Yönetim Kurullarının Yeni Gündemi : Kişisel Verilerin Korunması

Gündem çok hızlı değişiyor. Küresel ölçekte meydana gelen olaylar, ardı ardına gündemi değiştirmekte, bireyler ve kurumlar olarak bu gündemi takip etmekte, hatta bu konularda bilgi sahibi olmakta bile zorlanabiliyoruz. Bir yandan teknolojik olarak, insanoğlunun atılımlarını büyük bir heyecanla takip ediyor, bunları iş süreçlerimize ve gündelik yaşantılarımıza entegre etmenin refahını yaşıyoruz. Diğer yandan göçmen sorunu, iklim değişimi gibi olaylar bizleri tedirgin ediyor; stratejilerimizi etkiliyor, bizi derinden etkiliyor. Zamanın ibresi umuttan yana dönse de yaşamın özünde yer alan değişim olumlu ve olumsuz sonuçlar doğurabiliyor. Bununla birlikte, şurası açık ki yaşadığımız bugünlerin uzun süre unutulmayacağı ortadadır. Bu dönemde meydana gelen bazı gelişmeler gerek kurumları gerek bireyleri ciddi bir şekilde etkileme potansiyeli taşıyor. Bu potansiyele sahip olmakla birlikte, yaşadığımız küresel gelişmeler, bu olayları gölgede bırakabiliyor. Böylece, bu olaylara gündemimizde daha az yer ayırıyor olabiliyoruz. Bir birey olarak bu gözden kaçırma sadece bizleri etkilediği için ciddi sorunlara yol açmıyor olabilir. Oysa kurumların bu olayları gözden kaçırmasının etkisi çok yıkıcı olabiliyor. Bu nedenle, kurumların, bu konuya duyarlı olmaları ve önemli gelişmeleri, hiyerarşinin en üst kademesinden, yani yönetim kurullarından takip etmesi büyük önem taşıyor. Son dönemde meydana gelen bu gelişmelerden biri Kişisel Verilerin Korunması Kanunu'dur. Kişisel Verilerin Korunması Kanunu, Türkiye Büyük Millet Meclisi'nde kabul edildikten sonra 7 Nisan 2016'da Resmi Gazete'de yayımlandı. Kanunda belirtilen maddeler (8, 9, 11, 13, 14, 15, 16, 17 ve 18) yayımdan altı ay sonra yürürlüğe girerken, geriye kalan diğer maddeler ise yürürlüğe girdi. Büyük verinin, siber saldırıların kurumların en önemli gündem maddeleri arasında yer aldığı günümüz iş dünyasında, bu kanun amacı, kanunda şöyle düzenlenmiştir: "Bu Kanunun amacı, kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemektir." Kurumların sahip olduğu en önemli varlıklar arasında, sahip olunan birikimin bulunduğunu biliyoruz. Birikim dediğimiz bu değerin önemli bir bileşeni de verilerden oluşuyor. Analitik analiz yöntemleri ile kurumlar sahip oldukları müşterilere ait kişisel verileri ile bugün uzun dönemli stratejiler yaparken, bu verilere dayalı olarak geliştirdikleri ürünlere büyük yatırımlar yapabiliyor. Bu yolla tasarladıkları bir ürün kurumlara büyük kazançlar sağlayabiliyor. Pazarda söz sahibi olmak için sadece güncel mal ve hizmet üretilmiyor, uzun dönemli projeksiyonlarla yeni mal ve hizmet üretim yöntemleri geliştirilmesi için inovasyona büyük önem veriliyor. Analiz, inovasyon, projeksiyon gibi geleceğe odaklı kavramların en önemli bileşeni veridir. Nitelikli, kullanılabilir veri, geleceğin planlanmasında en önemli girdiler arasında yer alıyor. Kurumlar için verinin sahip olduğu bu önem, Kişisel Verilerin Korunması Kanunu ile farklı bir boyut daha kazandı. Daha önce de Anayasa, Türk Ceza Kanunu, Elektronik Ticaretin Düzenlenmesi Hakkında Kanun, İş Kanunu, Borçlar Kanunu, Bankacılık Kanunu, vb düzenlemeler, kişisel verilerin korunması konusunda hükümler taşıyordu. Kişisel Verilerin Korunması Kanunu konuyu düzenleyerek şöyle bir kapsama oturttu: "Bu Kanun hükümleri, kişisel verileri işlenen gerçek kişiler ile bu verileri tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işleyen gerçek ve tüzel kişiler hakkında uygulanır." Kurumlar için önemli olan bu verilerin, temel hak ve özgürlüklere uygun şekilde yönetilmemesinin hapis ve para cezaları yanında ciddi itibar kayıplarına da neden olma riski taşıması nedeniyle, konunun titizlikle ele alınması gerekiyor. Bu nedenle, kişisel veri güvenliğinin, yönetim kurulları seviyesinde ele alınması önem taşıyacaktır. Yönetim kurulları, kişisel verilerin korunmasını gündemlerine aldıklarında nelere dikkat etmeliler? Kanun, "Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi" kişisel veri kapsamında değerlendiriyor. Bu bağlamda, kurumlar için üç çeşit kişisel veriden bahsedebiliriz. Bunlar, çalışanlara ait kişisel veriler, iş ortaklarına ve danışmanlarına ait kişisel veriler ile müşterilere ait kişisel veriler. Kurumda, öncelikle

bu çerçevede, verilerin sınıflandırılması önemli olacaktır. Bu yolla, kurumda sahip olunan kişisel verilerin envanteri belirlenecektir. Veri envanteri belirlendikten sonra veriler ayrıca önem derecelerine göre de sınıflandırılmalıdır. Bu sınıflandırma işlemi, verilerin korunması için kullanışlı bir çalışma olacaktır. Envanter belirleme işleminde, kişisel verilerin nasıl ve kimler tarafından işlendiği, kimlerin hangi verilere erişebildiği gibi konuların da ele alınması gerekiyor. Verilere yetkisiz kişilerin erişememesi ve bu verilerin üçüncü taraflarla paylaşılmaması dikkat edilmesi gereken konulardır. Bu erişim kısıtlama işlemlerini yeniden ele alırken, kurumlardaki çalışmaların etkinliği bozmayacak bir yöntem uygulanmalıdır. Kurumun sahip olduğu bu veri envanteri belirlendikten sonra, bu verilerin gerekliliği sorgulanmalıdır. Kurum, hangi verilere, neden ihtiyaç duyuyor? Bu süreçte, kurumun ihtiyaç duymadığı bir veri varsa, bu verinin tutulmaması, tutulan verinin de imha edilmesi sağlanmalıdır. İhtiyaç nedeniyle sahip olunan verilerin ise, veri sorumlusu tarafından, ilgili kanunun 12. Maddesinin c bendine göre “Kişisel verilerin muhafazasını sağlamak, amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır” Dikkate alınması gereken diğer bir konu kurum dışından gelecek tehditler olmalıdır. İhtiyaç duyulan kişisel veriler meşru amaçlar için doğru ve güncel bir şekilde tutuluyor, hukuka ve dürüstlük kurallarına uygun olacak elde ediliyor, elde edilen veriler kurum içinde korunuyor olsa da siber saldırı riski gözden kaçırılmamalıdır. Uzmanlar, kişisel verileri hedefleyen siber saldırılara karşı ülkemizdeki kurumların mevcut hazırlıklarının yeterli olmadığını ifade ediyor. Dolayısıyla, kişisel verilerin korunması bağlamında, siber saldırılara karşı da gerekli önlemlerin alınması gerekiyor. Yönetim kurulları, bu çalışmaları talep ederken, kurum bünyesinde buna uygun nitelikte bir insan ve teknoloji kaynağı olup olmadığını da sorgulamalıdır. Gerekiyorsa, bu konularda sahip olunan kaynağın güçlendirilmesi yoluna başvurulmalıdır. Bu hususlar gündeme geldikten ve gerekli çalışmaların yapıldığı anlaşıldıktan sonra, bir veri ihlali olduğunda, bu veri ihlalinin yönetim kurulunun gündemine gelmesi için etkin iletişim yolları kurulmalıdır. Böyle bir ihlal ortaya çıktığında, kurumun yapacağı, olayın üstünü örtmek değil, veri sahibi başta olmak üzere gerekli kişi ve kurumların bilgilendirilmesi olmalıdır. Bu ihlalden sonra, etkin bir teknik analiz yapmak, bu ihlale neden olan faktörleri anlamak, ortaya çıkan kaybı hesaplamak bu sürecin en az kayıpla atlatılması için gerekli olan adımlardır. Neticede, bugün, kurumlar birçok kişisel veriyi tutarak bunları işliyor olabiliyor. Bu verilerin işlenmesinde, Kişisel Verilerin Korunması Kanunu’nun 2. Maddesinde belirtilen “hukuka ve dürüstlük kurallarına uygun olma, doğru ve gerektiğinde güncel olma, belirli, açık ve meşru amaçlar için işlenme, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma, ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme” ilkelerine uyulması zorunluluğu bulunmaktadır. Bu konuda gerekli hassasiyetin gösterilmesi, çalışanları olası hapis ve para cezalarına karşı koruyacak; kurumların olası itibar erozyonlarını önleyecektir. Bu nedenle, yönetim kurullarının, kişisel verilerin korunmasını gündemlerine alarak, bu konuda kuruma yol gösterici olması, onlara liderlik etmesi gerekiyor.

Ali Kamil UZUN, CPA, CFE, MA, CRMA, CAC
Deloitte Türkiye Yönetim Kurulu Danışmanı