Ünite 3: Türkiye'de Kişisel Verilerin Korunması

Giriş

Türkiye'de kişisel verileri dijital ortamda toplayan, kayıt eden, birbirleri ile ilişkilendiren ve üçüncü kişilere aktaran sistemler yaygın bir biçimde kullanılırken bu kullanımdan kaynaklı önemli "yan etkileri" ortadan kaldırmaya yönelik olan kişisel verilerin korunması alanında, hukuksal düzenlemelerin yetersiz olduğu belirtilmelidir. Ancak bu, konuya ilişkin Türkiye'de hiçbir bir düzenleme olmadığı anlamına gelmez.

Başta Türkiye Cumhuriyeti Anayasası olmak üzere iç hukukumuzda kişisel verilerin korunmasını açıkça tanıyan bazı düzenlemeler bulunmaktadır.

Türkiye Cumhuriyeti Anayasası

Türkiye Cumhuriyeti Anayasasında kişisel verilerin korunmasının normatif temelini oluşturacak çeşitli hükümler bulunur. Bu kapsamda ilk olarak *kişinin maddi* ve *manevi varlığını geliştirme hakkı* dikkate alınmalıdır. Anayasa'nın başlangıç 6. paragrafında ve 17/1 hükmünde kişinin maddi ve manevi varlığını koruma ve geliştirme hakkı hüküm altına alınmıştır. Bunun yanında Anayasa uyarınca *"Devletin temel amaç ve görevleri"* arasında *"insanın maddi* vc *manevi varlığının gelişmesi için gerekli şartları hazırlamaya çalışmak"* (m.5) yer alır.

Kişisel verilerin korunmasına yönelik Türk hukuk mevzuatındaki en önemli düzenleme yine Anayasada yer alır. Anayasa'nın 20. Maddesine 2010 Anayasa değişiklikleri ile eklenmiş olan son fıkra şöyledir: *"Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak, kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir".* Belirtilen hüküm ile Türkiye'de kişisel verilerin korunması açıkça anayasal bir hak olarak düzenlenmiştir.

Kişisel verilerin korunması hakkının anayasada açıkça yer alması olumlu bir gelişme olsa da hükümde bazı eksiklikler bulunduğu dikkatten kaçmamalıdır. Öncelikle Anayasanın 20. maddesinin 3. fıkrası kapsamında kişisel verilerin korunması hakkından değil, kişisel verilerin korunmasını "isteme" hakkında söz edilmesi anayasa koyucunun bu korumaya ilişkin yeterli güvenceyi sağlamada isteksiz olduğu şeklinde yorumlanabilir. Dikkat çeken bir diğer husus, Avrupa Birliği Temel Haklar Şartı'nın 8. maddesinin aksine hükümde kişisel verilerin korunmasında hâkim olan ilkelerin uygulamasını denetleyecek bağımsız bir organın kurulmasına yer verilmemiştir. Elbette bu durum bağımsız bir denetim organının kurulması önünde engel değildir. Nitekim Kişisel Verilerin Korunması Kanun Tasarısı'nda Veri Koruma Kurulu adıyla böylesine bir organa yer verilmiştir.

Bunun yanında Anayasa Mahkemesinin kişisel verilerin korunmasına ilişkin oldukça tartışmalı kararlarının bulunduğunu da belirtmek gerekir. 2Û00'li yıllara gelinceye kadar Anayasa Mahkemesi konuya ilişkin üç önemli karar vermiştir. Bunlardan ilk ikisi nüfus cüzdanlarında din hanesinin bulunmasına ilişkindir. Anayasa Mahkemesi yaptığı her iki incelemede de aile kütüklerinde ve nüfus cüzdanlarında din hanesinin bulunma zorunluluğunun Anayasaya aykırı olmadığına karar vermiştir. Anayasa Mahkemesi'nin bir diğer önemli kararı ise Kimlik Bildirme Kanunu'na eklenen bir hükme ilişkindir. İlgili hüküm uyarınca genel kolluk kuvvetlerinin bilgisayarlarında otel motel, yurt, misafirhane gibi konaklama yerlerinde kalan kişilerin kişisel verilerinin toplanması zorunluluğu getirilmektedir. Ancak bu zorunluluk getirirken kolluk kuvvetlerinin uyacakları esaslar yasada belirlenmemiştir.

Diğer taraftan, Mahkemenin 2008 yılında verdiği bir karar, kişisel verilerin korunmasının özel yaşamın gizliliği ve düşünce özgürlüğü çerçevesinde gördüğünü açıkça ortaya koymaktadır. Bu karara konu olan Türkiye İstatistik Kanunu'nun ilgili hükümleri uyarınca istatistik amacıyla gerçek kişilerin de dâhil olduğu "istatistikî birimler"den her türlü bilgi istenebilir. Bu isteğin istenilen şekil, süre ve standartlarda ücretsiz olarak karşılanması zorunludur. Bu zorunluluğu yerine getirmeyenler ise idari para cezası yaptırımı ile karşılaşacaklardır. Anayasa Mahkemesi ilgili hükümleri, "kişilerin bilgi toplama, saklama, işleme tekeline sahip idareye ve diğer kişilere karşı korumasız bırakılması ve veri toplamanın sınırlarına yasal düzenlemelerde yer verilmemesi" nedeniyle Anayasaya aykırı bulmuştur (E. 2006/17, K. 2008/86, 20/3/2008). Anayasa Mahkemesi'nin başta sağlık verilerinin korunması ile ilişkili olmak üzere yakın zamanda verdiği başka bazı kararlar da bulunmaktadır. Öte yandan Anayasa Mahkemesi, 2012 Eylül ayından itibaren bireysel başvuruları da kabul etmeye başlamıştır.

Kişisel verilerin korumasının anayasal temellerini incelerken dikkate alınması gereken bir diğer hüküm, Anayasa'nın 90. maddesinde yer alır. Anayasa'nın 90. maddesi uyarınca *"Usulüne göre yürürlüğe konulmuş Milletlerarası antlaşmalar kanun hükmündedir'".* Dolayısıyla Türk hukuk sisteminde uluslararası antlaşmalar iç hukuk sisteminin bir parçasıdır. Bu antlaşmanın temel hak ve özgürlüklere ilişkin olması durumunda ise, sözleşme hükümlerinin yasaların bile üzerinde yer aldığı söylenebilir. Nitekim 90. maddeye 2004 yılında eklenen bir hüküm uyarınca: *"Usulüne göre yürürlüğe konulmuş temel hak ve özgürlüklere ilişkin antlaşmalarla kanunların aynı konuda farklı hükümler içermesi nedeniyle çıkabilecek uyuşmazlıklarda milletlerarası antlaşma hükümleri esas alınır".* Bu düzenleme, konumuz açısından özellikle Avrupa İnsan Hakları Sözleşmesi'nin (AİHS) konumu dolayısıyla önemlidir.

Avrupa İnsan Haklan Sözleşmesi

Avrupa İnsan Hakları Mahkemesi (AİHM) verdiği kararlarla, kişisel verilerin korunmasında temel ilkelerin büyük bil' bölümünü AİHS'nin 8. maddesi kapsamında tanımaktadır. Sözleşme hükümlerinin sınır ve kapsamlarını belirleyebilmek için AİHM'nin yorumlarının önemi açıktır. AİHS'nin "Özel ve aile yaşamına saygı hakkı" kenar başlıklı 8. maddesi şu hükmü içerir:

1. "Herkes özel ve aile yaşamına, konutuna ve haberleşmesine saygı gösterilmesi hakkına sahiptir.

2. Bu hakkın kullanılmasına bir kamu otoritesinin müdahalesi, ancak ulusal güvenlik, kamu emniyeti, ülkenin ekonomik refahı, dirlik ve düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için, demokratik bir toplumda gerekli olan ölçüde ve yasayla öngörülmüş olmak koşuluyla söz konusu olabilir".

Kişisel verilerin korunması hakkının 8. madde kapsamında değerlendirilmesi, Sözleşme hükümlerinin yorumlanmasında yeni gelişmelere açık bir bakışın hâkim olduğunun da göstergesidir. Nitekim AİHM'ye göre Sözleşme, *"güncel koşullar ışığında yorumlanması gereken yaşayan bir enstrüman"*dır (Tyrer, Birleşik Krallık, 5856/72,28/4/1978). Mahkemenin görevi, Sözleşmeyi yorumlarken sosyal değişimleri de yansıtmaktır AİHM'nin çeşitli kararlarında da belirttiği üzere, Sözleşme ile güdülen amaç, hakların hayali ya da teorik olarak değil, etkili ve elverişli bir şekilde güvence altına alınmasıdır.

Bireylere ilişkin kişisel bilgilerin resmi makamlarca toplanarak arşivlenmesi, telefon görüşmelerine ilişkin kayıtları izleme, toplanan verilerin toplanma amacı dışında kullanılması, sağlık verilerinin gizliliği, emniyet güçleri tarafından parmak izi ve fotoğrafların alınması, kişisel verilere erişim hakkı, kişisel verilerin gerektiğinden uzun süre tutulması gibi konular Mahkemenin çeşitli kararlarında 8/1 hükmü kapsamında değerlendirilmiştir. Bunun yanında Mahkemenin içtihadı uyarınca "özel yaşam", kimlik hakkını ve 8. maddedeki güvencelerin yorumlanmasında oldukça önemli olan, kişilik ve bireysel özerklik ilkeleri dolayısıyla, kişisel gelişim hakkını da kapsamaktadır.

AİHS'nin 8. maddesinde düzenlenen özel yaşama saygı hakkının sınırları, aynı maddenin 2. fıkrasında yer alır. Bu özel yaşama saygı hakkına bir müdahale olduğu saptandığında, Mahkeme bu müdahalenin meşruiyet kazanıp kazanmadığını değerlendirir. Bu değerlendirme 2. fıkrada belirlenen koşul ve ölçütlere uygunluk açısından yapılmaktadır. AİHS 8/2 hükmü uyarınca özel ve aile yaşamına müdahale: Burada sınırlı sayımla belirtilmiş amaçlardan bir ya da bir kaçına yönelik; yasada öngörülmüş ve demokratik toplum için gerekli ve öngörülen amaç ile orantılı olması durumunda meşrudur. Sınırlı sayımla belirlenen ve özel ve aile yaşamına saygı hakkına istisna getiren meşru amaçlar ise şunlardır: ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, dirlik ve düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının haklarının korunması.

Görüldüğü gibi meşru amaçlar oldukça geniş bir şekilde belirlenmiştir. O kadar ki herhangi bir müdahalenin burada belirlenen meşru amaçları karşılayamaması oldukça zordur. Ancak bir müdahalenin Sözleşme'de belirlenen ilkelere uygun olması için meşru bir amaca yönelik olması ve yasa ile öngörülmesi yeterli değildir. Bunların yanında ayrıca ve mutlaka demokratik bir toplum için gerekli ve orantılı olması da gerekir. Bu, kişisel verilerin korunması ile hedeflenen denge yaklaşımı ile de uyumludur.

Türk Ceza Kanunu

1 Haziran 2005 tarihinde yürürlüğe giren yeni Türk Ceza Kanunu uyarınca kişisel verilerin hukuka aykırı kayıt edilmesi, verileri hukuka aykırı verme, yayma veya ele geçirme ile gereken sürelerin geçmesine karşın verileri yok etmeme suç olarak düzenlenmiştir. Bu açıdan Türk hukuk sisteminde yasal düzeyde konuya ilişkin en kapsamlı korumanın Türk Ceza Kanunu'nda (TCK) yer aldığı söylenebilir.

Öncelikle TCK'nin 135. maddesi uyarınca kişisel verilerin hukuka aykırı olarak kaydedilmesi suçtur.

Buna göre kişisel verileri hukuka aykırı olarak kayıt eden kimseye bir yıldan üç yıla kadar hapis cezasının verilmesi öngörülmüştür. Kişilerin ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına ve sendikal bağlantılarına ilişkin bilgileri hukuka aykırı olarak kaydeden kimse de aynı yaptırım ile cezalandırılacaktır.

TCK'nin 136. maddesinde ise kişisel verileri hukuka aykırı olarak başkasına vermek, yaymak ve ele geçirmek suçu düzenlenmiştir. Buna göre; *"Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, iki yıldan dört yıla kadar hapis cezası ile cezalandırılır".* Belirtilen eylemlerin yaptırıma bağlanmasındaki amaç kişisel verilerin yetkisiz üçüncü kişilere aktarılmasını ve ele geçirilmesini önlemektir. Bu bakımdan verinin kaydedilmesinin hukuka uygun olup olmadığı, suçun oluşması açısından önemli değildir. 136. maddede yer alan düzenleme kişisel verilerin korunmasını sağlayıcı bir niteliktedir. Bu noktada önlenmek istenen eylemler arasında kimlik hırsızlığı örnek olarak gösterilebilir.

Konuya ilişkin bir diğer önemli düzenlemenin TCK'nin 138. maddesinde yer aldığı görülür. Buna göre: *"Kanunların belirlediği sürenin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde bir yıldan iki yıla kadar hapis cezası verilir".* Hükme 2014 yılında eklenen fıkra uyarınca İse *"Suçun konusunun Ceza Muhakemesi Kanunu hükümlerine göre ortadan kaldırılması veya yok edilmesi gereken veri olması hâlinde verilecek ceza bir kat artırılır."* TCK'nin 138.maddesi ile kişisel verilerin korunması alanında temel ilkelerden biri olan verilerin süresiz olarak tutulmaması gerekliliğinin karşılandığı söylenebilir.

Belirtmek gerekir ki bu suçların hiç birinin takibi şikâyete bağlı değildir. Ayrıca Türk Ceza Kanunun 135. ve 136. maddesinde düzenlenen suçların kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle ya da belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle işlenmesi hâli ağırlaştırıcı sebep olarak belirlenmiş ve cezanın yarı oranında arttırılacağı hüküm altına alınmıştır. Bunun yanında bu üç maddede yer alan suçların tüzel kişiler tarafından işlenmesi hâlinde bunlara özgü güvenlik tedbirleri uygulanacaktır.

TCK'de konuya ilişkin olarak belirtilen suçlara ve yaptırımlara yer verilmiş olmasına karşın, bu eylemlerin tanımlandığı ve kişisel verilerin korunmasında temel ilkelerin belirlendiği bir düzenlemenin bulunmaması önemli bir eksiklik olarak hissedilmektedir. Bu kapsamda özellikle "kişisel verilerin tanımı konusunda mevzuatımızda açıklayıcı hükümlerin son derece sınırlı olması ve temel ilkelerin düzenlememesi nedeniyle "hukuka aykırılık"ın belirlenmesinde yaşanan güçlükler özellikle dikkat çekicidir.

Türk Medeni Kanunu

Türk hukuk mevzuatında medeni hukukun kişilik haklarına yönelik düzenlemelerinin kişisel verilerin korunmasına açısından bazı olumlu sonuçlar sağlayabileceği söylenebilir. Medeni hukukta, kişisel verilerin korunması ile yakından ilişkili olan, kişinin onur ve saygınlığı, adı ve resmi üzerindeki hakları ile sır alanı kişilik haklarının alanı içerisinde değerlendirilmektedir. Bu doğrultuda konuya ilişkin hukuksal korumanın ise Türk Medeni Kanunu'nun (MK) 24. ve 25. maddelerinde getirildiği görülmektedir. MK'nin 24. maddesinde kişiliğe yönelik saldırılara karşı temel ilke, 25. maddede ise başvurulabilecek hukuksal yollar belirlenmiştir.

Türk Borçlar Kanunu

Türk Borçlar Kanunu'nda işçinin kişisel verilerinin korunmasına yönelik bir hüküm yer almaktadır. Yeni Borçlar Kanunu'nun 419. maddesi uyarınca *"İşveren, işçiye ait kişisel verileri, ancak işçinin işe yatkınlığıyla ilgili veya hizmet sözleşmesinin ifası için zorunlu olduğu ölçüde kullanabilir".* İş ilişkisi, niteliği gereği işçinin dezavantajlı olduğu bir durum yaratmaktadır. Bu nedenle işçinin kişisel verilerinin yasal düzenlemeler uyarınca korunması son derece önemlidir.

Elektronik Haberleşme ve Elektronik Ticaret Kanunları

Elektronik ticaret ve elektronik haberleşme sektörlerinde kişisel veriler işlenirken uyulacak temel kurallar, Elektronik Haberleşme Kanunu ve Elektronik Ticaret Kanununda düzenlenmiştir.

Elektronik Haberleşme Kanunu

2015 yılında yapılan düzenlemeyle, Elektronik Haberleşme Kanunu'nun "kişisel verilerin işlenmesi ve gizliliğinin korunması" kenar başlıklı 51. maddesi bu sektörde veri işleme süreçlerine ilişkin kuralları belirleyen bir hüküm hâlini almıştır. Bu madde kapsamında verilerin kaliteli olması ilkesine işaret edildiği görülmektedir.

Buna göre elektronik haberleşme alanında veri işleme süreçlerinde bu ilkenin bileşenlerine uyumlu hareket etmek bir zorunluluktur. Ayrıca elektronik haberleşmenin ve ilgili trafik verisinin gizliliği temel kural olarak benimsenmiştir. Bunun istisnası ilgili mevzuatın ve yargı kararlarının öngördüğü durumlardır. Bunun haricinde haberleşmeye taraf olanların tamamının rızası olmaksızın haberleşmenin dinlenmesi, kaydedilmesi, saklanması, kesilmesi ve takip edilmesi yasaklanmıştır.

Elektronik Haberleşme Kanunu'ndaki düzenlemenin dikkat çeken bir diğer yönü "çerez"lerin (cookie) kullanımına getirilen sınırlamadır, çerez, kullanıcı bir İnternet sitesini ziyaret ettiğinde bağlantı kurduğu cihazın sabit diskine kaydedilen bir tür tanımlama dosyası olarak tarif edilebilir. Bu dosyalarda kişilerin ziyaret ettiği siteler gibi bazı bilgiler saklanabilmektedir. Elektronik Haberleşme Kanunu'nun 51.maddesi ile bir yandan kişisel verilerin korunmasına yönelik bu kurallar hüküm altına alınırken diğer yandan kişisel verilerin saklanmasına yönelik bazı hükümler getirilmiştir. Nitekim bu kanun kapsamında sunulan hizmetlere ilişkin olarak; soruşturma, inceleme, denetleme veya uzlaşmazlığa konu olan kişisel veriler ilgili süreç tamamlanıncaya kadar kişisel verilere ve ilişkili diğer sistemlere yapılan erişimlere ilişkin işlem kayıtları iki yıl, kişisel verilerin işlenmesine yönelik abonelerin, kullanıcıların rızalarını gösteren kayıtlar asgari olarak abonelik süresince saklanacağı hüküm altına alınmıştır.

Elektronik Ticaret Kanunu

6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanunun 6. maddesi uyarınca: *"(1) Ticari elektronik iletiler, alıcılara ancak önceden onayları alınmak kaydıyla gönderilebilir. Bu onay, yazılı olarak veya her türlü elektronik iletişim araçlarıyla alınabilir. Kendisiyle iletişime geçilmesi amacıyla alıcının iletişim bilgilerini vermesi hâlinde, temin edilen mal veya hizmetlere ilişkin değişiklik, kullanım ve bakıma yönelik ticari elektronik iletiler için ayrıca onay alınmaz. (2) Esnaf ve tacirlere önceden onay alınmaksızın ticari elektronik iletiler gönderilebilir".* Burada kastedilen ticari ileti, reklam, pazarlama gibi amaçlarla cep telefonlarına ya da e-posta adreslerine gönderilen mesajlar, e-postalar ya da yapılan aramalardır.

Kanun'un 10. maddesi ise doğrudan kişisel verilerin korunmasına yöneliktir. Buna göre: *"(1) Hizmet sağlayıcı* ve *aracı hizmet sağlayıcı: a)Bu Kanun çerçevesinde yapmış olduğu işlemler nedeniyle elde ettiği kişisel verilerin saklanmasından ve güvenliğinden sorumludur, b) Kişisel verileri ilgili kişinin onayı olmaksızın üçüncü kişilere iletemez ve başka amaçlarla kullanamaz".* Böylelikle elektronik ticaret etkinlikleri yürüten firmaların, bu süreç içerisinde elde ettikleri kişisel verileri korumaları hüküm altına alınmıştır. Ancak Elektronik Ticaret Kanunu'nda bu yükümlülüğe aykırı hareket edenler için bir yaptırım öngörülmemiş olması bir eksiklik olarak değerlendirilebilir.

Kişisel Verilerin Korunması Kanunu

Bankacılık Kanunu, Ceza Muhakemesi Kanunu, Hasta Hakları Yönetmeliği gibi çeşitli düzenlemelerde de konuya ilişkin hükümler yer almaktadır. Ancak bu hükümlerin uygulamada sınırlı bir koruma sağladığı dikkat çekmektedir. Bu bağlamda, Türkiye'de kişisel verilerin korunmasına yönelik temel ilkeleri belirleyerek önleyici koruma sağlayacak Kişisel Verilerin Korunması Kanunu uzun zamandır beklenmektedir.

Veri koruma alanında temel ilkeleri belirlemeye yönelik yasa hazırlıkları 1989 yılında başlamıştır. 2008 yılında TBMM'ye bir tasarı sevk edilmiş, ancak kadük olmuştur. 2010 yılı Anayasa değişiklikleri kapsamında kişisel verilerin korunmasını isteme hakkının anayasal bir hak olarak açıkça düzenlenmesi ile veri koruma alanında çerçeve nitelikte bir yasal düzenleme bir beklenti olmaktan öte anayasal bir zorunluluk hâline gelmiştir. 2012 yılında Adalet Bakanlığı bünyesinde yeni bir komisyon kurulmuş ve bu komisyonun çalışmaları neticesinde şekillenen yeni taslak üzerinde çeşitli değişiklik ve düzenlemelerin yapılmasının ardından 26 Aralık 2014 tarihinde Kişisel Verilerin Korunması Kanun Tasarısı Meclise sevk edilmiştir.

Kişisel Verilerin Korunması Kanunu 2016 yılında yasalaşmıştır. Kanunun 1. maddesine göre "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". Kişisel Verilerin Korunması Kanunu Yedi bölümden oluşmaktadır. Buna göre birinci bölümde Kanunun amaç ve kapsamı belirlenmiş; ayrıca kişisel veri, verilerin işlenmesi gibi konuya ilişkin son derece önemli tanımlara yer verilmiştir. Kanunun "kişisel verilerin işlenmesi" kenar başlıklı ikinci bölümünde ise veri işlemede hâkim olan temel ilkelere, kişisel verilerin işlenme şartlarına, özel nitelikli(hassas) kişisel verilere, verilerin silinmesi yok edilmesi ve anonim hâle getirilmesi ile kişisel verilerin aktarılması düzenlenmiştir. Kanunun ikinci bölümünde ayrıca kişisel verilerin üçüncü kişilere ve yurt dışında aktarımına ilişkin hükümler yer almaktadır.

Kanunun üçüncü bölümünde veri sorumlusunun aydınlatma yükümlülüğü ve veri güvenliğine ilişkin yükümlülükler ile birlikte ilgili kişinin hakları düzenlenmiştir. Bu düzenlemelerdeki temel hedef kişinin kendisi ile dijital ortamlarda her gün artan oranda işlenen verileri arasındaki bağın korunmasıdır. Bu açıdan önemli başka bazı hükümler de

dördüncü bölümde yer alır. Nitekim burada özellikle altıncı bölümde oluşum ve işleyiş prensipleri benimsenen Kişisel Verilerin Korunması Kuruluna şikâyet, bu şikâyetlerin inceleme esasları, yine Kurul Genel Sekreterliği tarafından tutulacak "Veri Sorumluları Sicilli" hüküm altına alınmıştır.

Kanunun 18. maddesi ile "görev ve yetkilerini kendi sorumluluğu altında, bağımsız olarak" yerine getireceği belirtilen bir Kişisel Verileri Koruma Kurulu oluşturulması öngörülmektedir. Görev alanına giren konularla ilgili olarak hiçbir organ, makam, merci veya kişi, Kurula emir ve talimat veremez, tavsiye veya telkinde bulunamaz. Kurul, dokuz üyeden oluşur. Kurulun beş üyesi Türkiye Büyük Millet Meclisi, dört üyesi Cumhurbaşkanı tarafından seçilir. Kurula üye olabilmek için; kurumun görev alanındaki konularda bilgi ve deneyim sahibi olmak, 14/7/1965 tarihli ve 657 sayılı Devlet Memurları Kanununun 48. maddesinin birinci fıkrasının (A) bendinin (1), (4), (5), (6) ve (7) numaralı alt bentlerinde belirtilen nitelikleri taşımak, herhangi bir siyasi parti üyesi olmamak ve en az dört yıllık lisans düzeyinde yükseköğrenim görmüş olmak şartlarını taşımak gerekir. Kurulun görev ve yetkileri ise şunlardır:

- Kişisel verilerin, temel hak ve özgürlüklere uygun şekilde işlenmesini sağlamak
- Kişisel verilerle ilgili haklarının ihlal edildiğini ileri sürenlerin şikâyetlerini karara bağlamak
- Şikâyet üzerine veya ihlal iddiasını öğrenmesi durumunda resen görev alanına giren konularda kişisel verilerin kanunlara uygun olarak işlenip işlenmediğini incelemek ve gerektiğinde bu konuda geçici önlemler almak
- Özel nitelikli kişisel verilerin işlenmesi için aranan yeterli önlemleri belirlemek
- Veri Sorumluları Sicilinin tutulmasını sağlamak.
- Kurulun görev alanı ile Kurumun işleyişine ilişkin konularda gerekli düzenleyici işlemleri yapmak
- Veri güvenliğine ilişkin yükümlülükleri belirlemek amacıyla düzenleyici işlem yapmak
- Veri sorumlusunun ve temsilcisinin görev, yetki ve sorumluluklarına ilişkin düzenleyici işlem yapmak.
- Bu Kanunda öngörülen idari yaptırımlara karar vermek

Kanunun yedinci bölümünde yer alan istisnalar, yani bütüncül olarak Kanunim kapsamı dışında kalacak alanlar en çok tartışılan hükümleri arasındadır. Bu noktada ilk dikkat çeken istisna istihbarat gibi bazı etkinliklerin kapsam dışında tutulmasıdır. İstihbaratın niteliği gereği gizli yürütülen bir etkinlik olduğu kabul edilse bile, hukuka ve dürüstlük kurallarına uygun olmak, belirli açık ve meşru amaçlar için işlenmek ya da işlendikleri amaç için gerekli olan süre kadar muhafaza edilmek gibi ilkeler bu alanda da öncelikle ve mutlaka geçerli olmalıdır.

Hukuksal güvenceler, bilişim teknolojileri ile temel hak ve özgürlükler arasındaki dengenin kurulabilmesi için en önemli araçtır. Ancak bunun yanında konuya ilişkin farkındalığın arttırılması ve kişisel önlemlerin alınması gerekir. Etkin veri koruması sağlanması yönündeki çalışmalar içerisinde teknolojideki gelişmelerden yardım almak ise son yıllarda dikkat çeken bir önem kazanmıştır. "Dizayn aracılığıyla gizlilik" (privacy by design, PbD) ya da "varsayılanlar aracılığıyla gizlilik" (privacy by default) bu kapsamda verilebilecek bir kaç örnektir.