BEYDER / 2018, 13:2 (121-138)

KİŞİSEL VERİLERİN KORUNMASI HUKUKUNUN GENEL İLKELERİ

Sefer OĞUZ*

Özet

Kişisel veri bir kişiyi tek başına veya birden fazla verinin bir araya gelmesiyle belirleyen ya da belirlenebilir hale getiren her türlü kişisel bilgidir. Bu itibarla, Kişisel verilerin işlenmesiyle ilgili olarak gerçek kişilerin verilerinin korunmasını talep etme hakkı Anayasa'nın 20. maddesinde ve Avrupa Birliği Temel Haklar Bildirgesinin 8. maddesinde temel bir hak olarak değerlendirilmektedir. Dolayısıyla herkes kendisiyle ilgili kişisel bilgilerin korunmasında hak sahibidir. Bu nedenle toplanan verilerin zarar verme veya zarar verme ihtimalinden bulunmasından dolayı korunması gerekir.

Türkiye hükümeti Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunmasına İlişkin 1981 tarihli Sözleşmeyi (108 sayılı Sözleşme) imzalamıştır. Bu sözleşme, TBMM tarafından 30 Ocak 2016 tarihinde 6669 sayılı Kanunla onaylanması uygun bulunmuştur†. Bu kapsamda Avrupa Birliği'nin (AB) 1995 tarih ve 46 sayılı Veri Korunması Yönergesi esas alınarak oluşturulan 6698 sayılı Kişisel Verilerin Korunması Kanunu'nu (KVKK) Parlamentoda 24.03.2016 tarihinde kabul edilmiş ve 07.04.2016 tarihli Resmi Gazetede yayımlanarak yürürlüğe girmiştir.

Kişisel veri, kimliği belirli veya kimliği belirlenebilir gerçek kişiye ilişkin her türlü bilgi olarak tanımlanmıştır (KVKK m. 3, f. d). Bu kapsamda bir gerçek kişiyi tek başına belirleyen veya birden fazla bilginin doğrudan ya da dolaylı olarak birlikte kullanılmasıyla belirlenebilir hale getiren her türlü bilgi kişisel veri olarak tanımlanabilir. Her gerçek kişi kişisel verilerini koruma hakkına sahiptir. Kişisel veri şahsa sıkı sıkıya bağlı şahıs varlığı hakkı olarak değerlendirilebilir. Bu nedenle, kişisel veriler KVKK da düzenlenen özel hükümler yanında Türk Medeni Kanunda düzenlenen kişilik haklarını koruyan genel hükümlere göre korunabilir. Kişisel verileri koruyan tüm kanun hükümleri kişisel verileri koruma hukukunun genel ilkelerine göre yorumlanması gerekir.

Eğer veri işleyen sıfatına sahip bir gerçek veya tüzel kişi AB sınırları içinde faaliyette bulunmak istiyorsa Avrupa Birliği Genel Veri Koruma Tüzüğüne (General Data Protection Regulation/GDPR) ve KVKK'ya uygun davranması gerekir.

Anahtar Sözcükler; Kişisel veri, kişisel verilerin toplanması, kişisel verilerin işlenmesi, kişisel verilerin aktarılması ve yok edilmesi.

GENERAL PRINCIPLES OF PERSONAL DATA PROTECTION LAW

Abstract

Personal data is any kind of personal information either a data lonely, which can identify a person, or data, which can be combined more than one, is identify a person. Therefore it is evaluated that demand protection of naturel persons in relating to processed personal data is a fundamental right article 20 of Turkish Constitution and article 8(1) of the Charter of Fundamental Rights of the European Union That's way everyone has right to protection of personal data concerning him or her. Therefore, collected personal datas should be protected legally. Because this datas' may cause harm or potentiality of causing may come up.

Turkish government signed the Council of Europe Convention for the Protection Individuals with regard to Automatic Processing of Personal Data of 1981. This Convention was accepted and approved with Act numbered 6669 by Turkish Great assembly at January 30, 2016. For this reason, it is legalized numbered 6698 Personal Data Protection Act (PDPA) enacted by parliament on 24.03.2016 and by taking effect after announcing by official Gazette. PDPA derives from Directive 95/46/EC of European Parliament and the Council on the protection of

* Dr. Şekerbank T.A.Ş Hukuk Baş Müşaviri sefer.oguz@sekerbank.com.tr
Gönderim/Kabul Tarihi: 20 Mayıs 2018 / 20 Eylül 2018, Submitted/Accepted dates: May 20, 2018 /September 2018

† Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'nin Onaylanmasının Uygun Bulunduğuna Dair Kanun (2016). T.C. Resmi Gazete, 29628, 18 Şubat 2016.

Individuals with regard to Automatic Processing of Personal Data and on the free movement of such data[‡]. According to this act, it is defined personal data is identified or identifiable data as any information linked to any system (PDPA atr. 3 sub art. I-d). In this context, personal data can be defined as any information that identified real person or use more than a data directly, indirectly or jointly definable. Each natural person has a right to the protection of his personal data. Personal data is evaluated personal right linked strictly to personality. Thus personal data can be protected by side of the special provision of PDPA rules, also the provision of Turkish Civil Code on protection of personality. All rules protected personal datas must be interpreted according to general principles of personal data legalized in PDPA.

If ones have data processor title would like to make a business in EC zone, ones should processes personal data comply with GDPR and PDPA.

Keywords ; Personal data, collection of personal data, processing of personal data, transmitting of personal data and delete personal data.

Giriş

Gerçek kişilere ait verilerin kaydedilmek suretiyle toplanması devlet organizasyonunun ortaya çıkmasıyla başladığı söylenebilir. Zira devletin, kendisini korumak ve kamusal hizmet sunmak için insan kaynağını bilmesi gerekir. Bu itibarla, ilk veri sorumlusunun devletler olduğu rahatlıkla söylenebilir. Devlet dışındaki özel sektör kuruluşlarının veri sorumlusu olmaları ise tüketim ekonomisine geçişle kişilerin belirli mal ve hizmetlerin müşterisi haline gelmesiyle başlamıştır. Bu mal veya hizmet üreten veya sağlayan kişiler, veri sorumlusu sıfatını ticari işletmenin esaslı unsuru olan müşteri çevresi oluşturan kişilerin listesini tutmakla başlamışlardır.

Gerçek kişilere ait verilerin devlet dışında özel sektöre ait organizasyon ve kişiler tarafından tutulması tüketim ekonomisinin bir sonucu gibi görünmesine rağmen iletişim teknolojisinin gelişmesinin de etkisi olmuştur. Çünkü analog teknolojide[§] kullanılan iletişim araçlarının aksine dijital teknolojide[**] objektif kodların yüklendiği bilgisayar ile erişilen kullanıcı bilgisayarlarınında dahil olduğu bir kısım makine üzerinden geçici veya sürekli kopyalamalar ile gerçekleşmektedir (Topaloğlu, 2005: 9). Böylece ikili sayı sistemi (*binary system*)[††] olarak ifade edilen sistem bir veriyi, işlemeye, şekillendirmeye, renklendirmeye, grafik ve tablo çizmeye, ortaya çıkan sonuçları arayıp bulmaya ve sonuçlarını bir taşıyıcı ve sonuçlarını bir taşıyıcı materyale tespite ve aktarılmasına imkan verir. Dolayısıyla, dijital iletişim teknolojisinin doğasında bulunan her bir işlem, verilerin iletilmesindeki bu geçici kopyalama istenildiğinde kolayca kalıcı kişisel verilerin toplanmasını ve işlenmesinde kullanılabilmektedir.

Bu yöntemle kişilerin medeni adı, adresi, telefon numarası, e-posta adresi ile IP numarası gibi verilerin toplanmasında (*derlenmesinde*) esaslı bir yatırım yapılmış veya ortaya çıkan

[‡] The Data Protection Directive, OJ L28, 23.11.95, p.31.

[§] Manuel teknoloji, kullanılması veya kontrol edilmesi insan veya hayvanın kas gücünde dayalı olan araç ve gereçlerin üretilme esas ve tekniği olarak tanımlanabilir. (www.encyclopedia.com; Erişim tarihi: 18.7.2018).

[**] Dijital teknoloji, ikili sayı sisteminde "0" ile "1"lerin bir araya gelmesiyle oluşan sözcük ve görüntülerin kaydedilmesine, iletilmesine ve depolanmasına imkan veren teknik olarak tanımlanabilir. (www.encyclopedia.com; Erişim tarihi: 18.7.2018).

[††] Sayısal sistem (binary system), 10'luk sisteme benzeyen 2'lik sisteme dayanır. Bu sistemde kelime ve görüntüler "0" ile "1"lerin çeşitli kombinasyonlarından oluşur. Bu nedenle aynı kavram, 10'luk sisteme göre daha geniş karakterlere ifade edilir (www.encyclopedia.com; Erişim tarihi: 18.7.2018).

derlemede bir düşünce yaratıcılığı ortaya konması halinde veri tabanı hakkı da ortaya çıkabilir[‡‡]. Veri tabanı hakkının korunması ise fikri mülkiyet hukukunun konusudur.

Öte yandan teknolojik imkanlar, internet üzerinden mal veya hizmet sunan kişilerin sayısal olarak büyük miktarlarda kişisel veri toplaması ve işlemesini mümkün hale gelmiştir. Bu teknoloji kişisel verilerin daha kolay depolanmasını, erişilmesini ve aktarılmasını kısaca işlenmesini kolaylaştırmıştır. Ancak, aynı teknolojik imkanlar bu verilerin kötü niyetli üçüncü kişilerin eline geçmesini de kolaylaştırmıştır. Böyle bir ihtimalde toplanan ve işlenen verilerin kişilerin maddi veya manevi zararına sebep olacak şekilde kullanılması da mümkündür. Nitekim, merkezi Londra'da bulunan *Cambridge Analytica* şirketi 50 milyon Facebook kullanıcısının hesaplarından izinsiz olarak topladığı kişisel verileri Kasım 2016 tarihinde yapılan ABD başkanlık seçimleri ile Haziran 2016 tarihinde yapılan İngiltere'de Brexit referandumu sonuçlarını etkilemek için verilerin yasa dışı kullanması ihtimaliyle soruşturma açılmıştır[§§].

Avrupa'da bunu önlemek için kişisel verilerin korunmasına hukuki zemin arayışları 40 yıl öncesine kadar gitmektedir (Arslan, 2011: 53; Korkmaz, 2016: 83). Bu konuda mahkeme içtihatlarının kişisel verilerin gelişmesinde önemli bir rol oynamıştır. Avrupa Birliğinde kişisel verilerin korunması önce Yönerge sonra Tüzük olarak düzenlenmiştir. Almanya, Avusturya ve İsviçre gibi ülkeler ise kişisel verilerin korunmasını kanun olarak düzenleme yoluna gittikleri görülmektedir (Bu konuda bkz. Ünver, 2008: 163-198; Döner, 2015: 461-476).

İnsan Hakları Evrensel Beyannamesi'nin 12. maddesi ile Kişisel ve Siyasal Haklar Uluslararası Sözleşmesi'nin 17. maddesi özel hayatın gizliliğinin korunması kapsamında "kişisel verilerin" korunmasına temel teşkil eden ilk uluslararası genel mahiyet taşıyan metinler olduğu söylenebilir (Kılınç, 2012: 1094). Bununla birlikte, Birlermiş Milletler Genel Kurulu tavsiye mahiyetinde olsa da 14.12.1990 tarihinde kişisel verilerin korunmasına ilişkin olarak kaleme alınan "*Bilgisayarla İşlenmiş Kişisel Veri Dosyalarına İlişkin Rehber İlkeleri*" kabul etmiştir (Arslan, 2011: 37; Kılınç, 2012: 1097).

Ulusal mevzuat yönünden Anayasa'nın 20. maddesine 5982 sayılı Kanun[***] ile 3. fıkra olarak kişisel verilerin korunmasına dair hüküm eklenmiştir. Kişisel verilerin korunması talep etme hakkı, özel hayatın gizliliğinin korunması hakkından doğan temel hak ve özgürlüklerden birisidir. Başka bir deyişle kişisel verilerin korunması özel hayatın gizliliği ve korunmasıyla doğrudan ilişkili ve bu hakkın parçasıdır (Aksoy, 2010:55; Kılınç, 2012:1103; Zeybek Ünsal, 2013:102). Bu itibarla, kişisel verilere karşı yapılan mevcut veya yapılacak muhtemel saldırıların TMK m. 24 ve 25 hükümlerine dayanarak dava yoluyla korunması mümkündür. Ancak, dava açmak suretiyle koruma talebi hem pratik olarak hem de hukuk tekniği açısından makul bir çözüm yöntemi değildir (Başalp, 2008: 293).

---

‡‡ Veri tabanı konusunda FSEK m. 6, f. XI'de "*Belirli bir maksada göre belirli bir plan dahilinde verilerin ve materyallerin seçilip derlenmesi sonucu ortaya çıkan ve bir araç ile okunabilir veya diğer biçimdeki veri tabanları"* ifadesine yer verilmiştir.(Veri tabanı konusunda ayrıntılı bilgi için bkz. Şener, 2013: 32).

§§ www.theguardian.com/technology/2017/may/07/the-great-british-brexit-robbery-hijacked-democracy, (Son erişim: 27.03.2018).

*** Türkiye Cumhuriyeti Anayasası'nın Bazı Maddelerinde Değişiklik Yapılmasına Hakkında (2014). T.C. Resmi Gazete, 27580, 13 Mayıs 2014.

Türk hukukunda 6698 sayılı Kişisel Verilerin Korunması Kanunu'nu (KVKK) yürürlüğe girmesinden önce bazı kanunlarda kişisel verilerin korunmasını düzenleyen hükümlere yer verilmiştir[†††]. Ancak, bu hükümler iletişim araçlarının gelişimi sonucunda kişisel verilerin korunmasında yetersiz kalmıştır (Ünver, 2008: 164). Bu ihtiyacı karşılamak için kanunlaştırılan KVKK ile bir yandan kişisel verileri kullananların hak ve yükümlülüklerini belirlerken, diğer yandan kişinin temel hak ve özgürlükleri korunurken, verilerin yurt dışına aktarılması kontrol altına alınmak istenmiştir. Bu kapsamda kişisel verilerin işlenmesi ve yurt dışına aktarılması konusu ise sadece KVKK'da düzenlenmiştir.

KVKK ile kişisel verilerin korunması konusunda ortaya konan ilkeleri denetlemek ve bu alandaki faaliyetleri düzenlemek üzere Kişisel Verileri Koruma Kurumu ihdas edilmiştir. Bu kurumun görevi KVKK'nın amaçlarını gerçekleştirmektir (Bu konuda bkz. aşa 4).

Haksız ele geçirilen kişisel verilerin kara borsada ticareti yapılmaktadır (Hannesson, 2008:310). Kuşkusuz başkasına ait bu kişisel veriler haksız kullanılarak elektronik ortamda veya dışında suç işlenmektedir. Bir kişinin nüfus cüzdanı bilgileri kullanılarak şirket kurulmakta ve sonra suç işlendikten sonra kimliğin tanımladığı kişi bu suçu işlemediğini ispat[‡‡‡] etmek zorunda kalmamaktadır. Elektronik ortamda çeşitli ele yöntemlerle ele geçirilen kimlik bilgileriyle birlikte özellikle kredi kartı bilgileriyle veya internet bankacılığı parola ve şifreleri kullanılarak hesaplardan para çekilmesi suçları işlenmektedir.

Bu nedenle, kişisel verilerin kullanılmasının adeta zorunlu olduğu ve bu nedenle en çok hizmet sağlayıcı olarak elektronik ticaret faaliyetinde bulunan gerçek ve tüzel kişiler tarafından işlendiği dikkate alındığında 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanunu[§§§] m. 10'un özel bir önemi bulunmaktadır. Zira, özel olarak elektronik ticaretin yaygınlaşması ve güven içinde yapılması için kişisel verilerin gizliliğinin sağlanması ve korunması büyük önem taşır (Sırabaşı, 2008:298).

Yine ETDHK'da özel bir ceza hükmü öngörülmezken KVKK m. 17'de kişisel verilere ilişkin suçlar bakımından TCK m. 135 ila 140 hükümlerin uygulanacağı kabul edilmiştir (Bu konuda bkz. Şen, 2009: 1204-1207). Ayrıca, KVKK m. 7'ye aykırı olarak kişisel verileri silmeyen veya anonim hale getirmeyen kişilere TCK m. 138 hükümlerinin uygulanacağı tanzim edilmiştir. Ayrıca kişisel verilerin hukuka aykırı olarak kaydedilmesi suç olarak düzenlenmiştir (TCK m. 137). Bununla birlikte doktrinde suç düzenlemelerinde kişisel verilerin ne ceza hukuk alanında

[†††] 4721 sayılı Türk Medeni Kanunu; 6098 sayılı Türk Borçlar Kanunu; 6102 sayılı Türk Ticaret Kanunu; 4857 sayılı İş Kanunu; 5237 sayılı Türk Ceza Kanunu; 5271 sayılı Ceza Muhakemesi Kanunu; 6328 sayılı Kamu Denetçiliği Kurumu Kanunu; 5411 sayılı Bankacılık Kanunu; 663 sayılı Sağlık Bakanlığı ve Bağlı Kuruluşlarının Teşkilat ve Görevleri Hakkında KHK; 1774 sayılı Kimlik Bildirme Kanunu; 2559 sayılı Polis Vazife ve Salahiyet Kanunu; 4982 sayılı Bilgi Edinme Kanunu; 2920 sayılı Türk Sivil Havacılık Kanunu; 5258 sayılı Aile Hekimliği Kanunu; 5429 sayılı Türkiye İstatistik Kanunu; 5490 sayılı Nüfus Hizmetleri Kanunu; 5502 sayılı Sosyal Güvenlik Kurumu Kanunu; 5549 sayılı Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanunu; 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarlar Mücadele Edilmesi Hakkında Kanun; 5718 sayılı Milletlerarası Özel Hukuk ve Usul Hukuku Hakkında Kanun (Ayrıntılı bilgi için bkz. Kaya/Taştan, 2018:137-237).

[‡‡‡] Kişisel verilerin yargılama hukuku yönünden de önem arz eder. Buna göre kişisel veri Hukuk Muhakemesi Kanununa göre "*belge*" (HMK m. 199), delil serbestisi çerçevesinde Ceza Muhakemesi Kanununa göre usulüne uygun elde edilmesi şartıyla (CMK m. 116, 119, 134) delil olarak kabul edilmektedir (Bu konuda bkz. Kızılyar, 2014: 72-89).

[§§§] Elektronik Ticaretin Korunması Hakkında Kanun (2014). T.C. Resmi Gazete, 29166, 5 Kasım 2014.

ne olduğu veya neyin anlaşılması gerektiği konusunda bir açık bir hüküm bulunmaması "*Suç ve cezanın kanuniliği*" ilkesine aykırı olup olmadığı konusunda tartışma bulunmaktadır (Bu konuda bkz. Başalp, 2008: 296; Gülnihal Şener, 2011: 74). Bir suçun unsurlarında tanımlanan kavramlar her hukuk dalı için farklılık gösterebilir. Kanaatimizce, özellikle kişinin hürriyetini sınırlanmasına neden olabilecek ceza öngörülmesi halinde kavramların ceza hukukundaki tanımlarının da yapılması gerekir. Zira ceza hukukundaki kişisel verilerin ihlal edilmesi suçlarının müeyyidesi paraya çevrilebilir sınırlar içinde kalsa da hapis cezası olarak düzenlenmiştir.

1. Kişisel Veri ve Türleri

Tüzel kişiler ile vefat eden hakkındaki kişisel verilerin korunması KVKK kapsamı dışındadır. Benzer bir açıklamaya GDPR giriş 27. maddede yer verilmiştir. Ancak, GDPR vefat eden kişiler hakkındaki kişisel verilerinin koruma kapsamına alma konusunda üye ülkeler serbest bırakmıştır. Bununla birlikte, ölene ilişkin ölmeden önce işlenen verilerinde diğer aile üyelerini uzaktan ilgilendirse dahi bu kişisel verilerin mirasçıları tarafından imhasını talep hakkı tanınması isabetli olurdu. Zira, kişisel verilerin korunması konusunun, üst norm olarak kaynağı (AY m. 20, f. I) olarak özel hayatın gizliliğini koruyan hükümlerdir. Bu itibarla kişisel veriler şahıs varlığı hakkının özel bir görünümüdür.

AB veri koruma yönergesinde vefat eden hakkındaki kişisel verilerinin korunmasında uygulanıp uygulanmayacağı konusunda bir açıklık bulunmamaktadır (Bainbridge, 2000:46; Jay/Hamilton, 2003: 316). Öte yandan yaşayan gerçek kişilerin verilerinin korunmasında uygulaması ve vefat edenin gizlilik koruması tanınmaması geride kalan aile üyelerine büyük bir üzüntü yaratabilir. Bu nedenle, kişilerin ölümünden sonra kişisel verilerinin korunması gerekir (Jay/Hamilton, 2003: 316). Türk ve İsviçre hukukunda genel kabul gören ve eser sahibinin vefatından sonra eser üzerindeki manevi hakların korunmasını düzenleyen FSEK m. 19'da temelini bulan ölüm sonrası şahıs varlığı hakkının korunması mümkün olmalıdır. Ölüm sonrası şahıs varlığı hakkının korunması teorisine göre vefat edenin verileri TMK m. 24 ve TBK m. 58 kapsamında korunması savunulabilir (Bu konuda bkz. Gezder, 2007: 207-222).

KVKK kapsamında kişisel verilerin korunması sadece gerçek kişilerin verileriyle sınırlı olduğunu yukarıda ifade edilmişti. Ancak bu verinin doğrudan bir gerçek kişinin tüzel kişinin organ veya temsilcisi sıfatıyla yaptığı hukuki işlemler sebebiyle toplanması arasında bir fark bulunmamaktadır. Burada maksat gerçek kişilere ait kişisel verilerin korunmasıdır. Veri sorumlusu, kişisel verinin zarara sebep vermesi, kazayla olsa bile kaybı haksız ve hukuka aykırı şekilde işlenmesini önlemek için idari ve teknik olarak bütün önlemleri almak mecburiyetindedir (Jay/Hamilton, 2003:169). Kişisel verilerin işlenmesinde en önemli tehditlerden birisi, veri sorumlusunun çalışanlarıdır. Çalışanlar veri sorumlusunun sisteminde bulunan ve eriştikleri kişisel verileri kendi amaçları doğrultusunda kullanmamasını önlemek için çalışanlarının seçiminde ve denetlenmesinde gerekli idari tedbirler alması gerekir (Bainbridge, 2000: 63).

Bu noktadan hareketle tüzel kişiye ait olan ancak gerçek kişiyle ilgili verilerin de korunma kapsamında olduğu rahatlıkla söylenebilir (Korkmaz, 2016: 91). Zira, bir tüzel kişilikte organ veya temsilci sıfatıyla işlem yapan bir kişinin, bu veri sebebiyle belirli yahut belirlenebilir hale gelmesi mümkündür.

1.1. Kişisel Veri

Kişisel veri, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi olarak ifade edilebilir (KVKK m. 3, f. I-d). Bu kanuni tanımdan hareketle kişisel veri, belirli veya belirlenebilir olmak kaydıyla bir gerçek kişiye ait bütün bilgiler olarak tanımlanabilir (Başalp, 2008: 293; Şen, 2009: 1200; Aksoy, 2010:11; Akgül, 2013: 23; Korkmaz, 2016: 94). Bu kapsamda kişisel veri, bir kişiyi doğrudan veya dolayısıyla tek başına veya birden fazla verinin bir araya gelmesiyle belirleyen veya belirlenebilir hale getiren her türlü bilgidir (Sırabaşı, 2008: 303).

Kişisel veri konusunda düzenlemelerde özel (hassas) kişisel veri ile genel kişisel veri şeklinde ikili bir tasnif yapılmaktadır (Taştan, 2017: 40; Akgül, 2013: 21). Özel nitelikli kişisel verilerin korunmasında veri sorumlularına hukuki ve teknik olarak daha sıkı önlem alma konusunda yükümlülükler getirilmiştir[****].

Kişisel veriler üst başlığı altında, özel kişisel veri tanımı yapılarak kendi içinde ikili bir tasnif yapıldığının kabul edilmesi gerekir[††††]. Biz KVKK'da yapılan kişisel veri adlandırmasının karşılığı olarak hukuk terminolojisinde sıradan sözcüğünü ifade etmek üzere adi kişisel veriler adlandırmasını kullanacağız.

Kanun koyucu özel kişisel veri ile adi kişisel verinin korunmasında farklılıklar öngörmüştür. Bunlardan ilki, özel kişisel verinin işlenmesi için mutlak surette açık rıza aranmasıdır (KVKK m. 6, f. II). Diğeri ise özel kişisel verinin hukuka aykırı olarak kaydedilmesinde bu daha ağır müeyyidesinin öngörüldüğü suçun nitelikli hali olarak düzenlenmiştir (TCK m. 137, f. I-b).

1.1.1. Özel Kişisel Veri

Özel kişisel veri, özel nitelikte kişisel veri (*special categories of personal data*) ve hassas veri (*sensitive data*) olarak da anılmaktadır. Doktrinde bu ayrımı özel kişisel verilerin doğrudan temel hak ve özgürlüklerle dayanması sebebiyle açıklamaktadır (Bainbridge, 2000: 88; Aksoy, 2010:30). Özel kişisel veri olarak sayılanlar, özellikle II. Dünya Savaşı sonrasında ortaya çıkan ayrımcılık karşıtı ve insan onurunu korumayı hedefleyen düşüncenin bir sonucudur (Aksoy, 2010: 32; Küzeci, 2010:233).

AB hukukunda "***özel nitelikli veriler***" başlığı altında ırksal ve etnik kökeni, siyasi görüşü, dini veya felsefi inançları ya da sendika üyeliğine ilişkin bilgiler, genetik veriler, biyometrik veriler, bir gerçek kişiyi ayırt edici şekilde tanımlamak amacıyla ve sağlıkla ilgili verilerin[‡‡‡‡§§§§] (fiziki

---

[****] Kişisel Verileri Koruma Kurulu'nun 31.01.2018 tarih 2018/10 sayılı Kararı (2018). T.C. Resmi Gazete, 30353, 07 Mart 2018.

[††††] Yargıtay kişisel verileri 5 grupta tasnif etmiştir. Buna göre, yaşam şekline ilişkin kişisel veriler, ekonomik ve finansal kişisel veriler, politik kişisel veriler, bilişim alanına ilişkin kişisel veriler, sağlıkla ilgili kişisel veriler (bkz. CGK, 17.06.2014, 2012/1510 E., 2014/331. K).

[‡‡‡‡] Sağlık hizmetinin daha yüksek kalitede sunulması için sağlık verilerinin kaydedilmesi ve işlenmesi mecburiyeti bulunmaktadır. Bu amaçla sağlık verilerinin Sağlık Bakanlığı tarafından belirlenen standartlar çerçevesinde ve toplanması, işlemesi ve veri tabanına iletilmesi gerekir. Bu nedenle, ülkede bulunan tüm hastanelerin Sağlık Bakanlığı bünyesindeki sağlık merkezine bu verilerin gönderilmesi istenmiştir (Bu konuda bkz. Ülgü, e-Sağlık, 2009:16-18).

.

ve zihinsel sağlığıyla ilgili veriler) veya gerçek kişinin cinsel hayatı veya cinsel tercihlerine ilişkin veriler olarak sayılmıştır (GDPR Art. 9, Subart. 1).

Türk hukukunda, kanun koyucu tarafından, "***özel kişisel veri"*** olarak kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili veriler ile biyometrik ve genetik veriler tahdidi olarak sayılmıştır. Buna göre kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik veriler özel nitelikli kişisel veridir (KVKK m. 6, f. I). Bu tip veriler diğer verilerinden farklı olarak mahiyetleri itibariyle ayrımcılığa sebep olabilecek nitelikte olmalarıyla önem arz eder. Böyle bir özel grup veri yaratılmasında diğer amaç, kişiler arasında daha ciddi bir ayrımcılığa yol açabileceğinden daha güçlü bir koruma sağlamaktır. (Bu konuda bkz. Kaya, 2011: 318-321: Akgül, 2013: 27; Başalp, 2004: 43; Gülnihal Şener, 2011: 77; Kılınç, 2012:1112).

İki hukuk kaynağı arasında bazı verilerde farklılıklar bulunmaktadır. KVKK tanımında kılık ve kıyafet ile dernek ve vakıf üyeliği GDPR'da bulunmamaktadır. Buna karşılık, GDPR'da ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili veriler sayılmamıştır. Doktrinde ülkemiz açısından kamuoyunda dernek ve vakıf üyeliği ile kılık kıyafet tercihleri bir ayrımcılık sebebi olarak algılandığından, bunların özel nitelikte kişisel veri olarak sayılması isabetli olduğu yönünde görüş bulunmaktadır (Taştan, 2017: 42). Ancak, dernek ve vakıf üyeliği gizli kalması mümkündür. Ancak, kılık ve kıyafet tercihleri için aynı şeyi söylemek mümkün değildir. Zira, ifade özgürlüğünün bir parçası olan kılık kıyafet tercihi doğası gereği bizzat giyen kişi tarafından kamuya açık edilen bir veridir. Bu sebeple kişinin bizzat ilgili kişinin kendisi tarafından alenileştirilen bilgi olması sebebiyle KVKK m. m. 5, I-d ile çelişki yaratabilir.

1.1.2. Adi Kişisel Veri

"*Adi*" ibaresi hukuk literatüründe mutat olduğu için "*özel kişisel veri*" dışında kalan veriler için "*adi kişisel veri*" ifadesi kullanılmıştır. Adi kişisel veri ibaresinden kasıt "*özel kişisel veri*" tanımı kapsamı dışında kalan bir gerçek kişiyi belirleyen veya belirlenebilir hale getiren her türlü bilgidir. Bu kapsamda özel nitelikli veriler sayma usulü belirlenirken (*numerus clausus*) adi kişisel verilerde sınırlı sayı ilkesi geçerli değildir. Bu kapsamda, teknolojinin gelişmesi sonucunda kişiyi belirleyebilir hale getiren tüm yeni verilerin aksine bir düzenleme yapılmadığı sürece adi veri kapsamında olacağını söylemek mümkündür.

1.2. Kişisel Verilerin İşlenmesi Kavramı

Kişisel verilerin işlenmesi kavramının tanımı GDPR Art. 4, Subart. 2 ile KVKK m. 3, f. I-e'de de yapılmıştır. Aşağıda görüldüğü üzere GDPR'da yapılan tanım, KVKK'da ile aynı kapsamda yapılmış bir tanımdır.

"Otomatik olarak veya olmadan kişisel veriler veya kişisel veri setleri elde etme, kaydetme, düzenleme, yapılandırma, depolama, uyarlama veya değiştirme, erişme başvurma, kullanma, yayınlamak, yaymak ve diğer şekilde ulaşılır hale getirmek suretiyle ifşa etme, sıralama veya birleştirme, sınırlama, silme veya imha etme gibi faaliyet veya faaliyet setleri" kişisel verilerin işlenmesi olarak tanımlanmıştır*"* (GDPR m. Art. 4, Subart. 2).

"*Kişisel verilerin tamamen veya kısmen otomatik olan veya herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem"* şeklinde tanımlanmıştır (KVKK m. 3, f. I-e)*."*

Bu tanım kapsamında bir gerçek kişiye ait verinin, internete veya elektronik kapalı bir sisteme bağlı bir bilgisayara yüklenmesiyle birlikte iletime, saklama veya imha edilmeye dair her işlemin, kişisel verinin işlenmesi olduğu rahatlıkla söylenebilir.

Bu tanımlar esas alındığında işlemenin bir ortama kayıt edilmesinden sonra silme ve imha işlemi de dahil her türlü değişikliğe uğratma ile aleni hale getirilmesi verilerin işlenmesi olarak kabul edilebilir. Özetle, kişisel verinin işlenmesi, verinin kaydedilmesiyle başlayan geri döndürülmeyecek şekilde silinmesi ve imha edilmesine kadar olan bir süreç olarak tanımlanabilir.

Kişisel verilerin muhafaza edildiği, erişildiği veya işlendiği ortam otomatik (digital) veya veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan (analog) olabilir. GDPR'da yapılan bu tanımda KVKK'da yapılan tanımından "*veri kayıt sistemi*" ifadesi geçmemesi sebebiyle farklı olduğu söylenebilir. Ancak, kişisel verilerin veri kayıt sistemi olmadan işlenmesi mümkün olmadığından tanımda GDPR'da yapılan tanımda bulunmaması bir eksiklik olarak değerlendirilmesi mümkün değildir.

Özel nitelikli kişisel verilerin veri sahibinin açık rızası olmaksızın işlenmesi yasaktır. Sağlık ve cinsel hayat dışındaki hassas kişisel veriler, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir (KVKK m. 6, f. I, III). KVKK'nın taslak halindeki madde gerekçesinde askerlik yapacak kişilerin bazı özel sağlık bilgilerinin ilgili kanun hükümleri uyarınca işlenmesinin, yine hastanelerin, eczanelerin ya da Sosyal Güvenlik Kurumunun hastalarla ilgili veri işlemesinin mümkün olduğu örnek olarak sayılmıştır. Ayrıca yine taslak madde gerekçesinde bir işverenin, engelli çalıştırma zorunluluğu kapsamında, işyerinde, bu statüde çalıştırdığı kişilere ilişkin rapor ve belgeleri işlemesi bir hakkın tesisi, kullanılması ve korunması kapsamında sağlık verilerinin işlenebileceği örneklendirilmiştir. Yasalaşan metinde sağlık verilerinin açık rıza olmaksızın işlenmesinde açıkça "kanunlarda öngörülme" hususu yer almadığından bu konuda tereddütler oluşmuştur. Her ne kadar yasalaşan metinde bu ibarenin yer almaması tereddütte yol açsa da taslak metin gerekçesinde yer alan bu hususlar işin niteliği gereği zorunlu ve kanunun emrettiği özel durumlar olduğundan bu durumlarda sağlık verilerinin de açık rıza olmadan işlenmesinin mümkün olması gerekmektedir (Jay/Hamilton, 2003:191).

Yapılan bu tanımdan hareketle kişisel verilerin elde edilmesinden başlayarak silinmesi, değiştirilmesi, yok edilmesi, işaretlenmesi, sınıflandırılması ve anonim hale getirilmesi de dahil olmak üzere kişisel verilerin üzerindeki tüm işlemler veri işleme olarak kabul edilmelidir. Doktrinde kişisel verilerin aktarılması işleminin de hukuki mahiyeti itibariyle işleme olduğu görüşü ileri sürülmüştür (Arslan, 2011: 41). Bu kapsamda verilerle ilgili her türlü işlem işleme olarak kabul edilebilir.

Finansal piyasa analizlerinde bazen birden çok ülkenin kurumlarından veriler toplanarak, bu veriler genel kabul gören bilimsel analiz yöntemlerine göre işlenmektedir. Bu işleme sonucunda

ortaya çıkan sonuçlara göre gerekli yeni tasnifler önerilmekte, düzeltme ve önlemler alınmaktadır (Finansal piyasalar için bkz. Aktaş/ Doğanay, 2007: 77-91).

Öncelikle işlenecek olan kişisel verilerin hukuka uygun şekilde veriyi teslim etmeye veya işlenmesine rıza göstermeye yetkili olan kişilerden elde edilmesi gerekir (Baindbridge, 2000: 59). Hukuka uygun biçimde elde edilen kişisel verilerin de bu ilkelere uyulmadan işlenmesi halinde veri sorumlusu ve veri işleyenlerin hukuki sorumluluğu gündeme gelebilir.

Avrupa Adalet Divanı 6 Kasım 2013 tarihli kararında C-101/01 sayılı "*Bodil Lindqvist*" kararında kişisel verilerin korunması hukuku bakımından önemli ilkeleri tekrar edilmiştir. Bu kapsamda başkalarına ait kişisel verilerin internette yayınlanması işleme olarak kabul edilmiştir (Başalp, 2009: 19-21).

2. Kişisel Verilerin İşlenmesinde Genel İlkeler

Kişisel verilerin toplanması ve işlenmesiyle ilgili genel ilkeler 95/46 sayılı AB Yönergesi'nin 3 maddesinden iktibas edilerek KVKK m. 4'te 95/46 sayılı AB Yönergesine paralel olarak sayılmıştır. Bunlar hukuka ve dürüstlük kurallarına uygun olma, doğru ve gerektiğinde güncel olma, belirli, açık ve meşru amaçlar için işlenme, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ve öngörülen ve işlendikleri amaç için gerekli olan süre kadar muhafaza edilme olarak sayılmıştır. Kişiliğin korunması kapsamında kişisel verilerin korunması KVKK'da düzenlenen bu genel ilkeler çerçevesinde yorumlanacaktır. Bu ilkelere GDPR'ın 5. maddesi 2. fıkrasıyla getirilen hesap verilebilirlik *(accountability*) ilkesi de eklenebilir. Bu ilkelerin birbirinden kesin çizgilerle ayrılması mümkün değildir. Zira, bazen bir ilke diğer bir ilkeye kaynaklık ederken, diğer bir ilke onun tamamlayıcı bir fonksiyona sahip olabilir.

Doktrinde kişisel verilerin korunması konusundaki genel ilkeler dürüst toplama, asgarilik, amaca bağlılık, sınırlı kullanım, doğruluk, koruma güvenlik, bireyin katılması ve sorumluluk ilkesi olarak tasnif edilmiştir (Ünver, 2008: 175). Bu ilkeler, dağınık olarak düzenlenmiş olan kişisel verilerin toplanması ve işlenmesi ile ilgili tüm düzenlemelerde geçerlidir. Kişisel verilerin işlenmesindeki genel ilkeler tek başına hukuka uygunluk sebebi değildir. Ancak, rıza olsa bile verilerin bu ilkelere aykırı olarak işlenmesi halinde hukuka aykırı veri işleme gündeme gelecektir. Bu nedenle, bu genel ilkelerin her türlü veri işleme faaliyetinde dikkate alınması gerekir (Develioğlu: 2017:44; Çekin, 2018: 42). Bu itibarla, kişisel veri sahibi kendisine zarar verme ihtimali veya verisinin pazarlama amacıyla kullanılmasına engel olabilir (Jay/Hamilton, 2003:168). Kişisel veri ancak elde edilme amacına benzer ve bu amaca paralel olan işlemlerde hukuka uygun veri işlemesi olarak kabul edilebilir (Bainbridge, 2000: 60; Küzeci, 2010:201). Bu kapsamda kişisel veri kanuna, ultra vires'e ve sır saklama yükümlülüğüne aykırı işleniyorsa, bu hukuka aykırı işlemedir (Jay/Hamilton, 2003:150).

Hukuka aykırı işleme, kişisel verinin hukuka uygun olmayan ve kanuni haklı bir gerekçe olmadan işlenmesi olarak tanımlanabilir. Burada kanuni haklı gerekçeden kasıt KVKK m.5'te sayılan hukuka uygunluk sebepleridir. Kişisel verilerin korunması hakkı kamu idaresinin doğasından kaynaklanan gerekçelerle kamu düzeni ve kamu menfaati amacıyla sınırlanabilir. Ancak, bu sınırlama sadece ülke içindeki kamu düzeni ve kamu menfaati gerekçeleri için geçerli olabilir (Kılınç, 2012:1124).

KVKK'nın yürürlüğe girmesinden önce işlenmiş veriler için aydınlatma yükümlülüğü adresine tebligat adresine posta, veri sahibi adına kayıtlı cep telefonu numarasına yazılı veya sesli mesaj,

e-posta adresine veya kayıtlı e-posta adreslerine katmanlı bilgilendirme yapılarak yerine getirilebilir. Bu iletişim kanallarından ulaşılmayan veri sahiplerine ise gerçek veya tüzel kişinin resmi internet sitesinden aydınlatma metni yayımlanarak bu sorumluluk yerine getirilmiş sayılır (TTK m. 39, f. II).

2.1.Rıza Gösterilmesi

Kişisel verilerin işlenmesinde esas olan işlemenin hukuk uygun olmasıdır. Açık rızanın veriler işlenmeye başlanmadan önce alınması gerekir. Ancak, verinin işlenmesi "*açık rıza*" veya bunun dışında kanunlarda işlemenin açık bir şekilde izin verildiği hukuka uygunluk sebeplerinden birisi kapsamında işlenmesi halinde veri işleme hukuka uygun hale gelir (Taştan, 2017: 152; Develioğlu, 2017: 51). Kişisel verinin ilgili kişinin bizzat kendisi tarafından alenileştirilmesi halinde rızaya ihtiyaç duyulmaması gerekir (KVKK m. 5, f. II-d).

Kişisel verilerin işlenmesine rıza gösterilmesi konusunu ehliyet ve rızanın verilmesi şekli konularında ele alınması uygun bulunmuştur.

2.1.1.Rıza Gösteren Kimsenin Ehliyeti

Gerçek kişilerde kimlerin kişisel verilerinin açıklanmasına rıza göstermeye ehil olduklarının tespiti için öncelikle kişisel veriler üzerindeki hakkın niteliğinin belirlenmesi gerekir. Kişisel veriler veri sahibinin özel hayatının gizliliği kapsamında kişiye sıkı sıkıya bağlı haklardandır.

Kişisel verilerin hukuki niteliğine ilişkin bir takım görüşler ileri sürülmüştür (Bu konuda bkz. Aksoy, 2010: 37-68; Küzeci,2010: 60-102). Kişisel verilerin korunmasını talep hakkı, özel hayatın gizliliği kapsamında kişilik haklarının korunmasının bir uzantısı olduğu görünümü vermektedir. Zira, kişisel verilerin korunmasını talep hakkı gerçek kişilere verilerinin gizli olup olmadığına bakılmaksızın hukuka aykırı olarak sınırsız bir şekilde kaydedilmesi, işlenmesi ve paylaşılması konularında ona bir hak tanımakta ve onu basit bir veri nesnesi olmaktan çıkarmaktadır (Küzeci, 2010: 69). Ancak, kişiye verileri üzerinde sınırsız bir hak da vermemektedir. Devlet otoritesine kişinin verileri üzerindeki hakkının sınırlarının kişinin hak ve özgürlüklerini dikkate alarak belirleme yetkisi vermektedir. Böylece, kişisel verilerin korunması hukuku bir yandan kişinin hak ve özgürlüklerini dışa karşı korurken, diğer yandan kamu yararını da gözetmektedir (Aksoy, 2010: 72). Kişisel verileri açıklayan bu görüşler kişisel verilerin kişiye sıkı sıkıya bağlı hak olduğu noktasından hareket etmektedir.

Bu kapsamda, tam ehliyetliler ile sınırlı ehliyetlilerin kişisel verilerinin işlenmesinde kimsenin izin veya icazetine ihtiyaç duymadan rıza gösterebilirler.

Ancak, tam ehliyetsizler ile sınırlı ehliyetsizlerde bunu söylemek mümkün değildir. Tam ehliyetsizler yönünden bir değerlendirme yapabilmek için kişisel verilerin işlenmesine rıza gösterme hakkı mutlak anlamda kişiye sıkı sıkıya bağlı hak mı yoksa nisbi anlamda kişiye sıkı sıkıya bağlı hak mı olduğu noktasında değerlendirmek gerekir (Bu konuda bkz. Oğuzman/ Seliçi/ Oktay Özdemir, 2014: 83; Dural/ Ögüz, 2014: 80). Kişisel veriler, gerçek kişinin tıpkı bir kişinin medeni adı gibi onu tanımlayan belirli veya belirlenebilir her türlü bilgi olarak tanımlanmıştır (KVKK m. 3, f. I-d). Bu noktadan hareketle kişisel veri, nisbi anlamda kişiye sıkı sıkıya bağlı hak değerlendirilebilir. Bu hakkın kullanılmasının ancak yasal temsilcisi tarafından kullanılabileceğini kabul etmek gerekir.

Doktrinde sınırlı ehliyetsizlerin tek başına rıza gösterip gösteremeyecekleri konusu tartışmalıdır. Bir görüşe göre, mümeyyiz küçük ve kısıtlıların kişisel verileri TMK m. 16, f. I kapsamında kişiye sıkı sıkıya bağlı haklardan olduğu için, tek başlarına rıza göstermeleri gerekir (Taştan, 2017: 163). Diğer bir görüşü göre kişisel verilerin işlenmesine rıza gösterme hakkı mutlak anlamda kişiye sıkı sıkıya bağlı hak olmaması sebebiyle tek başına kullanılamaz. Ancak, kişisel verileri işlenmesine rıza gösterilmesi nisbi anlamda kişiye sıkı sıkıya bağlı hak olması sebebiyle sınırlı ehliyetsiz ile birlikte yasal temsilcinin açık rızasıyla verilebilir. Ancak, bu rızaya yasal temsilcisinin önceden izni veya en azından açıklanması anında katılması gerekir (bu konuda bkz. Aksoy, 2009: 67). Kanaatimizce, ikinci görüş daha isabetli görünmektedir. Zira, ilk görüşün hukuki temeli olan TMK m. 16 hükmünün amacı sınırlı ehliyetsizleri korumaktır. İlk görüşün kabulü halinde bu sınırlı ehliyetsizlerin korunmasız bırakılması ihtimali ortaya çıkabilir.

Öte yandan verilen bu rıza herhangi bir sınırlamaya tabi olmadan her zaman geri alınabilir. Aksine verilen rızanın geri alınamayacağına yönelik bir taahhüt, kişilik haklarına aykırı olduğu için geçersizliği gündeme gelecektir.

2.1.2.Rıza Göstermenin Şekli

Açık rıza (*explicit consent*), hem özel nitelikli hem de adi nitelikteki kişisel verilerin işlenmesini hukuka uygun hale getirmesi için şarttır (KVKK m. 3, f. a). Ancak kişisel verilerin elde edilmesi sırasında aydınlatma yükümlülüğünün yerine getirilmesi gerekir (KVKK m. 10). Bu aydınlatmanın Tebliğ'de[*****] belirlenen usul ve esaslara uygun şekilde yapılması gerekir. Rızanın hukuka uygun olabilmesi için temyiz kudretine sahip olan kişi tarafından bir irade sakatlanmasına neden olmadan verilmesi gerekir. Bu kapsamda sonradan verilen rıza, kişilik hakkına yapılan hukuka aykırı saldırıyı hukuka uygun hale getirebilir. Başka bir deyişle, kişisel verilerin işlenmesinde ilgili kişinin usulüne uygun açık rıza göstermesi, bu işlemeyi baştan hukuka uygun hale getirmeye yeterlidir (Develioğlu, 2017: 51). Bu müessese, ilgili kişinin işlemeye aktif katılım sağlayarak kişisel verilerinin geleceği hakkına hizmet etmektedir (Taştan, 2017: 152).

Rızanın, konuya özel olması önem arz eder. Bununla birlikte açık rızanın bir unsuru olarak aydınlatmaya (bilgilendirmeye) dayalı alınması gerekir. Bu nedenle rıza genel olmamalı ve belirli veya belirlenebilir işleme faaliyetine yönelik ise ona uygun rıza alınması gerekir. Rıza yazılı olarak alınması şart olmasa da anlaşılır, yalın ve güncel sözcükler kullanılarak alınmalıdır. Kanun koyucu rızanın gösterilmesini bir şekil şartına bağlamamıştır. Başka bir deyişle rıza, özgür iradeyle, açık, hiçbir tereddüde yer vermeyecek şekilde açık olmak kaydıyla sözlü, yazılı veya elektronik ortamda alınabilir (Arslan, 2012: 45). Bu kapsamda susma kabul değil ret anlamına geldiğini kabul etmek gerekir (Küzeci, 2010; 221).

Veri sahiplerinin, geleceğe yönelik olarak genel ve kapsayıcı rıza (battaniye rıza) vermeleri halinde bu rıza geçersizdir. Bu nedenle, rıza kişisel verilerin işlenmesinde sonradan değişmesine karşı geniş ve kapsamlı bir rıza alınması halinde bu rıza belirsiz olduğundan geçerli bir rıza olarak kabul edilmeyecektir. Öte yandan her türlü işlemde rıza alınması da

[*****] Aydınlatma Yükümlülüğünün yerine getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ, 10.03.2018 tarih (2018). T.C. Resmi Gazete, 30356, 10Mart 2018.

kişilerde rıza verme yorgunluğuna sebep olabilir. Ancak, verilen rıza makul beklenti kapsamında kalması halinde yeniden rıza alınmasına ihtiyaç duyulmaması gerekir.

Ancak, rızanın verildiğini ispat yükü veri sorumlusunda olduğu için ispat kolaylığı açısından, bir taşıyıcıya üçüncü kişilerin doğrudan veya bir araç vasıtasıyla algılanabilecek ve ilgiliye ait olduğunu ispat edecek şekilde tespit edilmesi gerekir.

Doktrinde rızanın verilmesinde örtülü beyanın yeterli olup olmadığı konusu tartışmalıdır. Bir görüşe göre şüpheye yer bırakmayacak şekilde veri sahibinin iradesini ortaya koyan örtülü beyan rıza olarak kabule yeterlidir (Küzeci, 2010:222). Diğer bir görüşe göre örtülü beyanın açık rızanın kabulü mümkün değildir (Taştan, 2017: 156). Kanaatimizce kişinin neye rıza gösterdiğini açık bir şekilde göstermesi aranmalıdır Ancak doğası gereği kişisel verilerin açıklanmadan veya bir taşıyıcıda teslim edilmeden verilmesi mümkün olmayan hizmetlerde rızanın var olduğu kabul edilmelidir.

2.2.Verinin Hukuka ve Dürüstlük Kuralına ve Şeffaflık İlkesine Uygun İşlenmesi

Kişisel veriler hukuka ve dürüstlük kurallarına uygun olarak işlenmesi gerekir (KVKK m. 4). Bu nedenle kişi, kendisi hakkında veri toplayan kişiyi bilmesi, bilgi edineme, bilgi edinme, düzeltme ve sildirme gibi katılım haklarını kullanmasını kolaylaştıracaktır. Bu hakların kullanılmasını kolaylaştırmak için veri sorumluları siciline kayıt mecburi hale getirilmiştir (Ünsal Zeybek, 2013:116). Ayrıca, veri sorumlusunun temsilcisi ve bu temsilcinin iletişim bilgilerinin sicile bildirilmesi gerekir. Kanunların açıkça izin verdiği haller dışında hiçbir şekilde veri işlenmesi mümkün değildir. Buna ek olarak kanunun izin verdiği ölçüler içinde dürüstlük kurallarına da uyulması gerekir. Burada dürüstlük kuralından kasıt, veri işleyen kişilerin veri işlenmesi sürecinde veri sahibinin menfaat ve beklentilerini dikkate almalarıdır. (Küzeci, 2010:196). Başka bir deyişle, kanun verilerin işlenmesine izin vermesine rağmen veri sorumlusu böyle bir işlemeye ihtiyaç duymuyorsa işlemeden kaçınması gerekir.

Kişisel verilerin işlenmesi hukuka ve dürüstlük kurallarına uygun olarak işlenmesi diğer ilkelere kaynaklık eden temel ilkedir. Bu ilke TMK m. 2, f. II'de düzenlenmiş olan dürüstlük kuralıyla eş anlama sahip değildir. Burada veri sorumlularının verileri işlerken "adil davranmakla" yükümlü olduklarına yönelik bir düzenlemedir. Bu ilke "haklı menfaat" ile "haklı beklenti" arasında denge kurmayı hedefler (Küzeci, 2010:196; Çekin, 2018: 45). Veri sorumlusu veya veri işleyen veri işlemeye izin veren hukuk kuralının amacı doğrultusunda mümkün olduğunda en az miktarda veri işlemeli ve ayrıca veri sahibinin çıkarlarını ve makul beklentilerini gözetmelidir. Müşteri bilgilerinin reklam amacıyla dürüstlük kuralına aykırı olarak kullanılması bu duruma örnek olarak verilebilir (Kişisel Verilerin Korunması Kurulu, Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi, KVKK Yayınları, Mart 2018, s.64-66).

Bu ilke kişisel verilen toplanmasından başlayarak, işlenmesi ve silinmesi, yok edilmesi veya anonim hale getirilmesine kadar geçerlidir. Bu itibarla kişisel verinin öncelikle hukuka uygun olarak toplanması veya kayıt altına alınması ve işlenmesi gerekir. Aksi halde hukuka uygun olamayan veri toplama, işleme ve depolama faaliyeti Anayasa ile teminat altına alınan kişinin maddi ve manevi varlığını koruma ve geliştirme hakkı (AY m. 17) ile özel hayatın gizliliği ve korunması hakkının ihlali (AY m. 20-22) anlamına gelebilir.

Bunlara birde şeffaflık (açıklık) ilkesi eklenmiştir (GDPR art. 5, f. I-a). Bu ilkenin getirilmesindeki amaç kişisel verilerin kimin tarafından hangi maksatla işlendiğini bilinmesini sağlamaktır (Bainbridge, 2000:59; Develioğlu, 2017: 44). Kanun koyucu verilerin hukuka ve dürüstlük kurallarına uygun olmayan işlemeleri bir cezai yaptırıma tabi tutmuştur (TCK m. 135).

Bu ilkenin en önemli istisnası veri sorumlusunun kanun hükmünü yerine getirilmesi veya sözleşmenin ifası için verinin açıklamak zorunda olmasıdır (Jay/Hamilton, 2003: 166). Veri sorumlusu kanundan veya sözleşmeden doğan yükümlülüğünü yerine getirmesi sebebiyle kişisel verilerin işlenmesi konusunda önemli bir istisnadır (KVKK m. 5, II-ç-e). Bir hakkın korunması için mecburi kişisel verilerin işlenmesini düzenleyen hükümlere CMK'da rastlanmıştır. Bu kapsamda, iletişimin kayda alınması ve bilgisayardaki bilgilerin yedeklenmesi hukuken işleme mahiyetindedir (CMK m. 134-135). (Bilgisayardaki verilerin yedeklenmesi usulü konusunda bkz. Özdilek, 2010: 1497-1502). Bu kapsamda CMK m. 140, f. V'de elde edilen verilerin kullanılmasının veri sahibin yoğun suç şüphesi altında olması, ikincil bir mahiyet taşımasını gerektirmekte ve bir suç soruşturma ve kovuşturmasında hakim kararı ile işleme mahiyetindeki bu yedeklemenin yapılabileceği konusundaki bir sınırlama getirildiği görülmektedir (Bu konuda bkz. Baştürk, 2010: 23-32; Candan, 2010: 1331-1341). Ceza soruşturmasında toplanan delillerin, disiplin soruşturmalarında da delil olarak kabul edilebilecektir (Koçer, 2009: 5-39).

2.3.Verinin Doğru ve Gerektiğinde Güncel Olması

Doğru ve gerektiğinde güncel olma ilkesiyle, kişisel verilerin gerçeğe uygun şekilde işlenmesi kastedilmektedir. Bu ilkeye göre ilgili kişilerin, işlenen verilerinin doğruluklarını doğru ve gerektiğinde güncel bir şekilde işlenmesini talep ve işlenen kişisel verilerinde doğruluklarını periyodik olarak kontrol etme hakkına sahiptir. (Küzeci, 2010: 208; Taştan, 2017: 47). Nitekim Kanun koyucu, bu hakkın varlığını "….*kişisel verilerin yanlış veya eksik işlenmiş olması halinde bunların düzeltilmesini isteyebilir*" şeklindeki hüküm ile ortaya koymuştur (KVKK m. 11). Kısaca kişisel verileri işleyen kimse, verilerin doğru olduğundan emin olmak zorundadır. Bu kapsamda kişisel verilerin toplanması, işlenmesi ve iletilmesi sürecinde ortaya çıkan hataların düzeltilmesi gerekir (Ünsal Zeybek, 2013: 115).

Veri sorumlusu, verilerin verileri doğru, hatasız ve güncel tutmak konusunda kendisinden beklenen özeni (*reasonable care*) göstermesi gerekir (Bainbridge, 2000: 61; Çekin, 2018: 52). Bu kapsamda, veri sorumlusu için doğru olmayan verilerin işlenmesi riski bulunuyorsa, bu durumda veri sorumlusunun sisteme etkili bir veri doğrulama sistemi koyması gerekir (Bainbridge, 2000: 61). Zira, kişisel verilerin doğru tutulması ilgili kişinin temel hak ve özgürlüklerine ve özellikle iktisadi menfaatlerine ve manevi bütünlüğüne zarar verme riskini ortaya çıkarır (Develioğlu, 2017: 48). Örneğin, adres bilgisi hatalı kaydedilen kişiye yapılan tebligatların kendisi yerine üçüncü bir kişiye ulaşması ciddi zararlara yol açabilecektir (Kişisel Verilerin Korunması Kurulu, Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi, KVKK Yayınları, Mart 2018, s.66)

Bu itibarla, veri sorumlusunun işlediği ve tutmaya devam ettiği verilerin, ilgili kişilerin verilerini güncellenmesi için bir sistem kurması ve gerektiğinde güncelleme imkanı sunması gerekir.

2.4.Verinin Meşru, Belirli ve Açık Amaçla İşlenmesi

Kişisel veriler, bu ilkeye göre ancak meşru, belirli ve rızanın alındığı amaçla sınırlı olmak üzere işlenebilir. Meşru olmanın sınırlarını, rıza ile birlikte bu rızanın emredici hükümlere, kamu düzeni ile kişilik haklarına aykırı olmaması gerekir (TBK m. 27).

Ayrıca, kişisel verilerin işlenmesi için alınan rızanın belirli bir veya iki amaçla sınırlı olması ve verinin de bu amaçlarla işlenmesi gerekir. Kişisel verinin toplanma amacı en geç, verinin toplanması anında belirlenmiş olmalıdır. Bu nedenle, mevcut durumda bilinmeyen ve gelecekte ortaya çıkacak ihtiyaçları hedef tutan amaçlar için de veri işlenemez (Zeybek Ünsal, 2013: 112; Taştan, 2017: 48). Belirli ve rızanın alındığı amaç dışında kişisel verinin işlenmesinin hukuka aykırı olduğu kabul edilir. Bu itibarla yeni bir amaçla verinin işlenmesi için muhakkak yeni bir rızanın alınması gerekir (Bainbridge, 2000: 60; Jay/Hamilton, 2003: 162).

2.5.Verinin Toplanma Amacıyla Bağlantılı, Sınırlı ve (Asgari) Ölçülü İşlenmesi

Bu ilke, minimizasyon, veri ekonomisi ve verilerin asgarileştirmesi ilkesi olarak da bilinir. Bu ilkenin amacı en az sayıda veri ile işlemlerin yapılmasını sağlamaktır. Bu ilke GDPR'da düzenlenen tasarımda "*privacy of design*" ve ilk kullanımda "*privacy of default*" ilkeleri ile desteklenmiştir. Zira verilerin amaç hasıl olacak veya amaca yetecek oranda işlenmesi gerekir. Veriyi işleyen kişi, yetecek en az miktardaki kişisel veriyle yetinmesi gerekir (Jay/Hamilton, 2003: 165; Küzeci, 2010: 204). Veri sorumlusu, kişisel verileri kendisine faydalı olduğu ve kullandığı için tutmaktadır. Bu nedenle veri sorumlusu kullanmadığı veya kendisine faydalı olamayan kişisel verileri tutmaması gerekir (Jay/Hamilton, 2003: 166). Bu ilkeye diğer kanuni düzenlemelerde de yer verildiği görülmektedir. Bunlardan ilki, TBK m. 419'da iş ilişkisine işçinin işe yatkınlığı veya hizmet sözleşmesinin ifasıyla ilgili olarak sınırlandırılmasıdır.

Bu ilke gereği, belirlenen amaca kişisel verilerin işlenmesinden başka bir araçla ulaşılabiliyorsa, öncelikle bu araçlar tercih edilmelidir. Bununla birlikte bu araçlar kişisel verilerin korunması hedeflenen temel hak ve özgürlüklere hiç veya daha az müdahale ediyorsa yine bunların tercih edilmesi icap eder (Çekin, 2018: 53). Ölçülülük ilkesi, veri işleme yapılmaksızın amaca ulaşmanın mümkün olmadığı hallerde kişisel veriler işlenirken gündeme gelir. Bu halde dahi en az sayıda verinin işlenmesi esastır. Alternatif bulunan hallerde kişisel verilerin işlenmesine izin verilmemesi gerekir.

Böyle bir durumda, verinin işlenmesi amacıyla uyumlu, sınırlı ve ölçülü olması gerekir. Bu nedenle, gelecekte kişisel verinin faydalı olabileceği ihtimali ile nasıl kullanılacağı belirlenmeden tutulması kabul edilmesi mümkün değildir (Jay/Hamilton, 2003: 166). Bu noktadan hareketle verinin işlenmesi amacıyla ilgili, uyumlu ve sınırlı olması iktiza eder. Dolayısıyla, amaçla ilgili olmayan verilerin işlenmesi halinde bu ilkeye aykırılık söz konusu olabilecektir.

2.6.Verinin İlgili Mevzuatta Öngörülen veya İşlendiği Amaçla Sınırlı Süre İle Tutulması

Bu ilkeye göre kişisel verinin, varsa mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar saklanması gerekir. Buna göre verinin elde edildiği amaç gerçekleşmesinden sonra eğer saklanma konusunda bir kanuni mecburiyet bulunmuyorsa kişisel verilerin imha edilmesi iktiza eder (KVKK m. 7). Örneğin, bu ilke gereğince bir bankaya kredi için müracaat eden bir gerçek kişinin kredi sicilinin kredi verilemeyecek şekilde çıkması sebebiyle, talebinin

ret edilmesinden sonra silinmelidir. Ancak, alınan yazılar ve faaliyetlerle ilgili belgelerin 10 yıl saklanacağı belirtilmiştir (BankK m. 42).

Kişisel verilerin işleme sürelerinin belirlenmesinde kural olarak kanunlarda yazılan sürelerin dikkate alınması gerekir. Kanunlarda belirlenen süreler dışında kalan alanlarda Kişisel Verilerin Korunması Kurulunun aldığı ilke kararı ile süre belirlemesi de mümkündür. Böyle bir sınırlamada bulunmuyorsa, veri sorumlusu verileri ancak işlediği amaçla sınırlı olan süreyle muhafaza edebilir (Bainbridge, 2000: 61; Küzeci, 2010: 203; Taştan, 2017: 49; Develioğlu, 2017: 49). Bu nedenle, veri sorumlusu gerekli olan amaçtan daha fazlası için tutmaması gerekir (Jay/Hamilton, 2003: 167). Kişisel veriler saklama amaçları açısından gerekli değilse derhal anonimleştirilmeleri veya silinmeleri gerekir.

Veri sorumluları işledikleri amaçla belirli olan azami süreyi, bu süreyi bildirmekle yükümlü tutulmuşlardır (KVKK m. 16). Veri sorumlusu bu azami süreyi, verinin mevcut ve gelecekteki değeri, veriyi muhafaza etmeye veya güncellemeye devam etmesi halinde bulun maliyet, risk ve sorumluluğu gibi faktörleri dikkate alarak belirlemesi gerekir (Taştan, 2017: 50 dn. 156).

2.7. Hesap Verilebilirlik

KVKK'da düzenlenmeyen uygun ortam sağlanarak "*verilerin bütünlük ve gizlilik*" içinde işlenmesi (GDPR m. 5, f. I-f) ile "*sorumluluk*" ilkesi (GDPR m. 5, f. II) AB Tüzüğünde tanzim edilmiştir. Verilerin korunmasından kasıt kaybolma, yetkisiz kişiler tarafından erişilme, tahrip etme, kullanma, değiştirilme ve ifşa gibi işlemlere karşı güvelik tedbirlerinin alınmış olması gerekir (Zeybek Ünsal, 2013: 113).

Veri sorumlularından veri işleyenlerin kişisel verilerin korunmasına yönelik kurumsal politikalar geliştirmesi, bu kapsamda teknik ve idari tedbirler alması ve yüksek risk taşıyan işlemler ile özel nitelikteki veriler için ön denetim mekanizmaları kurması beklenmektedir (Develioğlu, 2017: 50). Bankalara müşterilerine her türlü hizmetlerinden doğan sorularına cevap verecek bir sistem kurulması konusunda getirilen mecburiyette bu kapsamda düşünülebilir (BankK m. 76, f. I). İlgili kişilerin veri sorumlularına başvuru usul ve esasları bir Tebliğ[†††††] ile düzenlenmiştir. Veri sorumlusuna yapılacak bu başvurular talebin niteliğine göre en kısa sürede ve en geç 30 gün içinde ücretsiz olarak sonuçlandırılması gerekir. Bu cevap ayrıca bir maliyet ortaya çıkıyorsa başvuruya verilecek cevap 10 sayfayı geçiyorsa geçen her bir sayfa için 1 TL ücret alınabilir. Ancak, başvuru veri sorumlusunun hatasından kaynaklanıyorsa, hiç kimse kendi kusuruna dayanarak hak talep edemeyeceği ilkesinden hareketle bu alınan bu ücretin ilgiliye iade edilmesi gerekir.

AB Tüzüğünde "*Sorumluluk ilkesi*" olarak düzenlenen ilkenin KVKK'da bire bir karşılığı olmasa da hukuka aykırı işleme ve davranışların müeyyidelere bağlanan hükümlerinden aynı sonuca varmak mümkündür.

2.8. Kişisel Verilerin Ülke Dışına Aktarılması

Kişisel veriler, ilgili kişinin açık rızası olmaksızın başka bir ülkeye aktarılamaz (KVKK m. 9, f. I). Bu genel kuralın istisnası ise yeterli korumanın bulunmaması halinde Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli korumayı yazılı olarak taahhüt etmeleri ve kurulun

[†††††] Veri Sorumlusuna Başvuru Usul ve Esaslar Hakkında Tebliğ, 10.03.2018 tarih (2018). T.C. Resmi Gazete, 30356, 10Mart 2018.

izni bulunması kaydıyla ilgili kişinin açık rızası aranmaksızın yurt dışına aktarılabilir (KVKK m. 9, f. II).

Kişisel veri, ancak yabancı ülkeye aynı düzeyinde koruma sağlayan veya bu korumanın üstünde koruma sağlanan güvenli ülkelere transfer edilebilir (Bainbridge, 2000: 66: Jay/Hamilton, 2003: 171). Güvenli ülkeler, her devletin ve Avrupa Birliğinde veri koruma otoriteleri tarafından liste halinde yayınlanmaktadır. Kanun koyucu da Kişisel Verileri Koruma Kuruluna da korumanın bulunduğu güvenli ülkeleri belirleyerek ilan etme görevi vermiştir (KVKK m. 9, f. III).

3. Kişisel Verileri Koruma Kurumu

Kişisel Verileri Koruma Kurumu (Kurum) idari ve mali özerkliğe sahip bağımsız idari otorite olarak kurulmuştur (Kağıtçıoğlu, 2016:94). Kurum, karar organı olan Kişisel Verileri Koruma Kurulu ile Başkanlıktan oluşur (KVKK m. 19, IV). Kurumun görevlerinden biri alanı itibariyle uygulama ve mevzuattaki gelişmeleri takip etmek, değerlendirme ve önerilerde bulunmak, araştırma ve incelemeler yapmak veya yaptırmaktır. Bununla birlikte Kurum, kamu kurum ve kuruluşları, sivil toplum kuruluşları, meslek örgütleri, üniversiteler ve uluslararası kuruluşlar ile işbirliği yapmakla görevlendirilmiştir. Ayrıca diğer kanunlarla verilecek diğer görevleri yapmak yanında faaliyet raporunu Başbakanlığa sunmakla görevlidir (KVKK m. 20).

Kişisel Verileri Koruma Kurulu (Kurul) gerekli şartları taşıyan ve bu alanda bilgi ve deneyim sahibi olan ve kamu veya özel sektörde en az 10 yılı çalışmış olan 9 kişiden teşekkül eder. Kurul, üyeleri arasından Başkan ve İkinci Başkanı seçer.

Başkanlık ise Daire Başkanlıkları şeklinde teşkilatlanan hizmet birimleri ve Başkan yardımcılığından oluşur (KVKK m. 25). Kurulun başkanı, Kurumunda başkanıdır (KVKK m. 21, f. VII). Başkan Kurumun genel temsil ve yönetiminden sorumludur. Ayrıca Başkan, Kurum ve Kurulun en üst amiridir. Başkan Kurumun hizmetlerini, Kurumun amaç ve politikalarına, stratejik planına, performans ölçütlerine ve hizmet kalite standartlarına uygun olarak düzenler, yürütür ve hizmet birimleri arsında koordinasyonu sağlamakla görevlendirilmiştir (KVKK m. 25). Ayrıca Başkan, başkan yardımcısı, daire başkanları ve kurum personelini atamaya yetkilidir (KVKK m. 24).

Sonuç

Kişisel verilerin özellikle küresel çapta ve veri toplayan ana bilgisayarları (*host*) yurt dışında olan başta arama motorları www.google.com ve www.amazon.com, www.alibaba.com ve www.e-bay.com veya sosyal iletişim gibi web siteleri otomatik olarak çok büyük miktarda veri toplamaktadır. Bu veriler, daha sonra aynı kanallardan yapılan yayınlarla herhangi bir ülkenin bireylerinin veya kamunun algı yönetiminde rahatlıkla kullanılma tehlikesi bulunduğu ciddi biçimde tartışılmaktadır. Bu nedenle, kişisel verilerin hukuken korunması bir zorunluluk haline gelmiştir (Bu konuda bkz. Küzeci, 2011: 11).

Açık rıza, hem özel nitelikte veriler hem de adi nitelikte kişisel verilerin işlenmesini hukuka uygun hale getirir. Esas olan aydınlatma sağladıktan sonra veri işlenmeden açık rızanın alınmış olmasıdır. Verinin açık rıza alınmadan işlenmesi hukuka aykırı olsa bile bu rıza sonradan verilmesi halinde hukuka uygun hale gelebilir. Nitekim şahıs varlığı haklarına yapılan tecavüzlerde rıza sonradan icazet şeklinde de verilebilir (TMK m. 23). Açık rıza dışında kanuna uygun işlemenin varlığı kabul edildiğinde hak ihlali söz konusu olmayacaktır (KVKK m. 5).

Nihayet kişisel veriler hukuka aykırı işlemeye karşı kamu hukukunda (TCK m. 135-140) ve özel hukukta tazminat yaptırımı ile koruma sağlanmıştır (KVKK m. 11). Bu kapsamda, kişisel verileri hukuka aykırı olarak işlendiği iddiasında bulunan kişiler maddi ve manevi tazminat ile önleme, durdurma ve tespit davalarından faydalanması mümkündür.

Ayrıca GDPR hukuka aykırı davranan veri sorumlularına para cezası öngörülmüştür (GDPR m. 83, f. V). Benzer şekilde Kişisel Verileri Koruma Kurulu tarafından kanuna aykırı davranan veri sorumlularına uygulanacak idari para cezaları düzenlenmiştir (KVKK m. 18).

Öte yandan, kişisel verilerin korunmasıyla görevli kamu tüzel kişisi olması halinde ortaya çıkan zararın tazmini için açılacak davalarda idare hukuku içinde tespit edilmesi gerekir. Buna göre bir kamu tüzel kişisinin faaliyeti sonucunda ortaya çıkan zarardan, ilgili idare zarar gören kişi bu zarara eşit tazminatı tam yargı davasıyla talep edebilir (Akgül, 2013: 34; Kağıtçıoğlu, 2016: 80).

Yukarıda ifade edildiği üzere hizmet ilişkisi içinde çalışan kişilerin özlük haklarını kullanabilmeleri açısından sağlık verilerinin işverenle paylaşılması bir kanuna veya sözleşmeye dayanan mecburiyet olarak ortaya çıkmaktadır (Jay/Hamilton, 2003: 191). Burada hizmet ilişkisini kamu ve özel hukuka tabi tüm çalışanlar ile yapılan sözleşmeleri kapsayacak şekilde düşünülmesi gerekir. Bu mecburiyet çalışma hukukundaki yükümlülüklere uymanın sonucu olarak da çıkabilir (GDPR, art. 9, II-b). Bu itibarla çalışanların verilerinin işlenmesi konusunda KVKK'da işveren lehine açık rıza aranmaması yönünde bir hüküm bulunmaması ciddi bir eksiklik olarak değerlendirilebilir.

Ayrıca, uygulamada kılık kıyafet tercihi doğası gereği bizzat giyen kişi tarafından kamuya açık edilen bir kişisel veridir. Bu sebeple kişinin bizzat kendisi tarafından alenileştirilen veri olması sebebiyle KVKK m. m. 5, I-d ile çelişki yaratabilir.

Kaynakça

Akgül, Aydın (2013). Danıştay Kararları Işığında Kişisel Sağlık Verilerin Korunması, Danıştay Dergisi, (133), 21-45.

Aktaş, Ramazan/ Doğanay, M. Mete (2007). Gelişmekte Olan Hisse Senedi Piyasalarının Piyasa Verilerine Göre Gruplanması, BDDK Bankacılık ve Finansal Piyasalar Dergisi, 1(2), 77-91.

Arslan, Çetin (2011). Avrupa Birliği Hukukunda Kişisel Verilerin Üçüncü Ülkelere Aktarılması, BAÜHF Kazancı Hakemli Hukuk Dergisi, Mart-Nisan 2011 (79-80), 31-61.

Aksoy, Hüseyin Can (2010). Kişisel Verilerin Korunması, Ankara: Çakmak Yayınevi.

Aksoy, Hüseyin Can (2009). Kişisel Verilerin İşlenmesi Kapsamında Rıza Unsuru ve Sınırlı Ehliyetsizlerin Durumu, Haluk Konuralp Anısına Armağan, 3, 47-69.

Aksoy, Hüseyin Can (2008). The Right to Personality and Its Different Manifestations as the Core of Personal Data, Ankara Law Review 2008, 5(2), 235-249.

Başalp, Nilgün (2015). Avrupa Birliği Veri Koruması Genel Regülasyonu'nun Temel Yenilikleri, MÜHFHAD 2015, 21(1), 79-105.

Başalp, Nilgün (2009). Kişisel Verilerin İnternette Açıklanması Üzerine Bir Avrupa Adalet Divanı Kararı: Kişisel Verilerin ve Özellikle Sağlık Verilerinin İnternette Açıklanması 95/46 Sayılı Yönergenin Uygulama Alanına Girer mi ? Ankara Barosu Bilişim ve Hukuk Dergisi, Ocak-Mark 2009, 1, 19-21.

Başalp, Nilgün/Sırabaşı, Volkan/İlbaş, Çığır/Hanesson, Einar (2008). Kişisel Verilerin Korunması, Ankara Barosu Uluslararası Hukuk Kurultayı 2008 Bilişim ve Hukuk, II, 291-323 (Yazarların bölümlerine kendi adları gösterilerek atıf yapılmıştır.

Baştürk, İhsan (2010). Bilgisayara Sistemleri İle verilerinde Arama, Kopyalama ve El Koyma, Fasikül Aylık Hukuk Dergisi, Ağustos 2010, 9, 23-32.

Bainbridge, David (2000). Data Protection, Welwyn Garden City: CLT Professional Publishing.

Candan, Burak (2010). Teknolojik Araçlarla Elde Edilen Verilerin Ceza Muhakemesi Hukuku Açısından Değerlendirilmesi, GSÜHFD, 1(II), (Prof. Dr. Köksal Bayraktar'a Armağan) 1331-1341.

Çekin, Mesut Serdar (2018). 6698 Sayılı Kişisel Verilerin Korunması Kanunu, İstanbul: onikilevha yayınevi.

Develioğlu, Hüseyin Murat (2017). Avrupa Birliği Genel Veri Koruma Tüzüğü, İstanbul: Oniki levha yayınevi.

Döner, Ayhan (2015). Kişisel Verilerin Korunması Hakkında Federal Kanun, Erzincan Üniversitesi Hukuk Fakültesi Dergisi, X(1-2), 461-476.

Dural, Mustafa/ Öğüz, Tufan (2014). Kişiler Hukuku, 15. B, İstanbul: Filiz Kitapevi.

Gezder, Ümit (2007). Ölüm Sonrası Hatırayı Koruma Doktrini ve Ölüm Sonrası Kişiliğin Korunması Teorisi, İÜHFD, LXV(1), 207-222.

Jay, Rosemary/Hamilton, Angus (2003). Data Protection Law and Practice: London: Sweet&Maxwell.

Kağıtçıoğlu, Mutlu (2016). Kişisel Verileri Koruma Kurumuna İdare Hukuku Çerçevesinden Bakış, İstanbul Kemerburgaz Üniversitesi Sosyal Bilimler Dergisi, 1(2), 72-99.

Kaya, Cemil (2011). Avrupa Birliği Veri Koruma Ekseni Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi, İÜHFM, (69), 317-334.

Kaya, Mehmet Bedii/ Taştan, Furkan Güven (2018). Kişisel Veri Koruma Hukuku- Mevzuat İçtihat, İstanbul: Oniki levha yayınevi.

Koçer, Kenan (2009). Telekomünikasyon Aracılığıyla Yapılan İletişimin Denetlenmesi, Gizli Soruşturmacı, Teknik Araçlarla İzleme Ya Da Bilgisayarda, Bilgisayar Programlarında ve Kütüklerinde Arama Kopyalama ve El Koyma Suretiyle Elde Edilen Sesli Veya Görüntülü Verilerin Disiplin Soruşturmasındaki Kıymeti, Ceza Hukuku Dergisi, Ağustos 2009, 10, 5-39.

Korkmaz, İbrahim (2016). Kişisel Verilerin Korunması Kanunu Hakkında Bir Değerlendirme, TBB Dergisi, 2016 (124), 81-152.

Kılınç, Doğan (2012). Anayasal Bir Hak Olarak Verilerin Korunması, AÜHFD, 61(3), 1089-1169.

Kızılyar, Murat (2014). Ceza Yargılamasında Dijital Verilerin Değeri, Adalet Dergisi, (50), 72-89.

Küzeci, Elif (2010). Kişisel Verilerin Korunması, Ankara: Turhan Kitapevi.

Küzeci, Elif (2014). Anayasal Bir Hak: Kişisel Verilerin Korunması, Türkiye Bilişim Derneği Bilişim Dergisi, (Ekim-Kasım-Aralık 2014), 142-148.

Şen, Ersan (2009). Kişisel Verilerin Korunması Kanunu Tasarısı'nın Anayasa ve Türk Ceza Kanunu Hükümleri Çerçevesinde Değerlendirilmesi, İBD, 83(3), 1197-11.

Şener, Gülnihal Emine (2011). Kişisel Verilerin Hukuka Aykırı Olarak Kaydedilmesi Suçu, Adalet Dergisi, (39), 72-86.

Şener, Yavuz Selim (2013). Fikri Mülkiyet Hukukunda Dijital Veri Tabanlarının Korunması, Ankara: Adalet Yayınevi.

Oğuzman, M. Kemal/ Seliçi/ Özer/ Oktay Özdemir, Saibe (2014). Kişiler Hukuku (Gerçek ve Tüzel Kişiler), 14. B, İstanbul: Filiz Kitapevi.

Özdilek, Ali Osman (2010). CMK m. 134 Uygulamasında Verilerin MD5 Algoritması ile "Hash" Değerlerinin Alınmasında Çakışma "*Collision*" Sorunu, 1(II), (Prof. Dr. Köksal Bayraktar'a Armağan) 1331-1341.

Ünver, Yener (2008). Kişisel Verilerin Korunması, GSÜHFD, 1, 163-198.

Ülgü, Mustafa Mahir, (2009). E-Sağlık ve Kişisel Verilerin Standardizasyonu, Ankara Barosu Bilişim ve Hukuk Dergisi, Ocak-Mark 2009, 1, 16-18.

Taştan, Furkan Güven (2017). Türk Sözleşme Hukukunda Kişisel Verilerin Korunması, İstanbul: onikilevha yayınevi.

Topaloğlu, Mustafa (2005). Bilişim Hukuku, Adana: Karahan Kitapevi.

Zeybek Ünsal, Çağrı (2013). Google'ın Yeni Gizlilik Politikası Google Inc. Tarafından 1 Marta 2012 Tarihinde Yayınlanan Politikasının Kişisel Verilerin Korunması ile Uyumluluğu ve Avrupa Birliğinin 95/46/EC Sayılı Veri Koruma Direktifi Açısından Değerlendirilmesi, Hacettepe Üniversitesi Hukuk Fakültesi Dergisi, 3(1), 99-124.

Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi, KVKK Yayınları, Mart 2018, 64-66.