GÜN + PARTNERS
AVUKATLIK BÜROSU

Verilerin Türkiye'de Depolanması Yönünde Gelişmeler

1. Giriş ve Yönetici Özeti

Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020-2023), Ulaştırma ve Altyapı Bakanlığı tarafından 29 Aralık 2020 tarihinde yayınlandı. Kritik altyapılar ile ilgili bu altyapıların korunması ve mukavemetin artırılması ile ilgili olarak yapılacak çalışmalarda yurt içinde üretilen verilerin yurt içinde kalması gibi konuların kilit bir rol oynayacağı vurgulandı.

Öte yandan, verilerin Türkiye'de depolanması yükümlülükleri açısından 2019/12 sayılı Bilgi ve İletişim Güvenliği Tedbirleri konulu Cumhurbaşkanlığı Genelgesi ("Genelge") 6 Temmuz 2019 tarihinde Resmi Gazete'de yayımlanarak yürürlüğe girmişti. Genelge ile de bilginin dijitalleşme sürecinde meydana gelebilecek ciddi güvenlik risklerinin azaltılması ve etkisiz kılınması ile özellikle kritik türdeki verilerin güvenliğinin sağlanması amaçlanmıştı. Genelge ile düzenlenen en önemli konulardan biri, nüfus, sağlık ve iletişim kayıt bilgileri ile genetik ve biyometrik veriler gibi kritik bilgi ve verilerin Türkiye içinde güvenli bir şekilde depolanması yükümlülüğüdür. Bu bir aktarım yasağı olarak değerlendirilmemekte, daha çok erişilebilirliği temin etmek için ilgili verilerin yedeğinin Türkiye'de de bulunması (depolama) gerekliliği olarak da yorumlanmaktadır.

Her ne kadar Genelge kamu kurum ve kuruluşları ile kritik altyapı niteliğinde hizmet veren işletmelere yönelik olsa da etkisibu kurum ve işletmelere hizmet veren özel hukuk tüzel kişilerini de kapsayacak şekilde uygulama alanı bulacaktır. Dolayısıyla, Genelge'nin verilerin yurt içinde depolanmasına ilişkin yükümlülükleri, kamu kurum ve kuruluşları ile kritik altyapı niteliğinde hizmet veren işletmelerin tedarikçileri ve iş ortakları açısından da dolaylı olarak uygulanmaktadır. Örneğin, Genelge'nin 3. maddesi uyarınca kamu kurum ve kuruluşlarına ait verilerin, kurumların kendi özel sistemleri veya kurum kontrolündeki yerli hizmet sağlayıcılar hariç bulut depolama hizmetlerinde saklanmaması gerekmektedir. Bu kapsamda, Genelge uyarınca herhangi bir kamu kurumuna hizmet sunan özel hukuk kişilerinin bu kuruma sunabileceği bulut hizmetleri açısından yurt içinde bir sunucu bulundurmasının şart olduğu sonucuna ulaşılabilmektedir. Ayrıca Genelge'nin 6. Maddesi uyarınca sosyal

medya ve haberleşme uygulamalarına ait yerli uygulamaların kullanımı tercih edilmesi de düzenlenmiştir.

Bununla birlikte, Genelge'nin uygulanabilirliği ve niteliği hakkında tartışmalar da mevcuttur. Genelge'nin ve Genelge'de belirtilen ilgili tedbirlerin uygulama şeklini ortaya koymak üzere Cumhurbaşkanlığı Dijital Dönüşüm Ofisi ("DDO") tarafından hazırlanan Bilgi ve İletişim Güvenliği Rehberi'nin ("Rehber") güvenlik standartları açısından bir kılavuz niteliği taşıdığı ve bağlayıcı olmadığı da değerlendirilebilmektedir.

Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020-2023) çerçevesinde verilerin yurt içinde tutulması ve aktarımının sınırlandırılmasına yönelik ek düzenlemelerin de gündeme gelebileceği konuşulmaktadır. Bir yandan da Kişisel Verileri Koruma Kurumu'nun kişisel veriler özelinde Kişisel Verilerin Korunması Kanunu'nun yurt dışı aktarımını Avrupa Veri Koruma Tüzüğü'ne kıyasen daha ağır şartlarda sınırlandıran 9. maddesi özelinde çalışma yaptığı da duyulmaktadır. Kurumun Kanun'da düzenlenmeyen ancak kuruma verilen yetki kapsamında Türkiye'de de kabul edilen bağlayıcı şirket kuralları gibi mekanizmalar ve alternatifler üretebilmesi de mümkün olabilir.

Belirli sektörler bakımından verinin yurt içinde depolanması yönündeki mevzuatın yanında, Genelge ile daha genel olarak veri kategorileri bazında getirilen yükümlülük bu yönde özel bir korumanın sağlanmak istendiğine işaret etmektedir. Veri aktarımı, lokalizasyon ve verinin ikameti ile ilgili gelişmelerin Türkiye'de ne yöne evrileceği büyük bir merak konusu.

2. Bilgi Güvenliği'nde Güncel Gelişmeler: Bilgi ve İletişim Güvenliği Rehberi

Genelge'de kamu kurum ve kuruluşları ile kritik altyapı niteliğinde hizmet veren işletmelerde uygulanmak üzere farklı güvenlik seviyeleri içeren Rehber'in DDO Başkanlığı koordinasyonunda hazırlanacağı ve yayınlanacağı belirtilmektedir. Bu kapsamda, Rehber, 24.07.2020 tarihinde onaylanmış ve DDO internet sitesinde yayınlanmıştır.

Rehber, verilerin güvenliğini sağlamak için alınması gereken detaylı eylem ve önlemlerden oluşan kapsamlı bir kılavuz olmasının yanı sıra şirketlerin uyum

çalışmaları sırasında kullanabilecekleri çeşitli ekler ve ayrıntılı şablonlara da yer vermektedir. Öte yandan, Rehber'de bahsedilen çoğu husus, sektörden aldığımız geri bildirimler çerçevesinde genellikle bilinen teknik konular ve idari önlemlerle ilgilidir. Yine de başta kapsamdaki kurum ve işletmecilerin, dolaylı olarak da bu kurum ve işletmecilere hizmet veren üçüncü kişilerin Rehber'de öngörülen zaman çizelgesini göz önüne alması ve iç süreçlerini mümkün mertebede Rehber'e paralel şekilde düzenlemesi önerilmektedir.

Rehber'de yer alan zaman çizelgesinin takip edilmesi açısından Rehber'in yayım tarihinden itibaren 6 ay içerisinde işletmelerin bünyeleri dâhilindeki varlık gruplarını belirlemeleri ve kritiklik derecelendirme ve boşluk analizlerini gerçekleştirmeleri gerekmektedir. Bu analiz sonrasında Rehber'e uyumlu hale gelmek adına izlenmesi gereken adımların yer alacağı uygulama yol haritası da yine ilk 6 aylık süre içinde hazırlanmalıdır. Bu süre, kamu kurum ve kuruluşları ile kritik altyapı niteliğinde hizmet veren işletmeler açısından 31.01.2021 tarihinde sona ermiştir.

Altı aylık sürenin ardından kritiklik derecesi 1 olarak belirlenen varlık gruplarına ilişkin tedbirlerin kritiklik derecelendirme ve boşluk analizinden itibaren en geç 12 ay içerisinde (Rehber'in yayın tarihinden itibaren en geç 18 ay içerisinde), kritiklik derecesi 2 olarak belirlenen varlık gruplarına ilişkin tedbirlerin ise kritiklik derecelendirme ve boşluk analizinden itibaren en geç 15 ay içerisinde (Rehber'in yayın tarihinden itibaren en geç 21 ay içerisinde) ve kritiklik derecesi 3 olarak belirlenen varlık gruplarına ilişkin tedbirlerin ise kritiklik derecelendirme ve boşluk analizinden itibaren en geç 18 ay içerisinde (Rehber'in yayın tarihinden itibaren en geç 24 ay içerisinde) uygulamaya konulması gerekmektedir. Tedbirler ve ne şekilde uygulanacağı konusunda da Rehber'de detaylı düzenlemeler bulunmaktadır.

Genelge'ye ek olarak Rehber'de de verilerin yurt içinde depolanması ve aktarımına temas eden düzenlemeler de bulunmaktadır. Örneğin, Genelge'de kamu kurum ve kuruluşlarına yönelik olarak bulut hizmeti kullanımında 'kamu kurum ve kuruluşlarına ait veriler, kurumların kendi özel sistemleri veya kurum kontrolündeki yerli hizmet sağlayıcılar hariç bulut depolama hizmetlerinde saklanmayacaktır' düzenlemesi yurt dışına veri aktarımına engel olarak da yorumlanabilirken Rehber'de de bulut hizmeti kullanımında 'kritik verilerin yurt

içinde depolandığı ve yurt dışında barındırılmayacağının garanti altına alınması' gerekliliğinden bahsedilmiştir. Bu kamu kurum ve kuruluşlarına hizmet veren tedarikçiler açısından sonuçları olabilecek bir düzenlemedir. Yine operatörler açısından da yurt içi iletişim trafiğinin ülke sınırları içerisinde kalmasının sağlanması, bu trafiğin ve abone kayıtlarının yurt dışına çıkarılarak tekrar yurt içine yönlendirilmesinin engellenmesi ile bulut ortamı güvenliğini temin etmek üzere sunuculara erişimde trafiğin yurt içinde kalmasına yönelik tedbirlerin uygulanması gerektiği vurgulanmaktadır.

Genelge, ayrıca kurum ve kuruluşların, Rehber'in uygulanmasına ilişkin denetim mekanizmalarını oluşturmasını ve yılda en az bir defa uygulamayı denetleyemesini öngörmektedir. Denetim sonuçlan ile yapılan düzeltici ve önleyici faaliyetler, Rehber'de belirtilen usul ve esaslara göre bir rapor halinde DDO'ne iletilmelidir. Ne var ki, yayınlanan Rehber'de bahsi geçen denetim faaliyetlerinin DDO'nin internet sitesinde yayınlanacak Bilgi ve İletişim Güvenliği Denetim Rehberi esas alınarak yürütüleceği belirtilmiş, ancak henüz bir denetim rehberi yayınlanmamıştır.

3. Aykırılık Halinde Uygulanabilecek Yaptırımlar

Genelge'de tüm kamu kurum ve kuruluşları ile kritik altyapı hizmeti veren işletmelerde yeni kurulacak bilgi sistemlerinin Rehber'e uygun olması zorunluluğundan bahsedilmiştir. Ayrıca DDO, söz konusu tedbirlere uyulmaması nedeniyle bir zafiyet oluşması durumunda hâlihazırda ilgili mevzuatta belirlenen yaptırımların geçerli olduğunu belirtmektedir. Genelge ve Rehber, özel olarak ayrı bir yaptırım öngörmemektedir, zaten bu şekilde bir yaptırımın düzenlenmesi de hukuken beklenmemektedir.

Kamu kurum ve kuruluşlarında çalışan memurlar açısından Türkiye Cumhuriyeti Anayasası'nın, 657 sayılı Devlet Memurları Kanunu'nun uygulama alanı bulabileceği açıktır. Memurların ve kamu görevlilerinin bu kapsamda hem devlete hem de kişilere karşı sorumlulukları olabilir. Bu husus, kamu ve kurumlarının iç süreçlerini organize etmelerini ve alacağı hizmetlere yönelik olarak tedarikçilerden bekleyebileceği taahhütleri etkileyebilir.

Kritik altyapı işletmeleri özelinde ise tabi oldukları mevzuat kapsamında bilgi güvenliği ile ilgili yaptırımlar uygulanabilir. Dolayısıyla düzenleyici ve denetleyici kurumların, bilgi güvenliği konusunda Genelge ve Rehber'i dikkate alarak ikincil mevzuatlarında bazı değişiklikler yapabilmesi de gündeme gelebilir. Bunun yanında Genelge ve Rehber'e uyuma yönelik yaptırımlar genel olarak da ayrıca düzenlenebilir. İlgili kritik sektörün düzenlenmesi ve denetlenmesinden sorumlu düzenleyici ve denetleyici yetkili kurumlar veya DDO tarafından gerçekleştirilebilecek bir denetimde Genelge ve Rehber'e bir aykırılığın söz konusu olması halinde ilgili kurumlarca hazırlanmış bilgi güvenliğine ilişkin yönetmelikler ve diğer ilgili mevzuat hükümleri uyarınca idari yaptırımlar uygulanabileceğinin de altı çizilmelidir.

Ayrıca, Genelge'de Rehber'in ihtiyaçlar, gelişen teknoloji, değişen şartlar ile ulusal siber güvenlik stratejisi ve eylem planlarında yapılabilecek değişiklikler göz önünde bulundurularak güncellenebileceği de belirtilmektedir.

Bazı kritik sektörler açısından ise Genelge ve Rehber'de düzenlenen hususlar yeni değildir. Örneğin, elektronik haberleşme operatörlerinin tabi olduğu mevzuat açısından olası yaptırımlara dayanak teşkil edebilecek hükümler 5809 sayılı Elektronik Haberleşme Kanunu, Bilgi Teknolojileri ve İletişim Kurumu İdari Yaptırımlar Yönetmeliği ve Kamu Kurum ve Kuruluşları ile Gerçek ve Tüzel Kişilerin Elektronik Haberleşme Hizmeti İçinde Kodlu veya Kriptolu Haberleşme Yapma Usul ve Esasları Hakkında Yönetmelik içerisinde yer alabilmektedir ve bu düzenlemeler ile Bilgi Teknolojileri ve İletişim Kurumu'nun diğer ikincil düzenlemeleri de Genelge ve Rehber'e paralel ya da benzer veri güvenliği önlemlerinin alınmasını zorunlu kulmaktadır. Bu bakış açısıyla, elektronik haberleşme işletmelerinin mevcut uygulamaları da genellikle Genelge ve Rehber'in öngördüğü tedbirlere uygundur. Yine de gelişmelerin takip edilmesi yararlı olacaktır. Örneğin, Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğin Korunmasına İlişkin Yönetmelik 4 Haziran 2021 tarihinde yürürlüğe girecek şekilde değiştirilmiştir. Yeni yönetmelik, eski yönetmeliğin aksine kişisel verilerin kural olarak yurtdışına aktarımını engellememektedir ve açık rıza ile aktarımı mümkün kılmaktadır. Genelge'de haberleşme hizmeti sağlamak üzere yetkilendirilmiş işletmecilerin Türkiye'de internet değişim noktası kurmakla yükümlülüğü olduğu belirtilmekte yurt içinde değiştirilmesi

gereken yurt içi iletişim trafiğinin yurtdışına çıkarılmamasına yönelik tedbirler alınacağı düzenlenmektedir. Bu düzenleme, kritik veriler ile ilgili olan yurt içinde depolama yükümlülüğünün ötesinde yurt dışına aktarımı da sınırlandıran bir düzenleme olarak görülebilmektedir. Öte yandan yeni Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğin Korunmasına İlişkin Yönetmelik'te milli güvenlik gerekçesiyle trafik ve konum verilerinin yurt dışına çıkarılmamasının esas olduğu belirtilse de trafik ve konum verilerinin dahi yurt dışına aktarımının söz konusu olabileceği durumlar da yok sayılmamıştır. İşletmecilerin trafik ve konum verilerinin üçüncü taraflara aktarımının söz konusu olduğu durumlar için ilgili üçüncü tarafın yurt dışında olması halinde verinin aktarılacağı ülkenin adını da abonelere açıklayarak abonenin açık rızası ile verileri yurt dışına da aktarabileceği düzenlenmektedir. Elektronik haberleşme işletmecilerinin Genelge ve Rehber'in kapsamında olduğu açıktır, bu çerçevede Genelge ve Rehber'in bu işletmeciler özelinde Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğin Korunmasına İlişkin Yönetmelik ile birlikte nasıl uygulanacağı da yakın şekilde takip edilmelidir.

Yine kritik sektör olarak belirlenmiş bir diğer sektör olan finans sektöründe de bilgi güvenliği açısından Genelge ve Rehber'e uygun bir güvenlik düzeyinin temin edilmediği durumlarda gerek Bankacılık Düzenleme ve Denetleme Kurumu'nun Bankaların İç Sistemleri ve İçsel Sermaye Yeterliliği Değerlendirme Süreci Hakkında Yönetmelik ve Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik gerekse de Finansal Kiralama, Faktoring ve Finansman Şirketlerinin Bilgi Sistemlerinin Yönetimine ve Denetimine İlişkin Tebliğ, ilgili işletmelere uygulanabilir. Nitekim diğer kritik sektörler olan enerji, ulaştırma ve su yönetimi sektörleri açısından da bakanlıklar ve ilgili düzenleyici kurum ve kuruluşlar nezdinde bu sektörlerde hizmet veren yetkili özel hukuk kişilerinin de Genelge ve Rehber'e uygun olarak bilgi güvenliği süreçlerini düzenlemeleri yararlı olacaktır. Zira, bu sektörlerde de genel olarak bilgi ve veri ile altyapı güvenliğine yönelik ikincil düzenlemeler Genelge ve Rehber'e aykırılıkları halinde yaptırım uygulanmasına neden olacak şekilde yorumlanabilir.

Son olarak, her ne kadar hem Genelge'nin hem de Rehber'in kamu kurumları tarafından uygulanıp uygulanmadığı konusunda bazı şüpheler olsa da

bakanlıkların konudan haberdar olduğu ve kamu kurumlarının tedarikçilerinin bu düzenlemeye uyumunu sağlamaya yönelik bazı önlemler alabildikleri görülmektedir. Örneğin, Genelge ve Rehber'in doğrudan uygulanmadığı özel hukuk tüzel kişileri de kamu ve kuruluşlarına verdikleri hizmetler kapsamında bu tedbirlere uyumlarını taahhüt ettikleri sözleşmesel yükümlülükler altına girebilmektedir. Yaygın bir uygulamaya başladığını gözlemlediğimiz üzere böyle bir taahhüdün ihale süreçleri içerisinde verilmesi, kritik altyapı niteliğinde hizmet vermeseler dahi özel hukuk kişilerinin ve şirketlerin Genelge ve Rehber'e uygun hareket etmedikleri mal ve hizmet tedariki süreçlerinde ihalelerden yasaklanması sonucunu dahi doğurabileceği için ciddi bir zarara yol açabilir.

Sonuç

Genelge ve Rehber'in özel hukuk kişileri üzerindeki bağlayıcılığı ise uygulama ve doktrinde oldukça tartışmalıdır. Genel olarak genelgeler, idare tarafından, alt idari birimlere ya da idare edilenlere yönelik olarak, üst hukuk kuralının nasıl yorumlanabileceğini ya da üst hukuk kuralının ne şekilde uygulanması gerektiğini ifade eden düzenlemelerdir. Çeşitli Danıştay kararlarında da ifade edildiği üzere genelgelerin hukuk âlemine yeni bir unsur katmaması, mevcut kuralları açıklayıcı nitelik taşıması ve en önemlisi de ilgililerin sübjektif haklarını, menfaatlerini ihlal etmemesi daha uygundur.

Genelge ve Rehber'in veri lokalizasyonu ya da veri aktarımını sınırlandıracak şekilde geniş kapsamlı olarak uygulanması bu çerçevede farklı tartışmalara da yol açabilecektir. Örneğin, kanun mertebesindeki bir düzenleme olan Kişisel Verilerin Korunması Kanunu kapsamında yurtdışı aktarımı belirli şartların varlığı halinde ya da her durumda kişisel verisi işlenen kişinin açık rızası ile mümkünken bu düzenlemenin sağladığı imkanların Genelge ya da Rehber'in uygulanması yoluyla sınırlandırılması, Genelge ve Rehber'in geçerliliğini ve yine bu kapsamda uygulanabilecek yaptırımların hukuka uygun olup olmadığını da tartışmaya açacaktır.