

KİŞİSEL VERİLERİN KORUNMASI KANUNU HAKKINDA BİR DEĞERLENDİRME

AN ASSESSMENT OF THE LAW ON PROTECTION OF PERSONAL DATA

İbrahim KORKMAZ*

Özet: Bilgi, modern yaşamın en önemli değerlerinden birisidir. Hergün, devlet kurumları ve özel kuruluşlar, bireyler hakkında önemli miktarda veriyi toplamakta, saklamakta, işlemekte ve nakletmektedirler. Bunun yanında, teknoloji görülmemiş şekilde kişilerin bilgiyi paylaşması ve dünya çapında yaymasına izin verecek şekilde gelişmiştir. Bütün bunlar, kişilerin bilgilerinin kontrolünü kaybederek, kendilerine karşı kullanılması gibi birçok tehlikeli durumun oluşmasına sebep olmaktadır. Kişisel verilerin korunması, bireylerin verilerinin başka kişi veya kuruluşlar tarafından yetkisiz kullanımına karşı sahip oldukları bir haktır. Bu hakkın korunmasıyla ilgili Kişisel Verilerin Korunması Kanunu 24 Mart 2016 tarihinde TBMM'nde kabul edilerek kanunlaşmıştır. Çalışmamızda Kişisel Verilerin Korunması Kanunu, bu alandaki uluslararası düzenlemeler ışığında incelenmiştir.

Anahtar Kelimeler: Kişisel Veri, Kişisel Verilerin Korunması Hakkı, Kişisel Verilerin İşlenmesi

Abstract: Information is one of the most valuable assets of modern life. Everyday, governmental and nongovernmental organizations collect, hold, process and transfer large quantities of information about individuals. Also, technology allows individuals to share and disseminate information globally on an unprecedented scale. These circumstances cause dangers to individuals such as losing control over their personal information that might be used against them. Data protection is a right that people have against possible unauthorized use of their personal information by other individuals or organizations. Law on Protection of Personal Data regarding the protection of this right was enacted by the Parliament on 24 March 2016. In our study Law on Protection of Personal Data will be examined in consideration of international regulations on this area.

Keywords: Personal Data, The Right to Protection of Personal Data, Processing of Personal Data.

* Ankara Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı Doktora Öğrencisi, ikorkmaz72@gmail.com

GİRİŞ

Çeşitli kişiler ve örgütlerce kişilere ilişkin bilgilere gereksinim, tarihin çok eski dönemlerinden beri bulunan bir gerçekliktir.¹ İnsanlar tarih boyunca, tehlikeden ve riskten kaçınmak, uygunsuz davranışları tespit etmek, başkalarının ne yaptığını kontrol etmek, kaydettikleri ilerlemeyi görmek ve toplumsal örgütlenme ve koruma amacıyla, etrafındakilerin yaptıklarına bakmışlar, gözetlemişlerdir.² Bu sebeple kişiler hakkında bilgi toplama, onları izleme veya gözetleme için geliştirilmiş birçok araç bulunmaktadır. Çağımızda teknolojik olanakların gelişmesiyle, gözetim çok daha etkili bir hal almıştır.³

Bireylerin kimliklerini belirlemeye elverişli her türlü bilgi olarak tanımlanabilecek kişisel verilere karşı gelişen tehditler, gözetim teknolojilerine karşı bir savunma mekanizmasının geliştirilmesini zorunlu kılmış ve kişisel verilerin korunması hukukunun⁴ gerekliliği anlaşılmıştır. Kişisel veriler üzerinde ilgili kişinin denetimini amaçlayan düzenlemeler, bilgisayarların hızla gelişmesi ve merkezi veri bankalarının oluşturulması ile birlikte, ilk olarak 1970'li yıllarda Avrupa'da ortaya çıkmış ve zamanla Dünyaya yayılmıştır.⁵

1982 Anayasası'nın 2. maddesinde belirtildiği gibi insan haklarına saygılı, demokratik bir hukuk devleti olan ülkemiz, Birleşmiş Milletler, Avrupa Konseyi, OECD gibi örgütlerin de üyesi olmasına rağmen, uzun bir süre kişisel verileri koruyan özel bir kanunun bulunmaması nedeniyle, bu alanda uluslararası kuruluşlarca benimsenen ilkeleri ulusal hukukumuzda aktaramamıştır. 2010 yılında yapılan

¹ David Lyon, *Surveillance After September 11*, Polity, 2003, s.2

² Zygmunt Bauman, *Yasa Koyucular ve Yorumcular*, Çev. Kemal Atakay, Metis Yayınevi, İstanbul 1996, s. 51 vd.

³ Daniel J. Solove, *The Digital Person, Technology and Privacy in the Information Age*, New York University Press, ABD 2004, s. 2.; David Lyon, *Surveillance Studies an Overview*, Polity Press, 2007, s. 12.

⁴ Kişisel verilerin korunması ile ilgili normlar, kişilerin toplumun bir bireyi olmasını engelleyen bu tip baskılar altında kalmalarını engellemek ve gözetleyen ve gözetlenen arasındaki güç dengesini eşitlemek açısından önemlidir. Kişisel verilerin korunması, özde verinin kendisinin değil, verinin sahibi olan bireyin temel hak ve özgürlüklerinin, kişilik hakkının ve özel alanının korunmasını amaçlamaktadır. Oğuz Şimşek, *Anayasa Hukukunda Kişisel Verilerin Korunması*, Beta Basım, İstanbul 2008, s. 4, Bundan sonra "Anayasa Hukukunda Kişisel Verilerin Korunması" olarak anılacaktır.

⁵ Vemon Bogdanor, *Blackwell'in Siyaset Bilimi Ansiklopedisi*, C.II, Çev. Erhan Yükselci, Sema Yükselci, Bülent Peker, Ümit Yayıncılık, Ankara 2003, s. 426.

referandumdan sonra 5982 sayılı Kanunla⁶ Anayasa'nın özel hayatın gizliliğini düzenleyen 20. maddesine "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" şeklinde bir fıkra eklenerek kişilerin kişisel verilerinin korunması açıkça anayasal güvence altına alınmıştır. Bu düzenleme doktrinde kişisel verilerin korunması hakkının hangi şartlarda sınırlanabileceğinin belirtilmediği⁷ ve kişisel verilerin işlenmesi hususunu denetleyecek bağımsız bir organ öngörülmediği⁸ için eleştirilmiştir.

Avrupa Konseyi bünyesinde hazırlanarak 28 Ocak 1981 tarihinde Strazburg'ta imzaya açılan ve 1 Ekim 1985 tarihinde yürürlüğe giren 108 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi,⁹ ülkemiz tarafından 28 Ocak 1981 yılında imzalanmış olmasına karşın, uzun süre onaylanmamış ve nihayet 30 Ocak 2016 tarihinde kabul edilen 6669 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun ile onaylanarak 18 Şubat 2016 Tarihli ve 29628 Sayılı Resmî Gazetede yayımlanmış ve aynı tarihte yürürlüğe girmiştir.¹⁰

Avrupa'da birçok devletin mevzuatında kişisel verilerin korunması ile kanunlar kırk yıldan fazladır yer almaktadır. Çağdaş devletle-

⁶ Türkiye Cumhuriyeti Anayasasının Bazı Maddelerinde Değişiklik Yapılması Hakkında Kanun, Kanun No: 5982; Resmi Gazete Tarihi: 13.05.2010, Sayı: 27580.

⁷ Elif Küzeci, Kişisel Verilerin Korunması, Turhan Kitabevi, Ankara 2010, s.266; Sultan Tahmazoğlu Uzeltürk, "Kişisel Verilerin Korunması Hakkında Anayasa Değişikliği", Legal Hukuk Dergisi, Sayı 93, Eylül 2010, s. 3155.

⁸ Küzeci, s. 266.

⁹ Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesinin Uygun Bulunduğuna Dair Kanun Gereçesi, (Çevrimiçi) <http://www.2.tbmm.gov.tr/d26/1/1-0320.pdf> (Erişim Tarihi: 07 Mart 2016)

¹⁰ Türkiye Sözleşmeyi imzalamasına rağmen, 30/1/2016 tarihine kadar onaylayıp yürürlüğe koymayan tek ülke konumundaydı. Kanun metni için bakınız. (Çevrimiçi) <http://www.resmigazete.gov.tr/main.aspx?home=http://www.resmigazete.gov.tr/eskiler/2016/02/20160218.htm&main=http://www.resmigazete.gov.tr/eskiler/2016/02/20160218.htm> (Erişim Tarihi: 07 Mart 2016)

rin neredeyse tamamı, bu konuda temel kanunlar çıkarmıştır. Henüz bu konuda bir düzenleme yapmamış devletlerin üzerinde ise bazı sebeplerle kişisel verilerin ulusal mevzuatta yer alan temel kanunlarla korunması yönünde artan bir baskı olduğu söylenebilir.¹¹ Bu yöndeki eğilimin ilk sebebi, daha önce otoriter rejimlerin bulunduğu ülkelerde tekrar bu deneyimlerin yaşanmaması için bireysel temel hak ve özgürlüklerin korunmasına önem verilmesidir. Bir diğer sebep, elektronik ticaret başta olmak üzere teknolojiyle gelişen ticaretin önündeki engelleri kaldırma isteğidir. Üçüncü sebep ise, 95/46/AT sayılı Avrupa Birliği Yönergesi'nin kişisel verilerin yeterli koruma sağlamayan ülkelere transferini yasaklaması sebebiyle Avrupa ilkeleriyle ticaret yapmak isteyen ülkelerin mevzuatlarında gerekli değişiklikleri yapmasıdır.¹²

Mevzuatımızda kişisel verilerin korunmasıyla ilgili dağınık hükümler bulunmasına rağmen,¹³ temel ilkelerin belirlendiği, bütünlüğü, özel bir kanunun bulunmayışı, uzun bir süre önemli bir eksiklik

¹¹ (Çevrimiçi) <http://uk.practicallaw.com/4-519-9017> (Erişim Tarihi: 07 Mart 2016); David Banisar, *Privacy and Data Protection Around the World*, s. 4, (Çevrimiçi) <https://www.pcpd.org.hk/english/infocentre/files/banisar-paper.doc>, (Erişim Tarihi: 07 Mart 2016). Ancak 95/46/AT sayılı Avrupa Birliği Yönergesi'nin kişisel verilerin yeterli koruma sağlamayan ülkelere transferini yasaklayan düzenlemeleri, gelişen ticaret ve Avrupa Birliği ile ilişkilerin sürdürülmesi gerekliliğinden dolayı Orta Doğu ve Afrika'da da kişisel verilerin korunması ile ilgili düzenlemelerin yapılması konusunda gittikçe artan bir baskı unsuru olmaya devam etmektedir. Küzeci, s. 352.

¹² David Banisar, "Freedom of Information and Access to Government Record Laws Around the World", *The Freedom info Global Survey*, Mayıs 2004, s. 2. Türkiye'nin Avrupa Bölgesel Savcılık Teşkilatı olarak bilinen EUROJUST ve Avrupa Polis Teşkilatı olarak bilinen EUROPOL ile operasyonel işbirliği anlaşması olmasına rağmen kişisel verilerin korunmasıyla ilgili özel bir kanunun olmaması nedeniyle bu anlaşmanın gerekleri yeterince yerine getirilememektedir. Ayrıca Dışişleri Bakanlığının yabancı ülkelere vatandaşlarla ilgili istediği askerlik, kimlik, vatandaşlık bilgileri veya o ülkelerin vatandaşlarıyla ilgili bilgilerin paylaşımında sorunlar yaşanmaktadır. Yine, Türk iş adamlarının yurt dışında yaptığı yatırımlar ve yabancı iş adamlarının Türkiye'de yaptığı yatırımlar nedeniyle kişisel veri paylaşımına ihtiyaç duyulması hâlinde, bu konuda özel kanunun olmaması nedeniyle veri paylaşımı yapılamaması pek çok ciddi sorunlara yol açmaktadır. Komisyon Raporu, s. 5.

¹³ Son dönemde ülkemizde kabul edilen TCK, CMK gibi temel yasalarda kişisel verilerin korunmasına yönelik ilkeler bulunsun da, bunlar sınırlı bir koruma sağlamakta ve bütüncül bir koruma sağlamada yetersiz kalmaktadır. Ayrıca bu düzenlemelerin çoğunluğunun bir zararın ortaya çıkmasından sonra uygulanabilir olması nedeniyle, herhangi bir zarar ortaya çıkmadan bireylerin bu alandaki hak ve özgürlüklerini koruma altına alabilecek önleyici bir düzenlemenin bulunması bir gerekliliktir. Küzeci, s. 357.

olarak görülmüştür.¹⁴ Ülkemizde kişisel verilerin korunmasıyla ilgili temel bir kanun bulunması için yukarıda belirtilen sebeplerin hepsi bulunmaktadır. İlk olarak, ülkemizde çeşitli dönemlerde yapılan hukuka aykırı fişlemeler, güvenlik soruşturmaları¹⁵ gibi bireylerin hak ve özgürlüklerine haksız müdahalelerin sonuçları, kişisel verilerin yeterince korunmaması durumunda oluşabilecek zararları göstermektedir. Gerekli ve yeterli tedbirler alınmadığı takdirde, bu şekilde haksız uygulamaların otoriter rejimler yanında demokratik yönetimlerde de gerçekleşme olasılığı her zaman vardır.¹⁶ Türkiye’de kişisel verilerin korunmasıyla ilgili özel bir yasa bulunması, her şeyden önce bunun temel bir insan hakkı olması nedeninden dolayı bir gerekliliktir.¹⁷

Bunun yanında, gelişmekte olan elektronik ticaret gibi ekonomik etkinliklerde ülkemizin geriye kalmaması için kişisel verilerin korunması gerekmektedir. Ayrıca, 95/46/AT sayılı Avrupa Yönergesi’nin 25 ve 26. maddelerinin yeterli koruma sağlamayan ülkelere kişisel verilerin transferini yasaklamasından dolayı, Avrupa ülkeleri ile etkin bir ticaret yapabilmenin sağlanabilmesi ve belirtilen hükümler dolayısıyla çeşitli sorunların yaşanmaması için¹⁸ ülkemizde bu yönde bir düzenlemenin yapılması önemlidir. Ayrıca, bu konuda yapılacak bir düzenleme, Türkiye’nin Avrupa Birliği adaylık süreci açısından da bir gerekliliktir.¹⁹

¹⁴ .Kişisel Verilerin Korunması Kanunu gerekçesinde de belirtildiği gibi, “kişisel verilerin işlenebilmesi hususunda özel bir kanun ve etkin bir denetim mekanizmasının bulunmaması, toplumumuzda olumsuz bir algının oluşmasına sebebiyet vermektedir. Oluşan bu algının ortadan kaldırılması için kişisel verilerin belli şartlar dahilinde işlenmesine, muhafaza edilmesine ve kontrolüne ilişkin esasların belirlenmesi gerekmektedir.” Adalet Komisyonu’nun 117 Sıra Sayılı Kişisel Verilerin Korunması Kanunu Tasarısı Raporunun metni için bakınız. (Çevrimiçi) <https://www.tbmm.gov.tr/sirasayi/donem26/yil01/ss117.pdf> (Erişim Tarihi: 07 Mart 2016) Bundan sonra “Komisyon Raporu” olarak anılacaktır.,

¹⁵ Güney Dinç, Güvensizlik Üçgeni, 1402’likler, Fişleme, Güvenlik Soruşturması, Say, İstanbul 1987, s. 197-198.

¹⁶ Küzeci, s.354. Kişisel Verilerin Korunması Kanunu Gerekçesinde de belirtildiği gibi, ülkemizde kişisel verilerin işlenmesi sürecini kontrol edecek ve denetleyecek bir kurumun bulunması önemlidir. Aksi takdirde, kişisel veriler yeterli düzenleme ve denetime tabi olmaksızın, birçok kişi veya kurum tarafından kullanılabilmekte ve bu durum bazı hak ihlallerinin yaşanmasına sebep olabilmektedir. Komisyon Raporu, s. 5.

¹⁷ Komisyon Raporu, s. 5.

¹⁸ *Türkiye Büyük Millet Meclisi Adalet Komisyonu Tutanak Dergisi* 27.01.2016 tarihli tutanak sayfa 5.

¹⁹ Komisyon Tarafından Avrupa Parlamentosuna ve Konseye Sunulan Bildirim Genişleme Stratejisi ve Başlıca Zorluklar 2013-2014, Brüksel, 16 Ekim 2013, SWD

Ülkemizde kişisel verilerin korunmasıyla ilgili özel bir kanun hazırlamak üzere ilk komisyon 1989 yılında kurulmuş ancak çalışmalarını tamamlayamamıştır.²⁰ Daha sonra 2000 yılında kurulan ikinci komisyon üç yıllık çalışma sonucunda Kişisel Verilerin Korunması Kanun Tasarısı'nı hazırlamıştır. Adalet Bakanlığı tarafından 7 Eylül 2003 tarihinde açıklanan Tasarı, Avrupa Birliği ilerleme raporları ve e-Dönüşüm Türkiye Projesi Kısa Dönem Eylem Planları gibi çeşitli belgelerde yer almasına karşın kanunlaşamamıştır.²¹

Adalet Bakanlığı Tasarı üzerinde ilave çalışmalar yaparak 2008 yılında Başbakanlık'a göndermiş, Başbakanlık tarafından 22 Nisan 2008 tarihinde Türkiye Büyük Millet Meclisi Başkanlığı'na gönderilmiştir.²² Tasarı, TBMM Başkanlığı tarafından 02 Mayıs 2008 tarihinde esas komisyon olarak Adalet Komisyonuna, tali komisyon olarak Avrupa Birliği Uyum Komisyonuna gönderilmiştir. Adalet Komisyonu tarafından 07.05.2008 tarihinde Alt Komisyona havale edilen Tasarı ile ilgili Alt Komisyonda birkaç toplantı yapıldıktan sonra yoğun gündem nedeniyle çalışmalara ara verilmiş ve araya TBMM Seçimlerinin girmesi nedeniyle Tasarı İhtüzüğü'nün 77. maddesi gereğince hükümsüz sayılmıştır.

Kişisel Verilerin Korunması Kanunu Tasarısı Adalet Bakanlığı'na yenilenerek Başbakanlık tarafından 26.12.2014 tarihinde tekrar TBMM'ye gönderilmesine rağmen TBMM seçimleri nedeniyle bu defa da yasalasamayarak hükümsüz kalmıştır.²³

-
- (2013) 417, (Çevrimiçi) http://www.abgs.gov.tr/files/AB_Iliskileri/AdaylikSureci/IlerlemeRaporlari/2013_ilerleme_raporu_tr.pdf, (Erişim Tarihi: 20 Mart 2016).
- ²⁰ Sedat Erdem Aydın, AİHM İhtihatları Kapsamında Kişisel Verilerin Kaydedilmesi Suçu, Yüksek Lisans Tezi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı, İstanbul 2014, s. 98.
- ²¹ Nilgün Başalp, Kişisel Verilerin Korunması ve Saklanması, Yetkin Yayınları, 2004, s. 107, Bundan sonra "Kişisel Verilerin Korunması ve Saklanması" olarak anılacaktır; Ceylin Beyli, Kişisel Verilerin Korunması Hakkında Kanun Tasarısı Üzerine Eleştiriler, Bilişim Hukuku, derleyen Mete Tevetoğlu, Kadir Has Üniversitesi Yayınları, İstanbul 2006, s. 70; Küzeci, s. 358; Uğur Ersoy, Bir İnsan Hakları Kavramı Olarak "Kişisel Verilerin Korunması", Yüksek Lisans Tezi, Gazi Üniversitesi Sosyal Bilimler Enstitüsü, Kamu Yönetimi Anabilim Dalı, Ankara 2009, s. 16; Bundan sonra "Kişisel Verilerin Korunması" olarak anılacaktır.
- ²² Başbakanlık'tan TBMM Başkanlığı'na gönderilen 2008 tarihli Tasarı'nın metni ve Gereke'sini içeren 22.04.2008 tarih, B.02.0.KKG.0.10/101.192/1812 sayılı ve "Kanun Tasarısı" konulu yazı metni için bakınız. (Çevrimiçi) <http://www2.tbmm.gov.tr/d23/1/1-0576.pdf>, (Erişim Tarihi:20 Mart 2016).
- ²³ Adalet Bakanlığı Kanunlar Genel Müdürlüğü'ne resmi web sitesinde bulunan du-

Tasarı, 18.01.2016 tarihinde tekrar Türkiye Büyük Millet Meclisi Başkanlığı'na gönderilmiştir.²⁴ TBMM Başkanlığı tarafından 19.01.2016 tarihinde esas komisyon olarak Adalet Komisyonuna,²⁵ tali komisyonlar olarak Anayasa Komisyonu, Avrupa Birliği Uyum Komisyonu, İnsan Haklarını İnceleme Komisyonu ve Plan ve Bütçe Komisyonuna gönderilen Tasarı hakkında Adalet Komisyonu 12.02.2016 tarihinde raporunu vermiştir.²⁶ 6698 sayılı Kişisel Verilerin Korunması Kanunu 24 Mart 2016 tarihinde nihayet TBMM'nde kabul edilerek kanunlaşmıştır. Çalışmamızda Kişisel Verilerin Korunması Kanunu, 108 sayılı Avrupa Konseyi Sözleşmesi ve 95/46/AT sayılı Avrupa Birliği Yönergesi başta olmak üzere kişisel verilerin korunması ile ilgili önemli görülen uluslararası düzenlemeler ışığında incelenmiştir.

I. KANUNUN AMACI, KAPSAMI VE TANIMLAR

A. Kanunun Amacı

6698 sayılı Kişisel Verilerin Korunması Kanunu'nun "Amaç" başlıklı 1. maddesinde Kanun ile elde edilmesi umulan amaç belirtilmiştir. Buna göre Kişisel Verilerin Korunması Kanunu'nun amacı, "*kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemektir.*"

Maddenin gerekçesinde, maddeyle Kanun'un amacının belirlendiği, bu amacın, kişisel verilerin işlenmesinin disiplin altına alınması ve Anayasa'da öngörülen başta özel hayatın gizliliği olmak üzere temel hak ve özgürlüklerin korunması olduğu belirtilmiştir. Gereçede ay-

yuruya göre, 2014 tarihli Kişisel Verilerin Korunması Kanunu Tasarısı Taslağı, 08 Haziran 2012 tarihinde Başbakanlık'a gönderilmiştir. (Çevrimiçi) <http://www.kgm.adalet.gov.tr/Tasariasamaları/Basbakanlik/Basbakanlik.html> , (Erişim Tarihi: 10 Mart 2016)

²⁴ Başbakanlık'tan TBMM Başkanlığı'na gönderilen 2016 tarihli Tasarı'nın metni ve Gereçe'sini içeren 16.01.2016 tarih, 31853594-101-580-249 sayılı ve "Kanun Tasarısı" konulu yazı metni için bakınız. (Çevrimiçi) <http://www2.tbmm.gov.tr/d26/1/1-0541.pdf> (Erişim Tarihi:07 Mart 2016). Bundan sonra "Tasarı" olarak anılacaktır.

²⁵ Kişisel Verilerin Korunması Kanunu Tasarısı 26'ncü Dönemde 64'üncü Cumhuriyet Hükümetinin Adalet Komisyonuna sevk ettiği ilk kanun tasarısıdır. Komisyon Raporu, s. 4.

²⁶ a.g.e., s. 5.

rıca, Kanun ile son yıllarda önem kazanan kişinin mahremiyet hakkı ile bilgi güvenliği hakkının korunması ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasların düzenlenmesinin amaçlandığı belirtilmiştir.²⁷ Madde metnine bakıldığında, Kanun'un amacının Anayasa'nın 20. maddesi çerçevesinde düzenlendiğini görmekteyiz.²⁸ Madde, 95/46/AT sayılı Avrupa Birliği Yönergesi'nin 1. maddesi²⁹ ve Avrupa Birliği Kişisel Verilerin Korunması Yönetmelik Taslağı'nın 1. maddesi³⁰ ile paralellik göstermektedir.

B. Kanunun Kapsamı

Kişisel Verilerin Korunması Kanunu'nun "Kapsam" başlıklı 2. maddesinde Kanun'un kapsamı düzenlenmiştir. Buna göre Kişisel Verilerin Korunması Kanunu "*kişisel verileri işlenen gerçek kişiler ile bu verileri tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işleyen gerçek ve tüzel kişiler hakkında uygulanır.*"

Kanunun gerekçesinde de³¹ belirtildiği gibi, Kanun, kişisel verileri işlenen gerçek kişiler ile bu verileri işleyen gerçek ve tüzel kişiler hakkında uygulanacaktır. Kanunun uygulaması bakımından kamu ve özel sektör ayrımı yapılmamış olup, düzenlenen usul ve esaslar her iki sektör bakımından da uygulama alanı bulmaktadır. Kanun, kişisel verilerin otomatik veya herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenmesi durumunda uygulanacaktır.³²

²⁷ Tasarı, s. 18.

²⁸ Anayasamızın 20. maddesine göre " Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir."

²⁹ 95/46/AT sayılı Avrupa Birliği Yönergesi'nin metni için bakınız. (Çevrimiçi) <http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:31995L0046> (Erişim Tarihi: 14 Mart 2016)

³⁰ Avrupa Birliği Kişisel Verilerin Korunması Yönetmelik Taslağı (Orjinal adı, Proposal for a Regulation Of The European Parliament and Of The Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) için bakınız. (Çevrimiçi) http://ec.europa.eu/justice/data-protection/document/revi-ew2012/com_2012_11_en.pdf (Erişim Tarihi: 14 Mart 2016) Bundan sonra "AB Yönetmelik Taslağı" olarak anılacaktır.

³¹ Tasarı, s. 18.

³² Veri kayıt sistemi, Kanununun 3. maddesinde, kişisel verilere ulaşımı kolaylaştıracak şekilde, belirli bir kritere göre yapılandırılmış kayıt sistemi olarak tanımlan-

Kişisel verilerin korunmasında kişi kavramının içeriği konusunda uluslararası doktrin ve mevzuatta farklı görüşler mevcuttur. Bir görüş sadece gerçek kişilere ait verilerin kişisel verilerin korunmasından yararlanması gerektiğini savunmaktadır.³³ Bir diğer görüş ise, tüzel kişilere ait verilerin de bu korumadan faydalanabileceğini savunmaktadır.³⁴

muştur. Veri kayıt sistemi sadece dijital veya elektronik ortamda olmak zorunda değildir. Kanunun düzenlemesinden anlaşıldığı ve gerekçede belirtildiği gibi, bir veri kayıt sisteminin parçası olmayan kişisel veriler otomatik olmayan yollarla işlendiklerinde Kanun kapsamında değerlendirilmeyeceklerdir. Gerekçede, bu durumun verilerin kişisel veri niteliğini etkilememesi nedeniyle, bu tür verilere ilişkin hukuka aykırı eylemlerin 5237 sayılı Türk Ceza Kanunu uyarınca suç teşkil etmeye devam edecekleri belirtilmiştir a.g.e., s. 18.

³³ Douwe Korff, EC Study on the Protection of the Rights and Interests of Legal Persons with Regard to the Processing of the Personal Data Relating to Such Persons, (Study Contract ETD/97/B5-9500/78) s. 41 (Çevrimiçi) http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1288583&download=yes, (Erişim Tarihi: 10 Mart 2016); Elif Mendos Kuşkonmaz, Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması, Yüksek Lisans Tezi, İstanbul 2013, s.8; I. N. Walden.- R.N. Sawage, "Data Protection and Privacy Laws: Should Organisations be Protected?", *International and Comparative Law Quarterly*, C.37, S. 22, 1988, s. 337; Hüseyin Can Aksoy, Kişisel Verilerin Korunması, Yüksek Lisans Tezi, Ankara Üniversitesi Sosyal Bilimler Enstitüsü Özel Hukuk (Medeni Hukuk) Anabilim Dalı, Ankara 2008, s. 24.; Engin Dinç, Kişisel Verilerin Korunmasında Uluslararası Düzenlemeler ve Türkiye'nin Durumu, Yüksek Lisans Tezi, Dicle Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı, Diyarbakır, 2006, s. 15, Bundan sonra "Kişisel Verilerin Korunmasında Uluslararası Düzenlemeler" olarak anılacaktır; Sadece gerçek kişilerin özel hayatından söz edilebileceğini savunan görüşe göre, tüzel kişilerin kişisel verilerinin korunması söz konusu olmayıp, ancak ticari sırlarının gizliliği söz konusu olabilir. AİHM'nin B. Company ve diğerleri v. Hollanda kararında da toplam sekiz şirketten oluşan başvuru, şirketin yıllık mali tablolarını yayımlama yükümlülüğü getiren kanuni düzenlemenin AİHS'e aykırı olduğunu ileri sürmüşler, AİHM verdiği kararda söz konusu durumun kişisel bir nitelik taşımadığını, bundan dolayı özel yaşama saygı hakkı kapsamında görülmeyeceğini belirtmiştir. Aydın, s. 7, 8.

³⁴ Diğer taraftan tüzel kişilerin kişisel verilerin de korunması gerektiği savunulmaktadır. Korff, tüzel kişilerin aralarında korunma ihtiyacı açısından farklılıklar bulunduğu, dini, siyasi ve sendikal örgütler şeklindeki tüzel kişilerin, diğer tüzel kişilere daha çok korunma ihtiyacı içinde olduklarını belirtmiştir. Korff, s. 57; Tüzel kişiler arasında farklı veri koruma sistemlerinin oluşturulması düşüncesi Korff'un fikrini destekler niteliktedir. Buna göre, uluslararası şirketler, özel girişimciler, kar amacı gütmeyen şirketler, her biri farklı güçte oluşumlardır. Bunların birbirlerine göre farklı koruma sistemlerine sahip olmaları gerekir, Walden - Sawage, s. 347; Tezcan ise, tüzel kişilere ait bilgilerin kişisel veri kapsamında değil ticari sır kapsamında korunması gerektiğini savunmaktadır, Durmuş Tezcan, "Bilgisayar Karşısında Özel Hayatın Korunması", *Anayasa Yargısı Dergisi*, 8. Cilt, 1991, s.389; Bir başka görüş ise tüzel kişilere ait verilerin kişisel verilerin korunması sisteminde ziyade, marka, patent, telif hakkı, gizlilik sözleşmesi gibi alternatif koruma

OECD Rehber İlkeleri ve 108 sayılı Avrupa Konseyi Sözleşmesi'nde sadece gerçek kişilere ait kişisel veriler korunmaktadır.³⁵ Buna benzer şekilde, 95/46/AT sayılı Avrupa Birliği Yönergesi'nin 2/a maddesindeki kişisel veri tanımında ve başlangıç bölümünün 2. maddesinde sadece gerçek kişilere ait veriler kişisel veri olarak kabul edilmiş ve tüzel kişilere ait veriler kapsam dışında tutulmuştur.³⁶ 2002/58/AT sayılı Elektronik Haberleşme Yönergesi'nin başlangıç bölümünde yer alan 12. maddede, elektronik haberleşme sektöründe gerçek kişiler yanında tüzel kişilere ait kişisel verilerin de koruma altına alınabileceği belirtilmiştir.³⁷

Kişisel verilerin korunması hakkı, öncelikle gerçek kişiler için söz konusudur. Kişisel Verilerin Korunması Kanunu'nda da sadece gerçek kişiler ile ilişkili verilerin korunduğu, hem ikinci maddeden hem de kişisel verinin tanımının yapıldığı üçüncü maddeden anlaşılmaktadır. Kişisel verilerin korunmasına dair uluslararası düzenlemelerde de öncelikle gerçek kişi ile ilişkili verilerin korunmasının hedef alındığı söylenebilir.³⁸ Tüzel kişilere ait veriler gerçek kişilerin verilerini de içe-

sistemleri ile korunması gerektiğini desteklemektedir. Jerry Kang, "Information Privacy in Cyberspace Transactions", Stanford Law Review, C.50, 1998, s.1211. Sonuç olarak tüzel kişilerin verilerinin, kişisel verilerin korunması mevzuatıyla korunup korunmaması hakkında mevzuatta ve öğretide bir görüş birliği bulunmamaktadır. Kuşkonmaz, s.9.

³⁵ OECD Rehber İlkeleri'nin 1/b ve 108 sayılı Avrupa Konseyi Sözleşmesi'nin 2/a maddelerinde yapılan kişisel veri tanımlarında sadece gerçek kişilere ait kişisel veriler kapsam içinde tutulmuştur.

³⁶ Korff, s. 14. Bununla birlikte Yönerge, tüzel kişilerin kişisel verilerinin korunup korunmayacağıyla ilgili düzenleme yapıp yapmamalarını taraf devletlerin takdirine bırakmıştır. Aydın, s. 8.

³⁷ Aksoy, s. 26; Kuşkonmaz, s.8; Aydın Akgül, Kişisel Verilerin Korunması Açısından İdarenin Hukuki Sorumluluğu ve Yargısal Denetimi, Doktora Tezi, Kocaeli Üniversitesi Sosyal Bilimler Enstitüsü, Kocaeli 2013., s. 10.

³⁸ 108 sayılı Avrupa Konseyi Sözleşmesi'nde gerçek kişiler ve gerçek kişilere ait kişisel veriler korunmaktadır (md. 2.a). Buna karşılık Sözleşme'ye katılan devletlerin, dolaylı veya doğrudan gerçek kişilerden oluşan kişi grupları, dernekler, vakıflar, topluluklar, kurumlar ve öteki organlarına da Sözleşme'nin kapsamı altında koruma sağlayabilecekleri yine Sözleşme'de yer almaktadır (md. 3. f.2b). OECD Rehber İlkelerinde de esas olarak gerçek kişilere ilişkin veriler korunmakta olup, tüzel kişileri veya kişi grupları uygulama alanına dâhil etmek üye devletlere bırakılmaktadır (m.6). 95/46/AT Sayılı Avrupa Birliği Yönergesi'nin uygulama alanını belirten 3. maddesinde de gerçek kişilere ait kişisel verilerin koruma altına alındığı görülmektedir. Bununla birlikte, Avusturya, Danimarka ve Lüksemburg gibi bazı ülkelerin veri koruma mevzuatlarında tüzel kişilere ait verileri de koruma altına aldıkları görülmektedir. Şimşek, Anayasa Hukukunda Kişisel Verilerin

riyorsa ve gerçek kişi tüzel kişinin verisi sayesinde belirli veya belirlenebilir hale geliyorsa,³⁹ bu durumda tüzel kişilere ait verilerde kişisel verilerin korunması hakkının kapsamı içinde olacaklardır.⁴⁰

Kişisel verilerin kamusal organlar karşısında korunması temel hakkının muhatabı esas olarak devlet olmakla birlikte, çeşitli uluslararası düzenlemelerde, devlet yanında özel sektör kurum ve kuruluşlarının da kişisel veri kurallarının muhatabı oldukları yer almaktadır.⁴¹

Kişisel Verilerin Korunması Kanunu'nun 2. maddesi düzenlenirken 95/46/AT sayılı Avrupa Birliği Yönergesi'nin örnek alındığı görülmektedir. 95/46/AT sayılı Avrupa Birliği Yönergesi'nin 3. maddesi Yönerge'nin uygulama bulacağı alanları belirtmiştir.⁴² Buna göre Yönerge, kişisel verilerin tamamen veya kısmen otomatik olarak işlenmesi ve bir dosyalama sistemine kaydedilen veya kaydedilecek kişisel verilerin otomatik olmayan yollarla işlenmesi durumlarında uygulama bulur.⁴³ Kişisel veriler otomatik olarak işlem görmese bile, bir dosya içerisinde organize edilmiş ve verilere ulaşılabilirlik belirli kriter veya

Korunması, s. 122. Doktrinde baskın olan görüşe göre, kişisel verilerin korunması hakkı temel bir insan hakkıdır. Akgül, s. 67. Her gerçek kişi, kişisel verilerin korunması temel hakkının sahibidir. Kişisel verilerin korunması hakkı, esas olarak kişinin verileri üzerindeki belirleme hakkını koruduğundan, hak sahibinin yaşayan gerçek kişi olması gerekir. Bu nedenle, ölü kişi, doğrudan kişisel verilerin korunması hakkının sahibi olamaz. Kişisel verilerin korunması hakkının, esas olarak insan onuru ve kişiliğini koruduğu söylenirse, bu hakkın tüzel kişileri kapsamadığı söylenebilir. Buna karşılık tüzel kişilerde, gerçek kişilere ait kişisel verilerin bulunması veya tüzel kişilere ait verilerde gerçek kişilere ait verilerin bulunması mümkündür. Tüzel kişilerde, doğrudan veya dolaylı olarak gerçek kişilere ait veriler varsa, bu durumda bu veriler mevcut düzenlemelere göre korunur.

³⁹ Örneğin, bir limited şirketin müdürü veya ortakları hakkındaki veriler.

⁴⁰ Şimşek, Anayasa Hukukunda Kişisel Verilerin Korunması, s. 122.

⁴¹ 108 sayılı Avrupa Konseyi Sözleşmesi, madde 1; OECD Verilerin Korunması İlkeleri madde 2.

⁴² Başalp., s.13; Şimşek, Anayasa Hukukunda Kişisel Verilerin Korunması, s.42; Daniel J Solove - Marc Rotenberg - Paul M. Schwartz, Information Privacy Law, İkinci Baskı, Aspen Publishers, New York 2006.,s. 902; Güray Dağ, Kişisel Verilerin Ceza Muhakemesi Hukukunda Delil Olarak Kullanılması, Doktora Tezi, Marmara Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Bilim Dalı, İstanbul 2011, s. 53.

⁴³ 95/46/AT sayılı Avrupa Birliği Yönergesi madde 3/1; David Bainbridge, Data Protection Law, CLT Professional Publishing, 2000, s. 17; Cristopher Kuner, European Data Protection Law: Corporate Compliance and Regulation, İkinci Baskı, Oxford University Press, 2007, s. 99. Bundan sonra "European Data Protection Law" olarak anılacaktır; Şimşek, Anayasa Hukukunda Kişisel Verilerin Korunması, s.42.

kriterlere göre kolaylaştırılmış⁴⁴ ise, bu işlemler Yönerge'nin koruması altındadır.⁴⁵ Bu anlamda kişisel verilerin bilgisayarda veya bir dosyada bulunması arasında fark yoktur. Otomatik veya elle işlenen bütün kişisel veriler Yönergenin kapsamı alanındadır.⁴⁶

C. Tanımlar

Kişisel Verilerin Korunması Kanunu'nun 3. maddesinde tanımlara yer verilmiştir.

1. Kişisel Veri

Kanunda kişisel veri, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi olarak tanımlanmıştır.⁴⁷ Bu bağlamda kişilerin kesin olarak belirlenmesini sağlayan adı, soyadı, doğum tarihi ve doğum yeri gibi bilgiler yanında, kişinin fiziki, ailevi, ekonomik ve sosyal özelliklerine ilişkin bilgiler de kişisel veri olarak kabul edilmelidir. Gerekçede, bir kişinin belirli veya belirlenebilir olması, "*mevcut verilerin herhangi bir şekilde bir gerçek kişiyle ilişkilendirilmesi suretiyle, o kişinin tanımlanabilir hale getirilmesi*" olarak tanımlanmıştır.⁴⁸ Gerekçede isim, telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak

⁴⁴ Örneğin, dosya içerisindeki kayıtların zaman sırasına göre tutulmuş olması gibi, Başalp, *Kişisel Verilerin Korunması ve İnternet*, s.14.

⁴⁵ Başalp, *Kişisel Verilerin Korunması ve Saklanması*, s.36.

⁴⁶ 108 sayılı Avrupa Konseyi Sözleşmesi ile karşılaştırıldığında Yönerge ile getirilen en önemli ilerleme elle işlenen kişisel verilerin de koruma içine alınmasıdır. Sözleşme'de üye ülkeler için elle işlenen kişisel verilerin korunmasıyla ilgili bir zorunluluk bulunmamaktadır. Akgül, s. 149; İngiltere, 95/46/AT sayılı Avrupa Birliği Yönergesi'nin elle işlenen kişisel verileri kapsamına itiraz etmiş ve buna karşılık sadece İngiltere'de elle işlenen kişisel verilerle ilgili 12 yıllık bir geçiş süreci olması kararlaştırılmıştır. Dorothee Heisenberg, *Negotiating Privacy: The European Union, the United States and Personal Data Protection*, Lynne Rienner Publishers, London 2005., s.28.

⁴⁷ Komisyon Raporu, s. 7.

⁴⁸ Gerekçeye göre, kişinin belirli veya belirlenebilir olması, "verilerin; kişinin fiziksel, ekonomik, kültürel, sosyal veya psikolojik kimliğini ifade eden somut bir içerik taşıması veya kimlik, vergi, sigorta numarası gibi herhangi bir kayıtlı ilişkilendirilmesi sonucunda kişinin belirlenmesini sağlayan tüm halleri kapsar" a.g.e, s. 7. Kişisel veri tanımında yer alan belirlenebilir kişi kavramında, "orantılılık prensibine" dikkat edilmelidir. Burada bir kişinin tespiti için orantısız olarak çok fazla zaman ve çaba gerekiyorsa bu durumda bu kişi belirlenebilir farz edilmemelidir. Bir kişinin kimliğinin belirlenebilir olup olmadığının tespitinde, başkaları tarafından kullanılacak makul yöntemler hesaba katılmalıdır. Tasarı, s. 18.

izleri, genetik bilgiler gibi verilerin kişileri belirli veya belirlenebilir kılma özelliklerinin bulunması nedeniyle kişisel veriler oldukları belirtilmiştir.⁴⁹

Kişisel verinin tanımı çeşitli uluslararası ve ulusal metinlerde yapılmıştır. Kişisel veriler, bu konuya ilişkin kabul edilmiş ilk uluslararası belge olan ve 1980 yılında OECD tarafından yayınlanan Kişisel Verilerin Sınırışan Trafiği ve Verilerin Korunmasına İlişkin Rehber İlkeleri'nin 1/b maddesinde⁵⁰ *"belirli veya belirlenebilir bir gerçek kişiye ilişkin tüm bilgiler"* olarak tanımlanmıştır.⁵¹

Kişisel verilerin korunmasına ilişkin kabul edilmiş ilk bağlayıcı uluslararası belge olan 28 Ocak 1981 tarih ve 108 sayılı "Kişisel Verilerin Otomatik Olarak İşlenmesi Sırasında Gerçek Kişilerin Korunmasına İlişkin Avrupa Konseyi Sözleşmesi" 2/a maddesinde⁵² yapılan bir başka tanımda ise, kişisel veriler, *"kimliği belirtilen veya belirtilebilen gerçek kişiye ait tüm bilgiler" şeklinde açıklanmıştır.*⁵³

95/46/AT sayılı ve 24 Ekim 1995 tarihli "Kişisel Verilerin İşlenmesi ve Bu Tür Verilerin Serbest Dolaşımına Dair Bireylerin Korunması Hakkındaki Avrupa Birliği Konseyi ve Avrupa Parlamentosu Yönergesi"⁵⁴ 2/a maddesinde yapılan tanımda ise kişisel veriler, *'belirli*

⁴⁹ a.g.e, s. 18.

⁵⁰ OECD Rehber İlkeleri, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data; (Çevrimiçi) <http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm>, (Erişim Tarihi: 12 Mart 2016), Bundan sonra "OECD Rehber İlkeleri" olarak anılacaktır. Kuner, European Data Protection Law, s.91.

⁵¹ Ahmet Boz, Kişisel Verilerin Korunması: Türkiye, ABD ve AB Örnekleri, Yüksek Lisans Tezi, Polis Akademisi Güvenlik Bilimleri Enstitüsü Güvenlik Stratejileri ve Yönetimi A.B.D., Ankara 2014, s. 7.

⁵² Kişisel Verilerin Otomatik Olarak İşlenmesi Sırasında Gerçek Kişilerin Korunmasına İlişkin Avrupa Konseyi Sözleşmesi, Sözleşme metni için bakınız. (Çevrimiçi) http://www.avrupakonseyi.org.tr/antlasma/aas_108.htm, (Erişim Tarihi: 10 Mart 2016) Bundan sonra "108 sayılı Avrupa Konseyi Sözleşmesi" olarak anılacaktır.

⁵³ Veli Özer Özbek, TCK İzmir Şerhi, Yeni Türk Ceza Kanununun Anlamı Özel Hükümler, C.II, Seçkin, Ankara 2008, s.948, Sabire Sanem Yılmaz, Tıp Alanında Kişisel Verilerin Hukuka Aykırı Olarak Verilmesinin Ceza Hukuku Açısından Değerlendirilmesi (Sır Saklama Yükümlülüğü Kapsamında), Yüksek Lisans Tezi, Bahçeşehir Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Yüksek Lisans Programı, İstanbul 2014, s. 22.

⁵⁴ Kişisel Verilerin İşlenmesi ve Bu Tür Verilerin Serbest Dolaşımına Dair Bireylerin Korunması Hakkındaki Avrupa Birliği Konseyi ve Avrupa Parlamentosu Yönergesi, Yönerge metni için bakınız. (Çevrimiçi) <http://eur-lex.europa.eu> (Erişim

veya belirlenebilir bir gerçek kişi hakkındaki tüm bilgiler” şeklinde yer almıştır.⁵⁵ “Belirlenebilir kişi” kavramı da aynı maddede “doğrudan veya dolaylı olarak özellikle bir kimlik numarası veya kişinin fiziksel, psikolojik, ruhsal, ekonomik, kültürel veya sosyal kimliğine bir veya birden fazla spesifik faktör referans alınarak, kimliği belirlenebilen kişi” olarak tanımlanmıştır.⁵⁶ TCK’nun gerekçesinde de “gerçek kişiyle ilgili her türlü bilgi, kişisel veri kabul edilmelidir” denmektedir.⁵⁷

Türk Dil Kurumu Güncel Türkçe Sözlük’e göre “kişisel” kelimesi, “kişi ile ilgili, kişiye ilişkin, kişinin kendi malı olan, şahsi, zatî”, “veri” ise “bilgi, data” olarak tanımlanmıştır.⁵⁸ Kişisel veri kavramı, en genel anlamıyla belirli veya kimliği belirlenebilir olmak, şartıyla bir kişiye⁵⁹ ilişkin bütün bilgileri ifade etmektedir.⁶⁰ Bu bilgiler; belli bir kimse- nin kimliği, etnik kökeni, fiziksel özellikleri, sağlık, eğitim, istihdam durumu, cinsel yaşamı, aile hayatı, başkaları ile yaptığı haberleşmeler, ikamet adresi, kredi kartı, kişisel düşünce ve inançları, dernek ve sendika üyelikleri, alışveriş alışkanlıkları gibi kişiyle ilgili, kişiyi belir-

-
- Tarihi: 10 Mart 2016), Bundan sonra “95/46/AT Sayılı Avrupa Birliği Yönergesi” olarak anılacaktır
- 55 Aksoy, s.15; Rosemary Jay -Angus Hamilton, Data Protection Law and Practice, Second Edition, Thomson, 2003, s.79; Bainbridge, s. 47; Cristopher Kuner, European Data Privacy Law and Online Business, Oxford University Press, 2003, s. 49, Bundan sonra “European Data Privacy Law” olarak anılacaktır; Aydın, s. 4.
- 56 Nil Melek Gültekin, Kişisel Verilerin Ceza Hukuku Yönünden Korunması, Yüksek Lisans Tezi, Galatasaray Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku A.B.D., İstanbul 2012, s. 7; Kuner, European Data Protection Law, s.91; Oğuz Şimşek, “4422 sayılı Çıkar Amaçlı Suç Örgütleriyle Mücadele Kanunu ve Kanununun 4. maddesine Göre “Kayıt ve Verilerin İncelenmesi ve Kişisel Nitelikli Verilerin Korunması”, *İzmir Barosu Dergisi*, S. 4, 2001, (Çevrimiçi) <http://web.deu.edu.tr/ab/MAKALE/deu%20MAK/0012.htm>, (Erişim Tarihi:10 Mart 2016).
- 57 Türk Ceza Kanunu madde gerekçeleri için bakınız. (Çevrimiçi) www.ceza-bb.adalet.gov.tr/mevzuat/maddegerekce.doc, (Erişim Tarihi: 15 Mart 2016); Gürsel Yalvaç, Karşılaştırmalı Gerekçeli TCK, CMK, CGTİK, 3. Bası, Adalet Yayınevi, Ankara 2007, s. 306;; Hale Akdağ, Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması, Yüksek Lisans Tezi, Ankara Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku (Ceza ve Ceza Usul Hukuku) A.B.D., Ankara 2010, s.6.
- 58 Türk Dil Kurumu Güncel Türkçe Sözlük, (Çevrimiçi) http://www.tdk.gov.tr/index.php?option=com_gts, (Erişim Tarihi: 10 Mart 2016).
- 59 Söz konusu kişinin gerçek veya tüzel kişi olması durumunda oluşacak farklılıklara ilerideki bölümlerde değinilecektir.
- 60 Başalp, Kişisel Verilerin Korunması ve Saklanması, s.22; Aksoy, s.1; Kuner, European Data Protection Law, s.92;; Dinç, Kişisel Verilerin Korunmasında Uluslararası Düzenlemeler, s. 4; Doğan Kılınç, Anayasal Bir Hak Olarak Kişisel Verilerin Korunması, AÜHFİD, C.61, S.3, 2012, s. 1090. Aydın, s. 4; Bu tanım 2014 tarihli Tasarınun 3//1-ç maddesinde de benzer şekilde yer almaktadır.

lenebilir hale getiren, doğrudan ya da dolaylı olarak bir gerçek kişiyle ilişkilendirilmesi suretiyle kişiyi tanımlayabilme özelliği bulunan bilgilerdir.⁶¹

2. Kişisel Verilerin İşlenmesi

Kanunda kişisel verilerin işlenmesi; *“kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem”* olarak, geniş bir alanı kapsayacak şekilde tanımlanmıştır. Gerekçede belirtildiği gibi, kişisel verilerin işlenmesi, verilerin ilk defa elde edilmesinden başlayarak veriler üzerinde gerçekleştirilen tüm işlem türlerini ifade etmektedir.⁶²

Kişisel verilerin korunması, bir ya da birden çok kişi veya kuruluşun dâhil olduğu bir sürece ilişkin düzenlemeleri içerir. Bu süreç, kişisel verilerin işlenmesi olarak adlandırılır.⁶³ İşleme, bilgisayarla ya da elle gerçekleştirilen her türlü süreci içerir.⁶⁴

3. Açık Rıza

Kanunda açık rıza, 95/46/AT sayılı Avrupa Birliği Yönergesi'nde yer aldığı şekilde *“Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza”* olarak tanımlanmıştır. Gerekçede de belirtildiği gibi, *“açık rıza ilgili kişinin kendisiyle ilgili veri işlenmesine, özgürce,*

⁶¹ Özbek, s.948; Kılınç, s.1092; Ersoy, Kişisel Verilerin Korunması, s. 16; Raymond Wacks, Personal Information Privacy and the Law, Clarendon Press, Oxford 1993, s. 26; Lee Bygrave, Data Protection Law - Approaching Its Rationale, Logic and Limits, Kluwer Law International, Newyork 2002, s. 43, Bundan sonra “Data Protection Law” olarak anılacaktır; Judith Wagner Decew, “The Scope of Privacy in Law and Ethics”, Law and Philosophy, 5, 1986, s.307; W. A. Parent, A New Definition of Privacy for the Law, Law and Philosophy, 2, 1983, s. 307.

⁶² Tasarı, s. 18.

⁶³ 95/46/AT sayılı Avrupa Birliği Yönergesi madde 2/b; Gültekin, s.70; Bainbridge, s. 48; Kuner, European Data Protection Law, s.242.

⁶⁴ Başalp, Kişisel Verilerin Korunması ve Saklanması, s. 15 - 16; 2014 tarihli Kişisel Verilerin Korunması Kanunu Tasarısı, md 3(e); Kuner, European Data Protection Law, s.79; Ersoy, Kişisel Verilerin Korunması, s. 17; Akgül, s. 62.

konuyla ilgili yeterli bilgi sahibi olarak, tereddüde yer bırakmayacak açıklıkta ve sadece o işlemle sınırlı olarak verdiği onay beyanı şeklinde anlaşılmalıdır.”⁶⁵

Kişisel verilerin korunmasında ilgili kişinin kişisel verileri üzerinde yapılan işlemlere rıza göstermesi, ilgili kişinin veri işleme sürecine katılmasını ve veriler üzerinde denetimini sağlayan, verilerin işlenmesine meşruluk katan önemli unsurlardan birisidir.⁶⁶ Birçok düzenlemede, belirli durumlarda kişisel verilerin toplanması, işlenmesi ve saklanmasıdan önce ilgili kişinin rızasının alınmasının gerekli olduğu belirtilmiştir.⁶⁷ Bu durumlarda rıza beyanı bu işlemlerin hukuka uygunluğunu sağlamaktadır. AB Temel Haklar Şartı'nın 8. maddesinde kişinin rıza beyanında bulunması ilkesine yer verilmiş, 95/46/AT sayılı Avrupa Birliği Yönergesi'nin 2/h ve 7/a maddelerinde ise ilgili kişinin rızası, veri işlemeyi meşru kılan durumlar arasında sayılmıştır.⁶⁸

4. Anonim Hale Getirme

Kanunda kişisel verilerin anonim hale getirilmesi, verilerin başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi olarak tanımlanmıştır. Bir başka deyişle, kişisel verinin anonim hale getirilmesi sonucunda elde kalan veri üzerinden bir izleme yapılarak başka verilerle eşleştirme ve destekleme sonrasında verinin kime ait olduğunun anlaşılabilmesi gerekir.⁶⁹

⁶⁵ Komisyon Raporu, s. 7.

⁶⁶ Küzeci, s.220; Şimşek, Anayasa Hukukunda Kişisel Verilerin Korunması, s.106. Kişisel verilerin korunması hakkının bir insan hakkı olduğu görüşü ilgili kişinin rıza beyanı ile etkinlik kazanmaktadır. Rıza beyanı, aynı zamanda bilgilerin geleceğini belirleme düşüncesinin bir yansımasıdır. Kuşkonmaz, s.101.

⁶⁷ Article 29 Data Protection Working Party, Opinion 15/2011 on the definition of consent, 01197/EN WP187, 13.07.2011, (Çevrimiçi), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf, (Erişim Tarihi: 12 Mart 2016).

⁶⁸ Şimşek, Anayasa Hukukunda Kişisel Verilerin Korunması, s.108; Peter Carey, Data Protection: A Practical Guide to UK and EU Law, Oxford University Press, 2004., s.250.

⁶⁹ Komisyon Raporu, s. 7. Çağımızdaki teknolojik gelişmeler dikkate alındığında kişisel verilerin anonimleştirilmesinin gittikçe zorlaştığı görülmektedir. Bir başka deyişle, her geçen gün yeni teknolojilerin gelişmesiyle kişisel veriler ile kişilerin arasındaki bağ kurulması daha kolaylaşmaktadır. Komisyon Raporu, s. 30.

Bir verinin kişiyi belirlenebilir kılıp kılmadığı hususunda incelenmesi gereken bir diğer konu da; takma ad kullanılan veriler,⁷⁰ şifreli veriler⁷¹ ve anonim verilerdir.⁷² Takma ad kullanılan veriler, özellikle istatistiki amaçlarla birden çok kişiye ilişkin birden çok veri toplanması gerektiğinde, bu kişilerin belirlenememesi için isimlerinin başka isimlerle değiştirilmesi durumunda oluşan verilerdir.⁷³ Şifreli verilerde ise kişilerin isimleri yerine bir kod numarası verilir ve bu kod numarası ayrı bir yerde saklanır. Kod numaralarına ulaşan birisinin bu numaralar vasıtasıyla ya da takma adları öğrenen birisinin bu takma adlar vasıtasıyla, kişilerin kimliğini öğrenebileceği mümkün olduğundan, takma adlı veriler ve şifreli veriler, veri koruma yasalarının koruması altındadır.⁷⁴ Takma adlı veriler Kişisel Verilerin Korunması Kanunu'nda tanımlanmamıştır.⁷⁵ Anonim verilerde ise, yapılan işlemler sonucunda belirlenebilir bir birey ile verinin arasındaki bağ koparılacak suretiyle bireyin kimliğinin tespiti olanaksız hale getirildiğinden, verilerin ait olduğu kişilere ulaşmak mümkün olmamaktadır. Bu nedenle anonim veriler, kişisel veri değildirler.⁷⁶ 95/46/AT sayılı Avrupa Birliği Yönergesi'nin başlangıç bölümününün 26. maddesinde anonim verilerin kişisel veri olmadığı belirtilmiştir.⁷⁷

5. Veri Kayıt Sistemi

Kanun kapsamında veri kayıt sistemi, kişisel verilerin belli kriterlere göre yapılandırılarak işlendiği bir kayıt sistemi olarak tanımlanmıştır. Kanunun gerekçesinde de belirtildiği gibi veri kayıt sistemleri elektronik veya fiziki ortamlarda oluşturulabilir.⁷⁸

⁷⁰ İngilizce, pseudonymised data.

⁷¹ İngilizce, key - coded data.

⁷² İngilizce, anonymous data.

⁷³ 95/46/AT sayılı Avrupa Birliği Yönergesi'nin 24 numaralı gerekçesi.

⁷⁴ Bazı yazarlar, şifreli verilerin ve takma ad kullanılan verilerin kişisel verilerle ilgili mevzuat altında korunmasının, özellikle tıbbi araştırmalar gibi uzun vadeli araştırmalar söz konusu olduğunda, mali açıdan külfetli ve pahalı olacağını savunmaktadırlar., Lucas Bergkamp - Jan Dhont, "Data Protection in Europe and the Internet: An Analysis of the European Community's Privacy Legislation in the Context of the World Wide Web", The EDI Law Review, S.7, 2000, s.74.

⁷⁵ Komisyon Raporu, s. 39.

⁷⁶ Walden Ian, "Anonymising Personal Data", International Journal of Law and Information Technology, C.10, S.2, 2002, s.224-237'den çeviren Kuşkonmaz s. 11.

⁷⁷ Aksoy, s. 36.

⁷⁸ Gerekçede veri kayıt sisteminde kişisel verilerin sınıflandırılması ile ilgili örnekler

95/46/AT sayılı Avrupa Birliği Yönergesi'nde veri kayıt sistemi yerine kişisel veri dosyalama sistemi terimi kullanılmıştır.⁷⁹ Yönerge'de, kişisel veri dosyalama sistemi, belirli bir ölçüte göre erişilebilecek şekilde yapılandırılmış kişisel veri kümesi olarak tanımlanmıştır. Bu veri topluluğunun merkezi veya merkezi olmayan veya fonksiyonel veya coğrafi temelde bölümlenmiş olması önemli değildir.⁸⁰

6. Veri Sorumlusu ve Veri İşleyen

Kanuna göre veri sorumlusu, kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu kişiler olup, bunlar gerçek kişiler veya tüzel kişiler olabilir.⁸¹ Veri işleyen ise, veri sorumlusu adına verileri işleyen gerçek ve tüzel kişilerdir.⁸²

108 sayılı Avrupa Konseyi Sözleşmesi'nde veri sorumlusu, ulusal hukuk kapsamında hangi tür kişisel verilerin hangi amaçla kaydedileceğine ve bunlara hangi işlemler uygulanacağına karar veren gerçek veya tüzel kişiler olarak tanımlanmaktadır.⁸³ 95/46/AT sayılı Avrupa Birliği Yönergesi, kişisel veri işleyenleri veri sorumlusu ve veri işlemcisi olarak iki gruba bölmüştür.⁸⁴ **Yönerge de veri sorumlusu, kişisel verilerin nasıl ve hangi amaçlar için işleneceğine tek başına veya başkalarıyla birlikte karar veren gerçek veya tüzel kişi, resmi ma-**

verilmiş olup buna göre, "veri kayıt sistemi, ad, soyad veya kimlik numarası üzerinden sınıflandırılabilmesi gibi, kredi borcunu ödemeyenlere ilişkin oluşturulacak sınıflandırma da bu kapsamda değerlendirilecektir." Tasarı, s. 19.

⁷⁹ İngilizce "personal data filing system".

⁸⁰ 95/46/AT sayılı Avrupa Birliği Yönergesi madde 2/c; Uygun, s. 50.

⁸¹ Komisyon Raporu, s. 7.

⁸² Veri işleyenler, kişisel verileri veri sorumluları tarafından verilen talimatlar çerçevesinde işleyen, bir başka deyişle veri sorumlularınca çalıştırılan kişiler olabileceği gibi, veri sorumlusu tarafından kendisinden verilerin işlenmesi hizmeti satın alınan ayrı bir gerçek veya tüzel kişi olabilir. Kanunun gerekçesinde verilen örnekte, bir muhasebe şirketinin kendi personeliyle ilgili tuttuğu verilerin işlenmesi açısından veri sorumlusu, aynı şirketin müşterisi olan şirketlere ilişkin kişisel verilerin işlenmesi açısından veri işleyen olarak kabul edilmesi gerektiği belirtilmiştir. a.g.e, s. 7.

⁸³ 108 sayılı Avrupa Konseyi Sözleşmesi md. 2-d; Songül Atak, "Avrupa Konseyinin Kişisel Veriler Açısından Sağladığı Temel Güvenceler", *Türkiye Barolar Birliği Dergisi*, S.87, 2010, s.96.

⁸⁴ Kuner, European Data Protection Law, s. 69; Kuner, European Data Privacy Law, s. 62.

kam, kuruluş veya diğer bir mercidir.⁸⁵ Veri sorumlusu, veri koruma memurundan farklıdır.⁸⁶ Veri sorumlusu, veri işlemcisinden de farklı birisidir. Veri işlemcisi, veri sorumlusunun talimatı üzerine kişisel verileri işleyen gerçek veya tüzel kişi, resmi makam, kuruluş veya diğer bir makamdır.⁸⁷

II. KİŞİSEL VERİLERİN İŞLENMESİ

A. Kişisel Verilerin İşlenmesiyle İlgili Genel İlkeler

Kişisel verilerin korunmasına ilişkin düzenlemelerde, verilerle ilgili yapılan işlemlerin insan onuru ve değerlerine uygun yapılması maksadıyla bazı ortak ilkeler belirlenmiştir.⁸⁸ Bu ilkelerin birbirinden kesin çizgilerle ayrılması zordur. Bazı ilkeler diğerlerine kaynaklık ederken bazıları da tamamlayıcı rol oynamaktadır.⁸⁹ Bu ilkelere riayet edilmemesi durumunda kişisel verilerin iyi niyetle, hukuka uygun olarak işlenmediği, ortada bir kötüye kullanımın bulunduğu kabul edilmektedir.⁹⁰ Kişisel verilerin işlenmesi ile ilgili genel ilkeler Kişisel Verilerin Korunması Kanunu'nun 4. maddesinde yer almaktadır.

Maddenin birinci fıkrasında kişisel verilerin ancak Kanunda ve diğer Kanunlarda öngörülen usul ve esaslar çerçevesinde işlenebileceği belirtildikten sonra ikinci fıkrada kişisel verilerin işlenmesi ile ilgili ilkeler sayılmıştır. Bu ilkeler; hukuka ve dürüstlük kurallarına uygun olma, doğru ve gerektiğinde güncel olma, belirli, açık ve meşru amaç-

⁸⁵ Kuner, European Data Protection Law, s. 117; Kuner, European Data Privacy Law, s. 62; Şimşek, Anayasa Hukukunda Kişisel Verilerin Korunması, s.44. Kişisel verilerin işlenmesi ile ilgili metotların ve amaçların milli veya Birlik kanunları tarafından belirlendiği durumlarda, veri sorumlusunun kim olduğu veya hangi özelliklere sahip olması gerektiği de düzenlenebilir. 95/46/AT sayılı Avrupa Birliği Yönergesi madde 2/d. Bu anlamda, tek başına ticaretle uğraşanlar, ortaklıklar ve şirketler veri sorumlusu olabilirler. Buna ilave olarak, okullar, yerel yönetimler, kolluk güçleri, hastaneler ve devlet kurumları gibi ticaret dışı topluluklarda veri sorumlusu olabilirler. Kuner, European Data Protection Law, s. 69; Kuner, European Data Privacy Law, s. 63..

⁸⁶ Veri koruma memuru, bir işletmede kişisel verilerin korunmasıyla ilgili kurallara uyulmasıyla sorumlu kişidir. Veri sorumlusunun veri koruma memuru atamak gibi bir zorunluluğu yoktur. Kuner, European Data Protection Law, s. 70.

⁸⁷ 95/46/AT sayılı Avrupa Birliği Yönergesi madde 2/e.

⁸⁸ Muammer Ketizmen, Türk Ceza Hukukunda Bilişim Suçları, Adalet Yayınevi, Ankara Ocak 2008, s. 269; Küzeci, s.196.

⁸⁹ Küzeci, s. 195; Akgül, s. 153.

⁹⁰ Kuşkonmaz, s.87.

lar için işlenme, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ve ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmediir.⁹¹

1. Hukuka ve Dürüstlük Kuralına Uygun Olma

Kişisel verilerle ilgili pek çok metinde, birbirine yakın ifadelerle, kişisel verilerin hukuka ve dürüstlük kuralına uygun olarak işlenmesi kuralına yer verilmiştir.⁹² Bu ilke diğer birçok ilkeyi kapsaması ve kaynağını oluşturması nedeniyle, kişisel verilerin korunması hukukunun ilk ilkesi olarak değerlendirilebilir.⁹³ Bu ilke, kişisel verilerin işlenmesi sırasında kanun ve diğer hukuksal düzenlemelere uygun olarak hareket edilmesi anlamına gelmektedir.⁹⁴ İlke, kişisel verilerin hukuka uygun olarak işlenmesi ve dürüstlük kuralına uygun olarak işlenmesi olarak ikiye ayrılabilir.

Kişisel verilerin hukuka uygun olarak işlenmesi, verilerin işlenmesinde kanunlara ve diğer hukuksal düzenlemelere uygun hareket edilmesi zorunluluğunu ifade eder.⁹⁵ Kişisel verilerin işlenmesinde dürüstlük kuralına⁹⁶ uygun hareket etme, veri sorumlularının verilerin işlenmesi sırasında şeffaflığa dikkat etmeleri ve ilgili kişilerin çıkarlarını ve beklentilerini dikkate almaları olarak tanımlanabilir.⁹⁷

⁹¹ Komisyon Raporu, s. 7.

⁹² Küzeci, s.196; Kuşkonmaz, s.88; Sevimli, s. 154; Dağ, s. 118.

⁹³ Akgül, s. 154.

⁹⁴ Küzeci, s.196; Ketizmen, s. 273; Dağ, s. 118.

⁹⁵ Küzeci, s.196; Akgül, s. 154. 95/46/AT sayılı Avrupa Birliği Yönergesi'nde ve 108 sayılı Avrupa Konseyi Sözleşmesi'nde verilerin işlenmesi, kişisel veri üzerinde uygulanan bütün süreçleri kapsayacak şekilde oldukça geniş bir şekilde tanımlanmış olup, işleme sürecinin tamamında hukuka uygun olarak hareket edilmesi, temel bir zorunluluktur. Küzeci, s.197; Kuşkonmaz, s.88.

⁹⁶ Medeni hukukun temel kavramlarından birisi olan ve Medeni Kanunun 2. maddesinde düzenlenen dürüstlük kuralı, toplum içinde kişilerin birbirleriyle olan ilişkilerinde nasıl davranmaları gerektiğini göstermekte ve kişilere buna göre davranma yükümlülüğü yüklemektedir, Kemal Oğuzman, Medeni Hukuk, Giriş, Kaynaklar, Temel Kavramlar, Filiz Kitabevi, İstanbul 2008, s.222.

⁹⁷ Akgül, s. 154. Bir başka deyişle kişisel verilerin ilgili kişiye bildirilen toplama ve işleme amaçları işlenmesini, ilgili kişinin bu hususta yanıtılmamasını kapsamaktadır. Hayrunnisa Özdemir, Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması, Seçkin Yayınları, Ankara 2009, s.138; Ketizmen, s.224; Kuşkonmaz, s.89. Kanuni bir temele dayanmadan veya kanunda belirlenen kısıtlamalara aykırı olarak kişisel verilerin gizli olarak işlenmesi dürüstlük ilkesine aykırı bir durumdur. Küzeci, s.197. Ayrıca, bu ilke gereği veri sorumluları, kişisel verilerin işlenmesi sırasında ilgili kişinin özel hayatın gizliliği hakkına ihlal

2. Doğru ve Gerekli İse Güncel Olma

Kişisel verilerin doğru olarak tutulması, kişisel verileri işleyen kişi yanında ilgili kişinin çıkarları açısından da gerekli ve önemli bir durumdur. Kişisel verilerin yanlış olarak tutulması, ilgili kişinin temel hak ve özgürlüklerini, ekonomik çıkarlarını ve manevi bütünlüğünü zedeleyici sonuçlar doğurabilir. Kişisel verileri işleyen veri sorumlusu kişisel verileri belli bir amaç için tutmaktadır. Kişisel verilerin yanlış olması veri sorumlusunun da çıkarlarını zedeleyecektir.⁹⁸

Kişisel verilerin doğru ve güncel tutulması, veri sorumlusunun yükümlülüklerindedir. Bu yükümlülük, 95/46/AT sayılı Avrupa Birliği Yönergesi'nin 6/1 d, 108 sayılı Avrupa Konseyi Sözleşmesi'nin 5/d maddesinde yer alırken, İsviçre Veri Koruma Yasası'nda sadece verilerin doğru olarak tutulmasına yer verilmiştir. OECD Rehber İlkelerinin 8. ve APEC Çerçeve Belgesinin 21. paragrafında kişisel verilerin doğru ve güncel olarak tutulması yanında tam olarak tutulması da bir zorunluluk olarak yer almaktadır.⁹⁹

3. Belirli, Açık ve Meşru Amaçlar İçin İşlenme

Kişisel verilerin belirli, açık ve meşru amaçlar için işlenmesi ilkesi, veri sorumlusunun, kişisel verileri işleme amacını açık ve kesin olarak belirlemesini ve bu amacın meşru olmasını zorunlu kılmaktadır. Veri sorumluları, kişisel verileri belirttikleri amaçlar dışında başka amaçlarla işlerlerse, bundan sorumlu olacaklardır. Gerekçede belirtildiği gibi, amacın meşru olması, veri sorumlusunun işlediği verilerin, yapmış olduğu iş veya sunmuş olduğu hizmetle bağlantılı ve bunlar için gerekli olması anlamına gelmektedir.¹⁰⁰

eden hareketlerden kaçınmalıdır. Bygrave, Data Protection Law, s.58.

⁹⁸ K. Ahmet Sevimli, İşçinin Özel Yaşamına Müdahalenin Sınırları, Doktora Tezi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, Özel Hukuk Anabilim Dalı, İstanbul 2006, s. 155; Küzeci, s. 203.

⁹⁹ Küzeci, s. 208. Kişisel verilerin doğru ve gerekli ise güncel olması ilkesi, kişisel verilere erişim hakkı ile yakından ilgilidir. İlgili kişi, kişisel verilerine erişemiyorsa bu verilerin doğru ve güncel olduğunun anlaşılması çok zor olacaktır. Veri sorumlusu, bunun için ilgili kişinin verilerine ulaşabilmesine olanak sağlayan bir sistem oluşturmalıdır. Web sitelerinde kullanıcıların bir şifre ile kişisel bilgilerine ulaşabildikleri sistemler buna örnek olarak gösterilebilir. Böylece veri sorumlusu üzerine düşen yükümlülüğü yerine getirmiş olacaktır. a.g.e., s. 209; Şimşek, Anayasa Hukukunda Kişisel Verilerin Korunması, s.85.

¹⁰⁰ Tasarı, s. 19.

Veri koruma düzenlemelerinin tamamında kabul edilen¹⁰¹ amaca bağlılık ilkesine göre; kişisel veriler hukuka uygun amaçlarla toplanmalı, toplanma amacı belirli ve açık olmalı¹⁰² ve işleme amacı toplama amacı ile uyumlu olmalıdır.¹⁰³ Amaca bağlılık ilkesi, kişisel verilerin dürüst ve hukuka uygun olarak işlenmesi ilkesinin uygulanıp uygulanmadığının tespiti açısından da önemli bir ilkedir.¹⁰⁴

Verilerin toplama amacının meşru olabilmesi için, bu amacın yasal bir temele dayanması, bütün hukuki gerekliliklerin tamamlanmış olması ve verilerin işlenmesinden elde edilen çıkar ile toplama amacının uyumlu olması gerekir.¹⁰⁵ 95/46/AT sayılı Avrupa Birliği Yönergesi'nin bu hususta tanıdığı bir istisna ise, üye devletlerin uygun önlemleri almaları koşulu ile kişisel verilerin tarihsel, istatistiksel ve bilimsel amaçlarla sonradan işlenmesidir.¹⁰⁶

¹⁰¹ AB Veri Koruma Yönergesi md. 6/1,c; 108 sayılı Avrupa Konseyi Sözleşmesi md. 5/b; OECD Rehber İlkeleri par. 9.

¹⁰² Verilerin toplama amacının belirli ve açık olması, belirsiz ifadelerin toplama amacıyla yer almamasını gerektirir. Ayrıca kişisel veriler ileriye kullanılmak amacıyla toplanmamalıdır. Bu, kişisel verilerin ilgili olduğu kişileri potansiyel suçlu konumuna sokar ve kişilerin kendilerini özgürce ifade etmelerini engeller. Özdemir, s.142; Akgül, s. 155. Kişisel verilerin toplanıp işlenmesi için ilgilinin rızası olmalı ya da hukuka uygun bir yetki olmalıdır. Kuşkonmaz, s.91.

¹⁰³ Kişisel veriler ilgili kişinin rızasına dayanılarak işleniyorsa, bu durumda rıza dar yorumlanmalıdır. Kişi, kişisel verilerinin hangi amaçla işlenmesine rıza gösteriyorsa, kişisel veriler ancak o amaç doğrultusunda toplanmalı ve işlenmelidir. Özdemir, s.142. 95/46/AT sayılı Avrupa Birliği Yönergesi'ne göre veri sorumluları, kişisel verilerin işleme amacını tam olarak belirlemeli ve bu amacı verilerin ilgili olduğu kişilere ve veri denetleme kurumlarına bildirmelidirler. Küzeci, s. 199; Kuşkonmaz, s.89; Sevimli, s. 154; Şimşek, Anayasa Hukukunda Kişisel Verilerin Korunması, s.83; Akgül, s. 72.

¹⁰⁴ Ketizmen, s.225.

¹⁰⁵ Kuner, European Data Protection Law, s. 100 Küzeci s. 202. 95/46/AT sayılı Avrupa Birliği Yönergesi'nin 7. maddesinde, kişisel verilerin işlenmesinin hangi durumlarda meşru olacağı belirlenmiştir. Buna göre; kişisel veriler, ilgili kişinin rızasının bulunması, ilgili kişinin taraf olduğu bir sözleşmenin ifa edilmesi ya da ilgili kişinin bir sözleşmenin tarafı olmadan önceki istemleri dolayısıyla işlemenin gerekli olması, veri sorumlusu tabi olduğu yasal bir yükümlülüğe uymak için işlemenin gerekli olması, ilgili kişinin yaşamsal çıkarlarının korunması için işlemenin gerekli olması, işlemenin kamu yararının bulunduğu bir hizmetin gerçekleştirilmesi ya da veri sorumlusunun veya verinin açıklandığı üçüncü kişinin resmi bir yetkisini kullanması için gerekli olması, Yönerge'nin 1/1 hükmü uyarınca ilgili kişinin temel hak ve özgürlüklerinden kaynaklı çıkarlarının baskın olduğu durumlardan hariç, veri sorumlusu veya verinin açıklandığı üçüncü kişinin meşru çıkarlarından kaynaklanan amaçlar için gerekli olması durumlarında işlendiği zaman bu işleme meşrudur.

¹⁰⁶ 95/46/AT sayılı Avrupa Birliği Yönergesi md. 1/b, 2. cümle.

4. Kişisel Verilerin, İşlendikleri Amaçla Bağlantılı, Sınırlı ve Ölçülü Olması

Bu ilke; belirlenen amaçları gerçekleştirmeye elverişli kişisel verilerin işlenmesi, amaçla ilgili olmayan veya amacın gerçekleştirilmesine hizmet etmeyecek kişisel verilerin işlenmesinden kaçınılmasını gerektirmektedir. Kanunun gerekçesinde belirtildiği gibi, kişisel verilerin sonradan ortaya çıkması muhtemel ihtiyaçların karşılanması amacıyla işlenebilmesi için, işlemeye ilk kez başlıyor gibi, 5. maddede yer alan şartlardan birinin gerçekleşmesi gerekecektir. Ayrıca işlenen veri sadece amacın gerçekleştirilmesi için gerekli olanla sınırlı tutulmalıdır.¹⁰⁷

Bu ilkeye göre, veri sorumlusu kişisel verileri toplamadan önce amacına ulaşmak için verilerin mutlaka kullanıp kullanmaması gerektiğini saptamalı, kişisel verilerden amaca ulaşmak için yeterli miktarını toplamalı ve işlemeli, gereğinden fazla veri toplamamalı ve işlememelidir.¹⁰⁸ İlkenin gereği olarak, kişisel veriler toplanma ve işleme amaçlarının gerçekleşmesi açısından gerekli ve yeterli miktarda tutulmalıdır.¹⁰⁹

¹⁰⁷ Tasarı, s. 19.

¹⁰⁸ Küzeci, s. 203; Akgül, s. 158. Bu ilkede, amaca ulaşmak için gerekli olan en az sayıda kişisel verinin işlenmesine çalışılmaktadır. Veri ekonomisi olarak adlandırılan bu yöntemle gereğinden fazla kişisel verinin işlenmesinin önüne geçilmeye çalışılarak, ilgili kişilerin mümkün olan en az miktarda risk altında tutulması amaçlanmaktadır.

¹⁰⁹ Kimi metinlerde "asgarilik ilkesi" olarak adlandırılan bu ilkeye göre, toplanan kişisel veri miktarı, verilerin toplanması ve işlenmesi amaçlarını başarmak için zorunlu olan miktarla sınırlı olarak tutulmalıdır. Kuşkonmaz, s.92; Küzeci, s.203. Bu ilke uyarınca veri sorumlusu, amacına ulaşabilmek için verilerin gerekli olup olmadığını saptamalıdır. Eğer kişisel veriler kullanılmadan veri sorumlusu amacına ulaşabilecek ise, kişisel veriler kullanılmamalıdır. Amaca ulaşmak için kişisel verilerin kullanılmasının zorunlu olduğu durumlarda ise veri sorumlusu mümkün olduğu kadar az veriyi kullanmalıdır. Federal Almanya Veri Koruma Yasası'nın 3a hükmünde de "...hiçbir verinin veya olanaklı bulunan en az miktarda kişisel verinin toplanması, işlenmesi veya kullanılması..." ibaresi bulunmaktadır. Küzeci s. 203. Burada amaca ulaşmak için gerektiğinden fazla kişisel verinin kullanılmasının önlenmesi amaçlanmıştır. Örneğin işverenin iş sözleşmesi çerçevesinde işçisinden isteyebileceği bilgiler, iş ilişkisi için gerekli olanlar ile sınırlı tutulmalıdır. Başalp, Kişisel Verilerin Korunması ve Saklanması, s.38. Aynı şekilde, ücretsiz e-mail hizmet sağlayıcısının gerekli olmamasına rağmen, ilgili kişinin yaş, cinsiyet bilgilerini de istemesi asgari sayıda verinin elde edilmesi ve amaca bağlılık ilkesine aykırılık teşkil eder. Küzeci, s.204. Veri sorumlusu, kişisel verilerin toplandığı her durumda amaca bağlılık ilkesinin gerektirdiği değerlendirmeyi yapmalıdır. a.g.e, s 203. Teknolojinin gelişmesiyle büyük miktarlarda kişisel verilerin kolayca

95/46/AT sayılı Avrupa Birliği Yönergesi'nin 6/1,c hükmü uyarınca, kişisel veriler, "toplanma ve/veya bunu izleyen işleme amaçları açısından yeterli ve onlarla ilgili olmalı, aşırı olmamalıdır." 108 sayılı Avrupa Konseyi Sözleşmesi'nde de bu ilke 95/46/AT sayılı Avrupa Birliği Yönergesi ile hemen hemen aynı şekilde yer almaktadır. 108 sayılı Avrupa Konseyi Sözleşmesi, 95/46/AT sayılı Avrupa Birliği Yönergesi'nden farklı olarak kişisel verilerin saklanma amacına da önem vermektedir. OECD Rehber İlkelerinde ve BM Rehber ilkelerinde ise bu ilkeye yer verilmemiştir. Ancak konu dürüstlük kuralı çerçevesinde değerlendirilebilir.¹¹⁰

5. İlgili Mevzuatta Öngörülen veya İşlendikleri Amaç İçin Gerekli Olan Süre Kadar Muhafaza Edilme

Kişisel verilerin, ancak ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmesi gerekir. Bu durumda veri sorumluları, kişisel verilerin muhafaza edilmesi süresini saptarken ilk olarak mevzuata bakacak, eğer mevzuatta bir süre belirlenmişse bu süre kadar muhafaza edebilecektir. Eğer mevzuatta bir süre belirlenmemişse, veri sorumluları kişisel verileri ancak işlendikleri amaç için gerekli olan süre kadar muhafaza edebileceklerdir. Bu sürenin sonunda kişisel veriler silinecek veya anonim hale getirileceklerdir. Kişisel veriler gelecekte kullanma ihtimaline binaen saklanmayacaktır. Veri sorumlusu, Kanun'un 16. maddesi uyarınca kişisel verilerin işlendikleri amaç için gerekli olan azami süreyi Sicile kayıt için başvururken bildirmek zorundadır.¹¹¹

95/46/AT sayılı Avrupa Birliği Yönergesi'nin 6/1-e maddesi, 108 sayılı Avrupa Konseyi Sözleşmesi'nin 5/c maddesi ve OECD Rehber İlkeleri'nin 8. paragrafında yer alan bu düzenlemeye göre kişisel ve

ve az bir maliyetle elde edilmesi sonucu, çok büyük miktarlarda kişisel veriler toplanabilmektedir. Bu durum kişisel verilerin korunmasıyla ilgili birçok sorun yaratabilecek kapasitedir. Örneğin, bir alışveriş merkezinde hırsızlığın önlenmesi için konulmuş kameraların mağazanın dışında yoldan geçen kişileri de kayıt altına aldığı durumda, amacı aşacak şekilde kişisel verilerin toplanması söz konusu olacaktır. Almanya'da görülen bir davada, sokaktan geçen kişilere gözetlenmedikleri bir alan bırakılarak görüntülerinin gereksiz yere kaydedilmemesi için market kameralarıyla kaldırımın en fazla bir metre uzağının gözetlenebileceğine karar verilmiştir. Küzeci, s. 210; Akgül, s. 159.

¹¹⁰ Bygrave, Data Protection Law, s.203.

¹¹¹ Komisyon Raporu, s. 8.

riler, ilgili kişinin teşhis edilmesine olanak sağlayacak şekilde, kişisel verilerin toplandığı veya daha sonra işlendiği amaçlar için gerekli olandan daha uzun süre tutulmamalıdır.¹¹²

B. Kişisel Verilerin İşlenme Şartları

Kişisel Verilerin Korunması Kanunu'nun 5. maddesinde kişisel verilerin işlenme koşulları düzenlenmiştir. Maddeye göre kural olarak kişisel verilerin ilgili kişinin açık rızasının bulunduğu durumlar veya maddede sayılan istisnalar dışında işlenmesi yasaktır.¹¹³

¹¹² Kuşkonmaz, s.93; Sevimli, s. 156; Akgül, s. 158. Kişisel verilerin tutulmasının ilgili kişi için potansiyel bir tehlike yarattığı düşünülürse bu ilkenin amacı ilgili kişiyi korumaktır. Kişisel verilerin amacın gerektirdiğinden daha uzun süre ileriye kullanılmaya ihtimaline karşı tutulması, ilgili kişinin kişisel verilerin korunması hukukunun dayanağını oluşturan bireysel özerklik, kişinin maddi ve manevi bütünlüğü ve özel yaşamın gizliliği gibi pek çok değerinin zarar görme ihtimalini arttıracaktır. Küzeci, s. 209. Nitekim AİHM'de S. ve Marper - Birleşik Krallık davasında kişisel verilerin süresiz olarak tutulmasına dair değerlendirmelerde bulunmuştur. Mahkeme, başvurucuların daha önceki davalarda alınan parmak izleri, hücre örnekleri ve DNA profillerinin beraat etmelerine ve ceza kovuşturmasına yer olmadığına karar verilmiş olmasına rağmen süresiz olarak tutulmaya devam edilmesinin, AİHS'nin 8. maddesine aykırı olduğuna karar vermiştir. S. ve Marper - Birleşik Krallık Davası, (Başvuru Numaraları: 30562/04 ve 30566/04) Karar Tarihi: 4 Aralık 2008, Kararın İngilizce metni için bakınız. AİHM kararlarında, kişisel verilerin olması gerekenden uzun süre tutulmasının AİHS'nin 8. maddesine aykırılık teşkil ettiğini belirtmiştir. AİHM, S. Ve Marper v. Birleşik Krallık Davasında, şüphelilerin suç nedeniyle parmak izi, DNA profili ve hücre örneklerinin belirsiz bir süre tutulmasına izin veren uygulamanın AİHS'nin 8. maddesine aykırı olduğuna karar vermiştir. Küzeci, s. 211; Akgül, s. 158.

¹¹³ Kişisel Verilerin Korunması Kanunu Gereğesinde 95/46/AT sayılı Avrupa Birliği Yönergesine göre rızanın ilgili kişinin kendisiyle ilgili veri işlenmesine, özgürce, konuyla ilgili yeterli bilgi sahibi olarak, tereddüde yer bırakmayacak açıklıkta ve sadece o işlemle sınırlı olarak verdiği onay beyanı olduğu belirtilmiştir. İlgili kişinin kişisel verilerinin işlenmesine gösterdiği rıza konusunda doktrinde çeşitli görüşler bulunmaktadır. Bir görüşe göre, birey, kişisel verilerinin işlenmesine rıza göstererek, kişisel verilerin korunması hakkını bizzat kullanmaktadır. Bir diğer görüşe göre ise, birey, kişisel verilerinin izlenilmesine rıza göstererek, kişisel verilerinin korunması hakkından vazgeçmektedir. Şimşek, Anayasa Hukukunda Kişisel Verilerin Korunması, s.108; Meral Ekici Şahin, Ceza Hukukunda Rıza, On İki Levha Yayıncılık, İstanbul 2012, s. 31. Her iki görüşte de ortak amaç, rıza beyanı sayesinde bireyi, veri işleme faaliyetlerinin basit bir objesi olmaktan korumak ve kişisel verileri üzerindeki denetimini arttırmaktır. Kişisel verilerin korunması hakkını mülkiyet hakkı kapsamında gören Amerikan Hukuku ile insan hakları kapsamında gören Avrupa Hukuku arasındaki fark, ilgili kişinin rıza beyanına yaklaşımda da görülmektedir. Amerikan hukukunda genel olarak kişisel veriler bir menfaat aracı olarak görüldüğünden, ilgili kişi kişisel verilerinin korunmasından tamamen feragat edebilmektedir. Kişisel verilerin korunmasının bir temel

1. Kişinin Açık Rızasının Bulunması

1982 Anayasası'nın 20. maddesine 2010 yılı Anayasa Değişikliği ile eklenen kişisel verilerin korunmasına ilişkin paragrafta da, "*kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir*" düzenlemesi yer almaktadır.

Avrupa Birliği Temel Haklar Şartı'nda ve 95/46/AT sayılı Avrupa Birliği Yönergesi'nde yer alan düzenlemelere göre, ilgili kişinin rıza beyanının geçerli sayılabilmesi için bazı gerekliliklerin karşılanması gerekmektedir. Yönerge'ye göre, ilgili kişinin rızasının bir hukuka uygunluk şartı olarak değerlendirilebilmesi için, "şüpheye yer bırakmayacak şekilde verilmiş" olması, bir başka deyişle "kesin" olması gerekir.¹¹⁴ Yine, özel nitelikli kişisel verilerin işlenmesinin söz konusu olduğu durumlarda da ilgili kişinin rızasının "açık" olması aranmaktadır.¹¹⁵

Rıza, ilgili kişinin açık ve kesin bir iradesi olmalı, bir başka deyişle ilgili kişinin kişisel verilerinin işlenmesine rıza gösterip göstermediği konusunda herhangi bir şüphe bulunmamalıdır.¹¹⁶ 95/46/AT sayılı

hak olarak benimsendiği Kıta Avrupası'nda ise, ilgili kişi, haklarının ihlali olan hareketlere karşı rıza göstermektedir. Kuşkonmaz, s.102.

¹¹⁴ 95/46/AT sayılı Avrupa Birliği Yönergesi madde 7/a.

¹¹⁵ 95/46/AT sayılı Avrupa Birliği Yönergesi madde 8/2 a. Özel nitelikteki kişisel verilerin işlenmesinde en önemli meşruiyet koşullarından birisi, ilgili kişinin rıza beyanında bulunmasıdır. Özel nitelikli kişisel verilerin işlenmesi için aranan rızanın, açık şekilde verilmesi, bir başka deyişle ilgili kişinin kabule yönelik iradesini ortaya koyan müspet bir hareketinin bulunması gerekmektedir. Kişinin hareket-siz kalması rıza gösterdiği şeklinde anlaşılmalıdır. Küzeci, s.240. 95/46/AT sayılı Avrupa Birliği Yönergesi'nde ilgili kişinin rıza beyanının geçerli olabilmesi için, dört durumun bir arada bulunduğu nitelikli bir rıza beyanının bulunması gerekmektedir.

¹¹⁶ Şüpheye yer bırakmayan rıza beyanı, açık veya örtülü şekilde yapılabilir; Başalp, Kişisel Verilerin Korunması ve Saklanması, s. 40; Beyanın anlam ve konusu, beyan vasıtalarından yani, kullanılan söz, yazı ve işaretlerden hiçbir yorum ve karışıklığa yer vermeyecek şekilde anlaşılıyorsa, bu bir açık rıza beyanıdır. Açık irade beyanın ilgili kişinin rıza beyanında 95/46/AT sayılı Avrupa Birliği Yönergesi'nce aranan ilk ölçütü karşıladığı açıktır. Küzeci, s.221. Örtülü rıza beyanında, birey rızasını dolaylı olarak başka davranış biçimleriyle veya bunların yorumuyla açıklamakta, hal ve şartlara göre değerlendirilen bu davranış biçimleri sonucunda kişinin rızasıyla ilgili kanaat elde edilmektedir. Mustafa Dural - Suat Sarı, Türk Özel Hukuku Cilt I, Temel Kavramlar ve Medeni Kanunun Başlangıç Bölümleri, İstanbul 2006, s.166'dan aktaran Kuşkonmaz, s.103; Beyan davranışı mevcut hal ve şartlara göre değerlendirildiğinde sonuçta beyanda bulunulduğuna dair bir kanaat elde edilebiliyorsa açık rıza beyanı gibi örtülü rıza beyanı da Yönerge'de

Avrupa Birliği Yönergesi'ne göre rıza, ilgili kişinin özgür iradesi sonucu olmalı, başka bir deyişle hiçbir etki altında kalınmadan verilmiş olmalıdır.¹¹⁷ 95/46/AT sayılı Avrupa Birliği Yönergesi'nde rıza beyanı ile ilgili aranan bir başka ölçüt ise, rızanın somut veri işlem faaliyetine ilişkin olmasıdır.¹¹⁸ İlgili kişinin kendisine ilişkin her türlü veri-

belirtilen ölçütü karşılamaktadır. Burada ilgili kişinin susması veya hareketsiz kalmasının rıza beyanı olarak kabul edilip edilemeyeceği tartışılabilir. Burada Yönerge'de belirtilen "şüpheye yer bırakmayacak" ifadesi önem kazanmaktadır. İlgili kişinin susması, başka davranış veya belirtilerle desteklenmesi nedeniyle şüpheye yer bırakmayacak şekilde rıza gösterdiğinin anlaşıldığı durumlar hariç, rıza beyanı olarak kabul edilemez; Başalp, Kişisel Verilerin Korunması ve Saklanması, s.40.

¹¹⁷ Bunun sağlanması için, ön şart, ilgili kişinin kişisel verilerinin işlenmesine rıza gösterip göstermeme konusunda gerçek bir seçim hakkı olmasıdır. Eğer ilgili kişi, rıza göstermeye mecbur bırakılmışsa veya üzerinde bu yönde bir baskı bulunuyorsa, bu durumda özgür iradesinin bulunduğundan söz edilemez. Özellikle ilgili kişi ile veri sorumlusu arasında işçi işveren ilişkisi gibi hiyerarşik bir ilişki varsa, bu durumda ilgili kişinin özgür iradesinin oluşup oluşmadığı sorgulanmalı ve ilgili kişi için ek bazı güvenceler sağlanmalıdır. Kuner, European Data Protection Law, s.68; Küzeci, s. 222. Carey, s.72,73. Bazı Avrupa Birliği üyesi ülkelerde işçilerin kişisel verilerinin korunması için işyerlerinde denetim sistemleri kurulmadan önce işveren işçi konseyleri ile anlaşmaya varması gerektiği düzenlenmiştir. İşçiler bu anlaşma çerçevesinde kişisel verilerinin korunmasında temsilcilerinden yardım almaktadır. Article 29 Working Party, Opinion on the Processing of Personal Data in the Employment Context, Opinion 8/2001, WP 48, 13.09.2001, s.23, (Çevrimiçi) http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2001/wp48sum_en.pdf (Erişim Tarihi: 15 Mart 2016). Bunun yanında, işçi işveren ilişkisi dışında, doktor hasta ilişkisi gibi ilgili kişinin veri sorumlusuna önemli oranda bağlı olduğu bazı diğer durumlarda da rızanın özgür irade ile verilip verilmediğinin özel olarak incelenmesi gerekebilir. Bu durumda ek bir güvence olarak, doktor hastaya, verilerinin işlenmesine rıza göstermemesinin tedavisini etkilemeyeceği açıkça belirtilmelidir. Kuşkonmaz, s.104. Yine ilgili kişi tarafından kişisel verilerinin işlenmesine rıza gösterilmemesi durumunda, ilgili kişi bir yaptırımla karşılaşacaksa, rızanın özgürce verildiğinden söz edilemez. Rızanın anlaşmanın yapılması için şart olarak yer aldığı durumlar buna örnek olarak verilebilir. Ancak rızanın gösterilmemesi durumunda öngörülen yaptırım çok hafif ise, bu durumda rızanın özgür bir irade sonucunda verildiği düşünülebilir. Örnek vermek gerekirse, parasız elektronik posta hizmetlerinin kullanılabilmesi için kullanıcı tarafından bilgisayarına çerez (cookies) yerleştirilmesi durumunda, eğer aynı hizmetin çerezlerin yerleştirilmesine gerek kalmaksızın ücretsiz olarak alınabileceği başka siteler varsa, ilgili kişi çerezlerin bilgisayarına yerleştirmek istemediği durumlarda bu hizmeti kolaylıkla başka sitelerden alabileceğinden, bu durumda rızanın özgürce verildiğini söyleyebiliriz. Küzeci, s.223.

¹¹⁸ Rıza belli bir duruma özgülenmiş, kişisel verilerin işlenmesine rıza gösterilen somut olay iyice tanımlanmış olmalıdır. Article 29 Working Party, Working Document on the processing of personal data relating to health in electronic health records (EHR), WP 131, 15.02.2007, s.9 (Çevrimiçi) http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp131_en.pdf (Erişim Tarihi: 15 Mart 2016).

nin işlenmesine rıza göstermesi şeklindeki bir rıza beyanı bu koşulun sağlanmamasından dolayı geçerli sayılmayacaktır.¹¹⁹ İlgili kişi, kişisel verilerinin işlenmesi ile ilgili, özellikle işlemenin içeriği, amacı, süresi, verilerin nerelerde kullanılacağı hakkında yeterince bilgilendirilmelidir.¹²⁰ 95/46/AT sayılı Avrupa Birliği Yönergesi'nde rıza beyanının şekline ilişkin herhangi bir koşul düzenlenmemiştir.¹²¹

İnternet ortamında yapılan rıza beyanları yukarıda belirtilen koşulları taşıyorsa kural olarak geçerli kabul edilmelidir. Ancak burada üzerinde durulması gereken, internet ortamında ilgili kişinin yeterli olarak bilgilendirilip bilgilendirilmediğidir.¹²² Bu konuda üzerinde durulması gereken bir başka hususta, "opt-in" ve "opt-out" olarak ifade edilen rıza türleridir.¹²³ "Opt-out" seçeneğinde kişinin hareketsiz kalması rıza beyanında bulunduğu anlamına geldiğinden, bu seçenek kişisel verilerin korunmasında "opt-in" seçeneğine göre daha zayıf bir koruma sağlamaktadır. 95/46/AT sayılı Avrupa Birliği Yönergesi'nin

¹¹⁹ Küzeci, s.223.

¹²⁰ Bir başka deyişle kişi, neye rıza gösterdiği konusunda bilgilendirilmiş olmalıdır. Kişisel verilerin ileriki dönemlerde de işlenmesi söz konusu ise, kişinin bundan da bilgisi olması gereklidir. Bu ölçüt, rızanın şüpheye yer bırakmayacak şekilde verilmesi gerekliliği ile de ilişkilidir. Ayrıca ilgili kişi neye rıza gösterdiği konusunda bilgilendirilirken anlaşılır bir dil kullanılmalıdır. Kişinin anlayamayacağı terimlerle dolu veya okuyamayacağı kadar küçük bir yazıyla yazılmış bir bilgilendirme formuna dayanan rıza beyanı Yönerge kapsamında geçerli bir beyan olarak kabul edilmeyecektir. Kuşkonmaz, s.105.

¹²¹ Bununla birlikte, Federal Almanya Veri Koruma Kanunu'nda rızanın yazılı olması gerektiği yer almaktadır. Elektronik ortamda yapılan rıza beyanlarında da genel kural olarak yazılılık koşulunun gerçekleştiği kabul edilmiştir. Korff, s. 32; Küzeci, s.224; Kuşkonmaz, s.105.

¹²² Bilgilendirme metninde yer alan bilgiler; fazla uzunsa, ifadeler açık değilse, sitenin içerisindeki yönlendirmelerle ulaşmak zorlaştırılmışsa veya ortalama bir kişinin anlayamayacağı teknik bir dille yazılmışsa, bu durumda ilgili kişinin yeterince bilgilendirildiği söylenemeyeceğinden rıza beyanı geçersiz sayılacaktır. Kuner, European Data Protection Law, s.68.

¹²³ Örneğin, e-maillerde "bu iletileri almak istemiyorsanız aşağıdaki kutuyu işaretleyiniz" gibi bir uyarı bulunuyorsa, bu "opt-out" rıza beyanına örnek olarak gösterilebilir. Burada kişi rıza beyanında bulunmak için herhangi bir eylemde bulunmaması, örnekte belirtilen kutuyu işaretlememelidir. Kişinin hareketsiz kalması rıza beyanında bulunduğu şekilde anlaşılmaktadır. Yine bir başka e-mailde "Kişisel bilgilerinizi size çeşitli fırsatlar sunacak X Şirketi ile paylaşmamızı istiyorsanız aşağıdaki kutuyu işaretleyiniz" gibi bir uyarı bulunuyorsa, bu durumda "opt-in" rıza beyanının bulunduğu bahsedilebilir. Burada ilgili kişi, rıza beyanında bulunmak için kutuyu işaretleyerek aktif bir hareket yapmaktadır. Kişinin hareketsiz kalması, rızasının olmadığı anlamına gelmektedir. Carey, s.254; Küzeci, s.225.

14. maddesi, doğrudan pazarlamaya ilişkin faaliyetlerde işlenen kişisel verilerle ilgili olarak “opt-out” seçeneğini standart olarak belirlemiştir.¹²⁴ Yönerge, diğer faaliyetlerde “opt-in” veya “opt-out” rıza koşulu bakımından zorunlu bir düzenleme içermemektedir. 2002/58/AT sayılı Avrupa Birliği Yönergesi de doğrudan pazarlama faaliyetlerinde “opt-in” seçeneğini standart olarak belirlemiştir.¹²⁵

2. İşlenme Yasağının İstisnaları

Maddenin ikinci fıkrasıyla ilgili kişinin açık rızası olmasa dahi bazı hallerde kişisel verilerin işlenebileceği düzenlenmiştir. Bu hallerden biri kanunda açıkça düzenlenmesidir.¹²⁶ Kişisel Verilerin Korunması Kanunu’na göre, rızanın açıklanamadığı veya geçerli olmadığı hallerde kişilerin hayat ve beden bütünlüklerinin korunması için gerekli ise kişisel veriler işlenebilir.¹²⁷ Kanunda yer alan ilgili kişinin açık rızası olmaksızın kişisel verilerinin işlenebileceği bir başka durum ise, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olmasıdır.¹²⁸

Kişisel Verilerin Korunması Kanunu’nun 5. maddesinin 2. fıkrasının (ç) bendine göre, veri sorumlusunun hukuki yükümlülüğünü ye-

¹²⁴ Kuner, European Data Protection Law, s.309.

¹²⁵ 2002/58/AT sayılı sayılı Avrupa Birliği Yönergesi madde 13/3. Article 29 Data Protection Working Party, Opinion 5/2004 on unsolicited communications for marketing purposes under Article 13 of Directive 2002/58/EC, WP 90, 27.02.2004, s.7, (Çevrimiçi) http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp90_en.pdf (Erişim Tarihi: 15 Mart 2016).

¹²⁶ Polis Vazife ve Selahiye Kanunu uyarınca şüphelilerin parmak izlerinin alınması, Adli Sicil Kanunu uyarınca Adalet Bakanlığınca adli sicil bilgilerinin işlenmesi Kanunun gerekçesinde verilen örneklerdir. Komisyon Raporu, s. 8.

¹²⁷ Gerekçede verilen örnekler göre, kişinin bilincinin olmadığı veya akıl hastası olması sebebiyle rızasının alınmadığı veya geçerli olmadığı durumlarda, hayat veya beden bütünlüğünün korunması amacıyla tıbbi müdahale yapılması gerekliyse, kan grubu, geçirilen hastalıklar ve ameliyatlar, kullanılan ilaçlar ile ilgili kişisel verileri işlenebilecektir. Yine hürriyeti tahdit edilen bir kişiyi kurtarmak amacıyla, kişinin veya şüphelinin yerinin belirlenebilmesi amacıyla kişisel verileri işlenebilecektir. a.g.e, s. 8.

¹²⁸ Kişisel Verilerin Korunması Kanunu, 5. madde 2/c. Gerekçede verilen örneğe göre, yapılan sözleşme gereği paranın ödenmesi için alacaklı tarafın hesap numarası alınabilecektir. Yine bu kapsamda, krdei sözleşmenin yapılması sırasında banka, kişinin maaş bordrosuna, tapu kayıtlarına, icra borcu olmadığına dair belgeye erişebilecektir. Komisyon Raporu, s. 9.

rine getirebilmesi için zorunlu olması durumunda, ilgili kişinin kişisel verileri açık rızası olmasa dahi işlenebilecektir.¹²⁹ Fıkranın (d) bendine göre, ilgili kişi, kişisel verilerini alenileştirmiş ise bir başka deyişle kendisi kamuoyuna açıklamış ise, bu kişisel veriler ilgili kişinin açık rızası olmasa dahi işlenebilecektir.¹³⁰ Burada ilgili kişi tarafından alenileştirilen, bunun sonucunda herkesin erişimine açık hale getirilen verilerin korunmasından beklenen hukuki yararın ortadan kalktığı kabul edilmektedir.¹³¹

Kişisel verilerin işlenmesinin bir hakkın tesisi, kullanılması veya korunması için zorunlu olduğu durumlarda, Kanunu'nun 5. maddesinin 2. fıkrasının (e) bendine göre ilgili kişinin açık rızası bulunmasa dahi kişisel verileri işlenebilecektir.¹³² Fıkranın (f) bendine göre, ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması durumunda da, ilgili kişinin açık rızası olmasa dahi kişisel verileri işlenebilecektir.¹³³

95/46/AT sayılı Avrupa Birliği Yönergesi de kişisel verilerin işlenebileceği durumları saymıştır.¹³⁴ Bu durumlar: ilgili kişinin herhangi

¹²⁹ Gereğede verilen örneğe göre, şirketler çalışanlarına maaş ödeyebilmek için, çalışanlarının banka hesap numarası, medeni durumu, eşinin çalışıp çalışmadığı, sosyal sigorta numarası gibi kişisel verilerini işleyebileceklerdir. Komisyon Raporu, s. 9.

¹³⁰ Kişisel verilerin alenileştirilmesinin nasıl yapıldığının, alenileştirme kavramının sınırlarının belirlenmesi önemlidir. Bu kapsamda yönetmelikte ayrıntılı düzenleme yapılması faydalı olabilir. Bu konunun yönetmelikle düzenlenmesi de Anayasa'nın temel hak ve özgürlüklerin kısıtlanmasına ilişkin 13. maddesine de aykırılık teşkil edebilir. Aksi takdirde konu içtihat ile aydınlatılacaktır.

¹³¹ Komisyon Raporu, s. 9.

¹³² Gereğede verilerin örneğe göre, bir şirketin kendi çalışanı tarafından açılan bir davada ispat için bazı verileri kullanması veya kısıtlı bir kişinin haklarının korunması amacıyla vasinin veya kayyımın, kısıtlının mali bilgilerini tutması hukuka uygundur. a.g.e, s. 9.

¹³³ Bu durumda, bir şirkette çalışanların kişisel verileri, temel hak ve özgürlüklerine zarar verilmemek kaydıyla, terfilerin, maaş zamlarının veya sosyal hakların düzenlenmesinde veya işletmenin yeniden yapılandırılması sürecinde görev ve rol dağılımında esas alınmak üzere, açık rızaları bulunmasa dahi işlenebilir. Burada şirket çalışanlarının terfilerinin, maaş zamlarının veya sosyal haklarının düzenlenmesi veya işletmenin yeniden yapılandırılması sürecinde çalışanların görev ve rol dağılımının yapılması veri sorumlusu statüsündeki şirket sahibinin meşru menfaatidir. Burada dikkat edilmesi gereken durum, aynı zamanda kişisel verilere ilişkin temel ilkelere uyulması ve veri sorumlusu ile verileri işlenen kişi arasındaki menfaat dengesinin gözetilmesidir a.g.e, s. 9.

¹³⁴ 95/46/AT sayılı Avrupa Birliği Yönergesi madde 7; Kuner, European Data Pri-

bir kuşkuya yer bırakmayacak şekilde kişisel verilerinin işlenmesine rıza göstermesi, ilgili kişinin taraf olduğu bir sözleşmeyi yerine getirmek veya bu sözleşmeye girmeden önce ilgili kişinin isteğiyle gerekli adımları atmak için kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun konu olduğu bir yasal zorunluluğa uymak için kişisel verilerin işlenmesi gerekmesi, ilgili kişinin hayati çıkarlarını korumak için kişisel verilerin işlenmesinin gerekmesi, kamu yararı için yapılan bir faaliyetin yerine getirilmesi veya veri sorumlusu veya verinin açıklandığı üçüncü tarafın kamu yetkisini kullanarak yaptığı bir faaliyetin yerine getirilmesi için kişisel verilerin işlenmesinin gerekli olması, Yönerge tarafından ilgili kişiye tanınan haklar ağır bastığı durumlar hariç olmak üzere, kişisel verileri işlemenin, veri sorumlusu veya verilerin açıklandığı üçüncü tarafın meşru çıkarları için gerekli olması durumlarıdır.

III. ÖZEL NİTELİKLİ KİŞİSEL VERİLERİN İŞLENME ŞARTLARI

A. Kapsam

Kişisel Verilerin Korunması Kanunu'nun 6. maddesinde, kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti,¹³⁵ dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri, özel nitelikli kişisel veri olarak sınıflandırılmıştır.¹³⁶ Kanundaki düzenlemeye göre, özel nitelikli kişisel verilerin, ilgili kişinin açık rızası olmaksızın işlenmesi yasaktır.¹³⁷

Kişisel verilerin korunması ile ilgili mevzuat incelendiğinde bazı verilerin diğerlerine kıyasla daha çok koruma altına alınmış oldukları görülmektedir. 95/46/AT sayılı Avrupa Birliği Yönergesi,¹³⁸ 108 sayılı

vacy Law, s. 58; Mustafa Topaloğlu, Bilişim Hukuku, Karahan Kitabevi, Adana 2005, s. 168; Ersoy, Kişisel Verilerin Korunması, s. 70.

¹³⁵ Kişilerin mezhebi ve kılık kıyafetinin özel nitelikli kişisel veri olarak kabul edilmesi sadece ülkemizde bulunmaktadır. Komisyon Raporu, s. 73.

¹³⁶ Gerekçede bu verilerin, başkaları tarafından öğrenildiği takdirde ilgili kişinin mağdur olabilmesine veya ayrımcılığa maruz kalabilmesine neden olabilecek nitelikte veriler olmaları nedeniyle özel nitelikli (hassas) veri olarak kabul edildikleri belirtilmiştir. a.g.e, s. 9.

¹³⁷ Kişisel Verilerin Korunması Kanunu, madde 6/(2).

¹³⁸ 95/46/AT sayılı Avrupa Birliği Yönergesi, madde 8.

Avrupa Konseyi Sözleşmesi,¹³⁹ BM Rehber İlkeleri,¹⁴⁰ belirli türdeki verilere özel koruma getirirken, OECD Rehber İlkeleri¹⁴¹ ve APEC Çerçeve Belgesinde bu şekilde özel bir koruma bulunmamaktadır.

Mevzuatta “hassas veri”,¹⁴² “özel koruma gerektiren veri»,¹⁴³ “özel tür veri”¹⁴⁴ gibi çeşitli isimler ile ifade edilen bu kişisel veriler, doğaları gereği kişilerin temel hak ve hürriyetleri ve mahremiyetleriyle ilişkili oldukları düşünülerek diğer kişisel verilerden farklı yollarla daha sıkı bir koruma altına alınmışlardır.¹⁴⁵ 108 sayılı Avrupa Konseyi Sözleşmesi’nin “Özel Veri Kategorileri” başlıklı 6. maddesinde iç hukukta uygun güvenceler sağlanmadığı sürece kişilerin ırksal kökeni, politik düşünceleri, dini veya diğer inançları, sağlık veya cinsel hayatları ve sabıka kayıtları ile ilgili kişisel verilerinin işlenemeyeceği düzenlenmiştir. 95/46/AT sayılı Avrupa Birliği Yönergesi’nin “Hassas Verilerin İşlenmesi” başlıklı 8. maddesinin 1. fıkrasında da, ırksal veya etnik köken, politik düşünceler, dini veya felsefi inançlar, sendika üyelikleri, sağlık ve cinsel yaşam ile ilgili kişisel verilerin işlenmesinin yasaklandığı düzenlenmiştir.¹⁴⁶

TCK’nin 135. maddesinin ikinci fıkrasında özel nitelikli kişisel veriler; “*kişilerin siyasi, felsefi veya dini görüşlerine, irki kökenlerine, hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgiler*” olarak belirtilmiştir.¹⁴⁷

¹³⁹ 108 sayılı Avrupa Konseyi Sözleşmesi madde 6.

¹⁴⁰ BM Rehber İlkeleri 5. ilke.

¹⁴¹ OECD Rehber İlkeleri, s. 40.

¹⁴² İngiliz 1998 tarihli Kişisel Verilerin Korunması Kanununda “sensitive personal data” olarak tanımlanmıştır.

¹⁴³ 108 sayılı Avrupa Konseyi Sözleşmesi’nin 6. maddesinde ise “özellikli veri kategorileri” kavramı kullanılmıştır.

¹⁴⁴ Hollanda Kişisel Verilerin Korunması Kanununda “special personal data” olarak tanımlanmıştır.

¹⁴⁵ Bainbridge, s. 48; Kuner, European Data Protection Law, s.101; Aksoy, s. 42; Sevimli, s. 148; Akgül, s.13; Aydın, s. 7.

¹⁴⁶ Kuner, European Data Protection Law, s.101; Aksoy, s. 42. Yönerge ve Sözleşme karşılaştırıldığında Avrupa Birliği ile Avrupa Konseyi’nin özel nitelikli kişisel verilerin belirlenmesi konusunda farklı tercihlerde buldukları anlaşılmaktadır. Kişilerin ırk, politik düşünceleri, dini inançları, sağlığı ile cinsel hayatına ait verileri Yönerge ve Sözleşme kapsamında özel nitelikli kişisel veri olarak koruma altına alınmışken, etnik unsur, felsefi inançları ve ticari birlik üyeliği Yönerge’de özel nitelikli kişisel veri olarak kabul edilmişken, Sözleşme’de diğer inançlar özel nitelikli kişisel veri olarak sayılmıştır. Akgül, s. 16; Yılmaz, s. 33.

¹⁴⁷ TCK’nda yer alan düzenlemenin, uluslararası düzenlemelerden en büyük farkı,

Özel nitelikli kişisel verilerin bazı ek güvencelerle korunmasındaki temel mantık, bunların diğer kişisel verilere kıyasla kişiye daha fazla zarar verebilme imkânına sahip olmalarıdır.¹⁴⁸ Her ne kadar temel mantık bu olsa da, bunun genel kabul eden görüş olduğu söylenemez.¹⁴⁹

Kanımızca bu durumda, kişisel verinin işlenmesinden elde edilecek yarar ile doğacak zarara bakmak gerekir. Bu ikisi arasında bir denge kurulması gereklidir. Kişisel verilerin korunması hukukunun temelinde yatan da bu düşüncedir. Bu düşünceden hareketle, kişisel verilerin her zaman tam olarak korunması gerektiği söylenemez. Kişisel verilerden beklenen yarar ile oluşturabileceği tehlike arasındaki denge sağlanabilmesi için bazı kişisel verilerin diğerlerine oranla daha fazla korunmasının yadırganmaması gerekir.

Bu konuda incelenmesi gereken bir başka husus ise, özel nitelikli kişisel veri kategorilerinin 95/46/AT sayılı Avrupa Birliği Yönergesi ve bu ayrımı benimseyen başka metinlerde, sınırlı sayma yöntemi ile belirlenmesi sonucu, bu verilerin tamamına aynı rejimi uygulamanın getireceği sakıncalardır. Özellikle, özel nitelikli kişisel verilerin işlenmesine getirilen genel istisnaların, kişinin dini inancı, etnik kökeni gibi özel nitelikli kişisel verilere bir ayırım gözetilmeden uygulanması

etnik kökenin 108 sayılı Avrupa Konseyi Sözleşmesi hariç uluslararası mevzuatta yer almasına rağmen TCK'da yer almaması ve ahlaki eğilimin uluslararası mevzuatta yer almamasına rağmen TCK'nda özel nitelikli kişisel veri olarak düzenlenmesidir. Küzeci, s. 73.

¹⁴⁸ Özel nitelikli kişisel verilerin açıklanması halinde kişiye zarar verebilecekleri veya kişi aleyhine ayrımcılığa yol açabilecekleri kabul edilmiştir. Bunların diğer kişisel verilerden ayrı bir rejime tabi tutulmalarının bir diğer nedeni de özelliklerinden dolayı daha sıkı bir denetime tabi tutulmalarını sağlamaktır. Akgül, s. 13; Kuner, European Data Protection Law, s.102.

¹⁴⁹ Örneğin, Federal Almanya Anayasa Mahkemesi, 1983 yılında verdiği Nüfus kararında, özel nitelikli kişisel verilere diğer kişisel verilere kıyasla ek güvence getirilemeyeceğini karara bağlamıştır. Mahkemeye göre, kişisel verilerin tamamı önemli olup, bunları daha çok önemliler şeklinde bir sınıflandırmaya tutmak yanlıştır. Başlangıçta tehlike taşımayan bir bilgi, tutulduğu işlemler sonucunda önemli hale gelebilir. Küzeci, s. 233; Doktrinde bazı yazarlar, bu görüşü desteklemektedir. Bu yazarlara göre, hangi verilerin korumaya değer olup olmadığı konusunda ayırımda bulunmak adil olmayıp, her kişisel verinin önem derecesi olayın özel şartlarına bakılarak değerlendirilmelidir. Ayrıca, kişisel veriler arasında özel nitelikli, özel nitelikli olmayan şeklinde bir ayırma gitmek, özel nitelikli olmayan kişisel verilerin tam olarak korunmadığı anlamına gelebilir. a.g.e., s. 234.

bazı sorunlar oluşturabilir.¹⁵⁰ Bunlara karşın, dinsel inançlara, siyasal tercihlerine, ırksal kökenlerine ilişkin kişisel verilerin işlenmesinin getirebileceği yararlar oldukça sınırlıdır.¹⁵¹

Buna karşın, kişilerin sağlık bilgileri, adli, idari sicilleri açısından durum farklıdır. Kişinin sağlık bilgilerinin kişi ile ilişkili tutulması, hasta açısından yararlı olacaktır.¹⁵² Bunun yanında tıbbi araştırmalar için sağlık ile ilgili kişisel veriler gerekebilir. Diğer taraftan, tıbbi veriler oldukça kişisel olup, kişilerin tıbbi bilgilerini gizli tutma hakları vardır. Bu bilgiler dolayısıyla, kişilerin tehdit edilebilecekleri, işlerinden ayrılmak zorunda kalabilecekleri, toplumdan soyutlanabilecekleri düşünüldüğünde, bu bilgilerin başkalarının eline geçmesinin ne kadar tehlikeli olabileceği anlaşılabilir.¹⁵³ Bunun yanında, kişinin tıbbi verilerinin yeterince korunmadığını düşünmesi, sağlık hizmetlerinden yararlanmamayı tercih etmesi gibi bir sonuçta doğurabilir.¹⁵⁴

¹⁵⁰ Kişinin dinsel inancı, ırksal kökeni ile bilgilerinin işlenmesinden, bireysel, sosyal ya da siyasal düzeyde ne gibi yarar elde edilebileceği tartışmalı bir konudur. Bir kişinin dinsel inancı ya da inançsızlığı, onun maneviyatı ile ilişkili olup, kişi, bu bilgiyi bir ya da birden çok kişiyle ancak kendi iradesiyle paylaşabilir. Kişinin bu bilgiyi başkalarıyla paylaşmama yönündeki iradesine karşın, bu bilginin işlenmesindeki yararın ne olacağı sorgulanmalıdır. Küzeci, s. 235. Demokratik devlet yapısında, örtülü ayrımcılık tehlikesi ile karşı karşıya kalmamak için, devletin kişinin dinsel inançları gibi konular karşısında gözlerinin bağlı olması gerekir. a.g.e., s. 235. Bu tür verilerin anonim olarak tutulmasının bile bazı sakıncaları olabilir. Örneğin, idarenin ibadethane inşa ederken, ülkedeki bu ibadethaneden yararlanacak kişilerin sayısını bilmesi gerekebilir. Ancak, bunlar istatistiksel olarak ulaşılacak bilgiler olup, bir kişinin dinsel inancının ne olduğunun bilinmesinden ziyade, yaklaşık olarak bir dine kaç kişinin inandığının bilinmesi yeterlidir. a.g.e., s. 235

¹⁵¹ Kimsesiz bir kişinin ani ölümü durumunda, bu kişinin cenaze işlemlerinin dinsel tercihlerine uygun bir şekilde gerçekleştirilebilmesi için dinsel inancı ile ilgili kişisel bilgilerine ihtiyaç tutulması örnek olarak verilebilir. a.g.e., s. 235. Eşitlik, demokratik bir hukuk devletinin önemli bir unsurudur. Hangi dini inanca, siyasal düşünceye sahip olsun, hangi ırksal kökenden gelirse gelsin, kişilerin kanun önünde eşit olması, eşit hizmet alması gerekir. Bu açıdan, çok istisnai durumlar hariç, idarenin planlama görevi açısından bu bilgilerin bir önemi olmaması gerekir. a.g.e., s. 235.

¹⁵² Doktorlar, doğru müdahalelerde bulunabilmek için çoğu zaman hastalarının sağlık ile ilgili kişisel verilerine ihtiyaç duyarlar.

¹⁵³ Sultan Üzeltürk, 1982 Anayasası ve İnsan Hakları Avrupa Sözleşmesine Göre Özel Hayatın Gizliliği Hakkı, Beta, İstanbul 2004, s. 112, Bundan sonra "Özel Hayatın Gizliliği Hakkı" olarak anılacaktır. 1982 yılında yayınlanan bir makalede, hastanede yatan bir hastanın kişisel bilgilerinin farklı gerekçe ve nedenlerle yaklaşık 75 kişi tarafından incelendiğinin tespit edildiği yer almaktadır. Yılmaz, s. 2.

¹⁵⁴ Bu konuya ilişkin AİHM'nin Finlandiya'ya karşı verdiği karar önemlidir. AİHM'e başvuru konusu olan olay, HIV virüsü ile ilgilidir. Mahkeme, bulaşıcı niteliği olan

Ceza hukukunda kuraların uygulanabilmesi için adli sicillerinin tutulması da sağlık ile ilgili kişisel veriler gibi değerlendirilebilir. Adli siciller ile ilgili kişisel veriler, kişilerin sosyal yaşamları ve ekonomik durumları üzerinde ciddi sonuçlar doğurabilecek etkiye sahiptirler. Buna benzer bir tartışma biyometrik veriler açısından da söz konusudur.¹⁵⁵ AİHM, kişisel veriler arasında, bu verilerin kişiler üzerinde doğurabilecekleri zararlara kıyasla bir ayırım yapılmasını ve bu nedenle daha sıkı koruma tedbirleri alınmasını makul görmektedir.¹⁵⁶

bu enfeksiyonla ilgili verilerin gizliliğinin korunmasının özellikle önemli olduğuna değinmiştir. Mahkeme'ye göre bu tür verilerin paylaşılması, kişinin özel ve aile yaşamının yanında sosyal durumunu ve iş durumunu da ciddi olarak etkiler. Bunun sonucunda, kişi toplumdan dışlanma ve adının lekelenmesi tehlikesi altına girebilir. Bu kararında AİHM, AİHS'ne taraf olan tüm devletlerin, tıbbi verilerin gizliliğine saygı göstermek zorunda olduğunu belirtmektedir. Sadece, hastanın özel hayatına saygı göstermek değil, hastanın tıp mesleğine ve genel olarak sağlık hizmetlerine duyduğu güveni de koruma şarttır. AİHM'e göre; böyle bir koruma olmazsa, tıbbi yardıma ihtiyacı olanlar, doğru tedavi görmek için ve hatta tıbbi yardım almak için gerekli olan kişisel veya mahrem bilgileri açıklamaktan caya-bilir; bu durumda hem kendi sağlıklarını, hem de bulaşıcı hastalıklar söz konusu olduğunda toplu sağlığını tehlikeye atar. AİHM kararında bu tür kişisel verilere yapılan müdahalelerin önemli bir kamu yararı bulunmadığı sürece AİHS'nin 8. maddesine aykırı olacağını belirtmiştir., Gilles Dutertre, Avrupa İnsan Hakları Kararlarından Örnekler, Avrupa Konseyi Yayınları, Ankara, 2003, s. 310 - 312, (Çevrimiçi) http://www.yargitay.gov.tr/abproje/belge/kitaplar/aih_m_kararlarindan_ornekler.pdf (Erişim Tarihi: 15 Mart 2016), Küzeci, s. 237; Akgül, s. 19.

¹⁵⁵ Küzeci, s. 237. Bu bağlamda bazı yazarlar, biyometrik yöntemler kullanılarak elde edilen kişisel verilerin kendi aralarında herhangi bir ayırma tabi tutulmadan değerlendirilmelerinin yanlış olacağı görüşündedirler. Cüneyd Er, Biyometrik Yöntemler ve Özel Hayatın Gizliliği Hakkı, Parmak İzi, Göz ve DNA Tarama Gibi Teknolojik Kimlik Denetleme Usullerinin Hukuki Statüsü, Yetkin, Ankara 2007., s. 115.; Leyla Keser Berber -, Murat Lostar, Bilişimde Biyometrik Yöntemler, Yetkin, Ankara 2006, s. 105 - 106; Küzeci, s. 238. Buna göre, örneğin işyerinde ses ve yüz tanıma teknolojilerinin yaratacağı sorunlar, parmak izi ve DNA kayıtlarının tutulmasından farklı değerlendirilmelidir. Çünkü burada kişinin yüz görüntüsü gibi, herkes tarafından bilinen, kamuya açık kişisel verilerinin iş sözleşmesi kapsamında kayıt altına alınması söz konusudur. Bu nedenle, kişinin parmak izi kaydı ile karşılaştırıldığında kişinin sosyal alanına daha sınırlı bir müdahale söz konusudur.

¹⁵⁶ Mahkeme, S. ve Marper Birleşik Krallık'a karşı davasında bu ayırma ayrıntılı olarak değinmiştir. Mahkemeye göre, hücre örnekleri, DNA profili ve parmak izi belirli veya belirlenebilir bir kişi ile ilişkilendirildiğinde tartışmasız bir şekilde kişisel veridir, ancak aralarındaki nitelik farkı dolayısıyla hücre örnekleri ve DNA profili ile parmak izi kayıtlarını ayrı tutmak gerekmektedir. Hücre örnekleri, kişinin sağlığına ilişkin bilgi içerirken, DNA profili kişinin etnik kökenini ortaya çıkarabilir. Oysa parmak izi kayıtlarının bu şekilde bir etkisi yoktur. Bu nedenle, AİHM'e göre, ilgili kişinin hücre örneklerinin ve DNA profilinin bir veri bankasında tutulmasının sonuçları, parmak izinin bir veri bankasında tutulmasına kıyasla çok daha ağırdır. AİHM S. ve Marper Birleşik Krallık'a karşı Davası, Baş-

Kanımızca bu konuda bir belirleme yapılırken, öncelikle somut olayın koşulları göz önünde bulundurulmalıdır.¹⁵⁷ İlk aşamada çok önemsiz görünen bir bilgi, bazı koşullarda ilgili kişi açısından hayati öneme sahip hale gelebilir. Özel nitelikli kişisel verilerin, kişilerin hayatlarındaki önemlerinden dolayı özel bir korumaya tabi tutulması yerindedir. Ancak, bu kapsama hangi kişisel verilerin dâhil edileceğini saptamak güçtür.¹⁵⁸ 95/46/AT sayılı Avrupa Birliği Yönergesi'nde, bu veri grupları sınırlı sayma yöntemi kullanılarak belirlenmiştir.¹⁵⁹ Ancak, bu sayılan verilerle aynı nitelikte değerlendirilebilecek başka verilerin kapsam dışında tutulması birçok yazar tarafından eleştirilmiştir.¹⁶⁰

vuru Numarası: 30562/04 ve 30566/04, Karar Tarihi: 4 Aralık 2008; Küzeci, s. 237. Ülkemizde de 2006 yılında kimlik tespiti veya adli amaçla DNA örneklerinin alınması, analiz yapılması, veilerin saklanması, yararlanılması ile Türkiye Millî DNA Veri Bankasının kuruluş ve görevlerine ilişkin "DNA Verileri ve Millî DNA Veri Bankası Kanunu Tasarısı" hazırlanmış olup halen yasalaşmamıştır. Tasarı'ya göre, oluşturulacak DNA Veri Bankasına Adli Tıp Kurumu, Jandarma Genel Komutanlığı Kriminal Daire Başkanlığı ve Emniyet Genel Müdürlüğü Kriminal Daire Başkanlığı tarafından veri girişi yapılabilecektir. Tasarı'nın 11. maddesine göre, ceza veya güvenlik tedbirine mahkûmiyet ya da düşme kararı verilmesi halinde, DNA içeren yapılar hükmün kesinleşmesinden sonra derhal yok edilmekle beraber bu yapılardan elde edilen bilgiler süresiz olarak saklanacaktır. Bu durum, kişisel verilerin korunması ilkelerinden amaca bağlılık ve ölçülülük ilkelerine bağdaşmamaktadır. Aydın, s. 95.

¹⁵⁷ Küzeci, s. 238.

¹⁵⁸ a.g.e., s. 238. Bu kapsamda, bir verinin özel nitelikli kişisel veri olup olmadığına saptanmasında, ilgili kişinin menfaatleri, kişisel verinin muhtemel alıcıları ve kişisel verinin işlenmesi durumunda ilgili kişi veya kişiler üzerinde doğuracağı sonuçlar göz önünde bulundurulmalıdır. Akgül, s. 15.

¹⁵⁹ Avrupa Birliği'ne üye ülkelerin kişisel verilerin korunmasıyla ilgili kanunlarına bakıldığında aralarında özel nitelikli kişisel verilerin belirlenmesiyle ilgili farklılıklar bulunduğu görülmektedir. Bu ülkelerden Çek Cumhuriyeti, Yunanistan, Avusturya, Estonya İtalya ve İngiltere'deki kişisel verilerin korunması kanunlarında özel nitelikli kişisel verinin tanımının yapıldığı görülmektedir. Fransa, Almanya, Polonya, İsveç ve Hollanda kanunlarında ise, özel nitelikli kişisel veri tanımlanmadan Yönerge'ye atıfta bulunulmuştur. Akgül, s. 17.

¹⁶⁰ Bu eleştirilerde 95/46/AT sayılı Avrupa Birliği Yönergesi'nde özel nitelikli kişisel verilerin belirlenmesinde İkinci Dünya Savaşı sonrasında oluşan insan onurunun korumayı ve ayrımcılığı önlemeyi amaçlayan düdşncenin etkili olduğu, ancak teknolojik gelişmeler sonucunda Yönerge'de belirlenen özel nitelikli kişisel veri türlerinden bir kısmının önemini kaybederken, Yönerge'de yer almayan başka tür kişisel verilerin korunması ihtiyacının arttığı belirtilmiştir. Akgül, s. 16. Örneğin, finansal veriler ve yer verileri bu kapsamda sayılmadığından özel koruma altında değildirler. Oysa belirtilen türdeki verilerin işlenmesinin kişiler açısından önemli sonuçlar yaratabileceğine ve önemlerinin gittikçe arttığına çeşitli kaynaklarda yer verilmektedir. Örneğin kişinin bulunduğu yer verisinin işlenmesi, kişiliğin

Bu konuda değinilmesi gerekli bir başka husus, özel nitelikli kişisel veri olarak sayılan veri kategorileri ile ilişkili her türlü verinin bu kapsamda değerlendirilip değerlendirilmeyeceğidir. Bazı durumlarda, özel nitelikli kişisel verilerin içine dâhil olan veri türlerinin özel bir koruma altına alınmadığı görülebilir.¹⁶¹ Ulusal hukuk sistemleri açısından bu konuda önemli olan, veri koruma otoritesinin ve nihai olarak mahkemenin somut olaya bakarak yaptıkları yorumdur.¹⁶²

B. Özel Nitelikli Verileri İşleme Yasağının İstisnaları

Kişisel Verilerin Korunması Kanunu'nun 6. maddesinin 3. fıkrasında, hangi hallerde ilgili kişinin açık rızası aranmaksızın özel nitelikli kişisel verilerin işlenebileceği düzenlenmiştir. Buna göre, maddenin

değişik görüntülerini açığa çıkarması nedeniyle (kişinin kumarhanede, işkili mekânda bulunması gibi) ayrımcılık tehlikesini meydana getirmekte, ayrıca bu verilerin adam kaçırmaya, soygun, tehdit gibi çeşitli suçlarda kullanılması da güvenlik sorunları doğurabilmektedir. Küzeci, s. 239

¹⁶¹ Örneğin, gözlüklü bir insanın resmi onun sağlık durumuna ilişkin bir bilgi içermektedir, fakat sadece bundan dolayı özel koruma altına alınacak mıdır? Kişinin dinsel inancını yansıtan bir adının olması, sırf bu sebeple kişinin adının geçtiği her türlü kişisel veriyi özel nitelikli kişisel veri kategorisine sokar mı? Örneğin görme bozukluğu olan kişilere veya belli bir dini inanca sahip kişilere yönelik ilanlar bu kapsamda değerlendirilebilir. Bir kişinin gözlüklü fotoğrafı ya da dini inancını yansıtan adı ancak herhangi bir değerlendirme söz konusu olduğunda özel nitelikli kişisel veri kapsamında değerlendirilebilir. Bunun için somut olayın özellikleri göz önünde bulundurulmalıdır. Örneğin siyasetçi bir toplantıya katılma üzerindeki söylemlerin ne derece siyasi nitelik taşıyacağı o toplantının anlamından çıkarılabilir. Bu kapsamda, herhangi bir siyasi görüşü olmayan bir kişinin siyasi bir toplantıya katılması sadece bilgi edinme kapsamında olabileceği gibi, siyasi bir protestoya katılması bu anlamda değerlendirilemez. a.g.e, s. 232.

¹⁶² Avrupa Birliği Adalet Divanı Lindqvist kararında, 95/46/ AT sayılı Avrupa Birliği Yönergesi'nin 8/1. maddesini geniş yorumlayarak, sağlık verilerinin kişinin fiziksel ve ruh sağlığı ile ilgili her türlü bilgiyi içerdiğini belirtip, ilgili kişinin ağrının incinmesi ile ilgili bir bilginin sağlık ile ilgili verisi olduğu, bundan dolayı da Yönerge'de yer alan özel nitelikli kişisel verilerle ilgili korumalardan yararlanması gerektiğini belirtmiştir. Küzeci, s. 232, 233; Akgül, s. 14; AİHM'nin M.S. v. İsveç kararına konu olayda, başvuru iş yerinde geçirdiği iş kazası nedeniyle geçirdiği bel rahatsızlıklarını öne sürerek tazminat talebinde bulunmuş, bunun üzerine İsveç Sosyal Sigortalar Kurumu, başvuru tazminat talebinin haklılığını incelemek amacıyla, başvuru tedavisi görmekte olduğu hastaneden raporları talep etmiş ve başvurucuyla ilgili bu raporlar İsveç Sosyal Sigortalar Kurumuna gönderilmiştir. Sağlık verilerinin bu şekilde gönderilmesinin AİHS'ni ihlala ettiği iddia eden başvuru, AİHM'de dava açmış ve AİHM verdiği kararlarda, başvurucuyla ilgili sağlık raporları incelenmeden tazminat talebi ile ilgili bir karar verilemeyeceği, bundan dolayı bu durumun demokratik bir toplumda izlenen amaçlarla orantılı olduğuna karar vermiştir. Aydın, s. 37; Yılmaz, s. 44.

ilk fıkrasında sayılan sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hallerde ilgili kişinin açık rızası aranmaksızın işlenebilecektir. Sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilecektir. Ayrıca maddenin dördüncü fıkrasında, özel nitelikli kişisel verilerin işlenmesinde, Kurul tarafından belirlenen yeterli önlemlerin alınması şart olduğu düzenlenmiştir.

Kişisel verilerin korunmasıyla ilgili uluslararası düzenlemele- re bakıldığında özel nitelikli kişisel verilerin işlenmesiyle ilgili istisnaların bulunduğu görülmektedir.¹⁶³ 95/46/AT sayılı Avrupa Birliği Yönergesi'nin 8/2 maddesi, özel nitelikli kişisel verilerin işlenebileceği durumları belirlemiştir. Buna göre, özel nitelikli kişisel veriler, ilgili kişinin açık rızası bulunması,¹⁶⁴ veri işleme, veri sorumlusunun iş hukukundan kaynaklanan özel hak ve yükümlülüklerin yerine getirmesi için zorunlu olması,¹⁶⁵ ilgili kişinin ya da diğer bir kişinin yaşamsal çıkarlarının korunması için gerekli olması,¹⁶⁶ işlemenin ilgili kişi ta-

¹⁶³ Düzenlemeler arasında farklar bulunsa da bunlar genel olarak; ilgili kişinin rızası, hayati çıkarlarının korunması, özel nitelikli kişisel verilerin kamuya yararlı kurum ve kuruluşlar tarafından işlenmesi, ilgili kişinin özel nitelikli kişisel verilerini kamuya açıklaması ve yargılama sebebiyle işlemedir. Özdemir, s. 128; Akgül, s. 20.

¹⁶⁴ Özel nitelikli kişisel verilerin işlenmesindeki en önemli meşruiyet koşulu, ilgili kişinin rızasının bulunmasıdır. Bu veriler, ilgili kişi ile yakından ilgili olması sebebiyle, kişi, bu verilerin işlenip işlenmeyeceğine dair kararı kendisi vermeli- dir. Bu rıza, diğer kişisel verilerin işlenmesinde aranan rızadan farklı olarak açık şekilde verilmelidir. Bu ise, ilgili kişinin rızasını belli eden müspet bir hareketin yapılmasını gerektirir. Kişinin hareketsiz kaldığı durumlarda rıza gösterdiğinin söylenmesi söz konusu değildir. Ayrıca üye devletler, ilgili kişinin rızası olsa bile kişisel verilerin işlenmesini yasaklayabilirler. Kuner, European Data Protection Law, s. 101; Article 29 Working Party, Working Document on the Processing of Personal Data Relating to Health in Electronic Health Records (EHR), WP 131, 15 Şubat 2007, s.9.

¹⁶⁵ Örneğin böyle bir zorunluluk, işçinin sendika kesintisini yapmak işverenin yasal göreviyse söz konusu olabilir. Bu istisnanın kapsamına yorum yoluyla ulaşmak söz konusu değildir. Bu koşulun sağlanması için verinin toplanması ve işlenmesi mutlaka gerekli olmalı ve yasal bir zorunluluktan kaynaklanmalıdır. Küzeci, s. 240.

¹⁶⁶ Bu istisnadan söz edebilmek için, ilgili kişinin hukuken veya fiziksel olarak rıza

rafından kamuya açıklanan verilere ilişkin ya da hakların kurulması, kullanılması ve korunması için gerekli olması,¹⁶⁷ kar amacı gütmeyen bir kurum tarafından yasal etkinliklerini yerine getirebilmesi için işleminin gerekli olması,¹⁶⁸ veri işleminin önleyici hekimlik, tıbbi teşhis, tıbbi yardım veya bakım veya sağlık hizmetlerinin idari olarak yürütülmesi için gerekli olması ve bu verilerin sağlık personeli veya sağlık personeli gibi sır saklama yükümlülüğüne tabi kişiler tarafından işlenmesi¹⁶⁹ durumlarında işlenebilir.¹⁷⁰ Bütün bunların yanında, Yönerge uyarınca üye devletler, uygun önlemleri almak koşuluyla, kamu yararı için başka istisnalar da belirleyebilirler.¹⁷¹ Örneğin Yönerge'de kişilerin idari ve adli mahkûmiyetlerine ilişkin verilerin bu kapsamda sayılıp sayılmayacağı üye devletlerin takdirine bırakılmıştır.¹⁷²

-
- göstermesinin imkânsız olması gerekir. Küzeci, s. 240. Aksi takdirde kararı verecek olan yine ilgili kişidir ve burada rızaya ilişkin koşulların bulunması gereklidir. Burada ilgili kişinin içinde bulunduğu özel durum sebebiyle rızasını açıklayabilme olanağına sahip olmadığı, eğer bu durum olmasaydı kesi olarak rızasının bulunacağı kabul edilmektedir. 95/46/AT Sayılı Avrupa Birliği Yönergesi, m. 8 - c. Kuner, European Data Protection Law, s.102. Bu durumda da kişinin rızasının varlığını garanti etmek için kişinin içinde bulunduğu olağanüstü durumun geçmesini müteakip açık rızasının alınması gerekir. Özdemir, s. 128; Akgül, s. 22.
- ¹⁶⁷ 95/46/AT Sayılı Avrupa Birliği Yönergesi, m. 8/2 e. İlgili kişinin özel nitelikli kişisel verilerinin bizzat kendisi tarafından kamuya açıklanması durumunda artık bu verilerin korunmadan yararlanması söz konusu olamaz. Örneğin kişinin kendisi tarafından haber muhabirlerine sağlık bilgileri ile ilgili yapılan bir açıklama sonrasında bu veriler kişisel verilerin korunması mevzuatının sağladığı korunmadan yararlanamayacaklardır. Özdemir, s. 129; Akgül, s. 22.
- ¹⁶⁸ 95/46/AT Sayılı Avrupa Birliği Yönergesi, m. 8/2 d. Bu istisnanın geçerli olması için, uygun önlemlerin alınması, verilerin kurumun üyeleri ya da bağlantılı kişilerle ilgili olması ve ilgili kişinin rızası olmaksızın üçüncü kişilere açıklanmaması gerekir. Burada belirtilen kar amacı gütmeyen kuruluş; dernek, vakıf, vb. olabileceği gibi, siyasal, felsefi, ya da sendikal bir amaca yönelik bir örgütlenme de olabilir. Küzeci, s. 241; Kuner, European Data Protection Law, s.102.
- ¹⁶⁹ 95/46/AT Sayılı Avrupa Birliği Yönergesi, m. 8/3; Burada sağlık hizmetlerinin sağlanmasına için bazı veri türlerinin işlenmesine istisna getirildiği görülmektedir. Ancak burada da verileri işleyebilecek olanlar sır saklama yükümlülüğüne tabi kişiler olarak sınırlandırılmıştır. Kuner, European Data Protection Law, s.102.
- ¹⁷⁰ Kuner, European Data Protection Law, s.101; Sevimli, s. 150-153.
- ¹⁷¹ 95/46/AT Sayılı Avrupa Birliği Yönergesi, m. 8/4
- ¹⁷² 95/46/AT Sayılı Avrupa Birliği Yönergesi m. 8/5. Bu istisnai durumlara ilişkin dikkat edilmesi gereken bir husus, bunların 95/46/AT sayılı Avrupa Birliği Yönergesi'nde belirlenen diğer kurallara uygun davranma zorunluluğunu ortadan kaldırmamalarıdır. Buradaki istisnai durum, sadece özel nitelikli kişisel verilere getirilen ilave korumaların uygulanmasına ilişkindir. Yönerge'de öngörülen diğer koruma tedbirleri ise uygulanmaya devam edecektir.

IV. KİŞİSEL VERİLERLE İLGİLİ İŞLEMLER

A. Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hâle Getirilmesi

Kişisel Verilerin Korunması Kanunu'nun 7. maddesiyle, kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi düzenlenmektedir.¹⁷³ Buna göre, hukuka uygun olarak işlenmiş kişisel verilerin işlenmesini gerektiren sebeplerin ortadan kalkması durumunda, bu kişisel veriler resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinecek,¹⁷⁴ yok edilecek¹⁷⁵ veya anonim hale getirilecektir.¹⁷⁶ İlgili kişi tarafından kişisel verilerin silinmesini isteme hakkı Anayasa'nın özel hayatın gizliliğini düzenleyen 20. madde-

¹⁷³ Komisyon Raporu, s. 10. Verileri yok etmeme suçu, TCK'nun 138. maddesinde "(1) Kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde bir yıldan iki yıla kadar hapis cezası verilir. (2) (Ek: 21/2/2014-6526/5 md.) Suçun konusunun Ceza Muhakemesi Kanunu hükümlerine göre ortadan kaldırılması veya yok edilmesi gereken veri olması hâlinde verilecek ceza bir kat artırılır." şeklinde düzenlenmiştir. Bu suçla, gerekçede de belirtildiği gibi kişisel verileri kanun tarafından öngörülen hukuki sürelerde yok etmekle yükümlü olan kişiler tarafından bu yükümlülüğe aykırı hareket edilerek yok edilmemesi hali yaptırıma bağlanmış ve bağımsız bir suç düzenlenerek kişisel verilerin keyfe bağlı olarak tutulmalarının önüne geçilmek istenilmiştir. Gültekin, s.181; Zeki Hafızoğulları -Muharrem Özen, Ceza Hukuku Özel Hükümler - Kişilere Karşı Suçlar, Us - A Yayıncılık, Ankara 2010.s.272; Özbek, s. 964; Ergün, s. 119; Murat Volkan Dülger, Bilişim Suçları, Seçkin, Ankara 2004, s.281; Taşkın, s. 110

¹⁷⁴ Kişisel verilerin silinmesi, gerekçede belirtildiği gibi, verilerin kayıtlı oldukları evrak, dosya, CD, disket, hard disk gibi kayıt ortamlarından tekrar hiçbir şekilde kullanılamayacak veya geri getirilemeyecek şekilde silinmesi anlamına gelmektedir. Tasarı, s. 22.

¹⁷⁵ Verilerin yok edilmesi ise, verilerin tekrar geri getirilemeyecek ve kullanılamayacak şekilde, verilerin kaydedildiği, evrak, dosya, CD, disket, hard disk gibi kayıt materyallerinin imha edilmesi demektir. Tasarı, s. 22.

¹⁷⁶ Verilerin anonim hale getirilmesinden, kişisel verilerin başka verilerle eşleştirilse dahi kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi kastedilmektedir. Anonim verilerde, yapılan işlemler sonucunda belirlenebilir bir birey ile verinin arasındaki bağ koparılmak suretiyle bireyin kimliğinin tespiti olanaksız hale getirildiğinden, verilerin ait olduğu kişilere ulaşmak mümkün olmamaktadır. Bu nedenle anonim veriler, kişisel veri değildirler. Ancak anonimleştirme sürecinin başlangıcında kişisel verilerin belirlenebilir olma özelliği yok olmadığından, süreç 95/46/AT sayılı Avrupa Birliği Yönergesi kapsamında korunmaktadır., Ian Walden, Anonymising Personal Data, International Journal of Law and Information Technology, C.10, S.2, 2002, s.224-237'den çeviren Kuşkonmaz s. 11. 95/46/AT sayılı Avrupa Birliği Yönergesi'nin başlangıç bölümünün 26. maddesinde de anonim verilerin kişisel veri olmadığı belirtilmiştir. Aksoy, s. 36.

sinin 3. fıkrasında da düzenlenmektedir.¹⁷⁷ 108 sayılı Avrupa Konseyi Sözleşmesi'ne göre ilgili kişiler, verileri Sözleşme hükümlerine aykırı olarak işlenmişse, bu verilerin silinmesini istemek; silinme talebinin reddi durumunda hukuksal yollara başvurabilmek haklarına sahiptir.¹⁷⁸ 95/46/AT sayılı Avrupa Birliği Yönergesi'nin 12. maddesine **göre ilgili kişi, Yönerge'ye aykırı olarak işlenmiş veya eksik veya yanlış kişisel verilerinin silinmesini veri sorumlusundan isteyebilir.**¹⁷⁹

Kişisel Verilerin Korunması Kanunu'nun 7. maddesinin ikinci fıkrasıyla, kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin diğer kanunlarda yer alan hükümlerin saklı tutulması düzenlenmiştir. Bu bağlamda, gerekçede verilen örnekte olduğu gibi, Adli Sicil Kanununda verilerin silinmesini veya yok edilmesini düzenleyen hükümler Kişisel Verilerin Korunması Kanunu'na göre öncelikli olarak uygulanacaktır.¹⁸⁰ Maddenin son fıkrasında ise, kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin usul ve esasların çıkarılacak yönetmelikle düzenleneceği öngörülmüştür.

B. Kişisel Verilerin Aktarılması

Kişisel Verilerin Korunması Kanunu'nun 8. maddesinde, kural olarak kişisel verilerin aktarılamayacağı düzenlendikten sonra, 5. maddenin ikinci fıkrasındaki durumlarda işlenen kişisel verilerin ve yeterli önlemler alınmak kaydıyla 6. maddenin üçüncü fıkrasında belirtilen şartlarda işlenen özel nitelikli (hassas) kişisel verilerin, ilgili kişinin açık rızası aranmaksızın aktarılabilceği düzenlenmiştir. Kanun'un 9.

¹⁷⁷ Bu değişiklik 07/05/2010 tarih ve 5983 sayılı, "Türkiye Cumhuriyeti Anayasasının Bazı Maddelerinde Değişiklik Yapılması Hakkındaki Kanun"un 2. maddesinde yer almaktadır ve 12/09/2010 tarihinde yapılan referandum ile yürürlüğe girmiştir.

¹⁷⁸ 108 sayılı Avrupa Konseyi Sözleşmesi md. 8; Atak, s. 96; Şimşek, Anayasa Hukukunda Kişisel Verilerin Korunması, s.24.

¹⁷⁹ 95/46/AT sayılı Avrupa Birliği Yönergesi madde 12/b.

¹⁸⁰ Kanunda geçen "diğer kanunlarda yer alan hükümler saklıdır" ifadesi, diğer kanunlarda yer alan hükümleri Kişisel Verilerin Korunması Kanununun dışında tutacağından, bu hükümlerle Kişisel Verilerin Korunması Kanunu hükümlerinin çatışması durumunda, diğer kanun hükümlerinin ayrıksı olarak uygulanması sonucunu doğuracak, böylece kişisel verilerin korunması konusunda birçok ayrıksı düzenlemenin bulunması sonucunda kişisel verilerin korunması alanını daraltacaktır. Komisyon Raporu, s. 33.

maddesinde kişisel verilerin yurtdışına aktarılma usul ve esasları düzenlendiğinden, burada söz konusu olan yurtiçinde aktarılacak kişisel verilerdir.

Kanuna göre özel nitelikli olmayan kişisel veriler ilgili kişinin açık rızası olmaksızın yurt içinde ancak; kişisel verilerin işlenmesinin kanunlarda açıkça öngörülmesi veya fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için verilerin işlenmesinin zorunlu olması veya bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması veya veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için kişisel verilerin işlenmesinin zorunlu olması veya kişisel verilerin ilgili kişinin kendisi tarafından alenileştirilmiş olması veya bir hakkın tesisi, kullanılması veya korunması için veri işlenmesinin zorunlu olması veya ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması şartlarının birisinin bulunması durumunda aktarılabilir.

Özel nitelikli kişisel verilerin ilgili kişinin rızası olmaksızın yurt içinde aktarılabilmesi için ise, kişisel verilerin işlenmesinin kanunlarda açıkça öngörülmesi veya kişisel verilerin kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi il sağlık hizmetlerinin planlanması, yönetimi ve finansmanı amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından işlenmesi şartlarından birisinin bulunması gereklidir.

Kanun'un 3. maddesinin 1. fıkrasının (d) bendi uyarınca, verilerin aktarılması veya devralınması kişisel verilerin işlenmesi olarak tanımlandığından; gerekçede de belirtildiği gibi, kişisel verilerin alıcıları açısından özel nitelikli olmayan verilerin işlenebilmesi için 5. maddede sayılan koşulların bulunması, özel nitelikli verilerin işlenebilmesi için ise Kurul tarafından belirlenen yeterli önlemlerin alınması şartıyla 6. maddede sayılan koşulların bulunması gerekir.¹⁸¹

¹⁸¹ Komisyon Raporu, s. 11.

Kanun'un 8. maddesinin üçüncü fıkrasında, kişisel verilerin üçüncü kişilere aktarılmasına ilişkin diğer kanunlarda yer alan hükümlerin saklı olduğu düzenlenmiştir.

Türk Dil Kurumu'nun Güncel Türkçe Sözlüğü'nde "aktarmak" kelimesi, "iletmek, bildirmek", "kaynak kişiden derlenen herhangi bir parçayı kitlelere duyurmak ve yaymak" olarak tanımlanmıştır.¹⁸² Bu kapsamda Kişisel Verilerin Korunması Kanunu'nun 8. maddesinde bahsedilen aktarma fiili, Türk Ceza Kanunu'nun 136. maddesinde düzenlenen verileri hukuka aykırı olarak verme, yayma veya ele geçirme suçunu oluşturan verme¹⁸³ ve yayma¹⁸⁴ fiillerini kapsamaktadır.¹⁸⁵

¹⁸² Türk Dil Kurumu Güncel Türkçe Sözlük, (Çevrimiçi) http://www.tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.56eafdac63bfb0.90656990 (Erişim Tarihi: 17 Mart 2016)

¹⁸³ Türk Dil Kurumu'nun Güncel Türkçe Sözlüğü'nde "vermek" kelimesi, "üzerinde, elinde veya yakınında olan bir şeyi birisine erdirtmek, iletmek", olarak tanımlanmıştır. Türk Dil Kurumu Güncel Türkçe Sözlük, (Çevrimiçi) http://www.tdk.gov.tr/index.php?option=com_gts, (Erişim Tarihi: 14 Mart 2016) Kişisel veriyi vermek fiilinde, bu veriyi bir kişiye ulaştırmak söz konusudur. Özbek, s.960; Ergün, s. 117; Mustafa Artuç, Kişilere Karşı Suçlar, Adalet Yayınevi, Ankara 2008, s. 1293; Yılmaz, s. 71. Vermenin yayma düzeyine ulaşmayan bir eylem olduğu söylenebilir. Şaban Cankat Taşkın, Bilişim Suçları, Beta, Bursa 2008, s. 107. Kişisel verilerin verilmesi eylemi birçok değişik şekilde gerçekleştirilebilir. Örnek olarak verilerin yazılı olduğu bir kâğıdı elden veya posta ile vermek veya CD, DVD, disk vb. ortamında vermek veya internet ortamında, e-mail vb. şekilde göndermek, vermek kavramının içine girer. Dülger, Bilişim Suçları, s. 277; Karagülmez, s.234; Taşkın, s. 107; Uygun, s. 94. Suç, kişisel verinin gönderilen kişinin eline geçmesi, onun tarafından öğrenilmesi ile sonlanır. Ahmet Gündel, Yeni Türk Ceza Kanunu Açıklaması, 3. Cilt, Ankara 2008, s. 2903. Kişisel verileri vermek suçunu sadece, verileri elinde bulunduran birisi işleyebilir. Hafızoğulları - Özen, Ceza Özel, s.271

¹⁸⁴ "Yaymak" kelimesi ise Türk Dil Kurumu'nun Güncel Türkçe Sözlüğü'nde "birçok kimseye duyurmak" olarak tanımlanmıştır. Kişisel verileri yaymak, onları birden fazla sayıda kişinin öğrenmesini sağlamaktır. Hafızoğulları - Özen, Ceza Özel, s.271; Osman Yaşar - Hasan Tahsin Gökcan -, Mustafa Artuç, Yorumlu - Uygulamalı Türk Ceza Kanunu, Cilt 3, 1. Baskı, Adalet Yayınevi, Ankara 2010, s.4126; Artuç, s. 1293. Yaymak fiili de pek çok şekilde yapılabilir. Kişisel verilerin yazılı olduğu kâğıtları birden çok kişiye mektupla göndermek veya CD, DVD, disk vb. ortamında birden çok kişiye postayla göndermek veya kişisel verileri pek çok kişinin ulaşabileceği bir yere, örneğin bir web sitesine koymak, bir forum odasında birden çok kişinin okuyabileceği şekilde yazmak, yaymak fiili kapsamı içinde bulunan hareketlerdir. Dülger, Bilişim Suçları, s. 278. Kişisel verilerin yayılması eylemi, yazılı, görsel veya işitsel olarak yapılabilir. Kişisel verilerin yayılması eylemi radyo, TV gibi basın, gazete gibi yazılı basın veya sanal basın yoluyla işlenebilir. Taşkın, s. 107. Kişisel verinin fiilen birileri tarafından öğrenip öğrenilmediği önemli değildir. Dülger, Bilişim Suçları, s.278; Akdağ, s. 122.

¹⁸⁵ Verileri hukuka aykırı olarak verme, yayma veya ele geçirme suçu, TCK'nun 136. maddesinde "(1) Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan

C. Kişisel Verilerin Yurt Dışına Aktarılması

Kişisel Verilerin Korunması Kanunu'nun 9. Maddesiyle, Kanun'un 5. maddesinde düzenlenen kişisel veriler ve 6. maddede düzenlenen özel nitelikli kişisel verilerin yurt dışına aktarılması düzenlenmektedir.

Maddenin birinci fıkrasına göre, kişisel veriler ilgilinin açık rızası olmaksızın yurtdışına aktarılamaz. *İkinci fıkrada ise bu kuralın istisnaları yer almaktadır.* Buna göre, *özel nitelikli olmayan kişisel verilerin ilgili kişinin açık rızası olmaksızın yurt dışına aktarılabilmesi için ilk olarak Kanun'un 5. maddesinin ikinci fıkrasında belirtilen şartlardan birisinin bulunması gerekmektedir.* Bu şartlar; kişisel verilerin işlenmesinin kanunlarda açıkça öngörülmesi veya fiili imkansızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için kişisel verilerin işlenmesinin zorunlu olması veya bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması veya veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için kişisel verilerin işlenmesinin zorunlu olması veya kişisel verilerin ilgili kişinin kendisi tarafından alenileştirilmiş olması veya bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması veya ilgili kişinin temel hak ve

veya ele geçiren kişi, iki yıldan dört yıla kadar hapis cezası ile cezalandırılır." şeklinde düzenlenmiştir. Dülger, s.276; Topaloğlu, s. 179. Gelişen teknolojiyle birlikte bireyler internet sitelerine üye olabilmek, mağazalardan indirim kartları alabilmek, bankalarda işlem yaptırabilmek gibi birçok amaçla kişisel verilerini çeşitli kuruluşlara vermekte ve bazen kişisel veriler bu kuruluşlar tarafından bireyin rızasıyla veya olmadan başkalarıyla paylaşılmaktadır. Ergün İsmail, Siber Suçların Cezalandırılması ve Türkiye'de Durum, Adalet Yayınevi, Ankara 2008, s. 113. Kişi hakkındaki veri ancak ilgili kişinin kendi rızası ile ya da kanunen yetkili kişilerce, ilgili kanun hükümleri uyarınca işlenebilir. Kişisel verilerin hukuka uygun paylaşımının artması, aynı zamanda hukuka aykırı paylaşımın da artmasına sebep olmuş ve birçok ülkede olduğu gibi ülkemizde de 5237 sayılı Türk Ceza Kanunu ile birlikte, kişisel verilerin korunması amacıyla bu tür fiilleri cezalandırmak için düzenleme yapılmıştır. Ergün, s. 116; Ersoy, Kişisel Verilerin Korunması, s. 95; Soyaslan Doğan, Ceza Hukuku Özel Hükümler, 8. Baskı, Ankara 2010, s.346; TCK'nun 136. maddesi, kişisel verilerin hukuka aykırı olarak verilmesi, yayılması ve ele geçirilmesini cezalandırmakta olup, diğer ülkelerde tanımlanan kimlik hırsızlığı suçunun da TCK'daki karşılığıdır. Kimlik hırsızlığı, bireyin adı, soyadı, sosyal güvenlik numarası, adresi ve kredi kart bilgileri gibi kişisel verilerini kullanarak, taklit edilmesi yoluyla çeşitli şekillerde menfaat elde edilmesidir. Dülger, s.276, Gültekin, s. 161; Ergün, s. 116; Taşkın, s. 105.

özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olmasıdır. Bu şartlardan birisinin bulunması da özel nitelikli olmayan kişisel verilerin yurt dışına aktarılması için yeterli olmayıp, bunların dışında kişisel verinin aktarılacağı yabancı ülkede kişisel veriler için yeterli korumanın bulunması veya yeterli korumanın bulunmaması durumunda Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri ve Kurulun izninin bulunması gereklidir.

Özel nitelikli kişisel verilerin ilgili kişinin açık rızası olmaksızın yurt dışına aktarılabilmesi için ise ilk olarak Kanun'un 6. maddenin üçüncü fıkrasında belirtilen şartlardan birinin bulunması gereklidir. Bu şartlar; kişisel verilerin işlenmesinin kanunlarda açıkça öngörülmesi veya kişisel verilerin kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, il sağlık hizmetlerinin planlanması, yönetimi ve finansmanı amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından işlenmesidir. Özel nitelikli kişisel verilerin ilgili kişinin açık rızası olmadan yurt dışına aktarılabilmesi için yukarıda sayılan Kanun'un 6. maddenin üçüncü fıkrasında belirtilen şartlardan birisinin bulunması yanında özel nitelikli kişisel verinin aktarılacağı yabancı ülkede kişisel veriler için yeterli korumanın bulunması veya yeterli korumanın bulunmaması durumunda Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri ve Kurulun izninin bulunması gereklidir.

Kanun, 9. maddenin üçüncü fıkrasıyla Kurula yabancı ülkelerde kişisel verilerle ilgili yeterli koruma bulunup bulunmadığını belirleme ve ilan etme yetki ve sorumluluğu vermiştir. Maddenin dördüncü fıkrası, Kurulun, kişisel veriler için yabancı ülkede yeterli koruma olup olmadığına karar verirken ve verilerin yurt dışına aktarılmasına izin verirken hangi kriterleri dikkate alacağını düzenlemektedir. Buna göre Kurul; Türkiye'nin taraf olduğu uluslararası sözleşmeleri, kişisel veri talep eden ülke ile Türkiye arasında veri aktarımına ilişkin karşılıklılık durumunu, her somut kişisel veri aktarımına ilişkin olarak, kişisel verinin niteliği ile işleme amaç ve süresini, kişisel verinin aktarılacağı ülkenin konuyla ilgili mevzuatı ve uygulamasını, kişisel verinin aktarılacağı ülkede bulunan veri sorumlusu tarafından taahhüt edilen önlemleri, değerlendirecek ve ihtiyaç duyulması halinde, ilgili kurum ve kuruluşların görüşünü de alarak karar verecektir.

Maddenin 5. fıkrasında kişisel verilerin, uluslararası sözleşme hükümleri saklı kalmak üzere, Türkiye'nin veya ilgili kişinin menfaatinin ciddi bir şekilde zarar göreceği durumlarda, ancak ilgili kamu kurum veya kuruluşunun görüşü alınarak Kişisel Verilerin Korunması Kurulunun izniyle yurt dışına aktarılabilceği düzenlenmiştir. Maddenin 6. fıkrasında, kişisel verilerin yurt dışına aktarılmasına ilişkin diğer kanunlarda yer alan hükümlerin saklı olduğu belirtilmiştir.

Kişisel verilerin ülkeler arasında aktarılması ile ilgili uluslararası mevzuatta da düzenlemeler bulunmaktadır. 108 sayılı Avrupa Konseyi Sözleşmesi'nin 12. maddesi, bir taraf devletten diğerine yapılacak veri aktarımlarının özel yaşam gerekçesiyle engellenmesini ya da özel bir izne tabi tutulmasını yasaklamaktadır.¹⁸⁶ 181 sayılı Ek Protokol'le getirilen düzenlemeye göre, kişisel verilerin Sözleşme'ye taraf olmayan bir uluslararası örgüte ya da ülkeye gönderilebilmesi için, o örgütün veya ülkenin Sözleşme'ye uygun veri koruma seviyesine sahip olması gerekmektedir.¹⁸⁷

95/46/AT sayılı Avrupa Birliği Yönergesi'nde genel olarak yeterli nitelikte bir koruma düzeyi bulunmayan¹⁸⁸ **üçüncü ülkelere veri transferini**¹⁸⁹ yasaklayan bir rejim kabul edilmiştir.¹⁹⁰ Bir başka deyişle, Avrupa Birliği'nden üçüncü ülkelere kişisel veri aktarımı, 95/46/AT sayılı Avrupa Birliği Yönergesi'nde düzenlenen istisnalar¹⁹¹ **dışında**,

¹⁸⁶ Ancak taraf devletler arasında belli kategori kişisel veriler hakkında farklı düzenlemeler bulunuyorsa, bu durumda veri aktarmada sınırlama yapılabilir.

¹⁸⁷ 181 sayılı Ek Protokol m. 2. Ancak kişisel verilerin transferinde ilgili kişinin üstün bir yararı bulunuyorsa veya ülkeler arasında veriler için alınacak güvenlik tedbirleri hakkında antlaşmalar varsa, bu durumda kişisel veriler Sözleşme'ye taraf olmayan devletlere veya kuruluşlara gönderilebilir. 181 sayılı Ek Protokol m. 2. f. 2; Atak, s.96.

¹⁸⁸ Koruma düzeyinin yeterliliği, ilgili ülkedeki veri koruma kurallarının içeriği ve bunların uygulamadaki geçerlilikleri dikkate alınarak tespit edilmektedir. Başalp, Kişisel Verilerin Korunması ve İnternet, s.16.

¹⁸⁹ Yönerge, veri transferinin tanımını yapmamıştır.

¹⁹⁰ Başalp, Kişisel Verilerin Korunması ve İnternet, s.15. Burada üçüncü ülkeler Avrupa Birliği üyesi olmayan ülkelerdir. 95/46/AT sayılı Avrupa Birliği Yönergesi madde 25/1; Heisenberg, s.31; Topaloğlu, s. 167; Bygrave, Data Protection Law, s. 79.

¹⁹¹ Bu istisnalar; kişisel veri ilgisinin rızasının bulunması, veri aktarımının ilgiliye karşı bir sözleşmesel yükümlülüğün yerine getirilmesi için gerekli olması, bir kamu yararının bulunması, bir mahkeme kararının yerine getirilmesi veya aktarımın yasal olarak düzenlenmiş olması durumlarıdır. 95/46/AT sayılı Avrupa Birliği Yönergesi madde 26/1-a; Heisenberg, s.31.

ancak bu ülkelerde Yönergeye uygun bir kişisel veri koruma düzeyinin¹⁹² bulunması halinde mümkündür.¹⁹³ Yönerge, yeterli koruma düzeyinin saptanmasında özellikle dikkat edilmesi gereken şartları belirtmiştir. Bu şartlar; verinin niteliği, işlemenin amacı ve süresi, çıkış ülkesi ve varacağı ülke, üçüncü ülkede geçerli olan genel ve sektörel hukuk kuralları, bu ülkede uyulan mesleki kurallar ve uygulanan güvenlik önlemleridir.¹⁹⁴ Eğer üçüncü ülkede yeterli koruma düzeyi yoksa veri sorumlusunun ilgililerin özel alanıyla temel hak ve hürriyetlerin korunması konusunda yeterli¹⁹⁵ garanti göstermesi ve üye devleti transfere onay vermesi hallerinde transfer yasağı kalkacaktır.¹⁹⁶ 2000 yılında Avrupa Parlamentosu Amerika Birleşik Devletleri tarafından kişisel verilerin korunmasında Avrupa Birliği normlarına uyum amacıyla çıkardıkları Safe Harbor ilkelerini¹⁹⁷

¹⁹² Üçüncü ülkede yeterli koruma düzeyi bulunup bulunmadığına kural olarak üye devletlerin veri koruma organlarının buluşmasıyla oluşan Komisyon tarafından resmi olarak karar verilmektedir. Böylece, bir kere Komisyon, örneğin Kanada'nın yeterli veri koruma düzeyi bulunduğu karar verirse, üye ülke veri koruma organları Kanada'da bulunan şirketlere kişisel verilerin transferine engel olamazlar. Şimşek, Anayasa Hukukunda Kişisel Verilerin Korunması, s. 55; Heisenberg, s.27; Başalp, Kişisel Verilerin Korunması ve Saklanması, s.67; 29. Madde Veri Çalışma Grubu, yeterli düzeyi açıklamak üzere Üçüncü Ülkelere Kişisel Verilerin Transferinde Temel Prensipler adlı bir karar yayımlamıştır. Buna göre "yeterlilik" ölçütünün her somut olaya göre değerlendirilmesi gerektiğini belirtmiştir. Ancak, Veri Çalışma Grubu, veri aktarımının yoğunluğu, aktarımdaki tarafların sayısı gibi nedenlerden dolayı her somut olayda incelemenin zor olduğundan, veri aktarımına ilişkin "beyaz listeler" oluşturulmasını teklif etmiştir. Bu listeler hangi ülkelerin yeterli koruma düzeyine sahip olduğuna dair fikir vermek amacıyla oluşturulacaktır. 29 Data Protection Working Party, First Orientations on Transfers of Personal Data to Third Countries-Possible Ways Forward in Assessing Adequacy, XV D/5020/97-EN final WP4 26.06.1997, s.3, (Çevrimiçi) http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1997/wp4_en.pdf (Erişim Tarihi: 15 Mart 2016)

¹⁹³ Dinç, Kişisel Verilerin Korunmasında Uluslararası Düzenlemeler, s. 49; Kong, Lingjie, Data Protection and Transborder Data Flow in the European and Global Context, European Journal of International Law, S. 21, 2010, s. 444.

¹⁹⁴ Kuşkonmaz, s.81; Başalp, Kişisel Verilerin Korunması ve İnternet, s.16.

¹⁹⁵ Veri sorumlusunun göstereceği garantide ilgilinin temel hak ve hürriyetlerinin ve özellikle özel alanının korunacağı garanti edilmelidir. Garantinin içeriği 95/46/AT sayılı Avrupa Birliği Yönergesi'nin 6, 7, 8, 11, 12 ve 14'üncü maddeleriyle uyumlu olmalıdır. Madde 26'da sayılan haklarda garanti altına alınmalıdır. Başalp, Kişisel Verilerin Korunması ve Saklanması, s.73; Şimşek, Anayasa Hukukunda Kişisel Verilerin Korunması, s. 55; Heisenberg, s.33.

¹⁹⁶ Başalp, Kişisel Verilerin Korunması ve İnternet, s.17, Kong, s. 444.

¹⁹⁷ ABD Ticaret Bakanlığı tarafından 21 Temmuz 200'de yayımlanan Safe Harbor Privacy Principles için bakınız.(Çevrimiçi) http://export.gov/safeharbor/eu/eg_main_018475.asp (Erişim Tarihi: 12 Mart 2016).

kişisel verilerin korunması bakımından makul bir düzenleme olarak kabul etmiştir. Safe Harbor ilkeleri Avrupa Birliği üyesi devletlerde kişisel verileri transfer etmek isteyen ABD işletmelerinin uyacakları prensipleri içermektedir.¹⁹⁸

Yönerge'nin kişisel verilerin korunmasıyla ilgili yeterli koruma düzeyi bulunmayan üçüncü ülkelere veri aktarımını yasaklayan hükmü, bu ülkelerde kişisel verilerin korunması ile ilgili düzenlemelerin yapılmasına yol açması sebebiyle, Yönerge'nin etkisini Avrupa Birliği dışına taşımıştır.¹⁹⁹

V. VERİ SORUMLUSUNUN YÜKÜMLÜLÜKLERİ VE İLGİLİ KİŞİNİN HAKLARI

A. Veri Sorumlusunun Aydınlatma Yükümlülüğü

Kişisel Verilerin Korunması Kanunu'nun 10. maddesi, gerekçede belirtildiği gibi 95/46/AT sayılı Avrupa Birliği Yönergesi'ne paralel şekilde, veri sorumlusunun ilgili kişiyi aydınlatma yükümlülüğünü düzenlemektedir.²⁰⁰

Kanuna göre, veri sorumlusu veya yetkilendirdiği kişi, aydınlatma yükümlülüğü kapsamında ilgili kişiyi; veri sorumlusunun ve varsa temsilcisinin kimliği, veri işleme amacı, verilerin kimlere ve hangi amaçla aktarılabileceği, veri toplamanın yöntemi ve hukuki sebebi ile Kanun'un 11. maddesinde sayılan diğer hakları konusunda bilgilendirecektir.

İlgili kişinin kişisel verilerinin işlenmesi hakkında bilgilendirilmesi iki açıdan önemli olup; bunlar, bireyin kişisel haklarını etkin

¹⁹⁸ Carey, s. 121; Kuner, European Data Protection Law, s.113; Heisenberg, s.74; Ersoy, Kişisel Verilerin Korunması, s. 84; Yedi temel yükümlülüğten oluşan Safe Harbor ilkelerine göre; AB üyesi ülkelere kişisel verileri transfer etmek isten Amerikalı şirketleri, söz konusu kişisel verileri, hangi amaçlarla topladıkları hakkında ilgili kişileri bilgilendirmek, izinleri olmadıkça üçüncü kişilerle paylaşmamak, bildirim yapılırsa ve izin alınsa bile kişisel verileri aynı düzeyde koruma sağlamayan üçüncü kişilere aktarmamak, kişisel verilerin bütünlüğü ve güvenliği için gereken önlemleri almak, ilgili kişilere verilerine erişim hakkı tanımak, şikayetleri ile ilgilenmek ve bu konularda çıkabilecek sorunları çözmek için bağımsız mekanizmalar oluşturmakla yükümlüdürler. Akgül, s. 133.

¹⁹⁹ Kuşkonmaz, s.86; Kuner, European Data Privacy Law, s. 79.

²⁰⁰ Komisyon Raporu, s. 11.

olarak kullanabilmesi ve idarenin şeffaflığının sağlanabilmesidir.²⁰¹ Ayrıca, ilgili kişinin bilgilendirilmesi dürüstlük kuralı ile de yakından ilgilidir.²⁰² Bu sebeplerden dolayı, ilgili kişinin kişisel verilerinin işlenmesi hakkında bilgilendirilmesi, kişisel verilerin korunmasında önemli bir yere sahiptir.²⁰³

İlgili kişinin bilgilendirilmesi yükümlülüğü, 95/46/AT sayılı Avrupa Birliği Yönergesi'nin 10 ve 11. maddelerinde, APEC Çerçeve Belgesi'nin 15. paragrafında,²⁰⁴ 108 sayılı Avrupa Konseyi Sözleşmesi'nin 8. maddesinde,²⁰⁵ OECD Rehber İlkeleri'nin 13. paragrafında²⁰⁶ ve BM Rehber İlkeleri'nden 4. ilkede²⁰⁷ düzenlenmiştir. Bunlardan en ayrıntılı düzenleme, 95/46/AT sayılı Avrupa Birliği Yönergesi'nde yer almaktadır. 95/46/AT sayılı Avrupa Birliği Yönergesi'nde kişisel verile-

²⁰¹ Küzeci, s.212; Dağ, s. 121. Kişinin verilerinin işlendiğini bilememesi durumunda haklarını da kullanamayacağından, verilerinin işlenmesi hakkında bilgilendirilmesi, menfaatlerini koruyabilmesi açısından çok önemlidir. Bu anlamda her kişi, hangi verilerinin, kim tarafından işlendiği konusunda veri sorumluları tarafından bilgilendirilmelidir. Sevimli, s. 157.

²⁰² Şimşek, Anayasa Hukukunda Kişisel Verilerin Korunması, s.88.

²⁰³ Bygrave, Data Protection Law, s.63.

²⁰⁴ APEC Çerçeve Belgesi'nin 15. paragrafında ilgili kişinin hangi verilerinin toplandığı ve bunların ne gibi amaçlarla kullanılacağı konularında bilgilendirilmesi gerektiği bildirilmiştir.

²⁰⁵ 108 sayılı Avrupa Konseyi Sözleşmesi'nin 8. maddesinde, ilgili kişinin, kendisine ilişkin kişisel veri veya verilerin varlığını, toplama amaçlarını, veri sorumlusunun ikametini ve bağlı olduğu kuruluşu öğrenmek, makul sürede, aşırı bir masrafa tabi olmaksızın, kendisi hakkında otomatik bir veri kaydedilip kaydedilmediği konusunda anlaşılabilir bir bildirim almak, eğer bu veriler Sözleşme hükümlerine aykırı olarak işlenmişse, bu verilerin silinmesini istemek, silinme talebinin reddi durumunda hukuksal yollara başvurabilmek hakkına sahip olduğu yer almaktadır.

²⁰⁶ OECD Rehber İlkeleri'nin 13. paragrafında, bireyin; "a) veri sorumlusundan kendisiyle ilgili veri bulunup bulunmadığının bildirilmesi, b) kendisiyle ilgili veri bulunuyorsa, bu verilerin makul bir zamanda, makul bir ücretle, makul ve anlaşılabilir bir şekilde kendisine açıklanması, c) a) ve b) fıkraları uyarınca yaptığı başvurunun reddedilmesi durumunda kendine ret sebeplerinin bildirilmesi ve buna karşı itiraz edebilme hakkı tanınması, d) kendisiyle ilgili verilerin içeriğine itiraz edebilme ve bu itiraz başarılı olduğunda verilerin silinmesi, düzeltilmesi, tamamlanması veya değiştirilmesini isteyebilme hakkının olması" gerektiği düzenlenmiştir.

²⁰⁷ BM Rehber İlkeleri'nden 4. ilkede belirtildiği şekilde, kimliğini belge ile kanıtlayan herkes, kendisi hakkında verilerin işlenip işlenmediğinin bildirilmesini, bu verilerin makul bir şekilde, gereksiz gecikme ve masraf olmaksızın kendisine verilmesini, verilerin hukuksuz, gereksiz ve yanlış şekilde kaydedilmiş olması halinde uygun düzeltme ve silinmelerin yapılmasını ve üçüncü kişilere aktarıldığında bilgilendirilmesini isteme hakları vardır.

rin doğrudan ilgili kişiden elde edilmesi²⁰⁸ ve üçüncü kişilerden elde edilmesi²⁰⁹ durumlarında farklı düzenlemeler yer almaktadır.²¹⁰ Belli şartların bulunması halinde, veri sorumlusunun bildirim yükümlülüğünün ortadan kalkması söz konusu olabilir. 95/46/AT sayılı Avrupa Birliği Yönergesi'nin 11/2 maddesinde düzenlenen bu durumlar; ilgili kişiye bilgi vermenin mümkün olmaması, bilgi vermenin oransız bir çaba gerektirmesi, verileri kaydetme veya işlemenin kanunda açıkça yer alması ve kişisel verilerin istatistiki, tarihi veya bilimsel amaçlarla işlenmesi halleridir.²¹¹

B. İlgili Kişinin Hakları

Kişisel Verilerin Korunması Kanunu'nun 11. maddesi kişisel verileri işlenen kişinin haklarını düzenlemektedir. Maddeye göre kişisel verileri işlenen kişi kendisiyle kişisel veri işlenip işlenmediğini öğrenme, işlenmişse buna ilişkin bilgileri talep etme, verilerin işlenme amacı ile bunların amacına uygun kullanılıp kullanılmadığını öğrenme, yurtiçinde veya yurtdışında verilerin aktarıldığı üçüncü kişileri bilme, 7 nci maddede öngörülen koşullar çerçevesinde kişisel verilerin silinmesini, yok edilmesini veya verinin içeriğinin eksik ya da gerçeğe aykırı olması hallerinde bunların düzeltilmesini isteme hakkına sahiptir.²¹²

Madde kapsamında ilgili kişi, talebi doğrultusunda yapılan düzeltme, silme ve yok etme işlemlerinin, verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme, verilerinin kanuna aykırı olarak işlen-

²⁰⁸ Yönerge'nin 10. maddesi uyarınca, bilgiler doğrudan ilgili kişiden elde ediliyorsa, veri sorumlusu veya temsilcisi, ilgili kişiye, ilgili kişinin zaten bildiği durumlar hariç olmak üzere; veri sorumlusunun veya temsilcisinin kimliği, kişisel verilerin işlenme amacı, veri alıcıları veya alıcı kategorileri, sorulara cevap vermenin zorunlu veya isteğe bağlı olma durumu ve olası bir cevap vermemenin sonuçları, ilgili kişinin kişisel verileri hakkında bilgi alma ve düzeltme hakkının mevcut olduğu, veri işlemede özel nitelikli kişisel veriler gibi bazı özel durumların varlığı halinde dürüst işlemeyi temin edecek gerekli bilgileri vermesi gereklidir.

²⁰⁹ Yönerge, kişisel verilerin ilgili kişi yerine üçüncü kişilerden elde edilmesi durumunda veri sorumlusunun bilgilendirme yükümlülüğünü, 11. maddede düzenlemiştir. Buna göre, kişisel veriler üçüncü kişilerden temin edildiği veya ilgili kişiden temin edilmekle beraber üçüncü kişilerle paylaşıldığı durumlarda, ilgili kişi bu kapsamda bilgilendirilmelidir.

²¹⁰ Bainbridge, s. 108.

²¹¹ Kuşkonmaz, s.96.

²¹² Komisyon Raporu, s. 12.

mesi sebebiyle zarara uğraması halinde, veri sorumlusundan zararın giderilmesini talep etme hakkına da sahiptir.

Maddeyle ilgili kişinin, kişisel verilerinin otomatik sistemler kullanılarak analiz edilmesi suretiyle kendisi hakkında çıkacak aleyhe sonuçlara itiraz hakkının olduğu öngörülmüştür. Gereğede verilen örnekte olduğu gibi, bu maddeyle bir çalışan, performansının otomatik sistemlerde kişisel verileri kullanılarak ölçülmesine itiraz edebilecektir.²¹³

Kişisel verilerin korunması hukuku kapsamında, çeşitli düzenlemelerde ilgili kişiye kişisel verilerinin korunması için sürece aktif olarak katılmasını ve verileri üzerinde denetimini gerçekleştirebilmesini sağlayan bazı haklar verilmiştir. Kişisel verilere erişim hakkı, verilerin düzeltilmesini isteme hakkı ve bazı durumlarda veri işlemeye itiraz hakkı bu kapsamda sayılabilecek haklardandır.²¹⁴

Verilere erişim hakkı, bilgilendirme yükümlülüğü ile yakından ilişkilidir. Veri sorumlusunun, kişisel verilerinin işlendiği konusunda ilgili kişiyi bilgilendirmemesi durumunda, ilgili kişinin bundan haberi olamayacağından, verilere erişim, düzeltme, sildirme, yok etme, üçüncü kişilere aktarılmasını engelleme gibi haklarını da kullanması söz konusu olamayacaktır.²¹⁵

İlgilin verilerine erişim hakkı, birçok metinde kabul edilmiş olup, özellikle 95/46/AT sayılı Avrupa Birliği Yönergesi'ndeki düzenleme en kapsamlı olanıdır.²¹⁶ Bunun dışında 108 sayılı Avrupa Konseyi Sözleşmesi,²¹⁷ OECD Rehber İlkeleri²¹⁸ ve BM Rehber İlkeleri'nde²¹⁹ bu yönde düzenlemeler bulunmaktadır. AİHM de kararlarında ilgili kişinin verilerine erişim hakkının AİHS'nin 8. maddesi kapsamında korunduğunu belirtmiştir.²²⁰

²¹³ a.g.e, s. 12.

²¹⁴ OECD Rehber İlkelerinin 13. Paragrafında, ilgili kişinin verilerin işlenmesi sürecine katılımına yönelik ilkeler topluca düzenlenmiştir. Bununla birlikte diğer metinlerde ilgili kişinin haklarının tek bir madde de toplanmayıp çeşitli maddelerde yer aldığı görülmektedir. Bygrave, Data Protection Law, s.63.

²¹⁵ Şimşek, Anayasa Hukukunda Kişisel Verilerin Korunması, s.90.

²¹⁶ Bygrave, Data Protection Law, s.65.

²¹⁷ 108 sayılı Avrupa Konseyi Sözleşmesi m.8.

²¹⁸ OECD Rehber İlkeleri par. 13.

²¹⁹ BM Rehber İlkeleri 4. ilke.

²²⁰ AİHM'nin ilgili kişinin verilere erişim hakkı kapsamında verdiği bir karar Leander

95/46/AT sayılı Avrupa Birliği Yönergesi'nin 12. maddesi, ilgili kişiye, veri sorumlusundan kendisine bazı bilgileri vermesini isteme yetkisi vermektedir. Burada yer alan düzenlemede, ilgili kişiye, kendisine ilişkin verilere ulaşma hakkı yanında, gereksiz masraf ve gecikme olmaksızın, verilerin nasıl kullanıldığı, işleme araçları, verinin kaynağı ve alıcıları gibi başka bilgilere ulaşma hakkı da verilmiştir.²²¹

95/46/AT sayılı Avrupa Birliği Yönergesi'nin 12/b hükmü gereğince ilgili kişi veri sorumlusundan, Yönerge'nin hükümlerine aykırı şekilde işlenen kişisel verisi varsa, özellikle kişisel verilerin eksik veya doğru olmaması durumlarında, bu kişisel verilerin silinmesi, düzeltilmesi veya erişime engellenmesini isteyebilir.²²²

İlgili kişinin itiraz hakkı 95/46/AT sayılı Avrupa Birliği Yönergesi'nin 14. maddesinde düzenlenmiş olup, buna göre, ilgili kişi, genel olarak verilerin işlenmesine veya doğrudan pazarlanmasına itiraz edebilir.²²³

- İsveç davasında verdiği karardır. Mahkeme, kararında, başvuranın kendisiyle ilgili güvenlik kayıtlarına ulaşmasına, ulusal güvenlik gerekçesiyle izin verilmesinin Sözleşme'nin 8. maddesi kapsamında özel hayata müdahale oluşturduğunu belirtmiştir. Leander - İsveç davası (Başvuru Numarası: 9248/81) Karar Tarihi: 26 Mart 1987, Kararın İngilizce metni için bakınız. (Çevrimiçi) [http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-57519#{"itemid":\["001-57519"\]}](http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-57519#{) (Erişim tarihi: 12 Mart 2016).

²²¹ Küzeci, s.215; Bainbridge, s. 109. Yönerge'nin düzenleniş şekliyle ilgilinin verilere erişim hakkı, uygulamada bazı sorunları barındırmaya meyilli görünmektedir. Bunlardan bazıları, verilere erişim ile ilgili istenen ücretin hangi koşullarda makul sayılacağı, verilerin birden çok kişiyle ilgili olduğu durumlarda verilerin ilgili kişilere nasıl verileceği, hangi bilgilerin çıkartılacağı gibi durumlardır. Ayrıca, Yönerge'de kişisel verilerin ilgili kişiye anlaşılır bir biçimde verilmesi gerektiği düzenlendiğinden, özellikle elektronik işlemlerde ilgili kişinin teknik bilgiden yoksun olduğu durumlarda, veriler ilgili kişiye basit bir biçimde verilmelidir. Bu bilgiler verilirken üzerinde durulması gereken bir başka konu ise, ticari sır ve fikri mülkiyet hukuku ile ilgili düzenlemelerinde göz önünde bulundurulması gerekliliğidir. 95/46/AT sayılı Avrupa Birliği Yönergesi'nin 41 numaralı Gerekçesi; Kuşkonmaz, s.98.

²²² Dağ, s. 122. İlgili kişinin verilerinin düzeltilmesini isteyebilmesi için ilk olarak kendisi ile ilgili eksik veya yanlış bir verinin tutulduğunu bilmesi gerektiğinden, bu hak, veri sorumlusunun verilerin işlenmesi sırasında ilgili kişinin bilgilendirilmesi yükümlülüğü ve ilgili kişinin kişisel verilere erişim hakkı ile yakından ilgilidir. Küzeci, s.216. Bunun dışında ilgili kişinin verilerini düzeltme hakkı, verilerin doğru ve güncel tutulması ilkesi ile de yakından ilişkilidir. Şimşek, Anayasa Hukukunda Kişisel Verilerin Korunması, s.92.

²²³ Sevimli, s. 163; Dağ, s. 122. Yönerge'nin 14/a maddesi gereğince belirli durumların bulunması halinde ilgili kişi kişisel verilerinin işlenmesine itiraz edebilir. Bu durumlar: Yönerge'nin 7/e fıkrasında düzenlenen, kişisel verilerin işlenme-

95/46/AT sayılı Avrupa Birliği Yönergesi'nin 15. maddesinde, kişinin bireysel özerkliği ile yakından ilişkili olan ilgili kişinin otomatik kararların konusu olmama hakkı düzenlenmiştir.²²⁴ Bir başka deyişle burada kişiye, kendisiyle ilgili otomatikleştirilmiş, insan müdahalesinin bulunmadığı kararların²²⁵ konusu olmama seçeneği verilmektedir.

Bu düzenleme ile kişilerin karakterlerinin tamamen otomatik yollardan değerlendirilmesinin, onların çıkarlarını önemli derecede etkileyecek kararların temelini oluşturmaması amaçlanmaktadır. Bundan dolayı şirketler, kişileri önemli derecede etkileyecek kararların en son

sinin kamu yararı için yapılan bir faaliyetin veya veri sorumlusu veya verinin açıklandığı üçüncü tarafın kamu yetkisini kullanarak yaptığı bir faaliyetin yerine getirilmesi için gerekli olması durumu ve Yönerge'nin 7/f fıkrasında düzenlenen, kişisel verilerin işlenmesinin, Yönerge tarafından ilgili kişiye tanınan haklar ağır bastığı durumlar hariç olmak üzere, veri sorumlusu veya verilerin açıklandığı üçüncü tarafın meşru çıkarları için gerekli olması durumudur. Yönerge'nin 14/b hükmünde ise, kişisel verilerin, veri sorumlusu veya üçüncü kişiler tarafından doğrudan pazarlama amacıyla işlendiği durumlarda, ilgili kişinin herhangi bir ücrete tabi olmadan verilerinin işlenmesine itiraz edebileceği düzenlenmiştir. Ayrıca ilgili kişinin bu hakkı konusunda bilgilendirilmesi gerektiği de Yönerge'de yer almaktadır. Yönerge'de doğrudan pazarlamanın tanımı yapılmamıştır. Küzeci, s.219.

²²⁴ Yönerge'nin 15/1 hükmü, kişilere, işindeki performansı, kredibilitesi, güvenilirliği, davranışları gibi kişiyle ilgili çeşitli kişisel özellikleri değerlendirmek amacıyla kişisel verilerinin otomatik olarak işlenmesi sonucunda elde edilen, bireyi önemli derecede etkileyerek, hukuksal sonuçlar doğuran kararların konusu olmama hakkı vermektedir. Madde hükmünde sayılan durumlar sınırlı sayıda değildir. Başalp, Kişisel Verilerin Korunması ve Saklanması, s. 54. 1978 tarihli eski Fransız Veri Koruma Kanunu'nda da yer alan bu düzenleme, üye ülkeler tarafından kabul edilmesine rağmen, uygulamasına nadiren rastlanmaktadır. Küzeci, s.219; Dağ, s. 122, 123.

²²⁵ Örneğin iş başvurusunda bulunan kişilere tamamen bilgisayar yardımıyla uygulanan psikolojik testler sonucu verilen işe alıp almama kararları bu tip kararlardandır. Başalp, Kişisel Verilerin Korunması ve Saklanması, s. 54. Yönerge'de bu hakkın iki istisnası da düzenlenmiştir. Yönerge'nin 15/2-a maddesine göre, eğer otomatikleştirilmiş karar, ilgili kişinin kendi görüşünü uygulamasına imkân veren koşulların yaratılması gibi tatmin edici veya uygun önlemler alındıktan sonra ilgili kişinin kendi isteğiyle bir sözleşmenin tarafı olması veya mevcut bir sözleşmenin hükümlerinin yerine getirilmesi için alınıyorsa, bu durumda karar ilgili kişi için kabul edilebilir olacaktır. Yine Yönerge'nin 15/2-b maddesine göre, bu kararın alınmasına, ilgili kişinin meşru çıkarlarını korumak için tedbirler öngören bir kanun hükmü izin veriyorsa, bu durumda da karar kabul edilebilir. Burada dikkat edilmesi gereken bir nokta Yönerge'de belirtilen "tatmin edici önlemler" ve "ilgili kişinin meşru çıkarı" kavramlarının belirsizliğidir., Frederico Ferretti, The Law and Consumer Credit Information in the European Community, The Regulation of Credit Information Systems, Routledge-Cavendish, ABD-Kanada 2008, s.174'ten aktaran Küzeci, s.220.

aşamasının bir insan tarafından verilmesi için gerekli tedbirleri almalarıdır.²²⁶

C. Veri Güvenliğine İlişkin Yükümlülükler

Veri sorumlusunun kişisel verilerin güvenliklerine ilişkin yükümlülükleri Kişisel Verilerin Korunması Kanunu'nun 12. maddesinde düzenlenmiştir. Maddeye göre veri sorumlusu, kişisel verilerin hukuka aykırı olarak işlenmesini ve verilere hukuka aykırı olarak erişilmesini önlemek, ayrıca verilerin muhafazasını sağlamak için uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almakla yükümlüdür.²²⁷

Maddenin ikinci fıkrasında, veri sorumlusunun, kişisel verilerin kendi adına başka bir gerçek veya tüzel kişi tarafından işlenmesi durumunda, maddenin ilk fıkrasındaki tedbirlerin alınmasından bu kişilerle birlikte müştereken sorumlu olacağı düzenlenmektedir.²²⁸ Maddenin üçüncü fıkrasında, veri sorumlusunun kendi kurum veya kuruluşunda, Kişisel Verilerin Korunması Kanunu'nun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapmak ve yaptırmak zorunda olduğu düzenlenmiştir.

Dördüncü fıkra, veri sorumluları ile veri işleyenlerin sır saklama yükümlülüğünü düzenlemekte olup, buna göre, veri sorumluları ile veri işleyenler, öğrendikleri kişisel verileri, Kanuna aykırı olarak başkalarına açıklayamaz veya şahsi çıkarları için kullanamazlar. Bu yükümlülük veri sorumluları ile veri işleyenler görevlerinden ayrılırlar bile devam eder.²²⁹

²²⁶ Kuner, European Data Privacy Law, s.65.

²²⁷ Adalet Komisyonu Raporunda bulunan muhalefet gerekçesinde belirtildiği gibi, söz konusu yükümlülük, Borçlar Kanunu'nun 65. ve 71. maddeleri arasında düzenlenen "kusursuz sorumluluk" müessesine benzer olup, bu bağlamda, Borçlar Kanununun adaç çalıştırmanın, çalışanını seçerken, işiyle ilgili talimat verirken, gözetim ve denetimde bulunurken, zararın doğmasını engellemek için gerekli özeni gösterdiğini ispat etmesi halinde sorumluluktan kurtulacağını düzenleyen 66. maddesinin 2. fıkrasına benzer bir düzenlemenin yapılması uygun olabilirdi. Komisyon Raporu, s. 35.

²²⁸ Gerekeceği verilen örneğe göre, bir şirket sahibi veri sorumlusu, şirketinin muhasebe kayıtlarının tutulması için bir muhasebe şirketi ile çalışıyorsa, bu durumda şirket sahibi ve muhasebe şirketi kişisel verilerin işlenmesiyle ilgili maddenin ilk fıkrasındaki tedbirlerin alınmasından sorumludur. Komisyon Raporu, s. 12.

²²⁹ a.g.e, s. 12.

Kanun'un 12. maddesinin beşinci fıkrasında, işlenen verilerin kanuni olmayan yollarla başkaları tarafından ele geçirilmesi halinde, veri sorumlusunun bu durumu en kısa sürede²³⁰ ilgisine ve Kurula bildireceği düzenlenmektedir. Kurul, gerekmesi halinde bu durumu, kendi internet sitesinde veya uygun göreceği bir başka yolla ilan edecektir.²³¹

Veri güvenliğinde kişilerin değil doğrudan verilerin güvenliği amaçlanmıştır. Veri güvenliğinin sağlanması için alınan tedbirler ile verilerin ilişkili olduğu kişilerde korunuyorsa verilerin korunması da sağlanabilir.²³² Bu nedenle kişisel verilerin korunmasına ilişkin birçok hukuksal düzenlemede veri güvenliği temel ilkeler arasında yer almaktadır. Kişisel verilerin korunması kavramının veri güvenliğini kapsadığını söylemek yanlış olmayacaktır. Kişisel verilerin korunması için veri güvenliğinin de sağlanması gerekmektedir.²³³

Verilerin güvenliği ilkesi, OECD Rehber İlkeleri²³⁴ ve 95/46/AT sayılı Avrupa Birliği Yönergesi'nde²³⁵ gelişmelere açık şekilde düzenlenmiştir. 108 sayılı Avrupa Konseyi Sözleşmesi'nde de²³⁶ verilerin korunması için uygun güvenlik tedbirlerinin alınması gerektiği belirtilmiştir.²³⁷

²³⁰ Avrupa Birliği Kişisel Verilerin Korunması Yönetmelik Taslağı'nın 31. maddesinin 1. fıkrasında kişisel verilerin işlenmesine ilişkin ihlallerde bildirim süresi 24 saat olarak öngörülmüştür. Komisyon Raporu, s. 35.

²³¹ Komisyon Raporu, s. 12.

²³² a.g.e, s.13

²³³ Ersoy, Kişisel Verilerin Korunması, s. 23. Bilişim teknolojisi kullanılarak kişisel verilere yapılan saldırılar amaçları açısından iki grupta toplanabilir. Birinci grupta, kişisel verilerin ele geçirilerek elektronik ortamda yapılan bankacılık, e-ticaret gibi alanlarda başkasının adına sahte işlemler yapılması, ikinci grupta ise, bu yasadışı işlemlerin yanı sıra kişisel verilerin kişilerin izni olmadan çeşitli ortamlarda açıklanmasıdır. Birinci gruba giren saldırılar daha çok veri güvenliği ile ilgili olup, ikinci gruptaki saldırılar ise kişisel verilerin korunması ile ilgilidir. Ersoy, Kişisel Verilerin Korunması, s. 25.

²³⁴ OECD Rehber İlkeleri, madde 11.

²³⁵ 95/46/AT sayılı Avrupa Birliği Yönergesi madde 17. Yönerge'de kişisel verilerin tesadüfen veya hukuka aykırı olarak yok edilmesine, yetkisiz şekilde elde edilmesine veya el değiştirilmesine, hukuka aykırı olarak devredilmesine veya ağda aktarılmasına veya hukuka aykırı olarak her türlü işleme faaliyetine karşı veri sorumlusu tarafından gerekli önlemlerin alınacağı düzenlenmiştir. Şimşek, Anayasa Hukukunda Kişisel Verilerin Korunması, s.96.

²³⁶ 108 sayılı Avrupa Konseyi Sözleşmesi madde 7.Sözleşme'de otomatik olarak kaydedilen kişisel verilerin kazaen veya izinsiz olarak imhası, kaybolması, yetkisiz kişiler tarafından elde edilmesi, değiştirilmesi ya da izinsiz olarak yayınlanmasına karşı uygun güvenlik tedbirlerinin alınması gerektiği belirtilmiştir. Şimşek, Anayasa Hukukunda Kişisel Verilerin Korunması, s.96.

²³⁷ Şimşek, Anayasa Hukukunda Kişisel Verilerin Korunması, s.96. Kişisel verilerin

Yönerge'ye göre, belirtilen önlemler, hem ilgili sistemin kurulma aşamasında, hem de verilerin işleme aşamasında alınmalıdır.²³⁸ Bunun yanında, uygun önlemler tespit edilirken, teknolojinin ulaştığı düzey,²³⁹ korunacak kişisel verilerin niteliği, mevcut ihlal tehlikesi ve maliyet göz önünde bulundurulmalıdır.²⁴⁰ Ayrıca, veri sorumlusu, kişisel verilerin işlenmesinde çalışan kişilerin kişisel verilere zarar verebilecek muhtemel eylemlerine karşı, teknik ve örgütsel güvenlik bağlamında gerekli önlemleri almakla ve bunları belgelemekle sorumludur.²⁴¹

Veri güvenliğinin yeterli düzeyde sağlanamaması, kişiler ve kurumlar üzerinde ekonomik, siyasal, sosyal ve fiziksel zararlara sebep olabilir.²⁴² Bu zararlardan korunmak için, veri güvenliği hem ilgili kişiler, hem de veri sorumluları tarafından sağlanması gerekir. Verileri toplayan ve işleyen sistemlerin korunması yanında, bireyler de kendilerini korumalıdır. Kişisel verilere yetkisiz erişim ve benzeri müdahaleler birçok ülkede suç olarak tanımlanmış ve bu eylemleri gerçekleştiren-

kazara ortadan kaldırılması, yetkisiz erişim, değiştirilme, silinme ve yayınlanmalarını engelleyecek önlemlerin veri sorumluları tarafından alınmasını gerektiren veri güvenliği ilkesi, kişisel verilerin korunması hukukunun ayrılmaz bir parçasıdır. Bu ilkeye göre, verilerin tutulduğu süre zarfında veri sorumlusu tarafından güvenlikleri sağlanmalıdır. Aksi durumda, ilgili kişinin ekonomik, sosyal vb. zararlara uğraması söz konusu olabilir. Bundan kaçınmak için, verilere yönelik her türlü tehlikeye karşı gereken her türlü idari ve teknik tedbirler alınmalıdır. Örneğin elektronik ortamda tutulan kişisel veriler kazara kaybolmalara, değiştirilmelere karşı yedeklenmeli, saldırılara karşı verilerin tutulduğu sistemlere güvenlik duvarları örülmelidir. Kuşkonmaz, s. 116. Bunun dışında, telefonla veya online bankacılık hizmetlerinde veri güvenliğinin sağlanması önemlidir. Alınacak teknik güvenlik tedbirleri ile hem bankaya hem de müşterilere karşı yapılacak müdahalelere karşı önlemler alınmalıdır. Küzeci, s.245.

²³⁸ 95/46/AT sayılı Avrupa Birliği Yönergesi başlangıç kısmı, 46. paragraf.

²³⁹ Teknolojik gelişmelerle birlikte veri güvenliğini sağlayan yöntemler ve müdahale yöntemleri ile zamanlı olarak gelişmektedir. Bu nedenle, verilerin etkili güvenliğinin sağlanabilmesi için alınan teknik önlemlerin sürekli güncellenmesi, yenilenmesi bir zorunluluktur. Küzeci, s.244.

²⁴⁰ 95/46/AT sayılı Avrupa Birliği m.17/1, 2. cümle.

²⁴¹ 95/46/AT sayılı Avrupa Birliği Yönergesi m. 17/2. Kişisel verileri işleyenlerin de verilere karşı haksız müdahalelerde bulunabilecekleri göz ardı edilmemelidir. Verileri işleyenlerin mümkün olduğu kadar en az miktarda veriye ulaşması sağlanmalı ve bu kişilerin etkinlikleri uygun araçlarla kontrol edilmelidir. Küzeci, s.244.

²⁴² Cambridge Üniversitesi'nde çalışanların adres bilgilerinin sızması sonucunda, evleri hayvan hakları savunucularınca hedef alınmıştır. İngiltere'de kredi kartı bilgilerinin basına sızması sonucunda, politikacıların alkol tüketimlerine ilişkin kişilik haklarına zarar verici bilgiler yayınlanmıştır. Dilemmas of Privacy and Surveillance, Challenges of Technological Change, The Royal Academy of Engineering, Mart 2007, s.22'den aktaran Küzeci, s. 245.

lere karşı yaptırımlar düzenlenmiş olsa da, bu suç oluşmadan, kişisel verilerin veri güvenliği ilkesini benimsemiş kurumlar ve kişiler tarafından korunmasının daha etkili bir yöntem olduğu unutulmamalıdır.

D. Veri Sorumlusuna Başvuru

Kişisel Verilerin Korunması Kanunu'nun 13. maddesi ilgili kişinin veri sorumlusuna başvuru yolunu düzenlemektedir.²⁴³ Maddeye göre, ilgili kişiler, Kanunun uygulanması ile ilgili taleplerini öncelikle veri sorumlusuna iletmek zorundadırlar. İlgili kişiler bu iletimi yazılı veya uygulamada oluşacak ihtiyaca göre Kurulun belirleyeceği diğer yöntemlerle yapabilirler.²⁴⁴ İlgili kişinin bu talebini alan veri sorumlusu, ücretsiz veya işlemin bir maliyeti gerektirmesi halinde Kurul tarafından belirlenen tarifeye göre ücret almayı müteakip, en kısa sürede veya en geç otuz gün içinde talebi incelemesi, kabul veya gerekçesini açıklayarak reddetmesi ve cevabını ilgili kişiye yazılı veya elektronik ortamda bildirmesi gerekmektedir.²⁴⁵

Maddenin en son fıkrasına göre, veri sorumlusunun talebi kabul etmesi halinde, gereğini yerine getirmesi gerekmektedir. İlgili kişinin başvurusunun nedeni veri sorumlusunun hatası ise, veri sorumlusu başvuru için aldığı ücreti ilgili kişiye iade etmek zorundadır.

E. Kurula Şikâyet

Kişisel Verilerin Korunması Kanununun 14. maddesi, ilgili kişi tarafından Kişisel Verileri Koruma Kuruluna **şikâyet** yolunu **düzen-**

²⁴³ İlgili kişilerin veri sorumlusuna başvurması çeşitli uluslararası belgelerde de düzenlenmiştir. APEC Çerçeve Belgesine göre, ilgili kişiler, veri sorumlusundan: kendisi hakkında veri tutulup tutulmadığının bildirilmesi; kimliği hakkında yeterli kanıt sağladıktan sonra, kendisi hakkındaki verilerin, makul bir zamanda, makul bir ücretle, uygun bir yöntemle, anlaşılabilir bir biçimde kendisine ulaştırılması; kendisi ile ilgili tutulan verinin doğruluğuna itiraz etme, eğer mümkün ve uygunsa, düzeltilmesi, tamamlanması, değiştirilmesi veya silinmesini isteyebilir. APEC Çerçeve Belgesi 23. madde.

²⁴⁴ Komisyon Raporu, s. 12

²⁴⁵ Gerekçede, madde metninde "bildirmesi" kavramının kullanılmasının sebebi olarak, veri sorumlusunun gerçek kişi veya özel hukuk tüzel kişisel olabileceği ve bundan dolayı 7201 sayılı Tebligat Kanunu hükümlerine tabi olmayabileceği olarak verilmiştir. Gerekçeye göre bu bildirim, bir ispat sorunu olup gerektiğinde yargı mercilerince ele alınacaktır. Bu kapsamda 7201 sayılı Tebligat Kanununa tabi kuruluşlar da Kişisel Verilerin Korunması Kanunu uyarınca yapacakları bildirimleri resmi tebligat yoluyla da yapabilirler. Komisyon Raporu, s. 13.

lenmektedir. Buna göre, ilgili kişinin, Kanununun 13. maddesi uyarınca veri sorumlusuna yapmış olduğu başvurunun reddedilmesi, verilen cevabın yetersiz bulunması veya süresinde başvuruya cevap verilmesi hallerinde ilgili kişi veri sorumlusunun cevabını öğrendiği tarihten itibaren otuz ve her halde başvuru tarihinden itibaren altmış gün içinde Kişisel Verileri Koruma Kuruluna **şikâyette** bulunabilir.

Maddenin ikinci fıkrasında, Kanun'un 13. maddesinde düzenlenen başvuru müessesesinin, zorunlu bir başvuru yolu olduğu ve bu yol tüketilmeden **şikâyet** edilemeyeceği düzenlenmiştir. Bu düzenleme ile uyuşmazlıkların ilk olarak veri sorumlusu ile ilgili kişi arasında halledilmesi ve bu suretle Kişisel Verileri Koruma Kurulunun yoğun bir iş yükü altında kalmaması amaçlanmaktadır.²⁴⁶ Maddenin üçüncü fıkrasında, kişilik hakları ihlal edilenlerin, genel hükümlere göre tazminat hakkı saklı tutulmaktadır. Veri sorumlusunun hukuki statüsüne göre ilgili kişiler adli ya da idari yargıda tazminat istemli dava açabileceklerdir.

F. Şikâyet Üzerine veya Resen İncelemenin Usul ve Esasları

Kanun'un 15. maddesiyle, Kişisel Verileri Koruma Kurulu tarafından yapılan incelemenin usul ve esasları düzenlenmektedir. Kişisel Verileri Koruma Kurulu, **şikâyet** üzerine veya ihlal iddiasını öğrenmesi halinde resen, görev alanına giren konularda gerekli incelemeyi yapabilecektir. Kurul, **şikâyet** veya resen öğrenilen **şikâyet** konusuna bağlı olup, resen genel inceleme yetki ve görevi bulunmamaktadır.²⁴⁷ Veri sorumluları, Devlet sırrı niteliğindeki bilgi ve belgeler hariç, Kurul tarafından istenen bilgi ve belgeleri, on beş gün içinde Kurula göndermek veya gerektiğinde yerinde inceleme yapılmasına imkân sağlamak zorundadırlar.

Kanunda, ilgili kişinin yaptığı **şikâyet** üzerine Kurulun yapacağı inceleme sonunda cevap vermesi öngörülmekte olup, **şikâyet** tarihin-

²⁴⁶ Gereğede belirtildiği gibi, veri sorumlusuna başvurunun zorunlu, şikâyetin ise ihtiyari olması sebebiyle, başvurusu zimnen veya açıkça reddedilen ilgili kişi aynı anda hem Kişisel Verileri Koruma Kuruluna şikâyette bulunabilecek, hem de adli veya idari yargıya başvurabilecektir. Tasarı, s. 25.

²⁴⁷ Gereğede belirtildiği gibi Dilekçe Hakkının Kullanılmasına Dair Kanununun 6. maddesinde belirtilen şartları taşımayan ihbar ve şikâyetler incelemeye alınmayacaktır. Tasarı, s. 25.

den altmış gün içinde cevap verilmezse talep reddedilmiş sayılacaktır. Bunun üzerine ilgili kişinin idari yargıda dava açma süresi başlamaktadır. Kurul tarafından resen yapılacak incelemeler için Kanunda herhangi bir süre bulunmamaktadır.

Kişisel Verileri Koruma Kurulu, **şikâyet** üzerine veya resen yapılacak inceleme sonucunda, Kişisel Verilerin Korunması Kanunu hükümlerinin ihlal edildiği kanaatine varırsa, tespit ettiği hukuka aykırılıkların ilgili veri sorumlusu tarafından giderilmesine karar verir ve bu kararını ilgililere tebliğ eder. Kanuna göre, bu karar, tebliğden itibaren gecikmeksizin ve en geç otuz gün içinde yerine getirilecektir.

Kurul tarafından, **şikâyet** üzerine veya resen yapılan inceleme sonucunda, Kişisel Verilerin Korunması Kanununa aykırı olan uygulamanın yaygın olduğu tespit edilirse, Kurul, bu konuda ilgili kurum ve kuruluşların görüşünü de alarak ilke kararı alır ve kararı yayımlar.

Kurul, telafisi güç veya imkânsız zararların doğması ve açıkça hukuka aykırılık şartlarının birlikte gerçekleşmesi halinde, nihai karardan önce veri işlenmesinin veya verinin yurtdışına aktarılmasının durdurulmasına karar verebilir. **İlgililer Kurulun kararlarına karşı idare mahkemelerinde dava açabilirler.**

G. Veri Sorumluları Sicili

Kişisel Verilerin Korunması Kanunu'nun 16. maddesiyle, veri sorumlularının kaydedileceği Veri Sorumluları Sicili düzenlenmektedir. Maddeyle, veri sorumlularının kaydedilmesi amacıyla Kişisel Verileri Koruma Kurulunun gözetiminde Başkanlık tarafından kamuya açık olarak tutulan Veri Sorumluları Sicili düzenlenmektedir. Veri sorumluları veri işlemeye başlamadan önce Kişisel Verileri Koruma Kuruluna başvurarak Veri Sorumluları Siciline kaydolacaklardır.²⁴⁸ Kişisel Verileri Koruma Kurulu tarafından belirlenecek objektif kriterlere göre, Kurul tarafından, işlenen verinin niteliği, sayısı, veri işlemenin kanundan kaynaklanması

²⁴⁸ Komisyon Raporunda yer alan mühalefet gerekçesine göre, maddede öngörülen sistem, Avrupa Komisyonu'nun veri siciline ilişkin yeni yaklaşımının aksi yönündedir. Buna göre temel prensip, bildirim usulüne tabi ön inceleme ve kontrol mekanizmalarının oluşturulması değil, herhangi bir bildirimde bulunmaksızın serbest faaliyette bulunan veri sorumlularının sonradan denetimlerinin sağlanmasına yönelik mekanizmaların tasarlanmasıdır. Komisyon Raporu, s. 36.

veya üçüncü kişilere aktarılma durumu gibi hususlarda Veri Sorumluları Siciline kayıt zorunluluğuna istisnalar getirilebilecektir.

Maddenin üçüncü fıkrasında Veri Sorumluları Siciline kayıt başvurusunda bildirilmesi gereken hususlar düzenlenmektedir. Bu kapsamda, gerekçede de belirtildiği gibi, örneğin veri sorumlusu ve varsa temsilcisinin kimlik ve adres bilgileri, kişisel verilerin hangi amaçla işleneceği, kişisel verilerin aktarılacağı alıcı veya alıcı grupları, veri güvenliğine ilişkin alınan tedbirler, kişisel verilerin işlendikleri amaç için gerekli olan azami süre gibi hususlar Veri Sorumluları Siciline kayıt başvurusunda bildirilmelidir. Ayrıca, üçüncü fıkra uyarınca bildirilmesi gerekli bilgilerde meydana gelen değişiklikler de derhal Başkanlığa bildirilecektir. Veri Sorumluları Siciline ilişkin diğer hususlar yönetmelikle düzenlenecektir.²⁴⁹

VI. SUÇLAR VE KABAHAHLER

A. Suçlar

Kişisel Verilerin Korunması Kanunu'nun 17. maddesinde, kişisel verilere ilişkin suçlar ve cezai yaptırımlar için 5237 sayılı Türk Ceza Kanunu'nun ilgili hükümlerine atıf yapılmaktadır. Maddenin ikinci fıkrasında, kişisel verileri silmeyen veya anonim hale getirmeyenlerin ise Türk Ceza Kanunu'nun 138. maddesi hükmü uyarınca cezalandırılmaları gerektiği düzenlenmiştir.

Kişisel Verilerin Korunması Kanunu'nun 30. maddesinin ikinci fıkrasıyla 5237 sayılı Türk Ceza Kanunu'nun 135. maddesinin ikinci fıkrasında yer alan "Kişilerin" ibaresi "Kişisel verinin, kişilerin" şeklinde; "bilgileri kişisel veri olarak kaydeden kimse, yukarıdaki fıkra hükmüne göre cezalandırılır" ibaresi "olması durumunda birinci fıkraya uyarınca verilecek ceza yarı oranında artırılır" şeklinde değiştirilmiştir. Böylece fıkra metni "*Kişisel verinin, kişinin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin olması durumunda birinci fıkra uyarınca verilecek ceza yarı oranında artırılır*" haline almıştır. Böylece Türk Ceza Kanunu'nda sayılan bu özel nitelikli ve-

²⁴⁹ Komisyon Raporu, s. 14.

rilerin kaydedilmesi durumunda ceza arttırılacağından bu fıkra suçun nitelikli hali olmuştur.

TCK “özel hayatı” ve “hayatın gizli alanını” korumaktadır. Kişinin kendisine ait bilgiler özel hayata ve hayatın gizli alanına dâhildir. Kişilere ait bilgilere karşı eylemlerde bulunanları Ceza Hukuku vasıtasıyla cezalandırmak amacıyla, 5237 sayılı Türk Ceza Kanunu’nda kişisel verilere karşı suçlar ihdas edilmiştir. Kanun’un “Kişilere Karşı Suçlar” başlıklı ikinci kısmının “Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar” başlıklı dokuzuncu bölümünde, 135. maddede “kişisel verilerin kaydedilmesi”, 136. maddesinde “verileri hukuka aykırı olarak verme veya ele geçirme” ve 138. maddede “verileri yok etmeme” suçları düzenlenmiş, 137. maddede ise cezanın arttırılmasını gerektiren nitelikli haller sayılmıştır.²⁵⁰ Kişisel Verilerin Korunması Kanunu kişisel verilerin işlenmesinin hukuka uygunluk hallerini düzenleyerek, Türk Ceza Kanunu’ndaki kişisel verilere karşı suçların içeriğinin belirlenmesini, hangi fiillerin suç teşkil ettiğine dair uygulamadaki ciddi tereddütlerin giderilmesini sağlamıştır.

TCK’da nelerin kişisel veriler olduğuna dair açık bir düzenleme bulunmamakta olup, kişisel verilerin kaydedilmesi suçunu düzenleyen TCK 135. maddesinin gerekçesinde, suçun konusunun kişisel veriler olduğundan bahsedilerek, gerçek kişilerle ilgili her türlü bilginin kişisel veri olarak kabul edilmesi gerektiği belirtilmiştir.²⁵¹ Kişisel Verilerin Korunması Kanunu’nun yürürlüğe girmesinden önce, doktrininde Türk Ceza Kanunu metninde kişisel verinin tanımının yapılmamış olması birçok yönden eleştirilmiştir. Kişisel verinin tanımı yapılmayarak kapsamının geniş tutulmasının ceza hukukunun belirlilik ilkesine aykırı düştüğü belirtilmiştir.²⁵² Aynı düşüncede olan yazarlara göre, o dönemde kişisel veriyi tanımlayan bir kanun bulunmaması nedeniyle, bu durum aynı zamanda kanunilik ilkesini de ihlal etmekteydi.²⁵³ Kişisel Verilerin Korunması Kanunu’nun 3. maddesinde kişisel verinin tanımının yapılmış olması bu konudaki birçok sorunu **çözmüştür**.

²⁵⁰ Özen - Baştürk, s.122; Ketizmen, s. 230-242; Topaloğlu, s.179,180.

²⁵¹ Özen - Baştürk, s. 123; Hafızoğulları - Özen, Ceza Özel, s. 267,268.

²⁵² Dülger, Bilişim Suçları, s. 271. Belirlilik ilkesinin amacı, ceza normunu uygulayan hâkimin suç ve cezanın öngörülebilirliğini engelleyici, hukuk yaratıcı ya da yorumlayıcı öznel davranış ve kararlarının önüne geçilmesidir.

²⁵³ Küzeci, s.286; Yaşar - Gökcan - Artuç, s. 4116.

B. Kabahatler

Kişisel Verilerin Korunması Kanunu'nun 18. maddesinde, Kanunda öngörülen yükümlülüklerle aykırı davranılması halinde uygulanacak idari yaptırımlar düzenlenmektedir. Madde kapsamında aydınlatma ve veri güvenliğini sağlama, Kurul kararlarını yerine getirme ve Sicile kayıt ve bildirim yükümlülüklerine aykırı davranılması kabahat olarak düzenlenmekte ve idari para cezası yaptırımına bağlanmaktadır. Kişisel Verileri Koruma Kurulu idari yaptırımlara karar verecek olup, yaptırım kararlarına karşı idari yargı yolu açıktır.²⁵⁴

Maddenin ikinci fıkrasında belirtildiği gibi, idari para cezaları veri sorumlusu olan gerçek kişiler ile özel hukuk tüzel kişiler hakkında uygulanacak olup, üçüncü fıkraya göre, kabahat olarak düzenlenen eylemlerin kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşları bünyesinde işlenmesi halinde, Kişisel Verileri Koruma Kurulunun yapacağı bildirim üzerine, ilgili kamu kurum ve kuruluşunda görev yapan memurlar ile diğer kamu görevlileri ile kamu kurumu niteliğindeki meslek kuruluşlarında görev yapanlar hakkında disiplin hükümlerine göre işlem yapılacaktır.²⁵⁵

VII. KİŞİSEL VERİLERİ KORUMA KURUMU VE TEŞKİLAT

A. Kişisel Verileri Koruma Kurumu

Kişisel Verilerin Korunması Kanunu'nun 19. maddesinde, Kanun'un verdiği görevleri yerine getirmek üzere kurulan, idari ve mali özerkliğe sahip, kamu tüzel kişiliğini haiz Kişisel Verileri Koruma Kurumunun kuruluşu düzenlenmektedir.²⁵⁶

²⁵⁴ Gerekçede, maddede yer alan kabahatler karşılığında öngörülen idari para cezalarının alt ve üst sınırları arasındaki makasın bilinçli olarak geniş tutulduğu belirtilmiş olup, Kişisel Verileri Koruma Kurulu karar verirken kabahatler hususunda genel kanun niteliğinde olan 5326 sayılı Kabahatler Kanununun 17. maddesinin ikinci fıkrasında belirtildiği gibi kabahatin haksızlık içeriği ile failin kusuru ve ekonomik durumunu dikkate alacaktır. Bu şekilde düzenleme yapılmak suretiyle, söz konusu kabahatlerin çok farklı ekonomik güce sahip gerçek veya tüzel kişiler hakkında uygulanacak olması nedeniyle yaptırım uygulamasında hakkaniyet sağlanmaya çalışılmıştır. Gerekçede verilen örneğe göre, küçük bir şehirde faaliyet gösteren bir aile şirketiyle ülke çapında faaliyet gösteren bir holdingin Kanun hükümlerini ihlal etmesi durumunda belirlenecek idari para cezalarının miktarı söz konusu şirketlerin ekonomik durumlarına göre farklı olacaktır. Tasarı, s. 26.

²⁵⁵ Her ne kadar Kanunda belirtilmemiş olsa da, gerekçede de belirtildiği gibi, Kişisel Verilerin Korunması Kanununda hüküm bulunmayan hallerde genel kanun niteliğindeki 5326 sayılı Kabahatler Kanunu hükümleri uygulanacaktır. Tasarı, s. 26.

²⁵⁶ Gerekçede de belirtildiği gibi, Avrupa Konseyinin 108 sayılı Sözleşmesi ve Avru-

B. Kurumun Görevleri

Kanun'un 20. maddesiyle, Kişisel Verilerin Koruma Kurumunun görevleri belirlenmektedir. Maddeye göre, Kişisel Verilerin Korunması Kurumunun, başlıca ulusal ve uluslararası düzlemde uygulama ve mevzuattaki gelişmeleri takip ederek araştırma ve inceleme faaliyetlerinde bulunma ve ulusal ve uluslararası kurum ve kuruluşlarla işbirliği yapma ve ihtiyaç duyulan hususlarda önerilerde bulunma görevleri bulunmaktadır.

Kanuna göre Kurum, yıllık faaliyet raporunu Cumhurbaşkanlığına, Türkiye Büyük Millet Meclisi İnsan Haklarını İnceleme Komisyonuna ve Başbakanlığa sunmak ve Kanunlarla verilen diğer görevleri yerine getirmekle görevlidir.

C. Kişisel Verileri Koruma Kurulu

Kişisel Verilerin Korunması Kanunu'nun 21. maddesiyle, Kişisel Verileri Koruma Kurumunun karar organı olan Kişisel Verileri Koruma Kurulu düzenlenmektedir.²⁵⁷ Kanun'da, Kişisel Verileri Koruma Kurulunun, Kanunla ve diğer mevzuatla verilen görev ve yetkilerini kendi sorumluluğu altında, bağımsız olarak yerine getireceği ve kullanacağı, görev alanına giren konularla ilgili olarak hiçbir organ, makam, merci veya kişinin Kurula emir ve talimat veremeyeceği hüküm altına alınmıştır.

Maddenin ikinci fıkrasında, Kişisel Verileri Koruma Kurulunun dokuz üyeden oluştuğu, beş üyesi Türkiye Büyük Millet Meclisi, iki üyesi Cumhurbaşkanı, iki üyesinin Bakanlar Kurulu tarafından seçileceği düzenlenmiştir.

Maddenin üçüncü fıkrasında, Kurula üye olabilmek için gereken şartlar düzenlenmiştir. Dördüncü fıkrada, Kurul üyeliğine seçilecek-

pa Birliğinin 95/46/AT sayılı Yönergesi, kişisel verilerin işlenmesine ilişkin ilkelere uygulanmasını izlemek ve yönlendirmek üzere fonksiyonel olarak bağımsız bir şekilde görev yapacak otoritelerin oluşmasını düzenlemektedir. Avrupa Birliği üyesi tüm ülkelerde benzer şekilde kurulmuş bağımsız otoriteler bulunmaktadır. Kişisel Verileri Koruma Kurulu ve Başkanlıktan oluşan Kişisel Verileri Koruma Kurumu, Başbakanlıkla ilişkili olup, merkezi Ankara'dadır. Tasarı, s. 26.

²⁵⁷ Gerekçede, Kişisel Verileri Koruma Kurulunun, Avrupa Konseyinin 108 sayılı Sözleşmesi ve Avrupa Birliğinin 95/45/AT sayılı Yönergesine uygun şekilde bağımsız olarak kurulduğu belirtilmiştir. Tasarı, s. 27.

rin muvafakatlarının aranacağı, seçimde, Kurumun görev alanına giren konularda bilgi ve deneyimi bulunanların çoğulcu bir şekilde temsiline özen gösterileceği belirtilmiştir. Beşinci fıkrada Türkiye Büyük Millet Meclisi tarafından Kurula üye seçimi usulü düzenlenmiştir. Altıncı fıkrada ise Cumhurbaşkanı veya Bakanlar Kurulu tarafından Kurula seçim yapılması düzenlenmiştir. Yedinci fıkraya göre, Kurul, üyeleri arasından Başkan ve İkinci Başkan seçer. Sekizinci fıkraya göre, Kurul üyelerinin görev süresi dört yıl olup, süresi biten üye tekrar seçilebilir. Seçilen üyeler Yargıtay Birinci Başkanlık Kurulu huzurunda yemin ederler.²⁵⁸ Kanunda Kurul üyelerinin görevleri sebebiyle işledikleri suçlara ilişkin soruşturmaları 4483 sayılı Memurlar ve Diğer Kamu Görevlilerinin Yargılanması Hakkında Kanuna göre yapılır ve bunlar hakkında soruşturma izni Başbakan tarafından verilir. Madde- nin 11. fıkrasında sayılan durumlarda üyelerin Kurul kararıyla üyelikleri sona erer. Maddenin 12. fıkrasında Kurul üyeliklerine seçilenlerin Kurulda görev yaptıkları sürece önceki görevleri ile ilişkilerinin kesileceği, kamu görevlisi iken üyeliğe seçilenlerin, Kanunda belirtilen şartlarda tekrar kamu görevlisi olarak atanabileceği düzenlenmiştir.

D. Kurulun Görev ve Yetkileri

Kişisel Verileri Koruma Kanunu'nun 22. maddesinde, Kişisel Verileri Koruma Kurulunun görev ve yetkileri düzenlenmektedir.²⁵⁹

²⁵⁸ Kurul üyeleri özel bir kanuna dayanmadıkça, Kuruldaki resmi görevlerinin yürütülmesi dışında resmi veya özel hiçbir görev alamaz, dernek, vakıf, kooperatif ve benzeri yerlerde yöneticilik yapamaz, ticaretle uğraşamaz, serbest meslek faaliyetinde bulunamaz, hakemlik ve bilirkişilik yapamazlar. Ancak, Kurul üyeleri, asli görevlerini aksatmayacak şekilde bilimsel amaçlı yayın yapabilir, ders ve konferans verebilir ve bunlardan doğacak telif hakları ile ders ve konferans ücretlerini alabilirler.

²⁵⁹ Maddeye göre, Kişisel Verileri Koruma Kurulunun görevleri; kişisel verilerin, temel hak ve özgürlüklere uygun şekilde işlenmesinin sağlanması, kişisel verilerle ilgili haklarının ihlal edildiğini ileri sürenlerin şikayetlerinin karara bağlanması, şikayet üzerine veya Kurul tarafından ihlal iddiasının öğrenilmesi durumunda resen, görev alanına giren konularda kişisel verilerin kanunlara uygun olarak işlenip işlenmediğinin incelenmesi ve gerektiğinde bu konuda geçici önlemler alınması, özel nitelikli kişisel verilerin işlenmesi için aranan yeterli önlemlerin belirlenmesi, Veri Sorumluları Sicilinin tutulmasının sağlanması, Kurulun görev alanı ile Kurumun işleyişine ilişkin konularda gerekli düzenleyici işlemlerin yapılması, veri güvenliğine ilişkin yükümlülükleri belirlemek amacıyla düzenleyici işlemlerin yapılması, veri sorumlusunun ve temsilcisinin görev, yetki ve sorumluluklarına ilişkin düzenleyici işlemlerin yapılması, Kişisel Verilerin Korunması Kanu-

E. Kurulun Çalışma Esasları

Kanun'un 23. maddesinde Kişisel Verileri Koruma Kurulunun çalışma esasları düzenlenmektedir. Madde kapsamında, Kişisel Verileri Koruma Kurulunun toplantı ve karar yeter sayısı, Kurul üyelerinin kendilerini ve yakınlarını ilgilendiren konularda yasaklılıkları ve sır saklama yükümlülükleri düzenlenmektedir. Kurulun çalışma usul ve esasları ile kararların yazımı ve diğer hususlar yönetmelikle düzenlenecektir.

F. Başkan

Kişisel Verileri Koruma Kanunu'nun 24. maddesinde, Kişisel Verileri Koruma Kurumu Başkanının görevleri düzenlenmektedir. Maddede Kişisel Verileri Koruma Kurumu Başkanının görevleri olarak, Kurumu yönetmek ve temsil etmek, stratejik planın uygulanmasını sağlamak, Kurumun ve hizmet birimlerinin uyumlu, verimli, disiplinli ve düzenli bir biçimde çalışmasını temin etmek yanında, Kurul toplantılarının gündemini belirleyerek toplantılara başkanlık etmek ve Kurumun mali tabloları ile bütçesini hazırlamak başlıca görevleri arasındadır. Kurum Başkanına İkinci Başkan vekâlet edecektir.

G. Başkanlığın Oluşumu ve Görevleri

Kanunun 25. maddesinde Kişisel Verileri Koruma Kurumu Başkanlığının oluşumu ve görevleri düzenlenmektedir. Maddeye göre, Başkanlık, Kurumun ve Kurulun idari ve mali işleri ile sekreteryaya hizmetlerini yerine getirecektir. Başkanlık, Başkan Yardımcısı ve daire başkanlıkları şeklinde teşkilatlanmış hizmet birimlerinden oluşmaktadır. Maddeyle, Başkan Yardımcısı ve Daire Başkanlarının nitelikleri ve atanma usulü ile Başkanlığın görevleri ayrıntıları olarak düzenlenmektedir. Hizmet birimleri ile bu birimlerin çalışma usul ve esasları Bakanlar Kurulu kararı ile yürürlüğe konulan yönetmelikle düzenlenecektir.

nunda öngörülen idari yaptırımlara karar verilmesi, diğer kurum ve kuruluşlarca hazırlanan ve kişisel verilere ilişkin hüküm içeren mevzuat tasarıları hakkında görüş bildirilmesi, Kişisel Verileri Koruma Kurumunun stratejik planının karara bağlanması, amaç ve hedeflerinin, hizmet kalite standartlarının ve performans kriterlerinin belirlenmesi, Kurumun stratejik planı ile amaç ve hedeflerine uygun olarak hazırlanan bütçe teklifinin görüşülmesi ve karara bağlanması, Kurumun performansı, mali durumu, yıllık faaliyetleri ve ihtiyaç duyulan konular hakkında hazırlanan rapor tasarılarının onaylanması ve yayımlanması, taşınmaz alımı, satımı ve kiralanması konularındaki görüşlerin görüşülüp karara bağlanması ve kanunlarda verilen diğer görevlerin yerine getirilmesidir.

H. Kişisel Verileri Koruma Uzmanı ve Uzman Yardımcıları

Kanun'un 26. maddesinde Kişisel Verileri Koruma Uzmanı ve Uzman Yardımcıları ile ilgili esaslar düzenlenmektedir. Kişisel Verileri Koruma Kurumu görevlerinin daha etkin bir şekilde yerine getirilmesi için Kurumda Kişisel Verileri Koruma Uzmanı ve Kişisel Verileri Koruma Uzman Yardımcısı çalıştırılacak olup, maddeyle bu kadrolara atanmak için 657 sayılı Kanun'un ek 41. maddesine atıf yapılmaktadır.

I. Personele ve Özlük Haklarına İlişkin Hükümler

Kişisel Verileri Koruma Kanunu'nun 27. maddesinde, Kurul Başkan ve üyeleri ile Kurum personelinin mali ve sosyal hakları düzenlenmektedir. Maddede başka kurum ve kuruluşlarda çalışanlardan uzmanlığına ihtiyaç duyulanların Kurumda görevlendirilmesine ilişkin düzenleme hüküm altına alınmakta ve Kurumda istihdam edilecek personele ilişkin kadro unvan ve sayıları da belirlenmektedir.

VIII. İSTİSNALAR

Kişisel Verilerin Korunması Kanunu'nun 28. maddesinde Kanun kapsamı dışında tutulan hususlar düzenlenmektedir.

Maddenin birinci fıkrasında tamamen Kanun kapsamı dışında tutulan hususlar düzenlenmektedir. Maddenin düzenlemesine göre kişisel verilerin, üçüncü kişilere verilmemek ve veri güvenliğine ilişkin yükümlülüklerle uyulmak kaydıyla, gerçek kişiler tarafından kendisiyle veya aynı konutta yaşayan aile fertleriyle ilgili faaliyetleri kapsamında; resmi istatistik ile anonim hale getirilmek suretiyle araştırma, planlama ve istatistik gibi amaçlarla, milli savunmayı, milli güvenliği, kamu güvenliğini, kamu düzenini, ekonomik güvenliği, özel hayatın gizliliğini veya kişilik haklarını ihlal etmemek ya da suç teşkil etmemek kaydıyla, sanat, tarih, edebiyat veya bilimsel amaçlarla ya da ifade özgürlüğü kapsamında, milli savunmayı, milli güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbari faaliyetler kapsamında, soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi, Kanun'un tamamen kapsamı dışında tutulmuştur.

Maddenin ikinci fıkrasında, kısmen Kanun kapsamı dışında kalan hususlar düzenlenmiştir. Buna göre, kural olarak bu fıkrada sayılan haller kanun hükümlerine tabi olmakla birlikte, sadece fıkrada belirtilen kanun maddelerinde düzenlenen hükümler bakımından istisna tutulmaktadır. Bu kapsamda maddenin ikinci fıkrasında, Kanunun amacına ve temel ilkelerine uygun ve orantılı olmak kaydıyla veri sorumlusunun aydınlatma yükümlülüğünü düzenleyen 10., zararın giderilmesini talep etme hakkı hariç, ilgili kişinin haklarını düzenleyen 11. ve Veri Sorumluları Siciline kayıt yükümlülüğünü düzenleyen 16. maddelerinin uygulanmayacağı haller düzenlenmektedir. Bu haller; kişisel veri işleminin suç işlenmesinin önlenmesi veya suç soruşturması için gerekli olması, ilgili kişinin kendisi tarafından alenileştirilmiş kişisel verilerin işlenmesi, kişisel veri işleminin kanunun verdiği yetkiye dayanılarak görevli ve yetkili kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarınca, denetleme veya düzenleme görevlerinin yürütülmesi ile didiplin soruşturma veya kovuşturması için gerekli olması, kişisel veri işleminin bütçe, vergi ve mali konulara ilişkin olarak Devletin ekonomik ve mali çıkarlarının korunması için gerekli olması halleridir.

Uluslararası düzenlemelerde de kişisel verilerin korunmasına bir takım sınırlamalar getirildiği görülmektedir. Avrupa İnsan Hakları Sözleşmesi'nin 8. maddesinin birinci fıkrasında herkesin, özel hayatın gizliliğine saygı gösterilmesi hakkını hazi olduğu hükme bağlandıktan sonra, ikinci fıkrasında da bu hakkın kullanılmasına bir kamu otoritesinin müdahalesinin ancak ulusal güvenlik, kamu emniyeti, ülkenin ekonomik refahı, dirlik ve düzenin korunması, suç işlenmesinin önlenmesi, sağlığın ve ahlakın veya başkalarının hak ve özgürlüklerinin korunması için demokratik bir toplumda zorunlu olan ölçüde kanunla öngörülmüş olmak koşuluyla mümkün olabileceği düzenlenmiştir.²⁶⁰

108 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Avrupa Konseyi Sözleşmesi'nin "İstisnalar ve Kısıtlamalar" başlıklı 9. maddesinde; hangi durumlarda kişisel verilerin korunması hakkına istisna getirilebileceği düzenlenmiştir. Maddede taraf Devletlerin kanunlarında öngörülmüş olmak kaydıyla demokratik bir toplumda; devlet güvenliğinin korunması, kamu güvenliği, devletin ekonomik menfaatlerinin korunması ve suçlarla mücadelenin söz

²⁶⁰ Komisyon Raporu, s. 23

konusu olması, ilgilinin veya üçüncü kişilerin haklarının korunması, verilerin istatistiki veya bilimsel amaçlarla kullanılması durumlarında ilgilinin katılım haklarına bir sınırlama getirerek üye devletlere kişisel verilerin korunmasında istisnalar getirebileceklerini düzenlenmiştir.

95/46/AT sayılı Kişisel Verilerin İşlenmesi ve Bu Tür Verilerin Serbest Dolaşımına Dair Bireylerin Korunması Hakkında Avrupa Birliği Yönergesi'nin "İstisnalar ve Sınırlamalar" başlıklı 13. maddesinde; kanunla öngörülmüş olmak kaydıyla üye devletlerin, milli güvenlik, ülke savunması, kamu güvenliği, suç işlenmesinin önlenmesi, suçların soruşturulması ve kovuşturulması, Avrupa Birliği'nin veya üye devletin mali, bütçe veya vergi konularında önemli ekonomik ve finansal yararı, belli durumlarda resmi makamların inceleme ve denetleme yapabilmeleri, ilgili kişinin korunması, diğer kişilerin hak ve özgürlüklerinin korunması gibi nedenlerle Yönerge'de öngörülen koruma tedbirlerine istisnalar getirebilecekleri düzenlenmiştir.²⁶¹

Kişisel verilerin korunması hakkı, sınırsız olarak korunan bir hak olmayıp, belirli koşullar altında müdahale yapılması olanaklıdır.²⁶² Özellikle kamusal organlar tarafından yapılacak müdahaleye karşı kişinin rızası yoksa ancak üstün bir kamu yararının bulunması ve bu konuda verilerin korunması ile ilgili anayasal düzenlemelere uygun yapılmış kanun seviyesinde²⁶³ bir yasal düzenlemenin olması gerekir. Aynı zamanda bu yasal düzenlemenin normların açıklığı ve ölçülülük ilkelerine uygun olması gerekir. Kişisel Verilerin Korunması Kanunu gerekçesinde de belirtildiği gibi, kişisel verilerin korunması hakkına getirilen istisnalar, kişisel verilerin korunması hakkı ile diğer kamusal ve kişisel menfaatler arasında denge ve ölçülülük sağlanması açısından da gereklidir.²⁶⁴

SONUÇ

Bilişim ve iletişim teknolojilerindeki gelişmeler ve küreselleşme sonucunda, günümüzde bilgi, meta ve güç halini almış, kamu kurumları ve özel teşebbüslerden artan talep nedeniyle belirli veya belirlenebilir

²⁶¹ Komisyon Raporu, s. 23.

²⁶² Dağ, s. 96.

²⁶³ Demokratik hukuk devletlerinde kabul edilmiş ve yerleşmiş temel bir ilke olan kanunilik ilkesine göre; temel hak ve özgürlükler idari düzenlemelerle sınırlanamaz; sınırlama ancak yasama organı tarafından çıkarılacak bir kanunla yapılabilir.

²⁶⁴ Komisyon Raporu, s. 23.

nitelikteki bir kişiye ilişkin her türlü bilgiyi ifade eden kişisel verilerin kaydedilmesi, tutulması, paylaşımı, işlenmesi ve transferindeki miktar ve çeşitlilik artmıştır. Günümüzde bilgisayar, internet ve cep telefonları gibi modern iletişim araçlarının yardımıyla bireylere ait kişisel verilere kolayca ulaşılabilmekte ve bu veriler kişiler, şirketler ve ülkeler arasında çok hızlı şekilde paylaşılabilir. Bu durum, kişisel verilerin sahibi olan bireylerin hukuki güvenliğini tehdit edecek ve özel yaşamlarının gizliliğini bozabilecek bir seviyeye gelmiştir. Bütün bu karmaşa içinde, veri işlem faaliyetleri kapsamında geri planda kalan bireyin kişiliğini koruyarak geliştirmeye devam edebilmesi için, kişisel verilerin korunması hususunda düzenlemeler yapılması gerekmektedir. Uluslararası ve ulusal kaynaklarda, temel hak ve özgürlükler arasında, bireylerin özel hayatlarının gizliliğinin bir parçası olarak görülen kişisel verilerin korunması, bireylerin kişiliklerini koruyarak, kendilerini serbestçe geliştirmeleri ve verileri üzerinde kontrol sağlayarak onların geleceğini belirleyebilmeleri için son derece önemlidir. Bireyin kişisel verilerinin korunması, onun aynı zamanda özel yaşamın gizliliği, haberleşme özgürlüğü, düşünceyi açıklama özgürlüğü gibi diğer temel hak ve özgürlüklerinin garanti altına alınmasıyla da ilgilidir. İnsan onuru temeline dayanan kişisel verilerin korunması hakkı; kişisel verilerin işlenmesi nedeniyle bireyin maruz kaldığı riskler karşısında korunmasını sağlayan anayasal bir haktır. Kişisel verilerin korunması hukuku, kişisel verilerin işlenmesi sırasında bireylerin özel hayatlarının gizliliğini korumakla birlikte, kişisel verilerin güvenle paylaşılabilmesini amaçlamaktadır. Böylece birey kişisel verileri üzerinde serbestçe karar verebilecek ve böylece bireyin temel hak ve özgürlükleri korunacaktır.

Türkiye, 1981 yılında 108 Sayılı Avrupa Konseyi Sözleşmesi'ni imzalamış olmasına karşın, uzun bir süre Sözleşme'de zorunlu olarak belirtilen kişisel verilerin korunması alanını düzenleyen özel bir kanun çıkarmaması nedeniyle, Sözleşme'yi imzalayıp onaylamayan tek ülke olmuştur. Bu konu özellikle 95/46/AT sayılı Avrupa Birliği Yönergesi uyarınca Avrupa ülkelerinin kişisel verileri eşdeğer koruma bulunmayan ülkelere aktarmamaları nedeniyle ülkemiz açısından sorun oluşturan bir alan olmuş, bunun dışında insan haklarına saygılı, demokratik bir hukuk devleti olma yolunda ilerleyen ülkemiz açısından kişisel verilerin korunması alanında özel bir düzenleme yapılması bir zorunluluk halini almıştır. Nihayet 24 Mart 2016 tarihinde Kişisel Verilerin Korunması Kanunu Türkiye Büyük Millet Meclisi tarafından kabul edilerek kanunlaşmış ve bu konudaki büyük bir hukuki boşluk doldurulmuştur.

Kaynakça

- Akdağ Hale, Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması, Yüksek Lisans Tezi, Ankara Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku (Ceza ve Ceza Usul Hukuku) A.B.D., Ankara 2010.
- Akgül Aydın, Kişisel Verilerin Korunması Açısından İdarenin Hukuki Sorumluluğu ve Yargısal Denetimi, Doktora Tezi, Kocaeli Üniversitesi Sosyal Bilimler Enstitüsü, Kocaeli 2013.
- Aksoy Hüseyin Can, Kişisel Verilerin Korunması, Yüksek Lisans Tezi, Ankara Üniversitesi Sosyal Bilimler Enstitüsü Özel Hukuk (Medeni Hukuk) Anabilim Dalı, Ankara 2008.
- Artuç Mustafa, Kişilere Karşı Suçlar, Adalet Yayınevi, Ankara 2008, s. 1293
- Atak Songül, "Avrupa Konseyinin Kişisel Veriler Açısından Sağladığı Temel Güvençeler", Türkiye Barolar Birliği Dergisi, S.87, 2010.
- Aydın Sedat Erdem, AİHM İçtihatları Kapsamında Kişisel Verilerin Kaydedilmesi Suçu, Yüksek Lisans Tezi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı, İstanbul 2014.
- Bagdamor Vemon, Blackwell'in Siyaset Bilimi Ansiklopedisi, C.II, Çev. Erhan Yükselci, Sema Yükselci, Bülent Peker, Ümit Yayıncılık, Ankara 2003.
- Bainbridge David, Data Protection Law, CLT Professional Publishing, 2000.
- Banisar David, "Freedom of Information and Access to Government Record Laws Around the World", The Freedom info Global Survey, Mayıs 2004.
- Başalp Nilgün, Kişisel Verilerin Korunması ve Saklanması, Yetkin Yayınları, 2004.
- Bauman Zygmunt, Yasa Koyucular ve Yorumcular, Çev. Kemal Atakay, Metis Yayınevi, İstanbul 1996.
- Berber Leyla Keser - Lostar Murat, Bilişimde Biyometrik Yöntemler, Yetkin, Ankara 2006.
- Bergkamp Lucas - Dhont Jan, "Data Protection in Europe and the Internet: An Analysis of the European Community's Privacy Legislation in the Context of the World Wide Web", The EDI Law Review, S.7, 2000.
- Beyli Ceylin, Kişisel Verilerin Korunması Hakkında Kanun Tasarısı Üzerine Eleştiriler, Bilişim Hukuku, derleyen Mete Tevetoğlu, Kadir Has Üniversitesi Yayınları, İstanbul 2006.
- Boz Ahmet, Kişisel Verilerin Korunması: Türkiye, ABD ve AB Örnekleri, Yüksek Lisans Tezi, Polis Akademisi Güvenlik Bilimleri Enstitüsü Güvenlik Stratejileri ve Yönetimi A.B.D., Ankara 2014.
- Bygrave Lee, Data Protection Law - Approaching Its Rationale, Logic and Limits, Kluwer Law International, Newyork 2002.
- Carey Peter, Data Protection: A Practical Guide to UK and EU Law, Oxford University Press, 2004.
- Dağ Güray, Kişisel Verilerin Ceza Muhakemesi Hukukunda Delil Olarak Kullanılması, Doktora Tezi, Marmara Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Bilim Dalı, İstanbul 2011.
- Decew Judith Wagner, "The Scope of Privacy in Law and Ethics", Law and Philosophy, 5, 1986.
- Dinç Engin, Kişisel Verilerin Korunmasında Uluslararası Düzenlemeler ve Türkiye'nin Durumu, Yüksek Lisans Tezi, Dicle Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı, Diyarbakır, 2006.

- Dinç Güney, Güvensizlik Üçgeni, 1402'likler, Fişleme, Güvenlik Soruşturması, Say, İstanbul 1987.
- Dülger, Murat Volkan, Bilişim Suçları, Seçkin, Ankara 2004.
- Er Cüneyd, Biyometrik Yöntemler ve Özel Hayatın Gizliliği Hakkı, Parmak İzi, Göz ve DNA Tarama Gibi Teknolojik Kimlik Denetleme Usullerinin Hukuki Statüsü, Yetkin, Ankara 2007.
- Eren Fikret, Borçlar Hukuku, Genel Hükümler, Beta, 9. Baskı, İstanbul 2006.
- Ergün İsmail, Siber Suçların Cezalandırılması ve Türkiye'de Durum, Adalet Yayınevi, Ankara 2008.
- Ersoy Uğur, Bir İnsan Hakları Kavramı Olarak "Kişisel Verilerin Korunması", Yüksek Lisans Tezi, Gazi Üniversitesi Sosyal Bilimler Enstitüsü, Kamu Yönetimi Anabilim Dalı, Ankara 2009.
- Gültekin Nil Melek, Kişisel Verilerin Ceza Hukuku Yönünden Korunması, Yüksek Lisans Tezi, Galatasaray Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku A.B.D., İstanbul 2012.
- Gündel Ahmet, Yeni Türk Ceza Kanunu Açıklaması, 3. Cilt, Ankara 2008.
- Hafizoğulları Zeki - Özen Muharrem, Ceza Hukuku Özel Hükümler - Kişilere Karşı Suçlar, Us - A Yayıncılık, Ankara 2010.
- Heisenberg Dorothee, Negotiating Privacy: The European Union, the United States and Personal Data Protection, Lynne Rienner Publishers, London 2005.
- Jay Rosemary -Hamilton Angus, Data Protection Law and Practice, Second Edition, Thomson, 2003.
- Kanadoğlu O. Korkut, Türk ve Alman Anayasa Yargısında Anayasal Değerlerin Çatışması ve Uyumlaştırılması, Beta, İstanbul 2000.
- Kang Jerry, "Information Privacy in Cyberspace Transactions", Stanford Law Review, C.50, 1998.
- Ketizmen Muammer, Türk Ceza Hukukunda Bilişim Suçları, Adalet Yayınevi, Ankara Ocak 2008, s. 238
- Kılınç Doğan, "Anayasal Bir Hak Olarak Kişisel Verilerin Korunması", AÜHFD, C.61, S.3, 2012.
- Korff Douwe ,EC Study on the Protection of the Rights and Interests of Legal Persons with Regard to the Processing of the Personal Data Relating to Such Persons, (Study Contract ETD/97/B5-9500/78).
- Kuner Cristopher, European Data Privacy Law and Online Business, Oxford University Press, 2003.
- Kuner Cristopher, European Data Protection Law: Corporate Compliance and Regulation, İkinci Baskı, Oxford University Press, 2007.
- Kuşkonmaz Elif Mendos, Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması, Yüksek Lisans Tezi, İstanbul 2013.
- Küzeci Elif, Kişisel Verilerin Korunması, Turhan Kitabevi, Ankara 2010.
- Lyon David, Surveillance Studies an Overview, Polity Press, 2007.
- Lyon David, Surveillance After September 11, Polity, 2003.
- Oğuzman Kemal, Medeni Hukuk, Giriş, Kaynaklar, Temel Kavramlar, Filiz Kitabevi, İstanbul 2008.
- Özbek, Veli Özer, TCK İzmir Şerhi, Yeni Türk Ceza Kanununun Anlamı Özel Hükümler, C.II, Seçkin, Ankara 2008,

- Özdemir Hayrunnisa, Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması, Seçkin Yayınları, Ankara 2009.
- Parent, W. A., "A New Definition of Privacy for the Law", Law and Philosophy, 2, 1983.
- Sevimli K. Ahmet, İşçinin Özel Yaşamına Müdahalenin Sınırları, Doktora Tezi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, Özel Hukuk Anabilim Dalı, İstanbul 2006.
- Solove Daniel J. - Rotenberg Marc - Schwartz Paul M., Information Privacy Law, İkinci Baskı, Aspen Publishers, New York 2006.
- Solove Daniel J., The Digital Person, Technology and Privacy in the Information Age, New York University Press, ABD 2004.
- Soyaslan Doğan, Ceza Hukuku Özel Hükümler, 8. Baskı, Ankara 2010.
- Şahin Meral Ekici, Ceza Hukukunda Rıza, On İki Levha Yayıncılık, İstanbul 2012.
- Şimşek Oğuz, "4422 sayılı Çıkar Amaçlı Suç Örgütleriyle Mücadele Kanunu ve Kanununun 4. maddesine Göre "Kayıt ve Verilerin İncelenmesi ve Kişisel Nitelikli Verilerin Korunması", *İzmir Barosu Dergisi*, S. 4, 2001.
- Şimşek Oğuz, Anayasa Hukukunda Kişisel Verilerin Korunması, Beta Basım, İstanbul 2008.
- Taşkın Şaban Cankat, Bilişim Suçları, Beta, Bursa 2008.
- Tezcan Durmuş, "Bilgisayar Karşısında Özel Hayatın Korunması", *Anayasa Yargısı Dergisi*, 8. Cilt, 1991.
- Topaloğlu Mustafa, Bilişim Hukuku, Karahan Kitabevi, Adana 2005.
- Üzeltürk Sultan Tahmazoğlu, "Kişisel Verilerin Korunması Hakkında Anayasa Değişikliği", *Legal Hukuk Dergisi*, Sayı 93, Eylül 2010.
- Üzeltürk Sultan Tahmazoğlu, 1982 Anayasası ve İnsan Hakları Avrupa Sözleşmesine Göre Özel Hayatın Gizliliği Hakkı, Beta, İstanbul 2004.
- Wacks Raymond, Personal Information Privacy and the Law, Clarendon Press, Oxford 1993.
- Walden I. N. - Sawage R.N., "Data Protection and Privacy Laws: Should Organisations be Protected?", *International and Comparative Law Quarterly*, C.37, S. 22, 1988.
- Yalvaç Gürsel, Karşılaştırmalı Gerekçeli TCK, CMK, CGTİK, 3. Bası, Adalet Yayınevi, Ankara 2007.
- Yaşar Osman - Gökcan Hasan Tahsin - Artuç Mustafa, Yorumlu - Uygulamalı Türk Ceza Kanunu, Cilt 3, 1. Baskı, Adalet Yayınevi, Ankara 2010.
- Yılmaz, Sabire Sanem, Tıp Alanında Kişisel Verilerin Hukuka Aykırı Olarak Verilmesinin Ceza Hukuku Açısından Değerlendirilmesi (Sır Saklama Yükümlülüğü Kapsamında), Yüksek Lisans Tezi, Bahçeşehir Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Yüksek Lisans Programı, İstanbul 2014.