

ÖZET

Avrupa Birliği'nde uzun bir geçmişe sahip olan kişisel verilerin korunması konusu, 7 Mart 2016 tarihinde Resmî Gazetede yayımlanan 6698 sayılı Kişisel Verilerin Korunması Kanunu ile Türk hukukunda da genel bir kanun şeklinde düzenlenmiştir. Söz konusu Kanun, yine bir AB düzenlemesi olan 95/46 no.lu Kişisel Verilerin İşlenmesi ve Bu Tür Verilerin Serbest Dolaşımına Dair Bireylerin Korunması Direktiften esinlenerek kaleme alınmıştır. Bununla birlikte Kanun'un yürürlüğe girmesinden hemen sonra, 4 Mayıs 2016 tarihinde, 1995 yılında çıkartılan 95/46 no.lu Direktifin revize eden ve teknolojik gelişmelerin mahremiyet ve kişisel verilerin korunması alanlarındaki ihtiyaçlarını karşılamayı amaçlayan Genel Veri Koruma Tüzüğü Avrupa Birliği Resmî Gazetesinde yayımlanmıştır. Her ne kadar 6698 sayılı Kanun, 95/46 no.lu Direktiften esinlenerek kaleme alınmış olsa da, özellikle sağlık verilerinin işlenmesi ve yurtdışına veri aktarımı bağlamında farklı bir sistematik benimsemiş, ayrıca Genel Veri Koruma Tüzüğü ile getirilen değişiklikler de söz konusu Kanun'a yansıtılmamıştır. Bu çalışmanın amacı da 6698 sayılı Kanun'un Avrupa Birliği hukukundaki düzenlemelerden ayrıştığı noktaları tespit etmek, bu vesileyle özellikle yabancı okuyuculara Türk hukuku uygulamasına dair fikir sunmaktır.

Bu çerçevede Kanunun uygulama alanına dair tespitler kısmında Kanunun yer bakımından uygulama alanına ilişkin bir hüküm içermemesine rağmen Kişisel Verileri Koruma Kurumu'nun Türkiye Cumhuriyetindeki gerçek kişilerin kişisel verilerinin Kanuna aykırı şekilde yurtdışında işlendiği hallerde yaptırımlar öngördüğüne dikkat çekilmiştir. Yine Kanunun tanımlar kısmında üçüncü kişi ya da alıcı gibi birçok tanıma yer verilmediği tespit edilmiştir. Kanunun genel ilkeler kısmında Genel Veri Koruma Tüzüğüne nazaran hesap verilebilirlik ilkesinin yokluğu, özellikle veri güvenliğine ilişkin yükümlülükler bakımından farklı bir yaklaşıma sebebiyet vermektedir. İşleme şartları bağlamında ise özellikle Kurul'un açık rıza bağlamında hakkın kötüye kullanılması yasağına aykırılık, açık rızanın hizmet şartı yapılması gibi önemli kararları incelenmiştir. Bir diğer işleme şartı olan meşru menfaat kıstası, her ne kadar Birlik hukukunda önemli bir yere sahip olsa da, Türk hukukunda geniş bir uygulama alanına sahip değildir. Özel nitelikli kişisel verilerin işlenmesi noktasında ise kişisel sağlık verilerinin münhasıran belirli amaçlar ve belirli kişiler tarafından işlenebilmesinin uygulamada sebebiyet verdiği olumsuz sonuçlara dikkat çekilmiştir. Benzer şekilde yurtdışına aktarım mekanizmasında yaşanan zorluklar, taahhütname

süreçlerinin yeteri kadar işlevsel olmaması, açık rızanın gerek özel nitelikli kişisel veriler gerekse yurtdışı veri aktarımı bağlamında istisnadan çok kural haline gelmesi sorunlarına işaret edilmiştir. Veri sorumlusu ile veri işleyen ilişkisinin nasıl şekillendirilmesi gerektiğine dair Kanun, Direktife kıyasla herhangi bir hüküm içermemektedir. Keza alıcı ve üçüncü kişi tanımlarına da yer verilmemektedir. Buna rağmen Kişisel Verileri Koruma Kurulu tarafından çıkartılan rehberler ve uygulama dikkate alındığında bu eksikliğin yine Direktif ve Genel Veri Koruma Tüzüğüne benzer şekilde çözüme kavuşturulduğu belirtilmiştir. Hesap verilebilirlik ilkesinin eksikliği ile Genel Veri Koruma Tüzüğü ile birlikte öngörülen Privacy by Design, Privacy by Default, Veri Koruma Etki Analizi, Davranış Kuralları, Sertifikasyon mekanizmalarının eksikliği de belirtilmiştir. Yine her ne kadar Direktif döneminde mevcut olsa da Veri Koruma Görevlisi müessesesinin Kanunda yer bulmadığı, bunun yerine Kurul duyurusuyla böyle bir sertifikasyon mekanizmasının öngörüldüğü de aktarılmıştır. Çalışmanın son kısmında ise yaptırımlara ilişkin açıklamalara yer verilmiştir.