin anonimleştirilmesi veya takma isimle paylaşılması da koruma açısından alınabilecek önlemlerdendir. İsimsiz verilerle bir kişinin kimliğini belirli kılmak mümkün değildir. İsimsizleştirilmiş veriler (anonim veriler) belirli bir kişiyle ilgilidir, bilginin kimle ilgili olduğu belli değildir¹⁷³. Ancak isimsizleştirilmiş verilerde kişinin kimliği tespit edilebilir. Takma isimli verilerde ise bilginin kime ait olduğu yalnızca ilgili kod çözülerek belirlenebilir¹⁷⁴. Hastanın verilerinin doğrudan paylaşılması yerine anonimleştirilerek veya takma isimle paylaşılması koruma açısından daha uygundur.

Sağlık Bakanlığı tarafından hazırlanan Kişisel Sağlık Verilerinin İşlenmesi ve Veri Mahremiyetinin Sağlanması Hakkında Yönetmelik Taslağı'nın¹⁷⁵ 6. maddesinde veri paylaşımının esasları düzenlenmiştir. Madde şu şekildedir;

“(1) Kişisel sağlık verisini işlemek üzere isteyen kişi veya kuruluşlar, yazılı veya ispatlanabilir elektronik ortamda veri sorumlusuna veri paylaşım talebini bildirir. Veri sorumlusu talebi, mevzuatla tanımlanmış görevlerin ifa ve icrasına uygunluğu açısından değerlendirerek uygun görmesi halinde veri paylaşımını yapar. Veri paylaşım talebinde; kurum/kuruluş, kişi adı soyadı, iletişim bilgileri, veri işleme amacı ve hukuki dayanağı, istenilen verinin içeriği ve kapsamı belirtilir.

(2) Alıcı, paylaşım ile elde ettiği verileri 5'inci madde hükümlerine uygun şekilde işlemek ve bu verileri her kullanımında ilgili veri sorumlusunu kaynak göstermek zorundadır.

(3) Kişisel sağlık verilerinin uluslararası kuruluşlarla paylaşımına uluslararası hukuka uygun olarak Bakanlıkça izin verilebilir. Uluslararası kuruluşların, Avrupa Birliği veri koruması mevzuatına uygun seviyede bir korumayı garanti etmesi ve gerekli güvenlik önlemlerinin alındığını Bakanlığa yazılı olarak bildirmesi zorunludur”.

¹⁷² TBD Kamu-BİB Kamu Bilişim Platformu X, Kişisel Verilerin Korunması 2. Çalışma Grubu, http://www.tbd.org.tr/usr_img/cd/kamubib15/raporlarPDF/RP2-2008.pdf s.62, E.T. 28.10.2014.

¹⁷³ CMK' da moleküler genetik incelemede incelemeyi yapacak bilirkişiye incelenecek bulgunun, ilgilinin adı ve soyadı, adresi, doğum tarihi bildirilmeksizin verileceği düzenlenmiştir. (CMK m.79) Kişisel verilerin korunması açısından mevzuat için gerekli ve ileri bir uygulamadır.

¹⁷⁴ **Korff**, New Privacy Challenges, s.48.

¹⁷⁵ Kişisel Sağlık Verilerinin İşlenmesi ve Veri Mahremiyetinin Sağlanması Hakkında Yönetmelik Taslağı, <http://www.saglik.gov.tr/TR/belge/1-17634/kisisel-saglik-verilerinin-islenmesi-ve-veri-mahremiyet-.html> E.T. 30.10.2014.

Maddede; mevzuatta öngörülmüş olması halinde, veri sorumlusunu uygun görmesi durumunda ilgili kurum/ kuruluşun adı soyadı, iletişim bilgileri, veri işleme amacı ve hukuki dayanağı, istenilen verinin içeriği ve kapsamı belirtilecek kurumlar arası veri paylaşımının yapılabileceği düzenlenmiştir. Maddede atıf yapılan kişisel sağlık verilerinin işlenmesi esaslarını düzenleyen 5. maddede genel kurallar belirtilmiş ve söz konusu maddeler bu haliyle tam bir koruma sağlamaktan uzaktır. Madde hükmüne göre, veri paylaşımı veri sorumlusunun takdirine bırakılmıştır. Takdir yetkisinin denetlenmesinin güçlüğü dikkate alındığında geniş bir takdir yetkisi vermek yerine, sınırlanmış bir takdir yetkisi vermek veri koruma ilkelerine daha uygun olacaktır.

Kurumlar arası veri paylaşımında gerekli bir düzenleme olan asgari güvenlik tedbirlerine taslakta yer verilmemiştir. Ancak veri güvenliği için verinin paylaşılacağı kurumun asgari güvenlik tedbirlerini almış olduğunun ve bu verileri koruyabilecek niteliğe sahip olduğunun anlaşılması halinde veri paylaşılacağı şeklinde düzenlemeye gidilmelidir.

Taslakta veri paylaşırken anonimleştirmeye ya da takma isimle paylaşmaya ilişkin hüküm de yer almamaktadır. Yalnızca kişisel sağlık verilerinin işlendikten sonra yayımlanması halinde anonimleştirmeye yer verilmiştir. Taslağın 5. maddesinin ikinci fıkrası hükmüne göre işlenen kişisel sağlık verileri anonim hale getirilerek yayımlanabilir. Yayımlanırken aranan anonimleştirme şartı paylaşımında da kural haline getirilmelidir.

DDK denetim raporunda da değinildiği gibi, veri paylaşımına ile ilgili bir diğer husus verilerin taşınabilir elektronik ortamlar vasıtasıyla paylaşımıdır. Raporunda durum şu şekilde ifade edilmiştir; “Denetim çalışmaları sırasında kamu kurumlarının sahip oldukları pek çok kişisel ve hassas veriyi CD, DVD, taşınabilir bellek gibi taşınabilir elektronik ortamlar kullanarak çevrimdışı paylaştıkları görülmüştür. Çevrimiçi veri paylaşımında sorgu kayıtları aracılığı ile kontrol imkanı bulunmasına rağmen, çevrimdışı paylaşılan veriler üzerinde herhangi bir kontrol imkanı da kalmadığından, bu verilerin paylaşımına ilişkin gerekli güvenlik önlemlerinin alınması büyük önem taşımaktadır.

Buna rağmen, bazı örneklerde milyonlarca kişinin kimlik ve adres bilgisinin bulunduğu bilgilerin şifrelenmeden, kopyalanmaya karşı herhangi bir güvenlik önlemi alınmadan CD ortamında iletildiği; söz konusu verilerin ilgili kurumda hangi güvenlik önlemleri alınarak muhafaza edileceği ve kullanılabilirliği, çoğaltılıp çoğaltılamayacağı, söz konusu bilgilere olan ihtiyacın ortadan kalkması durumunda taşınabilir elektronik ortamın ne şekilde imha edileceği gibi hiçbir güvenlik hususunun belirlenmediği tespit edilmiştir”¹⁷⁶.

¹⁷⁶ Devlet Denetleme Kurulu Raporu, s.799.

Bu şekilde yapılan veri paylaşımı da bir standarda dayandırılmalıdır. Kimlerle bu şekilde veri paylaşımında bulunulabileceği tespit edilmeli, bu kişiler dışında kimsenin erişimine izin verilmemelidir. Bu amaçla şifreleme gibi uygun güvenlik tedbirleri alınmalıdır. Bu amaçla kullanılan şifreler titizlikle belirlenmeli, kolay tespit edilebilir nitelikte olmamalıdır. Amerika Birleşik Devletleri'nde 1996 tarihinde kabul edilen ve HIPAA (The Health Insurance Portability and Accountability Act) olarak bilinen "Sağlık Sigortasında Taşınabilirlik ve Denetlenebilirlik Yasası" yol gösterici nitelikte olabilir. Yasa sağlık bilgilerinin elektronik yollardan nasıl paylaşılacağını düzenlemektedir. Bu yasa tıbbi verilerin paylaşımında bir bakıma iyi bir fırsat sunarken aynı zamanda bir başkası tarafından kayıtlara erişilmek istenildiğinde önüne engeller (blokajlar) koymaktadır. Yasanın temel amaçları bireylere sağlık bakım sigortalarında daha büyük erişimi sağlamak, sağlık verilerinin mahremiyetini korumak, sağlık hizmet sektöründeki tüm sunucular yönünden standardizasyon ve verimliliği teşvik etmektir¹⁷⁷.

5. Hastanın Kişisel Verilerinin Korunması Açısından Hastane Kamera Kayıtları

Hastanelerde güvenliği sağlamak için kullanılan güvenlik kameraları, sağlık çalışanlarına şiddet olaylarının artması üzerine yaygınlaşmış, muayene odalarına bile kamera konulmaya başlanmıştır¹⁷⁸. Kameralar vasıta ile elde edilen görüntüler kişisel veri kapsamında değerlendirilmelidir. Nitekim Yargıtay 12. Ceza Dairesi'nin 11.9.2012 tarihli kararında "kişisel veri kavramından, kişinin, yetkisiz üçüncü kişilerin bilgisine sunmadığı, istediğinde başka kişilere açıklayarak ancak sınırlı bir çevre ile paylaştığı, herkes tarafından bilinmeyen ve/veya kolaylıkla ulaşılabilecek ve bilinmesi mümkün olmayan, kişinin kimliğini belirleyen veya belirlenebilir kılan, kişiyi toplumda yer alan diğer bireylerden ayıran ve onun niteliklerini ortaya koymaya elverişli, gerçek kişiye ait her türlü bilginin anlaşılması gerektiği; bir özel hayat görüntüsü ya da sesinin, kişisel veri olduğunda kuşku bulunmamakta..."¹⁷⁹ denilerek görüntünün kişisel veri olduğu benimsenmiştir.

Muayene, teşhis ve tedavinin yapıldığı alanlar hem hastanın hem de doktorun mahremiyet alanıdır. Bu alanlarda kamera kaydının alınması, birçok yasal düzenlemeyle hastaya tanınmış mahremiyet hakkının ve özel hayatın açık ihlalidir. Hastanın mahremiyeti ihlal edilmemiş olsa dahi kameralar vasıtasıyla elde edilen ve bir kişinin hangi poliklinikte muayene olduğunu gösteren görüntü dahi

¹⁷⁷ Mehmet Demir, "Kişiliğin Korunması ve Sağlık Hukuku Açıklarından Kişisel Verilerin Korunması Kanunu Tasarısının Değerlendirilmesi", Ankara Üniversitesi Hukuk Fakültesi Dergisi Ejder Yılmaz'a Armağan, C.I, Ankara 2014, s.746.

¹⁷⁸ Hakeri, s.170.

¹⁷⁹ Yargıtay 12. Ceza Dairesi, T. 11.9.2012, E. 2012/17703, K. 2012/18222; (Kazancı İçtihat Bilgi Bankası <http://www.kazanci.com/kho2/ibb/giris.htm> E.T. 30.10.2014).

kişisel veri kapsamında değerlendirilmelidir. Kişisel verilerin korunması açısından kameralar hastanenin her yerini göstermemelidir. Muayene odası, poliklinik önü gibi alanlar kamera görüş alanı dışında bırakılmalıdır.

Nitekim bu konuda Sağlık Bakanlığı Tedavi Hizmetleri Genel Müdürlüğü 07.02.2008 tarihinde Fotoğraf ve Kamera Çekimleri konulu genelge yayınlamıştır¹⁸⁰. Genelgede sağlık kurum ve kuruluşlarının huzur ve sükûnet içerisinde hizmet verebilmesi ve mahremiyet haklarının korunması için, kurum/kuruluş sahasında fotoğraf ya da kamera çekimi yapılmaması, kurum/kuruluş amirinin onayı ve geçerli bir gerekçe olmadan bu tür faaliyetlere izin verilmemesi gerektiği belirtilmiştir.

Türkiye Kamu Hastaneleri Kurumu tarafından güvenlik kameraları hakkında nispeten daha geniş kapsamlı düzenleme içeren 02.10.2012 tarihli "Güvenlik Kameraları ve Biometri Teknolojisinin Kurumumuza Bağlı Sağlık Tesislerinde Kullanılması" konulu genelge yayınlanmıştır¹⁸¹.

Genelgede; Avrupa İnsan Hakları Sözleşmesi ve Anayasa'nın özel hayatın gizliliğine ilişkin hükümler içerdiği, bu hükümlere göre insan hayatının, gizli veya sadece paylaşılmak istenen kişilere açık olan "*özel hayat*" ile bunun dışında kalan "*genel, müşterek hayat*" olmak üzere ikiye ayrıldığı belirtilmiştir. Toplumun diğer fertleriyle paylaşılan alanlar dışındaki özel hayatın, her türlü müdahaleye karşı koruma altına alınması istisnalar olmakla birlikte esastır. Bu istisnaların sayıldığı Türk Ceza Kanunu'nda, aleni olmayan konuşma ve görüntüleri izinsiz kaydedenler hakkında müeyyideler öngörüldüğü belirtilmiştir.

Hastanelerde kamuya açık ve müştereken istifade edilen, herkesin izne tabi olmaksızın rahatlıkla girip çıkabileceği bina giriş ve çıkışı, koridor gibi alanların müşterek alanlar olduğu, hukuken korunacak gizliliği ve sırrı olmayan bu alanlarda güvenlik gerekçesiyle kamera sistemi kurulmasına mani olmadığı, ancak hasta ve çalışan güvenliği için böyle bir sistem kurulurken muayene, teşhis, tedavi ve hastayla doğrudan teması gerektiren diğer işlemlerin makul bir gizlilik ortamında gerçekleştirilmesi gerektiği belirtilmiştir. Ayrıca kameraların, herkesin görebileceği yerlere kurulacağı ve bu alanların 24 saat izlendiği uyarısının da asılması gerektiği belirtilmiştir.

Hastane yöneticileri genelgede düzenlendiği şekliyle kişisel verilere ve mahremiyet hakkına saygı çerçevesinde kamera kaydı alınmasını sağlamalı, kişisel verileri koruma hukukuna ve hasta haklarına aykırı olacak şekilde kişilerin özel alanı ihlal edilmemelidir.

Kamera kayıtları konusunda değinilmesi gereken bir diğer husus basın mensuplarının kamera kaydı almasıdır. Basın mensuplarının sağlık kuruluşla-

¹⁸⁰ <http://www.saglik.gov.tr/TR/belge/1-1954/saglik-hizmetleri-genel-mudurlugu.html>, E.T. 30.10.2014.

¹⁸¹ http://www.tdb.org.tr/tdb/v2/ekler/SB_TKHK_kisisel_mahremiyet_02.10.2012.pdf, E.T. 30.10.2014.

rından görüntü alıp alamayacakları hususunda bu kuruluşların idarecilerinin tereddüdünü ortadan kaldırmak için Sağlık Bakanlığı Tedavi Hizmetleri Genel Müdürlüğü 07.02.2008 tarihinde yayınladığı fotoğraf ve kamera çekimleri konulu genelge ile kamera ve fotoğraf çekimi yasaklanmıştır. Ancak kurum yöneticisinin izni ve geçerli bir gerekçe ile izin verileceği düzenlenmiştir.

Haber alma özgürlüğü basına yasa ile tanınmış bir haktır. Bu çerçevede haberlerin doğru ve süratli bir biçimde alınması ve yine basın kanalıyla objektif olarak yansıtılması engellenmemelidir. Ancak basın görüntü alırken, haber yaparken hasta haklarına duyarlı ve özenli olmalı, mevcut işleyişi ve hizmeti aksatmamalıdır. Aksi takdirde basın mensuplarının muhatabından izin almadan çektikleri, hasta haklarına aykırı görüntüler de kişisel veri kapsamına dahil edilmelidir. Basın mensuplarının sağlık kuruluşlarından görüntü alması ve işlemesi ancak veri güvenliğine ilişkin tedbirlere, mesleki davranış kurallarına uygun olması ve basın özgürlüğü ve düşünceyi açıklama ve yayma hürriyeti sınırları çerçevesinde kalması halinde hukuka uygun sayılır.

6. Hastanın Kişisel Verilerinin Korunması Açısından Koğuş Sistemi Uygulaması

Çok sayıda hastanın aynı odada kalmasına koğuş sistemi denilmektedir. Tıbbi müdahale gerçekleştirilirken hastanın mahremiyetine saygı gösterilmesi esastır. Koğuş sisteminin kullanıldığı hastanelerde çok sayıda hasta aynı odada kalmakta, muayene, pansuman, bilgilendirme gibi birçok işlem diğer hastaların yanında yapılmaktadır. Bu durum kişinin sağlığı ile ilgili olan ve başkalarının bilmesini istemeyeceği bilgileri odada bulunan diğer kişilerin öğrenmesine sebep olduğu için kişisel verileri koruma hukukuyla bağdaşmamaktadır. Aynı zamanda Hasta Hakları Yönetmeliği'nin 21. maddesi ve Yataklı Tedavi Kurumları İşletme Yönetmeliği'nin 7. maddesinde düzenlenmiş bulunan mahremiyet hakkını ihlal etmektedir.

Etkin bir veri koruması ve hasta haklarına riayet için koğuş sisteminden vazgeçilmesi gerekmektedir. 2000'li yılların başından beri koğuş sisteminden vazgeçileceği gündemi meşgul etmektedir. Tamamen kaldırılmasa bile en azından hastalara pansuman, bilgilendirme gibi işlemler başka odada yapılmalıdır¹⁸².

7. Hastanın Kişisel Verilerinin Korunması Açısından Hasta Dosyası ve Hasta Bilgi Formu

Hasta bilgi formu ve hasta dosyası, hassas kişisel verileri ihtiva eden belgelerdir ve titizlikle korunmalıdır. Avrupa İnsan Hakları Mahkemesi 09.07.1991 yılında, *Chave - Fransa Davası*'nda başkalarının sağlığını ve hak ve özgürlüklerini, korumak üzere tasarlanmış kişisel dosyalar, ilgili gizlilik ve erişim kuralla-

¹⁸² Hakeri, s.165.

nyla korunur demiştir. Dava konusu olan psikiyatri hastanesine zorla yatırılması hakkında bilgi içeren dosyanın psikiyatri kliniğinin dışından sadece belirli kategorideki kişilerin erişimine açık olabileceğini belirtmiştir¹⁸³.

Sağlık Bakanlığı tarafından 06.11.2001 tarihinde yürürlüğe konulan Yataklı Tedavi Kurumları Tıbbi Kayıt ve Arşiv Hizmetleri Yönergesi¹⁸⁴ 4. maddesine göre hasta dosyası: yataklı tedavi kurumlarına müracaat eden hastaların, muayene, teşhis ve tedavi evrakının muhafaza edildiği; A4 kâğıdı boyutlarında, kenarlarında (EK-1) ve (EK-2)'de düzenlenen forma uygun renkli şeritler bulunan kartondan imal edilmiş ve iki kapaktan oluşan telli saklama aracı şeklinde tarif edilmiştir. Aynı yönergenin 12. maddesine göre hasta dosyasında şu evraklar bulunmalıdır; hasta kabul kağıdı, tıbbi müşahede ve muayene kağıdı, derece kağıdı, hasta tabelası, röntgen istek kağıdı ve raporları, laboratuvar istek kağıdı ve tetkik raporları, ameliyat kağıdı, hastanın muayene istek formu, çıkış özeti.

Etkin bir tedavi için sağlık hizmetlerinin geliştirilmesi tıbbi araştırmalar için hasta dosyası tutulması gereklidir. Ancak hasta dosyalarının tutulmasının gerekliliğinin yanı sıra veri güvenliğinin sağlanması da gereklidir.

Kağıt dosyalarla ilgili işleyişteki mevcut duruma bakıldığında sağlık hizmeti sunanların da sağlık hizmeti alanların da mahremiyete beklentisi ve kaygısı dikkate değer ölçülerde yüksek değildir. Kağıt ortamdaki hasta dosyaları ile elektronik hasta dosyaları arasındaki en önemli farklardan biri güvenlikle ilgilidir. Elektronik ortamdaki hasta kayıtlarından binlercesine çok kısa sürede ulaşmak mümkündür¹⁸⁵. Bu nedenle bu verilerin güvenliğinin sağlanması oldukça önemlidir.

Başka bir konu hasta dosyalarının koğuştta bulundurulmasıdır. Uygulamada hasta dosyaları koğuştta tutulmaktadır. Hasta Hakları Yönetmeliği 16. maddesinde hastanın sağlık durumu ile ilgili bilgiler bulunan dosya ve kayıtların sadece hastanın tedavisi ile doğrudan ilgili olanlar tarafından görülebileceği düzenlenmiştir. Dosyalar koğuştta tutulduğu zaman isteyen herkes hastanın bilgilerine kolayca erişebilecektir. Özellikle ziyaret saatlerinde odalarda bulunan dosyaların yetkisiz kişilerden korunması güçlük arz etmektedir. Hastaya ait verilerin korunabilmesi için dosyaların mümkün olduğunca koğuştlarda tutulmaması gerekmektedir.

Hasta dosyaları hasta taburcu edildikten sonra genellikle adli inceleme amaçlı, idari inceleme amaçlı ve araştırma amaçlı kullanılmaktadır. Yataklı Tedavi Kurumları Tıbbi Kayıt ve Arşiv Hizmetleri Yönergesi'nin 1. madde-

¹⁸³ Chave - Fransa Davası 09.07.1991 tarihli karar,

¹⁸⁴ Yataklı Tedavi Kurumları Tıbbi Kayıt ve Arşiv Hizmetleri Yönergesi,

¹⁸⁵ Berber/ Ülgü/ Er, s.321.

sinde dokümanların hastaların daha sonraki başvurularında veya araştırmacılar veyahut adli makamlarca her istenildiğinde hazır bulundurulacağı ifade edilmiştir. İdari amaçlı kullanımdan yönergede söz edilmemiştir. Hasta dosyalarının hasta taburcu olduktan sonraki kullanımlarında belirli kurallara uyulmalıdır.

Yönergenin “tıbbî istatistik ve kodlama bölümü” başlıklı 13/1-b bendine göre tıbbî araştırmalarda dosyalar, vekil dosya¹⁸⁶ ve zimmet karşılığı araştırmacıya verilir. Uygulamada hasta dosyaları asistanlar, doktorlar tarafından araştırma amaçlı hastane dışına çıkarılmaktadır günlerce getirilmemektedir. Bu durum veri güvenliği açısından tehdit edicidir. Elbette asistanların ve doktorların tıp ilminin gelişmesi bakımından hasta dosyalarını incelemesi zaruridir ancak bunun gelişigüzel olması değil bir standarda bağlanması gereklidir.

Yönergedeki söz konusu düzenleme dosyanın zimmet karşılığı araştırmacıya verileceği şeklindedir. Veri koruması açısından söz konusu düzenleme ayrıntılı ve yeterli değildir, daha detaylı şekilde düzenleme yapılmalıdır. Hastane arşiv sorumlusu öğretim elemanları ve asistanların araştırma veya tez amacı ile talepte buldukları dosyaların kontrolünü yapıp anonim hale getirmelidir. Hasta dosyalarında hastaların ismi ve diğer kişisel bilgilerinin tamamı yer almamalıdır sadece hastalıkla ilgili bilgiler yer almalıdır. Araştırmacıda kaç dosya olduğu bilinmelidir. Tek seferde alınabilecek dosya sayısına standart bir düzenleme getirilmeli ve dosyaların takibi arşiv görevlisi tarafından yapılmalıdır.

Bunun yanı sıra hastaya kişisel sağlık bilgilerini araştırma amacıyla kullanma izin belgesi imzalatılması veri koruma hukuku ve veri sahipliği ilkelerine daha uygundur. Araştırma yapılmadan önce kişiden izin alınması amacıyla Koç Üniversitesi Etik Kurulları tarafından bir form hazırlanmıştır¹⁸⁷. Formda araştırmacının adı (eğer araştırma adı hastanın gizlilik haklarını ihlal edecekse Etik Kurul Onay Numarası), araştırmacının adı soyadı, sorumlu araştırmacı, sorumlu araştırmacının telefon ve e-posta adresi, destekçi/fon veren kuruluş (eğer fon verilmişse), formun amacı¹⁸⁸, hangi kişisel sağlık bilgilerinin toplama-

¹⁸⁶ Yönerge'nin 4. maddesinde “*Vekil Dosya: Arşivden çıkarılan dosyaların dosya izleme fişiyle takip edilmesi amacıyla, asıl dosyanın yerine geçici olarak konulan ve asıl dosya ile aynı ebatlardaki, biri A4 kağıdı boyutunda diğeri büyük cebin üstünde dosya izleme fişinin konulacağı şeffaf iki ayrı cebi olan, (EK-3)'deki forma uygun olarak düzenlenen; araştırma için alınan ve diğer birimlere gönderilenlerin ayrı renkte olduğu plastik dosyayı; ifade eder*” şeklinde tanımlanmıştır.

¹⁸⁷ Koç Üniversitesi onam formu, <http://www.kisiselsaglikverileri.org/88-koc-unv-onam-formu.html>, E.T. 04.11.2014.

¹⁸⁸ Bu başlık altında sağlık bilgilerinin kullanılmasını ve açıklanmasını koruma altına alındığı, araştırmacının, araştırma ekibinin ve araştırma destekçisinin sağlık bilgilerini araştırma projesi kapsamında nasıl kullanabilecekleri açıklanmaktadır.

nıp/paylaşılacağı¹⁸⁹, kişisel sağlık bilgilerinin nasıl kullanılacağı, bu formu imzalamaya mecbur olmadığı, iznin belirli bir süreyle sınırlı olduğu ve iptal edebileceği bilgilerine yer verilmiş, en son da imza kısmı düzenlenmiştir. Formu ilgili kişi kendi imzalamaya yetkili değilse ebeveyn veya yasal temsilci etik kurul uygun görürse imzalayabilir. Etkin bir veri koruma hukukunun ve veri sahipliğinin amacına hizmet bakımından, kişisel sağlık bilgilerini araştırma amacıyla kullanma izin belgesinin tüm kamu ve özel hastanelerde kullanılmasının zorunlu tutulması faydalı olacaktır.

Hasta bilgi formunda genellikle dosya numarası, hastanın adı soyadı, doğum yeri, baba-anne adı, adresi, telefonu, TC. kimlik numarası, doğum tarihi, cinsiyet ve medeni hal, kan grubu, yakınının telefonu ve hangi bölümde hangi tanı konulduğu ve tedavi uygulandığı, giriş çıkış tarihi yer almaktadır. Yani hasta bilgi formu, birçok kişisel veriyi ihtiva eden bir belgedir.

Hasta formunda uygulama açısından önemli olan husus doktor anamnez¹⁹⁰ yazarken hastanın anlattığı her şeyi yazacak mıdır? Hastaya alerjileri, kullandığı ilaçlar, geçmiş tıbbi hikaye, en son ne yediği ve aciliyetin sebebi sorulur¹⁹¹. Doktor hastanın anlattığı her şeyi aynen yazmamalıdır. Hastadan veya yakınlarından edindiği bilgileri ayıklamalı, hastalıkla/teşhisle ilgisi olan veya olabilecek bilgileri yazmalı, hastalıkla ilgisi olmayan bilgileri yazmamalıdır.

Hasta bilgi formu konusunda değinilmesi gereken bir diğer husus da hastanın durumuyla ilgili isteyen herkese bilgi verilip verilmeyeceğidir. Hasta Hakları Yönetmeliği'nin 15. maddesine göre hastanın sağlık durumu ile ilgili gereken bilgiyi, bizzat hasta veya hastanın küçük, temyiz kudretinden yoksun veya kısıtlı olması halinde velisi veya vasisi isteyebilir. Hasta, sağlık durumu hakkında bilgi almak üzere bir başkasına da yetki verebilir. Ancak gerek görülen hallerde yetkinin belgelendirilmesi istenilebilir. Yönetmeliğin 20. maddesi ilgili mevzuat hükümlerine ve hastalığın mahiyetine göre yetkili mercilerce alınacak tedbirlerin gerektirdiği haller dışında; hastaya, sağlık durumu hakkında kendisine, ailesine veya yakınlarına bilgi verilmemesini isteme hakkı tanınmıştır.

Hastaların tetkik ve tedavi sırasında elde edilen bilgilerinin sağlık çalışanı dışında üçüncü kişilerle paylaşımındaki sorunların giderilmesi, hukuki açıdan hekim ve hastaların zor durumda kalmasının önlenmesi amacıyla; hasta yatışı sırasında

¹⁸⁹ Burada hastanın kullanılmasını istediği kişisel bilgilerini açıklamayı istenmiştir ve hastaya alternatifler sunulmuştur. Hasta belirteceği bir hastalık, durum ya da belirttiği tarih aralığındaki kişisel sağlık bilgilerinin kullanımına izin verebileceği gibi tüm kişisel sağlık bilgilerinin kullanımına da izin verebilir.

¹⁹⁰ Anamnez; hastanın problemini belirlemek amacıyla kendisinden veya ailesinden alınan bilgilerdir.

¹⁹¹ **Sinan Yenal**, "Anamnez Alma", <http://www.pdflibrary.org/pdf/anamnez-alma-dokuz-eylul-universitesi-www-deu-edu-tr-2.html>, E.T. 04.11.2014, s.24.

yatış kağıdına hastanın kendi el yazısı ile kendisi ve hastalığıyla ilgili bilgi almasında sakınca olmayan yakınlarının isim ve soyadlarını yazmaları istenmelidir¹⁹².

Denizli Devlet Hastanesi'nde, 06.11.2008 tarihinde hasta hakları kurulunda; bir fizik tedavi uzman hekiminin klinikte yatan hastasının tanısını (romatizma) hasta yakını olarak düşündüğü hastanın işverenine söylemesi iddiası ile ilgili başvuru görüşülmüş, bu dosya kapsamında hasta hakları kurulunun 'yatışı yapılacak hastalarda yatış sırasında hastalığı ile ilgili bilgi verilebilecek kişilerin isimleri alınıp hastaya imzalatılması' önerisi üzerine çalışma başlatılmıştır. Konu kurum kalite ve performans ekibinde görüşüldükten sonra çözüm olarak hasta yatış formuna 'hastalığım hakkında bilgi verilebilecek kişiler aşağıda yazılmıştır' ibaresinin altına hastalığı ile ilgili bilgi almasında sakınca olmayan yakınlarının isim, soyadlarını ve yakınlık derecelerini yazmaları önerilmiş, bunun üzerine hasta yatış formunun 15.11.2008 tarihinden itibaren yapılan revizyonu ile bilgi işleminden tüm birimlere dağılımı sağlanmıştır¹⁹³. Bu uygulama, Denizli Devlet Hastanesinde 2008 tarihinden itibaren uygulanmaktadır. Rastgele örnekleme ile alınan 200 yatan hastanın %39'unun 3 isim, %38'inin 1 isim, %19'unun 2 isim yazdığı belirlenmiştir. Hastaların belirttiği isimlerde; %74'ünün 1. derece yakınları olduğu, %19'unun 1. derece yakınları dışında isimler verdiği, %6'sında sadece kendi ismini verdiği saptanmıştır. Alınan örneklem grubunda 4 veya daha fazla yakınının adını yazan hastaya rastlanmamıştır¹⁹⁴.

Çıkan sonuçlara bakıldığında hastalar da kendisiyle ilgili bilgilere herkesin erişmesini istememektedir. Hastaların veri güvenliğinin sağlanması için örnek teşkil eden bu uygulamanın tüm kamu hastaneleri ve özel hastanelerde zorunlu hale getirilmesi yararlı olacaktır.

8. Hastanın Kişisel Verilerinin Korunması Açısından Kamu Hastanelerine İhale ile Tıbbi Cihaz Temin Edilmesi

Hastanelerde; hastalığın tanısı, önlenmesi, izlenmesi, tedavisi amacıyla birçok tıbbi cihaz kullanılmaktadır. Sağlık bakanlığı tarafından 07.06.2011 tarihinde yayınlanan Tıbbi Cihaz Yönetmeliği¹⁹⁵'nin 3/1-o bendinde tıbbi cihaz tanımlanmıştır¹⁹⁶.

¹⁹² Ramazan Canural/ Nalan Gökalp/ Gülseren Ekici/ Nevin Şahin, "Sağlık Hizmetlerinde Hasta Mahremiyeti: Hasta Sağlık Bilgilerinin Paylaşımı", Sağlık Bakanlığı Performans Yönetimi ve Kalite Geliştirme Daire Başkanlığı, Uluslararası Sağlıkta Performans ve Kalite Kongresi Bildiriler Kitabı Cilt:2, 19-21 Mart 2009 Antalya, s.55.

¹⁹³ Canural/ Gökalp/ Ekici/ Şahin, s.58.

¹⁹⁴ Canural/ Gökalp/ Ekici/ Şahin, s.59.

¹⁹⁵ Tıbbi Cihaz Yönetmeliği, RG, T.07.06.2011, S.27957.

¹⁹⁶ Tıbbi cihaz 3. maddede şu şekilde tanımlanmıştır; "Tıbbi cihaz: İnsanda kullanıldıklarında asli fonksiyonunu farmakolojik, immünolojik veya metabolik etkiler ile sağlamayan fakat fonksiyonunu yerine getirirken bu etkiler tarafından desteklenebilen ve insan üzerinde; 1) Hastalığın ta-

Tanı, teşhis, tedavi, önleme amacıyla kullanılan bu tıbbi cihazların kamu hastanelerinde ihale ile tedarik edildiği durumlar kişisel veriler açısından önem arz etmektedir. İhale ile tıbbi cihaz temin edilmesinin veri güvenliğine bakan yönü; tıbbi cihazın kullanımına başlandığı günden itibaren birçok hastanın verileri kaydedilmekte ve sözleşmede kararlaştırılan süre dolunca tıbbi cihazlar tedarikçiye hastaların verileriyle birlikte teslim edilmektedir.

Tıbbi Cihaz Yönetmeliği'nin "Gizlilik" başlıklı 20. maddesi şu şekildedir; "*Bakanlık, onaylanmış kuruluş ve bu Yönetmeliğin uygulanmasına katılan bütün taraflar, görevlerini yerine getirirken temin ettikleri bütün bilgilerin gizliliğini sağlar. Ancak, Bakanlığın diğer ülke yetkili kuruluşları ve onaylanmış kuruluşlar ile karşılıklı bilgi paylaşımı ve uyarı sistemi kapsamındaki yükümlülükleri saklıdır. Ayrıca gizlilik mahiyetine haiz bu bilgiler, kamu sağlığının ve düzeninin gerektirdiği hallerde, adli ve ilgili üst mercilerin talebi üzerine, Bakanlığa bilgi verilmek suretiyle açıklanabilir*". Yönetmeliğin bu maddesinde gizliliğin sağlanması gerektiği belirtilmiştir.

Sağlık Bakanlığı Tedavi Hizmetleri Genel Müdürlüğü tarafından 01.03.2010 tarihinde Tıbbi Cihazlarla İlgili Mal ve Hizmet Alımı İşlemleri konulu¹⁹⁷, Türkiye Kamu Hastaneleri Kurumu tarafından 19.11.2012 tarihinde Tıbbi Cihazlarla İlgili Mal ve Hizmet Alımları konulu genelge¹⁹⁸ yayımlanmıştır ancak bu genelgelerde bilgi güvenliği ile ilgili hükümlere yer verilmemiştir.

Sağlık Bakanlığı tarafından 16.10.2006 tarihinde yayımlanan Bilgi Sistemleri konulu genelgenin¹⁹⁹ 3. maddede veri teslimi konusu düzenlenmiştir²⁰⁰. İhale

nısı, önlenmesi, izlenmesi, tedavisi veya hafifletilmesi ya da 2) Yaralanma veya sakatlığın tanısı, izlenmesi, tedavisi, hafifletilmesi veya mağduriyetin giderilmesi ya da 3) Anatomik veya fizyolojik bir işlevin araştırılması, değiştirilmesi veya yerine başka bir şey konulması veyahut 4) Doğum kontrolü kullanılmak üzere imal edilmiş, tek başına veya birlikte kullanılabilen, imalatçısı tarafından özellikle tanı ve/veya tedavi amaçlı kullanılmak üzere imal edilmiş ve tıbbi cihazın amaçlanan işlevini yerine getirebilmesi için gerekli olan yazılımlar da dahil, her türlü araç, alet, teçhizat, yazılım, aksesuar veya diğer malzemeleri" ifade eder.

¹⁹⁷ Tıbbi Cihazlarla İlgili Mal ve Hizmet Alımı İşlemleri Hakkında Genelge (2010/11) <http://www.saglik.gov.tr/TR/belge/1-10051/tibbi-cihazlarla-iligili-mal-ve-hizmet-alimi-islemleri-h.html>, E.T. 10.11.2014.

¹⁹⁸ Tıbbi Cihazlarla İlgili Mal ve Hizmet Alımları Hakkında Genelge <http://www.tkhk.gov.tr/Dosyalar/2ac5fd5d77bb4fa08d179b7160a0ec31.pdf>.

¹⁹⁹ Bilgi Sistemleri Hakkında Genelge, http://www.ihs.gov.tr/indir/mevzuat/genelgeler/G_16102006_1.pdf E.T. 10.11.2014.

²⁰⁰ 3. madde şu şekildedir; "*Hizmet alımı yoluyla tedarik edilen yazılımların bir sonraki ihale döneminde kullanım dışı kalması durumu göz önünde bulundurulmalıdır. Bu sebeple, hastane bilgi sisteminde tutulan veriler Türkçe karakter içermeyen (ö, ü, ç, ş, ğ, ı, İ) ancak Türkçe alan ve tablo adlarına sahip ve anlaşılır tablolarda tutulmalıdır. Veriler teslim edilirken tablo yapıları, ilişkileri, anahtar alanlar ile ilgili bilgiler doküman halinde verilerle birlikte teslim edilmelidir. Teslim edilecek veri içinde firmaya ait know-how sayılabilecek herhangi bir yazılım kodu (trigger, procedur, vb) yer almamalıdır. Teslim eden firma veri tutarlılığının sağlanması ve data*

ile tıbbi cihaz temin edilirken ihale şartnamesine veri güvenliğinin sağlanmasıyla ilgili hükümler konulmalıdır.

İş bırakılırken, kayıtlı tüm veriler hiçbir surette, hiçbir zaman işi bırakan firmada kalmak üzere kopyalanamayacağı, çıktı alınamayacağı, firma sunucularına aktarılamayacağı, ifşa edilemeyeceği, aksi davrandığı tespit edilenler hakkında Türk Ceza Kanununun İlgili hükümlerine²⁰¹, ayrıca ihale mevzuatına aykırı davranmaktan dolayı Kamu İhale Mevzuatı hükümlerine göre idare tarafından hukuki süreç başlatılacağı ihale şartnamesine konulmalıdır. Böylece ihale şartnamelerine konulacak gerekli hükümlerle, ihale ile temin edilen tıbbi cihazlar kira süresinin bitiminde teslim edilirken hasta verilerinin güvenliği sağlanacaktır.

SONUÇ

Kişisel verilerin korunması ulusal ve uluslararası birçok hukuki metinde kendine yer bulmuş güncelliğini koruyan bir kavramdır. Kişisel sağlık verileri, özellikli koruma gerektiren veri kategorileri arasında sayılmış bu verilerin işlenmesi özel şartlara bağlanmıştır. Mevzuatımızda hastanın kişisel verilerinin korunması ile ilgili birtakım düzenlemeler mevcuttur ancak bu düzenlemeler kişisel verilerin korunması gerektiğini belirtmekten öteye geçememiş, hastanın verilerinin korunması açısından yeterli tedbirleri öngörmemiştir. Yani söz konusu düzenlemeler normatifliğin ötesine geçememiştir.

Kişisel veri toplanmasında birtakım genel ilkeler belirlenmeli ve veri işleyecek idareler veri koruması için gerekli olan idari, fiziksel ve teknik tedbirleri almalı ve idarenin denetimi altında veri işlemelidir. Sağlık hizmetinden yararlanan kişilerin verilerinin usulüne uygun şekilde işlenmesi ve sağlık hizmet sunucularının bu konudaki denetimi idarenin sorumluluğundadır.

kayıbı olmaması için, teslim ettiği verilerle ilgili tablo adetleri, tablolardaki kayıt sayılarını içeren özet bir raporu tutanak ile kurum idaresine ve yeni firmaya teslim etmelidir. Teslim edilecek veriler txt, csv, excel, vb formatında olmayıp kurumda çalışan orijinal veri tabanı formatında sadece veriler(data-only) olacak şekilde, kolay ve sorunsuz okunabilir bir medya (Taşınabilir Harddisk, vb.) üzerinde 2 kopya teslim edilmelidir. Okunmasında sorun olabilecek tape, kartuş, vb. kullanılmamalıdır. Yeni kurulacak sistemler için şartnamelerde; Yazılımın sahibi olan firmanın kuruma ait verileri (Legacy), kendi kuracağı veri tabanına aktarması şartı konacaktır. Veri aktarımı çalışmaları ise yeni programın kurum hizmetlerinde kullanılmaya başlanmasından önce yaptırılacak ve aktarımın sağlıklı bir şekilde yapılabildiğine dair testler önceden tamamlanmış olacaktır. Bu şartın sağlanıp sağlanmadığının tespiti için önceki firma, yeni firma ve kurum idaresinden yeterli sayıda personelin katılımıyla bir komisyon kurulacak, kurum idaresince gerek görülmesi halinde bir başka kurumdaki da bu komisyona üyeler davet edilecektir.”

²⁰¹ Bu hükümler şunlardır;

“Kişisel verilerin kaydedilmesi” başlıklı TCK m.135, “Verileri hukuka aykırı olarak verme veya ele geçirme” başlıklı TCK m.136, “Nitelikli haller” başlıklı TCK m.137, “Verileri yok etme” başlıklı TCK m.138, “Tüzel kişiler hakkında güvenlik tedbiri uygulanması” başlıklı TCK 140. madde.

Kanuni dayanak olmaksızın yetkisiz kişilerce veri toplanması Anayasa'ya aykırıdır. Kişisel Verilerin Korunması Kanunu Tasarısı 6. maddesinde kişisel sağlık verilerinin sır saklama yükümü altında bulunan kişiler tarafından işlenebileceği düzenlenmiştir. İdare gerekli denetimleri yaparak kanuni dayanak olmaksızın yetkisiz kişilerce veri toplanmasına ve işlenmesine engel olmalıdır.

Kanuna dayanan veri toplamlarında da verilerinin toplanmasındaki amaç dikkate alınarak amaçla bağdaşmayan veri toplamlarına engel olunmalıdır. Veri toplama asgarilik ilkesi gereği bilgi içeriklerinin sınırlandırılması, azaltılması ve ayıklanmasının yanı sıra, ad ve soyadın kodlanması, sadece hasta ve hekimin göreceği şekilde şifrelenmesi, bilgilerin korumalı başka bir veri tabanına kaydedilmesi gibi pek çok araç kullanılarak hasta verilerinin güvenli şekilde işlenmesi sağlanmalıdır.

Toplanan kişisel verilerin süresiz şekilde depolanması kişilik hakkına saldırı niteliğindedir. Hassas veri kategorisinde yer alan kişisel sağlık verilerinin uzun süre saklanmaması, amaç hasıl olduktan sonra bu verilerin imhası gerekmektedir. Hasta verilerini toplayıp işleyen tüm kamu kurum ve kuruluşlarıyla özel kuruluşlar için geçerli olmak üzere belirli süreler geçtikten sonra toplanan verilerin imhası standarda bağlayan düzenleme yapılmalıdır.

Veri koruma hukuku açısından kurumlar arası paylaşım da önemlidir. Öncelikle kurumlar arası veri paylaşımı kanunda öngörülmesi halinde ve kanunda öngörülen amaçla yapılmalıdır. Hangi amaç için veri talep ediliyorsa o amacı gerçekleştirmeye yetecek ölçüde verinin iletilmesi esas olmalıdır. Bunun yanında bilgiler paylaşılmadan önce ilgili kişiden izin alınmalı ve kişi bilgilerinin hangi kurumla paylaşıldığını bilmelidir. Ayrıca verilerin paylaşıldığı kurum veya kuruluşların da aynı derecede bilgi güvenliği sağlayabilecek nitelikte olması gerekmektedir. Aksi halde veriyi asıl olarak işleyen kurumun almış olduğu güvenlik önlemlerinin önemi kalmayacaktır. Kurumlar arası paylaşımında güvenliği sağlamak için kurumlar arasında ortak bir gizlilik ve güvenlik politikasının belirlenmesi gerekmektedir. Bunun yanında hastanın verilerinin doğrudan paylaşılması yerine anonimleştirilerek veya takma isimle paylaşılması koruma açısından daha uygundur.

Hastanelerde bulunan güvenlik kameraları, koğuş sistemi uygulaması, hasta dosyası, hasta bilgi formu ve son olarak kamu hastanelerinde ihale ile tıbbi cihaz temini veri güvenliğini ihlal edebilecek niteliğe sahiptir. Kişisel verilerin korunması açısından kameralar hastanenin her yerini göstermemelidir. Muayene odası, poliklinik önü gibi alanlar kamera görüş alanı dışında bırakılmalıdır. Koğuş sistemi uygulaması kaldırılmalı, tamamen kaldırılmasa bile en azından hastalara pansuman, bilgilendirme gibi işlemler başka odada yapılmalıdır. Hasta dosyalarının özellikle ziyaretçi saatlerinde korunması güç olduğu için koğuştaki bulundurulmaması gereklidir. Hasta dosyalarının hasta taburcu edildikten sonra

adli, idari inceleme ve araştırma amaçlı kullanılması ayrıntılı şekilde düzenlenmelidir. Dosya üzerinde inceleme yapılmadan önce hastaya kişisel sağlık bilgilerini araştırma amacıyla kullanma izin belgesi imzalatılması ve bunun tüm sağlık kurumlarında kullanımının sağlanması veri koruma hukuku ve veri sahipliği ilkelerine uygun düşecektir. Hastaların tetkik ve tedavi sırasında elde edilen bilgilerinin sağlık çalışanı dışında üçüncü kişilerle paylaşımındaki sorunların giderilmesi amacıyla hasta yatışı sırasında yatış kağıdına hastanın kendi el yazısı ile kendisi ve hastalığıyla ilgili bilgi almasında sakınca olmayan yakınlarının isim ve soyadlarını yazmaları istenmelidir. Bu uygulamanın tüm sağlık kurumlarında zorunlu hale getirilmesi yararlı olacaktır. İhale ile tıbbi cihaz temin edilirken ihale şartnamesine veri güvenliğinin sağlanmasıyla ilgili hükümler konulmalıdır. Şartnameye iş bırakılırken, kayıtlı tüm verilerin hiçbir surette, hiçbir zaman işi bırakan firmada kalmak üzere kopyalanamayacağı, çıktı alınamayacağı, firma sunucularına aktarılamayacağı, ifşa edilemeyeceği gibi hükümler konularak, ihale ile temin edilen tıbbi cihazlar kira süresinin bitiminde teslim edilirken hasta verilerinin güvenliği sağlanmalıdır.

KAYNAKÇA

- Akça, Gürsoy/ Beşer, Doğa**, “*Karanlığın Yok Oluşu*” *Gelişen Teknolojinin Gizlilik ve Mahremiyet Üzerindeki Etkileri*”, Muğla Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, Bahar 2011, Sayı 26, s.19-42.
- Akdağ, Hale**, Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması, Ankara 2013.
- Akgül, Aydın**, “*Danıştay Kararları Işığında Kişisel Sağlık Verilerin Korunması*”, Danıştay Dergisi, Sayı: 133, Yıl: 2013, s.21-45, (Akgül, Kişisel Sağlık Verileri).
- Akgül, Aydın**, Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması, İstanbul 2014, (Akgül, Kişisel Verilerin korunması).
- Aksoy, Hüseyin Can**, Medeni Hukuk ve Özellikle Kişiler Hukuku Yönünden Kişisel Verilerin Korunması, Ankara 2010.
- Akyol, Mehmet Can**, Avrupa İnsan Hakları Mahkemesi S. ve Marper Birleşik Krallık Davası Kararı(Başvuru no: (Başvuru no.30562/04 ve 30566/04) Strazburg 4 Aralık 2008, <http://www.fap.hsyk.gov.tr/dosyalar/aihm-kararinceleme/m8/sveMarperBirlesikKrallik.pdf> s.30-31, E.T. 13.11.2014.
- Birtek, Fatih**, “*Sağlık Hizmetlerinin Yürütülmesinde İdarenin Kusura Dayanan Sorumluluğu*”, Erciyes Üniversitesi Hukuk Fakültesi Dergisi, C. 2, S. 3-4, Y. 2007, s.81-128.
- Boz, Ahmet**, “*Kişisel Verilerin Korunması: Türkiye ABD ve AB Örnekleri*”, Polis Akademisi Güvenlik Bilimleri Enstitüsü Güvenlik Stratejileri ve Yönetimi Anabilim Dalı, (Yüksek Lisans Tezi), Ankara 2014.
- Bulut, Nihat**, “*4709 Sayılı Kanunla Yapılan Anayasa Değişikliği Çerçevesinde Hak ve Özgürlüklerin Sınırlanması Rejiminin Birey Devlet İlişkisi Açısından Değerlendirilmesi*”, AÜEHFD, C. V, S. 1-4, Y. 2001, s.37-64.
- Büyükcay, Yusuf**, “*Hekimin Sır Saklama Yükümlülüğü*”, Atatürk Üniversitesi Erzincan Hukuk Fakültesi Dergisi, C. VIII, S.1-2 (2004), s.383-396.
- Canural, Ramazan/ Gökalp, Nalan/ Ekici, Gülseren/ Şahin, Nevin**, “*Sağlık Hizmetlerinde Hasta Mahremiyeti: Hasta Sağlık Bilgilerinin Paylaşımı*”, Sağlık Bakanlığı Performans Yönetimi ve Kalite Geliştirme Daire Başkanlığı, Uluslararası Sağlıkta Performans ve Kalite Kongresi Bildiriler Kitabı Cilt: 2, 19-21 Mart 2009 Antalya, s.55-59.
- Değer, Mebrure**, “*Hastane Eczacılığında Sır*”, Türkiye Klinikleri Tıp Etiği-Hukuku-Tarihi Dergisi C. 5, S. 3, Y. 1997, s.133-135.
- Demir, Mehmet**, “*Kişiliğin Korunması ve Sağlık Hukuku Açıklarından Kişisel Verilerin Korunması Kanunu Tasarısının Değerlendirilmesi*”, Ankara Üniversitesi Hukuk Fakültesi Dergisi Ejder Yılmaz’a Armağan, C.I, Ankara 2014, s.743-753.
- Demir, Mehmet**, Tıbbi Organizasyon Kusuru Açısından Hastanelerin Hukuksal Sorumluluğu, Ankara 2010.

- Deryal, Yahya**, “*Hasta Hakları Bağlamında Mahremiyet ve Özel Hayata Saygı*”, Sağlık Hukuku Kurultayı, 1-3 Kasım 2007, Ankara, s.71-84.
- Doğan, Cahid**, “*Sağlık Haklarından Hekimlerin Sır (Kişisel Veri) Saklama Mükellefiyeti*”, Sağlık Hukuku Kurultayı, 1-3 Kasım 2007, Ankara, s.105-149.
- Doğan, Murat**, “*Hekimin Hukuki Sorumluluğu*”, Tıbbi Müdahaleden Kaynaklanan Hukuki Sorumluluk Sempozyumu (Mersin 2009), s.41-60.
- Doğru, Osman/ Nalbant, Atilla**, İnsan Hakları Avrupa Sözleşmesi Açıklama ve Önemli Kararlar, 2. Cilt, Ankara 2013.
- Dural, Mustafa / Ögüz, Turan**, Türk Özel Hukuku C.II Kişiler Hukuku, İstanbul 2009.
- Dutertre, Gilles**, Avrupa İnsan Hakları Mahkemesi Kararlarından Örnekler, Almanya 2003.
- Erdoğan, Yavuz**, “*Kişisel Verilerin Korunması Bakımından Türk Ceza Kanunu Hükmülerinin Değerlendirilmesi(m.135, 136, 137, 138)*”, Erciyes Üniversitesi Hukuk Fakültesi Dergisi, C. VIII, S. 2, Y. 2013, s.569-632.
- Erkal, Atilla**, “*Genel Olarak Bilgi ve Bilgi Teorisi Çerçevesinde Bilginin Hukuktaki Anlamı*”, Selçuk Üniversitesi Hukuk Fakültesi Dergisi, C. 17, S. 2, Y. 2009, s.11-30.
- Ersoy, Uğur**, Bir İnsan Hakları Kavramı Olarak Kişisel Verilerin Korunması, Gazi Üniversitesi Sosyal Bilimler Enstitüsü, (Yüksek Lisans Tezi), Ankara 2009.
- Hakeri, Hakan**, Tıp Hukuku, Ankara 2013.
- Helvacı, Serap**, Türk ve İsviçre Hukuklarında Kişilik Hakkını Koruyucu Davalar, İstanbul, 2001.
- İzgi, M. Cumhuri**, “*Mahremiyet Kavramı Bağlamında Kişisel Sağlık Verileri*”, Türkiye Biyoetik Dergisi, C.1, S.1, Y. 2014, s.25-37.
- Kaboğlu, İbrahim**, Özgürlükler Hukuku, İstanbul 1994.
- Keser Berber, Leyla / Ülgü, Mahir M. / Er, Cüneyd**, Elektronik Sağlık Kayıtları ve Özel Hayatın Gizliliği, İstanbul 2009.
- Kılınç, Doğan**, “*Anayasal Bir Hak Olarak Kişisel Verilerin Korunması*”, AÜHFD, 61 (3) 2012, s.1089-1169.
- Kırhdoğ, Melih**, “*Elektronik Sağlık Kayıtlarında Teknolojik Gelişmeler, Kullanım Alanları, Amaç ve Yasa Dışı Kullanımlar*”, Kişisel Sağlık Verilerine Mesleki Yaklaşımlar Çalıştayı, İstanbul 2013, s.58-87.
- Kilkelly, Ursula**, Özel Hayata ve Aile Hayatına Saygı Gösterilmesi Hakkı, (Avrupa İnsan Hakları Sözleşmesinin 8. Maddesinin Uygulanmasına İlişkin Kılavuz), Almanya 2001.
- Korff, Douwe**, “*Comparative Study on Different Approaches to New Privacy Challenges in Particular in the Light of Technological Developments*”, Working Paper no:2, Commission of the European Communities, <http://ec.europa.eu/justice/>

policies/privacy/docs/studies/new_privacy_challenges/final_report_working_paper_2_en.pdf, E.T. 01.10.2014, (Korff, New Privacy Challenges).

- Korff, Douwe**, “Study on The Protection of The Rights and Interests of Legal Persons With Regard to the Processing of Personal Data Relating to Such Persons” Final Report, Commission of the European, http://ec.europa.eu/justice/dataprotection/document/studies/files/20000202_rights_interests_legal_en.pdf, E.T. 30.09.2014.
- Küzeci, Elif**, “*Kişisel Sağlık Verileri ve Hukuki Haklar*” Kişisel Sağlık Verilerine Mesleki Yaklaşımlar Çalıştayı, İstanbul 2013, s.16-24.
- Küzeci, Elif**, Kişisel Verilerin Korunması, Ankara Üniversitesi Sosyal Bilimler Enstitüsü, (Doktora Tezi), Ankara 2010.
- Langmack, Hans**, “*Ceza Hukuku Açısından Hekimin Sır Saklama Yükümü*”, çeviren; **Erdener Yurtcan**, İÜHFM, C.39, S.1-4, Y. 1974, s.451-464.
- Özdemir, Hayrunnisa**, “*Hadım Etme ve Hekimin Sır Saklama Yükümlülüğü*”, Gazi Üniversitesi Hukuk Fakültesi Dergisi, C. XIV, S.1, Y. 2010, s.125-164.
- Öztürkler, Cemal**, Hukuk Uygulamasında Tıbbi Sorumluluk, Teşhis, Tedavi ve Tıbbi Müdahaleden Doğan Tazminat Davaları, Ankara 2006.
- Pekşirin, Hülya**, “*Kişisel Verilerin Korunması*”, Türkiye Bilişim Şurası Hukuk Çalışma Grubu Raporu, Ankara, <http://tr.scribd.com/doc/19952426/1-Bilisim-Surasi-Hukuk-Raporu>, E.T. 26.09.2014.
- Sert, Gürkan**, “*Kişisel Sağlık Verilerine Mesleki, Etik Yaklaşımlar*”, Kişisel Sağlık Verilerine Mesleki Yaklaşımlar Çalıştayı, İstanbul, 2013, s.7-15.
- Soysal, Hüseyin**, “*Sağlık Hizmetlerinde Kişisel Veri Toplanması*”, Türkiye Psikiyatri Derneği Bülteni, C. 16 S. 3, Y. 2013.
- Şen, Ersan**, “*Kişisel Verilerin Korunması Kanunu Tasarısı'nın Anayasa ve Türk Ceza Kanunu Hükümleri Çerçevesinde Değerlendirilmesi*”, İstanbul Barosu Dergisi, C. 83, S. 3, Y. 2009, s.1197- 1213.
- Şimşek, Oğuz**, Anayasa Hukukunda Kişisel Verilerin Korunması, İstanbul 2008.
- Taneri, Gökhan**, Hasta Hakları, Ankara 2014.
- Taneri, Gökhan**, Uygulamadan Örnek Hükümlerle Türk Hukukunda Hekim Ceza Sorumluluğu, Ankara 2014.
- Tezcan, Durmuş**, “*Bilgisayar Karşısında Özel Hayatın Korunması*”, Anayasa Yargısı Dergisi, C.8, Y.1991, s.385-392.
- Törenli Çakıroğlu, Maral**, “*Hekimin Borçlarından Özel Olarak Sır Saklama Borcu*”, DEÜHFD, C. 12, S. 2, Y. 2010, s.159-181.
- Yenal, Sinan**, “Anamnez Alma”, <https://www.google.com.tr/webhp?sourceid=chrome-instant&ion=1&espv=2&ie=UTF-8#q=anamnez%20alma> E.T. 04.11.2014.
- Yüksel, Mehmet**, “*Mahremiyet Hakkı ve Sosyo-Tarihsel Gelişimi*”, Ankara Üniversitesi SBF Dergisi, C. 58, S. 1, Y.2003, s.181-213.

Zevkliler, Aydın, “*Tedavi Amaçlı Müdahalelerle Kişilik Hakkına Saldırının Sonuçları*”, Dicle Üniversitesi Hukuk Fakültesi Dergisi, S. 1, Y. 1983, s.1-37.

İNTERNET KAYNAKLARI

Avrupa İnsan Hakları Mahkemesi Kişisel Verilerin Korunmasına İlişkin Bilgi Notu, Temmuz 2012, http://www.inhak.adalet.gov.tr/tematik/bilgi/kisisel_veriler.pdf, E.T. 13.11.2014.

Cumhurbaşkanlığı Devlet Denetleme Kurulu'nun 27.01.2013 tarih ve 2013/3 sayılı Kişisel Verilerin Korunmasına İlişkin Ulusal ve Uluslararası Durum Değerlendirmesi ile Bilgi Güvenliği ve Kişisel Verilerin Korunması Kapsamında Gerçekleştirilen Denetim Çalışmaları Raporu, <http://www.tccb.gov.tr/ddk/ddk56.pdf>, E.T. 28.10.2014.

Grand Chamber, Digital Rights Ireland Ltd. (C-293/12) v. Minister for Communications, Marine and Natural Resources, <http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62012CJ0293&rid=1> E.T. 13.01.2015.

İstanbul Tabip Odası Hukuk Bürosu, “25 Soruda Sağlık.NET 2 Sistemi”, <http://www.istabip.org.tr/icerik/net2sorucevap.pdf>, E.T. 13.10.2014.

Kazancı İçtihat Bilgi Bankası.

Kişisel Sağlık Verileri Çalışma Grubu, “*Sağlık Hizmetlerinde Kişisel Veri Toplanması, Korunması ve Değerlendirilmesi*” <http://www.kisisesaglikverileri.org/32-saglik-hizmetlerinde-kisisel-veri-toplanmasi-korunmasi-ve-degerlendirilmesi.html>.

Kişisel Verilerin Korunması Kanunu Tasarısı Hakkında Bilgi Notu, http://www.tbmm.gov.tr/arastirma_komisyonlari/bilisim_internet/docs/sunumlar/Adalet%20Bakanl%C4%B1%C4%9F%C4%B1%20Kanunlar%20Genel%20M%C3%BCd%C3%BCrl%C3%BC%C4%9F%C3%BC29-05-2012.pdf, E.T. 15.01.2015.

Sağlık. NET Hakkında, <http://www.e-saglik.gov.tr/belge/1-33811/sagliknet-hakkinda.html>, E.T. 13.10.2014

TBD Kamu-BİB Kamu Bilişim Platformu X, Kişisel Verilerin Korunması 2. Çalışma Grubu, http://www.tbd.org.tr/usr_img/cd/kamubib15/raporlarPDF/RP2-2008.pdf, E.T. 28.10.2014.

**Tez Özeti/
Abstract of Thesis**
