

Prof. Dr. Faruk BİLİR

“Kişisel Verilerin Korunması Kişinin Kendisinin Korunmasıdır”

RÖPORTAJ

Röportaj: Sezen YÜCE



İçinde bulunduğumuz dijitalleşme ile veri, kişisel veri, kişisel verilerin korunması ve mahremiyet gibi kavramların her geçen gün daha fazla önem arz ettiğini görmekteyiz. TRT Akademi Dergisi olarak kişisel veri nedir, dijital ortamda verilerimizi nasıl koruyabiliriz, kanun kapsamında sahip olduğumuz haklar nelerdir? Bunları Kişisel Verileri Koruma Kurumu (KVKK) Başkanı Prof. Dr. Faruk Bilir ile konuştuk.

TRT Akademi: Öncelikle kişisel veri nedir, kişisel verilerin korunması ne demektir? Kişisel verilerin korunması neden önemli ve ayrıca kişisel verilerin dünyadaki ve ülkemizdeki tarihsel gelişimini anlatır mısınız?

Prof. Dr. Faruk Bilir: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi kişisel veridir. Başka bir ifadeyle, kişisel veriler; kişiyi doğrudan veya dolaylı olarak tanımlanabilir hâle getiren bilgilerdir.

Kişisel verilerin korunması ise kişinin kendisinin korunmasıdır, temel bir insan hakkıdır. Esasında kişisel verilerin korunması bir araçtır, amaç ise kişinin bizzat kendisinin korunmasıdır.

Bilişim teknolojilerinin hızla ilerlemesi, mal ve hizmetlerin sunulmasında veriye dayalı yönetim anlayışının benimsenmesi ve günlük yaşamın işleyişi içerisinde kişi, kurum ve kuruluşların önemli ölçüde veri işleme faaliyetinde bulunması kişisel verilerin korunmasına yönelik ihtiyacı artırmıştır.

Kişisel verilerin korunması 1960’larda tartışılmaya, 70’li yıllarda ise hukuki düzenlemelere konu olmaya başlamıştır. Bu alanda ilk hukuki düzenleme, 1970 yılında Almanya’nın Hessen eyaletinde kabul edilen Veri Koruma Kanunu’dur.

İlk uluslararası bağlayıcı sözleşme ise 28 Ocak 1981 tarihinde imzaya açılan “108 No’lu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi”dir. Türkiye, bu sözleşmeyi ilk imzalayan ülkelerden biridir. İlerleyen yıllarda Avrupa Birliği, kişisel verilerin korunmasına ilişkin başlayan çalışmalar neticesinde 1995 yılında “Avrupa Parlamentosu ve Avrupa Konseyi Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Direktif”i kabul etmiştir. 95/46 sayılı direktifin temel amacı, Avrupa Birliği üye ülkelerindeki kişisel verilerin korunmasına ilişkin düzenlemelerin uyumlaştırılmasıdır. AB üyesi ülkeler, kişisel verilerin korunmasına ilişkin kanuni düzenlemelerini bu direktifi esas alarak yapmışlardır. 25 Mayıs 2018 tarihinde yürürlüğe giren AB Genel Veri Koruma Tüzüğü (GDPR) ile de kişisel verilere üst düzey koruma getirilmiştir.

Ülkemizde ise 2005 yılında yürürlüğe giren Türk Ceza Kanunu ile kişisel verilere yönelik suçlar düzenlenmiştir. Her ne kadar mevzuatımızda kişisel verilerin ko-

runmasını sağlayabilecek araçlar bulunsa da bu konudaki dönüm noktası 2010 anayasa değişikliği olmuştur. “Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir.” ifadesiyle, kişisel verilerin korunması hakkı anayasal bir hak olarak tanınmış ve anayasal güvence altına alınmıştır.

Yapılan kanun çalışmaları sonucunda ise 6698 sayılı Kişisel Verilerin Korunması Kanunu 7 Nisan 2016 tarihinde Resmî Gazete’de yayınlanmış, böylelikle ülkemizde kişisel verilerin korunması alanında yeni bir dönem başlamıştır. Kanun, 33 maddeden oluşan çerçeve nitelikte bir kanun olup düzenleyici bir özelliğe sahiptir. Aynı zamanda kişisel verilerin korunması alanı dinamik bir yapıya sahip olduğundan, güncellik gerektiren bir kanun olmakla birlikte, teknolojiden faydalanmayı engellememektedir. Diğer yandan Kişisel Verilerin Korunması Kanunu, 95/46 sayılı Direktif mehzaz alınarak düzenlenmiştir.

TRT Akademi: Kişisel Verileri Koruma Kurumu ve Kişisel Verilerin Korunması Kanunu hakkında genel bir bilgilendirme yapabilir misiniz?

Prof. Dr. Faruk Bilir: Kanunla birlikte idari ve mali açıdan özerk, yetkili bir otorite olan Kişisel Verileri Koruma Kurumu kurulmuştur. Kurum, aynı zamanda ülkemizde insan haklarını koruma mekanizmalarından biri olma özelliğine sahiptir. Kurumun karar organı kuruldur, Başkan dâhil 9 üyeden oluşmaktadır.

Kanun, temel hak ve özgürlüklerin korunmasını ve kişisel veri işlemede uyulacak usul ve esasların düzenlenerek veri işleme faaliyetinin disiplin altına alınmasını amaçlamaktadır. Kanun, kişisel verisi işlenen gerçek kişileri korumaktadır. Kişisel Verilerin Korunması Kanunu 4 ana başlık hâlinde incelenebilir. Bunlar; temel ilkeler, kişisel veri işleme şartları, ilgili kişinin hakları ve veri sorumlusunun yükümlülükleridir. Bu başlıklar için “Kanunun taşıyıcı sütunlarıdır.” demek yanlış olmayacaktır.

Hukuka ve dürüstlük kurallarına uygun olma, doğru ve gerektiğinde güncel olma, belirli, açık ve meşru amaçlar için işleme, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma, ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme Kanununun temel ilkeleridir. Söz konusu ilkeler, veri işleme faaliyetinin olmazsa olmazı niteliğindedir.

Her ne kadar kanunda bu ifade direkt olarak yer almasa da özel nitelikli kişisel verilerin dışında kalan bütün kişisel verilere genel nitelikli kişisel veriler denilebilir. Genel nitelikli verilerin işleme şartları; açık rıza, kanunlarda açıkça öngörülme, fiili imkânsızlık, sözleşmenin kurulması veya ifası, veri sorumlusunun hukuki yükümlülüğü, ilgili kişinin kendisi tarafından alenileştirilmesi, bir hakkın tesisi, kullanılması veya korunması ve meşru menfaat olarak sayılabilir.

Özel nitelikli kişisel veriler ise öğrenildiğinde bireyin ayrımcılığa ve mağduriyet yaşamasına neden olabilecek nitelikteki verilerdir. Bu tür veriler, kanunun gerekçesinde hassas veriler olarak da adlandırılmaktadır. Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir. Görüldüğü üzere, özel nitelikli kişisel veriler sınırlı sayma yoluyla belirlenmiştir.

Söz konusu veriler, açık rıza yoluyla işlenebilir. Bununla birlikte, sağlık ve cinsel hayat dışındaki veriler, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir.

Sağlık ve cinsel hayata ilişkin veriler ise kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla; sır saklama yükümlülüğü altında bulunan kişiler, yetkili kurum ve kuruluşlar tarafından kişinin açık rızası aranmaksızın işlenebilir.

Kişisel verilerin işleme amaçlarını ve araçlarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi, kanunda veri sorumlusu olarak anılmaktadır. Kanun, veri sorumlularına; temel ilkelere uygunluk sağlama, veri işleme şartlarına uyum, gerektiren durumlarda imha işlemlerinin uygulanması, aydınlatma yükümlülüğü, ilgili kişinin haklarının kullanılabilmesi, veri güvenliğine ilişkin yükümlülükler, kurul kararlarının yerine getirilmesi ve veri sorumluları siciline kayıt yükümlülüğü gibi birtakım yükümlülükler getirmiştir.

TRT Akademi: Kanun kapsamında sahip olduğumuz haklar nelerdir? Sahip olduğumuz hakları nasıl kullanabiliriz?

Prof. Dr. Faruk Bilir: Herkes veri sorumlusuna başvurarak kendisiyle ilgili; kişisel veri işlenip işlenmediğini öğrenme, işlenmişse bilgi talep etme, işlenme amacını ve amacına uygun kullanılıp kullanılmadığını öğrenme, aktarıldığı üçüncü kişileri bilme, eksik veya yanlış işlenmiş olması hâlinde düzeltilmesini isteme, verilerin silinmesini veya yok edilmesini isteme, düzeltme ve imha işlemlerinin üçüncü kişilere bildirilmesini isteme, verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme ve zararın giderilmesini talep etme haklarına sahiptir.

Kanun, hakların kullanımı konusunda iki aşamalı bir başvuru usulü öngörmüştür. Buna göre; kişisel verisi işlenen gerçek kişiler, yani kanundaki ifadeyle ilgili kişi-

ler, önce veri sorumlusuna başvurmalıdır. Veri sorumlusuna yapılan başvurudaki talebin reddedilmesi, verilen cevabın yetersiz bulunması veya başvuruya süresinde cevap verilmemiş olması durumlarında kişiler Kurula şikâyet hakkını elde edeceklerdir.

Şikâyet yoluna başvurulabilmesi için ilk olarak kişinin veri sorumlusuna yapmış olduğu başvurunun reddedilmesi, verilen cevabın yetersiz bulunması veya otuz gün içinde başvuruya cevap verilmemiş olması gereklidir. İlgili kişinin Kurula şikâyette bulunmasında öngörülen süre, veri sorumlusunun cevabını öğrendiği tarihten itibaren otuz ve her hâlde başvuru tarihinden itibaren altmış gündür. Veri sorumlusuna başvuru zorunlu, Kurula şikâyet ise isteğe bağlıdır.

TRT Akademi: Veri ihlal bildirimini nedir? İhlal bildirimini nasıl yapılmalıdır? Veri ihlali müdahale planı ne anlama gelmektedir?

Prof. Dr. Faruk Bilir: Kişisel veri ihlali bildirimini; veri sorumlusu veya yetkilendirdiği kişilerce işlenen kişisel verilerin, kanuni olmayan yollarla başkaları tarafından elde edilmesi durumunda, veri sorumlusunun Kurula ve ihlalden etkilenen kişilere yapmak zorunda olduğu bildirimdir.

Bildirim, Kurum internet sitesinde bulunan “Veri İhlali Bildirim Formu”nun doldurularak Kurula iletilmesi ve ayrıca ihlalden etkilenen kişilere gerekli bilgilendirmenin yapılması şeklinde gerçekleştirilir.

Veri İhlali Müdahale Planı aslında bir çeşit kriz yönetimidir. Veri sorumlusu tarafından kendi nezdinde kimlere raporlama yapılacağı, yapılacak bildirimler ile ihlalin olası sonuçlarının değerlendirilmesi hususunda sorumluluğun kimde olduğunun belirlenmesi gibi konuları içeren bir veri ihlali müdahale planı hazırlanmalı, belirli aralıklarla gözden geçirilmelidir.

TRT Akademi: Dijital çağda verilerimizi korumamız mümkün mü? Bireysel olarak kendi veri güvenliğimizi sağlamak için neler yapabiliriz?

Prof. Dr. Faruk Bilir: Kişisel verilerin korunmasında bireylere de düşen görevler bulunmaktadır. Kişisel veriler paylaşılmadan önce aydınlatma metni ve gerekli ise açık rıza metni dikkatlice okunmalı. Kişiler, verilerini talep eden uygulamalara karşı daha bilinçli yaklaşmalıdır. Uygulamanın güvenli olup olmadığını sorgulayıp araştırmalıdır.

Sosyal medyada hangi paylaşımı kimlerin göreceğini belirlemek, kişisel verilerin güvenliğini sağlamak adına gerekli bir adımdır. Bireylerin çevrim içi ya da gerçek ortamda ortaya çıkabilecek mahremiyet ihlallerine karşı bilgi sahibi olmaları büyük önem taşımaktadır. Dolayısıyla kişisel verilerin korunması konusunda farkındalık kazanılmalıdır. Çünkü farkındalık, güvenliğe açılan kapının anahtarındır.

Öte yandan sahte ve gerçek dışı duyurular, kişisel veri güvenliği için de risk teşkil etmektedir. Bu tarz kötü niyetli paylaşımların bizleri maddi ve manevi açıdan zor durumda bırakabileceğini unutmamalıyız. Bu çerçevede gizlilik ve güvenlik ayarlarını düzenlemeli, güçlü parolalar kullanmalı ve hukuka aykırılık teşkil eden paylaşımlardan kaçınmalıyız. Aksi takdirde sadece kendi verilerimizi değil, yakınlarımızın ve başka kişilerin de kişisel verilerini riske atmış oluruz.

TRT Akademi: Geride bıraktığımız 2020 yılında Kişisel Verileri Koruma Kurulunun aldığı en önemli kararlardan biri unutulma hakkına ilişkin karar oldu. Unutulma hakkı nedir? Bu haktan yararlanmak için hangi adımlar atılabilir?

Prof. Dr. Faruk Bilir: Unutulma hakkı; bireyin geçmişte hukuka uygun olarak yayılmış ve doğru nitelikteki bilgilerinin zamanın geçmesine bağlı olarak erişimden kaldırılmasını ya da gündeme getirilmemesini talep edebilmesidir. Unutulma hakkı "istisnai" bir haktr.

Kurul, taleplerin değerlendirilmesinde; kişinin temel hak ve özgürlükleriyle kamunun söz konusu bilgiyi edinmesinden sağlayacağı menfaatler arasında bir denge testinin yapılmasını ve yarışan menfaatlerden hangisinin ağır bastığının gözetilmesi gerektiğini karara bağlamıştır. Buna ek olarak, bu konudaki kriterleri belirleyerek ilan etmiştir.

“Arama sonuçlarının öznesi bir çocuk mu?”, “Arama sonuçlarında yer alan bilgi özel nitelikli kişisel veri niteliği taşıyor mu?”, “Arama sonuçlarında ulaşılan bilgi güncel mi?”, “Arama sonucunda yer alan bilgi, kişi açısından bir risk doğuruyor mu?”, “Orijinal içerik, gazetecilik faaliyeti kapsamında işlenen verileri mi kapsıyor?” gibi toplamda 13 kriter, ilgili Kurul kararıyla birlikte yayımlanmıştır. Ancak her somut olay özelinde Kurul tarafından ilave ölçütler gündeme getirilebileceği de ifade edilmiştir.

Kanun gereği kişilerin, arama sonuçlarının indeksten çıkarılmasına yönelik talepleriyle ilgili olarak öncelikle arama motorlarına başvuruda bulunmaları gerekmektedir. Arama motorlarının söz konusu talepleri reddetmeleri veya başvuru sahibine cevap vermemeleri hâlinde Kurula şikâyetle bulunulabilir. Kişiler, Kurula şikâyet seçeneğini tercih ederken aynı zamanda doğrudan yargı yoluna da gidebilir.

TRT Akademi: Veri güvenliğinde en çok yapılan ihmallere nelerdir?

Prof. Dr. Faruk Bilir: Günümüzde zararlı yazılımlar, oltalama ve kimlik avı, ransomware ve DDOS gibi siber saldırıların sıklıkla görüldüğü kuşku götürmez bir gerçektir.

Buna karşın veri güvenliğinde en önemli konulardan biri, çalışanların eğitilmesidir. Çünkü farkındalık düzeyi arttıkça insan hatasından kaynaklı veri ihlalleri azalmaktadır. Bu açıdan veri sorumluları, veri işleme süreçlerinde yer alan tüm çalışanlarına belirli aralıklarla ciddi eğitimler vermelidir.

Bir diğer önemli konu ise sürdürülebilirliktir. Siber saldırıların gün geçtikçe nitelikli hâle geldiği günümüzde, veri güvenliği konvansiyonel yöntemlerle sağlanamaz. Dolayısıyla güncelliğe açık, inovasyona dayalı bir anlayış benimsenmelidir. Bir de mümkün olduğunca yerli ve milli çözümlerin üretilmesi son derece önemlidir.

TRT Akademi: Verilerimiz mahremiyetimizi ne derece açık hâle getiriyor?

Prof. Dr. Faruk Bilir: Mahremiyet, kişinin yalnız bırakılma hakkıdır. Bunu, bireylerin kendi hayat alanlarını "diğerleri" ile ne ölçüde paylaşacaklarını belirleme hakkı olarak da düşünebiliriz. Mahremiyet, aynı zamanda kişinin özgürlüğünün bir parçasıdır. Bu bağlamda özellikle çevrim içi ortam ile sürekli etkileşim hâlinde bulunan bireylerin kişisel verilere yönelik algıları, konuyla ilgili farkındalıkları ve kişisel verilerin kullanımına yönelik bilinç düzeyleri önem arz etmektedir.

Bazen gerçek hayatta herkesle paylaşmayacağımız bir bilgiyi çevrim içi ortamlarda herkese açık bir şekilde paylaşabiliyoruz. Bu olgu, bireyin mahremiyetinin dijital ortamlarda da tesis edilmesi gerekliliğini ortaya çıkarmış ve dijital mahremiyet kavramını gündeme getirmiştir.

Dijital mahremiyet, gerçek hayattaki mahremiyet kavramının dijital ortamdaki boyutudur. Nasıl ki fiziksel hayatta kendimize ait özel alanları koruyor isek, dijital ortamlarda da bize ait alanları mümkün olduğunca korumamız gerekir. Çünkü bireyin hayatına hâkim olması, kişisel verileri üzerinde kontrol ve denetim hakkına sahip olmasıyla mümkündür.

TRT Akademi: Dijital ortamda verilerimiz nasıl toplanıyor ve hangi amaçlarla kullanılıyor?

Prof. Dr. Faruk Bilir: Teknolojinin ilerlemesi, kişisel veriler üzerinde her türlü işlemin yapılmasını mümkün hâle getirmiştir. Bunun sonucunda algoritmaların hayatımıza olan etkisi artmış, kişisel verilerin hayatımızı ciddi bir biçimde etkileyebildiğinin farkına varılmıştır. Şunu da eklemek gerekir ki; bizler de dijital ortamlarda vakit geçirerek sürekli veri üretiyoruz. Birtakım otomatik sistemler vasıtasıyla bu verilerden kişi hakkında çeşitli sonuçlar elde edilebiliyor. Eğer kişi hakkında olumsuz bir sonuç ortaya çıkıyorsa, kanunda buna itiraz hakkı mevcuttur.

Diğer taraftan veri sorumluları, kişisel verilerin kullanım amaçlarını aydınlatma yükümlülüğü kapsamında açıklamak zorundadır.

TRT Akademi: WhatsApp uygulaması ile ilgili yaşanan sıkıntılar bağlamında biraz bilgi verir misiniz?

Prof. Dr. Faruk Bilir: Bahsettiğiniz uygulama, gizlilik politikasını güncelleyerek rıza vermeyen kullanıcıların uygulamayı kullanamayacağını belirtmiştir. Bunun dışında uygulamanın gizlilik politikasında, kişisel verilerin aktarılacağı üçüncü kişiler ve aktarıma amacı konusunda belirsizlikler olabileceği gündeme gelmiştir.

Bilindiği gibi Kurul, kanuna göre; şikâyet üzerine veya ihlal iddiasını öğrenmesi durumunda re'sen, görev alanına giren konularda gerekli incelemeyi yapma yetkisine sahiptir. Bu yetki çerçevesinde kanundaki temel ilkeler, açık rızanın unsurları, veri işleme şartları ve yurt dışına veri aktarımı yönlerinden re'sen inceleme başlatılmıştır.

TRT Akademi: İnsanlar kendi iradeleriyle verilerini sosyal medya platformlarına yüklüyorlar. Burada bir koruma söz konusu mu?

Prof. Dr. Faruk Bilir: Burada öncelikle “alenileştirme” kavramından kısaca bahsetmek istiyorum. Yalın bir ifadeyle alenileştirme, ilgili kişinin verilerinin kendisi tarafından kamuoyuna açıklanmasıdır. Bu çerçevede verinin, aleni kabul edilebilmesi için ortada alenileştirme iradesinin var olması gerekir. Bu anlamda tek başına kişisel verinin kamuoyuna açık hâle gelmesi alenileştirme bakımından yeterli değildir. Kişinin iradesi ile desteklenmesi gerekmektedir.

Ancak alenileştirme eylemi; kişilerin, verilerini kamuoyu ile paylaşması amacı ile sınırlıdır. Başka bir ifadeyle, bir verinin alenileştirilmiş olması o verinin gelişigüzel kullanılabileceği anlamına gelmez. Bununla ilgili Kurul kararlarımız da mevcuttur. Dileyenler, Kurumun resmî internet sayfasından erişim sağlayabilirler.

TRT Akademi: Sosyal medya platformlarında veya uygulamaları akıllı cihazlarımıza indirirken bir sözleşme karşımıza çıkıyor. Bunu genel itibarıyla okuyan olmuyor. Burada nasıl hareket etmeliyiz? Bugün neredeyse tüm dijital platformlar kişisel verilerimize erişim izni istiyor. Kişisel verilerimizi vermeden önce veya verirken nelere dikkat etmeliyiz?

Prof. Dr. Faruk Bilir: Bizim bu konuda öncelikle dijital okuryazarlığımızı ve hak arama kültürümüzü geliştirmemiz gerekir. Öte yandan bir uygulamayı indirirken bazı hususlara dikkat etmekte büyük fayda var.

Örneğin; kaynağı bilinmeyen uygulamalardan uzak durmalı, akıllı cihazımızın ayarlarından bu konudaki tercihimizi belirlemeliyiz. Bir uygulamayı indirmeden önce, o uygulamanın hangi kişisel verilerimize erişim izni istediğini okumalı, gizlilik politikasını incelemeliyiz. İndirme esnasında sahte uygulamalara dikkat etmeliyiz. Uygulama geliştiricisi ve uygulama adının doğruluğundan emin olmalıyız.

Bazı uygulamalar ilk bakışta eğlenceli gibi gözükse de arka planda birtakım kişisel verilerimizi hedefleyebilmektedir. Kendimizi ve özellikle çocuklarımızı bu tarz popüler uygulamalardan uzak tutmaya çalışmalıyız.

Şunu unutmamalıyız: "Kişisel veriler sadece geçmişte bıraktığımız izler değil, aynı zamanda geleceğe bırakacağımız izlerdir."

TRT Akademi: Sosyal medya veya benzer platformlardan kendimizle ilgili toplanan verileri alma, silme imkânımız var mı?

Prof. Dr. Faruk Bilir: Kişiler, veri sorumlusu konumundaki gerçek ve tüzel kişilere başvurarak kendileriyle ilgili veriler hakkında bilgi talep etme hakkına sahiptir. Diğer yandan kanunun 7. maddesinde öngörülen şartlar çerçevesinde kişisel verilerin silinmesini veya yok edilmesini isteme hakkına da sahiptir. Bu, herhangi bir sosyal medya şirketi de olabilir, başka bir sektörde faaliyet gösteren bir şirket de olabilir.

Burada esas önemli olan, haklarımızı bilmek ve haklarımızın farkında olmaktır.

Çünkü güvenlik, farkındalıkla mümkündür.



Kişisel verilerin korunması, Pixabay