

Kişisel Verileri Koruma Kurulunun 17 Temmuz 2019 Tarihli Karar Özetlerine İlişkin Değerlendirme

Doç. Dr. Murat Volkan Dülger*

6698 sayılı Kanun ve konuya ilişkin diğer mevzuatta kendisine verilen görev ve yetkilerini yerine getirmek ve kullanmakla görevli olan Kişisel Verileri Koruma Kurulu, bu doğrultuda kişisel verilerle ilgili haklarının ihlal edildiğini ileri sürenlerin şikayetlerini karara bağlamakla da yetkilidir. Kurul, ayrıca şikâyet üzerine veya ihlal iddiasını öğrenmesi durumunda resen görev alanına giren konularda kişisel verilerin hukuka uygun olarak işlenip işlenmediğini inceleyecek ve gerektiğinde de bu konuda önlemler alacaktır.

Kanun'un yürürlüğe girmesi ve konuya ilişkin diğer hukuki düzenlemelerin oluşturulmasıyla kişisel verilerin korunması hukukuna ilişkin genel bir çerçevenin çizilmesinin ardından Kurul, bu görev ve yetkilerine dayanarak konuya ilişkin olarak somut olayları karara bağlamakta ve bunlardan gerekli gördüğünü kamuoyu ile özet biçiminde paylaşmaktadır. Bu yazının konusunu da Kurul'un 17 Temmuz 2019 tarihinde yayınlamış olduğu farklı tarihlere ait kararları oluşturmaktadır. Kararları, özellikle somut olaydaki soru ve sorunlar ile Kurulun buna karşı bakış açısı bağlamında ele alacak, son olarak görüş ve önerilerimle değerlendirip sonuçlandıracağım.

1. Kurumsal e-posta hizmetinin, Google (gmail) üzerinden yine aynı uzantıya sahip olarak kullanılıp kullanılamayacağı ilişkin Kişisel Verileri Koruma Kurulunun 31/05/2019 Tarihli ve 2019/157 Sayılı Karar Özeti

Gelişen teknolojiyle birlikte bulut bilişim hizmetlerinin daha ekonomik, daha güvenli ve daha kolay kullanılabilir hale gelmesiyle bilhassa özel sektörde ve vakıf üniversiteleri gibi büyük kurumsal yapılarda hem bilgi teknolojileri alt yapısı hem verilerin yedeklenmesi hem de e-posta gibi yollarla iletişimin sağlanması bulut bilişim hizmetleri aracılığıyla yapılmaya başlanmıştır.

Bulut bilişimin en önemli özelliklerinden birisi bu hizmeti verenlerin genellikle "Google" ya da "Microsoft" gibi küresel şirketler olmalarıdır. Bu yapılarının bir sonucu olarak da hem hizmet verdikleri sunucu gibi ürünler hem de çalışanları dünyanın çeşitli merkezlerinde yer alabilmektedir. Örneğin "gmail" ya da "hotmail" uzantılı bir mail adresi kullanıldığında söz konusu mail (ki muhtemelen çok sayıda kişisel veri de içermektedir) dünyanın herhangi bir yerinde hizmet veren bu şirkete ait ya da şirketin kiraladığı bir sunucu üzerinde barınabilmektedir. Bu işleyiş, küresel bilişim teknolojileri şirketlerinin ve bulut bilişim hizmetlerinin kendine has yapısından kaynaklanmaktadır.

6698 sayılı Kanun yürürlüğe girene kadar ülkemizde bu işleyişe ilişkin herhangi bir sorun bulunmamaktaydı. Zira hiçbir kural bulunmadığı için her türlü kişisel veri kaydedilebilmekte, işlenebilmekte ve aktarılabilmekteydi. Kanun yürürlüğü girmesiyle birlikte 9. maddede yurt dışına aktarımın bazı sıkı şartlara bağlanması nedeniyle kafalarda soru işaretleri oluşmaya başladı. Bu sorulardan ilki, bulut bilişim hizmetlerini kullanmanın, özellikle kurumsal elektronik posta hesaplarının bulut bilişim hizmetleri veren yabancı şirketlerden almanın yurt dışına veri aktarımı olarak kabul edilip edilmeyeceğiydi. KVK Kurulu ile yapılan çeşitli görüşlerde ve kendilerine

* Akademisyen / Avukat.

yöneltiren sorularda bu konuda Kurul'a bırakılmış bir takdir hakkının olmadığı, Kanun'un lafzının açık olduğu ve bu tür kullanımların yurt dışına veri aktarımı olarak sayılması gerektiği ifade edilmişti.

İkinci soru ise eğer bu yurt dışına aktarım olarak kabul edilirse, bu hizmetlerin kullanılmasına nasıl devam edilebileceği? Zira bu hizmetler, kullanıcı şirketlerin son derece alıştığı, bütün kurumsal işleyişin üzerine oturtulduğu ve fayda-maliyet analizlerinde son derece olumlu neticelerin alındığı yapılardı.

Ben, bu soruların sorulduğu ve tartışmaların yapıldığı dönemde de, bulut bilişimin yurt dışına aktarım olarak kabul edileceğini, şirketlerin buna karşı bir önlem alması gerektiğini, özellikle bu hizmetleri sunan şirketlerin bu işten önemli derecede kar ettiklerini ve bu kazançlarını kaybetmemeleri için mutlaka bu konuda önlemler almaları gerektiğini defalarca söylemiştim. Ancak bu konuda hiçbir şey yapılmayıp, Kurul'un ya bulut bilişimi yurt dışına aktarım olarak kabul etmemesi ya da ediyorsa güvenli ülke listesini açıklaması ve böylelikle bulut bilişim hizmetlerinin güvenli ülke listesinde bulunan ülkelerden alınarak bir şekilde bu soruna bir çözüm oluşturulması beklentisine girildi.

Ve nihayet "doom day" geldi! Kurul güvenli ülke listesini "kendi elinde olmayan nedenlerle" açıklayamadığı gibi bulut bilişim üzerinde hizmet alımının bir parçası olan elektronik posta hizmeti alımını yurt dışına veri aktarımı olarak kabul etti. Kurul:

"Google firmasına ait G-mail e-posta hizmeti altyapısının kullanılması durumunda gönderilen ve alınan e-postaların dünyanın çeşitli yerlerinde bulunan veri merkezlerinde tutulması söz konusu olacağından, böyle bir durumda kişisel verilerin yurt dışına aktarılmış olacağına ve veri sorumlularının söz konusu uygulamayı 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) "Kişisel verilerin yurt dışına aktarılması" başlıklı 9 uncu maddesi hükümlerine uygun olarak gerçekleştirmesine"

karar verdi. Kurul, kendisine yapılan başvuru yalnızca elektronik postalarla ilgili olmasına rağmen verilerin barındırılmasıyla ilgili görüşünü de araya sıkıştırdı ve bu konuya da açıklık getirdi:

"Server'ları yurt dışında bulunan veri sorumlularından/veri işleyenlerden temin edilen saklama hizmetlerinin de Kanunun 9 uncu maddesi hükümlerine uygun olarak gerçekleştirilmesine"

karar vererek, bu tartışmaya şimdilik son noktayı koydu.

Buna göre bulut bilişim hizmetlerinden yararlanılarak elektronik posta ve/veya veri saklama hizmetinin alınması halinde KVK Kurulu'na göre bu bir yurt dışına veri aktarımı olarak kabul edilmekte ve bunun yapılabilmesi için de 6698 sayılı Kanun'un 9. maddesinde belirtilen yurt dışına veri aktarımının şartlarına uyulması gerekmektedir. O halde ya bu hizmetleri kullanan veri ilgililerinden tek tek açık rıza alınması gerekir ya da hizmeti veren şirketten taahhüt alınarak KVK Kurulu'na izin için başvuru yapılması gerekir. Açıkçası veri ilgililerinden tek tek açık rıza alınmasının çok zor olması, Kurul'un ise karşılıklılık ilkesi sağlanamadığı için onay vermesinin kısa vadede pek de mümkün olmadığını düşünüyorum.

Dolayısıyla bu kararının şirket ve organizasyonlarla hem kurumsal işleyiş (alt yapı değişikliği) hem ekonomik (ek ve daha fazla maliyetlerin ortaya çıkması) hem de verimlilik (çalışanların yeni sistemlere alışması esnasında ortaya çıkacak verim kaybı) açısından önemli etkileri olacağını düşünüyorum. Ve bu yükün altından nasıl kalkılacağını da öngöremiyorum.

Hukuk açısından ise kural, kuraldır! Nitekim Kurul da elindeki malzeme olan kuralı işletmiştir; zaten kural buyken farklı bir şey beklemek de açıkçası safdillik olurdu. O halde ne yapmak gerekir? Son günlerin moda deyiimiyle küreselleşen bilişim teknolojileri alanında “yerli ve milli” çözümler üretmek. Ancak böyle bir ürününün üretilmesinin de özellikle maliyet açısından çok da kolay olmadığını düşünüyorum. Bardağa dolu tarafından bakarsak, bu durum başlangıçta iş dünyasını zorlasa da orta vadede ülkemizin bu alanda gelişmesini ve ekonomik bir değer ortaya çıkmasını sağlayabilir.

Bu konuda kısa vadede üretilcek bir çözüm ise elektronik postada adresinin sonunun kurumsal unvan yapılması ve bunun yerli bir şirketten alınmasıdır; ki bu sıklıkla karşılaştığımız bir durumdur. Ancak genellikle bu hizmeti satan yerli şirketler aslında büyük global şirketlerin ürünlerini belli bir komisyon karşılığı satmakta, kendileri gerçek bir hizmet ve ürün sağlamamaktadırlar. Dolayısıyla böyle bir işleğin olması sonucu etkilememekte, kurumlara bu şekilde uzantı kullanma hakkı verilmekte ancak aslında hizmeti veren arkadaki yabancı şirketin sunucuları üzerinden işlem yapılmaktadır. Bu tür yönetmelere yönelmenin kanunu dolanmaya çalışmak olduğu ve hukuka aykırı olduğu da açıktır.

Sonuç olarak bu karar ülkemizin BT sektöründe bazı taşların yerinden oynamasına neden olacak gibi görünmektedir. Dolayısıyla bu karar daha çok tartışma ve eleştiriye gebedir.

2. Bir varlık yönetim şirketinin ilgili kişiye aynı konu ile ilgili birden çok mesaj gönderimine ilişkin Kişisel Verileri Koruma Kurulunun 31/05/2019 Tarihli ve 2019/159 Sayılı Karar Özeti

Kurulun bir varlık yönetim şirketinin “sms” ile alacak takibine ilişkin vermiş olduğu karar oldukça ilginçtir. Satır başları halinde karadan çıkan sonuçlar şöyledir:

- Veri sorumlusu tarafından, veri ilgisinden alına talep mutlaka 30 gün içinde yanıtlanmalı, sorulan soruların tamamına doyurucu yanıtlar verilmeli ve yanıtın süresinde içinde verildiği ve içeriğin tam olduğu veri sorumlusu tarafından tevsik edilmelidir. Nitekim başvuruda bu hususlar eksiksiz olarak yerine getirildiği için Kurul bu konuda işlem yapılacak bir husus olmadığına karar vermiştir.
- Borçlar Kanunu gereğince alacağın temlik halinde, yeni alacaklının alacağını tahsili için borçlunun kişisel verisi 6698 sayılı Kanunun 5/2-e maddesi gereğince veri ilgisinin açık rızası olmaksızın işlenebilecektir. Dolayısıyla alacağın temlik halinde borçlunun verilerinin işlenmesi bir hakkın tesisi, kullanılması veya korunması için veri işlenmesinin zorunlu olması hukuka uygunluk nedeni kapsamındadır.
- Ancak bilindiği üzere, alacak takibi ya da bir takip olmasa dahi kredi, kredi kartı vs. gibi borçların hatırlatılmasında, vade günü dahi gelmeden borçlulara sürekli ve her kanaldan mesaj gönderilmekte veya arama yapılmaktadır. Hatta bu bazı hallerde tacize varan boyuta ulaşmaktadır. Kurul da bu durumu tespit ederek, bunun bir hakkın kötüye kullanımı olduğunu ve dolayısıyla Kanunun 4/2- a maddesinde yer alan kişisel verilerin işlenmesinin hukuka ve dürüstlük kurallarına uygun olma ilkesine aykırılık oluşturduğunu tespit etmiştir.
- Karardaki önemli bir ayrıntı, Kurul’un buradan yola çıkarak Kanunun 12/1-a maddesinde yer alan kişisel verilerin hukuka aykırı olarak işlenmesini önlemeye yönelik gerekli teknik ve

idari tedbirleri almayan veri sorumlusu hakkında 20.000 TL idari para cezası uygulanmasına karar vermesidir. Buradan çıkan anlam, Kurul'un varlık yönetim şirketi ya da alacak takibi yapan bir avukatlık bürosunun borçluların kişisel verilinin işlenmesini hukuka uygun bulduğudur. Ancak bu işleme taciz boyutuna varmamalıdır. Özellikle varlık yönetim şirketi gibi kurumsal yapılarda bu aramalar ve mesaj gönderme işlemleri belli bir sistematik dahilinde bilişim sistemleri tarafından yapılmaktadır. İşte Kurul da bu hususu dikkate alarak otomatik "sms" gönderim işleminin bu sıklıkta yapılmasının gerekli teknik ve idari tedbirlerin alınmamasına bağlı olduğunu tespit etmiştir. Dolayısıyla bu veya benzer konuda, bireylere bildirimde bulunan veri sorumluları ya da veri işleyenler bunun makul bir sıklıkta olması için gerekli idari ve teknik idari tedbirleri almak zorundadırlar.

Bu kararın, 6698 sayılı Kanunun 5/2-e maddesi gereğince veri ilgisinin açık rızası olmaksızın işlenebileceği hallere ilişkin önemli bir örnek oluşturduğunu, diğer yandan yalnızca alacak takibi açısından değil, günlük yaşamın pek çok alanında, özellikle de reklam hususunda çok sık olarak, tacize varacak şekilde "sms" ya da e-mail vb. gönderimlerinin bir hakka dayanması halinde dahi Kanun'un ihlalini oluşturabileceğini göstermesi bakımından önemli bir karar olduğunu düşünüyorum.

3. Bir anonim şirketin (veri sorumlusu) ilgili kişinin açık rızası dışı elektronik ticari ileti göndermesine ilişkin Kişisel Verileri Koruma Kurulunun 31.05.2019 Tarihli ve 2019/162 Sayılı Karar Özeti

Bu karar da günlük yaşantımızda sıklıkla karşılaştığımız ve Kurul'un daha önce de karar verdiği ve tartışmalara neden olan bir konu ile ilgilidir. Kurul, kararında yerinde olarak reklam amaçlı mesaj gönderilmesini için kişinin cep telefonu numarasının kullanılmasının bir kişisel veri işleme faaliyeti olduğunu belirtmiştir. Bu veri işlemenin yapılabilmesi için de veri niteliğine bağlı olarak Kanun'un 5. ya da 6. maddelerindeki veri işleme nedenlerinden birisinin bulunmasını gerektiğini ifade etmiştir.

Buradan çıkan ilk sonuç reklam göndermek için veri işlenmesi halinde bunun için mutlaka bir açık rızanın varlığının gerekli olmadığıdır. Hatırlanacağı üzere Kurul bu konuda daha önce vermiş olduğu kararında hukuka aykırılığı açık rızanın bulunmayışına dayandırmıştır. Oysa şimdi hem eski kararına atıf yapmamakta hem de yalnızca madde numaralarını belirterek genel bir ifade kullanmamaktadır. Bu ise bana açık rıza dışındaki işleme şartlarından birisinin bulunması halinde ticari reklam gönderilmesinin hukuka uygun kabul edilmesi için bir yol açılıp açılmadığını düşündürmektedir. Nitekim GDPR'da bazı durumlarda veri ilgisinin rızası alınmaksızın ticari reklam göndermenin hukuka uygun kabul edildiği haller bulunmaktadır.

Aslında konunun ilgilileri tarafından bildirgi üzere, ticari elektronik ileti gönderimi konusu Elektronik Ticaret Kanunu'nda yer almakta ve Ticaret Bakanlığı tarafından ayrı bir yönetmelikle düzenlenmektedir. Ancak KVK Kurulu da 2018 tarihinde vermiş olduğu ilke kararında kişisel verilerin korunması hukuku açısından ticari reklam gönderim işleminin hukuka uygun bir biçimde yapılabilmesi için Kanun'un 5/2. maddesine göre açık rıza alınması gerektiğini belirtmiştir. Bunun nedeni ise AB'de ticari reklam iletimine ilişkin düzenleme olan 2002/58/EC Direktifinin, 95/46/EC sayılı Direktif doğrultusunda ve bu Direktif'ten sonra çıkartılmasıdır. Türkiye'de ise söz konusu Direktif'e göre oluşturulan TTK hükümleri ve yönetmelik yürürlüğe girmiş sonrasında ise KVKK

kanunlaşmıştır. Dolayısıyla bunlar birbirinden farklı değil, birbirini tamamlayan düzenlemelerdir. Nitekim KVK Kurulu'nun yaklaşımı da bu yöndedir.

Ancak sonuçta Kurul'un ticari reklam gönderilebilmesi için kişisel verilerin işlenmesi hususunda (i) yalnızca Kanun'un 5/2. maddesinde yer alan ver ilgisinin açık rızası şartının mı gerektiği yoksa (ii) Kanun'un 5. veya 6. maddelerinde yer alan diğer veri işleme şartlarının da bu açıdan bir hukuka uygunluk nedeni olarak kabul edilip edilmediği konusunda bir açıklama getirmesi gerekmektedir. Konu bu açıdan hala muğlaklığını korumaktadır.

4. Spor salonu hizmeti sunan veri sorumlularının, üyelerinin giriş-çıkış kontrolünü biyometrik veri işleyerek yapması ile ilgili Kişisel Verileri Koruma Kurulunun 25/03/2019 Tarihli ve 2019/81 Sayılı Karar ve 31/05/2019 Tarihli ve 2019/165 sayılı Karar Özeti

Belli bir hizmet sunan kuruluşlar ile işyerlerine giriş çıkışlar sırasında işyerleri tarafından birtakım bilgilerin alınması gittikçe yaygınlaşan bir uygulamadır. Bu hemen her veri sorumlusu tarafından yapılmaktaysa da bilgilerin veri sorumlusu açısından zorunlu olup olmadığı, ilgili kişinin açık rızasına ihtiyaç duyup duymadığı ve son olarak ilgili kişinin açık rızasını vermemesi halinde söz konusu kuruluşa girilip girilemeyeceği başlı başına tartışmalı bir konudur. Bu husus şüphesiz özel nitelikli kişisel veriler bakımından daha da büyük bir önem taşır. En basit örneğiyle, bir işyerine girişte ziyaretçi kartının verilmesi için ad, soyad, telefon numarası gibi kimlik ve iletişim bilgisinin alınması kabul edilebilirse de sağlık veya din bilgisinin alınması mümkün değildir.

Bu karar da özel nitelikli veri türü olmasına rağmen gittikçe yaygınlaşan biyometrik veri toplanması ve işlenmesi uygulamaları ele alınmıştır. Ayrıca özel nitelikli olmayan kişisel verilerin de herhangi bir amaca dayanmaksızın ifşa edilmesi hususu değerlendirilmiştir. Somut olayda üyelerinin giriş-çıkış kontrolünde el – avuç okutma sistemine geçmiş olan ve spor salonu hizmeti sunan iki ayrı veri sorumlusu söz konusudur. Bu yetmezmiş gibi, kaydı tutulan üyelere ait vesikalık fotoğraf, son ziyaret saati gibi bilgiler de herkesin görebileceği bir TV ekranına yansıtılmaktadır. Bu bilgilerin güvenli bir şekilde muhafaza edilip edilmediğinde duyulan şüpheler, nihayet Kuruma intikal etmiştir.

Kurul, öncelikle Kanun'da kapsamlı bir biçimde düzenlenmemiş olan biyometrik verinin tanımına ulaşmaya çalışarak içtihat oluşturma mantığı bakımından çok yerinde bir iş yapmıştır. Bu noktada dikkat çekmek istediğim ilk nokta, Kurul'un vermiş olduğu kararlarda ilk kez GDPR hükümlerine atıf yapmış olmasıdır. Böylece Kurul'un GDPR hükümlerini de dikkate aldığını ve karar verirken bu hükümlerden faydalandığını anlıyoruz.

Ulusal mevzuatın Avrupa Birliği ve Avrupa ülkelerinin veri koruma mevzuatlarına kıyasla biyometrik veri gibi teknolojinin gelişmesi ve yaygınlaşmasıyla ortaya çıkan kişisel verilere ilişkin düzenlemeler bakımından eksik olduğu açıktır. Bu durum, biyometrik veri toplanması ve işlenmesine ilişkin teknolojilerin kullanımının burada da yaygınlaşmasıyla beraber gelişmelidir. Bu kararın bu açılardan da önemli olduğunu düşünüyorum.

a. Biyometrik veri

- *GDPR açısından:*

GDPR, biyometrik veriyi “*yüz görüntüleri veya daktiloskopik veriler gibi bir gerçek kişinin özgün bir şekilde teşhis edilmesini sağlayan veya teyit eden fiziksel, fizyolojik veya davranışsal özelliklerine ilişkin olarak spesifik teknik işlemeden kaynaklanan kişisel veriler*” olarak tanımlamaktadır. Bu verilerin işlenmesi Kanun’la benzer olarak daha sıkı şartlara tabi tutulmuştur. Ayrıca üye devletlerin buna ek koşullar getirebileceği de belirtilmiştir.

Kurul, ayrıca Recital 51’den söz etmiştir. Buna göre fotoğrafların işlenmesi doğrudan biyometrik veri olarak nitelendirilmeyip; bunların gerçek bir kişinin benzersiz bir şekilde tanımlanmasına veya doğrulanmasına izin veren belirli bir teknik yöntemle işlendiğinde biyometrik verilerin işlenmesi olarak kabul edilecektir. Dolayısıyla burada biyometrik verinin kişiyi tanımlama ve doğrulama noktasındaki kesinliğine değinilmiştir. Bu kesinlik, şu an için doğrudan eleştirilemese de teknolojinin biyometrik verilerin dahi kopyalanabileceği bir seviyeye geleceğini düşünüyorum. Elbette ki aynı doğrultuda biyometrik veri teknolojisi de gelişecektir. Dolayısıyla bizi biz yapan her bilgi biyometrik verilerde yer almakta ve kaçınılmaz olarak tanımlanmamızı sağlamaktadır.

- *Danıştay açısından:*

Kurul, Danıştay’ın biyometrik kimlik doğrulamasının yaptırılmasını zorunlu tutan ilgili yasal düzenlemenin yürütmesinin durdurulması konulu kararına atıf yapmıştır¹.

Danıştay yürütmeyi durdurmuş olduğu kararında, biyometrik veriyi “*ölçülebilir fizyolojik ve bireysel özellikleri aracılığıyla gerçekleştirilen ve otomatik şekilde doğrulanabilen kimlik denetleme teknikleri*” şeklinde açıklamıştır. Ayrıca parmak izi tanıma, avuç içi tarama, el geometrisi tanıma, iris tanıma, yüz tanıma, retina tanıma, DNA tanıma gibi yöntemlerin bu kapsamda olduğunu belirtmiştir.

Dolayısıyla somut olayda spor salonu tarafından el ve parmak izinin taranması suretiyle yapılan kimlik doğrulama uygulaması, biyometrik verilerin işlenmesi kapsamında değerlendirilmelidir.

b. “Kişisel verilerin işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma” ilkesinin somut olaya uygulanması

Kanun’un 4. maddesi veri sorumlularının gerçekleştirdikleri kişisel veri işleme faaliyetlerinde hiçbir istisnası olmaksızın uymaları gereken usul ve esasları düzenler. Somut olayla ilgisi açısından veri işlemede söz konusu olan kişisel veriler, işleme amacıyla bağlantılı, sınırlı ve ölçülü olmalıdır.

Kurula göre bu ilkedan anlaşılması gereken şudur:

- *İşlenen verilerin belirlenen amaçların gerçekleştirilebilmesine elverişli olması,*
- *Amacın gerçekleştirilmesiyle ilgili olmayan veya ihtiyaç duyulmayan kişisel verilerin işlenmesinden kaçınılmasını gerektirdiği,*
- *Sonradan ortaya çıkması muhtemel ihtiyaçların karşılanmasına yönelik olarak veri işlenmesi yoluna gidilmemesi gerektiği.*

Buna göre işleme faaliyeti ile veri sorumlusunun gerçekleştirmek istediği amaç arasında makul bir denge kurulmalıdır: Veri işleme, amacı gerçekleştirecek ölçüde olmalıdır! Bu amacın ise zaten diğer

¹ 15. Danıştay Dairesi, 2014/4562 E.

bir ilkeye göre “belirli, meşru ve açık” olması gerektiği unutulmamalıdır. Bu kapsamda veri sorumlusu, işleme faaliyetinin gerçekleşmesi için gerekli olmayan kişisel verileri işleyemeyecektir, işleyeceği kişisel veriler amaçla sınırlı ve ölçülü olmalıdır.

Genel ilkelere uygunluğun istisnalara tabi tutulması ise somut olayda bulunan başka herhangi bir durumun ilkelere uyulmamasını hukuka uygun bir hale getiremeyeceği anlamına gelir. Ayrıca özel nitelikli kişisel verilerin işleme şartlarının Kanun’la sınırlı bir şekilde belirlenmiş olduğu ve spor salonuna girişlerde böyle bir işlemeye yasal dayanak oluşturabilecek herhangi bir şartın yer almadığı dikkate alındığında ilgili kişinin açık rızası da Kanun’da olmayan bir işleme faaliyetini meşrulaştırmayacaktır. Örneğin, veri sorumlusunun bu noktada ilgili kişinin açık rızasının alındığına ilişkin savunması hiçbir anlam ifade etmeyecektir. Zira genel ilkeler, bireysel menfaatten çok daha öte veri koruma hukukunun toplumsal yönüne ilişkin olup; verilerin korunmasının felsefesini oluşturur.

Kaldı ki böyle bir durumda açık rıza şartlarının oluştuğunu söyleyebilmek her zaman mümkün değildir. İlgili kişinin açık rızası belirli bir konuya ilişkin ve bilgilendirmeye dayanmakla birlikte özgür iradeyle de açıklanmış olmalıdır. Veri ilgilisi, açık rıza vermemesi halinde herhangi bir yaptırıma veya farklı muameleye maruz kalmayacağından emin olmalıdır ve yaptığı seçimin sonuçları seçim özgürlüğünü kısıtlamamalıdır. Bu nedenle de Kurulun daha önce vermiş olduğu kararlardan da anlaşıldığı üzere bir ürün veya hizmet sunumunun açık rıza verme ön şartına bağlanması açık rıza beyanını sakatlar.

Veri sorumlusunun, üyelik sözleşmesinde el ve parmak tarama sistemi için açık rıza verilmemesi halini haklı fesih sebebi olarak düzenlemesi, kişisel verilerin işlenmesine ilişkin verilecek olan açık rızanın şartla bağlandığı ve açıkça yaptırıma tabi tutulduğu anlamına gelir.

Kurul, bu konuda Danıştay’ın yüz tarama sistemi uygulaması kullanan idare hakkında verilen kararı² ile parmak izi ya da yüz tarama sistemi gibi biyometrik verilerin kamusal alanda da olsa özel hayatın gizliliği kapsamında olduğu ve ileride başka bir şekilde kullanılmayacağına dair güvencenin mevcut olması gerektiğine ilişkin kararlarına³ atıf yapmıştır.

Bunun yanında Madde 29 Çalışma Grubu tarafından konuyla ilişkili olarak hazırlanan raporda⁴ doğrudan somut olaya ilişkin verilen örnekten söz edilmiştir. Buna göre, spor salonu üyelerinin salona girişi ve ilgili hizmetlere erişimi için tüm üyelerin ve personelin parmak izlerinin depolanarak işlenmesi, kulübe erişimi kolaylaştırma ve üyelikleri yönetme ihtiyacı ile orantısız bir işlemdir. Söz konusu ihtiyacın bunun yerine farklı yöntemler kullanılarak giderilmesi mümkündür.

Kurul, yukarıda verilen bilgiler ve kararlar ışığında spor salonuna giriş için el ve parmak izi tarama sisteminin kullanılmasını, kişisel verilerin işlenen amaçla bağlantılı, sınırlı ve özellikle ölçülü olma ilkesine aykırı olarak değerlendirmiştir. Gerçekten, üye kontrolünün yapılması ve güvenliğin sağlanması üye listesinin yapılması, elektronik kart uygulamasının kullanılması ve giriş ve çıkışlarda yeterli güvenlik sisteminin bulundurulması gibi uygulamalarla sağlanabilecekken üyelerin biyometrik verilerine başvurulması hukuka aykırıdır. Bir veri işleme faaliyetinde veri sorumlusu tarafından

² 11. Danıştay Dairesi, 2017/816 E. 2017/4906 (13 Haziran 2017)

³ Danıştay İdari Dava Daireleri Kurulu, 2014/2242 E. 2015/4991 K. (19 Temmuz 2018).

⁴ Article 29 Data Protection Working Party, 00720/12/EN, WP193, Opinion 3/2012 on developments in biometric Technologies., 27 Nisan 2012.

ulařılmak istenen amacın karřılanması iin hangi kiřisel veri trleri ve iřleme amaları ilgili kiřinin kiřisel verilerinin korunması hakkına daha az mdahale anlamına geliyorsa, o veri ve iřleme amacı kullanılmalıdır. Bunun tesinde alınan her veri, belirtilen her ama veri koruma hukukunun ilkelerine aykırı olup, ilgili kiřilerin temel hak ve zgrlklerine haksız mdahale anlamına gelir.

c. Karar

Sonuç olarak Kurulun karar verdiėi yaptırımlar řu řekildedir:

- Kiřisel verilerin iřlendikleri amala baėlantılı, sınırlı ve ll olma ilkesi ile aık rıza alma srelerine ynelik hukuka aykırılıklar sebebiyle idari para cezası,
- Kurulun 21/12/2017 tarih ve 2017/62 sayılı “Banko, Giře, Masa Gibi Hizmet Alanlarında Kiřisel Verilerin Korunması”na iliřkin Kararı erevesinde gerekli teknik ve idari tedbirleri almayan veri sorumlusu hakkında idari para cezası,
- Spor salonunun alternatif yollar saėlaması ve biyometrik veri uygulamasının ivedilikle durdurulması hususunda veri sorumlusunun talimatlandırılması,
- Bugne kadar iřlenmiř olan ve muhafaza edilen biyometrik verilerin, nc kiřilere aktarılanlar da dahil olmak zere Kanun ve Kiřisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Ynetmelik hkmlerine uygun olarak ivedilikle imha edilmesi ynnde veri sorumlusunun talimatlandırılması.

5. İlgili kiřiye ait telefon numarasına kendisine ait olmayan ieriėin gnderilmesi ile ilgili Kiřisel Verileri Koruma Kurulunun 31/05/2019 Tarihli ve 2019/166 sayılı Karar zeti

Son karar, ilgili kiřinin kendisine ait telefon numarasına kendisine ait olmayan ieriėin gnderilmesi ile ilgilidir. Somut olayda kendisine ait olmayan ieriėin gnderildiėi řikayeti, bununla ilgili veri sorumlusuna bařvurmuř ve veri sorumlusu cevabında sz konusu gnderimin personel hatasından kaynaklandığını ve bařka bir aboneye ait giriř yapılırken 1 rakam hatası sonucu kendisine ierik gnderildiėi aıklamasını yapmıřtır. řikayeti, buna karřılık sz konusu ieriėin yeėenine ait olduėunu fark etmiř ancak yeėenin numarasının kendi numarasıyla benzer olmadığını belirtmiřtir. Bu kapsamda yapılan bařvuruda, ilgili kiři veri sorumlusu hakkında gereėinin yapılmasını talep etmiřtir.

Kurul, bu doėrultuda yaptıėı incelemede tek bir hareketle iki farklı veri iřleme faaliyeti sonucunda ihlal yapıldığı sonucuna varmıřtır. Buna gre “řikayetinin yeėenine ait ad, soy ad ve hizmet numarasının řikayetiye gnderilmesi” ve “řikayetiye ait telefon numarası bilgisinin iřleme řartlarına dayanmadan iřlenmesi” kiřisel verilerin hukuka aykırı olarak iřlenmesini nlemek ykmllėine aykırıdır.

Bu kapsamda, Kurul tarafından veri sorumlusu hakkında 50.000 TL idari para cezasının uygulanmasına hkmetmiřtir.

Bu karar alacak tahsilatı iin borluları arayan bir avukat tarafından yapılmıřtır. Maalesef alacakların takibi alanında uzmanlařan avukatlar, borluyla ilgili elde edebildikleri her bilgiyi deėerlendirmekte, asıl borlunun kim olduėuna bakmaksızın, ilgili kiřinin yakınlarına ait elde ettikleri tm kiřisel verileri alacağı tahsil etmek iin kullanabilmektedirler. İřte Kurul ok yerinde olarak byle bir řikyet

üzerine anılan kararı vermiştir. Dolayısıyla alacak takibi yapan avukatların bu konuda daha dikkatli olması gerekir. Nitekim bu karar üzerinde Türkiye Barolar Birliği üyesi olan tüm avukatlara “sms” yoluyla kararı bildirmiş ve bu konuda dikkatli olması gerektiği konusunda uyarıda bulunmuştur.

Sonuç

Daha önce yayınlanan kararlara ilişkin yaptığım değerlendirmelerde de tekrar ettiğim gibi, kişisel verilerin korunmasına ilişkin atılan her adımı, her şeyden önce konuyla ilgili gelişme ve iyileşme gösterecek olması nedeniyle oldukça olumlu karşılamaktayım. Yukarıda incelenen kararlar ise yalnızca bir adım olma niteliğinden dolayı faydalı olmanın çok daha ötesinde nitelik ve netice bakımından önemlidir.

Yukarıda belirtilenleri tekrar etmemek adına bu kısımda değerlendirme konusu kararları içerik olarak tek tek belirtmeyeceğim. Ancak Kurul’un hem karar verme tekniği hem de verilen kararları yayınlama açısından biz uygulayıcılara daha fazla yol gösterici kararlara imza attığını belirtmeliyim. Şikayetlerin değerlendirilmesi aşamasının kapsamlı bir biçimde yapılması ve olayın detaylı bir şekilde ele alınmaya başlanması konuyla ilgili içtihat oluşumuna yardımcıdır. Ayrıca kararlara ulusal ve uluslararası makamların kararlarına da atıf yapılarak varılan kanaatin desteklenmeye çalışılması hukuki değerlendirmenin niteliği bakımından önemlidir. Böylece hem daha detaylı bir değerlendirme yapılabilmekte hem de önceki somut olaylar da göz önünde bulundurularak doğru veya yanlışlar daha iyi görünebilmektedir.

Bununla birlikte özellikle bulut bilişimle ilgili kararın sektörde nasıl bir karşılık bulacağını ve istisnasız bir biçimde uygulanıp uygulanamayacağını merakla beklemekteyim.