

KVKK Rejiminin İlk Büyük İhlali: Kişisel Verileri Koruma Kurulu’nun Facebook’a Karşı Hükmettiği 1.650.000 TL İdari Para Cezası

I. Giriş

6698 sayılı Kişisel Verilerin Korunması Kanunu (Kanun) ve konuya ilişkin diğer mevzuatta kendisine verilen görev ve yetkilerini yerine getirmek ve kullanmakla görevli olan Kişisel Verileri Koruma Kurulu (Kurul), bu doğrultuda kişisel verilerle ilgili haklarının ihlal edildiğini ileri sürenlerin şikâyetlerini 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 son olarak, 10 Mayıs 2019 tarihinde yayınlamış olduğu, 2019/104 K. sayılı ve 11.04.2019 tarihli “Facebook kararı” oluşturmaktadır.

II. Facebook Kararı

A. Veri İhlali

Kurul’un kararına konu veri ihlali, kamuoyuna yansıyan ve “Fotoğraf API” olarak adlandırılan 13 Eylül – 25 Eylül 2018 tarihleri arasında bazı üçüncü taraf uygulamalarının on iki gün boyunca yetkisini aşan düzeyde, Facebook üzerinden fotoğraflara erişmiş olabileceği iddiasına dayanmaktadır. Facebook Mühendislik Direktörü Tomer Bar bu açığı, 14 Aralık 2018’de <https://developers.facebook.com/blog/post/2018/12/14/notifying-our-developer-ecosystem-about-a-photo-api-bug/> adresinden “*Geliştirici ekosistemimizin bir fotoğraf API’si hatası hakkında bilgilendirme*” başlığıyla yayımladığı bir açıklamayla bu iddiayı doğrulamıştır.

Açıklamada, Facebook kullanıcı fotoğraflarına erişmek için üçüncü taraf uygulamalara izin veren bir fotoğraf API hatası keşfedildiği, sorunun çözüldüğü ancak bu kusur nedeniyle 13 Eylül - 25 Eylül 2018 tarihleri arasında bazı üçüncü taraf uygulamaların 12 gün boyunca yetkisini aşan düzeyde fotoğraflara erişmiş olabileceği belirtilmiştir. Bunun yanında Facebook, 12 gün boyunca üçüncü parti bir uygulamaya Facebook platformu üzerinden Facebook kullanıcısı tarafından fotoğraflarına erişim izni verildiğinde sadece zaman çizelgesinde paylaştığı fotoğraflara erişim sağlaması gerekirken, açıklanan kusurdan kaynaklı Marketplace veya Facebook Stories’de paylaşılan diğer fotoğraflara da üçüncü parti uygulamaların erişim sağladığı ortaya çıkmıştır. Yani, yazılımcılar

kullanıcıların Facebook'a yüklediği ancak paylaşmadığı fotoğraflara da erişebilmiştir. Açıklanan kusurun, Facebook'un fotoğraf API'sına erişmek için izin alan ve kişilerin fotoğraflarına erişebilen uygulamaları etkilediği ve toplamda 6,8 milyon kullanıcıyı ve 876 geliştirici tarafından oluşturulan 1.500 uygulamayı etkilemiş olabileceği ifade edilmiştir. Facebook son olarak, uygulama geliştiricilerinin, uygulamalarını kullanan ve bu kusurdan etkilenen kişileri belirlemelerine imkân sağlayacak araçların geliştirileceğini belirtmektedir.

B. Kurul'un Görüşü

Kurul öncelikle, Facebook'un veri ihlalinde bildirim yükümlülüğünü yerine getirip getirmediği hususunu incelemektedir. Kurul, Kanun'un 12. maddesinin 5. fıkrasında yer alan, *"İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir."* hükmü uyarınca Facebook tarafından Kurul'a veri ihlalinin bildirilmesi gerektiğini ancak herhangi bir bildirimin yapılmadığı tespit etmektedir. Buna göre, Kanun'un 15. maddesinin ilk fıkrası gereği, *"Kurul, şikâyet üzerine veya ihlal iddiasını öğrenmesi durumunda resen, görev alanına giren konularda gerekli incelemeyi yapar."* Bu hüküm uyarınca Kurul resen inceleme yapma kararı almıştır.

API hatası, Facebook tarafından yapılan inceleme sonrası bu durumu potansiyel bir yazılım bozukluğu olarak rapor edilmiştir. Bu durumda Kurul'a göre, API hatasının 13 Eylül - 25 Eylül 2018 tarihleri arasında on iki gün boyunca gerçekleştiği, bahse konu API hatasına Facebook tarafından zamanında müdahale edilmemesi bu konuda teknik ve idari tedbirlerin alınmasında eksikliklerin göstergesidir.

Kurul, üçüncü taraf bir uygulamaya Facebook platformu üzerinden Facebook kullanıcısı tarafından fotoğraflarına erişim izni verildiğinde sadece zaman çizelgesinde paylaştığı fotoğraflara erişim sağlaması gerekirken, açıklanan ihlalden kaynaklı Marketplace veya Facebook Stories'de paylaşılan diğer fotoğraflara da üçüncü taraf uygulamaların erişim sağladığı ve Facebook kullanıcılarının Facebook'a taslak olarak yüklediği ve henüz paylaşımına açmadığı fotoğraflara da söz konusu üçüncü taraf uygulamaların erişim sağladığı hususlarını kararında göz önünde bulundurmaktadır. Kurul, Facebook'un bu şekilde, kullanıcılarının genel olarak izin vermiş olduğu kapasiteden çok daha fazla sayıda fotoğraflara erişim sağlanmasının; Kanunun m. 12/1 ve m. 4/2-a hükmünde yer alan *"Hukuka ve dürüstlük kurallarına uygun olma"* ve 4/2-ç bendinde düzenlenen *"işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma"* ilkelerine aykırılık teşkil ettiği görüşündedir.

Kurul devamında, Facebook'un üçüncü taraf uygulamaların normalde erişime izin verilmiş olan sayıdan daha fazla spesifik fotoğrafa gerçekten erişip erişemediklerini belirleyemediği ve Facebook'un kendi platformundaki veri akışını kontrol etme noktasında sıkıntılar yaşadığını

gösterdiğini belirtmektedir. Veri akışının Facebook tarafından kontrol edilemiyor oluşu, Kanunun m. 12/1 hükmü ile yer verilen, “*Veri Güvenliği*”ne ilişkin yükümlülüklerine aykırılık teşkil etmektedir.

Facebook platformu uygulamaları daha ilk aşamada “*Arkadaşların, bağlantıların ve birlikte oyun oynadığın diğer kişiler senin oyun hareketlerini görebilecek. Oyunun senin herkese açık profiline ve bu oyunu oynayan tanıdığın kişilere erişimi vardır*” ifadesini kullanarak, kullanıcının arkadaş bilgilerine veya diğer bilgilere kişi istemese bile ulaşabilecek şekilde çalışması hususunda izin almaktadır. İlgili kişilerin uygulamada paylaşmaya izin verecekleri kişisel verilerinin neler olması gerektiği ve yükleme aşamasında gizlilik ayarlarıyla ilgili seçimlere imkân sağlamayarak, kişisel verilerin bu şekilde işlenmesini açık rızaya dayandırmaktadır. Kurul bu durum karşısında, açık rızanın özgür irade ile açıklanması gerektiğinden, ilgili kişinin açık rızasının alınması, bir ürün veya hizmetin sunulmasının ya da ürün veya hizmetten yararlandırılmasının ön şartı olarak ileri sürülmemesi gerektiğini ifade etmektedir.

Açıklanan ihlalin 6,8 milyon kullanıcıyı ve 876 geliştirici tarafından oluşturulan 1.500 uygulamayı etkilemiş ve Türkiye’de bulunan yaklaşık 300 bin kullanıcının veri ihlalinin etkilenmiş olabileceği, karara konu veri ihlalinin Facebook Mühendislik Direktörü Tomer Bar tarafından duyurulmasının böyle bir ihlalin varlığı ve Facebook tarafından kabulü anlamına geleceği belirtilmelidir.

Kurul sonuç olarak, yukarıdaki anlatımlarım çerçevesinde gerçekleşen somut olayın bir veri ihlali oluşturduğu ve Facebook’un bu ihlalin oluşmaması için gerekli teknik ve idari tedbirleri almadığından bahisle, Kanunun 18. maddesi uyarınca 1.100.000 TL idari para cezası uygulanmasına ve söz konusu veri ihlalinin 19 Eylül 2018 tarihinde tespit edilmiş olmasına karşın, Kuruma bildirim yapılmadığından bahisle, 550.000 TL idari para cezası uygulanmasına oybirliği ile karar vermiştir.

III. Kararın Hukuki Değerlendirilmesi

Kişisel verilerin korunmasını düzenleyen neredeyse bütün ulusal düzenlemeler tarafından bu kanunların gereklerinin yerine getirilip getirilmediğini denetlemek üzere veri koruma otoriteleri oluşturulmuştur. 6698 sayılı Kanun ile beraber getirilen en önemli düzenlemelerden biri de Kanun ile verilen görevleri yerine getirmek üzere bir düzenleme ve denetim organının öngörülmesi olmasıdır. Bu amaçla Kişisel Verileri Koruma Kurumu kurulmuş ve Kurum’un esas karar organı olarak Kişisel Verileri Koruma Kurulu göreve başlamıştır.

Makalenin konusunu oluşturan, kısa bir değerlendirmesini paylaştığım Kurul’un söz konusu “Facebook Kararı” da Türk Kişisel Verilerin Korunması Hukuku bakımından yalnızca önemli bir ihlalin tespiti ve Kanun ile öngörülen en yüksek haddten bir para cezasına hükmedilmiş olmasıyla değil, aynı zamanda bir “ilk” olması açısından tarihi bir karardır.

Kararın gerekçesini oluşturan veri güvenliği yükümlülüğü, kişisel verilerin hukuka aykırı olarak işlenmesi ile kişisel verilere hukuka aykırı olarak erişilmesinin önüne geçilerek kişisel verilerin muhafazasının sağlanması ve bireylerin temel hak ve özgürlüklerinin korunmasının temini için veri sorumlularına gerekli zaman, kaynak ve uzmanlığın sağlanarak uygun teknik ve idari tedbirlerin alınması sorumluluğunu yüklemektedir. Veri güvenliğinin sağlanabilmesi için ise veri korunmasına ilişkin ortaya çıkabilecek tüm mevcut risk ile tehditlerin ve risklerin gerçekleşme olasılıkları ile gerçekleşmeleri halinde yol açacağı kayıpların doğru belirlenebilmesi gerekmektedir. Veri sorumlusu ayrıca çalışanlarını eğitmeli ve bu konuda farkındalık çalışmaları gerçekleştirmeli, bir veri güvenliği politikası geliştirmeli ve prosedürlerini belirlemelidir¹.

Facebook, üçüncü parti bir uygulamaya Facebook platformu üzerinden sadece kullanıcıların zaman çizelgesinde paylaştığı fotoğraflara erişim sağlaması gerekirken, açıklanan kusurdan kaynaklı Marketplace veya Facebook Stories’de paylaşılan diğer fotoğraflara da üçüncü parti uygulamaların erişim sağlanması ve Facebook’un üçüncü taraf uygulamaların normalde erişime izin verilmiş olan sayıdan daha fazla spesifik fotoğrafa gerçekten erişip erişemediklerini belirleyememesi şeklinde gelişen olayın, Facebook’un kendi platformundaki veri akışını kontrol edemediği görülmekte ve bu anlamda Facebook yukarıda açıkladığım veri güvenliği yükümlülüğünü açıkça yerine getirememektedir. Facebook “Fotoğraf API” veri ihlalinin ulaştığı boyut göz önüne alındığında, Kanunun m. 18/1-b uyarınca en yüksek had olarak güncellenen 1.200.000 TL idari para cezasına çok yakın bir miktara hükmedilmesi ise gerekli, ölçülü ve yerindedir.

Bunun dışında, Kurul son derece önemli bir hususa işaret etmiş ve Facebook’un uygulamalarının ilk aşamada, yalnızca kapsamı belirsiz bir ifadeye yer vererek ve kişilere seçim imkânı tanımayarak, alacağı izin ile “açık rıza”ya dayanarak kişisel verileri işlemesine de değinmiştir. Kurul son derece isabetli şekilde, açık rızanın özgür irade ile açıklanması gerektiğinden; ilgili kişinin açık rızasının alınması, bir ürün veya hizmetin sunulmasının ya da ürün veya hizmetten yararlandırılmasının ön şartı olarak ileri sürülmemesi gerektiğinin altını çizmiştir.

Hükmün ikinci kısmını ise veri güvenliği yükümlülüklerinden birini oluşturan “*Veri İhlali Bildirim Yükümlülüğü*”nün yerine getirilmemesi oluşturmaktadır. Kanunun 12. maddesinin 5. fıkrası, “*İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.*” hükmünü düzenlemekte ve veri sorumlusuna bildirimde bulunma yükümlülüğü tanımaktadır. Facebook’un yaptığı açıklamayla bu açığı duyurması

¹ **Kişisel Verileri Koruma Kurumu**, Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler), s. 2-11.

ancak Kurul'a ihlal bildiriminde bulunmaması karşısında, Kanunun 18. maddesi uyarınca 550.000 TL idari para cezasına hükmedilmiştir.

Son olarak Kurul'un ihlal bildirimi olmadan, yalnızca Facebook yetkilisi tarafından yapılan açıklamaya binaen ve bunu bir ikrar sayarak, re'sen harekete geçmesine değinmem gerekir. Söz konusu durum her şeyden önce, KVKK'nın uygulaması açısından son derece olumlu bir gelişme olmakla birlikte, her veri sorumlusunu yükümlölüklerine uyması ve gerektiğinde bildirimde bulunmasını konusunda Kurul'un girişimlerinin göstergesidir.

Veri sorumlusu ve veri işleyenler KVKK ile uyumluluk konusunda gerekli adımları atmazlar ise Kurul gereğini yapmakta gecikmeyecektir. Nitekim Microsoft'un da 8 Mayıs 2019 tarihinde veri ihlali bildiriminde bulunması ve Kurum tarafından bunun 10 Mayıs tarihinde kamuoyuna duyurulması da artık büyük şirketlerin, KVKK'nın sahip olduđu yaptırım tehditleri ile birlikte, uyumluluđu sağlama yönündeki ciddi adımlar attığını ortaya koymaktadır.