Kişisel Verileri Koruma Kurulunun "Kurula Şikâyette Bulunma Süresi" ile "Veri İhlali Bildirimi"ne İlişkin Kamuoyu Duyuruları Hakkında Değerlendirme

Doç. Dr. Murat Volkan Dülger*

Kişisel verilerin korunması alanına ilişkin her geçen gün yeni gelişmelerin yaşandığı günümüzde, son olarak yine Kurul tarafından bir dizi kamuoyu duyurusunu içeren önemli bir adım atılmıştır. Belirtmeliyim ki, bir hukuk dalının oluşması o konuya özgü bir mevzuat düzenlemesi ve teori oluşturulmasından çok daha öte bir meseledir. Bir hukuk dalının oluşması için pozitif hukuk normlarının düzenlenmesi zorunlu bir unsur olmakla birlikte tek başına yeterli değildir. Bunun için daha ziyade konuya ilişkin somut olayların gerçekleşmesi, düzenlenmiş olan hukuk normlarının somut olaylara uygulanması ve bu olaylara ilişkin kararlar verilmesi gerekir. Dolayısıyla konuya ilişkin mevzuatın yanı sıra bu mevzuatın bir uygulama alanı olmalıdır. Böylece hukukun vazgeçilmez ve aynı zamanda da tamamlayıcı bir unsuru olan içtihat kavramı ortaya çıkacaktır. Zira ancak bu şekilde bir hukuk dalının oluştuğundan söz edilebilir.

İşte kişisel verilerin korunması alanı da tam olarak bu noktadadır. Kişisel Verileri Koruma Kanunu'nun yayınlanmasından bu yana özellikle yasal düzenlemeler bakımından atılan adımlar sonucunda kapsamlı bir mevzuat oluşmuştur. Kurul tarafından kendisine yapılan şikâyetler sonucunda ve somut olaylar kapsamında verilen kararlar konuya özgü uygulamanın ve içtihadın oluşmasını sağlamaktadır. Öte yandan Kanun kapsamında yapılan başvuru, şikâyet ve ihlal bildirimlerinin yayınlanması, ortaya somut örneklerin çıkması bakımından önemlidir. Bu nedenle kişisel verilerin korunması bilincinin gelişmesi ve somut olaylara konu edilmesi, nihayet bu olaylar hakkında ilgili mevzuat kapsamında kararlar verilmesi, her şeyden önce adım adım bir kişisel verilerin korunması hukukunun oluşması açısından sevindiricidir.

Bu noktada da mevzuata dayalı teorik bilgi vermekten mümkün olduğunca kaçınarak yalnızca söz konusu kararları değerlendirmeye ve uygulamada nelere dikkat edilmesi gerektiğini açıklamaya çalışacağım. Zira bugüne kadar kişisel verilerin korunması hukukunun ve bu hukukun değindiği hemen her konuda kitap, makale veya değerlendirme yazısı şeklinde yazmaya çalıştım. Bundan sonra, özellikle somut olaylara ilişkin değerlendirmelerimde hiç teorik bilgilere girmeden, doğrudan kararlara geçeceğim.

Yazının konusu olan iki temel husus şu şekilde özetlenebilir:

- Kişisel Verileri Koruma Kurulu 24.01.2019 tarihli ve 2019/9 sayılı Kararıyla bir Kamuoyu Duyurusu yayınlamıştır. Bu duyuruda veri sorumlusuna başvuru ile ilgili düzenlemeler getirilmiştir. Bu kapsamda veri sorumlusuna başvuru süreleri ile ilgili belirsiz noktalar açıklığa kavuşturulmaya çalışılmıştır.
- İkinci olarak, Kişisel Verileri Koruma Kurulu değişik tarih ve sayılı kararlarıyla veri sorumluları tarafından kendisine yapılan veri ihlali bildirimlerinden gerekli gördüklerini yayınlamıştır.

* Akademisyen / Avukat.

Bu iki temel hususu sırasıyla değerlendireceğim.

1. Kişisel Verileri Koruma Kurulunun 24.01.2019 tarih ve 2019/9 sayılı Kararı

6698 sayılı Kanun'un *"Veri sorumlusuna başvuru"* başlıklı 13. maddesiyle ilgili kişinin veri sorumlusuna başvurusu usulü ve süresi düzenlenmiştir. Buna göre, ilgili kişi, Kanunun uygulanmasına yönelik taleplerini yazılı veya Kurulun belirlediği diğer yöntemlerle veri sorumlusuna iletir. Veri sorumlusu ise başvuruda yer alan talepleri talebin niteliğine göre en kısa sürede ve en geç otuz içinde sonuçlandırmalıdır.

Kanun'un *"Kurula şikâyet"* başlıklı 14. maddesinde ise ilgili kişinin Kurula şikâyette bulunma durumu düzenlenmiştir. Buna göre, ilgili kişi, 13. madde kapsamındaki başvurusunun reddedilmesi, verilen cevabın yetersiz bulunması veya süresinde başvuruya cevap verilmemesi hallerinde, cevabı öğrendiği tarihten itibaren otuz gün; her halde başvuru tarihinden itibaren altmış gün içinde Kurula şikâyette bulunabilir.

Ancak bu noktada bazı belirsiz hususlara ilişkin sorular ortaya çıkmaktadır. Bu sorular ve Kurulun söz konusu kararıyla verilen cevaplar şu şekildedir:

- *Veri sorumlusu, ilgili kişinin başvurusuna 30 gün içinde cevap verdiği hallerde Kurula şikâyet süresi nereden başlamaktadır, ilgili kişinin ne kadar süresi vardır?*

İlgili kişi, Kanun'un 13. maddesi kapsamında veri sorumlusuna başvuruda bulundu ve veri sorumlusu söz konusu maddeye uygun olarak 30 gün içinde ilgili kişiye cevap verdi. Bu durumda ilgili kişinin Kanun'un 14. maddesi kapsamında bulunan Kurula şikâyet hakkı, veri sorumlusunun cevap verdiği tarihten itibaren başlar. Diyelim ki, veri sorumlusu ilgili kişiye 15 gün sonra cevap verdi, ilgili kişinin Kurula şikâyet hakkını kullanabilmesi için otuz günlük süresi bu cevabın verildiği tarihin ertesi günü başlar. Öyleyse böyle bir durumda ilgili kişinin toplam süresi 45 gündür. Dolayısıyla ilgili kişinin veri sorumlusuna başvurduğu tarihten itibaren her halde 60 günlük bir şikâyet süresi söz konusu değildir.

Veri sorumlusuna taleplerini iletecek olan ilgili kişilerin bu duruma dikkat etmesi gerekir. Esasen Kanun hükmünden bu durum açıkça anlaşılmaktadır. Ancak her halde 60 günlük bir sürenin söz konusu olması, ilgili kişinin cevap verilsin veya verilmesin, Kurula başvurmak için veri sorumlusuna başvurma tarihinden itibaren 60 günlük süresinin olduğu gibi yanlış bir algıya neden olmuştur. Bu yanlış algı, her ne kadar Kanun hükmüyle zaten anlaşılsa da açıkça altı çizilerek giderilmeye çalışılmıştır.

- *Veri sorumlusu, ilgili kişinin başvurusuna kendisine tanınan 30 günlük süre içerisinde cevap vermemesi halinde ilgili kişinin şikâyette bulunma süresi kaç gündür?*

İlgili kişi, Kanun'un 13. maddesi kapsamında veri sorumlusuna başvuruda bulundu ve veri sorumlusu bu maddeyle kendisine tanınan 30 günlük süre içerisinde cevap vermedi. Bu durumda ilgili kişinin Kurula şikâyet hakkı, 30 günlük süre sonunda başlayacağı için, veri sorumlusuna başvurduğu tarihten itibaren 60 günlük süre içerisinde Kurula şikâyette bulunma hakkı vardır.

Belirtmeliyim ki veri sorumlusunun ilgili kişi tarafından kendisine yapılan başvuruya cevap vermemesi durumu Kanun hükmü ile hiçbir şekilde belirli değildir. Dahası madde açıkça hatalı bir ifade içermektedir. Maddeyle, veri sorumlusunun cevap vermemesi hali, ilgili kişinin cevabı öğrendiği tarihe bağlanmıştır. Ancak verilmeyen bir cevap söz konusu iken ilgili kişi cevabı nasıl öğrenecektir? Aslında idare hukukunda, idareye yapılan başvurunun belli bir süre suskunlukla geçirilmesi halinde, söz konusu başvurunun reddedilmiş sayılacağı ve ilgili dava açma sürelerinin bu sürenin sonundan itibaren başlayacağına ilişkin özellikle 2577 sayılı İdari Yargılama Usulü Kanunu'nda düzenleme bulunmaktadır (m. 10). Ancak KVKK'da yapılan başvuru her zaman idareye olmayıp veri sorumlusu niteliğine sahip gerçek ya da tüzel kişi ya da kamu hukuku veya özel hukuk tüzel kişisi olabilmektedir. Buna göre İYUK hükümlerinin kıyasen burada uygulanması da mümkün değildir.

Dolayısıyla Kurulun bu durumu açıklığa kavuşturması oluşacak yorum farklılıklarını gidermesi bakımından önemlidir. Bununla birlikte kanaatimce bu açıklama yeterli görülmemeli ve Kanun'da yer alan açık ifade hatası giderilmelidir.

- *Veri sorumlusunun, ilgili kişinin başvurusuna kendisine tanınan 30 günlük süre geçtikten sonra cevap vermesi halinde ilgili kişi şikâyet hakkını nasıl kullanacaktır?*

İlgili kişi, Kanun'un 13. maddesi kapsamında veri sorumlusuna başvuruda bulundu ve veri sorumlusu cevap verdi ancak bu arada ilgili maddeyle kendisine tanınan 30 günlük süre geçti. Bu durumda ilgili kişinin şikâyet hakkı esasen yukarıdaki soruyla paraleldir. Veri sorumlusuna cevap vermesi için 30 günlük süre tanındığına göre, cevap vermemesi ile bu süre geçtikten sonra verilen cevap arasında bir fark olmamalıdır. Zira ilgili kişi, veri sorumlusunun ne zaman cevap vereceğini tahmin edebilmek ve verilecek cevabı beklemekle yükümlü değildir. Bu nedenle 30 gün geçtikten sonra verilen cevabın süreye herhangi bir etkisi kabul edilmemiştir. Bu durumda da ilgili kişinin Kurula şikâyet hakkı veri sorumlusuna başvurduğu tarihten itibaren 60 gündür. Özellikle bu durumun açıklığa kavuşturulması faydalı olmuştur.

Aslında idare hukukunun ve idari yargılama hukukunun sürelere ilişkin bu düzenlemeleri hukukçular tarafından gayet iyi bilinmektedir. Ancak bu Kanun toplumun her kesimine hitap ettiği ve bireylerin bir hukukçunun yardımı olmadan da başvuruda bulunmaları sıkça görülen bir durum olduğu için Kurum, yerinde olarak, bir yandan hukuka uygun işlem yapabilmek bir yandan da hak kayıplarına neden olmamak için bu şekilde bir karar almış ve ilan etmek yolunu seçmiştir.

2. Veri İhlali Bildirimine İlişkin Kamuoyu Duyurusu

Kurul, veri sorumluları tarafından kendisine yapılan veri ihlalleri bildirimlerinden dokuz tanesini 24 Ocak, 6 Şubat ve 14 Şubat tarihlerinde kamuoyu duyurusu şeklinde yayınlamıştır. Duyuruların tümü veri ihlali bildirimlerine ilişkindir. Bu duyurularda bildirimi yapan veri sorumluları da ilan edilmiştir.

Veri sorumlusunun veri ihlallerini bildirme yükümlülüğü Kanun'un *"Veri güvenliğine ilişkin yükümlülükler*" başlıklı 12. maddesinin 5. fıkrasıyla şu şekilde düzenlenmiştir:

"İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgilisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir."

Buna göre, veri sorumlusu tarafından hukuka uygun olarak işlenen kişisel verilerin başkaları tarafından elde edilmesi halinde veri sorumlusunun bu hususu veri ilgilisine ve Kurula bildirmesi bir yükümlülük olarak düzenlenmiştir. Veri sorumlusunun bu yükümlülüğünü yerine getirmemesi veri güvenliğine ilişkin yükümlülüklerini ihlal ettiği anlamına gelir ve Kanun'da öngörülen idari para cezası ile sonuçlanır. Ayrıca Kurula, bu bildirimleri gerekli gördüğü takdirde yayınlama yetkisi verilmiştir.

Yukarıda da belirtildiği gibi bu duyuruların tümü veri ihlali bildirimlerine ilişkindir. Bu duyuruların her birini tek tek açıklayarak birbirini tekrar etmek yerine, Kurul'un yayınlamış olduğu bildirilerde hangi hususları göz önünde bulundurmuş olduğuna ilişkin bir ayrımın yapılmasını daha doğru ve faydalı buluyorum. Zira söz konusu duyurular zaten Kurulun resmi sitesinde bulunmaktadır ve burada tekrar etmenin hiçbir anlamı olmayacaktır[1]. Bu nedenle aşağıda duyuruları değil, bu duyurularda göze çarpan hususları ayırarak bir değerlendirmede bulunacağım. Böylece veri sorumlularının dikkat etmeleri gereken hususları belirlemeye çalışacağım.

a. Kurulun hangi veri ihlali bildirimini ilan edeceğine ilişkin gereklilik ölçütü

Kurul yukarıda belirtilen Kanun hükmüyle kendisine yapılan ihlal bildirimlerinden gerekli gördüklerini ilan etmekle yetkili kılınmış ve bu yetkisine dayanarak gerekli olduklarına kanaat getirdiği bildirimleri yayınlamıştır. Bu noktada ilk eleştirim, Kurulun kendisine yapılan veri ihlali bildirimlerinden hangisini ilan edeceği noktasında göz önünde bulundurduğu kriterlerin yeterince belirli olmamasıdır. Kanun hükmü göz önünde bulundurulduğunda, ilan etmiş olduğu bildirimleri gerekli gördüğü anlaşılmakla birlikte, bu gereklilik kanaatinin neye göre yapıldığı belirsizdir. Kurul tarafından *"ilan edilmesi gerekli"* veya *"ilan edilmesine gerek yok"* ayrımı neye göre yapılmaktadır?

Bununla birlikte yayınlanan duyuruların içeriğine bakıldığında veri sorumluları tarafından yapılan bildirime yer verildiği görülür. Bu bildirimlerde yer alan ortak hususlar şüphesiz Kurulun önemli bulduğu ve ilan edilmesi gerektiğini düşündüğü veri ihlali bildirimlerine işaret eder. Öyleyse her ne kadar Kanun hükmüyle hangi bildirimlerin neye göre ilan edileceği açıkça belirlenmiş olmasa da Kurul tarafından ilan edilen bildirimler bir arada ele alındığında hangilerinin gerekli görüldüğü anlaşılabilmektedir. Ancak yine de kamuoyu duyurusu şeklinde yayınlanan veri ihlal bildirimlerinin neye göre gerekli görüldüğünün özet olarak açıklığa kavuşturulması taraftarı olduğumu belirtmeliyim.

b. Bildirimlerde yer alan veri ihlallerinden etkilenen kişi sayısı

Yayınlanan bildirimlere bakıldığı zaman bazılarında söz konusu veri ihlallerinden etkilenen kişi sayısının da belirtilmiş olduğu görülüyor. Öyleyse Kurulun kendisine yapılan bildirimleri ilan etmesinde gerçekleştirilen veri ihlalinin kapsamını göz önünde bulundurduğu sonucuna

[1] Bkz: www.kvkk.gov.tr.

ulaşılabilir. Bu noktada özellikle veri sorumlusuna yönelik olarak gerçekleştirilen siber saldırılar neticesinde verileri elde edilmiş olabilen ilgili kişi sayısının belirtilmiş olması dikkat çekicidir. Kanaatimce Kurul, diğerlerine kıyasla daha fazla veri sahibini etkileme tehlikesi bulunan veri ihlallerine öncelik vererek, bu ihlalleri içeren bildirimleri yayınlamayı gerekli görmüştür.

c. Bildirimlerde yer alan veri ihlallerine konu olan kişisel verilerin niteliği

Bazı bildirimlerde söz konusu veri ihlallerine konu olan kişisel verilerin nelerden oluştuğuna da yer verilmiştir. Belirtmeliyim ki, hukuka aykırı olarak elde edilen kişisel veriler, yalnızca ad ve soyad gibi daha genel ve temel olarak nitelendirilebilecek kişisel verilerden oluşmamaktadır. İlgili kişinin ad ve soyadından başlayıp, tüm kimlik ve iletişim bilgilerinin ihlali söz konusudur. Daha da ötesi özel nitelikli kişisel verilerin yer aldığı sağlık raporu dahi veri ihlaline konu olmuştur. Veri ihlallerinde konu olan kişisel verilerin miktarı, yoğunluğu ve niteliği Kurul tarafından önemsenen diğer bir husus olmuştur. Dolayısıyla büyük sayıda ve önemde kişisel verinin siber saldırı ya da sızıntı sonucu hukuka aykırı olarak üçüncü kişiler tarafından ele geçirilmesi halinde bulunulan ihlal bildirimlerinin Kurul tarafından ilan edildiğini düşünmekteyim.

Görünen o ki, Kurul, belli bir yoğunluk ve önemi dikkate alarak kamuoyuna açıklamada bulunmaktadır. Ancak bu konuda Kurul'un herkes tarafından bilinen ölçütler belirlemesi ve ilan etmesinin daha uygun olacağını düşünmekteyim. Zira uygulamada gördüğümüz bazı örnekler kamuoyuna ilan endişesiyle bazı veri sorumlularının veri ihlali bildiriminden kaçındıkları ve bu konuda olası bir riski üstlendikleri yönündedir. Kamuoyu duyurusu açısından belirliliğin sağlanması bu tür hukuka aykırı uygulamaların da önüne geçebilecektir.

d. Aralarında iş ilişkisi bulunan şirketlerden birinin saldırıya uğraması

Kurul tarafından ilan edilen veri ihlali bildirimlerinde kanaatimce en dikkat çeken ortak husus aralarında iş ilişkisi bulunan veri sorumlularının durumudur. Bildirimlerin büyük bir çoğunluğu bir şirkete yapılan siber saldırıyı içermektedir. Bu şirkete yapılan siber saldırı sonucunda şirket ile arasında iş ilişkisi bulunan birden fazla veri sorumlusu da doğal olarak etkilenmiştir.

Günümüzde şirketler, ticari ilişkilerini yürütebilmek ve geliştirebilmek için belli alanlarda o konuya özgü çözümler getiren başka veri sorumlularıyla çalışmaktadır. Bu durum ihtiyaç olduğu kadar günümüz ticaret yaşamının da bir zorunluluğudur. Böyle bir durumda iş ilişkisi kurulan şirketle iş ilişkisi kurulan konuya özgü ve o konu için gerekli olan kişisel veriler paylaşılacaktır. Örneğin; X online alışveriş mağazasının sipariş takip ve teslim işlemlerini yönetmek amacıyla Y kargo firmasıyla arasında iş ilişkisi kurduğunu düşünelim. Bu durumda X mağazasından alışveriş yapan ilgili kişinin, iletişim ve adres bilgileri Y firmasıyla paylaşılacaktır. Y firmasına yapılan bir siber saldırı sonucunda da X mağazasının müşterileri, dolayısıyla X mağazası da etkilenecektir.

Yayınlanan bildirimlere konu olan somut olaylara paralel olarak, bir araç kiralama şirketi, müşterilerine kiraladığı araçların hasar ve kaza süreçlerini yönetmek amacıyla bir başka şirketle

iş ilişkisi kurulmuştur. İş ilişkisi kurulan şirkete yapılan siber saldırı, çözüm sunduğu birçok veri sorumlusunu da etkilemiştir.

Ancak veri sorumlusu ile yapmış olduğu sözleşme gereğince veri sorumlusu adına veri işleyen ve hatta kendisi de veri sorumlusu olarak kabul edilebilecek olan gerçek ya da tüzel kişilerin KVK Kuruna veri ihlali bildiriminde bulunup bulunmamaları gerektiğine ilişkin bir tartışma bulunmaktadır. Kurul vermiş olduğu kararında *"Veri işleyen nezdinde bulunan kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi halinde, veri işleyenin bu konuda herhangi bir gecikmeye yer vermeksizin veri sorumlusuna bildirimde bulunmasına"* diyerek aslında konuya bir nebze olsun açıklık getirmiştir.

Buna göre veri işleyenlerin veri ihlalini doğrudan Kurula bildirmek gibi bir yükümlülüğü bulunmamaktadır. Kanun'da da belirtildiği üzere, Kanun'dan kaynaklanan tüm yükümlülüklerin muhatabı veri sorumlusudur. Dolayısıyla veri ihlali bildiriminde bulunmak yükümlülüğü de veri sorumlusundadır; Kurul da veri işleyenin bildirimde bulunmak yükümlülüğünün veri sorumlusuna karşı olduğunu belirtmiştir.

Burada tartışmalı kalan tek nokta veri sorumlusu ile veri işleyen kavramlarının aynı kişide birleşmesi konusunda ne olacağıdır? Bu durumda, söz konusu nitelikleri aynı anda taşıyan kişinin kişisel verileri, veri sorumlusu sıfatıyla mı yoksa veri işleyen sıfatıyla mı bulundurduğu ve/veya işlediğine bakılmalıdır. Buna verilecek yanıt, sorumluluğu da belirleyecektir. Ancak unutulmamalıdır ki, veri sorumlusu sıfatını taşıyan pek çok kişi aynı anda aynı veya başka veri setleri için de veri işleyen olarak hareket etmektedirler. Bu ayrımın yapılmasına rağmen, veri ihlaline neden olan veri setleri üzerinde hem veri sorumlusu hem de veri işleyen sıfatları birleşiyorsa, bu durumda artık esas olanın veri sorumlusu olduğu ve ihlal bildiriminde bulunma yükümlülüklerinin bulunduğu kabul edilmelidir. Ancak GDPR'da olduğu gibi (m. 28) veri işleyen ile veri sorumlusunun ilişkisinin ve yükümlülüklerinin açık bir şekilde düzenlemesi daha yerinde bir çözüm olur.

e. Veri ihlal bildiriminin 72 saat içinde yapılması

Bilindiği üzere 6698 sayılı Kanun, AB'nin 95/46/EC sayılı Direktifi esas alınarak hazırlanmıştır. 6698 sayılı Kanun'un yürürlüğe girdiği 7 Nisan 2016 tarihinden yaklaşık iki yıl sonra AB yeni bir düzenleme getirerek söz konusu Direktifi yürürlükten kaldırmıştır. 28 Mayıs 2018'de yürürlüğe giren GDPR, kişisel verileri koruma konusunda öncüsü olan Direktife göre çok daha kapsamlı ve ayrıntılı düzenlemeler getirmiştir.

Veri ihlali bildirimi konusunda 6698 sayılı Kanun'un 12. maddesinin 5. fıkrasında, işlenen kişisel verilerin hukuka uygun olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusunun bu durumu "en kısa sürede" ilgilisine ve Kişisel Verileri Koruma Kuruluna bildireceği düzenlenmiştir. Ancak "en kısa süre" kavramından ne anlaşması gerektiği konusunda bir açıklık bulunmamaktadır. GDPR ise 33. maddesinde bu konuda açık bir düzenleme yaparak veri ihlali bildiriminin 72 saat içinde yapılması gerektiğini düzenlenmiştir.

İşte Kurul da bu konuda GDPR'ı esas alarak bu doğrultuda karar vermiştir. Buna göre *"Veri ihlal bildirimlerinde, Kurula ve ihlalden etkilenmiş kişilere bildirim yapılmasındaki amacın,*

ihlal nedeniyle bu kişiler hakkında ortaya çıkabilecek olumsuz sonuçların bir an önce önüne geçilmesi veya en aza indirilmesine imkan verecek önlemler alınmasını sağlamak olduğu, öte yandan 6698 sayılı Kanuna kaynak teşkil eden Avrupa Birliğinin 95/46/EC sayılı Direktifini ilga eden Avrupa Genel Veri Koruma Tüzüğünde de veri ihlal bildirimlerine ilişkin olarak Direktifin aksine detaylı düzenlemelere yer verildiği dikkate alındığında Kurul tarafından bu konuda alınacak kararlar arasında herhangi bir uyumsuzluğa mahal verilmemesi ve uygulamada bir standartlaşma sağlanabilmesini teminen; Kişisel Verileri Koruma Kurulunun 24.01.2019 tarih ve 2019/10 sayılı Kararı ile; Kanunun 12 nci maddesinin (5) numaralı fıkrasının 'İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgilisine ve Kurula bildirir….' hükmünde yer alan 'en kısa sürede' ifadesinin 72 saat olarak yorumlanmasına ve bu kapsamda veri sorumlusunun bu durumu öğrendiği tarihten itibaren gecikmeksizin ve en geç 72 saat içinde Kurula bildirmesine" karar vermiştir. Buna göre artık ülkemizde de veri ihlali gerçekleştiği andan itibaren 72 saat içinde bildirimde bulunulması gerekmektedir.

Ancak siber saldırı ya da veri sızıntısı sonrası daha fazla saldırı veya sızıntı gerçekleşmesini önlemek ya da adli bilişim yöntemleriyle saldırı ya da sızıntıya ilişkin delilleri toplamak ve gerekli önlemleri almak 72 saatten fazla bir süreyi gerektirebilmektedir. Aslında bu her somut duruma göre farklılık gösteren bir süredir. Bu durumu düşünen GDPR 33. maddesinde *"Denetim makamına yönelik bildirimin 72 saat içerisinde yapılmadığı hallerde, bu bildirimle birlikte gecikme sebeplerine de yer verilir."* düzenlemesine yer vermiştir. Bu hükmü esas alan Kurul da, vermiş olduğu kararda *"Veri sorumlusu tarafından Kurula haklı bir gerekçe ile 72 saat içinde bildirim yapılamaması halinde, yapılacak bildirimle birlikte gecikmenin nedenlerinin de Kurula açıklanmasına,"* ifadesine yer vermiştir.

Bunların yanı sıra aynı kararda veri sorumlusu tarafından veri ihlalinden etkilenen kişilerin belirlenmesinden sonra ilgili kişilere de makul olan en kısa süre içerisinde, ilgili kişinin iletişim adresine ulaşılabiliyorsa doğrudan, ulaşılamıyorsa veri sorumlusunun kendi web sitesi üzerinden yayımlanması gibi uygun yöntemlerle bildirim yapılmasına karar verilmiştir. Görüldüğü üzere burada belli bir süre öngörülmemiş ve "makul süreden" bahsedilmiştir. Makul süre her olay açısından değerlendirilmesi gereken bir ifade olmakla birlikte, Kurula yapılan bildirimden sonra çok fazla zaman beklenmemesi gerektiğini düşünmekteyim.

f. Veri ihlal bildiriminin şekli

Kararla getirilen en önemli yeniliklerden birisi ise Kurula yapılacak bildirimde Kurumun web yer verilen "Kişisel Veri İhlal Bildirim Formu"nun kullanılmasının zorunlu tutulmasıdır. Çok çeşitli biçimlerde bildirim alan ve bunları değerlendiren Kurulun işleyişinin kolaylaşması açısından bunun da yerinde bir adım olduğunu düşünmekteyim. Kararda ayrıca formda yer alan bilgilerin aynı anda sağlanmasının mümkün olmadığı hallerde, bu bilgilerin gecikmeye mahal verilmeksizin aşamalı olarak sağlanması gerektiği belirtilmiştir. Bunun yanı sıra veri sorumlusu tarafından veri ihlallerine ilişkin bilgilerin, etkilerinin ve alınan önlemlerin kayıt altına alınması ve Kurulun incelemesine hazır halde bulundurulması istenmiştir, ki bu da yerindedir.

g. Yurt dışında yerleşik veri ihlali bildirimi

Veri ihlalinin yurtdışında yerleşik veri sorumlusu nezdinde yaşanması halinde, bu ihlalin sonuçlarının Türkiye'de yerleşik ilgili kişileri etkilemesi ve ilgili kişilerin sunulan ürün ve hizmetlerden Türkiye'de faydalanmaları durumunda, bu veri sorumlusu tarafından da aynı esaslar çerçevesinde Kurula bildirimde bulunulmasına karar verilmiştir. Böylelikle adeta GDPR'ın 3. maddesinde düzenlenen bölgesel kapsama benzer şekilde, ihlal yurt dışında gerçekleşse bile, bundan etkilenenlerin Türkiye'de bulunması halinde, KVK Kuruluna bildirimde bulunma zorunluluğu getirilmiştir. Böylelikle 6698 sayılı Kanunun uygulama alanı bir anlamda genişletilmiştir. Kararın bu yönü özellikle yurt dışında bulunan ve Türkiye'de yaşayan kişilerin kişisel verilerini işleyen kişiler tarafından özellikle dikkate alınması gerekir.

h. Veri ihlali prosedürünün hazırlanması

Kurulun söz konusu kararında, *"Veri ihlali gerçekleşmesi halinde veri sorumlusu tarafından kendi nezdinde kimlere raporlama yapılacağı, Kanun kapsamında yapılacak bildirimler ile veri ihlalinin olası sonuçlarının değerlendirilmesi hususunda, kendi nezdindeki sorumluluğun kimde olduğunun belirlenmesi gibi konuları içeren bir veri ihlali müdahale planı hazırlanarak belirli aralıklarla bu planın gözden geçirilmesine"* karar verilmiştir.

Böylelikle daha önce kişisel verilerin işlenmesi; silinmesi, yok edilmesi ve imha edilmesi gibi konularda getirilen ilke ve prosedürlerin belirlenmesi zorunluluğu, veri ihlali halinde izlenmesi gereken prosedür için de getirilmiştir. Özellikle uyum süreci yürüten veri sorumlularının ve bu hususta danışmanlık verenlerin, artık uyum süreçlerine bu başlığı da eklemeleri gerekir. Bunun da olumlu yönde atılmış bir adım olduğu son derece açıktır. Bu tür düzenlemelerin önceden yapılması kriz anında hızlı ve etkili adımlar atılarak zararın en aza indirgenmesini sağlamaktadır.

i. Siber saldırı yapılmış olmakla birlikte veri ihlalinin olup olmadığının belirsiz olması

Yapılan bazı veri ihlali bildirimlerinde siber saldırının yapılmış olduğunda tereddüt olmamakla birlikte bunun sonucunda verilerin kopyalanmış olup olmadığı henüz belirlenememiştir. Kurul, bu bildirimler karşısında konuya ilişkin incelemelerin devam ettiğini belirtmiş ve bu aşamada söz konusu veri ihlallerinin ilan edilmesine karar vermiştir.

Ayrıca veri sorumlusu, siber saldırı yapıldığını tespit etmiş olmakla birlikte, henüz veri ihlali olup olmadığını belirleyemediği bir aşamada da Kurula bildirim yapmak zorunda mıdır? Yayınlananlardan iki tanesinde henüz veri ihlali kesin değilken bildirim yapılmışsa da, yapılmaması veri güvenliğine ilişkin yükümlülüklerin ihlal edildiği anlamına gelir mi? Çünkü Kanun'da veri ihlali olması halinde denilmekte, veri ihlali olduğundan şüphe duyulması halinde denilmemektedir. Kurulun şikâyet üzerine ya da resen inceleme başlatması ve veri sorumlusu tam da bir siber saldırının ve veri sızıntısının olup olmadığını anlamaya çalışırken acaba yaptırım uygulaması doğru mudur?

Bence her iki sorunun da yanıtı hayırdır. Hatta somut durumun özelliklerine göre 72 saat geçmişse dahi, henüz saldırı ve sonuçları tam olarak anlaşılmamış ve buna ilişkin bir rapor çıkartılamamışsa ya da devam eden bir saldırı ile mücadele ediliyorsa Kurul yaptırım

uygulamamalıdır. Kurulun bugünkü yapısı ve genel olarak olumlu ve yapıcı tavrı dikkate alındığında, veri sorumlusunun kasten bir ihmali olmaması halinde böyle bir yaptırımı uygulamayacaklarını düşündüğümü de belirtmeliyim. Tabi bu tamamen benim kişisel görüşümdür.

Sonuç

Yukarıda Kurul tarafından atılan adımlar iki temel başlık olarak ele alınmıştır. Bu başlıklardan ilki, konuya ilişkin Kanun hükmü göz önünde bulundurulduğunda yanlış algılara ve yorum farklılıklarına neden olabilecek bir hususun Kurul tarafından açıklığa kavuşturulmasına ilişkindir. İkinci başlıkta ise, Kurul tarafından kendisine yapılan veri ihlalleri bildirimleri arasında gerekli görünenlerin Kanun ile verilen yetki kapsamında ilan edilmesi ele alınmıştır. Bu kapsamda Kurulun yapılan bildirimler arasında neden söz konusu olan bildirimleri yayınladığı anlaşılmaya çalışılmıştır. Böylece Kurulun, veri ihlallerinde üzerinde durduğu ve önem verdiği hususlar tespit edilmiştir.

Her iki başlık yukarıda içerik bakımından açıklanmış olmakla birlikte, bu gelişmeler genel olarak Kurulun, kişisel verilerin korunması hukukunun oluşması ve yerleşmesi açısından gayretini göstermektedir. Bu nedenle ele alınan konulara özel olarak yukarıda yaptığım açıklamalarla yetiniyorum. Bu noktada ise yalnızca Kurulun, Kanun hükümlerinde yapılan hatalar sonucu oluşan tartışmaları gidermeye çalışmasını ve kendisine yapılan veri ihlali bildirimlerini değerlendirip ilan ederek Kanun ile verilen yetkilerini kullanması karşısında memnuniyetimi ifade etmek istiyorum.

Ayrıca buradan çıkan önemli bir sonuç da Kurulun açık bir biçimde GDPR'ı dikkate alarak karar verdiğidir. Kurulun bu yaklaşımı nedeniyle ülkemiz kişisel verilerin korunması mevzuatının beklenenden daha erken bir zamanda GDPR ile uyumlaştırılması çalışmalarının başladığı ve hatta bunun kısa bir süre içerisinde gerçekleşmesinin şaşırtıcı olmayacağı ortadadır. Bu durumun ise kişisel verilerin korunması hukuku ve ülkemiz açısından son derece olumlu bir gelişme olduğu son derece açıktır.