

Konuşmadığımız şeyler var: Türkiye, AB Veri Güvenliği Reformuna hazır mı?

AB veri güvenliği standartları gereği, AB'nin üçüncü ülkelerle karşılıklı veri paylaşımında bulunabilmesi için üçüncü ülkedeki ilgili düzenlemelerin yeterli seviyeye erişmesi; özel durumların mevcudiyeti veya geçerli önlemleri içeren ikili anlaşmaların düzenlenmiş olması aranıyor. Bu durum, AB'deki paydaşlarıyla karşılıklı veri etkileşimine girmeyi öngören Türk şirketler için de geçerli

Ahmet Ceran İKV Uzmanı

AB ülkeleri ve kurumları, küresel ölçekte veri güvenliği standartlarını yeniden tanımlayacak AB Genel Veri Koruma Tüzüğü'nün (GDPR) 25 Mayıs'ta yürürlüğe girmesine hazırlanırken, AB teknoloji çevreleri zamana karşı yarış içerisinde; gergin, heyecanlı ve kaygılı. Çünkü GDPR açıkça ortaya koyuyor: Tarafların gözünün yaşına kati surette bakılmayacak. Veri ihlali halinde, AB Üye Devletlerindeki veri kontrolörleri, 20 milyon Avro veya hizmet sağlayıcısının küresel gelirinin yüzde 4'üne varan miktarlarda cezaya çarptırılacak. Aslında Birlik ile doğrudan yakın siyasi, ekonomik ve sosyal ilişki içerisindeki aralarında Türkiye'nin de bulunduğu üçüncü ülkelerin de benzer heyecanı taşıması gerekirken, fazlasıyla "asayiş berkemal" bir atmosferin hâkim olması çok sağlıklı değil.



Ahmet Ceran

AB veri güvenliği standartları gereği, AB'nin üçüncü ülkelerle karşılıklı veri paylaşımında bulunabilmesi için üçüncü ülkedeki ilgili düzenlemelerin yeterli seviyeye erişmesi; özel durumların mevcudiyeti veya geçerli önlemleri içeren ikili anlaşmaların düzenlenmiş olması aranıyor. Bu durum, AB'deki paydaşlarıyla karşılıklı veri etkileşimine girmeyi öngören Türk şirketler için de geçerli. Basit ifadeyle, verinin yeni petrol olarak nitelendirilmeye başladığı dijital dönüşüm çağında kamu, özel, sivil toplum fark etmeden Türkiye'deki bütün sektör

oyuncularının AB ile veri odaklı işbirliği yapabilmesi ancak GDPR ile uyumlu, AB standartlarında iç düzenlemelerle mümkün hale gelecek. Peki, AB neden bu kadar sert ve yönlendirici bir tutum sergiliyor?

GDPR, AB'nin dış politika etki aracına mı dönüştü?

Mülteci krizi, küresel terör, mali zorluklar, Brexit, yükselen popülizm derken tarihinin en karmaşık sınamalarıyla boğuştuğu bir dönemde dijital dönüşüm ve Dijital Tek Pazar stratejileri, Birli-



AB veri güvenliği ihlalinde hizmet sağlayıcıya 20 milyon Euro ceza kesebilecek

ğin en başarılı yürüttüğü atılımlar arasında. Dijital Tek Pazar stratejisini bütün hukukî düzenlemeleriyle birlikte etkin şekilde hayata geçirmesi durumunda AB ekonomisinin yıllık 416 milyar Avro katma değere sahne olması ve yüzbinlerce yeni istihdam sağlaması bekleniyor. Bu yenilenme çabasının merkezinde ise veri güvenliği reformu, yani GDPR'ın AB çapında benimsenmesi yer alıyor.

Mesele, bir noktadan sonra, AB'nin etkileşim içerisinde olduğu ülkelerin tamamı üzerinde uygulamaya çalıştığı bir dış politika etki aracına dönüşmüş durumda. Böylelikle, küresel sistemin kaotik ve çok kutuplu, belirsizliklerle bezeli son döneminde ileri seviye AB değerlerini ve standartlarını yansıtabilecekleri, uygulatabilecekleri; yönlendirici ve kural koyucu rol üstlenebildikleri bir alan açılmış oldu. AB, konuya hak temelli ve vatandaş-

ların gizliliğini koruma odaklı perspektifle yaklaştığı için de aslında bu dönüşüm kritik ve değerli. Sert tutumları da bu yüzden. Öyle ki AB, tarihsel ve kültürel açıdan en yakın müttefiki ABD'ye de dayatmacı bir politika uyguluyor, aday ülkelere de, yükselen küresel güçlere de, arka bahçesindeki Kuzey Afrika ülkelerine de.

AB, en güncel bilgiler ışığında Andora, İsviçre, İsrail, Man Adaları, Arjantin ve Faroe Adaları gibi birbirinden farklı nitelik ve ölçekteki ülkelerin veri güvenliği standartlarını yeterli kabul etmiş durumda. Japonya ve Güney Kore ile ise müzakereler devam ediyor. Stratejik olarak, AB tarafından büyük ölçekli ticaret müzakerelerinde de hak temelli boyutuyla veri güvenliği meselesi sıkça gündeme taşınıyor. Dolayısıyla Türkiye ile Gümrük Birliği'nin modernizasyonu sürecinde, konunun gün yüzüne çıkması şaşkıncı olmayacak. Ama Türkiye açısından, konunun asıl hayati önem taşıdığı boyutlardan biriyle, Türkiye-AB vize serbestliği diyalogunda karşılıyoruz. Avrupa Komisyonu'nun öne sür-

AB, en güncel bilgiler ışığında Andora, İsviçre, İsrail, Man Adaları, Arjantin ve Faroe Adaları gibi birbirinden farklı nitelik ve ölçekteki ülkelerin veri güvenliği standartlarını yeterli kabul etmiş durumda. Japonya ve Güney Kore ile ise müzakereler devam ediyor. Stratejik olarak, AB tarafından büyük ölçekli ticaret müzakerelerinde de hak temelli boyutuyla veri güvenliği meselesi sıkça gündeme taşınıyor



düğü üzere, Türk vatandaşlarına vizesiz Avrupa kapılarının açılabilmesi için ileri standartlarda bir veri güvenliği mevzuatının oluşturulması, en öncelikli kriterlerden.

2017'nin sonunda ilgili bakanlıklar tarafından kalan kriterlerin karşılanması yönünde hazırlanan ve bu yılın Şubat ayı başında Türkiye'nin Brüksel'deki daimî temsilciliği tarafından Komisyonun Birinci Başkan Yardımcısı Frans Timmermans'a sunulan pozisyon belgesinde de veri güvenliği reformuna ilişkin taahhütlerin yer alması öngörülüyor. Öte yandan, Türk kolluk ve göç yönetim birimlerinin AB'deki paydaşlarıyla ileri seviye operasyonel bilgi/istihbarat paylaşımı da ancak veri güvenliği alanında atı-

lacak adımlarla mümkün. Dolayısıyla 2018 yılında veri güvenliği meselesinin Türkiye'nin de gündeminde olmasını bekleyebiliriz.

Türkiye'de veri güvenliğine yeterli önem gösterilmiyor
Biraz da Türk iş çevrelerinin konuyu hangi oranda dikkate aldığına bakmak gerekiyor. Neticede her gün Sanayi 4.0 fenomenine ilişkin sayısız seminer ve bilgilendirme etkinliğinin düzenlendiği, fütüristik dijitalleşme fotoğraflarının sosyal medyada cirit attığı bir dönemde, konunun "daha az havalı" bu boyutuna ilişkin farkındalık çok önemli. Lakin bu farkındalığın AB'de bile yeterli oranlara ulaşamadığı dikkate alındığında Türkiye'de

hal ve gidişin sıfırın altında olması çok da şaşkınlıkla karşılanmamalı.

International Association of Privacy Professionals (IAPP) tarafından AB ve ABD merkezli 500 veri güvenliği uzmanıyla gerçekleştirilen anket çalışmasına göre, her dört AB merkezli şirketten birinin (yüzde 28) Mayıs 2018'de GDPR'a hazır olması beklenmiyor. TÜSİAD tarafından Boston Consulting Group işbirliğiyle hazırlanan Türkiye'nin Sanayide Dijital Dönüşüm Yetkinliği başlıklı rapor ise Türkiye'de çok daha vahim bir tabloyu gözler önüne seriyor. 2017 yılında Türkiye'deki şirketlerin yüzde 95'inin dijital dönüşüm konusuna ilgi gösterdiğini ortaya koyan rapora göre veri güvenliği eksikliği Türk şirketler için dijitalleşme önündeki ilk 5 tehdit arasında yer almıyor. Bu, bir bakıma Türkiye'de henüz iş dünyasının geneline yayıldığında, veri güvenliği konusuna yeterli önemin verilmemesini gösteriyor. Dolayısıyla şirketlerin konuya ilişkin farkındalığının artırılmasında meslek kuruluşlarına, odalar ve borsalarla birlikte teknoloji odaklı sivil toplum kuruluşlarına önemli rol düşüyor.