

ANAYASAL BİR HAK OLARAK KİŞİSEL VERİLERİN KORUNMASI

Protection of Personal Data as a Constitutional Right

Dođan KILINÇ*

ÖZET

Demokratik ÷lkelerde bireylerin temel hak ve özgürlükleri, anayasalar tarafından güvence altına alınmıştır. Bireylere ait kişisel verilerin korunması da bu kapsamda değerlendirilmelidir. Kişisel veriler; belirli veya kimliği belirlenebilir gerçek ve tüzel kişilerle ilgili tüm bilgileri ifade eder. Kimlik bilgisi, yaş, medeni durum, telefon numaraları, adres bilgisi, sağlık bilgileri, pasaport bilgileri konuya örnek olarak verilebilir.

Kişisel verilerin hukuksal güvence altına alınması, temel hak ve özgürlüklerin korunması açısından önem taşımaktadır. Çünkü kişinin kendisine ait kişisel verilerin korunmasını talep etmesi temel hak ve özgürlüklerdendir.

Bilgi ve iletişim teknolojilerinde yaşanan gelişmeler, bilgiye elektronik ortamda erişimin kolaylaşması kişisel verilerin korunmasının önemini arttırmıştır. Örneğin, e-devlet uygulamalarıyla birlikte pek çok kişisel veri elektronik ortamda tutulmaktadır. Bu çalışmada, Türk hukukunda ve mukayeseli hukukta kişisel verilerin korunması incelenmiştir.

Anahtar Sözcükler: Kişisel veri, kişisel verilerin korunması, mahremiyet, anayasal hak.

* Dr., Bilgi Teknolojileri ve İletişim Kurumu (dkilinc@btk.gov.tr).

ABSTRACT

The fundamental rights and freedoms of the individuals have been assured by the Constitutions at the democratic states. Protection of the personal data shall be evaluated within this context. Personal data means all the data as to identified and to be identified real persons and legal entities. ID information, age, marital status, phone number, address information, medical history, passport information could be given as an illustration.

Ensuring legal protection of the personal data is of utmost importance for the protection of the fundamental rights and freedoms because the request from the individuals as to the protection of his or her own the personal data is deemed as a fundamental right and freedom.

Developments in the information and communication technology and easing of the access to the information electronically improved the importance of the protection of the personal data. For instance, most of the personal data could be kept and maintained electronically with the e-state practices. In this study, the protection of the personal data in Turkish law and comparative law has been examined.

Keywords: Personal data, protection of personal data, privacy, constitutional right.

GİRİŞ

Küreselleşme, günümüz dünyasını pek çok noktada etkileyen bir olgudur. Küreselleşmeyle beraber dünyada siyasal, ekonomik, sosyal ve kültürel yapılarda ciddi değişimler yaşanmaktadır. Bu değişimi etkileyen temel faktör ise bilgi ve iletişim teknolojilerinde meydana gelen baş döndürücü gelişmelerdir.

Yirminci yüzyıl siyasal, ekonomik, sosyal, teknoloji alanlarında hızlı gelişim ve değişimlerin yaşandığı bir dönem olarak tarihe geçmiştir. Gerçekten de bu yüzyılda özellikle bilgi ve iletişim teknolojilerinde çok hızlı gelişmeler görülmüştür. Bu teknolojiler, pek çok kolaylıklar yanında hukuki anlamda bazı sorunları da beraberinde getirmiştir. Bilgisayar vasıtasıyla yapılan dolandırıcılık, verilere yasa dışı erişim veya müdahale, bilgisayarlar aracılığı ile yapılan saldırılar (hacking), elektronik ticarete ortaya çıkan uyumsuzluklar konuya örnek olarak verilebilir.

Doğası gereği statik bir yapıya sahip olan hukukun, dinamik toplum hayatının gerisinde kalabildiği bilinen bir gerçekliktir. Bu durum, hukuk sistemi ile toplum yaşamı arasında çeşitli sorunlarının doğmasına neden olmuştur. Çağımızın fenomeni olan İnternet nedeniyle benzer sıkıntıların yaşandığını söyleyebiliriz.

Özel hayatın gizliliği, insan haklarıyla ilgili uluslararası belgelerde ve demokratik anayasalarda güvence altına alınmıştır. Kişinin fiziksel özellikleri, kişinin din, vicdan, düşünce ve görüşleri, sağlık, öğrenim, istihdam durumu ile ilgili bilgiler ve aile yaşamı, başkaları ile yaptığı haberleşmeler özel hayat kapsamındadır. Batılı hukuk sistemlerine göre özel hayatın gizliliği ve korunması esastır¹.

İçinde yaşadığımız dönem “bilgi çağı” olarak adlandırılmaktadır. Bu çağda bilgi ve iletişim teknolojilerinde inanılmaz bir gelişme yaşanmakta ve bu teknolojiler hızla sosyal hayatı kuşatmaktadır. Bilişim teknolojilerinin gelişimine paralel olarak, yazılı bilgi, ses, fotoğraf ve video vb. kişisel bilgiler içeren objelerin sanal ortamlarda paylaşımı giderek yaygınlaşmaktadır². İnternet, bilgi ve iletişim teknolojilerinin yaygınlaşmasında lokomotif bir rol oynamaktadır.

Bilgi ve iletişim teknolojileri sayesinde, kişisel verilerin derleme, sınıflandırma, saklama işlemlerine tabi tutulması ve istendiğinde kolayca sunulabilmesi kolaylaşmış ve bunun sonucunda özel yaşamla ilgili bu bilgilerin haksız olarak kullanılması riski ortaya çıkmıştır³. Bu teknolojiler, kişisel verilerin kişinin rızası alınmadan başkalarına açıklanmasına ve bilginin bulunduğu yerden başka yerlere aktarılmasına imkân sağlamaktadır⁴.

Sosyal ağlar, kişisel verilerin korunması konusundaki kaygılara çarpıcı bir örnektir. Sosyal ağlar; kişiler arasındaki olağan iletişim yollarını değiştiren, aradaki mesafelere bakmaksızın kişileri bir araya getiren ve kişilerin birbirleriyle İnternet ortamında iletişim kurmasını sağlayan sosyal ve ekonomik bir olgu olarak ortaya çıkmış ve son yıllarda hızla

¹ Pekşirin, Hülya, “Kişisel Verilerin Korunması Üzerine” 06.03.2011 tarihinde <http://bilisimsurasi.org.tr/listeler/tbs-hukuk/Feb/0026.html> adresinden erişildi.

² Cate, 2000, s. 877.

³ Cate, 1998, s. 3.

⁴ 06.03.2011 tarihinde <http://www.3sutun.com/NK/kisiselveri.html> adresinden erişildi.

yaygınlaşmıştır. Sosyal ağların üye sayısı dünyadaki pek çok ülkenin nüfusundan daha fazladır. Örneğin Facebook.com 800 milyon⁵, Twitter.com 500 milyon⁶, Myspace.com 125 milyon⁷, LinkedIn.com 135 milyon dolayında üye sayısına sahiptir⁸.

Sosyal paylaşım siteleri, kullanıcıların sosyal ağda yer alan profillerinden indirilen tüm bilgi ve resimlere erişilebilmeye ve bunların internet kullanan herkes tarafından görülebilmesine imkân sağlamaktadır. Başka bir ifadeyle, pek çok kişisel veri bu ortamlarda paylaşılmaktadır. Bu paylaşımlar dikkat edilmediği takdirde kişisel verilerin korunmasında bazı riskleri içermektedir.

Günümüzde gerek devlet gerekse özel sektör elektronik ortamda çeşitli hizmetler vermektedir. Bu hizmetlerin verilebilmesi için kişisel verilerin toplanması ve işlenmesi gerekmektedir⁹. Bu nedenle günümüzde, kişisel verilerin yaygın bir şekilde toplanarak işlenmesini kolaylaştırmak ve bunları bireylerin yararlanmasına sunmak adeta zorunlu hale gelmiştir.

Kişisel verilerin işlenmesi, çeşitli sorunları ortaya çıkarmıştır. Örneğin, öncelikle hangi veriler kişisel veri olarak kabul edilecektir? Bu verileri kimler toplayacaktır? Bu veriler nerelerde kullanılacaktır? Bu veriler ne kadar süre saklanacaktır? Bu verilere kimler ulaşabilecektir? şeklinde sorular çoğaltılabilir. Kısaca, toplanan kişisel verilerin nasıl korunacağı temel bir sorun olarak karşımıza çıkmaktadır.

Türkiye, kişisel verilerin korunmasıyla ilgili uluslararası düzenlemeleri takip etmektedir. Örneğin Türkiye, Avrupa Konseyince hazırlanan 108 sayılı “Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşme”yi imzalamıştır. 2010 yılında Anayasada yapılan değişikliklerle kişisel verilerin korunmasını anayasal bir hak haline getirilmiştir. Konuyla ilgili kanun tasarısı ise TBMM Adalet Komisyonunda görüşülmektedir.

⁵ 15 Ocak 2012 tarihinde <http://sosyalmedya.co/facebook-1-milyar/> adresinden erişildi.

⁶ 23 Ocak 2012 tarihinde <http://www.sosyalmedyahaber.com/twitter-kullanici-sayisi-500-milyona-ulasti/> adresinden erişildi.

⁷ 23 Ocak 2012 tarihinde <http://siberkultur.com/?q=myspace-webmail> adresinden erişildi.

⁸ 23 Ocak 2012 tarihinde <http://www.linkedin.com/> adresinden erişildi.

⁹ Edwards, 2004, s.316.

Bu çalışmada, anayasal bir hak olarak düzenlenen kişisel verilerin korunması, konuya ilişkin ulusal ve uluslararası düzenlemeler çerçevesinde incelenmiştir.

I- Kişisel Veri Kavramı, Kişisel Verilerin Korunması ve Tarihçesi

Kişilerin konu olduğu bilgilere “isme bağlı veriler” veya “bireysel veriler” denilmektedir. İsmeye bağlı veriler, gerçek veya tüzel kişi tarafından depo edilmekte, işlenerek bilgi haline getirilmekte, talep halinde üçüncü kişilere verilebilmektedir. Bu dolaşım bazen sınır ötesine de geçebilmektedir. Gerçek ve tüzel kişisel veri toplayıcıdır. Başta devlet olmak üzere, kamu yönetimleri, çeşitli kamu kuruluşları, özel hukuktaki kâr amaçlı kuruluşlar, sivil toplum kuruluşları çeşitli verileri toplamaktadır. Konuyla ilgili mesleklere ise doktorluk, avukatlık, noterlik, bankacılık örnek olarak verilebilir. Kısaca ifade etmek gerekirse, toplumda hemen herkes kişisel veri toplamakta, değerlendirmekte ve bunları çeşitli işlemlere tabi tutmaktadır¹⁰.

Kişisel verilerle ilgili öğretide ve konuya ilişkin hukuksal düzenlemelerde çeşitli tanımlar bulunmaktadır¹¹. Bunlardan en yaygın olan tanıma göre kişisel veri; “Belirli veya kimliği belirlenebilir bir kişiye ilişkin bütün bilgiler”dir¹².

Türk Dil Kurumu’na göre “kişisel” kelimesi “kişi ile ilgili, kişiye ilişkin, kişinin kendi malı olan, şahsi, zati” olarak; işlenmemiş ham bilgi olarak da ifade edilen “veri” ise “bilgi, data” olarak tanımlanmıştır¹³. Veri, “data” karşılığı olarak kullanılan ve “datum” sözcüğünün çoğulu olarak kullanılan kavramdır. Veri, çeşitli durumların, gözlemlerin veya oluşumların her türlü gösterimidir. Bilgi ve iletişim teknolojilerinde veri, “Bir durum hakkında, birbiriyle henüz bağlantısı kurulmamış bilinenler veya kısaca sayısal ortamlarda bulunan ve taşınan sinyaller ve/veya bit dizeleri” olarak tanımlanmaktadır¹⁴.

¹⁰ Akıllıoğlu, Tekin, “İdari Usul ve Kişisel Verilerin Korunması”, 6 Mart 2011 tarihinde www.idare.gen.tr/akillioglu-idariusul.htm adresinden erişildi.

¹¹ Millard, Christopher- Hon, W. Kuan, “Defining Personal Data in e-Social Science”, 6 Mart 2011 tarihinde <http://ssrn.com/abstract=1809182> adresinden erişildi.

¹² 6 Mart 2011 tarihinde <http://www.cnil.fr/english/the-cnil/personal-data/> adresinden erişildi.

¹³ 6 Mart 2011 tarihinde <http://tdkterim.gov.tr/bts/> adresinden erişildi.

¹⁴ 6 Mart 2011 tarihinde http://www.chip.com.tr/blog/thecrowsalvation/veri-bilgi-ve-bilisim_3332.html adresinden erişildi.

Kişisel Verilerin Korunması Hakkında Kanun Tasarısının 3. maddesinde kişisel veri; “Belirli veya kimliği belirlenebilir gerçek ve tüzel kişilere ilişkin bütün bilgiler” şeklinde ifade edilmiştir¹⁵.

Avrupa Konseyi tarafından hazırlanan “Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşme”nin 2. maddesinde kişisel veri; “Kimliği belirtilen veya belirtilebilen gerçek kişiyle ilgili tüm bilgiler” olarak tanımlanmıştır¹⁶.

Avrupa Birliğinde kişisel verilerle ilgili ilk düzenleme olan 1995/46 sayılı Direktif’in 2. maddesinde kişisel veri; “Kimliği belirtilen veya belirlenebilen bir kişiyle ilgili bilgi” olarak tanımlanmıştır¹⁷. Maddeye göre; bir kişinin doğrudan veya dolaylı olarak tanımlanabilmesine imkan sağlayan kişinin kimlik numarası, fiziksel, psikolojik, duygusal, ekonomik ve kültürel kimliği veya sosyal kimliği kişisel veri olarak değerlendirilebilir¹⁸. Yine, isim, telefon numarası, elektronik posta adresi, doğum tarihi, parmak izi, DNA, adres, sosyal güvenlik numarası, hesap numarası bu kapsamdadır.

Almanya Verilerin Korunması Kanunu'nda kişisel veri; “Belirli ya da belirlenebilen bir gerçek kişinin kişisel ya da maddi ilişkilerine ait münferit veriler olarak tanımlanmıştır. Avusturya Verilerin Korunması Kanunu'nda kişisel veri “Kimliği belirli ya da belirlenebilen ilgili hakkındaki bilgiler” şeklinde tanımlanmakta ve bireyin kişisel verilerinin korunması isteğinin temel haklardan birisi olduğu belirtilmektedir¹⁹.

¹⁵ 6 Mart 2011 tarihinde <http://www.kgm.adalet.gov.tr/tbmmkom/kisiselveriler.pdf> adresinden erişildi.

¹⁶ 10 Mart 2011 tarihinde http://www.avrupakonseyi.org.tr/antlasma/aas_108.htm adresinden erişildi

¹⁷ Millard and Hon, 2011, s. 3; Korff, Douwe, EC Study On Implementation Of Data Protection Directive, 2002, s.19 15 Mart 2011 tarihinde <http://ssrn.com/abstract=1287667> adresinden erişildi.

¹⁸ 15 Mart 2011 tarihinde http://epic.org/privacy/intl/eu_data_protection_directive.html#background; <http://www.cnil.fr/english/the-cnil/personal-data/> adreslerinden erişildi; Pekşirin, 2002.

¹⁹ Şimşek, Oğuz, “ 4422 sayılı Çıkar Amaçlı Suç Örgütleriyle Mücadele Kanunu ve Kanununun 4. Maddesine Göre “Kayıt ve Verilerin İncelenmesi” ve Kişisel Nitelikli Verilerin Korunması”, 15 Mart 2011 tarihinde <http://web.deu.edu.tr/ab/MAKALE/deu%20MAK/0012.htm> adresinden erişildi.

Bu tanımlardan hareketle kişisel veriyi kişiyi belirlenebilir kılan her türlü bilgi olarak tanımlayabiliriz. Bu bilgi gerçek kişilere ait olabileceği gibi tüzel kişilere de ait olabilir.

“Veri işleme” ise; kişisel bilgileri toplama, kullanma, açıklama, uyarılama, değiştirme, düzeltme, alma, birleştirme, engelleme, silme, aktarma, imha etme, kaydetme, düzenleme, saklama ve kullanma dâhil, otomatik araçlarla yapılp yapılmamasına bakılmaksızın kişisel bilgileri içeren herhangi bir işlemler dizisidir²⁰.

Kişisel verilerin korunması, özel hayatın gizliliği ve korunmasıyla doğrudan ilgilidir. Özel hayatın gizliliği, insan haklarının en önemlilerinden birisi olup, pek çok uluslararası düzenlemeye konu olmuştur. 1948 tarihli **İnsan Hakları Evrensel Bildirgesi** ’nin 12 inci maddesine göre²¹;

“Hiç kimsenin özel yaşamına, ailesine konut dokunulmazlığına ya da yazışma özgürlüğüne keyfi olarak karışılmaz; kimsenin onur ve ününe karşı kötü davranışlarda bulunulamaz. Herkesin bu karışma ve kötü davranışlara karşı yasalarla korunma hakkı vardır”.

Kişisel Verilen Korunması hususunda en eski düzenlemelerden birisi, 1950 tarihli A.İ.H.S.’in “Özel Hayatın ve Aile Yaşamının Korunması” başlıklı 8. maddesidir. 8. maddede kişisel veriler, özel hayatın gizliliği ilkesine dayanarak korunmuştur. Maddeye göre²²;

“Herkes özel ve aile hayatına, konutuna ve haberleşmesine saygı gösterilmesi hakkına sahiptir. Bu hakkın kullanılmasına bir kamu otoritesinin müdahalesi, ancak milli 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, zorunlu olan ölçüde ve yasayla öngörölmüş olmak koşuluyla söz konusu olabilir” Sözleşmeyle, belirli sınırlamalar dışında özel hayat koruma altına alınmıştır.

²⁰ Millard and Hon, 2011; Korff, 2002, s. 23.

²¹ 15 Mart 2011 tarihinde http://www.unicef.org/turkey/udhr/_gi17.html adresinden erişildi.

²² 15 Mart 2011 tarihinde <http://www.uhdigm.adalet.gov.tr/ihs.htm> adresinden erişildi.

1982 tarihli Anayasamızın 20. maddesine göre²³;“ Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz. Millî güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlâkın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak, usulüne göre verilmiş hâkim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; kimsenin üstü, özel kâğıtları ve eşyası aranamaz ve bunlara el konulamaz... ”. Görüldüğü gibi Anayasanın 20. maddesi Avrupa İnsan Hakları Sözleşmesiyle paralel bir şekilde kaleme alınmıştır.

İnsan Haklarını konu alan diğer birçok uluslararası belgede de benzer hükümler yer almaktadır. Kişisel verilerin korunmasına ilişkin ilk hukuki düzenlemeler **Avrupa Konseyince hazırlanmıştır**. Konsey, **1973 ve 1974 yıllarında** kabul ettiği iki kararla kişisel verilerin korunması için gerek kamu ve gerek özel sektör kurum ve kuruluşlarında göz önünde bulundurulması gereken ilkeleri belirlemiştir²⁴. Bu iki karar; özel ve kamu sektöründeki elektronik veri bankalarında tutulan kişisel verilerin korunmasında alınması gereken önlemlerdeki standartları belirlemiştir²⁵. Bu çalışmalarla, ulusal düzeyde çıkarılacak hukuksal düzenlemelere örnek olunmak istenmiştir. Ancak, bağlayıcı bir uluslararası belge çıkarılmadan ulusal mevzuatın istenen yönde gelişmesinin mümkün olmayacağı bu kararların tartışma sürecinde anlaşılmıştır²⁶. Bu nedenle, konuya ilişkin bir uluslararası sözleşme hazırlanmasına yönelik bir çalışma başlatılmıştır. Yapılan bu çalışmalar sonucunda, Avrupa Konseyi 1981 yılında “*Otomatik Olarak İşlenen Kişisel Veriler Bakımından Bireylerin Korunması Hakkında Sözleşme*”yi kabul edip imzaya açmıştır. *Bu sözleşme genelde 108 sayılı Sözleşme* olarak da bilinmektedir²⁷.

²³ 15 Mart 2011 tarihinde <http://www.anayasa.gov.tr/index.php?l=template&id=188&lang=0> adresinden erişildi.

²⁴ Robinson, Graux, Botterman, Valeri, 2009, s. 6; Pekşirin, 2002.

²⁵ Atak, s. 92.

²⁶ 15 Mart 2011 tarihinde <http://www.3sutun.com/NK/kisiselveri.html>; http://www.f1proje.com/eticaret/kisisel_verilerin_korunmasi_ve_gizliliği.php adreslerinden erişildi.

²⁷ 15 Mart 2011 tarihinde http://www.avrupakonseyi.org.tr/antlasma/aas_108.htm adresinden erişildi.

108 sayılı Sözleşme 1985 yılında yürürlüğe girmiştir. Avrupa Konseyi bu belge ile ilgili olarak bugüne kadar çeşitli tavsiye kararları almıştır. **1999** yılında Sözleşmede bazı değişiklikler yapılmıştır. **108 sayılı Sözleşme, kişisel verilerin korunması konusunda** yalnız Avrupa ülkelerinde değil, bütün dünyada kabul görmüş ve ulusal mevzuatın hazırlanmasında dikkate alınmıştır²⁸.

Kişisel verilerin korunmasındaki diğer uluslararası belge, Ekonomik İşbirliği ve Kalkınma Teşkilatı (OECD) tarafından 1981 yılında kabul edilmiş olan “Mahremiyetin Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkeler”dir²⁹. **Birleşmiş Milletler Genel Asamblesi** ise **1990** yılında “*Bilgisayarla İşlenen Kişisel Veri Dosyaları Hakkında Yönlendirici İlkeler*” adını taşıyan bir belge Kabul etmiştir³⁰.

Avrupa Birliği, 1995 yılında kişisel verilerin korunmasıyla ilgili 1995/46 sayılı Direktifi kabul etmiştir. Bu Direktif, kişisel verilere gerek kamudan gerekse de özel kişi ve kuruluşlardan gelebilecek ihlallere karşı önlem almayı ve ihlâl öncesi sistemli bir koruma sağlamayı amaçlamıştır³¹. Bu Direktif daha sonraki yıllarda revize edilmiştir. İlk değişiklik 2002³², daha sonraki değişiklik ise 2006³³ yılında yapılmıştır.

II- Kişisel Verilerin Korunması ve İnsan Hakları İçindeki Yeri

İnsan hakları, bireylerin doğuştan sahip olduğu dokunulmaz, devredilmez haklar olarak kabul edilmektedir. İnsan hakları, bildirilerde, anayasalarda ve uluslararası belgelerde yer alan önemli bir konudur. İngiltere’de 1215 Büyük Özgürlükler Fermanı ve 1689 Haklar Bildirisi, Amerika’da 1776 Virginia İnsan Hakları Bildirisi ve Amerikan Bağımsızlık

²⁸ Sırabaşı, Volkan, “Kişisel Verilerin (Bilgilerin) Gizliliği ve Korunması”, 16 Mart 2011 tarihinde http://www.fenafil.com/hukuk/internet/kisisel_veriler.htm adresinden erişildi; Pekşirin, 2002.

²⁹ 16 Mart 2011 tarihinde http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html adresinden erişildi.

³⁰ 16 Mart 2011 tarihinde <http://www.unhcr.org/refworld/publisher,UNGA,THEMGUIDE,,3ddcafaac,0.html> adresinden erişildi.

³¹ 16 Mart 2011 tarihinde <http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML> adresinden erişildi; Sırabaşı, 2011.

³² 16 Mart 2011 tarihinde <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:NOT> adresinden erişildi.

³³ 16 Mart 2011 tarihinde <http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:EN:HTML> adresinden erişildi.

Bildirisi, Fransa'da 1789 Fransız İnsan ve Vatandaş Hakları Bildirisi, konuya ilişkin başlıca bildirimlerdir. 1787 ve 1791 ABD Anayasaları, 1791 Fransız Anayasası, 1876 Kanuni Esasi ve günümüzün hemen hemen bütün anayasaları insan haklarına yer vermiştir.

İnsan hakları kavramı doğal hukuk anlayışına dayanmaktadır. İnsan, salt insan olma dolayısıyla bu haklara sahiptir, bu haklara sahip olabilmek için başka bir şart aranmaz. Bu haklar, vazgeçilmez, devredilmez ve zaman aşımına uğramazlar. Yürürlükteki hukuktan beklenen, bu hakları tanıması, koruması ve güvence altına almasıdır. Bu hakların varlığı, siyasal iktidarın tanınmasından bağımsızdır³⁴.

Tarihsel gelişimine baktığımızda insan haklarının üç kuşak halinde geliştiğini görürüz. Birinci kuşak haklar (kişi özgürlükleri ve siyasal haklar), ikinci kuşak haklar (sosyal, ekonomik hak ve özgürlükler), üçüncü kuşak haklar (dayanışma hakları).

Kişi özgürlükleri, negatif statü hakları olarak da ifade edilmektedir. Kişiyi devlete ve topluma karşı koruyan haklardır. Bu nedenle, koruyucu haklar olarak da ifade edilmektedir. Sosyal ekonomik haklar ile bireye, devletin müdahalelerine karşı ileri sürebileceği negatif haklar yanında, devletten olumlu bir davranış, hizmet ve yardım isteme hakkı veren pozitif haklar da tanınmıştır. Böylece devlet, vatandaşlarına sadece özgürlük vermekle yetinmeyecek, insan onuruna yakışır bir hayat sağlamakla da yükümlü olacaktır. Bu kategori, ikinci kuşak haklar olarak da ifade edilmektedir. Bu hakların ortaya çıkmasında sömürgecilikten yeni kurtulan üçüncü dünya devletlerinin önemli bir etkisi olmuştur. Üçüncü kuşak hakların ortaya çıkış sebebi ise bilim ve teknolojiye meydana gelen gelişmelerdir³⁵.

Federal Alman Anayasa Mahkemesi, "Nüfus Sayımı" kararında, bireyin kişisel nitelikli verileri üzerinde bir hakkının olduğunu kabul etmiştir. Bu hak, kişisel nitelikli verilerin akıbetini belirleme hakkıdır. Kararda bu hakkın, kişiliğin serbestçe geliştirilmesi hakkı ile insan onurundan kaynaklanan genel kişilik hakkının bu alandaki garantisi olduğu ifade edilmiştir. İsviçre Federal Mahkemesi de, devlet iktidarının bireye ilişkin

³⁴ Tunç, s.76.

³⁵ Kaboğlu, s. 28.

kişisel nitelikteki verilere sınırsız ve mutlak olarak müdahale yasağını, yazılı olmayan bir anayasal ölçü olarak kişi özgürlüğünden çıkararak bireyin kişisel nitelikli verilerine ilişkin hakkının hukuksal açıdan korunması gerektiği sonucuna ulaşmıştır³⁶.

Kişisel verilerin korunması negatif statü haklarından birisidir ve özel hayatın gizliliği temel hakkına dayanmaktadır. Özel hayatın gizliliği insanın şahsiyetinin korunmasında önemli bir araçtır.

Özel hayatın gizliliği, bütün modern demokratik hukuk devletlerinde benimsenmiş bir anayasa hukuku ilkesidir. Günümüz hukuk devletlerinde, kişi her yönüyle bir bütün olarak kabul edilmekte ve özel hayat da bu bütünün önemli bir parçası olarak görülmektedir. Özel hayatın hukuksal düzenlemelere konu olmasındaki temel amaç; insan kişiliğinin serbestçe gelişmesine imkân vermek, kişiye kendisi ve yakınları ile baş başa kalabileceği, devletçe ve başkalarınca rahatsız edilemeyeceği özerk bir alan sağlamaktır. Özel hayatın korunması insan şerefının korunmasında bir araçtır³⁷.

Gerek ulusal gerekse uluslararası düzenlemelerde özel hayatın tanımı yapılmamıştır. Ancak, öğreti ve yargı kararları vasıtasıyla bu eksiklik giderilmektedir. Örneğin, Avrupa İnsan Hakları Mahkemesine göre (A.İ.H.M.) özel hayat bütün unsurlarıyla tanımlanamayacak kadar geniş bir kavramdır. Ancak bu kavram, açık bir biçimde mahremiyet hakkından daha geniştir ve herkesin özgür olarak kişiliğini oluşturmasını ve geliştirmesini sağlayan bir alan içermekte olup, diğer insanlarla ve dış dünyayla ilişki geliştirmek hakkını da kapsar³⁸.

A.İ.H.M. Klass kararı³⁹ ile bireyin özel hayatına ilişkin verilerin kamusal organlar tarafından toplanmasına, depolanmasına ve işlenmesine dayanak oluşturacak önemli ilkeleri belirlemiştir. Bu kararda A.İ.H.M., bireyin özel yaşamı kapsamındaki bilgilere ilişkin kamusal müdahaleleri,

³⁶ Şimşek, 2001, 16 Mart 2011 tarihinde <http://www.bundesverfassungsgericht.de/entscheidungen.html> adresinden erişildi.

³⁷ Özbudun, 1997, s. 265

³⁸ Özdemir, Kenan, "Türk Hukukunda Ve Avrupa İnsan Hakları Sözleşmesi İle Avrupa İnsan Hakları Mahkemesi Kararlarında Özel Hayatın Gizliliği", 20 Mart 2011 tarihinde http://www.hukuki.net/hukuk/index.php?article=515#_ftnref62 adresinden erişildi.

³⁹ 20 Mart 2011 tarihinde <http://ihami.anadolu.edu.tr/aihmgoster.asp?id=30> adresinden erişildi.

bireyi koruyucu uygun ve etkili garantiler içeren yasal düzenlemeler bulunmadığı sürece Sözleşmenin 8. maddesinde belirtilen hakların bir ihlali olarak değerlendirmiştir⁴⁰.

A.İ.H.M., 1992 yılında vermiş olduğu Niemietz – Almanya kararında özel hayatla ilgili görüşlerini açıklamıştır. Mahkemeye göre; “*Özel hayat kavramını, bireyin kişisel hayatını istediği gibi yaşayabileceği bir ‘iç alan’la kısıtlamak ve bu alanın dışında kalan dış dünyayı bu alandan tamamen hariç tutmak aşırı sınırlayıcı bir yaklaşımdır. Özel hayata saygı, başka insanlarla ilişki kurmak ve söz konusu ilişkileri geliştirmek hakkını da bir dereceye kadar içermelidir*⁴¹.” Dolayısıyla, özel hayat, iç alanla sınırlanmamalı, dış dünya da konuya dahil edilmelidir. Mahkemeye göre; bir bireyin cinsel ilişkiler dahil çeşitli tür ilişkiler oluşturabilmesi ve cinsel kimliğini belirleme ve benimseme tercihi, yapılan telefon konuşmasının içeriği ne olursa olsun, özel haberleşmeye müdahale amaçlı gizli teknolojik aletlerin kullanılması, bir devlet tarafından bireyler hakkında rızaları alınmaksızın bilgi toplanması, zorunlu tıbbî tedaviler, başka insanlarla ilişki kurma ve bu ilişkileri geliştirme özel hayat kapsamında değerlendirilmelidir⁴².

Avrupa Konseyi Parlamenterler Meclisi’nin 428 sayılı kararında, özel hayat, “*zorunlu olarak bireyin kendi hayatını en az müdahale ile yaşamasını içerir. Özel, aile ve ev hayatı, fiziksel ve moral bütünlüğü, onuru ve şöhreti, aldatılma durumunda olmaktan sakınmak, ilgisiz ve utandırıcı gerçeklerin açıklanmaması, özel fotoğrafların izinsiz yayınlanmaması, güvenilerek verilen veya alınan enformasyonun açıklanmasının engellenmesi*” biçiminde tanımlanmıştır⁴³.

Özel hayat, doktrinde “Kişinin sadece kendisi için saklı tuttuğu ve başkalarının bilgisinden uzak kalmasını istediği yaşam görünümü”, “Herkes tarafından bilinmeyen, özel araştırma ve bilgi edinmeyle sağlanan kişiye ait hususlar”, “Kişilerin gizli hayat alanlarında yapmış oldukları faaliyetlerin başkaları tarafından bilinmemesini istedikleri taraflar”, “Bireyin

⁴⁰ Şimşek, 2001.

⁴¹ Özdemir, 2005.

⁴² Avcı, s. 5.

⁴³ Üzeltürk, Sultan, 1982 Anayasası ve İnsan Hakları Avrupa Sözleşmesine Göre özel Hayatın Gizliliği Hakkı, Beta, İstanbul 2004, s.168; İlkiz, Fikret, “Özel hayatın gizliliğinin ihlali”, 2007, 20 Mart 2011 tarihinde <http://bianet.org/bianet/bianet/98197-ozel-hayatin-gizliliginin-ihlali> adresinden erişildi.

kişiliğini geliştirmek ve manevi değerlerine güvence sağlamak için başkaları tarafından bilinmesini istemediği hususların oluşturduğu ve korunması hukuken gerekli görülen hayat üzerindeki hakkı⁴⁴ şeklinde tanımlanmaktadır.

Tanımlarda ortak olan nokta, kişiye ait bir alan ve bu alanın başkaları tarafından bilinmemesidir. Başka bir ifadeyle, özel yaşamda birey bu özgün alanın kendine hasredilmesini talep etmektedir.

Özel hayatta neyin gizlilik kapsamında olduğu tartışmalıdır. Bireyin kendine özgü ve başkasını ilgilendirmeyen bilgilerinin gizli kalması gerektiği söylenebilir. Örneğin, dini inanç, felsefi veya ideolojik görüş, bireyin katıldığı bir sosyal grup, kişisel veriler bu kapsamda değerlendirilebilir⁴⁵. Bu konuda yargı içtihatları bize yardımcı olmaktadır. A.İ.H.M. içtihatlarına göre; cinsiyet, medeni hal, doğum yeri, diğer kişisel veriler ile ilgili bilgileri içeren uygulamalar, parmak izi, fotoğraf ve diğer kişisel bilgilerin kaydedilmesi; tıbbi verilerin toplanması ve tıbbi kayıtların tutulması, sağlık, sosyal hizmetler ve vergi gibi idari ve sivil konuları ele alan bireysel kimlik belirleme sistemi kişisel veriler kapsamında değerlendirilmiştir⁴⁶.

Özel hayatın gizliliği, kişilik hakkının unsurlarından birisidir. Kişinin hak ve fiil ehliyeti yanında hayatı, sağlığı, şeref ve haysiyeti, sırları, vücut bütünlüğü, ismi ve diğer değerleri üzerindeki hakların tamamıdır⁴⁷. Kişilik hakları, çeşitli hukuk disiplinleri tarafından koruma altına alınmıştır. Kamu hukuku ve özel hukukta kişilik haklarını koruyan çeşitli hükümler bulunmaktadır.

Özel hayat, başlıca üç alanı kapsamaktadır⁴⁸.

Birincisi ortak alandır. Ortak hayat alanı, başkaları tarafından bilinmesinde herhangi bir sakınca görülmeyen ve topluma açık olan alandır. Başka bir ifadeyle ortak alan, bir kimsenin kültürel faaliyetlerde

⁴⁴ Avcı, 2006, s. 6.

⁴⁵ Doğan, Yusuf Hakkı, “Özel Hayata Karşı İşlenen Suçlar”, 20 Mart 2011 tarihinde <http://www.cezabb.adalet.gov.tr/makale/146.doc> adresinden erişildi.

⁴⁶ Doğan, 2005; Günaydın, 2007, s. 34

⁴⁷ Öztan, s. 251.

⁴⁸ Üzeltürk, 2004, s. 4.

bulunması, alışveriş merkezlerine gitmesi, toplu taşıma araçlarına binmesi gibi kamuya açık alanlardaki eylemlerinden oluşan alandır⁴⁹.

Ortak alanda kişinin statüsü de belirleyici bir etkidir. Bir bakanın, milletvekilinin, futbolcunun veya pop şarkıcısının ortak yaşamı ile sıradan bir kişinin ortak alanı şüphesiz farklı olacaktır. Bu tür durumlarda, özel yaşamınız ve özel yaşamınızdaki sınırlar daralır ve ortadan kalkar, artık kamuya açılmış ve ortak yaşam alanında yer alan bir kişi olarak, herkes sizin ne yaptığınızı, ne yediğinizi, ne içtiğinizi, nerelerde kiminle dolaştığınızı bilmek isteyecektir⁵⁰.

İkincisi, özel alandır. Bir kişinin ailesi, dostları, akrabaları, iş arkadaşları ve arkadaşlarıyla paylaştığı yaşam alanına, özel alan denir. Herkesin, özel hayat alanına giren olayların gizli kalmasını isteme hakkı vardır. Başka bir ifadeyle, kişiler özel yaşamına ilişkin konuların başkaları tarafından bilinmemesini isteyebilirler. Özel alan, gizli alana göre daha alenidir. Ancak, bu alenilik toplum nezdinde bir aleniliği ifade etmez⁵¹. Kişi, özel alana ait olayları yalnızca yakınlarıyla paylaşır. Bu nedenle, bu alana giren olayların üçüncü kişilere duyurulması halinde, özel hayat alanı ihlal edilmiş olur⁵².

Üçüncüsü, gizli alandır. Gizli alan, sır alan olarak da ifade edilmektedir. Kişi burada başkaları tarafından öğrenilmesini istemediği bir hayat yaşar ve bu alana giren olayları, sadece özel olarak, yakınlık hissettiği kişilerle paylaşır. Gizli hayat alanı, bir kimsenin hayatının en özel ve gizli kısmını oluşturur⁵³. Kişinin sırları, duyguları, düşünceleri, ümitleri, korkuları, tercihleri, gibi konular bu alana girer. Kişilerin yalnız kalma hakları vardır. Gizli alan dokunulmaz olduğu gibi, her türlü müdahaleye karşı da hukuki koruma altındadır. Bu alanda yer alan bilgiler basın, yayına kapalıdır. Özel alan gibi gizli alan da hem kamu hukuku hem de özel hukuk kuralları ile koruma altına alınmıştır⁵⁴. Siyasal

⁴⁹ Özbudun, 1997, s. 266.

⁵⁰ Özbudun, 1997, s. 266; Fikret İlkiz, “ Kişilik Hakları ve Medya”, 16 Mart 2011 tarihinde http://www.byegm.gov.tr/seminerler/mardin_viii/mardin_17.htm adresinden erişildi.

⁵¹ İlkiz, 2006, Günaydın, 2007, s. 34; Özbudun, 1997, s. 266.

⁵² Ülkü, Muhammet Murat. (2005). *5237 Sayılı TCK 132-140 Maddelerinde Yer Alan Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar*. Samsun, s.10.

⁵³ Ülkü, 2005, s. 10.

⁵⁴ Günaydın, 2007, s. 34.

mahremiyet, tıbbi mahremiyet, İnternette mahremiyeti, devlet müdahalelerine karşı mahremiyet, iş yeri mahremiyeti de özel alan kapsamında değerlendirilmelidir.

Özel hayatın gizliliği hakkı, ülkemizde iki şekilde korunmaktadır. Birincisi, özel kişilerin tecavüzlerine karşı korumadır. Burada hem ceza hem de özel hukuk mevzuatı bu korumayı sağlayıcı tedbirleri içermektedir. İkincisi ise, özel hayatın gizliliğinin devletin ihlallerine karşı korunmasıdır. Bu yönüyle de konu, bir anayasa hukuku sorunu olduğundan anayasal düzenlemelere konu olmaktadır⁵⁵. Devlet, cebir kullanan bir cihaz olduğundan, özel hayatın gizliliğine karşı devletten gelebilecek tecavüzlerin, özel kişilerden gelebilecek olanlara oranla, daha ciddi olacağı söylenebilir.

Devlet müdahalelerine karşı mahremiyet üzerinde durulması gereken bir husustur⁵⁶. 1960'lı ve 1970'li yıllarda bilgi teknolojilerindeki gelişmelerle birlikte mahremiyet hakkına ilgi artmıştır. Gözetim potansiyeli yüksek bilgisayar sistemleri, kişisel bilgileri toplama ve işleme yönetiminde spesifik düzenlemeleri harekete geçirmiştir. "Mahremiyet Hakkı"nın yasal çerçevede korunması fikri Amerikan kökenli olmasına rağmen, konu ilk olarak Avrupa'da kapsamlı düzenlemelere konu olmuştur. Bu alandaki ilk düzenleme 1970 yılında Almanya'da yapılmıştır. Bunu 1973'te İsveç, 1974'te Amerika Birleşik Devletleri ve 1977'de Fransa izlemiştir⁵⁷.

Mahremiyet, insan haysiyetinin temelini oluşturan ifade özgürlüğü, örgütlenme özgürlüğü gibi temel insan hak ve özgürlüklerden birisidir. Bir anlamda mahremiyet, "Bütün insan haklarının bir parçasıdır"⁵⁸. Her insanın bu hakkına saygı gösterilmesini istemesi makul bir beklentidir. Bilgi ve iletişim teknolojilerinde meydana gelen gelişmelerden dolayı mahremiyet modern zamanlardaki en önemli insan haklarından birisi olmuştur. Mahremiyet, insan haklarının korunmasında anahtar bir değerdir. Mahremiyet; sadece gerçek kişileri ilgilendiren bir konu değildir. Gerçek

⁵⁵ Özbudun, 1997, s. 267.

⁵⁶ Cate, 2000, s. 884.

⁵⁷ Cate, 1998, s. 5; 16 Mart 2011 tarihinde [https://www.privacyinternational.org/article/phr2006-overview-privacy#\[1\]](https://www.privacyinternational.org/article/phr2006-overview-privacy#[1]) adresinden erişildi.

⁵⁸ 16 Mart 2011 tarihinde [https://www.privacyinternational.org/article/phr2006-overview-privacy#\[1\]](https://www.privacyinternational.org/article/phr2006-overview-privacy#[1]) adresinden erişildi.

kişilerin yanı sıra, tüzel kişilerin de bu kavram dâhilinde hakları bulunmaktadır⁵⁹.

Mahremiyet, pek çok bölgesel ve uluslararası insan hakları sözleşmelerinde koruma altına alınmıştır. Birleşmiş Milletler İnsan Hakları Evrensel Bildirisi ile Medeni ve Siyasi Haklar Sözleşmesi, Avrupa İnsan Hakları Sözleşmesi konuya örnek olarak verilebilir. Yine mahremiyet pek çok ülkede anayasal bir hak olarak düzenlenmektedir. Mahremiyet, anayasalarda genellikle açıkça tanımlanmamakta terimin kapsamı yargı içtihatlarıyla şekillenmektedir⁶⁰.

Mahremiyet, pek çok ülkede veri koruma içerisinde erimiştir. Başka bir ifadeyle, terim kişisel verilerin korunması içerisinde değerlendirilmektedir. Mahremiyet, özel hayat kavramıyla yakından ilgili olup, dünyada kültürlere ve bölgelere göre çeşitli şekillerde tanımlanmaktadır. Mahremiyetin tanımı toplumlara ve çevreye göre değişmektedir. Bu nedenle mahremiyet, insan hakları kataloğu içerisinde tanımlanması en zor olan kavramlardan birisidir⁶¹.

Mahremiyet; yalnız olma durumu ve başka kimseler tarafından gözetlenmeme veya rahatsız edilmeme halidir⁶². Terim, Türk Dil Kurumu Sözlüğünde kişisel gizlilik olarak tanımlanmıştır⁶³. Başka bir tanıma göre mahremiyet; bireylerin, grupların veya kurumların kendilerine dair bilgilerin ne zaman, nasıl ve ne ölçüde diğerlerine aktarılabilceğini kendilerinin belirleme hakkıdır.

Mahremiyet, ABD yargıcı Cooley tarafından 1888’de “yalnız kalma hakkı” tanımlanmıştır. Başka bir ifadeyle, gözden irak olma hakkıdır. 1890’da Amerikalı hukukçular, Louis Brandeis ve Samuel Warren mahremiyeti detaylı olarak irdelemişler ve kavramı “Yalnız bırakılma hakkı,

⁵⁹ Arslan, Hilmiye, “Amerika İle Avrupa Birliği Hukuki Düzenlemelerinin Gizlilik Haklarına Bakış Açısının Karşılaştırılması”, s. 1, 16 Mart 2011 tarihinde <http://inet-tr.org.tr/inetconf10/bildiri/18.doc> adresinden erişildi.

⁶⁰ 16 Mart 2011 tarihinde <https://www.privacyinternational.org/article/phr2006-overview-privacy#> adresinden erişildi.

⁶¹ 16 Mart 2011 tarihinde <https://www.privacyinternational.org/article/phr2006-overview-privacy#> adresinden erişildi.

⁶² Arslan, 2010.

⁶³ 16 Mart 2011 tarihinde <http://tdkterim.gov.tr/bts/?kategori=verilst&kelime=mahremiyet&ayn=tam> adresinden erişildi.

hakların en kapsamlısı ve özgür insanlar tarafından en çok değer verilen hak” olarak tanımlamışlardır⁶⁴. Brandeis’e göre; mahremiyet anayasal demokrasinin önemli bir göstergesidir. Başka bir bilim adamı mahremiyeti; açık olma ile yalnız, özel, anonim olabilme arasında karar verebilme olarak tanımlamıştır⁶⁵. Özgür ve demokratik bir toplum olmak, bireyin bağımsızlığına saygı göstermeyi gerektirir.

Mahremiyet, rahatsız edici unsurlardan özgür olduğumuz fiziksel alan arzusu, kendimiz hakkındaki kişisel bilgileri açıklama zaman ve tarzını kontrol edebilme yetisidir. Mahremiyet, insan kişiliği ile ilgilidir ve bireyin kişiliğini, bağımsızlığını, onurunu ve bütünlüğünü korur⁶⁶.

Mahremiyet hakkı, sırları gizli tutma hakkını ve onları ancak özel konuşmalarda paylaşmayı kapsar. Mahremiyet üç unsurdan oluşur. Gizlilik, anonimlik ve yalnızlık. Mahremiyet, bireyin kendi seçimine bağlı kaybolma hakkı olarak da ifade edilmektedir⁶⁷. Mahremiyet kavramının, başkasının iletişiminin yasa dışı denetlenmemesi veya kişisel bilgilerinin yasal olmayan yollarla işlenmemesi ya da başka bir kimseyle paylaşılmaması gibi yönleri de bulunmaktadır⁶⁸.

Mahremiyet kavramının üç çeşidi bulunmaktadır. Birincisi, mekansal mahremiyet, ikincisi, kişi mahremiyeti ve üçüncüsü de bilgi mahremiyetidir. Mekansal mahremiyet; kişiyi çevreleyen yakın fiziksel alanı korumayı, kişi mahremiyeti; kişiyi haksız müdahalelere karşı korumayı, bilgi mahremiyeti ise, kişisel verilerin toplanma, saklanma, işleme ve dağıtımının nasıl

⁶⁴ Samuel Warren and Louis Brandeis. (1890). The Right to Privacy, *Harvard Law Review* Vol. 4, s. 193-220, aktaran Robinson, Graux, Botterman, Valeri, 2009, s.1; Kleve Pieter and De Mulder Richard, “Privacy Protection and the right to information: in search of a new symbiosis in the information age”, Ed. Kierkegaard Sylvia Mercado, Ankara Bar Association Cyberlaw Security & Privacy, The Second International Conference on Legal, Security and Privacy Issues in Information Technology (LSPI) 2007, Beijing China, s. 331; Tansuğ, Avniye, “AB’nin Yeni Ekonomik Silahı: Veri Saklama Hukuku”, http://www.acikradyo.com.tr/default.aspx?_mv=a&aid=14260 adreslerinden erişildi.

⁶⁵ Cate, 2000, s.877; 20 Mart 2011 tarihinde <https://www.privacyinternational.org/article/phr2006-overview-privacy#> adresinden erişildi.

⁶⁶ 20 Mart 2011 tarihinde [https://www.privacyinternational.org/article/phr2006-overview-privacy#\[](https://www.privacyinternational.org/article/phr2006-overview-privacy#[) adresinden erişildi.

⁶⁷ Eralp, Özgür, “KPS (Kimlik Paylaşım Sistemi), AKS(Adres Kayıt Sistemi) Uygulamaları Işığında Bireysel Mahremiyet” 20 Mart 2011 tarihinde <http://www.ozgureralp.av.tr/makaleler/tckimliktdb.htm> adresinden erişildi.

⁶⁸ Arslan, 2010.

yapılacağını veya yapılmayacağını kontrol etmeyi gerektirir⁶⁹.

Mahremiyet bir insan hakkı olarak değerlendirildiğinde, mahremiyetin öncelikle güç tekeli elinde bulunduran devlete karşı korunması gerektiği söylenebilir. Uluslararası düzeyde korunan insan hakları belgelerinde özel hayatın gizliliği, kişilerin birbirleriyle olan ilişkilerindeki ihlallerden ziyade devletin yaptığı ihlallere yönelik bir koruma sağlamaktadır. Kişilerin gizli bilgilerine ulaşılması devletler için birçok konuda gereklidir. Özellikle adli soruşturma ve kovuşturmalarda, bu bilgilere ulaşılması adaletin gerçekleştirilmesi açısından hayati önemi haizdir⁷⁰. Bilişim teknolojilerinin oldukça geliştiği ve yaygınlaştığı günümüzde, yargı kararıyla iletişimin denetlenmesi suçla mücadelede önemli birer araç olarak karşımıza çıkmaktadır⁷¹.

Özel hayat, Avrupa Konseyi Parlamenterler Meclisi tarafından 428 (1970) sayılı kararı ile kabul edilen “Kitleli İletişim Araçları ve İnsan Hakları Bildirisi”nde bir kişinin hayatını minimum müdahaleyle yaşama hakkı olarak tanımlanmıştır. Bildiriye göre özel hayat; esas olarak kişinin kendi hayatını en az müdahale ile sürdürmesinden ibarettir. Bu hak özel hayat, aile hayatı ile kişinin fiziksel ve ruhsal bütünlüğünü, onurunu, kişiyi olduğundan farklı göstermekten kaçınmayı, gereksiz ve utandırıcı şeylerin açıklanmasını, özel fotoğrafların izin alınmadan yayınlanmamasını, casusluğa karşı korumayı ve haklı görülemez ve kabul edilemez yerli yersiz konuşmayı, özel iletişimin kötüye kullanılmasına karşı korumayı, kişi tarafından gizli olarak iletilmiş ve elde edilmiş bilgilerin ifşa edilmesine karşı korumayı da içermektedir⁷². Karara göre; kişinin özel hayatına en düşük düzeyde müdahale esastır.

III- Uluslararası Düzenlemelerde Kişisel Verilerin Korunması

Elektronik ortamlarda yapılan işlem sayısının her geçen gün artması, kişisel verilerin korunmasında yeni önlemler alınması ve düzenlemeler yapılmasını zorunlu hale getirmiştir. Gerek devletler, gerekse uluslararası

⁶⁹ Eralp, 2007.

⁷⁰ Günaydın, 2007, s. 38.

⁷¹ Bu konuda ayrıntılı bir çalışma için bkz. Yardımcı, Murat, Türk Hukukunda İletişimin Denetlenmesi, Seçkin Yayıncılık, Ankara, 2009.

⁷² İlkiz, Fikret, “Özel hayatın gizliliğinin ihlali”, 2007, 20 Mart 2011 tarihinde <http://bianet.org/bianet/bianet/98197-ozel-hayatin-gizliliğinin-ihlali> adresinden erişildi.

örgütler konuyla ilgili önlemler almaya çalışmaktadır. Günümüzde bir taraftan kişisel verilerin elektronik ortamlarda kullanılması adeta zorunlu hale gelirken diğer taraftan, hakkında veri toplanan kişinin kişilik haklarının korunması da gerekmektedir⁷³.

Özel hayat, Birleşmiş Milletler İnsan Hakları Bildirisi, Medeni ve Siyasal Haklar Sözleşmesi başta olmak üzere, pek çok uluslararası belgede temel insan haklarından birisi olarak düzenlenmiştir⁷⁴. Uluslararası hukukta mahremiyet ve kişisel verilerin korunmasında devletleri hukuksal düzenleme yapmaya zorlayan üç önemli neden bulunmaktadır. Birincisi; geçmişteki adaletsiz uygulamaları düzeltmektir. Pek çok ülkede geçmişteki otoriter rejimler döneminde meydana gelen mahremiyet ihlalleri, veri korumada düzenleme yapılmasının temel nedenlerinden birisi olmuştur. Özellikle Orta Avrupa ülkeleri, Güney Amerika ve Güney Afrika bu kapsamdaki yerlerdendir⁷⁵.

Devletleri düzenleme yapmaya iten ikinci neden elektronik ticareti desteklemektir. Dünyada pek çok ülke elektronik ortamda ticareti desteklemek için hukuk sistemlerini geliştiren düzenlemeler yapmışlardır. Özellikle Asya kıtasında ve gelişmiş ülkelerde bu durumu görürüz. Bu ülkeler, günümüzde kişisel bilgilere ulaşmanın kolaylığı karşısında tüketicilere güvenceler sağlamak için çeşitli düzenlemeler yapmışlardır. Sınır ötesi veri paylaşımında sağlanan güvenceler konuya örnek olarak verilebilir. Mahremiyet düzenlemeleri, elektronik ticaretin kurallarını belirleyen paketdeki ilk parçalardan birisi olmuştur⁷⁶.

Kişisel verilerin korunmasında devletleri hukuksal düzenleme yapmaya zorlayan üçüncü neden ise; Avrupa Birliği Hukukunda yeknesaklık sağlamaktır⁷⁷. Merkez ve Doğu Avrupa'daki pek çok ülke Avrupa Konseyi'nin kişisel verilerin korunmasına ilişkin 108 Sayılı Sözleşmesi ile

⁷³ Ersoy, Eren "Gizlilik, Bireysel Haklar, Kişisel Verilerin Korunması", s. 4 20 Mart 2011 tarihinde <http://ab.org.tr/ab06/bildiri/6.doc> adresinden erişildi.

⁷⁴ Robinson, Graux, Botterman, Valeri, 2009, s. 6.

⁷⁵ 20 Mart 2011 tarihinde <https://www.privacyinternational.org/article/phr2006-overview-privacy#> adresinden erişildi.

⁷⁶ 20 Mart 2011 tarihinde <https://www.privacyinternational.org/article/phr2006-overview-privacy#> adresinden erişildi.

⁷⁷ 20 Mart 2011 tarihinde <https://www.privacyinternational.org/article/phr2006-overview-privacy#> adresinden erişildi.

Avrupa Birliği'nin Veri Koruma Direktifini kabul etmişlerdir. Bu düzenlemeler veri korumada yeknesaklığı sağlamada önemli enstrümanlardandır⁷⁸.

Uluslararası belgelerde kişisel verilerin korunmasında ortak temel ilkeleri şunlardır⁷⁹:

- Bireyler, kişisel verileri toplandığında bundan haberdar edilmelidir.

- Bireylerin talebi üzerine, veriyi kimin hangi nedenle istendiği söylenmelidir. Bunun için de veri öznesinin veriyi kısmen veya tamamen kontrol edebilmesi sağlanmalıdır.

-Bireylere, kendileri hakkındaki verilere bunların doğruluk ve güncelliğini denetlemek için nasıl ulaşabilecekleri belirtilmelidir.

- Bireylerin verilerinin kötüye kullanmalara karşı nasıl korunacağı belirtilmelidir.

Bu şartların, büyük miktarlarda kişisel verilerin toplandığı, işlendiği ve transfer edildiği günümüz dünyasında uygulanması pek kolay değildir⁸⁰. Günümüzde gerek devletler güvenlik ve kamu hizmetlerini geliştirmek amacıyla gerekse şirketler ticari amaçlarla verileri işlemektedirler. Ancak, yine de veri öznesinin haklarına saygı çerçevesine bu ilkelerin etkin bir şekilde uygulanmasına çalışılmalıdır.

A. Ekonomik İşbirliği ve Kalkınma Teşkilatı Belgelerinde Kişisel Verilerin Korunması

Kişisel verilerin korunması konusundaki çok uluslu ilk inisiyatif 1980'de ortaya çıkmıştır. Ekonomik İşbirliği ve Kalkınma Teşkilatı (OECD), 1980 yılında "Mahremiyetin Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkeler"i kabul etmiştir⁸¹. Bu belgeyle; verilerin korunması ve sınır ötesi dolaşımına ilişkin temel prensipler belirlenmiştir. Ancak, bu kılavuzun hukuksal bir bağlayıcılığı bulunmamaktadır. Kılavuz, ayrıca uygulamalarda devletlere geniş bir takdir yetkisi vermektedir⁸².

⁷⁸ Edwards, 2004, s. 320.

⁷⁹ Robinson, Graux, Botterman, Valeri, 2009, s. 2.

⁸⁰ Tene, 2010, s. 1.

⁸¹ Tansuğ, 2006; Pekşirin, 2002.

⁸² Tene, 2010, s.1; Cate, 1998 s. 6.

Bu belge, kişisel verilerin toplanması, yönetilmesi ve korunması ile sınır ötesi paylaşımında temel ilkelerin belirlenmesi amacıyla hükümetler, iş dünyası, sivil toplum örgütleri katılımıyla kabul edilmiştir. Böylece, uluslararası konsensüsün sağlanması, gizliliğin korunmasında etkinlik ile verilerin akışındaki serbestlik arasında dengenin kurulması ve ülkelerin gerek kamu sektörü gerekse de özel sektör bazında uygulamalarını temin etmek amacıyla iç düzenlemeler yapması konusunda fikir uyandırılması amaçlanmıştır⁸³.

Rehber İlkeler'de, otomatik veri işleme yöntemlerinin geliştirilmesiyle beraber büyük miktardaki verilerin kısa sürede sınır ötesine iletilmenin mümkün olduğu, bu nedenle kişisel verilerle ilgili gizliliğin korunmasına yönelik ilkelerin belirlenmesine ihtiyaç duyulduğu, zira kişisel verilerin kanun dışı yollarla kaydedilmesi ve depolanması veya bunların yetkisiz olarak açıklanması veya kötüye kullanılması gibi durumların insan haklarına aykırı olacağı, son yıllarda geliştirilen yeni bilgisayar ve iletişim teknolojisinin yaygınlaşmasıyla büyük bir hızda artan veri transferleri üzerinde bazı sınırlamalara gidilmesi gerektiği, ancak bu tür sınırlamaların özellikle bankacılık ve sigortacılık gibi ekonomi üzerinde büyük öneme sahip sektörlerde ciddi sorunlara yol açabileceği, o nedenle kişisel verilerin korunması ile veri akışındaki serbestlik arasındaki dengenin titizlikle kurulması gerektiği ifade edilmiştir⁸⁴.

Rehber İlkelerin kapsamı, gizliliğin ve kişi özgürlüklerinin korunması amacıyla özel ve kamu sektöründe otomatik yöntemlerle işlenen kişisel veriler olduğu belirtilmiştir. Ancak, bunlara ulusal egemenlik, ulusal güvenlik ve kamu politikası ile ilgili istisnalar konulabilir.

Rehber İlkelerle ülkelerin alması gereken asgari veri koruma ilkeleri ise şunlardır⁸⁵:

1- Veri toplamasının sınırlı olması ilkesi: Bu ilkeye göre, kişisel verilerin toplanmasına sınır getirilmelidir. Kişisel verilerin toplanması, sadece hukuka uygun olarak, dürüst araçlarla, gerektiğinde veri öznesinin rızası veya bilgisi dâhilinde gerçekleştirilmelidir.

⁸³ Ersoy, 2009. s. 52.

⁸⁴ Ersoy, 2009, s. 53.

⁸⁵ Gür, 2009. s.111; Uygun, 2010, s. 27; 25 Mart 2011 tarihinde http://www.oecd.org/document/18/0,2340,en_2649_201185_1815186_1_1_1_1,00.html adresinden erişildi.

2- Veri kalitesi ilkesi: Kişisel veriler amacına uygun olmalı ve bu amaç için gerekli ölçüde, eksiksiz ve güncel olmalıdır.

3- Amacın belli olması ilkesi: Kişisel verilerin toplandığı amaç verilerin toplanma anında belirlenmiş olmalıdır. Veriler, daha sonra bu amaç dışında kullanılmamalıdır.

4- Kullanmanın sınırlı olması ilkesi: Bu ilkeye göre kişisel veriler, açıklanamaz. Ancak, veri öznesinin rızası veya kanun tarafından öngörülen durumlar bunun dışındadır.

5- Veri güvenliği ilkesi: Bu ilkeye göre kişisel veriler, kaybolma yetkisiz erişim, tahrip edilme, kullanma, değiştirilme veya ifşa edilme gibi risklere karşı uygun güvenlik önlemleri vasıtasıyla güvence altına alınmalıdır.

6- Açıklık ilkesi: Bu ilkeye göre kişisel verilere ilişkin olarak, işlemler ve önlemler genel olarak aleniyet politikası çerçevesinde gerçekleştirilmelidir.

7- Bireyin katılımı İlkesi: Bireyin katılım hakkı çerçevesinde birey, her şeyden önce esas veri sorumlusu vasıtasıyla ya da başka bir usulle kendisini ilgilendiren verilerin mevcut olup olmadığının onaylanmasını talep hakkına sahiptir. Burada, belirtilen hakların kullanımının reddedilmesi durumunda talebin neden reddedildiğinin gerekçe ile bildirilmesini isteme ve ret kararına karşı hukuk yollarına başvurabilme hakkı da düzenlenmiştir. Ayrıca veri öznesine, kendisi hakkında veri işlenmesine itirazda bulunma ve itirazın haklı bulunması halinde kendisi hakkındaki verilerin silinmesini, düzeltilmesini, eksikliklerinin tamamlanmasını veya değiştirilme yapılmasını isteme hakkı da öngörülmüştür⁸⁶.

8- Hesap verilebilirlik İlkesi: Veri sorumlusu yukarıdaki ilkelerin hayata geçirilebilmesi için gerekli önlemlere riayet etmesi bakımından hesap verebilir durumda olmak zorundadır.

⁸⁶ Gür, 2009, s. 112.

OECD tarafından hazırlanan diğer belgeler ise; 1985 tarihli “Sınırötesi Veri Transferi Hakkında Bildirge” ve 1998 tarihli “Global Ağ Gizliliğinin Korunması Hakkında Bakanlık Bildirgesi”dir⁸⁷.

OECD rehber ilkeleri, özel hayatın gizliliğinin korunmasına yönelik haklar ve gereksinimleri uyumlaştırmayı amaçlayan Avrupa Konseyinin çabalarına paralel olarak yapılan çalışmalardır. Ancak rehber ilkelerin hukuksal bir bağlayıcılığın bulunmamaktadır. Bununla birlikte OECD'nin kabul ettiği rehber ilkeler iletişim politikası hususunda uluslararası uzlaşmaya ulaşabileceğini göstermesi açısından önemlidir⁸⁸.

B. Birleşmiş Milletler Belgelerinde Kişisel Verilerin Korunması

Birleşmiş Milletler, 1990 yılında kişisel verilerin korunması konusunda “Bilgisayarla İşlenen Kişisel Veri Dosyaları Hakkında Yönlendirici İlkeler” adını taşıyan bir belge kabul etmiştir⁸⁹. Belgede kişisel verilerin korunmasına ilişkin ilkeler ayrıntılı bir şekilde açıklanmıştır. Bu ilkeler şunlardır⁹⁰:

1. Yasallık ve dürüstlük: Kişisel veriler kanuna aykırı ve dürüst olmayan yollarla toplanmamalı ve toplanış amacına ve temel haklar ve özgürlüklerle ilgili ilkelere aykırı olarak kullanılmamalıdır.

2. Doğruluk: Toplanan verilerin doğruluğu kontrol edilmeli ve doğru ve eksiksiz olarak saklanması ve güncelliğini sağlamak için saklandığı süre zarfında düzenli olarak kontrol edilmelidir.

3. Amacın belirli ve haklı olması: Kişisel verilerin hangi haklı amaçla toplandığı başlangıçta kesin olarak belirlenmeli ve bu amaç bütün ilgililere açık olarak bildirilmelidir.

4. İlgili kişilerin erişme hakkı: Kişisel veri ile ilgili kişi kimliğini kanıtlamak koşulu ile kendisi hakkında toplanan bilgilerin ne gibi bir işleme tabi tutulduğunu öğrenebilmeli ve bunların bir anlaşılabilir biçimdeki bir örneğini aşırı bir masraf ve zaman kaybı olmadan elde edebilmelidir.

⁸⁷ 25 Mart 2011 tarihinde <http://www.oecd.org/dataoecd/39/13/1840065.pdf> adresinden erişildi.

⁸⁸ Gür, 2009, s. 112.

⁸⁹ 25 Mart 2011 tarihinde <http://www.unhcr.org/refworld/publisher/UNGA,THEMGUIDE,,3ddcafaac,0.html> adresinden erişildi.

⁹⁰ Kesmez, 2001; Pekşirin, 2002.

5. Ayrımcılıktan kaçınma: Kişinin etnik kökeni, ırkı, cinsel yaşamı, dini veya felsefi inançları gibi duyarlılık konularla ilgili bilgiler ancak yasanın izin verdiği haklı ve gerekli durumlarda toplanmalıdır.

6. İstisna koyma yetkisi: Görevli makamlara, milli güvenliği, kamu düzenini, halk sağlığını, genel ahlakı korumak veya diğer kişilerin hak ve özgürlüklerine zarar vermemek amacıyla yasallık ve dürüstlük, doğruluk, amacın belirli ve haklı olması, ilgili kişilerin erişme hakkı ilkeleri ile ilgili önlemlerden ayrılma yetkisi tanınabilir. Ancak bu yetkinin kapsamı ve sınırları kanunda açıkça belirlenmelidir. Ayrımcılıktan kaçınma ilkesine getirilecek istisnanın her durumda temel hak ve özgürlüklere aykırı olmaması gerekir.

7. Güvenlik: Kişisel verilerin toplanması, saklanması ve işlenmesi ile görevli bütün kurum ve kişiler, bu verilerin doğal afetler, kazalar ve insanların işleyecekleri hata, kusur ve suçların yaratacağı tehlikelere karşı korunması için her türlü önlemi almalıdır.

8. Denetim ve yaptırım: Kişisel verilerin korunması ile ilgili düzenlemelerde öngörülen ilke ve kuralların uygulanması ve önlemlerin alınması ve gerekli denetimlerin yapılması sorumluluğu tarafsız, yetkin ve adil bir makama verilmelidir.

9. Sınır ötesi veri transferi: Kişisel verilerin saklanmakta olduğu ülkeden başka bir ülkeye aktarılması için öncelikle her iki ülkenin ulusal mevzuatlarının bu aktarmaya izin vermesi gerekir. Ayrıca, bu veriler için verinin gönderileceği ülkenin bu veri için sağladığı korumanın verinin bulunduğu ülkede sağlanan korumadan daha aşağı düzeyde olmaması da gerekir.

C. Avrupa Konseyi Düzenlemelerinde Kişisel Verilerin Korunması

Avrupa Konseyi, kişisel verilerin korunması konusunda, gerek kamu gerekse özel sektör kurum ve kuruluşlarında göz önünde bulundurulması gereken ilkeleri saptamak ve konunun ulusal düzeyde çıkarılacak mevzuat ile düzenlenmesine ön ayak olmak amacıyla 1981 yılında 108 sayılı “Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşme” yi kabul etmiştir⁹¹. Bu sözleşmenin özelliği;

⁹¹ Cate, 1998, s.6; Tansuğ, 2006.

kişisel verilerin korunması konusunda hukuksal bağlayıcılığı olan ilk belge olmasıdır.

108 sayılı Sözleşme 1981 yılında diğer Avrupa Konseyi üyeleriyle birlikte Türkiye tarafından da imzalanmış ve 1985 yılında yürürlüğe girmiştir. Sözleşme, ülkemizde henüz onaylanmamıştır. 108 sayılı sözleşmenin uygulanması çerçevesinde Konsey, bu güne kadar çeşitli tavsiye kararları alınmıştır. 1999 yılında Sözleşmede bazı değişiklikler yapılmıştır. 108 sayılı sözleşme, kişisel verilerin korunmasında önemli bir kilometre taşı olmuş ve dünyada konuya ilişkin hukuksal düzenleme yapılırken dikkate alınmıştır.

108 sayılı sözleşmeye, 181 sayılı “Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunmasına Dair Sözleşmeye Ek Protokol” ile denetleyici otoriteler ve sınır ötesi veri transferine ilişkin ilaveler yapılmıştır. Bu protokol 2004’te yürürlüğe girmiştir. Türkiye, Ek Protokolü 8 Kasım 2001 tarihinde imzalamasına karşın henüz onaylamamıştır. Bu protokol, sınır ötesi veri korumada ulusal kontrol makamlarının oluşturulmasını zorunlu kılmış ve kişisel verilere yeterli düzeyde koruma sağlamayan ülkelere veri transferi yapılamayacağını hükme bağlamıştır⁹².

108 sayılı sözleşme, 27 maddeden oluşmaktadır. Bu Sözleşmenin amacı; her üye ülkede, uyruğu veya ikametgâhı ne olursa olsun gerçek kişilerin, temel hak ve özgürlüklerini ve özellikle kendilerini ilgilendiren kişisel nitelikteki verilerin, otomatik bilgi işleme tabi tutulması karşısında özel yaşam haklarını güvence altına almaktır. Otomatik işlem; tamamı veya bir kısmı otomatik yöntemlerle gerçekleştirilen verilerin kaydı, bu verilere biyolojik ve/veya aritmetik işlemlerin uygulanışı, verilerin değiştirilmesi, silinmesi, çıkarılması veya dağıtılması işlemi olarak tanımlanmıştır (m.2).

108 sayılı Sözleşme, hem kamu hem de özel sektördeki kişisel verileri kapsamaktadır. Ancak, akit taraflar isterse Sözleşmeyi topluluklar, dernekler, vakıflar, şirketler ve birlikle, tüzel kişilikten yararlanan veya yararlanmayan ve gerçek kişileri doğrudan veya dolaylı olarak bünyesinde toplayan diğer kuruluşlarla ilgili bilgiler hakkında uygulayacağını bildirebilirler. Burada belirtilmesi gereken diğer bir nokta Sözleşmenin sadece otomatik yollarla işlenen verilere yönelik koruma içermesidir.(m.3)

⁹² Atak, 2010, s. 94.

108 sayılı Sözleşmede üzerinde durulması gereken bir husus verilerin hangi standartlarda kaydedileceğidir. Sözleşme, kişisel verilerin tutulmasında göz önünde bulundurulması gereken ilkeleri de belirlemiştir. (m.5) Buna göre veriler; meşru ve yasal yoldan elde edilmeli ve işleme tâbi tutulmalıdır; belli ve meşru amaçlar için kaydedilmeli ve bu amaca aykırı şekilde kullanılmamalıdır; uygun ve elverişli olmalı ve kaydedildikleri amaca göre aşırı olmamalıdır; doğru ve güncel olmalıdır; ilgili kişilerin kimliklerini belirtecek bir biçim altında ve kaydedildikleri nihai amaç için gerekli görülen süreyi aşmayacak bir süre için muhafaza edilmelidir⁹³.

108 sayılı Sözleşmenin 6. maddesinde “hassas veri” olarak nitelendirilebilecek verilere yönelik özel bir hüküm getirilmiştir. Buna göre; iç hukukta uygun güvenceler sağlanmadıkça, ırk politik düşünceler, dini veya diğer inançları ortaya koyan kişisel nitelikteki verilerle sağlık veya cinsel yaşamla ilgili kişisel nitelikteki veriler ve ceza mahkûmiyetleri, otomatik bilgi işlemine tâbi tutulamazlar⁹⁴. Bu maddeden hareketle; kişilerin ırkını veya siyasal görüşlerini, dini veya diğer inançlarını, sağlık veya cinsel tercihlerini ve mahkûmiyetlerini ortaya çıkaran veriler hassas veri olarak tanımlanabilir.

Hassas verilerin işlenmesi kural olarak yasaktır. Bu veriler ancak istisnai hallerde işlenebilir. Kişisel verilerin işlenmesinde yer alan hassaslık ilkesi, hassas verilerin işlenmesinde sıradan verilerin işlenmesine nazaran daha katı denetim kurallarının var olması anlamına gelmektedir⁹⁵. Sözleşmenin 6. maddesinde, ulusal hukuka uygun güvenceler alınmadıkça hassas verilerin otomatik olarak işlenmeyeceği hükme bağlanmıştır. Hassas verilerin işlenebileceği istisnai hallere; veri sahibinin açık rızası, veri işleyeninin çalışma hukuku alanında veri işlemekle yükümlü olması, veri sahibinin hayati çıkarının olması hali örnek olarak verilebilir. Veri sahibinin fiili ya da hukuki nedenlerle onay veremeyeceği hallerde veri sahibinin veya diğer bir kişinin hayati çıkarlarını korumak için zorunlu ise hassas veriler işlenebilir. Bu istisna, insan hayatını tehdit eden durumların varlığı halinde hassas verilerin işlenmesini amaçlamaktadır⁹⁶.

⁹³ Cate, 1998, s. 6; Pekşirin, 2002.

⁹⁴ Wong, 2007, s. 2

⁹⁵ Kaya, 2011, s. 324.

⁹⁶ Kaya, 2011, s. 327.

Kişisel verilerin tutulmasıyla ilgili önemli bir sorun bunların güvenliğinin sağlanmasıdır. Kaydedilen kişisel nitelikteki verileri korumak için, bunların kazara veya izinsiz olarak imhasına veya zayi olmasına veya bunların elde edilmesine, değiştirilmesine veya izinsiz olarak dağıtılmasına karşı uygun güvenlik önlemleri alınması zorunludur. Ülkeler, verilerin güvenliğinin sağlanması için gerekli hukuksal düzenlemeleri yapmalıdır.

Demokratik hukuk devletlerinde bireylerin kendileri hakkında tutulan bilgilere ulaşabilmesi, temel hak ve hürriyetlerdendir⁹⁷. Sözleşmenin 8. maddesinde bireylerin bu kayıtlara ulaşma hakkı düzenlenmiştir. Buna göre herkes kendisi ile ilgili kişisel nitelikteki verilerin bulunup bulunmadığını teyidini yapmak ve bu bilgilerin anlaşılır bir biçim altında bildirilmesini sağlamak, gerekli olan durumlarda, bu verileri düzelttirmek veya sildirtmek hakkına sahiptir.

Sözleşmenin 9. maddesinde kişisel verilerin korunmasındaki istisnalar düzenlenmiştir. Buna göre; devlet güvenliğinin korunması, kamu güvenliği, devletin mali menfaatleri veya suçların önlenmesi, ilgili şahsın korunması ve başkasının hak ve özgürlükleri için zorunlu bir önlem teşkil ediyorsa, ilgili şahısların özel yaşamlarına açık bir tecavüz tehlikesi teşkil etmedikçe, istatistiği veya bilimsel amaçlar için kullanılan kişisel nitelikteki verilerin otomatik bilgi işleme tâbi tutulması halinde, Sözleşme hükümleri ihlal edilmiş olmayacaktır.

108 sayılı Sözleşmeye göre; akit devletler verilerin korunması hakkındaki temel ilkelere işlerlik sağlayan iç hukuk kurallarının ihlaliyle ilgili uygun yaptırımlar ve Kanun yolları getirmekle yükümlüdürler. (m.10)

108 sayılı Sözleşmenin temel özelliği, çerçeve niteliğinde olmasıdır. Başka bir ifadeyle, bu Sözleşme hükümleri doğrudan uygulanabilir nitelikte değildir. Sözleşmeciler devletler, iç hukuklarında kabul edecekleri uygulama yasalarıyla Sözleşmeyi ülke şartlarına uyduracaklardır⁹⁸.

20. yüzyılda bilgi ve iletişim teknolojilerinde yaşanan gelişmeler nedeniyle kişisel verilerin tutulmasında ciddi bir artış yaşanmış, İnternetin yaygınlaşması ise konuyu daha hassas hale getirmiştir. Avrupa Konseyi

⁹⁷ Bu konuda ayrıntılı bilgi için bkz. Kaya, Cemil. (2005). *İdare Hukukunda Bilgi Edinme Hakkı*. Ankara: Seçkin Yayınları.

⁹⁸ Atak, 2010, s. 97.

tarafından hazırlanmış olan uluslararası sözleşmeden bu yana geçen 20 yılı aşkın süre içinde, bilişim ve iletişim teknolojilerinin adeta birbiriyle birleşmesi şeklinde ortaya çıkan gelişmeler kişisel verilerin korunması hakkının, alanını genişletmiş ve önemini artırmıştır. Gerçekten bu gelişmeler, istihdam, istatistik, bankacılık, sosyal güvenlik, sağlık, sigortacılık, pazarlama, elektronik haberleşme, elektronik ticaret gibi alanlarda her bir alanın kendine özgü teknik özellikleri nedeniyle farklı alanlarda kişisel verilerin tutulmasına yönelik hukuksal düzenleme ihtiyacı ortaya çıkmıştır. Bu süreçte, konu ulusal ve uluslararası forumlarda tartışılmış ve çeşitli ulusal ve uluslararası belgeler hazırlanmıştır. Bugün, bir çok ülkede Kişisel Verilerin Korunması Hakkında Kanun başlığını taşıyan yasalar yanında yukarıda bahsedilen alanlarda kişisel verilerin korunması için özel düzenlemeler de yapılmıştır⁹⁹.

Avrupa Konseyi kişisel verilerin tutulması konusunda gerek 108 sayılı Sözleşmeyi güncellemek gerekse çeşitli alanlarda ortaya çıkan ihtiyaçları karşılamak amacıyla birçok karar almıştır. Sözleşmeye göre, hükümlerin uygulaması ve değişiklikler hakkında görüş oluşturulması amacıyla taraf devletlerin gönderecekleri birer temsilciden oluşturulan Danışma Komitesi'nin çalışmaları sonucunda Avrupa Konseyi Bakanlar Komitesinin aldığı tavsiye kararlardan bazıları şunlardır:

(2002) 9 sayılı Tavsiye: Sigorta amacıyla toplanan veriler, (99) 5 sayılı Tavsiye: İnternette Özel Hayatın Korunması, (98)17 Sayılı Tavsiye: İstatistik Amacıyla Toplanan Ve İşlenen Veriler, (97) 5 sayılı Tavsiye: Tıbbi veriler, (95) 4 sayılı Tavsiye: Telekomünikasyon Ve Özellikle Telefon Hizmetlerinde Kişisel Verilerin Korunması, (91)10 Sayılı Tavsiye: Kamu Kuruluşları Tarafından Tutulan Kişisel Verilerin Üçüncü Kişilere Verilmesi, (90) 19 Sayılı Tavsiye: Ödeme Ve Benzer Amaçlı Öteki İşlemlerde Kişisel Verilerin Korunması, (89) 2 Sayılı Tavsiye: İstihdam Amaçlı Tutulan Kişisel Verilerin Korunması, (87) 15 Sayılı Tavsiye: Poliste Tutulan Kişisel Verilerin Korunması, (86) 1 Sayılı Tavsiye: Sosyal Güvenlik Amaçlı Kişisel Veriler, (85) 20 sayılı Tavsiye: Pazarlama Amaçlı Kişisel Verilerin Korunması, (83) 10 Sayılı Tavsiye: Bilimsel Araştırma Ve İstatistik Amaçlı

⁹⁹ Kesmez, Necdet “Kişisel Verilerin Korunması Üzerine” Bilişim Şurası, 25 Mart 2011 tarihinde http://bilisimsurasi.org.tr/listeler/tbs-hukuk/Mar/att-0044/01-K__SEL_VER_LER_N_KORUNMASI.doc adresinden erişildi.

Kişisel Verilerin Korunması, (81) 1 Sayılı Tavsiye: Otomatik İşlem Yapan Tıbbi Veri Bankalarının Düzenlenmesi¹⁰⁰.

D- Avrupa Birliği Düzenlemelerinde Kişisel Verilerin Korunması

Kuruluş felsefesinde, barış, özgürlük, refah, demokrasi ve hukukun üstünlüğü ilkelerinin yer aldığı Avrupa Birliği¹⁰¹ Avrupa coğrafyasında olduğu kadar küresel düzeyde de etkili olmayı hedefleyen bir entegrasyon çabasıdır. AB eşitlik insan saygınlığı, temel hak ve özgürlüklerin korunması, demokratik kurumların varlığı, hukukun üstünlüğü ve şeffaflığın sağlanması gibi genel anlamda kabul görmüş ortak değerler üzerine kurgulanmıştır¹⁰². Kişilerin, malların, hizmetlerin, sermayenin ve bilginin serbestçe dolaşabilmesi için iç hukuklarda çalışmalar yapan AB'de serbestçe dolaşamayan şey AB vatandaşlarının kişisel verileridir¹⁰³.

Avrupa'da, II. Dünya savaşından sonra yürürlüğe giren hukuki metinlerde özel hayatın korunması temel insan haklarından birisi olarak düzenlenmiştir. Bu dönemde yaşanan trajediler ve canavarlıklar bu yaklaşımda etkili olmuştur. Çünkü bu dönemde kişisel veri tabanları ırkçılık, azınlık grupları yok etmek, soykırımı kolaylaştırmak amacıyla kullanılmıştır. Burada yaşanan olaylar, insanlığa kamunun özel alanı hangi oranda ihlal edebileceğini öğretmiştir. Bu nedenle, devletlerin kişisel verileri saklaması konusunda çok sıkı kurallar getirilmiş ve bu kuralların uygulanmasında büyük bir dikkat gösterilmiştir¹⁰⁴.

A.İ.H.S, kişisel verilerin korunmasında önemli bir enstrümandır. Sözleşmenin 8. maddesinde konuyla ilişkili özel hayat ve aile hayatı koruma altına alınmıştır. Sözleşmenin uygulanmasını denetleyen A.İ.H.M. özel hayatın korunması, kişisel verilerin korunması konularında verdiği kararlarla bu alanda hukuksal düzenlemeler yapılmasına ön ayak olmuştur¹⁰⁵.

¹⁰⁰ Akıllıoğlu, 2004, 25 Mart 2011 tarihinde http://www.coe.int/t/dghl/standardsetting/dataprotection/Legal_instruments_en.asp adresinden erişildi.

¹⁰¹ Cate, 1998, s. 8.

¹⁰² 3 Nisan 2011 tarihinde sodes.gov.tr/DocObjects/Download/2962/temelhak.pdf adresinden erişildi.

¹⁰³ Tansuğ, 2006.

¹⁰⁴ Robinson, Graux, Botterman, Valeri, 2009, s. 6.

¹⁰⁵ Korff, 2002, s. 12; Bignami, 2007, s.242; Şimşek, 2001. 3 Nisan 2011 tarihinde http://epic.org/privacy/intl/eu_data_protection_directive.html adresinden erişildi.

Kişisel verilerin korunması, Avrupa Birliği Temel Haklar Şartı'nın 8. maddesinde düzenlenmiştir. Buna göre; herkes, kendisini ilgilendiren kişisel verilerin korunması hakkına sahiptir. Kişisel verilerin tutulabilmesi iki halde mümkündür. Birincisi; ilgili kişinin rızası, diğeri yasa ile öngörölmüş meşru bir temeldir. Yine kişisel veriler, adil bir şekilde ve belirli amaçlar için tutulmalıdır. Şart'a göre kişiler, kendileri hakkında toplanmış verilere erişme ve bunları düzeltirme hakkına sahiptir. Kişisel verilerle ilgili kurallara uyulup uyulmadığı, bağımsız bir makam tarafından denetlenmelidir¹⁰⁶.

1990'lı yıllarda AB'de kişisel verilerin korunması konusunda çalışmalar yoğunlaşmış ve 24 Ekim 1995 tarihinde Avrupa Parlamentosu ve Konseyi 1995/46 sayılı "Kişisel Verilerin İşlenmesinde Gerçek Kişilerin Korunması Direktifi"ni kabul etmiş¹⁰⁷ ve bu Direktif 1998 yılında yürürlüğe girmiştir¹⁰⁸. Bu Direktifi desteklemek maksadıyla eksik kalan alanlarda Avrupa Parlamentosu ve Konseyi 1997 yılında 1997/66 "Telekomünikasyon Alanında Kişisel Verilerin İşlenmesi Ve Mahremiyetin Korunması Yönergesini" yürürlüğe koymuştur¹⁰⁹. Daha sonra AB bu Yönergeyi tamamlayan 2002/58 Sayılı "Özel Hayatın Korunması ve Elektronik İletişim Yönergesi"ni¹¹⁰ de ileri teknolojik ortamlardaki ilişkileri de kapsayan yeni bir veri saklama hukuku olarak ortaya koymuştur. Yine, 2002/58 sayılı Direktif ve 2006/24 sayılı Direktif¹¹¹ kişisel verilerin korunmasındaki diğere düzenlemelerdir¹¹².

¹⁰⁶ 3 Nisan 2011 tarihinde sodes.gov.tr/DocObjects/Download/2962/temelhak.pdf adresinden erişildi.

¹⁰⁷ 3 Nisan 2011 tarihinde <http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML> adresinden erişildi.

¹⁰⁸ 3 Nisan 2011 tarihinde <https://www.privacyinternational.org/article/phr2006-overview-privacy#> adresinden erişildi.

¹⁰⁹ 3 Nisan 2011 tarihinde http://eurlex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31997L0066&model=guichett adresinden erişildi.

¹¹⁰ 3 Nisan 2011 tarihinde <http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:NOT> adresinden erişildi.

¹¹¹ 3 Nisan 2011 tarihinde <http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:EN:HTML> adresinden erişildi.

¹¹² Tanrıkulu, Cengiz "Kişisel Verilerin Önemi Artıyor", 3 Nisan 2011 tarihinde <http://www.atgv.org.tr/dokumanlar/dergi/atgvdergi3sayi.pdf> adresinden erişildi; Tansuğ, 2006.

AB, kişisel verilerin korunması konusunda tüm üye ülkelerde aynı standartları sağlamayı hedeflemektedir¹¹³. Avrupa Birliği'nin düzenlemeleri, temel olarak kişisel verilere gerek kamudan, gerekse özel kişi ve kuruluşlardan gelecek saldırılara karşı önlem almak ve saldırı öncesi sistemli bir koruma ortaya koymak amacıyla¹¹⁴. AB Direktifleri, kişisel verilerin korunmasında özel veya kamu kesimi arasında herhangi bir ayırım yapmamıştır. AB, bu yaklaşımı ile Amerika uygulamasından ayrılmaktadır. Amerika'da kişisel verilerin daha çok özel sektör alanında düzenlemelere ihtiyaç duyduğu ve fakat kamu sektörünün parlamentoya karşı sorumlu olması ve bu kurum tarafından denetleniyor olması nedeniyle daha az düzenleme yapılması gerektiği ileri sürülmektedir¹¹⁵. Ancak, Avrupa Parlamentosu özellikle ABD'de ortaya çıkan bu gelişmenin aksine kişisel verilerin işlenmesi bakımından kamu idaresiyle özel sektör arasında herhangi bir ayrıma gitmeyerek her iki kesimi de aynı mevzuata tâbi kılmıştır¹¹⁶.

Avrupa Birliğinde kişisel verilerin işlenmesindeki hukuka uygunluk sebepleri sayılırken, kamu menfaati veya kamu düzeni gereği kişilerin kişisel verilerini herhangi bir izin alınmaksızın işlenebileceği kabul edilmiştir. Bu durum, her ne kadar kamu özel ayırımı yapılmassa da doğal olarak kamu idaresinin doğasından kaynaklanan ihtiyaçlar nedeniyle genel kuraldan ayrılmaların olabileceğini göstermektedir¹¹⁷.

Avrupa Birliği, piyasa içi süreçler yoluyla özel sektörün düzenlemelere gitmesine dayanan ABD'ye nazaran kişisel verilerin korunmasında¹¹⁸ daha fazla yasal düzenleme taraftarı bir yaklaşımı takip etmektedir. Başka bir ifadeyle, ABD'de özel sektörün öz düzenleme mekanizması ilk başta akla

¹¹³ Millard and Hon, 2011.

¹¹⁴ 3 Nisan 2011 tarihinde <https://www.privacyinternational.org/article/phr2006-overview-privacy#> adresinden erişildi.

¹¹⁵ Solove, Daniel J. Hoofnagle -Chris Jay "A Model Regime of Privacy Protection", GWU Law School Public Law Research Paper No. 132 University of Illinois Law Review, Vol. 2006, No. 2, 2006, s. 357 vd.

¹¹⁶ Tanrıkulu, 2007.

¹¹⁷ Tanrıkulu, 2007.

¹¹⁸ 3 Nisan 2011 tarihinde http://en.wikipedia.org/wiki/Data_Protection_Directive adresinden erişildi.

gelirken AB’de öncelikle hukuksal düzenlemeler öne çıkmaktadır. Kara Avrupası Hukuk anlayışı kişisel verilerin korunmasında da görülmektedir¹¹⁹.

1. Avrupa Birliği 1995/46 Sayılı Veri koruma Direktifi

Ekonomik İşbirliği ve Kalkınma Teşkilatı Rehber ilkeleri ve 108 sayılı Sözleşmenin verdiği izin çerçevesinde ulusal hukuk uygulamalarındaki çeşitlilik ve istikrarsızlık nedeniyle, Avrupa Birliği 1990 yılında kişisel verilerin korunmasına yönelik bir taslak hazırlamıştır. Taslak, beş yıllık çalışmadan sonra 1995 yılında yürürlüğe girmiştir. AB’de veri korumada coğrafi ve siyasi olarak merkezileşmiş bir yapı vardır¹²⁰.

24 Ekim 1995 tarihli “Kişisel Verilerin İşlenmesi Sırasında Gerçek Kişilerin Korunması ve Serbest Veri Trafikğine İlişkin Direktif”, kişisel verilerin korunmasıyla ilgili önemli ilkeleri içeren bir düzenlemedir. Direktif, kişisel verilerin korunmasında Avrupa düzeyinde genel bir çizgi belirlemiştir. Direktif, hem mahremiyeti destekleyici hükümler içermekte hem de bazı yeni haklar getirmektedir. Direktif, gerek Avrupa’da gerekse Avrupa dışında olsa bile Avrupa kaynaklı verilerin toplanmasında, işlenmesinde ve paylaşılmasında ciddi sınırlamalar getirmiştir¹²¹.

Direktif, gerek elektronik ortamda gerekse çevrim-dışı (offline) dosya tutma işlemlerinde uygulanacaktır. 1995/46 sayılı Direktifin öne çıkan özellikleri; özel sektör faaliyetlerinin geniş bir kısmını kapsamına alması ve kişisel verilerin işlenmesi ve kullanımının öncesi ve sonrası için ciddi kontrol mekanizmaları öngörmesidir¹²². 1995/46 sayılı Direktif, bireylerin mahremiyetinin en yüksek düzeyde korunmasına imkan sağlaması, ancak aynı zamanda kişisel verilerin serbest dolaşımına izin vermesi ile kişisel verilerin işlenmesi ve korunması meselesinde önemli bir adım olarak kabul edilmektedir¹²³.

Avrupa veri koruma modelinde anahtar kavram “uygulanabilirlik” tir. Veri öznelerinin haklarına ilişkin kurallar açık bir şekilde belirlenmiştir. Birlik

¹¹⁹ Gür, 2009, s. 12.

¹²⁰ 3 Nisan 2011 tarihinde http://ec.europa.eu/justice/data-protection/index_en.htm adresinden erişildi.

¹²¹ Cate, 1998, s. 3.

¹²² 3 Nisan 2011 tarihinde <https://www.privacyinternational.org/article/phr2006-overview-privacy#> adresinden erişildi.

¹²³ Robinson, Graux, Botterman, Valeri, 2009, s. 6.

üyeleri her ülke, kuralları uygulayacak “Veri Koruma Komiseri” veya “Veri Koruma Otorite” sine sahiptir. Birlik, kendisiyle ticari ilişkileri olan ülkelere de benzer denetimleri beklemektedir¹²⁴.

Direktifin dikkate değer dört özelliği bulunmaktadır. Birincisi, hem özel sektör hem de kamu sektöründe uygulanacaktır. İkincisi, veri toplama, depolama, kullanma ve dağıtımını da kapsayan geniş bir alanı tanzim etmektedir. Üçüncüsü, gönüllü olarak bu eylemleri uygulayacaklara (veri işlenmesi vb.) olumlu yükümlülükler yüklemektedir. Dördüncüsü, birkaç sektörel sınırlama getirmektedir. Direktif, veri öznesiyle ilgili olmaksızın uygulanacaktır¹²⁵.

Direktifte birbiriyle örtüşen sekiz prensip bulunmaktadır¹²⁶.

1- Sınırlı amaç ilkesi: Veriler belirli amaçlar için depolanmalı, işlenmeli ve bu amaçlar çerçevesinde kullanılmalıdır.

2- Kalite prensibi: Bilgiler doğru ve güncel olmalıdır.

3- Veri güvenliği ilkesi: Toplanan verilerin işlenmesi ve dağıtımını güvenli bir şekilde yapılmalıdır. Burada yalnızca fiziksel güvenlik kastedilmemektedir. Kazara veya yasadışı zarar görme veya kaybolma, yetkisiz değişim veya açıklama ve diğer yetkisiz işlemler veri güvenliği kapsamındadır.

4- Hassas veriler için özel koruma olmalıdır. Irksal ve ya etnik köken, politik düşünce, din, sağlık, cinsel tercihler gibi hassas veriler bu kapsamdadır¹²⁷.

1995/46 sayılı Direktifin 8. maddesine göre hassas verilerin işlenebileceği durumlar şunlardır: Veri sahibinin açık muvafakatı, çalışma hukuku alanındaki yükümlülükler uyma, veri sahibinin yaşamsal çıkarları, özel hukuk tüzel kişilerinin faaliyetleri, verilerin kamuya açıklanmış olması, hukuki iddiaları tesis etme, uygulama ve savunma, sağlık açısından gereklilik,

¹²⁴ 3 Nisan 2011 tarihinde <https://www.privacyinternational.org/article/phr2006-overview-privacy#> adresinden erişildi.

¹²⁵ Cate, 1998, s. 5.

¹²⁶ Cate, 1998, s. 12 vd.

¹²⁷ Millard and Hon, 2011.

suçlar, mahkûmiyetler ve güvenlik tedbirleridir. Başka bir ifadeyle, bu durumlar hassas verilerin işlenmesinin hukuka uygunluk nedenleridir¹²⁸.

Hassas verilerin işlenmesinde birinci istisna, veri sahibinin açık muvafakatıdır. Zımnî muvafakat yeterli değildir. Başka bir ifadeyle, hassas veriler ancak veri sahibinin açık onayıyla işlenebilecektir. Açık muvafakat, iradenin özgür, isteyerek ve bilinçli şekilde açıklanmasıyla ortaya çıkabilir. Ayrıca veri sahibi konu hakkında yeterli ölçüde bilgilendirilmelidir. Hassas verilerin işlenmesinde ikinci istisna, ülkelerin çalışma hukuku mevzuatıdır. Ülkelerin mevzuatı işverene veri işleme yükümlülüğü getirmişse hassas kişisel veriler işlenebilir. Çalışma hukukunu salt iş hukuku olarak değerlendirmemek gerekir. Konu, kamu hukuku çalışma alanını da kapsayacak şekilde düşünülmelidir¹²⁹.

Hassas verilerin işlenmesinde diğer bir istisna, siyasi, felsefi, dini veya sendikal amaç taşıyan bir vakfın, derneğin ve benzeri diğer kâr amacı gütmeyen kuruluşların veri işlemesidir. Ancak bu durumda veri işlemenin sadece bu kuruluşların üyeleri veya amaçları için bu kuruluşlarla düzenli irtibat halinde olan kişiler hakkında olması ve verilerin, veri sahiplerinin muvafakatı olmaksızın üçüncü kişilere açıklanmaması gerekir¹³⁰. Yine, veri sahibi tarafından kamuya açıklanan hassas veriler işlenebilir. Burada veri sahibi kendi iradesiyle hassas bir verisini açıklamaktadır. Başka bir ifadeyle, söz konusu veriler kamuya mâl olmaktadır. AIDS hastası olan bir kişinin televizyon programında HIV virüsü taşıyıcısı olduğunu söylemesi konuya örnek olarak verilebilir¹³¹.

Hassas verilerin işlenebildiği diğer bir istisna, hukuki iddiaları tesis etme, uygulama ve savunmadır. Avukatların müvekkilleriyle ilgili yapmış olduğu işlemler bu kapsamda değerlendirilebilir. Yine tıbbi teşhis, bakım ve tedavi sunma gibi sağlık hizmetlerinde zorunluluk varsa hassas veriler işlenebilir. Bu veriler, mesleki gizlilik yükümlülüğü ile ilgili yetkili kurumlar tarafından

¹²⁸ 5 Nisan 2011 tarihinde <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML> adresinden ulaşıldı.

¹²⁹ Kaya, 2011, s. 326.

¹³⁰ Kaya, 2011, s. 328.

¹³¹ Kaya, 2011, s. 329.

geliştirilen kurallara tabi sağlık görevlileri veya aynı düzeyde gizlilik yükümlülüğü bulunan diğer kişiler tarafından işlenebilir¹³².

Hassas verilerin işlenmesi sorunlara gebe bir konudur. Bu nedenle, normal verilerden farklı bir statüye tabi tutulmalı ve yasada hangi tür hassas verilerin işleneceğinin sınırları net bir şekilde belirlenmelidir.

5- Şeffaflık ilkesi: Veri işlemeye yönelik işlemler açık ve anlaşılabilir olmalıdır. Bu ilkenin asgari standardı veri toplamanın resmi bir şekilde yapılmasıdır. Bu nedenle, çoğu Avrupa ülkesinde veri toplama ve işlemeye önce veri öznesinin rızası alınmaktadır.

6- Veri transfer ilkesi: Buna göre; veri öznesinin rızası olmadan işlenen veriler üçüncü taraflara transfer edilemez. Sınır ötesi veri transferlerin de ise; söz konusu ülkede kişisel verilerin korunmasına yönelik “yeterli düzeyde korumanın” olması şartı aranır¹³³.

7- Bağımsız çözüm ilkesi: Bu ilkeye göre; veri toplama ve işleme eylemlerinde etkili ve bağımsız çözüm mekanizmaları olmalıdır.

8- Bireysel çözüm ilkesi: Buna göre; bireyler kendileri hakkında tutulan verilere girme ve yanlışlık varsa bunları düzeltme hakkına sahiptir. Bireyler, kanuna aykırı bir şekilde veri toplayanlara veya işleyenlere karşı yasal yollara başvurabilirler. Bireyler bunun yanı sıra hükümet otoritelerine de konunun soruşturulması için şikayette bulunabilirler.

1995/46 sayılı Direktifin temel amacı, kişisel verilerin işlenmesi sırasında kişi hak ve özgürlüklerinin korunmasını sağlamak ve üye devletler arasında serbest veri trafiğini temin etmektir¹³⁴. Bu maddeyle, kişisel veriler temel hak ve özgürlükler içindeki yerini almıştır. Bu Avrupa için yeni ve pek çok açılardan ihtilal niteliğinde bir durumdur. Direktifin en önemli yeniliklerinden birisi budur¹³⁵. Bu Direktifle, Birliğe üye devletler arasında verilerin korunmasında yeknesak bir hukuk düzeni oluşturulacaktır.

Avrupa Topluluğu Adalet Divanı'na göre Direktif'in amacı; ortak pazarın gerçekleştirilmesi amacı doğrultusunda ülkeler arası veri koruma

¹³² Kaya, 2011, s. 330.

¹³³ Tansuğ, 2006.

¹³⁴ Robinson, Graux, Botterman, Valeri, 2009, s.20; Korff, 2002, s. 12.

¹³⁵ Cate, 1998, s. 15.

uygulamaları farklılıklarının ortadan kaldırılması için mevzuatı uyumlaştırmaktır. Ortak pazar geliştikçe ülkeler arası veri transferleri artacaktır. Bu durumda kişilerin temel haklarının korunması önem kazanmaktadır. Direktif, verilerin işlenmesi ihtiyacı ile temel hakların korunması arasında denge kurmaya çalışmaktadır¹³⁶. Söz konusu Direktif, kişisel verilerin kısmen veya otomatik olarak işlenmesi halinde uygulanacaktır. (m.3)

Veri Koruma Direktifi ile oluşturulmak istenen koruma, kişisel verilerin işlenmesinin şartlarını düzenlemektir. Başka bir ifadeyle bu Direktif önleyici bir nitelik taşımaktadır. Amaç, bir saldırının ortaya çıkması halinde sağlanacak korumadan ziyade, muhtemel saldırılara karşı önleyici niteliğe sahip bir sistemin oluşturulmasıdır¹³⁷.

Bu Direktif, kamu güvenliği, savunma ve devletin güvenliğine ilişkin işlemlerde ve devletin ceza hukuku alanındaki faaliyetleri gibi Topluluk hukuku dışında kalan faaliyetlerinde uygulanmayacaktır. Yine, gerçek bir kişinin tamamen kişisel olan veya evi ve ailesiyle ilgili olan veri işlemlerinde bu Direktif hükümleri uygulanmayacaktır.

Direktifin 6. maddesinde veri işlenmesinde uyulması gereken ilkeler düzenlenmiştir. Bunların, 108 sayılı Sözleşme ve OECD Rehber ilkeleriyle paralel olduğu söylenebilir. Söz konusu veri koruma ilkeleri şunlardır¹³⁸:

1-Veriler dürüstlük kuralına uygun olarak ve hukuka uygun amaçlar için işlenmelidir. Hukuka uygunluk, kişisel verilerin mevcut yasal hükümlere ve diğer mesleki davranış kuralları gibi özel hukukî metinlere uygun olmasıdır. Dürüstlük kuralına uygun olmak ise; kişisel verilerin işlenmesinde verileri işlenen kişiye karşı şeffaf olunması gerekliliğini ifade eder. Bu kural, veri koruma görevlisinin bilgilendirme ve uyarı görevlerine

¹³⁶ Uygun, 2010, s. 36; 3 Nisan 2011 tarihinde <https://www.privacyinternational.org/article/phr2006-overview-privacy#> adresinden erişildi.

¹³⁷ Başalp, Nilgün, Kişisel Verilerin Korunması ve Saklanması, Yetkin Yayınları, Ankara, 2004, s. 31; 5 Nisan 2011 tarihinde <https://www.privacyinternational.org/article/phr2006-overview-privacy#> adresinden erişildi.

¹³⁸ Gür, 2009, s. 25; Keser Berber, Leyla- Ünlü, Mahir M.- Er, Cüneyd Elektronik Sağlık Kayıtları ve Özel Hayatın Gizliliği, Karakter Color AŞ, İstanbul, s.126 vd.; Cate, 1998,s. 12 vd.; Robinson, Graux, Botterman, Valeri, 2009, s. 49.

uygun bir şekilde hareket etmesini de içermektedir. İyi uygulama örnekleri ilkelerine uyulması diğer bir noktadır¹³⁹.

2- Veriler belirli, açık ve meşru amaçlar doğrultusunda toplanmalıdır. Veriler belirli, açık ve meşru amaçlar doğrultusunda toplanmalı ve bu amaçlarla uyuşmayacak şekilde işlenmemelidir. Ancak, veriler üye devletler tarafından gerekli güvenceler sağlanmış olması şartıyla tarihi, istatistik veya bilimsel amaçlarla sonradan işlenebilecektir. Veri koruma görevlisinin işleme amacını tam olarak belirlemesi ve bunu ilgili kişiye ve ulusal kontrol birimine bildirmesi gerekir. Veri işleme amacının meşru olması gerekir¹⁴⁰. Yani veri koruma görevlisi tarafından veri işlemede güdülen faydanın ilgili kişinin menfaatini aşmalıdır.

Amacın belirlenmiş olmasından kasıt, amacın yazılı şekilde belirtilmesidir. Böylece, verilerin hangi nedenle ve hangi ölçüde toplanmış ve işlenmiş olduğu denetlenebilecektir. Açıklıktan kasıt ise, kişisel verilerin ancak açıkça ortaya konulmuş amaçla toplanıp işlenmesidir. Bu ilke sayesinde üye ülkelerin belirsiz ifadelerle verilerin işlenmesinde amaca bağlılık ilkesini ihlal etmeleri önlenmeye çalışılmıştır¹⁴¹.

3- Kişisel verilerin uygun, ilgili olması ve aşırı olmaması gerekir.

Kişisel veri, açıklanan işleme amacı bakımından faydalı ve gerekli olmalıdır. İşleme amacıyla ilgisi olmayan veya gereksiz olan, ilgisiz verilerin toplanması veya kullanılması yasaktır. Veri koruma görevlisinin bu nedenle, amaca onlar olmadan da ulaşılabilecek olan kişisel verileri kullanmaktan kaçınmalıdır. Yine toplanan verilerin aşırı olmaması gerekir. Bunun anlamı; veri öznesinin çıkarlarını tehlikeye düşürecek bir orantısızlık tehlikesi olmamalıdır¹⁴². Başka bir ifadeyle, araç ile amaç arasında bir denge bulunmalıdır.

4- Kişisel veriler doğru ve güncel olmalıdır.

Kişisel veriler, doğru olarak ve güncel tutulmalı, verilerin hatalı veya güncel olmamaları durumunda, bunların silinmesi veya düzeltilmesi için gerekli işlemler yapılmalıdır. Bu işlemler, verinin kaliteli olmasını sağlar.

¹³⁹ Keser Berber, Ünlü, Er, s.126; Gür, 2009, s.25; Cate, 1998, s.12.

¹⁴⁰ Keser Berber, Ünlü, Er, s.127; Gür, 2009, s.25; Cate, 1998, s. 8.

¹⁴¹ Uygun, 2010, s.54.

¹⁴² Cate, 1998, s.8; Başalp, 2004, s. 38.

Veri koruma görevlisinin, verilerin doğru olmadığını bildiği veya bilmesi gereken hallerde, bunların silinmesi veya düzeltilmesi gerekir¹⁴³.

5- Kişisel veriler belirli süreyle saklanmalıdır.

Kişisel verilerin, veri öznesinin teşhis edilmesine imkân verecek şekilde, verilerin toplandığı ve işlendiği amaçlar için gerekli olan süreden daha fazla saklanmaması gerekir. Söz konusu amaca ulaşıldıktan sonra veriler anonim hale getirilmeli veya silinmelidir. Üye ülkeler, tarihi, istatistikî veya bilimsel amaçlarla güvence sağlamak şartıyla belirtilenden daha uzun süre kişisel verileri saklayabilirler¹⁴⁴. Pek çok üye ülkede bu amaçla düzenleme yapılmıştır.

6- Veri öznesinin haklarına riayet edilmelidir.

Direktifte, kişisel verilerin işlenmesinde veri öznesine bazı haklar verilmiştir. Bilgi edinme hakkı, kişisel verilere erişim hakkı, verilerin düzeltilmesini talep hakkı ile belirli durumlarda veri işlemeye itiraz etme hakkıdır. Direktif, bireylere kredi güvenirliliği ve istihdam dâhil olmak üzere kişisel verilerinin otomatik işleme tabi tutulması temelinde kendilerini etkileyen kararlara itiraz etme imkânı sağlamaktadır. Veri kütüğü sahibi, veri öznesinin bu haklarını kullanabilmesi için gerekli önlemleri almakla yükümlüdür¹⁴⁵.

Avrupa Birliği'nde, Kasım 2010'da Komisyon tarafından yayınlanan "Avrupa Birliği'nde Kişisel Verilerin Korunmasına Yönelik Kapsamlı Bir Yaklaşım" başlıklı bildiri ile hızlı teknolojik gelişmeler ve küreselleşme sonucunda kişisel verilerin korunmasında ortaya çıkan yeni sorunlara karşı 1995/46 sayılı Veri Koruma Direktifinin güncellenmesi gerektiği ifade edilmiştir¹⁴⁶.

AB'nin yeni hukuki yaklaşımında, kişisel verilerin korunmasına yönelik hukuksal çerçeve beş temel özelliğe dayanmalıdır¹⁴⁷:

¹⁴³ Keser Berber, Ünlü, Er, s. 127; Gür, 2009, s. 26.

¹⁴⁴ Keser Berber, Ünlü, Er, s. 127; Gür, 2009, s. 26.

¹⁴⁵ Keser Berber, Ünlü, Er, s. 128; Gür, 2009, s. 27.

¹⁴⁶ Helvacıoğlu Kuyucu, Aslı Deniz, "Avrupa Birliği'nde Kişisel Verilerin Korunmasında Yeni Yaklaşım", 5 Nisan 2011 tarihinde http://www.bilgicagi.com/Yazilar/4583avrupa_birliginde_kisisel_verilerin_korunmasinda_yeni_yaklasim.aspx adresinden erişildi.

¹⁴⁷ Helvacıoğlu Kuyucu, 2011.

- Yeni teknolojilerin etkisine cevap verebilecek kapsama sahip olmalıdır.

- Veri korunmasının iç pazardaki etkisini dikkate alınmalı ve ortak pazarda üye ülkelerin uyumunu güçlendirecek bir yapı kurulmalıdır.

- Küreselleşme bağlamında uluslararası veri transferlerini geliştirebilecek kolaylıkta tasarlanmalıdır.

- AB içerisinde Veri Koruma İdarelerini güçlendirerek, veri koruma kurallarının daha etkin olarak uygulanmasını sağlayacak bir idari yapı öngörmelidir.

- Tüm sektör ve politika alanlarında veri korunmasının bütünleştirilmesini sağlayacak etkinlikte olmalıdır.

AB'nin yeni yaklaşımı verilerin korunmasında bazı hedefler de belirlemiştir. Buna göre, yeni hukuki yapı bireylerin haklarını güçlendirecek ve yeni teknoloji kullanımının bireysel özgürlüklerin ve ortak pazarın rekabetçi ortamının üzerindeki etkilerini dikkate alacaktır. Yeni sistem şeffaflık ilkesine dayanarak veri işlenmesinde kişilerin açık ve detaylı bir şekilde bilgilendirilmesini öngörmektedir. Kişiler kendi verileri üzerinde daha etkin bir denetim hakkına sahip olacaklardır¹⁴⁸.

Yine Bildiriye göre; veri minimizasyonu prensibi güçlendirilecektir. Özellikle sosyal medya açısından önem taşıyan bu ilke ile unutulma hakkı kişinin verilerini dilediği takdirde silinmesini talep etmesini sağlayacaktır. Veri taşınabilirliği, kişilerin verileri bir uygulamadan diğerine taşımalarına olanak verecektir. Burada hukuk, kişilerin veri hakları konusunda bilinçlendirilmelerini destekleyecektir. Veri işleme kişilerin kendi rızaları ile mümkün olabilecektir. Hassas verilerin korunması, özellikle kişilerin etnik kökenleri, siyasi görüşleri, dini ve felsefi inançları, sahip oldukları üyeliklerin listesi, genetik gibi sağlıkla ilgili veya cinsel tercihlerine yönelik bilgileri¹⁴⁹ halihazırda zaten koruma altında ancak teknolojik gelişmeler ışığında bu verilerin hassasiyeti güvence altına alınacaktır¹⁵⁰.

¹⁴⁸ Helvacıoğlu Kuyucu, 2011.

¹⁴⁹ Wong, 2007, s. 1.

¹⁵⁰ Helvacıoğlu Kuyucu, 2011.

2. Avrupa Birliği 2002/58 Sayılı Direktifi

AB, 2002 yılında 1995/46 sayılı Veri Koruma Direktifini telekomünikasyon alanında tamamlayan 1997/66 sayılı Direktifi kabul etmiştir¹⁵¹. 2002/58 sayılı “Elektronik İletişim Sektöründe Kişisel Verilerin ve Özel Hayatın Korunması Direktifi” ile 1997/66 sayılı Direktif yürürlükten kalkmıştır.

2002/58 sayılı Direktif, 1995/46 sayılı Direktiften farklı olarak, yalnızca gerçek kişileri değil tüzel kişileri de kapsamaktadır. Söz konusu yönerge kişisel bilgilerin yasal sınırlar içerisinde üçüncü kişilere devrini de düzenlemiştir¹⁵².

AB, elektronik iletişim alanındaki bu düzenlemeyi yaparken modern iletişim araçlarının teknik olarak çokluğunu ve gelişmişliğini dikkate alarak, geleceğe yönelik ve tarafsız bir yaklaşım sergilemeye çalışmıştır. Direktif, halka açık iletişim ağları vasıtasıyla verilen elektronik iletişim hizmetleri hakkında uygulanacaktır¹⁵³. (m.3)

2002/58 sayılı Direktif, temel hak ve özgürlüklerin korunması kapsamında verileri kontrol edenlerin yükümlülükleri ve veri öznesinin hakları bakımından 1995/46 sayılı Direktifin hükümlerinin uygulanabileceğini belirtmiştir.

Bu Direktifle, üye devletler pek çok iletişim aracına ilişkin trafik ve yer bilgisini kaydetme yükümlülüğü altına girmiştir. Mobil telefon, SMS, sabit telefon, faks, elektronik posta, sohbet odaları, İnternet ve diğer iletişim araçları bu kapsamdadır. Milli güvenlik, suçun önlenmesi, suç soruşturması ve kovuşturmalarda kanunun öngördüğü şartlarda bu veriler kullanılabilir¹⁵⁴.

3. Avrupa Birliği 2006/24 Sayılı Direktifi

Avrupa Parlamentosu, 15 mart 2006’da 2006/24/ sayılı “Halka Açık İletişim Hizmetleri veya İletişim Ağlarına İlişkin Olarak Üretilen veya İşlenen Verilerin Saklanması İlişkin Direktif”i kabul etmiştir. Avrupa’da cezai soruşturmalarda işbirliğini kolaylaştırmak Direktifin önemli

¹⁵¹ Edwards, 2004, s. 320.

¹⁵² Arslan, 2010.

¹⁵³ Şimşek, Oğuz. (2008). *Anayasa Hukukunda Kişisel Verilerin Korunması*. İstanbul: Beta Yayınları, s. 57

¹⁵⁴ 5 Nisan 2011 tarihinde <https://www.privacyinternational.org/article/phr2006-overview-privacy#> adresinden erişildi.

amaçlarından birisidir¹⁵⁵. Yine, Direktif, özellikle adli vakaların incelenmesi ve suçlu takibinde, elektronik haberleşme altyapı ve hizmetlerinin kullanımı ile ortaya çıkan trafik ve konum bilgilerine ilişkin esasları düzenlemek amacıyla hazırlanmıştır.

Avrupa'da, Amerika'dan farklı olarak haberleşme servis sağlayıcıları ticari amaçlarla bilgileri rutin olarak depolamaktadır. Bu Direktifle birlikte artık servis sağlayıcılar ticari amaçlarla kaydettikleri bilgileri yasalar çerçevesinde mümkün olan en kısa sürede silmekle yükümlüdürler. Polis otoritelerine göre özellikle başta terör saldırıları olmak üzere suçla mücadelede bu veriler vazgeçilmez bir araçtır.

Direktif, suçun takibi ve yargıya intikali sürecinde gerekli verilerin sağlanabilmesi amacıyla elektronik haberleşme hizmet sağlayıcılarına bazı yükümlülükler getirmiş, bu kapsamda, saklanacak veri kategorileri, saklama süresi, verileri saklama koşulları ve veri güvenliği kapsamında gözetilecek kuralları düzenlemiştir.¹⁵⁶

Direktifin 5. maddesinde düzenlenen verilerin saklanması kişisel verilerin korunması açısından önem taşımaktadır. Buna göre servis sağlayıcılar, arayan ve aranan telefon numarası, abonenin adı ve adresi, İnternet kullanıcıları için kullanıcı kimliği ve adresi, iletişimin veya bağlantının tarihi, saati ve süresi ve coğrafi konumu gibi bilgileri 6 ay ile 2 yıl arası bir süre için saklamakla yükümlüdürler¹⁵⁷. Bu trafik verileri; İnternet telefonunu da içeren telefon numaraları, elektronik posta ve bunların tarih ve sürelerini de içermelidir. Üye ülkelerdeki ulusal polis kendi hukuk sistemlerine saygı ilkesi çerçevesinde bu bilgilere ulaşabilmelidir¹⁵⁸. Söz konusu verilere ancak, A.İ.H.S. çerçevesinde gereklilik ve ölçülülük ilkelerine uygun olarak yetkili ulusal makamlarca erişim sağlanabilecektir¹⁵⁹.

Bilindiği üzere Direktifler, AB üyesi ülkelerde uygulanan mevzuatın bir parçasıdır. Sonuçları açısından her muhatap üye devleti bağlar ancak şekil ve

¹⁵⁵ Bignami, 2007, s. 238.

¹⁵⁶ 5 Nisan 2011 tarihinde <https://www.privacyinternational.org/article/phr2006-overview-privacy#> adresinden erişildi.

¹⁵⁷ Bignami, 2007, s. 238.

5 Nisan 2011 tarihinde <https://www.privacyinternational.org/article/phr2006-overview-privacy#> adresinden erişildi.

¹⁵⁸ Bignami, 2007, s. 238.

¹⁵⁹ Uygun, 2010, s. 88.

yöntem seçimini ulusal makamlara bırakır¹⁶⁰. Direktiflerin uygulanabilmesi için tüzüklerden farklı olarak ulusal hukuka uyarlanması gerekir. Dolayısıyla, Direktiflerin kişisel verilerin korunmasında yeknesak bir hukuk düzeni oluşturmada önemli bir araç olduğu söylenebilir.

2006/24 sayılı Direktifin yapım sürecinde gündeme gelen belli başlı ilkeler şunlardır:

1-Kanun tarafından yetkilendirilme: Servis sağlayıcılar, ancak kanuni yetkileri çerçevesinde verileri tutabilirler. Yasal yetki olmaksızın haberleşmenin denetlenmesi A.İ.H.S.'nin 8. maddesi anlamında özel hayatın ihlali anlamına gelir. Veri Saklama Direktifi, üye ülkelerde konuya ilişkin ulusal kanunların yerini alacaktır. Başka bir ifadeyle, üye devletler ulusal mevzuatlarını bu Direktifle uyumlu hale getireceklerdir¹⁶¹.

2- Meşru amaç: A.İ.H.S.'nin 8. maddesindeki şartların yerine getirilmesi amacıyla Direktifin yapım aşamasında tartışılan diğer bir ilkedir¹⁶².

3- Ölçülülük ilkesi: Bu ilke, en çetrefilli sorunlardan birisidir. Ölçülülük, mahkeme veya yorumcuya bağlı olarak pek çok şekilde formüle edilmektedir. Hatta aynı mahkemede aynı oturumda farklı şekillerde analiz edilebilir¹⁶³. Bu ilkelerin, A.İ.H.M.'nin A.İ.H.S. çerçevesinde oluşturduğu içtihatlarından mülhem olduğu söylenebilir.

IV- Türk Hukukunda Kişisel Verilerin Korunması

A-Genel Olarak Türk Hukukunda Kişisel Verilerin Korunmasıyla İlgili Hukuksal Düzenlemeler

1. Kişisel Verilerin Korunmasında Hukuksal Çerçeve

Ülkemizde kişisel verilere ilişkin genel bir kanun bulunmamaktadır. Ancak, kişisel verilerin toplanması, korunması ve bunlara erişilmesi konusunda çeşitli hukuksal normlar bulunmaktadır. Konu, başta Anayasa olmak üzere, kanunlar ve çeşitli yönetmeliklerle düzenlenmiştir.

¹⁶⁰ 5 Nisan 2011 tarihinde http://www.ikv.org.tr/sozluk.asp?bas_harf=T&anahtar=&sayfa=2&id=1169 adresinden erişildi.

¹⁶¹ Bignami, 2007, s. 242.

¹⁶² Bignami, 2007, s. 245.

¹⁶³ Bignami, 2007, s. 246.

1.1. Anayasa

Ülkemizde kişisel verilerin korunması hakkının temelini oluşturacak anayasal hükümler 2010 anayasa değişikliğinden önce de mevcuttu. Hukuk devleti ilkesi (m.2), bireyin maddi ve manevi varlığını serbestçe geliştirme hakkı (m.17), özel hayatın gizliliği hakkı (m.20), konut dokunulmazlığı (m.21), haberleşmenin gizliliği (m.22), dini ve vicdani kanaatleri açıklamaya zorlanamama (m.24), düşünce ve kanaatleri açıklamaya zorlanamama (m.25) konuya örnek olarak verilebilir.

Kişisel verilerin devlet tarafından toplanması, depolanması, işlenmesi faaliyetleri sırasında her bireyin temel hak ve özgürlüklerinin korunmasını isteme hakkı vardır. Bu haklardan, özel yaşamın gizliliği, bireyin maddi ve manevi varlığını geliştirme hakkı, bireyin kişisel verilerinin korunmasının doğrudan anayasal dayanakları, diğer temel haklar ise ilgilendirdikleri özel yaşam ilişkisi alanında kişisel veriler için dolaylı olarak koruma sağlayan temel haklardır¹⁶⁴.

Bireyin kişisel verileri üzerindeki hakkı, kamusal organların kişisel veri ihtiyacının karşılanmasına yönelik faaliyetleri karşısında, bireyi veri işleme faaliyetlerinin öznesi haline gelmekten, özel yaşam ilişkilerinin bütün yönlerine ait verileriyle kamusal iktidar tarafından bilinen, kişilik profili çıkartılabilmesi mümkün olan, özel hayatında ne yaptığı veya yapabileceği bilinen ve bu suretle Anayasada ve uluslararası belgelerde koruma altına alınan özel hayatın gizliliği hakkı ortadan kaldırılmış ve kişiliği içerisine sıkıştırılmış bir insan profili haline dönüşmekten korumaya hizmet eder¹⁶⁵.

Anayasanın 20. maddesi, kişisel verilerin korunmasıyla doğrudan ilgili olup kenar başlığı “özel hayatın gizliliği ve korunması”dır. 2010 yılında yapılan değişiklikle kişisel verilerin korunması ilk kez anayasaya girmiştir¹⁶⁶. Buna göre;

“Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz...”

¹⁶⁴ Şimşek, 2001.

¹⁶⁵ Şimşek, 2001.

¹⁶⁶ 5 Mayıs 2011 tarihinde <http://www.resmigazete.gov.tr/main.aspx?home=http://www.resmigazete.gov.tr/eskiler/2010/05/20100513.htm&main=http://www.resmigazete.gov.tr/eskiler/2010/05/20100513.htm> adresinden erişildi.

...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.”

Bu maddeyle kişisel verilerin korunmasını hakkı anayasal düzeyde koruma altına alınmıştır. Böylece, bireylerin kendileriyle ilgili kişisel veriler üzerinde hangi hak ve yetkilere sahip olduğu ve kişisel verilerin hangi hallerde işlenebileceği hükme bağlanmıştır. Konuyla ilgili ayrıntılı düzenleme ise kanunla yapılacaktır.

1.2. Türk Medeni Kanunu

Türk Medeni Kanununun 24. maddesi, kişilik haklarının korunmasını düzenlemiştir. Kişisel verilerinin hukuka aykırı bir şekilde kullanıldığını düşünen bir kişi Medeni Kanun hükümlerinden yararlanarak bu ihlalin durdurulmasını isteyebilir¹⁶⁷.

Yine, yeni Borçlar Kanununun 49 vd. maddelerinde haksız fiillere karşı talep edilecek tazminatlar düzenlenmiştir. Bu hükümler kişisel verilerin ihlali halinde açılacak tazminat davalarında kullanılabilir¹⁶⁸.

Medeni Kanun ve Borçlar kanunu hükümleri gerek kişilik haklarına yönelik saldırıların önlenmesinde gerekse kişisel verilerin korunması açısından yasal dayanak oluşturmaktadır. Ancak, bu alanın kendine özgü niteliği gereği, genel hükümlerle kişisel verileri etkin bir şekilde korumak kolay değildir.

1.3. Türk Ceza Kanunu¹⁶⁹

5237 sayılı Türk Ceza Kanununun 134 vd. maddelerinde özel hayatın gizliliği ve kişisel verilerin toplanması ve korunmasıyla ilgili çeşitli konular düzenlemiştir.

¹⁶⁷ 15 Mayıs 2011 tarihinde <http://www.mevzuat.gov.tr/Metin.Aspx?MevzuatKod=1.5.4721&sourceXmlSearch=&MevzuatIliski=0> adresinden erişildi.

¹⁶⁸ 15 Mayıs 2011 tarihinde <http://www.mevzuat.gov.tr/Metin.Aspx?MevzuatKod=1.5.6098&MevzuatIliski=0&sourceXmlSearch=> adresinden erişildi.

¹⁶⁹ 15 Mayıs 2011 tarihinde <http://www.mevzuat.gov.tr/Metin.Aspx?MevzuatKod=1.5.5237&MevzuatIliski=0&sourceXmlSearch=> adresinden erişildi.

134. maddeye göre; kişilerin özel hayatının gizliliğini ihlâl eden kimse, hapis veya adlî para cezası ile cezalandırılır. Gizliliğin görüntü veya seslerin kayda alınması suretiyle ihlâl edilmesi hâlinde, ceza belirli oranda arttırılır. Yine aynı maddenin ikinci fıkrasında özel hayata ilişkin görüntü veya sesleri ifşa etmek de cezai yaptırıma bağlanmıştır. Bu yayma eylemi, basın ve yayın yoluyla işlenmesi hâlinde, ceza oranı arttırılacaktır.

135. maddede, kişisel verilerin hukuka aykırı olarak kaydedilmesi suç teşkil eden bir eylem olarak belirlenmiştir. Yine aynı maddeye göre; kişilerin siyasi, felsefi veya dinî görüşlerine, ırkî kökenlerine; hukuka aykırı olarak ahlâkî eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgileri kişisel veri olarak kaydeden kimsenin eyleminin de cezalandırılacağı hükme bağlanmıştır. Başka bir ifadeyle, hassas verilerle ilgili yapılan kaydetme işlemleri de cezai müeyyideye bağlanmıştır.

136. maddede, kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişinin eyleminin cezalandırılacağı hükme bağlanmıştır. Söz konusu verileri veren veya yayan kimsenin kamu görevlisi olması halinde verilen cezanın artması önemli bir noktadır.

Kaydedilen verilerin belirli bir süre sonra silinmesi kişisel verilerin korunması açısından önem taşır. 138. maddeye göre; kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlar görevlerini yerine getirmediklerinde takdirde hapis cezasıyla cezalandırılacaklardır. Buna göre; yasal çerçevede kaydedilen verilerin belirlenmiş sürenin sonunda imha edilmesi gerekmektedir.

Türk Ceza Kanunu, kişisel verilerin ceza hukuku açısından korunması ve kişisel verileri hukuka aykırı olarak işleyenler hakkında yaptırım öngörmesi açısından oldukça etkin bir sistem getirmiştir. Türk Ceza Kanununun yukarıda bahsedilen hükümleri konuya ilişkin AB Direktifleriyle de uyumludur. TBMM'de bulunan Kişisel Verilerin Korunmasına İlişkin Kanun Tasarısı, kişisel verilerin korunması alanında yeni müeyyideler getirmekten ziyade burada bahsedilen hükümlere atıf yapmaktadır.

1.4. Ceza Muhakemesi Kanunu¹⁷⁰

Kişisel verilerin işlenmesi, Ceza Muhakemesi Kanununun (CMK) 75 vd. maddelerinde düzenlenmiştir. Şüpheli, sanık veya diğer kişilerin beden muayenesi ve vücudundan örnek alınması, soy bağının veya elde edilen bulgunun şüpheli veya sanığa ya da mağdura ait olup olmadığının tespiti için zorunlu olması halinde moleküler genetik incelemeler yapılması konuya örnek olarak verilebilir.

Fiziki kimliğin tespiti yani, şüpheli veya sanığın, kimliğinin teşhisi için gerekli olması halinde, Cumhuriyet savcısının emriyle fotoğrafı, beden ölçüleri, parmak ve avuç içi izi, bedeninde yer almış olup teşhisini kolaylaştıracak diğer özellikleri ile sesi ve görüntüleri kaydedilebilir.

CMK 80. maddeye göre; 75, 76 ve 78 inci madde hükümlerine göre alınan örnekler üzerinde yapılan inceleme sonuçları kişisel veri niteliğinde olup, başka bir amaçla kullanılamaz, dosya içeriğini öğrenme yetkisine sahip bulunan kişiler tarafından bir başkasına verilemez.

Ceza Muhakemesi Kanununun 134 vd. maddelerinde ise bilgisayar ortamında verilerin kopyalanması, telekomünikasyon yoluyla yapılan iletişimin denetlenmesi, gizli soruşturmacı ve teknik araçlarla izlemeyle ilgili önlemler ve bu önlemlerin denetlenmesine ilişkin hükümler yer almaktadır.

135. maddeye göre; bir suç dolayısıyla yapılan soruşturma ve kovuşturmada, suç işlendiğine ilişkin kuvvetli şüphe sebeplerinin varlığı ve başka suretle delil elde edilmesi imkânının bulunmaması durumunda, hâkim veya gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısının kararıyla şüpheli veya sanığın telekomünikasyon yoluyla iletişimi tespit edilebilir, dinlenebilir, kayda alınabilir ve sinyal bilgileri değerlendirilebilir. Görüldüğü gibi, kişinin iletişimine müdahale edilebilmesi ancak yargı kararıyla mümkündür.

Yine 140. maddeye göre; maddede sayılan belli suçların işlendiği hususunda kuvvetli şüphe sebepleri bulunması ve başka suretle delil elde edilememesi hâlinde, şüpheli veya sanığın kamuya açık yerlerdeki faaliyetleri ve işyeri teknik araçlarla izlenebilir, ses veya görüntü kaydı alınabilir.

¹⁷⁰15 Mayıs 2011 tarihinde <http://www.mevzuat.gov.tr/Metin.Asp?MevzuatKod=1.5.5271&MevzuatIliski=0&sourceXmlSearch=> adresinden erişildi.

Günümüzde, bilgi ve iletişim teknolojilerinde yaşanan gelişmeler dikkate alındığında bu maddenin değerinin daha da arttığı söylenebilir. Çünkü, çağımızda telekomünikasyon yoluyla yapılan iletişim hiç olmadığı kadar yaygınlaşmış ve hayatın vazgeçilemez bir parçası haline gelmiştir.

1.5. Vergi Usul Kanunu¹⁷¹

Kişisel verilerin toplanmasına ilişkin olarak Vergi Usul Kanunu'nda, vergi yükümlüleri hakkında bilgi toplama ve saklamaya ilişkin özel hükümler bulunmaktadır. 148. madde, konuya örnek olarak verilebilir. Maddeye göre; kamu idare ve müesseseleri, mükellefler veya mükelleflerle muamelede bulunan diğer gerçek ve tüzel kişiler, Maliye Bakanlığının veya vergi incelemesi yapmaya yetkili olanların isteyecekleri bilgileri vermeye mecburdurlar. Bilgiler yazı veya sözle istenilir.

1.6. 4857 sayılı İş Kanunu

İş Kanunu işvereni, çalıştırdığı her işçi için bir özlük dosyası düzenlemek ve bu dosya da işçinin kimlik bilgilerinin yanında, düzenlemek zorunda olduğu her türlü belgeyi saklamak ve bunları istendiği zaman yetkili memur ve mercilere göstermekle yükümlü tutmuştur. Ayrıca Kanun işverene, işçi hakkında edindiği bilgileri dürüstlük kuralları ve hukuka uygun olarak kullanma ve gizli kalmasında işçinin haklı çıkarı bulunan bilgileri açıklamama ödevi getirmiştir¹⁷². (m. 75)

1.7. 5490 Sayılı Nüfus Hizmetleri Kanunu

5490 Sayılı Nüfus Hizmetleri Kanununun 1. maddesinde; kanunun amacının “Kişinin doğumundan ölümüne kadar kişisel ve medeni durumuna, uyrukluğuna ve bunlarda meydana gelebilecek değişikliklere ait doğal ve hukuki olayların belirlenip saptanması, bu amaçla düzenlenmiş kütüklere yazılması, elektronik ortamda ulusal adres veri tabanının oluşturulması, nüfus kayıtları ile adres bilgilerinin ilişkilendirilmesini sağlamak” olduğu ifade edilmiştir¹⁷³.

¹⁷¹15 Mayıs 2011 tarihinde <http://mevzuat.basbakanlik.gov.tr/Metin.Aspx?MevzuatKod=1.4.213&MevzuatIliski=0&sourceXmlSearch=> adresinden erişildi.

¹⁷²15 Mayıs 2011 tarihinde <http://mevzuat.basbakanlik.gov.tr/Metin.Aspx?MevzuatKod=1.5.4857&MevzuatIliski=0&sourceXmlSearch=> adresinden erişildi.

¹⁷³15 Mayıs 2011 tarihinde <http://mevzuat.basbakanlik.gov.tr/Metin.Aspx?MevzuatKod=1.5.5490&MevzuatIliski=0&sourceXmlSearch=> adresinden erişildi.

1.8. Bilgi Edinme Kanunu

4982 sayılı Bilgi Edinme Kanununda bilgi; kurum ve kuruluşların sahip oldukları kayıtlarda yer alan her türlü veri olarak tanımlanmıştır¹⁷⁴. Buradan hareketle bilgi edinme, kurum ve kuruluşların kaydettikleri verilere kanunun belirlediği çerçevede ulaşma hakkı olarak tanımlanabilir. Burada bahsedilen kurum ve kuruluşları, Kanunun 2. maddesinde bahsedildiği üzere; kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşları olarak anlamak gerekir.

Bilgi edinme hakkı, kişisel verilere ulaşma açısından önemli bir araçtır. Bu erişim sayesinde ilgili kişi kendisi hakkında tutulan verileri öğrenme imkanına sahip olacak, bu durum ise kurumları işlem yaparken objektif olmaya zorlayacaktır. Bilgi Edinme Değerlendirme Kurulu, çeşitli tarihlere verdiği kararlarla; kamu görevlileri için düzenlenen sicil raporları, özlük dosyaları ve benzeri belgelerin ilgisine karşı açık olduğunu, bilgi edinme hakkı kapsamında ilgilinin kendisiyle ilgili bilgi ve belgelere erişim hakkının bulunduğunu belirtmiştir¹⁷⁵.

1.9. Polis Vazife ve Salahiyet Kanunu¹⁷⁶

Polis Vazife ve Salahiyet Kanununda (PVSK) parmak izi ve fotoğrafların kayda alınması ile istihbarat amaçlı iletişimin tespiti konusunda özel hükümler bulunmaktadır. Bu hükümler arasında özellikle PVSK' nın Ek 7. maddesi iletişimin tespiti konusunda önemli yetkiler içermektedir. Başka bir ifadeyle, PVSK, kişisel verilerin korunması açısından önemli hükümleri haizdir.

PVSK 5. maddeye göre polis; her çeşit silah ruhsatı, sürücü belgesi, pasaport veya pasaport yerine geçen belge almak için başvuruda bulunan, başta polis olmak üzere, genel veya özel kolluk görevlisi ya da özel güvenlik görevlisi olarak istihdam edilen, Türk vatandaşlığına başvuruda bulunan, sığınma talebinde bulunan veya gerekli görülmesi halinde, ülkeye giriş yapan sair yabancı, gözaltına alınan kişilerin parmak izini alır. Sisteme kaydedilen bilgiler, kimlik tespiti, suçun önlenmesi veya yürütülmekte olan

¹⁷⁴15 Mayıs 2011 tarihinde <http://mevzuat.basbakanlik.gov.tr/Metin.aspx?MevzuatKod=1.5.4982&MevzuatIlski=0&sourceXmlSearch=> adresinden erişildi.

¹⁷⁵Kaya, 2005, s. 106; 15 Mayıs 2011 tarihinde <http://www.bedk.gov.tr/> adresinden erişildi.

¹⁷⁶15 Mayıs 2011 tarihinde <http://www.egm.gov.tr/pvsk.htm> adresinden erişildi.

soruşturma ve kovuşturma kapsamında maddî gerçeğin ortaya çıkarılması amacıyla mahkeme, hâkim, Cumhuriyet savcısı ve kolluk tarafından kullanılabilir.

Yine 5. maddeye göre; sistemde kayıtlı bilgilerin hangi kamu görevlisi tarafından ve ne amaçla kullanıldığının denetlenebilmesine imkân tanıyan bir güvenlik sistemi kurulur. Sistemde yer alan kayıtlar gizlidir ve 5. maddede belirlenen amaçlar dışında kullanılamaz. Sisteme kayıtlı olan parmak izi ve fotoğraflar, kişinin ölümünden itibaren on yıl ve her halde kayıt tarihinden itibaren seksen yıl geçtikten sonra sistemden silinir.

1.10. 5809 Sayılı Elektronik Haberleşme Kanunu¹⁷⁷

Elektronik Haberleşme Kanunu kişisel verilerin korunmasıyla ilgili hükümler içermektedir. Kanununun 12. maddesi işletmecilerin hak ve yükümlülükleri arasında kişisel veri ve gizliliğini sağlaması açık bir yükümlülük olarak belirlenmiştir. (m.4-d) Yine aynı maddede, işletmecilerden kanunlarla yetkili kılınan kurumlarca yasal dinleme ve iletişime müdahalenin yapılmasına teknik olanak sağlanmasını temin etmek bir yükümlülük olarak düzenlenmiştir (m. 4-g).

Kanununun 51. maddesine göre, Bilgi Teknolojileri ve İletişim Kurumu elektronik haberleşme sektörüyle ilgili kişisel verilerin işlenmesi ve gizliliğinin korunmasına yönelik usul ve esasları belirlemeye yetkilidir. Yine Kanununun 55. maddesine göre, Kurum tarafından izin verilmedikçe, abone kimlik ve iletişim bilgilerini taşıyan özel bilgiler veya cihazın teşhisine yarayan elektronik kimlik bilgileri yeniden oluşturulamaz, değiştirilemez, kopyalanarak çoğaltılamaz veya herhangi bir amaçla dağıtılamaz.

Kanununun 56. maddesine göre ise, abone kimlik ve iletişim bilgilerini taşıyan özel bilgiler ile cihazların elektronik kimlik bilgilerini taşıyan her türlü yazılım, kart, araç veya gereç yetkisiz ve izinsiz olarak kopyalanamaz, muhafaza edilemez, dağıtılamaz, kendisine veya başkasına yarar sağlamak amacıyla kullanılamaz.

¹⁷⁷15 Mayıs 2011 tarihinde <http://mevzuat.basbakanlik.gov.tr/Metin.aspx?MevzuatKod=1.5.5809&MevzuatIliski=0&sourceXmlSearch=> adresinden erişildi.

1.11. 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun

Mayıs 2007'de yürürlüğe giren 5651 sayılı kanun¹⁷⁸ İnternet ortamında yapılan yayınları düzenleyen bir kanundur. Kanunun temel amacı, İnternet ortamında işlenen bazı suçlarla mücadele etmektir. 5651 sayılı Kanunda ayrıca, erişim sağlayıcı, yer sağlayıcı, içerik sağlayıcı, İnternet toplu kullanım sağlayıcı ve ticari amaçla İnternet toplu kullanım sağlayıcıları düzenlenmiştir. Bu Kanunla İnternet aktörleri ilk kez tanımlanmış ve yükümlülükleri belirlenmiştir. Buna göre; İnternet aktörleri erişim sağlayıcı, yer sağlayıcı, içerik sağlayıcı, İnternet toplu kullanım sağlayıcı ve ticari amaçla İnternet toplu kullanım sağlayıcılarıdır.

Bu Kanununun 3. maddesi bilgilendirme yükümlülüğü ile ilgilidir. Bu maddeye göre, içerik, yer ve erişim sağlayıcıları, yönetmelikle belirlenen esas ve usuller çerçevesinde tanıtıcı bilgilerini kendilerine ait internet ortamında kullanıcıların ulaşabileceği şekilde ve güncel olarak bulundurmakla yükümlüdür. Bu hüküm, İnternet kullanıcılarının İnternet aktörleriyle iletişime geçmesini kolaylaştıran önemli bir araçtır.

5651 sayılı Kanunun diğer önemli bir özelliği, İnternet ortamında hakları ihlal edilenlere bunu giderme imkanı sağlamasıdır. 9. maddeye göre, İnternetteki bir içerik nedeniyle hakları ihlâl edildiğini iddia eden kişi, içerik sağlayıcısına, buna ulaşamaması halinde yer sağlayıcısına başvurarak kendisine ilişkin içeriğin yayından çıkarılmasını ve hazırladığı cevabın bir hafta süreyle internet ortamında yayımlanmasını isteyebilir. Kişisel verilerdeki yanlışlıkların düzeltilmesini sağlayan bu hüküm, veri korunmasında önemli bir araç olarak kullanılabilir.

1.12. 5070 sayılı Elektronik İmza Kanunundaki Düzenlemeler

5070 sayılı Elektronik İmza Kanununun 12. maddesi kişisel verilerin korunmasıyla ilgilidir¹⁷⁹. Elektronik sertifika hizmet sağlayıcısı;

¹⁷⁸15 Mayıs 2011 tarihinde <http://www.mevzuat.gov.tr/Metin.Asp?MevzuatKod=1.5.5651&MevzuatIlski=0&sourceXmlSearch=> adresinden erişildi.

¹⁷⁹ 15 Mayıs 2011 tarihinde http://www.tk.gov.tr/eimza/eimza_yasasi.htm adresinden erişildi.

- Elektronik sertifika talep eden kişiden, elektronik sertifika vermek için gerekli bilgiler hariç bilgi talep edemez ve bu bilgileri kişinin rızası dışında elde edemez.

- Elektronik sertifika sahibinin izni olmaksızın sertifikayı üçüncü kişilerin ulaşabileceği ortamlarda bulunduramaz.

- Elektronik sertifika talep eden kişinin yazılı rızası olmaksızın üçüncü kişilerin kişisel verileri elde etmesini engeller. Bu bilgileri sertifika sahibinin onayı olmaksızın üçüncü kişilere iletmez ve başka amaçlarla kullanamaz.

1.13. Ceza Muhakemesinde Beden Muayenesi, Genetik İncelemeler ve Fizik Kimliğin Tespiti Hakkında Yönetmelik¹⁸⁰

Bu Yönetmelik; bir suça ilişkin iz, eser, emare ve delillerin elde edilmesi; ayrıca, maddî gerçeğin ortaya çıkartılması bakımından şüpheli, sanık, mağdur ve diğer kişilerin beden muayenelerinin yapılması, tıbbî incelemelerde bulunmak üzere vücuttan, kan veya benzeri biyolojik örneklerle, saç, tükürük, tırnak gibi örneklerin alınması, moleküler genetik incelemeler ile şüpheli ve sanığın kimliğinin tespiti için gerekli fizikî özelliklerin tespitine ilişkin usul ve esasları düzenlemiştir (m. 1).

Yönetmelikte, şüpheli veya sanığın iç beden muayenesi, dış beden muayenesi, şüpheli veya sanığın vücudundan örnek alınması, diğer kişilerin beden muayenesi ve vücudundan örnek alınması, soy bağının araştırılması konuları düzenlenmiştir.

Yönetmelikte ayrıca fizik kimliğin tespiti için gerekli olan kayıt ve bilgilerin neler olduğu ve bunları almaya yetkili mercilerin kimler olduğu, verilerin imhası ve verilerin muhafazasına ilişkin hükümler bulunmaktadır.

Bu Yönetmelikte, beden muayenesi ve incelemenin türü, amacı, toplanacak verilerin içeriği, karar vermeye yetkili mercii, verilerin muhafazası, korunması ve imhası gibi konular düzenlenmektedir. Bu tür muayene ve incelemelerde elde edilen bilgilerin ve tespitlerin kişilere ait, onları belirleyici nitelik taşıması nedeniyle, bu incelemeler sonucu elde

¹⁸⁰15 Mayıs 2011 tarihinde <http://www.resmigazete.gov.tr/main.aspx?home=http://www.resmigazete.gov.tr/eskiler/2005/06/20050601.htm&main=http://www.resmigazete.gov.tr/eskiler/2005/06/20050601.htm> adresinden erişildi.

edilen verilerin kişisel verilerin korunması kapsamı içerisinde değerlendirilmesi gerekir.

1.14. Ceza Muhakemesi Kanununda Öngörülen Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi, Gizli Soruşturmacı ve Teknik Araçlarla İzleme Tedbirlerinin Uygulanmasına İlişkin Yönetmelik¹⁸¹

Günümüzde telekomünikasyon sektöründe yaşanan gelişmeler bu sektördeki araçları hayatımızın doğal bir parçasına haline getirmiştir. Bu durum, pek çok ülkede telekomünikasyon alanında kişisel verilerin korunması açısından özel düzenleme yapılmasına yol açmıştır.

Yönetmeliğin amacı, Ceza Muhakemesi Kanununda öngörülen telekomünikasyon yoluyla yapılan iletişimin denetlenmesi, gizli soruşturmacı ve teknik araçlarla izleme tedbirlerine ilişkin talepte bulunulması, kararların alınması ve uygulanmasında uyulacak usul ve esasları belirlemektir. Yönetmelik; telekomünikasyon yoluyla yapılan iletişimin denetlenmesi, teknik araçlarla izleme ve gizli soruşturmacı tayini olmak üzere üç temel konuyu düzenlemektedir.

Telekomünikasyon yoluyla yapılan iletişimin denetlenmesi başlığı altında; iletişimin tespiti, dinlenmesi, kayda alınması ve sinyal bilgilerinin değerlendirilmesi talebi ve kararı, talepte ve kararda belirtilmesi gereken hususlar, alınacak tedbirin kapsamı ve kimler hakkında alınacağı, tedbirin alınacağı suçlar, tedbirin nasıl icra edileceği, mevzuat ve bu Yönetmelik kapsamı dışındaki önlemlere itiraz ve kanuna aykırı elde edilmiş bulguların niteliği, işlem görevlileri, tedbirin alınabileceği süre ve bunun uzatılması, tespit ve dinlemeye ilişkin tedbirin geçersiz kılınması halinde kayıtların en geç 10 gün içinde yok edilmesi ve tesadüfen elde edilen delillerin hukuki niteliği gibi konuları düzenlemektedir.

Teknik araçlarla izleme başlığı altında; teknik araçlarla izleme talebi ve kararı, teknik araçlarla izlemeye ilişkin talep ve kararların içeriği, tedbirin kapsamı, tedbirin uygulanabileceği suçlar , teknik araçlarla izleme işleminin icrası, izleme süresi ve uzatılması, tedbir sonucu elde edilen delillerin

¹⁸¹15 Mayıs 2011 tarihinde <http://www.resmigazete.gov.tr/main.aspx?home=http://www.resmigazete.gov.tr/eskiler/2007/02/20070214.htm&main=http://www.resmigazete.gov.tr/eskiler/2007/02/20070214.htm> adresinden erişildi.

geçersiz kılınması halinde imha edilmesi ve teknik araçlarla izleme sırasında tesadüfen elde edilen delillerin durumu düzenlemiştir.

1.15. Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğin Korunması Hakkında Yönetmelik¹⁸²

Bilgi ve iletişim teknolojilerinde yaşanan baş döndürücü gelişmeler dünyayı küresel köy haline getirmiştir. Bilgi alışverişinin bu kadar kolay hale gelmesiyle birlikte verilerin korunmasının önemi daha da artmıştır¹⁸³. Günümüzde telekomünikasyon araçlarının yaygınlığı ve gelişimi dikkate alındığında bu sektördeki tutulan verilerin korunmasının ayrıca önemli olduğu söylenebilir.

Yönetmelik, Telekomünikasyon sektöründe, özel hayatın gizliliğine yönelik temel hakların tam ve etkin olarak korunması amacıyla 2002/58 sayılı AB Direktifi baz alınarak hazırlanmıştır. Yönetmelikte ağırlıklı olarak tüketicilerin telekomünikasyon hizmetlerinden yararlanırken sahip oldukları gizlilik haklarının korunması hedeflenmiştir. Yönetmeliğin amacı, telekomünikasyon sektöründe kişisel bilgilerin işlenmesi ve gizliliğinin korunmasını güvence altına almaktır. Yönetmelik, telekomünikasyon sektöründe hizmet veren ve alan gerçek ve tüzel kişileri kapsamaktadır.

Yönetmelikte kişisel veriler; tanımlanmış ya da doğrudan veya dolaylı olarak, bir kimlik numarası ya da fiziksel, psikolojik, zihinsel, ekonomik, kültürel ya da sosyal kimliğinin, sağlık, genetik, etnik, dini, ailevi ve siyasi bilgilerinin bir ya da birden fazla unsuruna dayanarak tanımlanabilen gerçek ve/veya tüzel kişilere ilişkin herhangi bir bilgi olarak tanımlanmıştır. (m.3)

Kişisel bilgilerin işlenmesi; otomatik olsun veya olmasın, toplama, kaydetme, hazırlama, yükleme, uyarlama, değiştirme, geri çağırma, danışma, kullanma, aktarma yoluyla açığa vurma, yayma ya da bunların dışında erişilebilir hale getirme, düzenleme, birleştirme, engelleme, silme gibi yollardan, kişisel bilgiler üzerinden yürütülmekte olan herhangi bir işlem ya da işlemler bütünüdür. (m.3)

¹⁸² 15 Mayıs 2011 tarihinde http://www.tk.gov.tr/mevzuat/yonetmelikler/dosyalar/Kisisel_Bil_Yon_06_02_04.pdf adresinden erişildi.

¹⁸³ Ersoy, 2006.

İşletmeciler, verilerin korunması çerçevesinde, verdikleri hizmetlerin güvenliğini sağlamak amacıyla, şebekenin güvenliğine ilişkin teknik ve yapısal önlemleri almakla yükümlüdür. (m.6) Bu önlemler, yazılım veya donanım vasıtasıyla olabilir.

Yönetmelikte işletmeciler tarafından tutulan verilerin gizli olduğu vurgulanmıştır. Yasaların ve yargı kararlarının öngördüğü durumlar haricinde, haberleşmeye taraf olanların tamamının izni olmaksızın, telekomünikasyonun üçüncü şahıslar tarafından dinlenmesi, kaydedilmesi, saklanması, kesilmesi veya gözetimi yasaklanmıştır. (m.8) Yine trafik verilerinin, işletmeci tarafından hizmet amaçları dışında kaydedilemeyeceği ve izlenmeyeceği ifade edilmiştir. Trafik verisi; bir şebekede haberleşmenin iletimi veya faturalama amacıyla işlenen her türlü veridir.

Yönetmeliğin 10. maddesinde trafik verisini tutabilecek kişiler belirlenmiştir. Bunlar; işletmecinin yetkisi altındaki kişiler, telekomünikasyon hizmetlerinin faturalama ve trafik idaresi, müşteri hizmetleri, yolsuzluk tespitleri, elektronik telekomünikasyon hizmetleri pazarlama veya katma değerli hizmet ile görevli kişilerdir. Bunlar dışındaki kişilerin veri kaydetmesi durumunda hukuki sorumluluk doğacaktır. Trafik bilgileri ancak, arabağlantı, faturalama veya benzeri anlaşmazlıkları çözmek amacıyla mahkeme veya uyuşmazlığı çözmekle yetkili gerçek ve tüzel kişilere verilebilir.

Yönetmeliğin 18. maddesinde trafik verilerinin kayıt süresi düzenlenmiştir. Bu sürenin belirlenmesi kişisel verilerin korunması açısından önemlidir. Söz konusu veriler; kötü niyetli veya rahatsızlık verici aramaların takibi amacıyla bir yıl süreyle saklanırlar. Bu süre, konuyu altı ay ile iki yıl arası bir zaman dilimi belirleyip takdiri üye ülkelere bırakan 2006/24 sayılı AB direktifiyle uyumludur.

Yönetmeliğin 20. maddesinde istek dışı haberleşmeler (spam) düzenlenmiştir. Buna göre, işletmeciler kişi müdahalesi olmadan çalışan fakslar, elektronik posta, kısa mesaj gibi otomatik arama sistemlerini, abonenin önceden izni olmadan siyasi propaganda amacıyla kullanamazlar. Yine, söz konusu otomatik arama sistemlerinin doğrudan pazarlama amacıyla da kullanamayacaklardır. Öte yandan, doğrudan pazarlama amacıyla gönderilen ve kimin adına haberleşme yapıldığı hususunda

göndericinin kimliğini saklayan veya alıcının bu iletişimin sonlandırılması konusunda talepte bulunacağı bir adres bulunmayan elektronik mektupların gönderilmesi abonenin bu yöndeki talebi halinde engelleneceği hükme bağlanmıştır.

Son olarak; işletmeciler kişisel bilgilerinin işlenmesi ve gizliliğinin korunması için gerekli terminal cihazlarını temin etmekle yükümlüdürler. Başka bir ifadeyle, işletmecilerin Yönetmeliğin uygulanabilmesi gerekli teknik sistemi kurmaları gerekir.

2. Avrupa Birliği İlerleme Raporları, Katılım Ortaklığı Belgesi ve Türkiye Ulusal Programında Kişisel Verilerin Korunması

Avrupa Birliği İlerleme Raporlarında, Ulusal Program ile Katılım Ortaklığı Belgesinde kişisel verilerin korunması yer almaktadır. İlerleme Raporları, aday ülkelerin Avrupa Birliğine katılım sürecinde Kopenhag kriterlerine uyum yönünde kaydettikleri gelişmeleri değerlendiren ve Avrupa Komisyonu tarafından 1998 yılından bu yana yıllık olarak hazırlanan raporlardır¹⁸⁴. Türkiye hakkında 2001 yılından itibaren hazırlanan ilerleme raporlarında, kişisel verilerin korunması alanında mevzuat eksikliğine vurgu yapılmakta ve bu eksikliğin giderilmesi talep edilmektedir¹⁸⁵.

Ulusal program ise, Avrupa Birliğine aday ülkeler tarafından hazırlanarak Avrupa Komisyonuna sunulan ve Katılım Ortaklığı Belgesinde yer alan önceliklerin ne şekilde yerine getirileceğine ilişkin belgedir. Ulusal Programda, AB müktesebatına uyum sağlamak için aday ülkelerin mevzuatlarında yapacakları düzenlemeler, uyum için gerekli beşeri ve mali kaynaklar, AB müktesebatının üstlenilmesi amacıyla geliştirilmesi gereken idari yapı ve tüm bu hususlara ilişkin kısa ve orta vadeli öncelikler takvimi yer almaktadır¹⁸⁶. 2001, 2003 ve 2008 yıllarında hazırlanan ulusal programlarda kişisel verilerin korunması alanında hukuksal düzenleme yapılacağı taahhüt edilmiştir¹⁸⁷.

¹⁸⁴ 20 Mayıs 2011 tarihinde <http://ekutup.dpt.gov.tr/ab/sozluk.pdf> adresinden erişildi.

¹⁸⁵ 20 Mayıs 2011 tarihinde <http://www.abgs.gov.tr/index.php?p=123&l=1> adresinden erişildi.

¹⁸⁶ Avrupa Birliği ve Türkiye, Başbakanlık Dış Ticaret Müsteşarlığı Avrupa Birliği Genel Müdürlüğü, Doğu Matbaacılık, 2002, Ankara, s. 464; 20 Mayıs 2011 tarihinde <http://ekutup.dpt.gov.tr/ab/sozluk.pdf> adresinden erişildi.

¹⁸⁷ 20 Mayıs 2011 tarihinde <http://www.abgs.gov.tr/index.php?p=123&l=1> adresinden erişildi.

Katılım Ortaklığı Belgesi ise; Avrupa Birliğine aday ülkeler için, Avrupa Komisyonu tarafından hazırlanan ve AB Konseyi tarafından kabul edilen, her bir aday ülkenin AB'ye katılım yönünde gelişme kaydetmesi öngörülen öncelikli alanların değerlendirildiği bir belgedir¹⁸⁸. Katılım Ortaklığı Belgesi, aday ülkenin Kopenhag kriterlerine uyum sağlama doğrultusundaki yükümlülükleri kapsamında, kısa ve orta vadeli önceliklere ilişkin bir takvim içerir.

Katılım Ortaklığı Belgeleri, 2001, 2003, 2006 ve 2008 yıllarında kabul edilmiştir. 2001 tarihli Katılım Ortaklığı Belgesinde göre aday ülkeler için; Schengen Bilgi Sistemi ve Europol'a katılabilmek için veri koruma alanında AB müktesebatını benimsemelerinden¹⁸⁹, 2003 tarihli Belgede; kişisel verilerin korunmasına ilişkin müktesebata uyum sağlanmasından¹⁹⁰, 2006 tarihli Belgede; Müktesebat doğrultusunda, kişisel verilerin korunması konusunda bir yasa kabul edilmesi ve bağımsız bir denetim makamı kurulmasından¹⁹¹, 2008 tarihli Belgede; kişisel verilerin korunması hakkındaki müktesebat ile ilgili mevzuatın uyumlaştırılması ve bağımsız bir, veri koruma denetleme otoritesinin kurulmasına yönelik çabaların artırılmasından bahsedilmiştir¹⁹².

3. Kişisel Verilerin Korunması Kanun Tasarısı

3.1. Genel Olarak

Türk hukukunda, gerek kamu gerekse özel sektörde kişisel verilerin korunmasını sağlayacak özel bir kanuni düzenleme bulunmamaktadır. Kişisel veriler, kişilik haklarına ilişkin genel hükümler aracılığıyla korunmaktadır¹⁹³. 2010 yılında yapılan anayasa değişikliği ile konu anayasal güvence altına alınmıştır.

¹⁸⁸ Avrupa Birliği ve Türkiye, s. 459.

¹⁸⁹ 20 Mayıs 2011 tarihinde http://www.abgs.gov.tr/files/AB_Iliskileri/AdaylikSureci/Kob/Turkiye_Kat_Ort_Belg_2001.pdf adresinden erişildi.

¹⁹⁰ 20 Mayıs 2011 tarihinde http://www.abgs.gov.tr/files/AB_Iliskileri/AdaylikSureci/Kob/Turkiye_Kat_Ort_Belg_2003.pdf adresinden erişildi.

¹⁹¹ 20 Mayıs 2011 tarihinde http://www.abgs.gov.tr/files/AB_Iliskileri/AdaylikSureci/Kob/Turkiye_Kat_Ort_Belg_2006.pdf adresinden erişildi.

¹⁹² 20 Mayıs 2011 tarihinde http://www.abgs.gov.tr/files/AB_Iliskileri/AdaylikSureci/Kob/Turkiye_Kat_Ort_Belg_2007.pdf adresinden erişildi.

¹⁹³ Şimşek, 2001.

Kişisel Verilerin Korunması Türkiye'nin gündemine 1981 yılında imzalanan "Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşme" ile girmiştir¹⁹⁴. Ancak ilginçtir ki, imza tarihinden itibaren bu yana Türkiye Sözleşmeyi onaylamadığı gibi, veri korunmasına ilişkin herhangi bir yasal düzenleme de yapmamıştır.

Adalet Bakanlığı'nda, kişisel verilerin korunmasına ilişkin çalışmalar ilk olarak 1988 yılında başlamış ve halen devam etmektedir. Bu süreçte, 2003 yılında kişisel veriler ile ilgili kanun çalışmalarının yapılması için bir komisyon oluşturulmuş ve burada hazırlanan "Kişisel Verilerin Korunması Kanun Tasarısı" 2005 tarihinde Başbakanlığa sevk edilmiştir. Tasarı, Adalet Bakanlığı tarafından son olarak 2007'de yenilenmiş ve Başbakanlığa gönderilmiş ve 2008 tarihinde de Meclise sevk edilmiştir. Avrupa Birliği Uyum Komisyonu tasarı hakkındaki raporunu 2009 tarihinde tamamlamış olup Tasarı şu anda Adalet Komisyonundadır¹⁹⁵.

3.2. Kişisel Verilerin Korunması Kanun Tasarısının Hükümleri

Kişisel verilerin korunması, çağımızda insan hakları kavramı ve korunması bilincinin gelişmesine paralel olarak önemi artmış bir konudur. Kişisel Verilerin Korunması Hakkında Kanun Tasarısı; kişisel verilerin yasal ve dürüst bir şekilde toplanması ve işlenmesi, belirli ve meşru amaçlar için güncelleştirilmesi ve kullanım amacına uygun bir süre için muhafaza edilmesi, verilerin amaca aykırı olarak paylaşılmaması, veri sahibi kişinin hakkındaki verileri öğrenme, değiştirme ve gerekirse silme haklarını düzenlemektedir.

Tasarı, kişisel verilerin korunması bakımından gerekli olan tüm hususlarda ilkeler belirlemekte ve öngördüğü Bağımsız Kurul ile de bu ilkelerin uygulanmasını sağlamaktadır. Avrupa Birliği ile müzakere sürecinde olan ülkemizin, kişisel verilerin korunması konusunda yaptığı çalışmalarda Avrupalı Devletlerin hassasiyetini ve bakış açısını paylaşması, ülkemiz için faydalı olacaktır. Bu kapsamda Tasarıda kamu kurum

¹⁹⁴ 20 Mayıs 2011 tarihinde <http://www.avrupakonseyi.org.tr/> adresinden erişildi.

¹⁹⁵ Kalaycı, Tahir Emre, "Haberleşme Özgürlüğü ve Kişisel Verilerin Korunması" EMO İzmir Şubesi, 2008, 20 Mayıs 2011 tarihinde http://yzgrafik.ege.edu.tr/~tekrei/dosyalar/yayinlar/200807_Emre.pdf adresinden erişildi; Ersoy, 2006.

kuruluşları ile özel hukuk tüzel kişileri ve gerçek kişiler arasında ayrıma gidilmesini olumludur. Ancak bu ayrımda kamu kurum ve kuruluşlarının özel hukuk kişilerine oranla kişisel verilerin korunması konusunda daha sıkı bir takım koşullara tabi olmalıdır. Halbuki Tasarıda, tam aksine bir durum sergilenecek kamu kurum ve kuruluşları lehine istisnalar tanınmıştır¹⁹⁶. Bu istisnalar, Kişisel Verileri Koruma Kurumunun yaptırım gücünü, bu kuruluşlar lehine azaltmakta ve Kurumun kamu kurum ve kuruluşlarına karşı olan yaptırım gücü istişari danışma organı düzeyine inmektedir. Öte yandan bu durum aynı zamanda, kişisel verilerin korunmasıyla ilgili durumları düzenlemek ve mevzuatı uygulamakla görevli, idari ve mali yönden özerk bir kurum yaratma düşüncesiyle de gelişmektedir.

Tasarı hükümleri, kamu kurum ve kuruluşları tarafından, kendi sahalarında kişisel verilerin korunması ile ilgili ihtiyacın hemen tespit edilebilmesini sağlayacak şekilde hazırlanmıştır. Bu nedenle, tasarı kanunlaştıktan sonra, örneğin sağlık alanında Sağlık Bakanlığının, iletişim ve ulaşım alanında Ulaştırma Bakanlığının, yargı ile ilgili olarak Adalet Bakanlığının, vakit kaybetmeden bu Kanuna uygun mevzuatı hazırlamaları gerekmektedir. Ancak bu düzenlemeler yapılırken, Tasarıda belirlenen ilkelerin dikkate alınması gerekmektedir.

Kişisel verilerin elektronik olarak işlenmesi, kişilere olduğu kadar özel ve kamu sektörüne de büyük yararlar sağlamaktadır. Bu şekilde mal ve hizmetler, daha kolay üretilebildiği gibi kişilerin veri işleme yoluyla tespit edilmiş tercihlerine bakılarak, bireylere ucuz ve süratle sunulabilmektedir. Elektronik veri işleme sistemleri keza, sağlık, sosyal güvenlik, eğitim, vergi, kamu düzeni ve güvenliği gibi alanlarda da benzer yararlar sağlamaktadır.

Tasarı, kişisel verileri işleme tabi tutulan kişiler ile bu verileri işleme tabi tutan kamu kurum ve kuruluşları ile gerçek ve tüzel kişilerini kapsamına almıştır. Tasarı, bu iki grubun çıkarlarını koruyarak dengelemek ve kişilik hakları ile temel hak ve hürriyetleri korumak amacıyla hazırlanmıştır.

¹⁹⁶ Kişisel Verilerin Korunması Kanun Tasarısı Hakkında Türkiye Bilişim Vakfı Görüşü, 20 Mayıs 2011 tarihinde <http://www.tbv.org.tr/TBV/Documents/BTHukuku/KisiselVerilerinKorunmasiKanunTasarisi-TBVGorus.pdf> adresinden erişildi.

Tasarı, beş kısımdan oluşmaktadır.

Birinci kısımda; Tasarının amaç ve kapsamı belirlenmiş ve Tasarıda kullanılan terimlerin tanımları yapılmış, kişisel verilerin niteliğine ilişkin ilkeler, kişisel verilerin işlenmesinde hukuka uygunluk sebepleri, özel niteliği olan kişisel veriler ve kişisel verilerin kamu kurum ve kuruluşları tarafından işlenmesi konuları düzenlenmiştir.

İkinci kısımda; veri konusu kişinin bilgilendirilmesi, bilgiye erişme hakkı, veri konusu kişinin itiraz hakkı, kişisel verilerin işlenmesinde tedbirler, kişisel verilerin yabancı ülkelere ve üçüncü kişilere aktarılması düzenlenmiştir.

Üçüncü kısımda; sicil ve Kurula bildirim ve ön inceleme konuları ile özel denetim kuruluşları, istisna getiren hükümler, mesleki davranış kuralları, kişisel verilerin silinmesi ve yok edilmesi konuları düzenlenmiştir.

Dördüncü kısımda; Kişisel Verileri Koruma Kurulunun oluşumu ile Kurulun yetki ve görevleri düzenlenmiştir.

Beşinci kısımda ise çeşitli hükümler düzenlenmiştir.

4. Kişisel Verilerin Korunması Kanun Tasarısının Maddelerinin Değerlendirilmesi

4.1. Amaç, Kapsam ve Tanımlar

Tasarının amacı, kişisel verilerin işlenmesini disiplin altına almak ve Anayasada yer alan kişinin dokunulmazlığı, maddi ve manevi varlığını korumaktır. Buradan hareketle, tasarının bireylerin temel hak ve özgürlüklerini korumak amacıyla hazırlandığı söylenebilir.

2. maddeyle gerçek ve tüzel kişiler Tasarı kapsamına alınmıştır. Tasarı, özel sektör ile kamu sektörü bakımından getirilen özel hükümler dışında ayırım yapılmadığından, öngörülen usul ve esaslar her iki sektöre de uygulanacaktır. Ancak kişisel verilerin gerçek kişiler tarafından sadece kişisel veya birlikte oturanlarla ilgili faaliyetlerine ilişkin olarak işlenmesi halinde Tasarı hükümleri uygulanmayacaktır¹⁹⁷. Burada, Tasarının 1995/46 sayılı Direktiften ayrılan yanı tüzel kişilere ait verilerin de koruma kapsamına alınmasıdır.

¹⁹⁷ 20 Mayıs 2011 tarihinde <http://www2.tbmm.gov.tr/d23/1/1-0576.pdf> adresinden erişildi.

Tasarıdaki tanımların, 1995/46 sayılı Direktifle paralel olduğu söylenebilir. Örneğin kişisel veri; “Belirli veya kimliği belirlenebilir gerçek ve tüzel kişilere ilişkin bütün bilgiler”, kişisel verileri işleyen; “Veri kütüğü sahibi adına, bu verileri işleyen gerçek ve tüzel kişiler”, kişisel verilerin işlenmesi eylemi; “Kişisel verilerin otomatik olan veya olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, değiştirilmesi, silinmesi veya yok edilmesi, yeniden düzenlenmesi, açıklanması veya başka bir şekilde elde edilebilir hale getirilmesi, üçüncü kişilere aktarılması, kullanılmasının sınırlanması amacıyla işaretlenmesi veya tasniflenmesi veya kullanılmasının engellenmesi gibi bu veriler üzerinde gerçekleştirilen bir işlem ya da işlemler bütünü”, olarak tanımlanmıştır.

Tasarıda veri kütüğü; “Gerçek ve tüzel kişilere ilişkin belirli bir kritere göre kişisel verilere ulaşımı kolaylaştıracak şekilde yapılandırılmış herhangi bir kişisel veri grubu”, veri kütüğü sahibi ise; “Kişisel verilerin işlenmesinin amaç ve metotlarını tek başına veya başkaları ile birlikte belirleyen gerçek ve tüzel kişiler” olarak tanımlanmıştır. Veri kütüğü ve veri kütüğü sahiplerinin Tasarının uygulanması açısından önemli aktörler olduğu söylenebilir.

Tasarı kapsamına giren kişisel veriler, sadece bireyin adı, soyadı, doğum tarihi ve doğum yeri gibi onun kesin teşhisini sağlayan bilgiler değil, aynı zamanda kişinin aklı, psikolojik, fizikî, kültürel, ekonomik, sosyal vb. özelliklerine ilişkin verilerdir. Bir kişinin belirli veya belirlenebilir olması, mevcut verilerin herhangi bir şekilde bir gerçek kişiyle ilişkilendirilmesi suretiyle, o kişinin tanımlanabilir hale getirilmesini ifade eder. Yani verilerin; kişinin fiziksel, ekonomik, kültürel, sosyal veya psikolojik kimliğini ifade eden somut bir içerik taşıması veya kimlik, vergi, sigorta numarası gibi herhangi bir kayıtlı ilişkilendirilmesi sonucunda kişinin belirlenmesini sağlayan tüm halleri kapsar¹⁹⁸. İsim, telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, genetik bilgiler gibi veriler dolaylı da olsa kişiyi belirlenebilir kılabilecek özellikleri nedeniyle kişisel verilerdir.

¹⁹⁸ 20 Mayıs 2011 tarihinde <http://www2.tbmm.gov.tr/d23/1/1-0576.pdf> adresinden erişildi.

4.2. Kişisel Verilerin İşlenmesi

Kamu kurum ve kuruluşlarının kişisel verileri işleyebilmesi, ancak kanunlarda öngörülen hallerle sınırlandırılmıştır. (m.4) 4. madde, Ceza Kanununda bulunan kanunilik ilkesi gibi düşünülebilir¹⁹⁹. Çünkü, ancak kanunla belirlenmişse kişisel veriler işlenebilecektir. Başka bir ifadeyle, yürütmenin ikincil düzenlemeleriyle verilerin işlenmesi mümkün değildir. Bu hükümle, bireylerin özel hayatlarının korunması ve verilerin işlenmesinde keyfiliğin önüne geçilebilmesi hedeflenmiştir.

5. maddenin birinci fıkrası, kişisel verilerin işlenmesine ilişkin temel ilkeleri düzenleyen en önemli hükümdür. Kişisel Verilerin Otomatik İşleme Tâbi Tutulması Karşısında Bireylerin Korunmasına İlişkin 108 sayılı Sözleşmenin 5 inci maddesine göre, Sözleşmeyi onaylayan devletlerin söz konusu temel ilkeleri iç hukuklarında yaşama geçirmek yükümlülüğü bulunmaktadır. Bu fıkra da belirlenen ilkeler, diğer maddelerde sözü geçen bütün veri işlemlerinde dikkate alınacaktır²⁰⁰. Bu maddeyle bu ilkeler hayata geçirilmiştir.

5. maddenin ikinci fıkrasında kişisel bu ilkelere bir istisna getirilmiştir. Buna göre; tarihî, istatistikî veya bilimsel amaçlarla kişisel verilerin, ilgili mevzuatta yeniden işleme amacına yönelik yeterli koruma tedbirleri getiren düzenlemenin bulunması veya kişisel verileri kontrol eden tarafından bu yönde gerekli tedbirlerin alınması şartıyla yeniden işlenebilecek veya işleme amacı için öngörülen süreden daha uzun bir süre saklanabilecektir.

4.3. Hukuka Uygunluk Sebepleri

6. maddede verilerin işlenmesinde hukuka uygunluk sebepleri belirtilmiştir. Kural olarak kişisel verilerin ilgili kişinin açık rızası ve maddede sayılan istisnalar dışında işlenmesi yasaktır. 1995/46 sayılı Avrupa Birliği Direktifinin ikinci maddesinde bendinde rızanın tanımı yapılmıştır. Buna göre rıza beyanı, ilgili kişinin kendisiyle ilgili veri işlenmesi fiiline, özgürce ve konuyla ilgili yeterli bilgi sahibi olarak verdiği ve sadece o işlemle sınırlı onay beyanıdır. Yine Direktifin 7 nci maddesine göre rıza, ilgili kişi tarafından “tereddüte yer bırakmayacak şekilde” verilmiş olmalıdır²⁰¹.

¹⁹⁹ Yüksel Civelek 2011, s.150.

²⁰⁰ 20 Mayıs 2011 tarihinde <http://www2.tbmm.gov.tr/d23/1/1-0576.pdf> adresinden erişildi.

²⁰¹ 20 Mayıs 2011 tarihinde <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML> adresinden erişildi.

6. maddeye göre kişisel verilerin işlenmesinde hukuka uygunluk sebepleri şunlardır:

- Kanunda öngörülen zorunluluklar dolayısıyla, kamu yararına veya resmi olarak verilmiş bir görevin yerine getirilmesi amacıyla veri işlenebilir.

- Kişisel verilerin, ilgili kişinin rızasını açıklayamayacak durumda olması hâlinde kendisinin veya başkasının hayatını veya beden bütünlüğünü korumak amacıyla veri işlenebilir.

- Bir sözleşmenin kurulması ve ifasıyla doğrudan doğruya ilgili olması kaydıyla veri işlenebilir.

- İlgili kişiler tarafından açıklanmış olması veya açık sicillerde mevcut bilgiler olması sebebiyle herkesçe bilinen veriler işlenebilir.

- Veri kütüğü sahibinin kendi haklı çıkarları için, ilgili kişinin temel hak ve özgürlükleri ile meşru çıkarlarına zarar vermediği sürece, veri işleminin zorunlu olması durumunda kişisel veriler işlenebilir.

Tasarının 7. maddesinde özel niteliği olan kişisel veriler sayılmakta ve genel kural olarak bu verilerin işlenemeyeceği düzenlenmektedir. Başka bir ifadeyle, bu maddede hassas verilerin işlenmesi kesin olarak yasaklanmış bulunmaktadır.

Buna göre kişilerin ırk, siyasi düşünce, felsefi inanç, din, mezhep veya diğer inançları, dernek, vakıf veya sendika üyeliği, sağlık ve özel yaşamları ve her türlü mahkûmiyetleri ile ilgili veriler özel niteliği olan kişisel veri olarak kabul edilmektedir. Bu veriler, başkalarının öğrenilmeleri halinde özellikleri gereği ilgili kişinin mağduriyetine yol açabilecek ve ayrımcılık tehlikesini oluşturacak nitelikte hassas verilerdir²⁰².

7. maddede hassas verilerin kesin olarak işlemeyeceği ifade edilmişken bir sonraki fıkrada yasağın istisnalarını düzenlemiştir. Başka bir ifadeyle hassas verilerin işlenebileceği hukuka uygunluk nedenleri sayılmıştır. Ancak bu durumda da özel hayatın ve aile hayatının gizliğinin korunması şartı bulunmaktadır. Hassas verilerin dahi işlenebildiği istisnai durumlardan birisi; kanunla yasaklanmayan hallerde kişinin yazılı rızasının alınmasıdır. 1995/46 sayılı AB Direktifinde ise kişinin açık rızası aranmaktadır.

Hukukî veya fiilî nedenlerle rızasını açıklayamayacak durumda bulunan bir kişinin kendisinin veya bir başkasının hayatı veya beden bütünlüğünün devamı için veri işleminin zorunlu olması, diğer bir istisnadır.

²⁰² Wong, 2007, s. 1.

Yine, vakıf, dernek, sendika ve siyasi partiler faaliyetlerini yerine getirebilmelerini sağlamak amacıyla hassas verileri işleyebilirler. Ancak bunlar, kuruluş amaçlarına ve tâbi oldukları mevzuata uygun ve faaliyet alanlarıyla sınırlı olmak şartıyla, üye ve mensuplarına yönelik ve ilgili kişinin rızası olmadan üçüncü kişilere açıklanmamak kaydıyla veri işleyebilirler.

Ayrıca ilgili kişi tarafından alenen açıklanmış olan veriler, yargılama faaliyetleri çerçevesinde bir hakkın korunması ve kullanılması için veri işlemenin zorunlu olması halleri de, maddenin diğer istisnalarındandır.

7. maddede, sayılan istisnalara ek olarak Kişisel Verileri Koruma Kuruluna, temel kamu yararlarının gerektirmesi hâlinde, özel hayatın ve aile hayatının gizliliğine dokunmamak şartıyla ve ilgili mevzuatta yeterli koruma tedbiri bulunması kaydıyla, özel niteliği olan kişisel verilerin işlenmesine karar verme yetkisi verilmektedir.

Son olarak, suçun soruşturma ve kovuşturmasına ilişkin özel nitelikteki kişisel veriler, ilgili kanunlarda yeterli koruma tedbiri bulunması kaydıyla, yetkili mercilerin kontrolü altında işlenebilecektir. Ancak, ceza mahkûmiyetlerine ilişkin sicil sadece Adalet Bakanlığının kontrolü altında tutulabilir.

7. maddede hassas verilerin işlenemeyeceği belirtildikten sonra istisnalar düzenlenmiştir. Ancak, istisnalara bakıldığında (10 farklı başlık) bunların istisna teriminin anlamını zorlayacak bir kapsamda olduğu söylenebilir. Kanımızca, hassas verilerin korunması açısından bu istisnaların azaltılması gerekir.

4.4. Kişisel Verilerin Üçüncü Kişilere Aktarılması ve Anonim Hale Getirilmesi

Kural olarak Tasarının 8. maddesinde belirtilen durumlar dışında kişisel veriler üçüncü kişilere aktarılamaz. Ancak bu kuralın istisnası maddede bentler halinde sayılmıştır.

Örneğin, birinci fıkranın (a) bendine göre, aktarma talebinde bulunan gerçek ve tüzel kişilerin belirli bir olayda kanundan doğan görevini yerine getirmesi için bu bilgiye ihtiyaç duyması halinde kişisel veriler, üçüncü kişiye aktarılabilir. Yine, Tasarının 6 ncı maddesinin üçüncü fıkrasında sayılan hâllerin yani hukuka uygunluk sebeplerinin varlığı halinde kişisel verilerin üçüncü kişiye aktarılacağı düzenlenmiştir.

8. maddenin üçüncü fıkrasında kamu kurum veya kuruluşlarının kamu yararı, sır saklama yükümlülüğü, ilgili kişinin meşru menfaati veya kişisel verilere ilişkin özel koruma kurallarının varlığından bahisle kişisel verilerin, üçüncü kişilere aktarılmasını reddetmesini, sınırlamasını veya şarta bağlamasını mümkün kılan bir düzenleme getirilmiştir. Bu halde Kurul, fıkrada belirtilen hallerin varlığını değerlendirecektir²⁰³. Maddenin son fıkrasına göre; kamu kurum veya kuruluşlarının görev alanlarıyla ilgili konularda yapacakları talep üzerine, gizlilik esaslarına göre görev yapan personelin bilgileri hariç olmak üzere, kişilerin nüfus kayıt örnekleri ve adresleri bildirilebilecektir.

Tasarının 9. maddesine göre; ihtiyaç duyulmayan kişisel veriler, koruma tedbiri veya ispat amacıyla muhafazasının gerekli olmadığı durumlarda, anonim hâle getirilir veya yok edilir. Kişisel verilerin, araştırma, planlama ve istatistik gibi kamuya yönelik amaçlarla kullanılabilmesi için anonim hale getirilmesi şartı vardır. Bu suretle elde edilen veriler üçüncü kişilere aktarılabilir veya yayımlanabilir (m.10).

4.5. İlgili kişinin Hakları ve Yurtdışına Veri Aktarımı

Tasarının 11 ile 14 üncü maddelerinde verileri işlenen kişinin hakları ve yurtdışına veri aktarımı konuları düzenlenmiştir.

4.5.1. Aydınlatma Yükümlülüğü

Kişisel verileri işleyen kurumların aydınlatma yükümlülüğü ile kişisel verileri işlenen kişilerin hakları, Tasarının 11 inci ve 12 inci maddelerinde yer almaktadır. 11. maddeyle, 1995/46 sayılı AB Veri Koruma Direktifinin 10 uncu maddesi düzenlemesi esas alınmak suretiyle, kişisel verilerin elde edilmesinde veri kütüğü sahibinin aydınlatma yükümlülüğü düzenlenmiştir. Bu maddeyle, kişisel verileri işleyen veri kütüğü sahibi; kendisinin veya varsa temsilcisinin kimliği, işleme amacı, verilerin kimlere aktarılacağı, veri toplamanın yöntemi, hukuki sebebi ve muhtemel sonuçları hakkında ilgili kişiyi bilgilendirir. Ayrıca verilerin daha sonraki kullanımları hakkında da ilgili kişiye bilgi verilmeli, böyle bir kullanıma izin verip vermeyeceği konusunda iradesi alınmalıdır. Yine eğer veri kütüğü sahibi, kişisel verileri daha sonraki bir zamanda, elindeki mevcut verileri elde ettiği esnada

²⁰³ 24 Mayıs 2011 tarihinde <http://www2.tbmm.gov.tr/d23/1/1-0576.pdf> adresinden erişildi.

belirtmediği bir amaç için kullanacaksa, bununla ilgili olarak ilgili kişiye bilgi vermeli ve bu konudaki rızasını almalıdır. Bu sayede veri kütüğü sistemi sahibi veri korumasında önemli ölçütler olan şeffaflık ve ilgili kişinin açık rızasını elde etmeyi gerçekleştirmiş olacaktır²⁰⁴.

4.5.2. İlgili Kişinin Hakları

12. maddeyle, ilgili kişinin hakları düzenlenmiştir. İlgili kişi kendisiyle ilgili kişisel veri kaydedilip kaydedilmediğini öğrenme, bunları isteme, verinin muhtevasının eksik veya gerçeğe aykırı olması hallerinde bunların düzeltilmesini, hukuka aykırı olması halinde silinmesini, yok edilmesini veya aktarımının engellenmesini isteme hakkına sahiptir. İlgili kişi aynı zamanda talebi doğrultusunda yapılan işlemlerin, verilerin açıklandığı üçüncü kişilere bildirilmesini isteme hakkına sahiptir²⁰⁵. Ancak bu haklar; milli güvenliğin korunması, milli savunmanın gerçekleştirilmesi, suçun önlenmesi veya istihbarat amacıyla yapılan faaliyetlerle ilgili olarak kanundan doğan bir görevin yerine getirilmesi veya ceza soruşturması veya kovuşturmasına zarar verilmesinin engellenmesi gerekçesiyle sınırlandırılabilir.

Yine aynı maddeye göre; veri kütüğü sahibi verilerin muhtevasının eksik veya gerçeğe aykırı olması hallerinde düzeltmekle, hukuka aykırı olması halinde silmek, yok etmek veya ilgili kişi hakkında veri işlemlerini durdurmak ve üçüncü kişilere aktarımını engellemekle yükümlü olacaktır. Verilerin yok edilmesi, otomatik olmayan yollarla veri işlenmesi halinde ilgili evrakların imhası, otomatik yollarla veri işlenmesi halinde verilerin veya ilgili kişiyle doğrudan ilişkilendirilmeyi sağlayacak bilgilerin kayıtlı olduğu CD, disket, USB disk, hard disk gibi araçlardan silinmesi veya diğerlerinden ayrıştırılarak yok edilmesi şeklinde gerçekleştirilecektir²⁰⁶.

İlgili kişilerin haklarını kullanabilmeleri için öngörülen başvuru usulü 13. maddede düzenlenmiştir. Başvurular, yazılı olarak yapılacak, veri kütüğü sahibi talep hakkında başvuru tarihinden itibaren onbeş iş günü içinde cevap vermekle yükümlü olacaktır. İlgili kişinin talebine cevap verilmediği,

²⁰⁴ 24 Mayıs 2011 tarihinde <http://www2.tbmm.gov.tr/d23/1/1-0576.pdf> adresinden erişildi.

²⁰⁵ 24 Mayıs 2011 tarihinde <http://www2.tbmm.gov.tr/d23/1/1-0576.pdf> adresinden erişildi.

²⁰⁶ 24 Mayıs 2011 tarihinde <http://www2.tbmm.gov.tr/d23/1/1-0576.pdf> adresinden erişildi.

cevabın olumsuz olduğu veya yeterli olmadığı durumlarda yirmi gün içinde Kişisel Verileri Koruma Kuruluna itiraz edilebilecektir.

4.5.3. Yurt Dışına Veri Aktarımı

14. maddeyle, 1995/46 sayılı AB Direktifinin 25 ve 26 ncı maddeleri dikkate alınarak, kişisel verilerin yurtdışına aktarımı düzenlenmiştir. Kural olarak, kişisel verilerin Türkiye dışındaki bir ülkeye aktarılabilmesi için yabancı ülkede de, ülkemizdekine eşdeğer ve etkin bir korumanın bulunması gerekir. Veri kütüğü sahipleri, ilgili ülkede yeterli düzeyde koruma olup olmadığını kontrol etmek zorundadır. Bu değerlendirme, işleme konu verinin niteliği, veri işlemenin amacı ve işleme süresi, verinin aktarıldığı ülkenin konuyla ilgili genel ve özel düzenlemeleri ile uygulanan güvenlik tedbirleri dikkate alınarak yapılacaktır²⁰⁷.

Türkiye dışındaki bir ülkeye aktarılabilmesi için yabancı ülkede de, ülkemizdekine eşdeğer ve etkin bir korumanın bulunması gerekir ise de bu kuralın bazı istisnaları bulunmaktadır. Buna göre; ilgili kişinin açık rızasının bulunması, ilgili kişi ile veri kütüğü sahibi arasında bir sözleşme ilişkisinin bulunması, suçun önlenmesi veya yargılama faaliyeti için gerekli olması, veri konusu kişinin hayatı veya beden bütünlüğünün idamesi için aktarımın zorunlu olması ve aktarımın kamuya açık bulunan sicillerden yapılması halinde, yabancı ülkede eşdeğer ve etkin bir koruma olmasa dahi kişisel verilerin aktarılması mümkün olacaktır.

4.5.4. Kişisel Verilerin İşlenmesine İlişkin Güvenlik Tedbirleri

15. maddeyle 108 sayılı Sözleşmenin 7 nci ve Direktifin 17 nci maddesine uygun olarak kişisel verilerin işlenmesinde alınacak teknik ve idarî tedbirler düzenlenmiştir. Maddede kişisel verileri kontrol edenlerin ve onlar adına işleyenlerin, kişisel verilerin işlenmesinde uygun teknik ve idari tedbirleri almak zorunda oldukları belirtilmiştir. Bu tedbirler, teknolojinin ulaştığı en üst düzey ve uygulanma maliyeti de dikkate alınarak, korunacak verinin niteliğine ve işlenmeden kaynaklanabilecek risklere karşı uygun bir güvenlik seviyesinde olmalıdır.

²⁰⁷ 24 Mayıs 2011 tarihinde <http://www2.tbmm.gov.tr/d23/1/1-0576.pdf> adresinden erişildi.

5. Veri Kütüğü Sicili

16. maddeyle, Kişisel Verileri Koruma Kurulu tarafından, kişisel veri işleyen veri kütüğü sahiplerinin tescil edileceği bir sicil oluşturulması öngörülmektedir. Kişisel veri işleyen gerçek kişiler ile kamu ve özel hukuk tüzel kişileri, veri kütüğünü kurmadan önce bu Sicile kaydolmak zorundadırlar. Sicil, aleniyet ilkesi gereği kamuya açık tutulur.

Kişisel verileri işleyenler sicile kayıt başvurusu yaparken; veri kütüğü sahibi veya varsa temsilcisinin kimlik ve adres bilgileri, kişisel veri işlemenin amaçları, veri konusu kişi grubu ve grupları ile bu kişilere ait veri kategorileri hakkındaki açıklamalar, verilerin açıklanabileceği alıcılar veya alıcı grupları, üçüncü ülkelere aktarımı öngörülen veriler, alınan güvenlik tedbirlerine ilişkin genel açıklamaları içeren bildirimde bulunmak zorundadır.

Ancak, bazı durumlarda bildirim zorunluluğu bulunmamaktadır. Kişilerin temel hak ve özgürlüklerini olumsuz yönde etkilemeyecek nitelikte veri işlenmesi, veri işlemenin kamuya bilgi verilmesi amacıyla tutulan ve yasal çıkarı bulunan herkesin incelemesine açık bir sicil için yapılması, hallerinde sicile bildirim yapılmayabilir. (m.18)

6. İstisnalar

22. maddede, AB Veri Koruma Direktifinin 13 üncü maddesi göz önüne alınarak genel kurallara getirilen istisnalara bentler halinde yer verilmiştir. Maddeye göre; birinci fıkrada bentler halinde sayılan durumlarda Tasarının; hukuka uygunluk sebepleri, aydınlatma yükümlülüğü, Veri Kütüğü Sicili, Sicile kayıt ve ön inceleme konularıyla ilgili maddeleri uygulanmayacaktır. Başka bir ifadeyle, aşağıda belirtilen durumlarda, Tasarının 6, 11, 16, 17 ve 19 uncu maddeleri uygulanmayacaktır.

Milli güvenliğin korunması, milli savunmanın gerçekleştirilmesi veya bu amaçla yapılan istihbari faaliyetlerin yürütülmesi, kamu düzeninin korunması, suçun önlenmesi, soruşturulması veya kovuşturulması, bütçe, vergi ve malî konulara ilişkin olarak Devletin önemli ekonomik veya malî çıkarları ve bu konularda, resmî mercilerin izleme, denetleme veya düzenleme görevlerinin gerektirmesi istisnai durumlardır. Ayrıca yine kişisel verileri işlenen kişiler, ilgili mevzuatta yeterli koruma tedbiri bulunması

kaydıyla, bilimsel araştırma veya istatistik oluşturma amaçları ile sınırlanabilecektir. (m.22)

7. Gazetecilik Amacıyla Veri İşlenmesi ve Mesleki Davranış Kuralları

Gazetecilik amacıyla kişisel verilerin işlenmesinde, düşüncüyü açıklama ve yayma hürriyeti sınırları çerçevesinde yayın sahipleri veya temsilcileri ve bunların çalışanlarının bilgilenme ihtiyaçlarının karşılanması gerekli olması halinde hukuka uygun sayılır. (m.23)

24. maddede kişisel verilerin işlenmesi bakımından meslekî davranış kuralları düzenlenmiştir. Burada, AB Veri Koruma Direktifinin 27 nci maddesi göz önüne alınmış olup, değişik sektörlerde farklı özelliklere sahip mesleklere yönelik olarak, kişisel verilerin işlenmesi bakımından hazırlanan veya değiştirilen mesleki davranış kurallarına ilişkin düzenleme taslakları hakkında Kuruldan görüş alınması öngörülmüştür.

8. Kişisel Verilerin Silinmesi

25. madde ile artık ihtiyaç duyulmayan kişisel verilerin silinmesi veya yok edilmesi konusu düzenlenmiştir. Burada, silinme veya yok edilmenin hangi yöntemlerle gerçekleştirileceği konusunda Kurulca, her sektörün özellikleri göz önünde tutularak özel kuralları içerecek yönetmelik hazırlanacağı hükme bağlanmıştır.

9. Kişisel Verileri Koruma Kurulu

26. maddeyle, kişisel verileri kontrol edenleri denetlemek ve Kanunla verilen görevleri yapmak üzere Kişisel Verileri Koruma Kurulunun oluşturulması öngörülmüştür. Kurul yetkilerini bağımsız olarak kullanır ve hiçbir organ, makam, merci Kurula emir ve talimat veremez. Kuşkusuz bu Kurulun bağımsızlığını sağlayacak önemli kuraldır. Ancak, Kurul'un idari ve mali özerkliği olmadığından bunun ne oranda gerçekleşeceği kanımızca tartışmalıdır. Yine Kurulun ayrı bir sekretaryasının olmaması ve bunun Başbakanlık tarafından yürütülmesi bağımsızlığı zedeleyen diğer bir unsurdur. (m.30)

108 sayılı Sözleşmenin 4 üncü maddesi, her devletin Sözleşmede öngörülen ilkeleri iç hukuklarında yaşama geçirmesini zorunlu kılmıştır. Sözleşmeyi onaylayan devletler bu amaçla birer kurumsal yapı

oluşturmuşlardır. Aynı şekilde 1995/46 sayılı AB Direktifinin 28 inci maddesinde üye devletlerin, kişisel verilerin işlenmesine ilişkin ilkelerin uygulanmasını izlemek ve yönlendirmek üzere kamu kuruluşunu görevlendirmeleri gereğine işaret edilmiştir. Avrupa Birliği üyesi ülkelerin tümünün, bu alanda yasama veya yürütme organlarına karşı bağımsız bir şekilde görev yapacak kurullar oluşturmuştur²⁰⁸. Almanya'da, Federal Verileri Koruma Görevlisi, Avusturya'da Verilerin Korunması Komisyonu, İsveç'te Verileri Denetim Kurulu, Fransa'da Enformatik ve Özgürlükler Milli Komitesi örnek olarak verilebilir.

27. maddede Kurulun oluşum biçimi, Kurul üyeliklerine seçileceklerde aranan nitelikler belirtilmiştir. Buna göre Kurul; Bakanlar Kurulu tarafından seçilen 7 üyeden oluşmaktadır. Üyeler, kamu veya özel sektörde 10 yıl görev yapan veya üniversitelerde 10 yıl öğretim üyeliği yapmış kişilerden oluşur. Kurul başkanı Bakanlar Kurulu tarafından, başkan vekili ise üyeler tarafından salt çoğunlukla seçilir.

Kişisel Verileri Koruma Kurulu, Kanunda öngörülen hükümlerin, kişisel veri sicillerini kontrol eden kamu kurum veya kuruluşlarınca uygulanmasını izleyip denetleyecek, ayrıca kendiliğinden veya başvuru üzerine herhangi bir konuyu inceleyerek açıklığa kavuşturacaktır. İnceleme sonucunda kanun hükümlerinin ihlal edildiğinin anlaşılması halinde Kurul, sorumlulardan kişisel verilerin işlenme tarzında değişiklik yapılmasını veya işlemeyi sona erdirmesini ve gerekiyorsa silinmesini ya da yok edilmesini isteyecektir.

28 vd. maddelerde; Kurul üyelerinin görev süreleri, Kurulun çalışma esasları, Kurulun görev ve yetkileri, şikâyet başvurusunun usulü düzenlenmiştir. Kurul üyelerinin görev süresi 6 yıldır ve tekrar seçilmek mümkün değildir. Kanımızca, bu hüküm bağımsızlığı gerçekleştirmede önemli bir araçtır. Tekrar seçilme endişesi taşımayan üye kararlarında daha objektif olabilecektir. Yine Başkan ve üyelerin görevden alınamamaları da diğer bir güvencedir.

Tasarıyla kurulması düşünülen Kişisel Verileri Koruma Yüksek Kurulu gerek Kurul üyelerinin seçilmesinde ve atanmasında belirlenen usul, gerekse

²⁰⁸ 24 Mayıs 2011 tarihinde <http://www2.tbmm.gov.tr/d23/1/1-0576.pdf> adresinden erişildi.

de Kurulun sahip olduğu yetkiler göz önünde bulundurulduğunda Kurulun etkin, bağımsız ve tarafsız olmasını engeller niteliktedir. Aynı zamanda Başkan dışında Kurulun diğer üyelerinin Kurumdaki görevleriyle birlikte asıl görevlerini de sürdürmesi Kurulun bağımsız ve özerk yapısına ters düşen bir durumdur.

Tasarının 32. maddesine göre; ilgili kişiler Kurula şikâyet başvurusunda bulunabilirler. İlgili kişiler, şikâyet konusu işlemin yapıldığı veya öğrenildiği tarihten itibaren 60 gün içinde Kurula şikâyette bulunabileceklerdir. Kurul, şikâyeti 3 ay içinde karara bağlar. Ancak, hukuki veya fiili nedenlerle bir kez olmak üzere 3 ay uzatma kararı da verebilir. Maddede ayrıca, Kurulun şikâyetleri inceleme usulü ve bu inceleme neticesinde yapacağı işlemler ile veri kütüğü sahibinin Kurul incelemesi ile ilgili olarak yükümlülükleri de burada düzenlenmiştir.

10. Yapıtlımlar

108 sayılı Sözleşmenin 10 uncu maddesinde, Sözleşmeyi onaylayan devletlerin, Sözleşmede öngörülen ilkelerin gereken şekilde uygulanabilmesini sağlamak üzere, iç hukuklarında etkin yapıtlımlar öngörmeleri istenmiştir. Aynı şekilde, 1995/46 sayılı AB Direktifi'nin 11 inci Bölümünde, üye devletler, ilkelerin ihlâli halinde yapıtlımlar uygulamaya davet edilmiştir. Bu düzenlemeleri iç hukuklarına aktaran devletlerde kişilik hakları ihlalinin ağırlık derecesine göre, idari para cezası veya hürriyeti bağlayıcı cezalar verilmektedir. Benzer durum, Tasarının 34 vd. maddelerinde görülmektedir. Ancak, burada yeni suç ihdas edilmemekte, 5237 sayılı Türk Ceza Kanununun 135 ve devamı maddelerine atıf yapılmaktadır.

SONUÇ

Bilgi ve iletişim teknolojilerinde meydana gelen gelişmeler yüzyılımıza damgasını vurmuştur. Özellikle İnternetin yaygınlaşması dünyadaki iletişim ve veri paylaşımını oldukça kolaylaştırmıştır. Örneğin, Ortadoğu'da meydana gelen halk ayaklanmalarında sosyal ağların dolayısıyla İnternetin oldukça önemli bir etken olduğu ileri sürülmektedir²⁰⁹.

²⁰⁹ 24 Mayıs 2011 tarihinde <http://www.gennaration.com.tr/manset1/arap-bahari-halkin-ag-gucu/>; <http://www.kigem.com/content.asp?bodyID=5737> adreslerinden erişildi; Bu konuda bkz. Gelvin, James L. The Arab Uprising, Oxford University Press, 2012, New York.

Kişisel verilerin korunması, temel insan hak ve özgürlüklerinden olup insan onuru temeline dayandırılmaktadır. A.İ.H.S' nin 8. maddesi ile özel hayat ile kişinin onuru, isim ve resim hakkı gibi manevi değerleri güvence altına alınmıştır.

Küreselleşen dünyada, veri paylaşımı da artık küresel boyutlardadır. Bu nedenle ülkeler yaptıkları uluslararası Sözleşmelerle verileri güvenli bir şekilde paylaşabilmenin yollarını aramaktadırlar. BM, OECD, Avrupa Konseyi ve AB bünyesinde yapılan çalışmalar bu kapsamda değerlendirilebilir.

Ülkemizde kişisel verilerin korunması, 2010 Anayasa değişikliği ile anayasal bir hak olarak düzenlenmiştir. Şüphesiz bu veri korumada çok önemli bir adımdır. Bu düzenleme, kişisel verilerin korunmasını temel bir hak olarak düzenleyen Avrupa Birliği Temel Hakları Şartıyla da uyumludur. Bugün artık kişisel verilerin korunması anayasal teminat altındadır.

Kişisel Verilerin Korunması Kanun Tasarısı, Avrupa Konseyince hazırlanan 108 sayılı Sözleşme ile AB Direktiflerine paralel bir şekilde hazırlanmıştır. Tasarı kişisel verilerin hukuka uygun olarak işlenmesinin çerçevesini belirlemekte, vatandaşlara konuyla ilgili çeşitli haklar vermektedir. Tasarının kanunlaşması, bu alandaki önemli bir boşluğu dolduracaktır. Yine tasarı, ulusal ve uluslararası alanda veri alışverişi ve veri korumada belirli bir standart sağlayacağından kişisel verilerin korunmasında önemli bir kilometre taşı olacak, bu durum da temel hak ve özgürlüklerin korunmasına ciddi katkılar sağlayacaktır.

Günümüzde kişisel veriler, devlet kadar ve özel sektör tarafından da işlenmektedir. Kamu veya özel sektör tarafından işlenen veriler, hukuka uygun olarak, belirli sürelerle, şeffaflık ilkesi çerçevesinde işlenmelidir. Kişiler, kendileriyle ilgili veri işlenip işlenmediğini öğrenebilmeli söz konusu bilgilerde eksiklik veya yanlışlık varsa düzeltebilmelidirler.

Bilgi ve iletişim teknolojilerinde yaşanan gelişmelerle, veri paylaşımının ülke sınırlarını aşması nedeniyle kişisel verilerin korunmasında uluslararası işbirliği hayati önemi haizdir. Bu nedenle, gerek uluslararası örgütler gerekse devletler bu konudaki çalışmalarını güncelleyerek ortak çalışmaya devam etmelidirler. Başka bir ifadeyle, veri korumada yeknesak bir hukuki koruma sistemi sağlanmalıdır.

Kişisel verilerin korunmasında temel ilkelerin uygulanmasını denetleyecek ve kişilerin şikâyetlerini inceleyecek veri koruma otoritesinin kurulması diğer önemli bir noktadır²¹⁰. Bu otoritenin görevini objektif bir şekilde yapabilmesi için idari ve mali özerklik olmalı ve üyeler için teminat getirilmelidir. Kişisel Verilerin Korunması Tasarısı incelendiğinde bu konuda problemlerin ortaya çıkabileceğini ileri sürmek kehanet olmayacaktır.

Kişisel Verilerin Korunması Tasarısında yer alan kişisel verilerin korunması hakkının yalnızca Anayasanın 17 nci maddesinde belirtilen kişinin dokunulmazlığı, maddi ve manevi varlığı hakkına dayandırıldığı görülmektedir. Oysa bu kavram kişinin dokunulmazlığı, maddi ve manevi varlığı hakkından daha çok özel hayatın gizliliği ile ilişkilidir. Bu nedenle, kanunun amacının belirlendiği madde özel hayatın gizliliğinin korunması hakkına vurgu yapılması suretiyle yeniden düzenlenmelidir.

Tasarıda yer alan “kamu yararının” kişisel verilerin işlenmesi için bir hukuka uygunluk nedeni olarak kabul edilmesi anayasaya aykırıdır. Çünkü, Anayasanın 13 üncü maddesine göre; temel hak ve hürriyetler ancak Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak sınırlanabilir. Anayasanın kişisel verilerin korunmasını düzenleyen 20 nci maddesine baktığımızda “kamu yararının” özel sınırlama nedeni olarak düzenlenmediğini görürüz. Dolayısıyla, kamu yararı ölçütünün anayasaya uygun olmadığı ileri sürülebilir. Bu itibarla, bunun tasarıdan çıkarılması yerinde olacaktır.

Yine Tasarıda yer alan, milli güvenlik, milli savunma, kamu düzeni gibi kavramlar herkesin anlamı üzerinde mutabık kaldığı terimler olmadığından bunların çerçevesinin uluslararası düzenlemelere de uygun olarak belirlenmesi önem arz etmektedir. İdarenin keyfi uygulamalarının önlenmesi ve özel hayatın gizliliğinin korunması açısından bu konu dikkatli bir şekilde düzenlenmelidir.

Ülkemizde, anayasa ve çeşitli kanunlardaki genel hükümlerle kişisel verilerin korunması ve gizliliğinin gereği gibi sağlanması mümkün değildir. Çünkü, bu kurallar bilgi teknolojilerindeki baş döndürücü gelişmeler karşısında kişilik haklarının korunmasında yetersiz kalmaktadır. Gerek özel

²¹⁰ Cate, 1998, s. 11.

hukuk gerekse de kamu hukuku açısından kişisel veriler için en iyi koruma yolunun konuya ilişkin özel bir kanuni düzenleme olduğu söylenebilir.

Kişisel Verilerin Korunması Kanun Tasarısının yasalaşması, Avrupa Birliği müzakere sürecinin gerekliliklerinden birisi olmasının yanı sıra 1981 yılında imzalanıp henüz onaylanmayan 108 sayılı Avrupa Konseyi Sözleşmesi açısından da hukuksal bir yükümlülüktür. Sonuç olarak, kişisel verilerin korunmasının Anayasada temel hak ve hürriyetler içinde düzenlenmesinin içinde yaşadığımız dijital çağ açısından oldukça önemli bir adım olduğu ifade edilebilir. Ancak, çıkarılacak kanunda veri koruma standartlarının modern demokratik ülkelerle paralel olmasının altı önemle çizilmelidir. Son olarak, bireyleri bilinçlendirmenin veri korumada en önemli unsurlardan birisi olduğu da unutulmamalıdır.

KAYNAKLAR

- Akıllıođlu, Tekin, “İdari Usul ve Kişisel Verilerin Korunması”, www.idare.gen.tr/akillioglu-idariusul.htm
- Arslan, Hilmiye, “Amerika İle Avrupa Birliđi Hukuki Düzenlemelerinin Gizlilik Haklarına Bakış Açısının Karşılaştırılması”, s.1, <http://inet-tr.org.tr/inetconf10/bildiri/18.doc>
- Atak, Songül. (2010). Avrupa Konseyinin Kişisel Veriler Açısından Sağladığı Güvenceler. *Türkiye Barolar Birliđi Dergisi*, Sayı 87.
- Avcı, Feyzullah (2006). *Ceza Yargılamasında Özel Hayatın Gizliliđi Hak Ve Hürriyetinin Hukuka Aykırı Olarak Elde Edilen Deliller Nedeniyle İhlali*, Selçuk Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı, Yayınlanmamış Yüksek Lisans Tezi, Konya.
- Avrupa Birliđi ve Türkiye, Başbakanlık Dış Ticaret Müsteşarlığı Avrupa Birliđi Genel Müdürlüğü, Dođuş Matbaacılık, Ankara, 2002.
- Başalp, Nilgün (2004). *Kişisel Verilerin Korunması ve Saklanması*, Ankara: Yetkin Yayınları.
- Bigname, Francesca, “Privacy and Law Enforcement in the European Union: The Data Retention Directive”, 2007
- Cate, Fred H (1998). Privacy and Telecommunications. *Wake Forest Law Review*, Volume, 33, Number, 1.
- Cate, Fred H. (2000). Principles of Internet Privacy. *Connecticut Law Review*, Vol. 32.
- Dođan, Yusuf Hakkı. “Özel Hayata Karşı İşlenen Suçlar”, <http://www.cezabb.adalet.gov.tr/makale/146.doc>
- Edwards, Lilian. (2004). The Problem with Privacy: A Modest Proposal, *International Review of Law Computers&Technology*, Volume 18, s.316; <http://epic.org/privacy/hew1973report/>
- Eralp, Özgür, “KPS (Kimlik Paylaşım Sistemi), AKS(Adres Kayıt Sistemi) Uygulamaları Işığında Bireysel Mahremiyet” <http://www.ozgureralp.av.tr/makaleler/tckimliktdb.htm>

- Ersoy, Eren “Gizlilik, Bireysel Haklar, Kişisel Verilerin Korunması”,
<http://ab.org.tr/ab06/bildiri/6.doc>
- Ersoy, Uğur. (2009). *Bir İnsan Hakkı Olarak, Kişisel Verilerin Korunması*
Gazi üniversitesi Sosyal Bilimler Enstitüsü Kamu yönetimi Anabilim
dalı Siyaset ve Sosyal Bilimler Bölüm Dalı, Yayınlanmamış Yüksek
Lisans Tezi, Ankara.
- Günaydın, Şerife. (2007). *İnsan Hakları Kapsamında Özel Hayatın Gizliliği*,
Çağ Üniversitesi Sosyal Bilimler Enstitüsü Genel Kamu Hukuku
anabilim Dalı Yayınlanmamış Yüksek Lisan Tezi, Adana.
- Gür, İkbâl. (2009). *Kişisel Verilerin Korunması Hususunda AB İle ABD
Arasında Çıkan Uyuşmazlıklar Ve Çözüm Yolları*, Ankara Üniversitesi
Sosyal Bilimler Enstitüsü Avrupa Toplulukları (Uluslararası İlişkiler)
Anabilimdalı, Yayınlanmamış Yüksek Lisans Tezi, Ankara.
- Helvacıoğlu Kuyucu, Aslı Deniz, “Avrupa Birliği’nde Kişisel Verilerin
Korunmasında Yeni Yaklaşım”,[http://www.bilgicagi.com/Yazilar/
4583avrupa_birliginde_kisisel_verilerin_korunmasinda_yeni_yaklasim.
aspx](http://www.bilgicagi.com/Yazilar/4583avrupa_birliginde_kisisel_verilerin_korunmasinda_yeni_yaklasim.aspx)
- İlkiz, Fikret, “Özel hayatın gizliliğinin ihlali”, 2007,
<http://bianet.org/bianet/bianet/98197-ozel-hayatin-gizliliğinin-ihlali>
- İlkiz, Fikret “Kişilik Hakları ve Medya”,
http://www.byegm.gov.tr/seminerler/mardin_viii/mardin_17.htm,
- Gelvin, James L. *The Arab Uprising*, Oxford University Press, 2012, New
York.
- Kaboğlu, İbrahim Ö. (1996). *Özgürlükler Hukuku, İnsan Haklarının
Hukuksal Yapısı Üzerine Bir Deneme*. İstanbul: Alfa Yayınları,
İstanbul.
- Kalaycı, Tahir Emre. (2008). *Haberleşme Özgürlüğü ve Kişisel Verilerin
Korunması*. EMO İzmir Şubesi, 2008
- Kaya, Cemil. (2005). *İdare Hukukunda Bilgi Edinme Hakkı*. Ankara: Seçkin
Yayınları.

- Kaya, Cemil (2011). Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi. *İÜHFM*, C. LXIX, S.1 - 2, s.317-334.
- Keser Berber, Leyla- Ünlü, Mahir M.- Er Cüneyd, Elektronik Sağlık Kayıtları ve Özel Hayatın Gizliliği, Karakter Color AŞ, İstanbul
- Kesmez, Necdet “Kişisel Verilerin Korunması Üzerine” Bilişim Şurası, http://bilisimsurasi.org.tr/listeler/tbs-hukuk/Mar/att-0044/01-K__SEL_VER_LER_N_KORUNMASI.doc
- Kleve Pieter and De Mulder Richard, “Privacy Protection and the right to information: in search of a new symbiosis in the information age”, Ed. Kierkegaard Sylvia Mercado, Ankara Bar Association Cyberlaw Security & Privacy, The Second International Conference on Legal, Security and Privacy Issues in Information Technology (LSPI) 2007, Beijing China.
- Korff, Douwe, EC Study On Implementation Of Data Protection Directive, 2002 <http://ssrn.com/abstract=1287667>.
- Millard, Christopher and Hon, W. Kuan, “Defining Personal Data in e-Social Science”, <http://ssrn.com/abstract=1809182>.
- Özbudun, Ergun. (1997). Anayasa Hukuku Bakımından Özel Haberleşmenin Gizliliği. *Ankara Hukuk Fakültesi Ellinci Yıl Armağanı*. Ankara: Sevinç Matbaası.
- Özdemir, Kenan, “Türk Hukukunda Ve Avrupa İnsan Hakları Sözleşmesi İle Avrupa İnsan Hakları Mahkemesi Kararlarında Özel Hayatın Gizliliği”, 2005 http://www.hukuki.net/hukuk/index.php?article=515#_ftnref62
- Öztan, Bilge. (2002). *Medeni Hukukun Temel Kavramları*. Ankara: Turhan Kitabevi.
- Pekşirin, Hülya, “Kişisel Verilerin Korunması Üzerine”, 2002 <http://bilisimsurasi.org.tr/listeler/tbs-hukuk/Feb/0026.html>
- Robinson, Neil, Graux, Hans, Botterman, Maarten, Valeri, Lorenzo “Review of the European Data Protection Directive”, Published by the RAND Corporation, United Kingdom, 2009,

- Sırabaşı, Volkan, “Kişisel Verilerin (Bilgilerin) Gizliliği ve Korunması”http://www.fenafil.com/hukuk/internet/kisisel_veriler.htm
- Solove, Daniel J. Hoofnagle -Chris Jay, “A Model Regime of Privacy Protection”, GWU Law School Public Law Research Paper No. 132 University of Illinois Law Review, Vol. 2, 2006
- Şimşek, Oğuz, “4422 sayılı Çıkar Amaçlı Suç Örgütleriyle Mücadele Kanunu ve Kanununun 4. Maddesine Göre "Kayıt ve Verilerin İncelenmesi" ve Kişisel Nitelikli Verilerin Korunması”, <http://web.deu.edu.tr/ab/MAKALE/deu%20MAK/0012.htm>
- Şimşek, Oğuz. (2008). Anayasa Hukukunda Kişisel Verilerin Korunması, İstanbul: Beta Yayınları.
- Tanrıkulu, Cengiz “Kişisel Verilerin Önemi Artıyor”, <http://www.atgv.org.tr/dokumanlar/dergi/atgvdergi3sayi.pdf>, s. 47.
- Tansuğ, Avniye, “AB’nin Yeni Ekonomik Silahı: Veri Saklama Hukuku”, http://www.acikradyo.com.tr/default.aspx?_mv=a&aid=14260
- Tene, Omer, “ Privacy: The New Generations”, International Data Privacy Law, 2010
- Tunç, Hasan. (1999). Anayasa Hukukuna Giriş. Ankara: Nobel Yayın Dağıtım.
- Uygun, Murat, “Avrupa Birliği’nin 95/46 Sayılı Veri Koruma Yönergesi Işığında Kişisel Verilerin Korunması” Gazi Üniversitesi Sosyal Bilimler Enstitüsü Özel Hukuk Anabilim Dalı Avrupa Birliği Hukuku Yayınlanmamış Yüksek Lisans Tezi, Ankara, 2010
- Ülkü, Muhammet Murat. (2005). *5237 Sayılı TCK 132-140 Maddelerinde Yer Alan Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar*, Samsun.
- Üzeltürk, Sultan. (2004). *1982 Anayasası Ve İnsan Hakları Avrupa Sözleşmesine Göre özel Hayatın Gizliliği Hakkı*. İstanbul: Beta.
- Wong, Rebecca. (2007). Data Protection Online: Alternative Approaches to Sensitive Data. *Journal of International Commercial Law and Technology*.

Yardımcı, Murat. (2009). *Türk Hukukunda İletişimin Denetlenmesi*, Ankara: Seçkin Yayıncılık.

Yüksel Civelek, Dilek (2011). *Kişisel Verilerin Korunması ve Bir Kurumsal Yapılanma Önerisi*, Başbakanlık Devlet Planlama Teşkilatı Müsteşarlığı Yayınlanmamış Uzmanlık Tezi, Ankara.

İNTERNET SİTELERİ

<http://www.3sutun.com/NK/kisiselveri.html>

<http://ssrn.com/abstract=1809182>

<http://www.cnil.fr/english/the-cnil/personal-data/>

<http://tdkterim.gov.tr/bts/>

http://www.chip.com.tr/blog/thecrowsalvation/veri-bilgi-ve-bilisim_3332.html

<http://www.kgm.adalet.gov.tr/tbmmkom/kisiselveriler.pdf>

http://www.avrupakonseysi.org.tr/antlasma/aas_108.htm

http://epic.org/privacy/intl/eu_data_protection_directive.html#background

<http://www.cnil.fr/english/the-cnil/personal-data/>

http://www.unicef.org/turkey/udhr/_gi17.html

<http://www.uhdigm.adalet.gov.tr/ihs.htm>

<http://www.anayasa.gov.tr/index.php?l=template&id=188&lang=0>

http://www.flproje.com/eticaret/kisisel_verilerin_korunmasi_ve_gizlilik.php

http://www.avrupakonseysi.org.tr/antlasma/aas_108.htm

http://www.fenafil.com/hukuk/internet/kisisel_veriler.htm

http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html

<http://www.unhcr.org/refworld/publisher,UNGA,THEMGUIDE,,3ddcafaac,0.html>

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML>

- <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:NOT>
- <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:EN:HTML>
- <http://ihami.anadolu.edu.tr/aihmgooster.asp?id=30>
- <http://bianet.org/bianet/bianet/98197-ozel-hayatin-gizlilikinin-ihlali>
- [https://www.privacyinternational.org/article/phr2006-overview-privacy#\[1\]](https://www.privacyinternational.org/article/phr2006-overview-privacy#[1])
- <http://tdkterim.gov.tr/bts/?kategori=verilst&kelime=mahremiyet&ayn=tam>
- http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/review_of_eu_dp_directive.pdf
- http://www.acikradyo.com.tr/default.aspx?_mv=a&aid=14260
- <http://www.oecd.org/dataoecd/39/13/1840065.pdf>
- <http://www.unhcr.org/refworld/publisher,UNGA,THEMGUIDE,,3ddcafaac,0.html>
- sodes.gov.tr/DocObjects/Download/2962/temelhak.pdf
- http://epic.org/privacy/intl/eu_data_protection_directive.html
- <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML>
- http://eurlex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31997L0066&model=guichett
- <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:NOT>
- <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:EN:HTML>
- http://en.wikipedia.org/wiki/Data_Protection_Directive
- http://ec.europa.eu/justice/data-protection/index_en.htm
- http://www.ikv.org.tr/sozluk.asp?bas_harf=T&anahtar=&sayfa=2&id=1169

<http://www.resmigazete.gov.tr/main.aspx?home=http://www.resmigazete.gov.tr/eskiler/2010/05/20100513.htm&main=http://www.resmigazete.gov.tr/eskiler/2010/05/20100513.htm>

<http://www.mevzuat.gov.tr/Metin.Aspx?MevzuatKod=1.5.4721&sourceXmlSearch=&MevzuatIliski=0>

<http://www.mevzuat.gov.tr/Metin.Aspx?MevzuatKod=1.5.6098&MevzuatIliski=0&sourceXmlSearch=>

<http://www.mevzuat.gov.tr/Metin.Aspx?MevzuatKod=1.5.5237&MevzuatIliski=0&sourceXmlSearch=>

<http://www.mevzuat.gov.tr/Metin.Aspx?MevzuatKod=1.5.5271&MevzuatIliski=0&sourceXmlSearch=>

<http://www.egm.gov.tr/pvsk.htm>

<http://mevzuat.basbakanlik.gov.tr/Metin.Aspx?MevzuatKod=1.5.5809&MevzuatIliski=0&sourceXmlSearch=>

<http://www.mevzuat.gov.tr/Metin.Aspx?MevzuatKod=1.5.5651&MevzuatIliski=0&sourceXmlSearch=>

<http://www.resmigazete.gov.tr/main.aspx?home=http://www.resmigazete.gov.tr/eskiler/2005/06/20050601.htm&main=http://www.resmigazete.gov.tr/eskiler/2005/06/20050601.htm>

<http://www.resmigazete.gov.tr/main.aspx?home=http://www.resmigazete.gov.tr/eskiler/2007/02/20070214.htm&main=http://www.resmigazete.gov.tr/eskiler/2007/02/20070214.htm>

<http://mevzuat.basbakanlik.gov.tr/Metin.Aspx?MevzuatKod=1.5.4857&MevzuatIliski=0&sourceXmlSearch=>

<http://mevzuat.basbakanlik.gov.tr/Metin.Aspx?MevzuatKod=1.5.5490&MevzuatIliski=0&sourceXmlSearch=>

<http://mevzuat.basbakanlik.gov.tr/Metin.Aspx?MevzuatKod=1.5.4982&MevzuatIliski=0&sourceXmlSearch=>

<http://www.bedk.gov.tr/>

http://www.tk.gov.tr/eimza/eimza_yasasi.htm

- <http://www.teknoscience.net/index.php/facebook-uye-sayisi-500-milyonu-devirdi/#>
- http://www.tk.gov.tr/mevzuat/yonetmelikler/dosyalar/Kisisel_Bil_Yon_06_02_04.pdf
- <http://ekutup.dpt.gov.tr/ab/sozluk.pdf>
- <http://www.abgs.gov.tr/index.php?p=123&l=1>
- <http://www.abgs.gov.tr/index.php?p=123&l=1>
- http://www.abgs.gov.tr/files/AB_Iliskileri/AdaylikSureci/Kob/Turkiye_Kat_Ort_Belg_2001.pdf
- <http://www.avrupakonseji.org.tr/>
- <http://www.tbv.org.tr/TBV/Documents/BTHukuku/KisiselVerilerinKorunmasiKanunTasarisi-TBVGorus.pdf>
- <http://www2.tbmm.gov.tr/d23/1/1-0576.pdf>
- <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML>
- <http://www.gennaration.com.tr/manset1/arap-bahari-halkin-ag-gucu/>
- <http://www.kigem.com/content.asp?bodyID=5737>
- http://www.oecd.org/document/18/0,2340,en_2649_201185_1815186_1_1_1_1,00.html
- http://www.coe.int/t/dghl/standardsetting/dataprotection/Legal_instruments_en.asp
- http://yzgrafik.ege.edu.tr/~tekrei/dosyalar/yayinlar/200807_Emre.pdf

MAKALE ÇEVİRİLERİ / *Article Translations*

