Türk Kişisel Verileri Koruma Mevzuatının Avrupa Birliği Genel Veri Koruma Tüzüğü İle Uyumlaştırılması Sürecinde Doğabilecek Sorunlar Ve Bu Sorunlara Yönelik Çözüm Önerileri

Yazarlar

Ayca Zanbaklar Seçkin[1]*

***Mensubiyet**

[1] Özel Hukuk Yüksek Lisans Programı, Yeditepe Üniversitesi, Sosyal Bilimler Enstitüsü, 34755, İstanbul, Türkiye

*Yazışma yapılacak kişi e-posta: ayca.zanbaklar@std.yeditepe.edu.tr

Özet

90'lı yıllardan itibaren bilgi teknolojileri alanında yaşanan gelişim, kişisel verilerin yasal olarak korunma ihtiyacını ön plana çıkarmıştır. Bu ihtiyaçtan yola çıkarak pek çok ülke kendi yasal mevzuatında düzenlemeler yapma gereği duymuştur. 1995 yılında 95/46/EC sayılı Direktifin kabul edilmesiyle Avrupa Birliği hukukunda kişisel veriler ilk kez yasal bir çerçeveye oturmuştur. 14 Nisan 2016 tarihinde onaylanan Avrupa Birliği Genel Veri Koruma Tüzüğü ise 25 Mayıs 2018 tarihinde yürürlüğe girmiştir. Türkiye'de ise 2010 yılında yapılan Anayasa değişikliğinden sonra 7 Nisan 2016 tarihinde Kişisel Verileri Koruma Kanunu (KVKK) kabul edilerek ilk çerçeve Yasa yürürlüğe girmiştir. Ne var ki Kişisel Verileri Koruma Kanunu'nun, 2 (iki) senelik uyum sürecinden sonra 25 Mayıs 2018 tarihinde yürürlüğe giren Genel Veri Koruma Tüzüğü ile mukayese edildiğinde yetersiz kaldığı görülmektedir. Bu yetersizliklerin temelinde, KVKK'nın, Avrupa Konseyi'nin 1 Ekim 1995 tarihinde kabul ettiği 95/46/EC sayılı "Kişisel Verilerin İşlenmesi ve Bu Verilerin Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Direktifi"ni referans alması yatmaktadır. Bu açıklamalardan hareket ile ülkemizdeki kişisel verilerin korunması yönündeki ihtiyacı karşılamaya yönelik hazırlanan Kişisel Verilerin Korunması Kanunu, Türkiye'nin Avrupa Birliğine uyum sürecinde hayati önemi haizdir. Dolayısıyla Tüzüğün, Türk mevzuatına uyumlaştırılması sürecinin karşılaştırılmalı olarak değerlendirilmesi ve ortaya çıkabilecek sorunların çözümüne yönelik çalışmalar yapılması gerekmektedir. Bu hususta, Türkiye'de yerleşik kişi ya da tüzel kişilerin, KVKK ile uyum içerisinde olması yeterli olmamakta, aynı zamanda AB Genel Veri Koruma Tüzüğü ile de uyumluluk göstermesi gerekmektedir. Kişisel Verileri Koruma Kanunu'nda yapılacak uyumlaştırma çalışmaları, halihazırda AB Genel Veri Koruma Tüzüğü'ne dahil olan gerçek kişi ve tüzel kişiler için önem taşıyacağı gibi Kişisel Verileri Koruma Kurulu bakımından ileride uygulamada oluşabilecek boşlukların doldurulmasında da önem kazanacaktır.

Anahtar Kelimeler: 6698 sayılı kişisel verileri koruma kanunu; genel veri koruma tüzüğü; kişisel veri; kişisel verilerin korunması

GİRİŞ

Günümüzde hızla ilerleyen teknolojik gelişmelerin ışığında kişisel verilerin korunma ihtiyacı giderek önem kazanmış ve bu alanda yapılan çalışmalar her geçen gün hız kazanarak ülkelerin yasal mevzuatında yer almaya başlamıştır. (Tezcan, 1991) Ülkelerin teknolojik gelişmelere ayak uydurma çabası içerisinde başta insan hak ve temel özgürlüklerini korumak, kişilerin özel hayat sınırlarına müdahaleyi engellemek ve kişisel veri ihlallerinin önüne geçmeye yönelik atılan bu adımlar, ülkemizde de "6698 sayılı Kişisel Verilerin Korunması Kanunu"'nun yürürlüğe girmesi ile önemli bir aşama kaydetmiştir. (Şimşek, 2008)

Bugün hayatımızın pek çok alanına hâkim olan teknolojik araçlar ile kişisel verilerimiz her an her dakika işlenmektedir. Bu işlemelere konu olan verilerin internet ortamında sınır ötesi ülkelere aktarımı ile kişisel verilerin korunması anlamındaki menfaat dengesi ise son derece hassas bir denge oluşturmaktadır. Özellikle 1990'lı yıllardan itibaren internet kullanımının yaygınlaşması ve beraberinde getirdiği teknolojik ilerlemeler ile kişisel verilerin işlenmesi, kayıt altına alınması, paylaşılması gibi hususlar yaygınlaşmıştır. Bu ilerlemelere karşın, verilerin güvenliğinin sağlanması bakımından gerek ülkelerin iç mevzuatları gerekse uluslararası alanda atılan adımların yetersiz kaldığı görülmüştür. Netice olarak, kişisel verilerin korunmasına ilişkin atılacak adımlarda hem çağa ayak uyduracak düzenlemelerin yapılması amaçlanmış, hem de ülkeler nezdinde yeknesak bir uygulama ihtiyacı ortaya çıkmıştır. Bu ihtiyaçları karşılamaya yönelik olarak, Avrupa Birliği'nin 24 Temmuz 1995 tarihli "95/46/EC sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Direktif"i kabul edilmiştir. AB'ye üye devletler, Direktif'i esas alarak kendi iç hukuk sistemlerine bu yeni düzenlemeleri uyumlaştırma çabalarını başlatmıştır. Ne var ki Direktif hükümlerinin üye devletler bakımından bağlayıcılığının olmaması, 2000'li yıllardan itibaren teknolojik gelişmelerin hızla aldığı seyir karşısında, 95/46/EC sayılı Direktif'in yeterli korumayı sağlayamadığı gözlemlenmiştir. (Başalp, 2015) Nihayetinde, tez konumuza kaynaklık eden "2016/679 sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü", 95/46/EC sayılı Direktif'in yürürlükten kalkması ile uygulamadaki yerini almıştır.

GVKT'nin getirdiği en önemli yenilik, tüzüğün üye devletler bakımından bağlayıcılığının olmasıdır. Zira Avrupa Birliği hukuku kaynakları arasında yer alan direktifler bütünüyle bağlayıcı

değillerdir. (Akıncı, 2017) Bu anlamıyla direktiflerin temel rolü, üye devletlerin kendi iç hukuk sistemine bu düzenlemeleri uyumlaştırma aracı olmasıdır. Tüzükler yapısı itibariyle, ülkelerin iç hukuk sistemlerinde ilave bir düzenlemeye ihtiyaç duymamaktadır.

Avrupa Birliği hukukunda gidişat böyle iken, ülkemizde kişisel verilerin korunması ile ilgili atılan adımlar geriden gelmiştir. Kişisel verileri korumaya yönelik atılan adımlara özellikle 2000'li yıllardan itibaren hız kazandırılmak istenmişse de mevcut yasal düzenleme olan Kişisel Verileri Koruma Kanunu'nun yürürlüğe girmesi 2016 yılına denk düşmektedir. Bu anlamda ülkemizde kişisel verilerin korunmasına ilişkin yasal mevzuatın oluşturulması uzun yıllar almıştır. 7 Mayıs 2010 tarihinde Anayasanın 20. maddesinde yapılan değişikliğe ilave olarak neticede 24 Mart 2016'da kabul edilen 7 Nisan 2016 tarihli ve 29677 sayılı Resmi Gazetede yayımlanarak yürürlüğe giren "6698 sayılı Kişisel Verilerin Korunması Kanunu" (KVKK) mevzuatımızda yerini almıştır. Avrupa Genel Veri Koruma Tüzüğü'nün yürürlük tarihine kıyasla, KVKK önceki tarihli bir düzenlemedir. Bununla birlikte KVKK, Avrupa Konseyi'nin 1 Ekim 1995 tarihinde kabul ettiği 108 sayılı Sözleşmeyi ve "95/46/EC sayılı Direktif"i referans alması ile çağımızın ihtiyaçlarına cevap olacak düzenlemelere sahip değildir.

KVKK'nın kabulünden kısa bir süre sonra yürürlüğe giren Tüzük ile amaçlanan, 95/46/EC sayılı Direktif'teki düzenlemelerin revize edilerek, güncel teknolojik gelişmelere ayak uyduracak yeterliliğe ulaşmasıdır. Bu anlamda Tüzük, Direktif ile karşılaştırıldığında, uygulanacak yaptırımlar, alınacak tedbirler, veri sorumlusuna yüklenecek sorumluluklar kapsamında daha geniş düzenlemelere yer vermiştir. Buna ek olarak, veri sahibine veri taşınabilirliği hakkı, unutulma hakkı gibi daha geniş haklar sunulmuştur. Bu güncellemeler ışığında, KVKK bakımından da benzer düzenlemelerin uygulamaya alınması gerekmektedir. Bu amaçların gerçekleştirilebilmesi için gerekli görülecek yasal düzenlemelerin mevzuata uygun düşecek şekilde Avrupa Veri Koruma Tüzüğüne uyumlu hale getirilmesi, halen sürmekte olan Avrupa Birliği aday ülkesi ülkemiz bakımından da son derece önemlidir.

Kişisel Verilerin Korunma İhtiyacının Hukuki Niteliği

Kişisel veriler doğal olarak insan mahremiyetinin bir parçasıdır. İçinde bulunduğumuz çağın "bilgi çağı" olarak ifade edildiği göz önüne alındığında, teknolojide yaşanan gelişmeler

sonucu mahremiyet haklarının kolaylıkla ihlal edilmesi, bu hakkın korunmasına yönelik önemi ifade etmektedir. (Çekin, 2020) Temel bir hak olarak kişisel verilerin korunması, bireylerin mahremiyetine ilişkin olup, kişilerin gizliliklerini korumayı da hukuken gerekli kılmaktadır. Ancak unutulmamalıdır ki, kişisel veri ihlaline sebep olacak unsurlar kişinin mahremiyet hakları ile sınırlandırılamayacak kadar geniş ölçüdedir.

Günümüzde teknolojinin ilerlemesi sonucu bilgi ve iletişim teknolojilerinin hayatımızda her geçen gün daha fazla kullanılıyor olmasıyla, kişisel verileri işlenen kişilerin özel hayatlarının ve gizliliklerinin ihlal edilmesi sorunu daha fazla önem kazanmıştır. Bu anlamda, kişilerin özel hayatına ilişkin her türlü ihlalin önüne geçmeyi konu alan pek çok ulusal ve uluslararası düzenlemeler yapılmıştır. Nitekim "Avrupa İnsan Hakları Sözleşmesi" (AİHS), 8. madde kapsamında, kişilerin özel ve aile yaşamlarında saygı görülme hakkını düzenlemiştir. Sözleşme'nin 8. maddesi, "özel hayat ve aile hayatına saygı hakkı" ile dört ana hakkı korumayı amaçlamıştır. Dört ana hak kapsamında, "özel hayata saygı", "aile yaşamına saygı", "haberleşme hakkına saygı" ve "konut hakkına saygı" hakları güvence altına alınmıştır. 8. madde de bu haklara ilişkin tanımlamalar yer almasa da Avrupa İnsan Hakları Sözleşmesi'nin 8. maddesinde bu haklar yorumlanmakta ve Avrupa İnsan Hakları Mahkemesi içtihatları ile de karara bağlanmaktadır.

Hukukumuzda da Anayasa m. 20 ile herkesin, özel ve aile hayatına saygı gösterilmesi hakkına sahip olduğu ifade edilmektedir. Bunun yanı sıra, AİHS'nin 8. maddesi ile korumaya alınan diğer haklar da Anayasa'nın ilgili maddeleri ile güvenceye kavuşmuştur. Özel hayatın gizliliği kavramı her ne kadar mahremiyet hakları ile eşdeğer ifade edilse de kişisel verilerin ihlalini oluşturacak her unsur kişinin mahremiyet haklarını kapsamayacak kadar geniş nitelikte olabilmektedir. (Roagna, 2012)

Kişisel verileri koruma hakkının temel bağımsız bir hak olarak ortaya çıkışı ise, özellikle AB Temel Haklar Şartı'nın 8. maddesi ile önem kazanmıştır. AB Temel Haklar Şartı 8. madde ile kişisel verileri koruma hakkı yeni ve bağımsız bir hak olarak değerlendirilmeye başlanmıştır. Özellikle ABAD'ın içtihatları ve AİHM içtihatları ile değerlendirildiğinde, kişisel verilerin koruma hakkının ayrı bir özerk hak statüsünde yer almaya başladığı görülmektedir. (Erdos, 2015)

Kişisel Veri Kavramı

Bir kişiyi doğrudan ya da dolaylı olarak tanımlamaya yetecek her türlü veri kişisel veri olarak kabul edilir. Kişiyi belirli ya da belirlenebilir kılan bilgilerin neler olduğu hususu, belirli bireye özgü ve o kişi ile ilişkili kılınacak bilgiler ile elde edilir. Örneğin, boy, saç rengi, kıyafet gibi kişinin dış görünümüne ait bilgiler ile bir isim, meslek gibi kişiyi hemen belirli kılmaya olanak tanımayan bilgiler, bir kişiyi belirli ya da belirlenebilir kılmaya yetecek nitelikte bir araya gelebilir. (Şimşek, 2008) Kişinin kimliğinin belirli olması, o kişiyi içerisinde bulunduğu toplumdan ayırt etmeye ve tanımaya yarayacak bilgiyi içerir. Kişinin kimliğinin belirlenebilir olması durumu ise kişiyi belirli kılmaya yetecek bilgilerin yetersiz kaldığı ya da o kişiyi tanımlamaya yetmediği ancak kişiyi içerisinde bulunduğu toplumdan bu ek bilgiler ile ayırt etmeye yarayacak bilgilerdir. Bir diğer ifade ile belirlenebilir olma hali, kişiyi net olarak tanımlamaya yetecek bilgilerin yanında yardımcı bilgilerin de vasıtasıyla gerçekleşir. (Taştan, 2017)

KVKK m. 3/f.1-d'de kişisel veri tanımının, ülkemizde 1981 tarihinde imzalanarak 2016 yılında onaylanan 108 sayılı Sözleşme hükmü ile aynı şekilde ifade edildiği görülmektedir. Buna göre "*kimliği belirli ya da belirlenebilir ve gerçek kişiye ait her türlü bilgi"* kişisel veriyi ifade eder. Bu anlamda kişisel verinin, uluslararası düzenlemelerde ortak ve oldukça geniş yorumlanabilen bir tanımı bulunmaktadır.

GVKT'nin 4. maddesine bakıldığında, gerçek kişiye ait belirli ya da belirlenebilir her bilgi kişisel veri olarak açıklandıktan sonra, gerçek kişi olarak veri sahibinin kişisel verileri kategorize edilmiştir. Buna göre gerçek bir kişinin zihinsel ya da fiziksel, fizyolojik ya da genetik, ekonomik, kültürel veya sosyal kimliğine ait bir ya da birden fazla faktöre atıfla doğrudan veya dolaylı olarak tanımlanabilen veriler, belirli ya da belirlenebilir nitelikte isim, bir kimlik numarası, konum verisi, çevrimiçi tanımlayıcılar kişisel veri olarak ifade edilmektedir.

Kişisel veriler genel nitelikli kişisel veriler ve özel nitelikli kişisel veriler olmak üzere ikiye ayrılır. Özel nitelikli veri kategorilerini genel nitelikteki kişisel verilerden ayıran unsur, verinin kişiler hakkında içerdiği bilginin hassasiyet düzeyi ile ilgilidir. Bu verilerin hassasiyet düzeyleri fazla olduğu için özel bir korumadan faydalanmaları gerektiği düşünülmüştür. (Bulut, 2020) Zira bu tür verilere yönelik eylemler, kişilerin mahremiyetlerine doğrudan bir saldırı niteliğinde olup

ihlal yaratma ihtimalleri de oldukça yüksektir. Nitekim bu veriler gerek mülga Direktif ve Tüzük hükümlerinde gerek KVKK'da sınırlı sayıda sayılmıştır. (Şimşek, 2008)

GVKT m. 9/f.1'de, kişilerin etnik kökenlerine ya da ırksal özelliklerine ilişkin bilgileri, dini ya da felsefi inançları ile siyasi düşüncelerine ilişkin bilgileri, sendika üyeliklerine ilişkin bilgileri, genetik ve biyometrik de dahil sağlık bilgileri ile cinsel yaşamlarına ilişkin bilgileri ve ceza mahkumiyetleri ile güvenlik tedbirlerine ilişkin verileri, özel nitelikli kişisel veriler olarak kabul edilmekte ve bu tür verilerin GVKT m. 9/f.2'de belirtilen istisnai haller dışında işlenmesi yasaklanmaktadır. Görüleceği üzere Tüzük, Direktif'ten farklı olarak genetik veriler ile biyometrik verileri de özel nitelikli veri olarak kabul etmiştir. Ayrıca belirtmek gerekir ki GVKT m. 9/f.4'te üye devletler Tüzük kapsamında ifade edilen genetik, biyometrik ya da sağlık verileri ile ilgili olarak ek koşullar belirleme serbestisine sahiptir.

Özel nitelikli kişisel veriler KVKK'nın "Özel nitelikli kişisel verilerin işlenme şartları" başlıklı 6. maddesinde tanımlanmıştır. KVKK m. 6/f.1'de kişilerin etnik kökenleri ya da ırksal özellikleri ile dini inançları, felsefi düşünceleri, siyasi görüşleri, dernek, vakıf ve sendika üyeliklerine ilişkin verileri, genetik ve biyometrik verileri de dahil sağlık verileri ile cinsel yaşamlarına ilişkin verileri, kılık ve kıyafetlerine ilişkin veriler ile ceza mahkumiyetleri ya da haklarında uygulanan güvenlik tedbirlerine ilişkin verileri özel nitelikte veriler olarak kabul edilmektedir.

Sınırlı sayıda sayılan ve verilerin hassasiyet düzeyi ile yakından ilgili olan hassas veriler dışındaki tüm kişisel veriler genel nitelikte kişisel veri kabul edilmektedir. Genel nitelikte kişisel verileri sınırlı sayıda saymak mümkün olmadığından bu veriler oldukça geniş yorumlanmaktadır.

Veri İşleme Faaliyetini Yürütenler Bakımından Tüzük ve KVKK Karşılaştırması

Veri Sorumlusu Bakımından

Kişisel verilerin işlenmesi faaliyetini sürdüren gerçek ya da tüzel kişilerin gerek KVKK gerek Tüzük hükümleri bakımından bazı farklılıklar taşıdığı açıktır. KVKK'nın 3. maddesine göre veri sorumlusu, *"Kişisel verilerin işlenme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi"* olarak ifade

edilmiştir. GVKT "Tanımlar" başlıklı m. 4/f.7'de veri sorumlusu kavramı, veri işlenme amaçlarını tek başına ya da başkalarıyla ortaklaşa belirleyen gerçek ve/veya tüzel kişileri, kamu kurum/ kuruluşları ya da diğer kuruluşlar şeklinde ifade edildiği görülmektedir. Veri sorumlusu, kişisel verilerin ne amaçla ve/veya hangi yöntemlerle işlemeye konu olacağını belirlemekle yükümlüdür. GVKT'de yer alan veri sorumlusu kavramı, Direktif ve Kanun hükümlerine nazaran daha ayrıntılı açıklamalar içermektedir. Kanun'un veri sorumlusuna ilişkin tanımında Tüzük'te yer aldığı şekliyle *"...kamu kuruluşu, kurumu veya diğer herhangi bir organ..."* ifadesine yer verilmemiştir. Bu durum uygulamada gerçek kişi ya da adi şirket ile devlet teşkilatı içerisinde yer alan üniversite, kamu hastaneleri ve tüzel kişiliği olan diğer kamu kurum/kuruluşu dışındaki kuruluşlar bakımından sorun teşkil etmektedir. (Çekin, 2020) Örneğin, tüzel kişiliği bulunmayan kurum ve kuruluşlardan Bakanlıkların veri sorumluluğu sıfatı tartışılabilir. Ancak böyle bir ihtimalde Bakanlığın tüzel kişiliği olmasa da veri sorumlusu olarak kabul edilmesi gerektiği ifade edilmiştir. (Çekin, 2020) Dolayısıyla Kanun'da veri sorumlusu ile ilgili yer verilen tanıma, kanaatimizce Tüzük ile uyumluluk gösterir nitelikte *"...kamu kuruluşu, kurumu veya diğer herhangi bir organ..."* ilavesinin yapılması isabetli olacaktır. Zira üniversitelerin, kamu hastaneleri gibi kamu kurum ve kuruluşlarının da KVKK kapsamında veri sorumlusu sayılacakları tartışmasız olduğundan "organ" ifadesinin KVKK metninde yapılacak değişiklerde yer alması gerektiği kanaatindeyiz.

Ortak Veri Sorumlusu (Joint Controllers) Bakımından

GVKT, iki ya da daha fazla veri sorumlusunun bir araya gelerek, kişisel verilerin işlenme amaçlarına ortak bir şekilde karar vermeleri halinde bu veri sorumlularını "ortak veri sorumlusu" olarak 26. maddede tanımlamaktadır. Ortak veri sorumlusu kavramından bahsedebilmek için öncelikle yer alması gereken ilk kriter, bir işleme faaliyetinin amaçlarının ve araçlarının belirlenmesine iki veya daha fazla gerçek kişi ya da tüzel kişinin ortak katılımının olmasıdır. (Küzeci, 2020) Bu ortak katılım halinde iki ya da daha fazla gerçek kişi veya tüzel kişi ortak bir şekilde karar alabileceği gibi sorumluluk paylaşımını aralarında yapacakları bir anlaşma ile farklı şekilde de yapabilmektedir. Yukarıda ifade ettiğimiz üzere böyle bir durumda "ortak veri sorumluları" GVKT m. 26 bakımından kendi sorumluluklarını belirleyen bir düzenleme de

yapmakla yükümlüdürler. Ayrıca yapılan bu düzenleme, kişisel verileri işlenen kişilere de bildirilmelidir.

KVKK'da ise ortak veri sorumlusu kavramına değinmemiştir. KVKK m. 3/f.1-ı'ya bakıldığında, Direktif hükümlerinde olduğu gibi "*tek başına ya da diğerleriyle"* ifadesine yer verilmediği görülmektedir. Doktrin, Direktif'teki gibi "tek başına ya da diğerleriyle" ifadesine yer verilmemiş olmasını KVKK'nın ortak veri sorumlusu kavramını kabul etmediği anlamına çıkmayacağını, zira Kanun'da "tek başına" ifadesinin de şart koşulmadığını ifade etmektedir. (Dülger, 2021) Dolayısıyla her ne kadar kanun metninde ortak veri sorumluları kavramına yer verilmemiş olsa da kanaatimizce birden fazla veri sorumlusu bir araya gelerek veri işleme faaliyetlerini gerçekleştirebilecektir.

Veri İşleyen Bakımından

KVKK m. 3/f.1-ğ'de veri işleyen, veri sorumlusu adına ve ondan aldığı emir ve talimatlarla işleme faaliyetini gerçekleştiren gerçek ve/veya tüzel kişi olarak tanımlanmıştır. GVKT m. 4/f.8'e göre de veri sorumlusu adına veri işleme faaliyetlerini gerçekleştiren gerçek ve/veya tüzel kişiliğe sahip kamu kurum ya da kuruluşları ile diğer organları ifade eden kişi veri işleyen olarak ifade edilmiştir. Veri işleyen, veri sorumlusundan talimatları doğrultusunda onun adına işleme faaliyetlerini gerçekleştirirken işlemenin daha ziyade teknik kısımları ile ilgilenen gerçek kişi, tüzel kişi ya da tüzel kişiliğe bağlı organı temsil eden kişi olarak ifade edilir. Buna göre veri işleyen sıfatını haiz olmanın iki temel koşulu olduğu ifade edilebilir. Bu koşullardan ilki, kişisel verileri veri sorumlusu adına işlemesi, ikinci koşul ise veri sorumlusundan ayrı bir gerçek kişiliği, tüzel kişiliği ya da tüzel kişiliğe bağlı bir organı temsil eden kişi bulunmasıdır.

Gerçek bir kişi ya da tüzel kişiliğin işleme faaliyetleri bakımından hem veri sorumlusu hem de veri işleyen olarak değerlendirilmesi mümkündür. Örneğin bir reklam ajansı kendi çalışanlarına karşı tuttuğu kişisel veriler bakımından veri sorumlusu sıfatını haiz iken, müşterilerine ilişkin tuttuğu kişisel veriler bakımından veri işleyen olarak değerlendirilecektir. (Küzeci, 2020) Bununla birlikte veri sorumlusu, işleme faaliyetlerini kendi çalışanlarından seçtiği bir veri işleyenle yürütebileceği gibi, dışarıdan aldığı bir hizmet ile sözleşme ilişkisine dayalı olarak da gerçekleştirebilir. (Memiş, 2017)

Veri işleyen, kişisel verilerin işlenmesi ile ilgili daha çok işin teknik yönü ile ilgilendiğinden, veri işlemenin gizliliği ve güvenliği anlamında önemli bir rol oynamaktadır. GVKT'nin "Tazminat Hakkı ve Sorumluluk" başlıklı 82. maddesinde, veri işleyenin yükümlülüklerini ihlal etmesi halinde doğrudan sorumlu tutulabileceği düzenlenmiştir. KVKK'da veri işleyen ile ilgili açıklamalara m. 3/f.1-ğ dışında, veri sorumlusunun kişisel verilerin işlenmesinde, veri güvenliğine ilişkin tedbirlerin alınması noktasında veri işleyenle birlikte müştereken sorumluluğunu ifade ettiği m. 12/f.2 ve veri sorumluları ile veri işleyenlerin, elde ettikleri kişisel verileri KVKK'ya aykırı olarak üçüncü kişilere açıklayamayacağı ve işleme amacı dışında kullanamayacaklarını ifade eden m. 12/f.4 hükümlerinde değinilmiştir. (Çekin, 2020) Ancak yine de KVKK bakımından veri işleyen ile ilgili açıklamaların son derece yetersiz olduğu anlaşılmaktadır. Nitekim, gerek mehaz düzenleme Direktif m. 2/f'de gerek GVKT m. 4/f.10'da üçüncü kişinin tanımına yer verilerek bu kişilerin veri işleyen ile arasındaki farklara yer verilmiştir. Oysa KVKK metninde üçüncü kişi tanımına yer verilmediği gibi üçüncü kişiye ilişkin ifadeler de çok muğlak ve sınırlıdır. (Çekin, 2020) Üstelik hem Direktif m. 17/f.2 hem de GVKT m. 28/f.1 ile özel bir düzenlemeye yer verilerek, Direktif m. 17/f.3 ve GVKT m. 28/f.3 ile veri sorumluları ile veri işleyenlerin aralarında yapılacak sözleşme sorumluluğuna ilişkin açıklamalara ve sözleşmenin taşıması gereken asgari unsurlara yer verilmiştir. (Çekin, 2020)

Alıcı (Recipient) ve Üçüncü Kişi (Third Party) Bakımından

GVKT m. 4/f.9'da alıcı, üçüncü bir kişi olup olmadığı fark etmeksizin, kişisel verilerin açıklandığı gerçek kişiler, tüzel kişiler, kamu kurum ya da kuruluşları ile bunlar dışında kalan diğer kuruluşları ifade etmektedir. "Alıcı", veri sorumlusu ya da veri işleyenin kişisel verilerini açıkladığı kişiler ile ilgili bu kişilere bilgi verme yükümlülüğünden dolayı önem arz eden bir kavramdır. O halde üçüncü şahısları kapsasın ya da kapsamasın, kişisel verilerin açıklandığı herkes alıcı olarak değerlendirilebilir. (Lambert, 2017) Örneğin bir veri sorumlusunun kişisel verileri bir başka kuruluşa, veri işleyene ya da diğer üçüncü bir tarafa göndermesi halinde, verilerin aktarıldığı kişi alıcı olarak değerlendirilecektir.

GVKT m. 4/f.10'da üçüncü kişi, bir veri sorumlusu, veri işleyen ya da veri sahibinin yetkisi altında ve kişisel verileri işleme yetkisi bulunan kişiler dışındaki tüm gerçek kişileri, tüzel kişileri ve kamu kurum/kuruluş ya da organları ifade etmektedir.

Kişisel verilerin korunması bakımından "üçüncü kişi" ile "alıcı" kavramları arasındaki temel fark, bu kişilerin veri sorumluları ile aralarındaki ilişkiden ve dolayısıyla veri sorumlusu tarafından tutulan kişisel verilere erişim yetkileri bakımından kaynaklanmaktadır. Bir diğer ifade ile "üçüncü kişi" ile "alıcı arasındaki ayrım, işlenen kişisel verilerin yasal olarak açıklanması hususu ile yakından ilişkilidir. Örneğin bir veri sorumlusunun çalışanları ya da veri işleyenler, kişisel verilerin işlenmesi aşamalarında yer alıyorlarsa, başkaca herhangi bir yasal gereklilik olmaksızın bu kişiler, kişisel verilerin alıcısı olarak kabul edilirler. Buna rağmen bir veri sorumlusu ya da veri işleyici tarafından yetkilendirilmeyen ya da yasal bir gerekçeye dayanmaksızın kişisel verileri elde eden bir kişi üçüncü kişi olabilmektedir. Bir diğer ifade ile veri sorumlusunun çalışanı, kişisel verileri veri sorumlusu adına ve onun talimatları ile kullandığından "üçüncü kişi" olarak değil, "alıcı" olarak değerlendirilecektir.

KVKK "alıcı" kavramına yer vermemiştir. Bununla birlikte KVKK m. 16/f.3-ç, "kişisel verilerin aktarılabileceği alıcı veya alıcı grupları" şeklindeki ifadeye yer vermiştir. Veri Sorumluları Sicili Hakkında Yönetmelik'in 4. maddesinin a bendinde ise alıcı grubu, veri sorumluları tarafından verilerin aktarıldığı gerçek ya da tüzel kişi kategorisi şeklinde ifade edilmektedir. Benzer şekilde Kanun'da "üçüncü kişi" tanımına yer verilmemişse de bazı madde hükümlerinde dolaylı olarak üçüncü kişi ifadesi yer almaktadır. (Çelik, 2022) Nitekim Kanun'un "Haklar ve Yükümlülükler" başlıklı üçüncü bölümünde "Veri sorumlusunun aydınlatma yükümlülüğü" başlıklı 10. maddesinde "yetkilendirdiği kişi" ifadesine yer verilmiş ancak bu kişinin kim olduğu, hukuki statüsünün ne şekilde yer aldığı ya da hangi şartlar altında yetkilendirileceğine ilişkin açıklamalara yer verilmemiştir. Dolayısıyla veri sorumlusu tarafından yetkilendirilen bu kişi veya kişilerin, işlenen kişisel veriler bakımından hangi sıfatla sorumlu olacakları muallaktır. Kanaatimizce KVKK m. 10'da yer alan "yetkilendirdiği kişi" ifadesi ile alıcıya atıf yapılmaktadır. Zira kişisel verilerin elde edilmesi sırasında veri sorumlusunun yetkilendirdiği kişi yasal amaçlar dahilinde kişisel verilere ulaşma ulaşmaktadır. O halde Tüzük hükümlerinde yer alan bu kavramların hukukumuz açısından da ayrımları net olarak ortaya konarak KVKK kapsamına alınması gereklidir. Böylelikle veri sorumlusu ve veri işleyen dışında

kişisel verilere ulaşan kişiler bakımından herhangi bir veri ihlalinde sorumlulukların ne şekilde doğacağına ilişkin daha net ifadeler KVKK bakımından da yerini alabilir.

KVKK'da Yer Almayan Pseudonymization (Takma Adlandırma) Kavramı

Pseudonymization kavramı, KVKK'da yer verilmeyen bir kavram olup, Kanun m. 3/f.1-b'de yer alan "anonim hale getirme" tanımı ile ayrımının yapılması bakımından son derece önemlidir. Kelime anlamı olarak Pseudonymization, takma adlandırma, takma ad konulmuş veri olarak ifade edilebilmektedir. Aynı zamanda, "bulanıklaştırma" olarak da ifade edilen pseudonymization kavramı, *"...Bir kişinin kimliğinin, o kişi ile ilgili veriler üzerinden izi sürülemez hale getirilmesi amacıyla, algoritmalar kullanarak kişiyi belirli kılan verilerin şifreli verilerle değiştirildiği teknik bir yöntem..."* olarak ifade edilmektedir. (Akıncı, 2019)

Anonimleştirme ve takma adlandırma kavramları, GVKT'nin yürürlüğe girmesinden bu yana çokça tartışılan iki kavram olmuştur. Her ne kadar Tüzük kapsamında anonimleştirme tanımına yer verilmemiş ise de Tüzük resitallerinde takma adlandırma ile anonimleştirme arasındaki ayrımın çizildiği açıklamalar yer almaktadır. GVKT m. 4/f.5'te takma adlandırma, kişisel verilerin belirlenebilir gerçek bir kişiyle ilişkilendirilmemesini sağlamak üzere kişiye ilişkin bir takım ek bilgilerin ayrı muhafaza edilmesini ve uygun güvenlik önlemlerine tabi olma şartıyla, bu verilerin söz konusu ek bilgiler kullanılmaksızın o gerçek kişi ile ilişkilendirilemeyecek yöntemlerle işlenmesi şeklinde ifade edilmiştir. Bununla birlikte takma ad verilerek yaratılan kişisel verilerin Tüzük kapsamında kişisel veri olarak kabul edileceği 26 No'lu resitalde ifade edilmiştir. GVKT 26 No'lu resital, gerçek bir kişi ile ilgisi olmayan ve onu belirlenebilir kılmaya yetmeyen ya da anonim hale gelen verilere uygulanmaması gerektiğini ifade etmiştir. (Çelikel, 2021) O halde takma adlandırmanın, bir kişiyi belirlenebilir kılan kişisel verilerinin çeşitli parçalara ayrılarak, bu parçalara belirli kodlar ya da şifreler verilmesiyle oluştuğunu ve bu parçalı verilerin bir araya getirilmeden gerçek bir kişiyi belirli ya da belirlenebilir kılmasının mümkün olmadığı işlenme olduğu ifade edebilir. (Develioğlu, 2017)

Bu noktada takma adlandırma ile anonimleştirme kavramları arasındaki ayrımın altının biraz daha çizilmesi gerekmektedir. Zira anonimleştirme ve takma adlandırma kişisel verilerin ait olduğu gerçek kişilerin kimliklerinin gizlenmesinin iki farklı yolu olup, her birinin özünde kendi

amacı bulunmaktadır. (Williamson, 2021) Kişisel verilerin takma adlandırma yöntemi ile oluşturulmasında kullanılan işlemler tersine çevrilebilir ve yetkili kullanıcıların korunan verileri daha sonra görüntülemesine ve yönetmesine izin verebilir. Bu yöntem daha çok kişilerin kimlik numaraları, sosyal güvenlik numaraları gibi verilerinin yetkisiz kullanıcılar için daha az erişilebilir hale getirilmesine yardımcı olan bir gizlilik yöntemidir. (Williamson, 2021)

Buna karşın anonimleştirme yöntemi kullanıldıktan sonra, kişisel verilerin artık gerçek bir kişiyi belirlenebilir kılması mümkün değildir. (Akıncı, 2019) Bu veriler artık herhangi bir kişiye atfedilemeyeceği gibi bir kişiyi belirli ya da belirlenebilir kılmaya yetecek ölçüde de değildir. Bununla birlikte hem anonimleştirme hem de takma adlandırma, GVKT'nin kişisel veri ihlallerini en aza indirmek ve bu verilerin kötüye kullanımlarını engellemek adına kullanılacak yöntemlerdendir. Ancak belirtmek gerekir ki, takma adlandırma yöntemi ile kişisel verilerin doğru bir şekilde gizlenememesi durumunda, kişisel verileri işleyenler açısından ağır yaptırımlar ortaya çıkacaktır. Üstelik yeterli gizlilik önemlerinin alınmadığı durumlarda bu kişisel verilerin kötü aktörlerin eline geçmesi de ihtimaller dahilinde olacaktır.

Yukarıda ifade edildiği üzere Direktif'i referans alan KVKK, takma adlandırma tanımına yer vermemiştir. Tüzük'ten ayrı olarak KVKK'nın 3. maddesi ile anonim hale getirme kavramına yer verilmişse de bu husus Kanun tasarı metninde eleştiri almıştır. Her ne kadar kişisel verilerin anonim hale getirildikten sonra geri döndürülmesi gelişen teknoloji ile imkânsız görünmemekteyse de aksi de söz konusu olabilmektedir. Bu şekilde Tüzük bakımından anonim hale gelen verilerin korumadan faydalanamayacağı açıktır. Aynı durum KVKK için de geçerlidir. Ancak KVKK'da takma adlandırma tanımına yer verilmemiş olması, takma adlandırma yöntemi ile muhafaza edilen kişisel verilerin korunmayacağı anlamına gelmemektedir. Nitekim Kişisel Verileri Koruma Kurumu'nun Rehberinde bu husus ifade edilmiştir. Rehberde takma adlandırmanın, verileri anonimleştirerek kişisel veri olma niteliğini sonlandırmadığını, kişisel verilerin anonim hale gelmediği sebeple kişisel veri niteliğini haiz olarak KVKK'ya tabi olacağı ifade edilmiştir. Kanaatimizce KVKK'da takma adlandırma yöntemine ilişkin bir düzenlemenin yer alarak, bu kavramın anonim hale getirmeden ayrımı ortaya konularak Kanun maddelerinde yer alması gereklidir.

Bir Hukuka Uygunluk Sebebi Olarak Rıza Kavramı

Hukuka aykırılık teşkil eden fiiller, kanun tarafından belirlenen özel durumlarda, kanunun gerektirdiği şartları sağlayarak hukuka uygun zemine oturabilirler. Kanunun, hukuka aykırı bir fiili hukuka uygun hale getiren, bir diğer ifade ile fiili hukuka aykırı olmaktan çıkaran bir unsuru da "rıza" kavramıdır. (Helvacı, 2021) Tüzük, rıza kavramını hem rıza (consent) hem de açık rıza (explicit consent) olarak ayrı ayrı ele alırken Kanunumuz yalnızca açık rıza kavramına yer vermektedir. Tüzük hükümlerinde olduğu gibi kanunumuz bakımından da açık rızanın geçerli olabilmesi için belirli unsurları barındırması gerekmektedir. Bu unsurlar üç unsur olarak kabul görmektedir. Buna göre açık rıza, spesifik bir konuya ilişkin olmalı, rıza aydınlatmaya/bilgi vermeye dayanmalı ve rıza özgür bir irade beyanı ile açıklanmış olmalıdır. (Braun, 2018) Ancak Direktif'i referans alan Kanunumuz bakımından rızanın 4 unsur olarak kabul görmesi gerektiği ve "tereddüde yer bırakmayacak açıklıkta" ifadesinin de son unsur olarak yer alması gerektiğine inanıyoruz.

KVKK'nın açık rıza ile ilgili "*belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza"* ifadesiyle yalnızca açık rıza tanımına yer vermiş olmasını, Tüzük bakımından değerlendiren bazı yazarlar, ilgili kişiden alınması gereken rıza şartlarının kuvvetlendirildiği yönünde yorumda bulunmuşlardır. (Dülger, 2019) Bu anlamda Tüzük bakımından açık rıza kavramına ayrı olarak yer verilmediği ifade edilerek, aslında KVKK ile yapılan mukayesede *"bilgilendirmeye dayalı rıza"* alınması ifadesinden bu rızanın da açık rıza olduğu ifade edilmiştir. (Dülger, 2019) Diğer yandan farklı bir görüş, KVKK'da yer verilen "açık rıza" tanımı ile aslında açık rızanın değil, mülga 95/46/EC sayılı Direktif hükümlerindeki açıklamalarıyla örtüşen "rıza" kavramının tanımının yapıldığını ifade etmiştir. (Braun, 2018) Zira KVKK'nın gerekçesinde açık rızanın tanımı yapılırken Direktif referans alınmıştır. (Braun, 2018) Referans alınan Direktif'in 7. maddesinin a bendi ise açık rızanın tanımını yaparken rızanın *"tereddüde yer bırakmayacak açıklıkta"* (unambiguously) olması gerektiğini belirtmektedir. Kanun'un gerekçesinde yer verilen *"tereddüde yer bırakmayacak açıklıkta"* ifadesi ise Kanun'un açık rıza tanımında yer almamaktadır. Dolayısıyla kanun koyucunun gerçek arzusunun açık rızanın değil rızanın tanımını yapmak istediği ifade edilmiştir. (Braun 2018) Bir diğer ifade ile ingilizce olarak "unambiguously" şeklinde ifade edilen hususun aslında KVKK'nın 5. maddesindeki genel nitelikli verilerin işlenmesinde aranan açık rıza kavramını karşıladığı belirtilmektedir. (Braun,

2018) Kanaatimizce bu görüş oldukça isabetlidir. Kanun'un açık rızaya ilişkin madde gerekçesi, Direktif'te yer alan açık rıza tanımı ve nihayetinde gerekçeden farklı olarak KVKK'da yer alan açık rıza tanımı dikkate alındığında bu görüşe katılıyoruz. KVKK bakımından rıza ile açık rıza ayrımının net olarak yapılmadığı ya da Direktif'in 7. maddesinin a bendinde olduğu gibi *"tereddüde yer bırakmayacak açıklıkta"* ifadesinin yer almadığı, tüm bunların karşılığı olarak ise yalnızca "açık rıza" kavramının kullanıldığı açıktır. (Braun, 2018) Doktrinde savunulan bu görüş, KVKK kapsamında genel ve özel nitelikli kişisel verilerin işlenmesi bakımından aranan rıza türünde bir ayrım yapılmamış ve açık rıza olarak ifade edilmekteyse de özel nitelikli kişisel verilerin işlenmesinde yer alan açık rıza kavramının Direktif'in 8. maddesinin 2. fıkrasının a bendinde yer alan "explicit consent" terimini karşıladığını belirtmiştir. (Braun, 2018) Dolayısıyla Direktif'in 7. maddesinin a bendinde yer alan rızanın KVKK'nın 5. maddesinde yer alan genel nitelikli kişisel verilerin işlenmesinde aranan açık rızayı karşıladığını, Direktif'in 8. maddesinin 2. fıkrasının a bendinde yer alan açık rızanın ise KVKK bakımından da özel bir koruma gerektiren 6. maddesinde yer alan özel nitelikli kişisel veriler için aranılan açık rızayı karşıladığını ifade etmektedir. (Braun, 2018)

Ancak her halükârda KVKK bakımından benimsenen açık rıza kavramın Tüzük ile uyumlu olmadığı ve aslında büyük bir kavram karmaşasına yol açtığı ifade edilebilir. Zira hukukumuzda yer alan açık rıza kavramı ne Direktif hükümlerine yer alan rıza kavramını ne de Tüzük hükümlerinde yer alan rıza kavramını tam karşılar nitelikte değildir. Üstelik bu kavram karmaşası yalnızca rıza ya da rızanın unsurları ile de sınırlı değildir. KVKK'nın var olan kavramlara yeni anlamlar yükleyerek bir kavram karmaşası oluştuğu doktrinde eleştirilmektedir. (Braun, 2018) Nitekim kanundaki boşlukların yalnızca mevzuat hükümlerimizle değil AB Hukukuna ait bilimsel görüş ve içtihatlarla doldurulması gerektiğinin altı çizilmiştir. (Braun, 2018) Bizim de katıldığımız görüşe göre, KVKK kapsamında her türlü kişisel verilerin işlenme faaliyetlerine açık rızanın uygulanması uygulamada sorunlara sebebiyet verdiği gibi "rıza" kavramı ile kıyaslandığında pratik de değildir. Diğer bir ifade ile kişisel verilerin işlenmesi noktasında AB hukukunda kabul edilen şekline uyumlu olarak, genel nitelikli kişisel verilerin işlenmesi bakımından zımni verilen rızaların kabulü gereklidir.

Veri Sahibinin Unutulma Hakkı

İlgili veri sahibi kişinin unutulma hakkı, GVKT'nin 17. maddesinde düzenlenmiş, ilgili kişinin en önemli haklarından biridir. Unutulma hakkı, Tüzük kapsamında "Silme Hakkı" (Right to Erasure) ya da "Unutulma hakkı" (Right to be forgotten) şeklinde ifade edilmektedir. Unutulma hakkı, ilgili kişinin kendiyle ilgili verilerinin işlenmesini artık istememesi ve kendisi ile ilgili elde edilen kişisel verilerin muhafaza edilmesinin artık bir amacı kalmadığını, dolayısıyla hukuka uygunluk koşullarının bulunmadığından bahisle kişisel verilerin silinmesi hakkı olarak ifade edilebilir. (Başalp, 2015) Bir diğer ifade ile unutulma hakkı, *"...dijital hafızada kişiye ait fotoğraf, kimlik bilgisi, adres ve diğer kişisel içeriklerin, ilgili kişinin talebi ile bir daha geri döndürülemeyecek şekilde ortadan kaldırılması..."* şeklinde ifade edilmektedir. (Gülener, 2012)

KVKK bakımından unutulma hakkına yer verilmemiş olsa da bu hak hem yargı kararlarına konu olmuş hem de doktrinde oldukça tartışılagelmiştir. Bununla birlikte bu hakka yasal dayanak olacak kanun maddeleri bulunmaktadır. Nitekim KVKK'nın 7. maddesi, kanuna uygun işlenme faaliyetine konu olan verilerin işleme amaçlarının kalmaması halinde re'sen ya da veri sahibinin talebiyle veri sorumlusunca tarafından silineceği, yok edileceği ya da anonimleştirileceğini ifade etmektedir. Kanun m. 11/f.1-e'de kişisel veri sahiplerinin veri sorumlusuna yapacakları bir başvuru ile ilgili verilerin silinmesini ya da yok edilmesini talep hakkı olduğunu ifade etmektedir. Kanun'un 7. maddesine aykırı hareket edenlerin ise m. 17 kapsamında TCK m. 138'e göre cezalandırılacağı ifade edilmiştir.

Veri Sahibinin Veri Taşınabilirliği Hakkı

Veri taşınabilirliği hakkı ("right to data portability") Genel Veri Koruma Tüzüğü'nde öngörülen yeni haklardan biri olup 95/46/EC sayılı Direktif'te düzenlenmemiştir. Veri taşınabilirliği hakkı GVKT'nin 20. maddesinde hüküm altına alınmış olup, işleme faaliyetleri rızaya ya da sözleşmeye dayanan ve işleme faaliyetlerinin otomatik araçlarla gerçekleştirildiği, ilgili veri sahibi kişinin kendiyle ilgili veri sorumlusuna sağlamış olduğu kişisel verileri, geniş ölçüde kullanım alanına sahip, yapılandırılmış ve elektronik sistemler aracılığıyla elde edilen verileri başka veri sorumlusuna aktarma hakkı olarak ifade edilmiştir.

Veri taşınabilirliği hakkına dahil olan veriler, veri sahibinin kendisi ile ilgili kişisel verilerini kapsar. Bir diğer ifade ile anonim ya da veri sahibini ilgilendirmeyen herhangi bir veri kapsam dahilinde olmayacaktır. Bununla birlikte, bir veri sahibiyle açık bir şekilde ilişkilendirilebilen takma adlı veriler, veri taşınabilirliği hakkına dahil kişisel veri olacaklarıdır. Elbette bu hakkın kullanımı GVKT m. 20/f.4 gereği başkalarının hak ve özgürlüklerini olumsuz etkilememelidir. Görüleceği üzere KVKK kapsamında yer almayan bu hakkın ilgili kişisel veri sahibi kişilerin haklarını korumada önemi büyüktür. Dolayısıyla kanaatimiz bu hakkın da KVKK kapsamında düzenlenmesi gerektiğidir.

Uyumlaştırma Kapsamında Uygulanacak İdari Para Cezaları

GVKT'nin yürürlüğe girmesi ile kişisel veri ihlallerinin önüne geçilebilmesi adına yapılan düzenlemelerin caydırıcı olması da hedeflenmiştir. Bu doğrultuda Tüzük hükümlerinin etkin bir şekilde uygulanabilmesi adına yapılan düzenlemelerin yanında uygulanacak idari para cezaları da bu amaç doğrultusunda belirlenmiştir. GVKT m. 83, idari para cezası kesilmesine ilişkin genel şartları ifade etmektedir. GVKT m. 83/f.1'de ifade edildiği üzere, kişisel veri ihlallerinde uygulanacak idari para cezaları her somut olaya göre ayrı olarak değerlendirilecektir.

İdari para cezalarının miktarının belirlenmesinde Tüzük kapsamında ikili bir ayrıma gidildiği görülmektedir. Buna göre, veri sorumlusunun ve/veya işleme faaliyetini gerçekleştiren işleyenlerin yükümlülüklerinin ihlali söz konusu olduğunda 10 milyon Euro'ya kadar ya da bir şirket söz konusu ise, bir önceki mali yılın dünya çapındaki cirosunun %2 sine kadar idari para cezasına hükmedilebileceği GVKT m. 83/f.4'te ifade edilmiştir.

GVKT m. 83/f.5'e bakıldığında ise, işleme faaliyetlerini temel alan ilkeler; ilgili veri sahibi kişinin hakları; Tüzüğün 44 ile 49. maddeler kapsamında üçüncü ülkedeki bir alıcıya ya da uluslararası bir kuruluşa yönelik gerçekleştirdiği veri aktarımları; üye devletlerce kabul edilen yükümlülükler ve denetim makamlarının bir yaptırımı neticesinde ortaya çıkan veri ihlallerinde uygulanacak idari para cezası 20 milyon Euro'ya kadar, bir şirket söz konusu ise, bir önceki mali yılın dünya çapında yıllık cirosunun %4 üne kadar idari para cezasına hükmedilebileceği ifade edilmiştir. Bununla birlikte Tüzük uyarınca uygulanacak idari para cezaları hususunda etkinliği ve

caydırıcılığı sağlamak adına her denetim makamının idari para cezası verme yetkisine sahip olması gerektiği ifade edilmiştir.

Görüldüğü üzere Tüzük kapsamında uygulanacak idari para cezalarının öncelikle etkin olmasına özellikle dikkat edilmiştir. Bununla birlikte denetim makamına da söz konusu para cezalarının miktarını belirlemede oldukça geniş bir yetki verildiği gözlemlenmektedir. Bu anlamda Tüzük, söz konusu denetim makamlarının belirleyeceği idari para cezalarındaki farklılıklardan dolayı 83. maddeyi son derece ayrıntılı düzenlemiştir. Üstelik Tüzük kapsamında idari para cezalarının belirlenme yöntemi de miktar ile sınırlı kalmamıştır. Daha önce yukarıda ifade edildiği üzere idari para cezaları söz konusu ihlale sebebiyet veren şirketlerin dünya çapındaki yıllık cirosuna göre belirli bir miktar dahilinde belirlenmiştir.

KVKK'ya bakıldığında ise idari para cezalarının 18. maddede düzenlendiği görülmektedir. Kanun'un "Kabahatler" başlıklı 18. madde hükmüne bakıldığında, Kanun'un 10. maddesi uyarınca aydınlatma yükümlülüğünü gerçekleştirmeyen veri sorumluları; 12. maddesi uyarınca veri güvenliğine ilişkin yükümlülükleri karşılamayan veri sorumluları ve veri işleyenler; 15. maddesi uyarınca Kurul tarafından kararlarına aykırı hareket eden ve 16. maddesi uyarınca VERBİS'e kayıt ve bildirim yükümlülüğüne uymayan veri sorumluları hakkında idari para cezası verileceği ifade edilmiştir. KVKK m. 18/f.2'de, hakkında idari para cezası uygulanacak kişiler, gerçek kişi olan veri sorumluları ile özel hukuk tüzel kişisi olan veri sorumlularıdır.

Görüldüğü üzere Tüzük hükümlerinin aksine Kanun'un 18. maddesi uyarınca idari para cezalarının miktarı belirlenirken her ne kadar bir alt sınır ve üst sınır belirtilmiş olsa da bu sınırların hangi hallerde geçerli olacağına ya da bu sınırların ne şekilde belirleneceğine ilişkin bir düzenlemeye yer verilmemiştir. Üstelik KVKK m. 18/f.1'e göre verilecek idari para cezaları sınırlı olarak sayılmıştır. Bir diğer ifade ile KVKK'da idari para cezasına hükmedilecek haller aydınlatma yükümlülüğüne aykırılık, veri güvenliğine ilişkin aykırılık, Kurul kararlarına aykırılık, Sicile kayıt ve bildirim yükümlülüğüne aykırılık olarak 4 ana başlık altında sayılmıştır. Buna karşın GVKT'nin 83. maddesi, idari para cezası verilmesine ilişkin veri ihlallerini çok daha kapsamlı olarak ele almıştır. Üstelik Tüzük, idari para cezalarının yalnızca alt ve üst sınır olarak değil aynı zamanda söz konusu ihlale sebebiyet veren şirketlerin yıllık toplam cirosuna göre oransal bir miktarda belirlenmesini öngörmüştür. Kanaatimizce KVKK kapsamında yapılacak uyumlaştırmaların idari para cezalarının gerek alt ve üst sınır bakımından gerekse Tüzük hükümlerinde olduğu şekli ile

kuruluşların yıllık ciro miktarları dikkate alınarak revize edilmesi gereklidir. Zira her şirketin yıllık ciro miktarları farklı olup, cezalarında bu oranlar dahilinde belirlenmesi daha adilane olacaktır.

SONUÇ

ülkemizde ise 2010 tarihli Anayasa değişikliği ile ilk kez kişisel veri koruması yasal bir zemine oturtulmuştur. 95/46/EC sayılı Direktif hükümlerini referans alan KVKK ise 2016 tarihinde yürürlüğe girmiştir. Avrupa'da yaklaşık 40 senedir yasal bir zemine oturan kişisel verilerin korunması konusu, ülkemizdeki taze geçmişine bakıldığında gerekli güncelliği henüz sağlayamamıştır. Özellikle KVKK'nın mülga 95/46/EC sayılı Direktif hükümlerini referans almış olması, içinde bulunduğumuz yılda büyük bir eksiklik olarak görülmektedir. Elbette KVKK yürürlüğe girdiği tarihten bu yana Kişisel Verileri Koruma Kurulu gerek ulusal mevzuatımız açısından eksiklikleri gerekse uluslararası alanda yapılan çalışmaları yakından takip etmiş ve bu alanda düzenli olarak çalışmalarını sürdürmüştür. Bu anlamda ayrıca Kanun hükümlerini esas alan pek çok yönetmelik, tebliğ ve kararnameler de çıkarılmış ve Kanun bakımından eksik kalan hususlar giderilmeye çalışılmıştır. Ayrıca Kişisel Verileri Koruma Kurulu, yaptığı konferans, seminer, sempozyum, panel gibi etkinliklerle toplumda her yaştan bireyin kişisel verilerin korunması anlamında farkındalığa ulaşması için çaba harcamakta, düzenli olarak yayımladığı rehber ve broşürler ile kamuoyunda farkındalık yaratma çabalarını sürdürmektedir.

Ancak Türkiye'nin kişisel verileri koruma anlamında Avrupa ülkelerinde olduğu seviyeyi yakaladığını söylemek oldukça güçtür. Öncelikle KVKK'nın hak ve yükümlülüklere ilişkin getirdiği düzenlemeler oldukça genel bir anlatıma sahip olduğundan, Kişisel Verileri Koruma Kurulu'na ve yargı mercilerine oldukça geniş bir inisiyatif bırakılmaktadır. Mevzuatımız açısından veri sorumlusunun yükümlülükleri, ilgili veri sahibi kişinin hakları, kişisel veri ihlallerine uygulanacak idari yaptırım gibi hususlarda da Kanun'da yapılacak düzenlemelere ihtiyaç duyulmaktadır. Örneğin, veri sorumlularının veri ihlallerine karşı gerekli ve yeterli önlemleri almalarında caydırıcı olmak adına idari para cezalarının miktarı artırılmalıdır. İdari para cezalarının miktarı belirlenirken Tüzük hükümlerinde olduğu gibi alt ve üst sınır çizilmeli, şirketlerin yıllık ciro miktarları dikkate alınarak adilane bir uygulama sağlanmalıdır. İlgili veri sahibinin veri taşınabilirliği hakkı, unutulma hakkı gibi hakları KVKK kapsamında düzenlenmeli, bu hakların hangi durumlarda kullanılacaklarına ilişkin gerekli açıklamalar Kanunda yer almalıdır.

Kişisel veri işleme faaliyetlerinde yer alan "alıcı" ve "üçüncü kişi" kavramları da KVKK'nın tanımlar başlıklı 3. maddesine ilave edilmelidir.

Bilindiği üzere 2019 yılında T.C. Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı 2019-2023 yıllarını kapsayan On Birinci Kalkınma Planını TBMM'ye sunmuştur. On Birinci Kalkınma Planında gerek KVKK gerek GVKT bakımından önemli açıklamalara yer verilmektedir. Dolayısıyla bu plan ile kişisel verilerin korunması ve mevzuat çalışmalarının revize edilmesi ve kişilerin mahremiyet haklarını sağlamayı güçlendirici politikalar uygulanması amaçlanmaktadır. Görüldüğü üzere, ülkemizde kişisel verilerin korunmasına duyulan ihtiyaç karşısında yasal mevzuatımızın Tüzük hükümlerine göre güncellenmesi, yapılacak düzenlemelerin uluslararası alanda kabul gören yaklaşımlar ile uyumlu hale getirilmesi, verilerin depolanması ve yurt dışına aktarımına ilişkin gerekli güncellemelerin yapılması hedeflenmektedir. Bu açıdan bakıldığında, özellikle her geçen gün artan siber tehditlerin sayısı, siber güvenliğin dolayısıyla da veri güvenliğinin korunması anlamındaki önemi de ortaya koymaktadır. Bu noktada yapılacak düzenlemeler ile ülkemizde kişisel verilerin korunması anlamında güncel, çağa uygun yaklaşımların benimseneceği kanaatindeyiz.

Kanunda çalışmalar yapılırken Tüzük maddelerinde yer alan düzenlemeler gerek ülkemizdeki doktrin görüşleri gerek ülkemiz dışında yer alan ortak tartışma konuları dikkate alınarak değerlendirilmeli ve buna göre revize edilmelidir. Örneğin tüzel kişilerin ya da ölen kişilerin kişisel verilerine ilişkin durumların neler olacağına ilişkin daha spesifik yaklaşımlar benimsenmelidir.

KAYNAKÇA VE NOTLAR

Akıncı A. N. (2017). Avrupa Birliği Genel Veri Koruma Tüzüğü' nün Getirdiği Yenilikler ve Türk Hukuku Bakımından Değerlendirilmesi, Çalışma Raporu 6, T.C. Kalkınma Bakanlığı Yayın No: 2968. :14

Akıncı A. N. (2019). Büyük Veri Uygulamalarında Kişisel Veri Mahremiyeti (Uzmanlık Tezi). T.C. Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı, Ankara.: xv

Başalp N. (2015). Avrupa Birliği Veri Koruması Genel Regülasyonu'nun Temel Yenilikleri, Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, Cilt: 21, Sayı: 1. :82

Braun C. (2018). Kişisel Verilerin İşlenmesinde Rıza, Yeditepe Üniversitesi Hukuk Fakültesi Dergisi, 15. :18

Bulut M. (2020). Özel Bir Hukuksal Koruma ve Veri Kategorisi Alanı: Hassas Kişisel Veriler, Ankara Barosu Dergisi. :109

Çekin M. S. (2020). Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku, 3. Baskı, On İki Levha Yayıncılık, İstanbul. : 5

Çelik I. (2022). 6698 Sayılı Kişisel Verilerin Korunması Kanunu ve 2016/679 Sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü Kapsamında Kişisel Verilerin Yurt Dışına Aktarılması, On İki Levha Yayıncılık. :15

Çelikel S. (2021). Kişisel Verilerin Korunması Hukuku Kapsamında Veri Sorumlusu ve Veri Sorumlusunun Yükümlülükleri, Doktora Tezi, Ankara. :74

Develioğlu M. (2017). 6698 Sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü Uyarınca Kişisel Verilerin Korunması Hukuku, On İki Levha Yayıncılık, İstanbul. :36

Dülger M. V. (2021). GDPR'da Bulunan Ancak KVKK'da Yer Verilmeyen Bir Kavram: Ortak Veri Sorumlusu Kavramı ve Güncel Kararlar Işığında Değerlendirilmesi. :1

Dülger M. V. (2019). Kişisel Verilerin Korunması Hukuku, 1. Bası, İstanbul.: 67

Erdos D. (2015). The Emergence of Personal Data Protection as a Fundamental Right of the EU, Cambridge Law Journal, vol. 74, no. 2.: 374-375

Gülener S. (2012) Dijital Hafizadan Silinmeyi İstemek: Temel Bir İnsan Hakkı Olarak "Unutulma Hakkı", TBB Dergisi, S: 102. :226

Helvacı S. (2021). Gerçek Kişiler, Legal Yayıncılık, 9. Bası. :149-150

Küzeci E. (2020) Kişisel Verilerin Korunması, On İki Levha Yayınları, 4. Baskı, İstanbul. :365

Lambert P. (2017). Understanding the New European Data Protection Rules, Taylor & Francis.: 126

Memiş T. (2017). Veri Sorumlusu ve Veri İşleyen Arasındaki İlişkiler ve Sorumluluk Düzeni, Beykent Üniversitesi Hukuk Fakültesi Dergisi, Cilt 3, Sayı 6. :14

Roagna I. (2012). Avrupa İnsan Hakları Sözleşmesi Kapsamında Özel Hayata ve Aile Hayatına Saygı Gösterilmesi Hakkının Korunması Avrupa Konseyi insan hakları el kitapları, Türkçeye Çeviren: Ayşe Gül Alkış Schäling, Avrupa Konseyi, Strazburg.: 12

Şimşek O. (2008). Anayasa Hukukunda Kişisel Verilerin Korunması, Beta yayınları :4

Taştan F. G. (2017). Türk Sözleşme Hukukunda Kişisel Verilerin Korunması, Oniki Levha, 1. Baskı, İstanbul. :34-35

Williamson C. (2021). They're Not Just Long Words: Anonymization and Pseudonymization Protect Data-driven Business, :66, Erişim 6 Temmuz 2021, https://www.protegrity.com/protegrity-blog/theyre-not-just-long-words-anonymization-and-pseudonymization-protect-data-driven-business