Dicle Üniversitesi Sosyal Bilimler Enstitüsü
Kamu Hukuku Anabilim Dalı

Yüksek Lisans Tezi

KİŞİSEL VERİLERİN KORUNMASI VE KOLLUK HİZMETLERİ

Ramazan KARABULUT

Diyarbakır 2014

Dicle Üniversitesi Sosyal Bilimler Enstitüsü
Kamu Hukuku Anabilim Dalı

Yüksek Lisans Tezi

KİŞİSEL VERİLERİN KORUNMASI VE KOLLUK HİZMETLERİ

Ramazan KARABULUT

Danışman
Yrd. Doç. Dr. SONGÜL ATAK

Diyarbakır 2014

TAAHHÜTNAME

SOSYAL BİLİMLERİ ENSTİTÜSÜ MÜDÜRLÜĞÜNE

Dicle Üniversitesi Lisansüstü Eğitim-Öğretim ve Sınav Yönetmeliğine göre hazırlamış olduğum **"KİŞİSEL VERİLERİN KORUNMASI VE KOLLUK HİZMETLERİ"** adlı tezin tamamen kendi çalışmam olduğunu ve her alıntıya kaynak gösterdiğimi ve tez yazım kılavuzuna uygun olarak hazırladığımı taahhüt eder, tezimin/projemin kağıt ve elektronik kopyalarının Dicle Üniversitesi Sosyal Bilimler Enstitüsü arşivlerinde aşağıda belirttiğim koşullarda saklanmasına izin verdiğimi onaylarım. Lisansüstü Eğitim-Öğretim yönetmeliğinin ilgili maddeleri uyarınca gereğinin yapılmasını arz ederim.

☐ Tezimin/Projemin tamamı her yerden erişime açılabilir.

☐ Tezim/Projemin sadece Dicle Üniversitesi yerleşkelerinden erişime açılabilir.

X Tezimin **5** yıl süreyle erişime açılmasını istemiyorum. Bu sürenin sonunda uzatma için başvuruda bulunmadığım takdirde, tezimin tamamı her yerden erişime açılabilir.

..../..../.....

Ramazan KARABULUT

KABUL VE ONAY

Ramazan KARABULUT tarafından hazırlanan **"Kişisel Verilerin Korunması ve Kolluk Hizmetleri"** adındaki çalışma, **03.07.2014** tarihinde yapılan savunma sınavı sonucunda jürimiz tarafından **Kamu Hukuku Anabilim Dalı YÜKSEK LİSANS TEZİ** olarak oybirliği ile kabul edilmiştir.

[İmza]

[Unvanı, Adı ve Soyadı] (Başkan)

Yrd. Doç. Dr. Songül ATAK

Yrd. Doç. Dr. Necat AZARKAN

Yrd. Doç. Dr. Hüseyin Murat IŞIK

Enstitü Müdürü

..../..../20

ÖNSÖZ

Kisisel verilerin korunması verinin korunması değil kisiyle ilgili verilerin islenmesi nedeniyle bireyin özgürlüğünün korunmasıdır; bir baska deyisle veri güvenliği sorunu değil, bir özgürlük sorunudur.

"KİŞİSEL VERİLERİN KORUNMASI VE KOLLUK HİZMETLERİ" adını taşıyan bu çalışma ile kişisel verilerin korunması ile ilgili genel ilkeler ışığında kolluk faaliyetlerinin incelenmesi amaçlanmıştır.

Bu çalışmanın hazırlanmasında bana sonsuz destek olan eşime ve özellikle oğlum Ahmet İhsan ve kızım İclal'e, çalışmama ev sahipliği yapan Dicle Üniversitesi'ne ve değerli danışmanım Yrd.Doç.Dr. SONGÜL ATAK'a, ayrica kisisel verilerin korunması alanındaki çalışmalarını istifademize sunan Doç. Dr. Oğuz ŞİMŞEK , Yrd. Doç. Dr. Elif KÜZECİ ve Dr. Aydın AKGÜL'e teşekkürlerimi sunarım.

Ramazan KARABULUT

Diyarbakır 2014

ÖZET

21'inci yüzyılda bilişim ve teknoloji alanında yaşanan baş döndürücü gelişmeler beraberinde özel hayatın gizliliği kavramının alanını daraltarak kişiye özel veriler olarak tanımlayabileceğimiz kişisel verilerin korunması problemini getirmiştir.

Kişisel verilerin korunması alanında uluslararası alanda birçok düzenleme yapılmış olmasına rağmen Avrupa Birliğine üye olma hedefinde olan ülkemizde, insan haklarının en temel öğeleri arasına girmiş bulunan kişisel verilerin korunması konusunda kapsamlı bir düzenleme yapılmamıştır. Bu durum temel hak ve özgürlüklerin korunması açısından büyük bir eksiklik oluşturmaktadır.

İdare tarafından suçların önlenmesi sırasında, kişisel verilerin korunması ve güvenli bir şekilde transferi idarenin yerine getirmesi gerekli en önemli görevlerindendir.

Özellikle kamu gücünün yoğun olarak kullanıldığı ve kolluk faaliyetleri sırasında kişisel veri niteliğinde olan bilgilerin toplaması ve değerlendirmesi işlemlerinin yasal olarak düzenlenmesi gerekmektedir.

Anahtar Kelimeler

Kişisel veri, kişisel verilerin korunması, kolluk hizmetleri.

ABSTRACT

In the 21th century breathtaking technological improvements cause the problem of saving private data described as confidential data, beside they restrict privacy of personal life.

Although there are a lot of arrangements on the international stage about private data protection known one of the basic human rights ;there hasn't been any arrangement about it in our country on the purpose of being an European union member. This fact creates a huge gap in the protection of basic rights and freedoms.

Protecting private data is one of the important duties of administration to be fulfilled at the time of preventing crimes.

Especially during gendarmerie- police forces' operations in which public force is used intensely, legal arrangement is needed to gather information known as private data.

Keywords

Private Data, Private Data Protection, Preventive Gendarmerie Services.

İÇİNDEKİLER

Sayfa No.

II. BÖLÜM

KİŞİSEL VERİLERİN KORUNMASI HUKUKUNUN TEMEL İLKELERİ

III. BÖLÜM

TÜRK HUKUKUNDA KİŞİSEL VERİLERİN KORUNMASIYLA İLGİLİ HUKUKSAL DÜZENLEMELER

İV. BÖLÜM

AVRUPA İNSAN HAKLARI MAHKEMESİ VE KİŞİSEL VERİLERİN KORUNMASI HAKKI

VI. BÖLÜM
KOLLUK HİZMETLERİ VE KİŞİSEL VERİLERİN KORUNMASI

KISALTMALAR

AB	Avrupa Birliği
ABD	Amerika Birleşik Devletleri
AET	Avrupa Ekonomik Topluluğu
a.g.e.	Adı Geçen Eser
a.g.m.	Adı Geçen Makale
a.g.w.s.	Adı Geçen Web Sayfası
AİHM	Avrupa İnsan Hakları Mahkemesi
AİHS	Avrupa İnsan Hakları Sözleşmesi
AK	Avrupa Konseyi
Bkz.	Bakınız
BM	Birleşmiş Milletler
md.	Madde
MOBESE	Mobil Elektronik Sistem Etegrasyonu
OECD	Avrupa Ekonomik İşbirliği Teşkilatı
TCK	Türk Ceza Kanunu
VKY	Veri Koruması Yönergesi

GİRİŞ

Teknolojik ve bilimsel gelişmeler neticesinde içinde yaşadığımız dünya sanal bir hale dönüşmüştür. Dünyamızı saran dijital ağ sayesinde evinde bilgisayar ve internet olan bir kişinin bilgiye ulaşması artık bir tuş mesafesi kadar kısalmıştır.

Bilgi Çağı toplumlarında kişinin kendisi hakkındaki bilgi/enformasyon üzerindeki tayin hakkı (self-determinasyon) bilgisayar sistemlerinin yaygınlaşması, internet kullanımının artması ve büyük miktarda verileri çok hızlı şekilde işleme ve iletme kapasitelerinin kişisel verilerin oluşturulması, saklanması ve kullanılmasında başta gelen araç olması nedeniyle kişinin kendi verileri üzerindeki kontrol yeteneği kaybolmuş, özel hayatın gizliliğinin korunmasına ilişkin kolaylıklar da ortadan kalkmıştır[1].

Kişisel verilerin korunmasında temel amaç verinin korunması değil verilerin sahibi olan bireyin temel hak ve özgürlüklerinin korunmasıdır.

Kamusal hizmetlerin yürütülmesi esnasında kişisel verilerimiz yoğun olarak kullanıldığı gibi ticari faaliyetlerde bulunan özel şirketler başta olmak üzere birçok kuruluş tarafından kişisel verilerimiz kayıt altına alınmakta ve değişik maksatlarla kullanılmaktadır.

Kişisel verilerin kaydedilmesi, korunması ve transferi sırasında kişisel hak ve özgürlüklerin korunması konusu yaklaşık yarım asırdır uluslararası toplumun gündeminde yer almasına rağmen ülkemizde henüz kişisel verilerin korunması alanında ciddi bir adım atılabilmiş değildir.

---

[1] KETİZMEN, Muammer., **Türk Ceza Hukukunda Bilişim Suçları**, 1. Basım, Adalet Yayınları, Ankara, 2008, s.194-195.

Kişisel verilerin korunması alanında gerekli yasal düzenlemeler yapılmadığı gibi özellikle kolluk faaliyetleri esnasında bu veriler yoğun olarak işleme tabi tutulmaktadır.

Bu çalışmada kişisel verilerin korunması ile ilgili kavramları, uluslararası düzenlemeleri, ülkemizde yapılan düzenlemeleri ve kolluk faaliyetleri esnasında kişisel veriler üzerinden yürütülen işlemleri inceleyerek bu alanda yapılan çalışmalara katkıda bulunmak amaçlanmıştır.

I.BÖLÜM

KİŞİSEL VERİ KAVRAMI VE ULUSLARARASI BELGELERDE KİŞİSEL VERİLERİN KORUNMASI

A. GENEL OLARAK

İletişim ve bilgi teknolojilerindeki hızlı gelişmeler neticesinde dünyamızın küçülerek küresel bir köy haline geldiği bir çağda yaşamaktayız. Bu durum beraberinde kişisel verilerimizin başta kamu kurumları ve ticari kuruluşlar olmak üzere birçok unsur tarafından toplanılması, kaydedilmesi ve kullanılmaya başlanılması ile özel hayatımıza ait kişisel alanın giderek daralmasına neden olmuştur. Özellikle internetin günlük hayatta artan şekilde kullanılmaya başlanmasının doğal sonucu olarak bireyi günlük hayatta tanımlayan ve belirleyen kişisel verilerin elektronik izdüşümlerinin oluşmasına, bu verilerin elektronik ortamda çeşitlenmesine ve daha fazla işlenmesine sebep olmuştur[2].

Kişisel verilerin korunması alanında uluslararası gelişmeler yirminci yüzyılın ortalarından itibaren başlamıştır. Avrupa Birliği bünyesinde yapılan çalışmalar üye devletlerin iç hukuklarına doğrudan etkisi olan düzenlemeler getirmiş ve ayrıca Avrupa İnsan Hakları Mahkemesi de kişisel verilerin korunması hakkında verdiği kararlar ile bu çalışmalara katkı sağlamıştır[3].

Ülkemizde de 2010 yılında gerçekleştirilen anayasa değişikliği ile birlikte "özel hayatın gizliliği ve korunması" maddesine eklenen bir fıkra sonucu anayasal bir

[2] CİVELEK, D., **Kişisel Verilerin Korunması Ve Bir Kurumsal Yapılanma Önerisi (Uzmanlık Tezi)**, Başbakanlık Devlet Planlama Teşkilatı Bilgi Tolumu Dairesi Başkanlığı Yayın No: 2821, Nisan 2011, s.6, http://www.bilgitoplumu.gov.tr/Documents/1/tezler/Kisisel_Verilerin_Korunmasi-Dilek_Civelek-DPT_Uzmanlik_Tezi.pdf (E.T. 04.06.2014)

[3] ÖZDEMİR, H., **Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması,** Seçkin Yayınları, Ankara, 2009, s.17.

dayanağa kavuşan kişisel verilerin korunmasına dönük olarak ayrıca Türk Ceza Kanunumuz kişisel verilerin hukuka aykırı olarak kaydedilmesini, verilmesini veya ele geçirilmesini suç olarak düzenlemiştir.

Avrupa Birliğine üye olma yolunda ilerleyen ülkemizde ise kişisel verilerin korunması hakkında mevcut yasal bir düzenleme bulunmamaktadır ve bu durum 2012 yılı Avrupa Birliği İlerleme Raporunda Kişisel Verilerin Korunması Kanunun henüz yasalaşmadığı belirtilerek eleştirilmektedir. Raporda ayrıca özel hayata ve aile hayatına saygıya ve özellikle kişisel verilerin korunmasına ilişkin olarak, ulusal mevzuatın, kişisel verilerin korunmasına ilişkin AB müktesebatı ile uyumlu hale getirilmesi tavsiye edilmektedir[4].

Kişisel verilerin korunması, bir taraftan veri toplamakta önemli bir biçim olan "gözetim" ve ona karsı çare olarak görülen gizliliğin korunması, diğer taraftan bu gizliliğin korunmasına karsı verilerin serbestçe dolaşımının sağlanması gibi çelişkileri ve çeşitli aktörleri içermektedir. Dolayısıyla kişisel veri korumasının bütüncül bir acıdan incelenmesini sağlayacak ekonomik politik yaklaşımla ele alınması uygun olmaktadır[5].

Konuya sadece hukuk penceresinden bakarak incelemek kişisel verilerin korunmasını özel hayatın gizliliği kavramına hapsetmek anlamına gelecektir. Kişisel verilerin korunmasına ilişkin kaygıların temelinde ticari faaliyetler esnasında bu verilerin toplanması, kaydedilmesi, üçüncü şahıs-şirket veya ülkelere transfer edilmesi faaliyetlerinin artması ile gündeme geldiği yapılan çalışmalarda göz önünde bulundurulmalıdır.

[4] Türkiye Cumhuriyeti Avrupa Birliği Bakanlığı resmi internet sayfası, Türkiye 2012 Yılı İlerleme Raporu, Komisyon Tarafından Avrupa Parlamentosu'na Ve Konsey'e Sunulan Bildirim, 10 Ekim 2012, Bürüksel, http://www.ab.gov.tr/files/AB_Iliskileri/AdaylikSureci/IlerlemeRaporlari/2012_ilerleme_raporu_tr.pdf (E.T. 04.06.2014).

[5] KARLIDAĞ Serpil., **Amme İdaresi Dergisi,** Cilt 46, Sayı 1, Mart 2013, http://yayin.todaie.gov.tr/yazar.php?Yazar=1085 s. 127-128.

B. KİŞİSEL VERİ KAVRAMI

Türkçe Sözlükte veri; olgu, kavram veya komutların, iletişim, yorum ve işlem için elverişli biçimli gösterimi olarak tanımlanmıştır[6].

Kişilerin konu olduğu bilgilere "isme bağlı veriler" veya "bireysel veriler" denilmektedir. İsme 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. Başta devlet olmak üzere, kamu yönetimleri, çeşitli kamu kuruluşları, özel hukuktaki kar 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 tutmaktadır[7].

Uluslararası ve ulusal alanda yapılan yasal düzenlemelerde güvence altına alınmış olan temel hak ve özgürlüklerimiz kapsamında değerlendirebileceğimiz kişisel verilerimiz "bir kişiyi belirleyen ya da onu belirlenebilir kılan her türlü bilgi" olarak tanımlanmaktadır.

Kişisel verileri kişisel olmayan verilerden ayırmak için iki unsurun varlığı aranacaktır. Birincisi verinin bir kişiye ilişkin olması, ikincisi kişinin belirli ya da belirlenebilir olması gereklidir[8].

Bu doğrultuda kişisel veri tanımında şu hususlar ön plana çıkmaktadır[9].

---

[6] Türk Dil Kurumu Güncel Türkçe Sözlük , http://www.tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.53b5ddd91f5103.96738836

[7] Tekin, Akıllıoğlu., Prof. Dr. Tekin Akıllıoğlu'nun Makaleleri, "İdari Usul ve Kişisel Verilerin Korunması", www.idare.gen.tr/akillioglu-idariusul.htm (11 Ağustos 2004), (E.T. 04.06.2014).

[8] KÜZECİ, Elif. **Kişisel Verilerin Korunması**, Turhan Kitabevi, ANKARA 2010, s.9.

[9] Türkiye Bilişim Derneği, Kamu-BİB Kamu Bilişim Platformu X, Kişisel Verilerin Korunması 2. Çalışma Grubu, Nihai Raporu, Belge No : TBD/Kamu-BİB/2008-ÇG2, Tarihi : 17/04/200, s. 24-25, http://www.tbd.org.tr/usr_img/cd/kamubib15/raporlarPDF/RP2-2008.pdf, (E.T. 04.06.2014).

· Kim olduğu, kimliği belirli veya dolaylı olarak belirlenebilen kişilere ait bilgi ya da enformasyon kişisel veridir.

· Kişisel verilerin korunmasına ilişkin düzenlemelerin kapsamına göre, tüzel kişiler hakkındaki bilgi ya da enformasyon da kişisel veri olarak kabul edilebilmektedir.

· Kişisel verilerin korunması bireyin özgürlüğünün/mahremiyetinin korunması açısından önemlidir.

· Kişisel verinin korunması ile ilgili sorumluluklar ve yükümlülükler, bir verinin kişisel veri olması ile bağlantılı olup kişisel verinin işlenmeye başlanması, bu alandaki sorumluluk ve yükümlülükleri beraberinde getirir.

· Ortada kişisel veri yoksa korunacak kişisel veri de söz konusu olamaz. Bu durumda, sadece bilgi güvenliği önemli hale gelir.

· Kişisel veri teriminde yer alan "kişisel" sıfatı, bir aidiyet/mülkiyet sorununu çözmeye yönelik değildir. Kişisel olma, verinin içerdiği bilgi ya da enformasyonun ilgili bir kişi hakkında olduğunu -kişinin kim olduğunun doğrudan ya da dolaylı olarak ortaya çıkarılabildiğini- vurgulamak için kullanılmaktadır.

1. Uluslararası Belgelerde Kişisel Veri Kavramı İle İlgili Tanımlar

Özel yaşama saygıyı ve halklar arasındaki serbest bilgi akışını düzenlemek amacı ile 1981 yılında Avrupa Konseyi tarafından kabul edilen Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşme kişisel veriyi; "Kimliği belirtilen veya belirtilebilen gerçek kişiyle ilgili tüm bilgileri ifade eder[10]" şeklinde tanımlamıştır. Bu sözleşme kişisel verilerin korunması konusunda kabul edilmiş olan bağlayıcı ilk uluslararası belge olması nedeni ile büyük bir önem taşımaktadır.

Kişisel Verilerin İşlenmesi Sürecinde Kişilerin Korunması ve Bu Verilerin Özgür Dolaşımına İlişkin Yönerge; "kişisel veri" fiziksel, fizyolojik, zihinsel,

[10] KILINÇ, Doğan., Anayasal Bir Hak Olarak Kişisel Verilerin Korunması, AÜHFD, 61 (3) 2012:1089-1169, s. 1094, http://dergiler.ankara.edu.tr/dergiler/38/1690/18020.pdf , (E.T. 04.06.2014).

ekonomik, kültürel veya sosyal kimliğine özel bir veya daha fazla faktöre veya bir kimlik numarasına atıf başta olmak üzere doğrudan veya dolaylı olarak tespit edilebilen bir tespit edilebilir kişi; tespit edilmiş veya tespit edilebilir gerçek kişiye ilişkin herhangi bir bilgi[11] şeklinde bir tanımlama yapmıştır. Bu tanım bir kişiyi belirli kılan veya belirlenebilir kılan her türlü unsuru içerdiği değerlendirilmektedir.

Dünyada genel anlamda bir veri koruma kanunu ilk kez Almanya da çıkarılmıştır[12]. Almanya'nın Hessen eyaletinde çıkarılan 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" seklinde tanımlanmakta ve bireyin kişisel verilerinin korunması hakkına açıkça yer verilmektedir. Buna göre: "herkes korunmaya değer bir yararı bulunduğu sürece, özel yaşamına ve aile yaşamına riayet bakımından, kendisini ilgilendiren kişisel nitelikli verilerinin gizli tutulması hususunda bir hakka sahiptir[13].

2. Ülkemizde Kişisel Veri Kavramı İle İlgili Tanımlar

Türkiye, Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşmeyi 1981 yılında imzalamış olmasına rağmen sözleşme gereği olarak iç hukukta gerekli düzenlemeyi yapmadığından dolayı onaylamamıştır[14]. Anayasamızın özel hayatın gizliliği ve korunması başlığını taşıyan 20. maddesinde 2010 yılında yapılan değişiklik ile kişisel verilerin korunmasının önemi vurgulanmış ancak bir tanım yapılmayarak bu görev çıkarılacak bir yasaya bırakılmıştır[15]. 2008 yılında hazırlanan ancak

---

[11] 95/46/EC numaralı Verilerin Korunmasına Dair Yönerge http://www.ihop.org.tr/dosya/coe/EC_DIRECTIVE_95_46_Kisisel_Veriler.pdf , (E.T. 04.06.2014).

[12] ŞİMŞEK, O., **Anayasa Hukukunda Kişisel Verilerin Korunması**, Beta , 2008 İSTANBUL, s.10.

[13] ŞİMŞEK, O**., 4422 sayılı Çıkar Amaçlı Suç Örgütleriyle Mücadele Kanunu ve Kanunun 4. Maddesine Göre "Kayıt ve Verilerin İncelenmesi" ve Kişisel Nitelikli Verilerin Korunması** http://web.deu.edu.tr/ab/MAKALE/deu%20MAK/0012.htm , (E.T. 04.06.2014).

[14] ATAK, S., Avrupa Konseyinin Kişisel Veriler Açısından Sağladığı Temel Güvenceler, **TBB Dergisi**, sayı 87, 2010, s. 94.

[15] Halkoylamasına sunulmak üzere 13 Mayıs 2010 tarih ve 27580 sayılı Resmî Gazetede yayınlanmıştır. Yüksek Seçim Kurulu, 13 Mayıs 2010 tarih ve 317 sayılı Kararıyla halkoylamasının 12 Eylül 2010 Pazar

yasalaşmayan kişisel verilerin korunması kanun tasarısında kişisel veri kavramı "belirli veya kimliği belirlenebilir gerçek ve tüzel kişilere ilişkin bütün bilgiler[16]" şeklinde tanımlamıştır.

Mevzuatımızda "kişisel veri" kavramı 5237 sayılı Türk Ceza Kanunumuzun[17] Özel Hayatın Gizliliğini İhlal suçunu düzenleyen 134. maddesinde, Kişisel Verilerin Kaydedilmesi suçunu düzenleyen 135. maddesinde, Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme suçunu düzenleyen 136. maddesinde kullanılmıştır.

TCK da tanım yapılmamış olmakla birlikte TCK gerekçesinde *"gerçek kişiyle ilgili her türlü bilgi"* kişisel veri olarak kabul edilmiştir.

Kişisel veri kavramı 5809 sayılı Haberleşme Kanunu 12. ve 51. maddesinde kullanılmakla birlikte tanımlanmamış bu kanuna istinaden hazırlanan Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi Ve Gizliliğinin Korunması Hakkında Yönetmelikte "belirli veya kimliği belirlenebilir gerçek ve tüzel kişilere ilişkin bütün bilgiler" olarak tanımlanmıştır.

Kişisel veri kavramını tanımlamak önemli olduğu kadar bireye ait hangi bilgilerin kişisel veri kapsamında değerlendirileceğinin belirlenmesi de önemlidir. Kişisel verilerin içeriğini oluşturan bilgiler toplumlara göre farklılık gösterebileceği gibi toplumu oluşturan bireyler arasında da farklılık gösterebilir.

C. KİŞİSEL VERİLERİN KORUNMASI VE ÖZEL HAYATIN GİZLİLİĞİ

Temel hak ve özgürlüklerimiz, uluslararası sözleşmeler ve anayasalar tarafından güvence altına alınmıştır. Bireylerin özel hayatının en önemli bölümünü oluşturan kişisel verilerin korunması temel hak ve özgürlüklerimiz kapsamında değerlendirilmelidir. Çünkü kişisel verilerin korunmasında amaç kişiyi belirleyen ya da

---

günü yapılmasına karar vermiştir. YSK'nın bu kararı 13 Mayıs 2010 tarih ve 27580 sayılı Mükerrer Resmî Gazetede yayınlanmıştır. http://www.anayasa.gen.tr/5982.htm (E.T. 04.06.2014).

[16] Kişisel Verilerin Korunması Kanun Tasarısı, T.C. Başbakanlık Kanunlar ve Kararlar Genel Müdürlüğü, 22.04.2008, http://www2.tbmm.gov.tr/d23/1/1-0576.pdf , (E.T. 04.06.2014).

[17] Türk Ceza Kanunu, Kanun Tertip: 5, Resmi Gazete Tarihi: 12.10.2004, Sayısı: 25611.

belirlenebilir kılan veriyi korumak değil bireyin kendisine ait bilgiler üzerinde sahip olduğu hak ve özgürlükleri güvence altına almaktır.

Kişisel verilerin korunması için yapılan düzenlemeler bireylerin ekonomik ve sosyal ilerlemesine, refahına ve ticari gelişmesine katkıda bulunurken eş zamanlı olarak bireyin temel hakları ve özgürlükleri olmak üzere kişisel mahremiyetini, özel hayatını, haberleşme hürriyetini korumalıdır.

Özel hayatın gizliliği temel bir insan hakkı olarak birçok metinde açıkça düzenlenmiş olmasına rağmen "özel hayat" kavramı tanımlanmış değildir. Bu tanımı yapmak kolay değildir çünkü kamusal alan ile özel alan arasındaki sınır, bir durumdan diğerine değişecektir. Özel hayat kavramının genel hatları ile belirlenmesinde Avrupa İnsan Hakları Mahkemesinin verdiği farklı kararlar ışığında bir fikir oluşması mümkün olabilecektir[18].

AİHM "özel hayat" kavramının kapsamlı bir tanımını yapmanın ne mümkün, ne de gerekli olduğunu görüşündedir. Ancak, bu kavramı bireyin kendi özel hayatını istediği gibi yaşayabileceği bir "iç alan" ile kısıtlamak ve bu alandan söz konusu alanın içinde olmayan dış dünyayı olduğu gibi hariç tutmak aşırı kısıtlayıcı olacağından özel hayat hakkı, belirli bir düzeye kadar başka insanlarla ilişkiler kurmayı ve bu ilişkileri devam ettirmeyi de içermelidir[19].

Özel hayat kavramı ile ilgili açıklamaların yanında mahremiyet kavramının da sınırlarını belirlemekte fayda olacaktır. Çünkü yaşadığımız toplumun kültürel yapısında bireyin özel yaşam alanı genellikle mahremiyet olarak ifade edilmektedir.

Özel hayatın gizliliği hakkı ilk olarak İnsan Hakları Evrensel Bildirisi'nde yer almıştır. Bildirinin 12. maddesine göre, "Hiç kimse özel hayatı, ailesi, meskeni veya yazışması hususlarında keyfi karışmalara, şeref ve şöhretine karsı tecavüzlere maruz bırakılamaz. Herkesin bu karışma ve tecavüzlere karsı kanun ile korunmaya hakkı vardır."

[18] DUTERTRE, Gilles., Avrupa İnsan Hakları Mahkemesi Kararlarından Örnekler, Avrupa Konseyi Yayınları, Ankara 2007, www.yargitay.gov.tr/abproje/belge/.../aihm_kararlarindan_ornekler.pdf , s.201, (E.T. 04.06.2014).

[19] Dutertre, a.g.e. s. s.201.

İnsan Hakları ve Temel Özgürlüklerinin Korunmasına İlişkin Sözleşme (Avrupa İnsan Hakları Sözleşmesi) de özel hayatın gizliliği açıkça düzenlenmiştir. Özel hayatın gizliliğinin düzenlendiği Özel hayatın ve aile hayatının korunması başlıklı 8. maddesi:

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

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

AİHS'ne benzer düzenleme Anayasamızın 20. maddesinde de yer almaktadır. "Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz. Milli güvenlik, kamu düzeni, suç islenmesinin önlenmesi, genel sağlık ve genel ahlakın 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 ustu, özel kâğıtları ve eşyası aranamaz ve bunlara el konulamaz."

Kişisel verilerin korunması amacı ile hazırlanan ve temel belge olma niteliğini taşıdığını söyleyebileceğimiz "Kişisel Verilerin Otomatik İşleme Tabi Tutulma Sürecinde Bireylerin Korunmasına İlişkin 108 sayılı Sözleşme ve Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair Yönerge incelendiğinde temel amacın kişisel verilerin işleme tabi tutulması esnasında bireyin "özel hayata saygı" hakkının korunması olduğu görülmektedir. Ayrıca üye devletlerarasında var olan veri akışı özel yaşamı korumaya yönelik nedenler ile yasaklanmayacak ve engellemeyecektir.

Özel hayatın gizliliğinin diğer gerçek ve tüzel kişiler tarafından bozulması üç şekilde gerçekleşebilir[20];

• Kişinin hayatının, başkalarınca bilinmesini istemediği bölgesine fiziksel güç kullanarak veya başka yollardan sızılması söz konusu olabilir.

• Bu şekilde veya başka meşru görülmeyen yollardan kişinin hayatının, başkalarına açık olmayan bir bölgesi hakkında bilgi, belge ve veriler edinilmesi söz konusu olabilir.

• Edinilmiş olan bu bilgi, belge ve verilerin kamuya açıklanması veya başka bir amaçla kullanılması söz konusu olabilir.

D. ULUSLARARASI BELGELERDE KİŞİSEL VERİLERİN KORUNMASI

1. Genel Olarak

Kişisel verilerin korunmasına ilişkin sorunlar çağımızda meydana gelen gelişmelere bağlı olmakla birlikte bireyin kendisine ait bilgilerin korunması düşüncesi çok eskiye dayanmaktadır. Günümüzde hala geçerliliğini koruyan ve hekimin sır saklama yükümlülüğünü belirleyen Hipokrat yemini hekimin kendisi tarafından öğrenilen hastalara ilişkin bilgileri saklama ve açıklamama yükümlülüğü getirmiştir[21].

Teknolojik gelişmeler sonucu kişisel verilerin devletler ve ticari örgütler tarafından toplanması, saklanması ve işlenmesi, kapsamlı veri tabanları oluşturulması ve güçlü iletişim ağları ve internet kanalıyla yüksek hızda veri transferinin mümkün olması verilerin korunması konusunda endişelerin doğmasına neden olmuş ve bu alanda koruyucu önlemler alınması gerektiği gerçeğini ortaya koymuştur[22].

---

[20] Aktaran Cavidan Soykan, Bireysel Gizlilik ve Kişisel Verilere Erişim Hakkı, XI. Türkiye'de İnternet Konferansı Bildirileri, , TOBB Ekonomi ve Teknoloji Üniversitesi, 21 - 23 Aralık 2006, Ankara, s.16. inet-tr.org.tr/inetconf11/bildiri/38.doc

[21] Şimşek, a.g.e. s.6.

[22] ATAK S., Kişisel Verilerin Korunmasına İlişkin Avrupa Birliği Yönergesinin Temel Özellikleri, **Kazancı Hakemli Hukuk Dergisi** (sayı 59-60), 2009, s. 201.

Kişisel verilerin toplanması, işlenmesi ve transferi esnasında bireyin hak ve özgürlüklerinin korunması, özel hayatın gizliliğinin güvence altına alınabilmesi için ulusal düzenlemelerin yeterli olmayacağı göz ardı edilemeyecek kadar önemli bir sorundur. Çünkü veriler sadece kamu otoritesi ve özel kişiler tarafından işleme tabi tutulmakla kalmayıp uluslararası organizasyonlar tarafından transfer edilerek kullanılmaktadır.

2. Ekonomik İşbirliği Ve Kalkınma Teşkilatı (OECD)

OECD olarak bilinen Ekonomik İşbirliği ve Kalkınma Teşkilatı İkinci Dünya Savaşının etkilerinin yok edilmesi gayesiyle, aralarında Türkiye'nin de bulunduğu 18 Avrupa ülkesine, ABD ve Kanada'nın katılmasıyla, 14 Aralık 1960'ta kurulmuştur. OECD üye ülkeler içinde, birlik, dayanışma ve işbirliğini sağlayan, ülkelerin ekonomik ve siyasal konularda görüşlerini belirleyip uyumlaştırmaya aracılık eden bir kuruluştur[23].

Kişisel verilerin korunması hakkının ayrı bir alan olarak doğrudan doğruya ele alınması ve bu konuda uluslararası kriterler belirlenmesine dair ilk çalışma Ekonomik İşbirliği ve Kalkınma Teşkilatı (OECD) tarafından 1980 yılında kabul edilmiş olan "Gizliliğin Korunması ve Sınır Ötesi Kişisel Veri Akışları Hakkında Rehber İlkeler" içeren bir belgedir[24]. Bu ilkeler 23 Eylül 1980 tarihinde kişisel verilerin toplanması, yönetilmesi ve korunması ile sınır ötesi bilgi akısının sağlanmasında asgari düzeyde uluslararası uzlaşının sağlanması ve temel ilkelerin belirlenmesi amacıyla hükümetler, iş dünyası, sivil toplum örgütleri ve tüketici temsilcilerinin yardımıyla kabul edilmiştir.

OECD ilkelerinin amacı kişisel verilerin korunması hakkının korunmasından çok bu verilerin gizliliğin korunmasında etkinlik ile verilerin akısındaki serbestlik arasında dengenin kurulması ve ülkelerin gerek kamu sektörü gerekse de özel sektör

[23] Vikipedi, http://tr.wikipedia.org/wiki/OECD , (E.T. 04.06.2014)

[24] http://www.oecd.org/document/18/0,2340, en_2649_34255_1815186_1_1_1_1,00.html, (E.T. 04.06.2014)

bazında uygulamalarını temin etmek amacıyla iç düzenlemeler yapması konusunda fikir oluşturmaktır[25].

Rehber İlkeler, hukuksal olarak bir tavsiye kararıdır ve üye ülkeler için bağlayıcılığı yoktur. Dolayısıyla OECD üyesi devletler, bu ilkeleri iç hukuklarının bir parçası haline getirip getirmemekte serbesttir. Konsey, temel olarak üye devletlere kişisel verilerin korunması ve bireysel özgürlüklerle ilgili bu ilkeleri, iç hukuklarında yapacakları yasal düzenlemelerde dikkate almalarını, sınır aşan veri trafiğinin haksız yere engellenmemesini, mevcut engellerin kaldırılmasını, bu ilkelerin yaşama geçirilmesinde iş birliği yapılmasını tavsiye etmektedir[26].

Rehber ilkeler beş temel bölümden oluşmaktadır; genel hükümler, iç hukuk alanındaki uygulama için genel ilkeler, uluslararası uygulama için temel ilkeler ve serbest veri trafiği, meşru sınırlamalar, iç hukuka aktarma ve uluslararası işbirliğidir[27].

Kabul edilen ilkeler kamusal sektörün yanında özel sektör için de geçerli hükümler öngörmektedir.

"OECD Rehber İlkeleri, kişisel verilerin korunmasına ilişkin politikaların belirlenmesi ve yasal düzenlemelerin yapılmasında ölçüt olarak kullanılan sekiz ilkeyi içermektedir. Bu ilkeler şunlardır:

1) Kişisel Veri Toplanması ve İşlenmesinin Sınırlı Olması ve İlkellere Bağlılığı (md. 7): Bu ilke ile kişisel verilerin toplanması ve islenmesinin sınırları olması ve verilerin hukuka uygun, meşru yollarla ve mümkün olduğunca veri konusu kişinin bilgisi veya rızası ile elde edilmesinin gerekliliği vurgulanmıştır.

2) Kişisel Veride Kalite İlkesi (md. 8): Bu ilke ile kişisel verilerin islenmesiyle ilgili gerekli nitelikler vurgulanmaktadır. Buna göre, kişisel verilerin güncel tutulması,

[25] ERSOY Uğur,. **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 2009, s. 52.

[26] OECD. Org. a.g.w.

[27] Şimşek, a.g.e. s.13.

tam ve doğru olması, kullanılacağı amaçla bağlantılı ve bu amacın gerekleriyle sınırlı olması şartlarına işaret edilmektedir.

3) Kişisel Veri Toplama ve İşlenmesinde Amacın Belirginliği İlkesi (md. 9): Kişisel verilerin toplanmasından önce, bu verilerin toplanmasının amaçlarının belli olması, sonraki kullanımların da bu amaçlarla sınırlı tutulması gereğine değinilmektedir. Toplanma amacının değişebileceği her durumda da, söz konusu değişen amaçların aynı şekilde belirgin olması gerektiği belirtilmektedir.

4) Amaca Uygun Kullanım İlkesi (md. 10): Yukarıda sözü geçen ilke ile doğrudan bağlantılı olan bu ilke gereğince, veri konusu kişinin rızası veya kanunun yetki verdiği haller hariç olmak üzere, kişisel verilerin toplandığı ve islendiği amaçlar dışında kullanılmaması, elde edilebilir hale getirilmemesi veya açıklanmaması öngörülmektedir.

5) Kişisel Verilerin Korunması İçin Gereken Tedbirlerin Alınması İlkesi (md. 11): Bu ilke ile kişisel verilerin, yetkisiz olarak erişilmesi, imhası, kullanılması, değiştirilmesi veya açıklanması ya da kaybolması gibi risklere karsı uygun güvenlik tedbirleriyle korunması gerektiğine dikkat çekilmektedir.

6) Açıklık İlkesi (md. 12): Kişisel verilerle ilgili olarak yürütülen politikalar ile uygulamalar ve gelişmeler hakkında genel bir açıklık politikası bulunması gereği vurgulanmaktadır. Veri konusu (öznesi) kişilerin bilgilendirilmesi ve bilgiye erişim hakkı, veriyi tutan kurum tarafından kurum sicili tutulması ve veri kontrolörünün kimlik ve adres bilgileri gibi bilgilerin mevcut bulundurulması gibi hususlar açıklık ilkesinin gerekliliklerindendir. Rehber İlkelerde verilerin toplanmasından, depolanmasından, kullanılmasından, açıklanmasından vs. sorumlu olan görevli olarak tanımlanmıştır.

7) Kişisel Veri Konusu Kişinin Bireysel Katılımı İlkesi (md. 13):Kişinin, veri kütüğü sahibinden, onunla ilgili veri olup olmadığına dair bilgi edinmeye; anlayabileceği bir şekilde, makul yollarla, tatbik ediliyorsa aşırı olmayan bir ücretle, makul süre için kendisine ilişkin veriler konusunda bilgilendirilmeye; bilgi edinme ve bilgilendirilme talepleri reddedilirse sebeplerini öğrenmeye, bu gibi reddedilmelere karşı itiraz veya kanun yollarına başvurabilmeye; kendisine ilişkin verilere itiraz

edebilme ve haklı itirazı halinde bu verileri sildirmeye, düzeltmeye, eksik ise tamamlatmaya ve değiştirmeye hakkı olması gerektiği vurgulanmaktadır.

8) Sorumlu Tutulabilirlik İlkesi (md. 14): Buna göre veri kütüğü sahibinin, yukarıda belirtilen prensiplere uyulması için getirilen tedbir ve yaptırımlara uymasını temin edecek şekilde sorumlu tutulması sağlanmalıdır. Veri kütüğü sahipleri, getirilen prensiplere uymakla yükümlü tutulmuştur. Bu yükümlülüklerini yerine getirmeyen veri kütüğü sahipleri idarî, hukukî ve cezaî yaptırımlara tâbi olacaktır"[28].

Bilgi sistemleri ve teknolojilerinin büyük ölçüde değişime uğradığı, ilerleyen teknolojiler ve internetin geniş kapsamlı kullanımının ulusal sınırları asarak enerji, ulaştırma ve finans gibi önemli altyapıları destekleyerek şirketlerin işleyişinde, hükümetlerin vatandaşlara ve teşebbüslere sundukları hizmetlerde ve bireylerin iletişim ve bilgi alışverişinde önemli bir rol oynadığı, bilgi alışverişinin doğası, hacmi ve hassasiyeti büyük ölçüde arttığı için temel hak ve özgürlüklerin ve kişisel verilerin korunması amacıyla yeni önlemler getirilmesi gerektiğinden bahisle, OECD üye ülke hükümetlerince şu metinler kabul edilerek söz konusu Rehber İlkeler geliştirilmiştir:

- 11 Nisan 1985 tarihli "Sınır Ötesi Veri Akısı Bildirisi"

- 26 Kasım 1992 tarihli "Bilgi Sistemlerinin Güvenliği için Rehber İlkeler"

- 27 Mart 1997 tarihli "Kriptografi Politikası Rehber İlkeleri",

- 7-9 Aralık 1998 tarihli "Küresel Ağlarda Mahremiyetin Korunmasına İlişkin Bakanlar Konseyi Bildirisi"[29].

3. Birleşmiş Milletler (BM)

Birleşmiş Milletler Örgütü ya da kısaca Birleşmiş Milletler (BM), 24 Ekim 1945'te kurulmuş dünya barışını, güvenliğini korumak ve uluslararasında ekonomik, toplumsal ve kültürel bir iş birliği oluşturmak için kurulan uluslararası bir örgüttür. Birleşmiş Milletler kendini "adalet ve güvenliği, ekonomik kalkınma ve sosyal eşitliği

[28] Ersoy, a.g.e. s. 54.

[29] Ersoy, a.g.e. s. 55-56.

uluslararasında tüm ülkelere sağlamayı amaç edinmiş küresel bir kuruluş" olarak tanımlamaktadır[30].

BM'nin kuruluşundan kısa bir sure sonra 10 Aralık 1948 yılında kabul edilen BM Evrensel İnsan Hakları Bildirisi, Örgüt'ün insan haklarının korunması alanında dünya ölçeğinde standart belirleme surecinin ilk adımıdır.

İnsan hak ve özgürlüklerinin korunmasında bu belge temel alınmaktadır. Bildirinin 12. maddesinde özel yaşamın gizliliği hakkı düzenlenmiştir. 12. madde hükmü şöyledir[31]:

"Hiç kimse, özel yaşamına, ailesine, konutuna ya da haberleşmesine yönelik keyfi müdahalelere ya da onur ve şöhretine yönelik saldırılara maruz bırakılmayacaktır. Herkesin, bu tür müdahale ya da saldırılara karşı yasa ile korunma hakkı vardır".

BM Bireysel ve Siyasal Haklar Uluslararası Sözleşmesi'nin 17. maddesinde de, hemen hemen aynı ifade ile bu hak alanına yer verilmiştir. Ancak daha önemlisi, kişisel verilerin korunması hakkının bu Sözleşmede yer alan özel yaşamın gizliliği hakkı kapsamında görüldüğünün BM İnsan Hakları Komitesi tarafından açıkça kabul edilmesidir. BM İnsan Hakları Komitesi 16. Genel Yorumu ile 17. maddenin kapsamına açıklık getirmiştir[32]. Buna göre:

"Tüm insanların toplum içerisinde yaşamalarının sonucu olarak, özel hayatın gizliliğinin korunması kaçınılmaz şekilde görecelidir. Ancak, Sözleşme' den anlaşıldığı üzere yetkili kamu otoriteleri, bilinmesi toplumun çıkarlarının korunması açısından gerekli olan, bireyin özel hayatıyla ilgili bir bilgiyi öğrenme talebinde bulunabilmelidir. Kamu otoritelerinin, özel kişi ve kurumların bilgisayarlarda, veri bankalarında veya benzeri cihazlarda kişisel bilgileri toplaması veya saklaması hukuki düzenlemeye tabi olmalıdır. Devletler, bir kimsenin özel hayatına dair bilgilerin hukuken bu bilgilere sahip olma ve kullanma yetkisine sahip olmayanların eline geçmesini ve bu bilgilerin

[30] Vikipedi, http://tr.wikipedia.org/wiki/Birle%C5%9Fmi%C5%9F_Milletler (E.T. 04.06.2014).

[31] Küzeci, a.g.e. s.133.

[32] GEMALMAZ, Mehmet Semih., **Ulusal üstü İnsan Hakları Hukukunun Genel Teorisine Giriş**, İstanbul 2012, s. 434.

Sözleşme'nin amaçlarına aykırılık teşkil edecek şekilde kullanılmasını engellemek için etkili tedbirler almalıdır. Özel hayatın gizliliğinin en etkili şekilde korunabilmesi için, her birey kişisel dosyalarda veya veri tabanlarında kendisiyle ilgili bilgiler saklanmışsa bu bilgilerin ne tür bilgiler olduğunu ve ne amaçla saklandığını öğrenme hakkına sahiptir.

Ayrıca, her birey hangi kamu otoritelerinin, özel kişilerin veya kurumların bu dosyaları kontrol altında tuttuğunu veya tutabileceğini öğrenebilmelidir. Söz konusu dosyaların, yanlış kişisel bilgilere yer vermesi halinde veya bu bilgilerin hukuka aykırı şekilde toplanması veya kullanılması halinde her birey düzeltme veya bilgilerin ortadan kaldırılmasını talep etme hakkına sahiptir".

14 Aralık 1990 yılında kişisel verilerin korunması konusunda "Bilgisayarla İşlenen Kişisel Veri Dosyaları Hakkında Yönlendirici İlkeler" adını taşıyan bir belge[33] Birleşmiş Milletler tarafından kendisine bağlı devletler ve kuruluşlar için kabul edilmiştir[34].

Belgede kişisel verilerin korunmasına ilişkin ilkeler ayrıntılı bir şekilde açıklanmıştır. Aşağıda sözü edilen ilkeler ve kısa bir açıklaması verilmektedir[35]:

1) Yasallık ve Dürüstlük: Kişisel veriler kanuna aykırı ve dürüst olmayan yollarla toplanmamalı, toplanış amacına, temel hak ve özgürlüklerle ilgili ilkelere aykırı olarak kullanılmamalıdır.

2) Doğruluk: Toplanan verilerin doğruluğu kontrol edilmeli, doğru ve eksiksiz olarak saklanmalı, güncelliğini sağlamak için saklandığı süre zarfında düzenli olarak kontrole tabi tutulmalıdır.

3) Amacın Belirli ve Haklı Olması: Kişisel verilerin hangi haklı amaçla toplandığı başlangıçta kesin olarak belirlenmeli ve bu amaç bütün ilgililere açık olarak bildirilmelidir.

[33] Kılınç, a.g.e. s. 1111.

[34] Şimşek, a.g.e. s.16.

[35] TBD Raporu, s.5-6.

4) Algılı Kişilerin Erişme Hakkı: Kişisel veri ile ilgili olarak, kimliğini kanıtlamak koşulu ile kişi kendisi hakkında toplanan bilgilerin ne gibi bir isleme tabi tutulduğunu öğrenebilmeli ve bunların anlaşılabilir biçimdeki bir örneğini aşırı bir masraf ve zaman kaybı olmadan elde edebilmelidir.

5) Ayrımcılıktan Kaçınma: Kişinin etnik kökeni, ırkı, cinsel yasamı, dini veya felsefi inançları gibi duyarlıklı konularla ilgili bilgiler ancak yasanın izin verdiği haklı ve gerekli durumlarda toplanmalıdır.

6) İstisna Koyma Yetkisi: Görevli makamlara, ulusal 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 halükarda temel hak ve özgürlüklere aykırı olmaması gerekir.

7) Güvenlik: Kişisel verilerin toplanması, saklanması ve islenmesi ile görevli bütün kurum ve kişiler bu verilerin doğal afetler ve kazaların ve insanların isleyecekleri hata, kusur ve suçların yaratacağı tehlikelere karsı korunması için her türlü önlemi almalıdırlar.

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

9) Sınır Ötesi Veri Aktarımı: Kişisel verilerin saklanmakta olduğu ülkeden başka bir ülkeye aktarılması için her iki ülkenin ulusal mevzuatlarının bu aktarmaya izin vermesi yanında, verinin gönderileceği ülkenin bu veri için sağladığı korumanın verinin bulunduğu ülkede sağlanan korumadan daha aşağı düzeyde olmaması gerekir.

BM'nin Rehber İlkeleri, kişisel verilerin korunmasına ilişkin ilkelerin uygulamasını denetleyecek yetkili ve bağımsız bir veri koruma organının kurulmasını öngören ilk uluslararası hukuk belgesidir[36].

4. Avrupa Konseyi (AK)

a. Genel Olarak

5 Mayıs 1949 tarihinde kurulan Avrupa Konseyi tarafından, insan haklarının korunması amacıyla birçok hukuki metin hazırlanmıştır. Türkiye'nin de taraf olduğu ve bugün Türk Hukukunun en temel kaynaklarından biri olan Avrupa İnsan Hakları Sözleşmesi de Avrupa Konseyi tarafından hazırlanan metinlerden biridir. Keza Avrupa İnsan Hakları Mahkemesi de Avrupa Konseyi bünyesinde çalışan ve finanse edilen bir hukuksal koruma organıdır. İnsan haklarının korunması alanında en fazla katkı sağlayan kuruluşların başında gelmektedir[37].

b. Avrupa İnsan Hakları Sözleşmesi (AİHS)

İnsan haklarının tanımlanması ve güvence altına alınması için hazırlanarak 4 Kasım 1950 yılında kabul edilen Avrupa İnsan Hakları Sözleşmesinde[38] kişisel veri kavramı ve kişisel verilerin korunması düzenlenmemiştir. Sözleşmenin amacı II. Dünya savaşında yaşanan acı tecrübelerin tekrar yaşanmaması ve insan hak ve özgürlüklerin uluslararası alanda korunmasını sağlamaktır.

AİHS insan haklarının korunmasına etkinlik kazandırmak amacı ile uluslararası bir denetim mekanizması olarak Avrupa İnsan Hakları Mahkemesinin kurulmasını öngörmüştür. AİHM sözleşme ile garanti altına alınan hakların korunmasına gerek bireysel gerekse devlet başvuruları aracılığı ile işlerlik kazandırmaktadır[39].

AİHS kişisel verilerin korunması açık olarak düzenlenmemekle birlikte Avrupa İnsan Hakları Mahkemesinin bireyin özel hayatı ile ilgili bilgilerin korunması konusunu

[36] Şimşek, a.g.e. s.16, Küzeci, a.g.e. s.134

[37] Şimşek, a.g.e. s.16, Küzeci. a.g.e. s.134.

[38] Avrupa İnsan Hakları Sözleşmesi, http://www.anayasa.gov.tr/files/bireysel_basvuru/AIHS_tr.pdf

[39] Şimşek, a.g.e. s.30.

özel yaşam hakkını koruyan 8. madde kapsamında değerlendirerek verdiği kararlar ile kişisel verilerin korunması alanında örtülü bir hukuksal koruma kalkanı oluşturmuştur.

c. Kişisel Verilerin Otomatik İşleme Tabi Tutulma Sürecinde Bireylerin Korunmasına İlişkin 108 Sayılı Sözleşme

Bilgi ve iletişim teknolojileri alanında sağlanan gelişmeler, kişisel verilerin gizliliğinin güvence altına alınması konusunda mevcut hukuki ve teknik önlemlerin yetersizliği konusunda artan bir endişenin oluşmasına neden olmuştur. Dijital devrimin potansiyel etkisi güçlü bir şekilde görülmeye başlanmış ve kişisel verilerin kapsamlı bir şekilde işlenmesine karşı bireyleri korumak için önlemler alınması ihtiyacı ortaya çıkmıştır[40].

Temel hak ve özgürlüklerden her birinin korunması hususunun otomatik bilgi işleme konu teşkil eden kişisel nitelikteki verilerin sınırlar ötesi akışının yoğunluk kazanması karşısında bilhassa özel yaşama saygı hakkının korunmasının gerekliliğine inanarak, sınırları hesaba katmaksızın, haber alma özgürlüğü koruyarak özel yaşama saygının ve halklar arasındaki serbest bilgi akımının temel değerler olduğu hususundaki mutabakatın gerekliliğini kabul eden Konsey 1981 yılında "Kişisel Verilerin Otomatik İşleme Tabi Tutulma Sürecinde Bireylerin Korunmasına İlişkin 108 sayılı Sözleşme'yi kabul etmiştir.

108 sayılı Sözleşme, kişisel verilerin korunması konusunda kabul edilmiş olan bağlayıcı ilk uluslararası belgedir. Sözleşme'nin hazırlandığı dönemde OECD tarafından "Özel Yaşamın Korunması ve Kişisel Verilerin Sınır Ötesi Transferine İlişkin Rehber İlkeler" başlığıyla bir belge yayınlamıştır. Bu belge kişisel verilerin korunması konusunda uluslararası alanda kabul edilen ilk belge olmakla beraber, yalnızca tavsiye niteliğindedir ve bağlayıcı özelliği yoktur[41].

Ülkemiz, Sözleşme'yi 1981 yılında imzalamış ancak henüz onaylamamıştır. Sözleşme'nin onaylanmamasının nedeni Sözleşme'nin 4. maddesindeki düzenlemedir. Bu düzenlemeye göre, taraf devletler Sözleşme'deki ilkeleri uygulayabilmek için iç

[40] Atak, **Veri Koruma Yönergesi,** a.g.m. s.87.

[41] Atak, **Veri Koruma Yönergesi,** a.g.m. s.87.

hukuklarında gerekli önlemleri almalıdır. Bu önlemler en geç Sözleşme'nin taraf devlet açısından yürürlüğe girdiği tarihte alınmış olmalıdır. Türkiye'de kişisel verilerin korunmasına ilişkin yasa henüz yürürlüğe girmediği için Sözleşme'nin onaylanması mümkün olmamaktadır[42].

Sözleşmenin amacı birinci maddede belirtildiği üzere sözleşmeye taraf olan her ülkede uyruğu veya ikametgâhı ne olursa olsun tüm 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.

Sözleşme kamusal ve özel sektörde kişisel verilerin otomatik yollarla işlenmesine uygulanmasını öngörmektedir. Gerçek kişilere ait ve otomatik yollarla işlenen kişisel verilere koruma sağlaması Sözleşme'nin uygulama alanını daraltmıştır, bu durum Sözleşme'nin eksikliklerinden birisidir. Bununla birlikte, Sözleşmeye taraf olan devletlerin Sözleşmede öngörülen güvencelerden daha geniş güvenceleri kendi iç hukuklarında kabul etmeleri mümkündür[43].

Sözleşme kişisel verilerin korunması konusunda asgari gerekleri ortaya koymakta ve üye devletlerin sözleşmenin getirdiği korumadan daha geniş bir koruma sağlamalarını mümkün kılmaktadır[44].

Her ne kadar Sözleşme kişisel verilerin korunması alanında uluslararası bağlayıcılığı olma özelliğine ilk sözleşme ise de öncelikle üye devletlerin iç hukuklarında yasal veri koruma alanı oluşturmalarını öngörmektedir. Sözleşme kişisel verilerin korunmasında genel prensipleri belirleyerek üye ülkelere rehber olma ve bilinç oluşturma görevini ifa etmektedir. Kişisel verilerin korunmasında amaç bir olgu olarak veriyi korumaktan öte kişisel hak ve özgürlüklerin koruması olduğu gibi yapılan uluslararası düzenlemeler de özünde bir bilinç oluşturmayı amaçlamaktadır.

Bu Sözleşmenin üye ülkelerin hukuk sistemleri üzerinde çok sınırlı bir etkisi olduğu kimi yazarlarca belirtilse de önemini ve güncelliğini halen korumasına neden

[42] Atak, **Veri Koruma Yönergesi,** a.g.m. s.93.

[43] Atak, **Veri Koruma Yönergesi,** a.g.m. s. 94.

[44] Şimşek, a.g.e. s. 23.

olan bazı özellikleri dikkatten kaçmamalıdır. Sözleşmenin, Avrupa Konseyi üyesi olmayan devletlerin de imzasına açık olması, yalnızca üye devletler için değil Sözleşmeye taraf olan üçüncü ülkeler için de konuya ilişkin bir çerçeve sunmaktadır. Ayrıca Sözleşme, halen kişisel verilerin korunması alanında bağlayıcı olan tek uluslararası metindir. Bu nedenle konuya ilişkin en önemli kaynaklardan biri olma özelliğini sürdürmektedir[45].

Sözleşmenin Verilerin Niteliği başlıklı 5. maddesi otomatik bilgi işleme konu teşkil edecek kişisel nitelikteki veriler için bazı özellikler aramaktadır. Bunlar;

. 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 icabında güncel olmalıdır;

. İlgili kişilerin kimliklerini belirtecek bir biçim altında ve kaydedildikleri nihai amaç için gerekli görülen süreyi aşmayacak bir süre için muhafaza edilmelidir.

d. Kişisel Verilerin Otomatik Yöntemlerle İşlenmesi, Denetleyici Otoriteler ve Sınır Ötesi Veri Akışları Hakkında Bireylerin Korunması Sözleşmesine Ek Protokolü (181 sayılı Sözleşme)

Avrupa Konseyi 2001 yılında "Kişisel Verilerin Otomatik Yöntemlerle İşlenmesi, Denetleyici Otoriteler ve Sınır Ötesi Veri Akışları Hakkında Bireylerin Korunması Sözleşmesine Ek Protokolü (181 sayılı Sözleşme)", kabul etmiştir. Protokole ile taraf olan ülkelerde, kişisel veri koruma uygulamalarından sorumlu bağımsız ve özerk bir denetleyici otorite (kurum) oluşturulması öngörülmüştür[46].

[45] Küzeci, a.g.e. s. 142.

[46] Civelek, a.g.e. s.66.

Protokol kişisel verilere yeterli düzeyde koruma sağlamayan ülkelere ve uluslararası örgütlere transfer edilmesini yasaklamıştır[47].

181 sayılı Sözleşme kişisel verilerin Sözleşme 'ye taraf olmayan bir uluslararası örgüte ya da ülkeye gönderilmesine ancak bu devletin ya da örgütün eşit düzeyde bir koruma sağlaması koşulu ile izin verilmektedir. Ancak Sözleşme'ye taraf devletin iç hukuku veri sahibinin spesifik menfaatlerini korumak için ya da meşru menfaatleri, özellikle de önemli kamusal menfaatleri korumak için veri transferine izin veriyorsa bu şart aranmayacaktır[48].

Protokol, üye devletlerin iç hukukta aldıkları önlemlerin Sözleşme ve Protokol'de yer alan ilkelere uygunluğunu güvence altına almaktan sorumlu olacak bir ya da birden fazla kontrol makamı oluşturma zorunluluğu getirmektedir. Bu kontrol makamları özellikle araştırma ve müdahalede bulunma yetkisine ve aynı zamanda hukuki sürece dahil olma ve kişisel verilerin işlenmesi ile bağlantılı olarak bireylerin kendi temel hak ve özgürlüklerini korumak amacıyla yaptıkları şikayetleri inceleme yetkisine sahip olacaklardır. Kontrol makamlarının görevlerini tam bir bağımsızlık içinde yerine getirmeleri öngörülmüş, ancak verdikleri kararlara karşı mahkemelere başvurma olanağı tanınmıştır[49].

5. Avrupa Birliği (AB)

a. Genel Olarak

Avrupa Birliği, Birliğe üye devletlerde uygulanan çok çeşitli ulusal kanunlar, yönetmelikler ve idari hükümlerin varlığından dolayı kişisel verilerin işlenmesine dair başta kişisel mahremiyet hakkı olmak üzere bireylerin hakları ve özgürlüklerinin korunma seviyesindeki farklılıklar veri transferinde aksaklılara ve haksız rekabete neden olabileceği düşüncesinden hareketle değişik çalışmalar yapmıştır.

---

[47] Atak, **Veri Koruma Yönergesi,** a.g.m. s. 94.

[48] Atak, **Veri Koruma Yönergesi,** a.g.m. s.98.- Civelek, a.g.e. s.66

[49] Atak, **Veri Koruma Yönergesi,** a.g.m. s.98.

Üye devletler uzun bir hazırlık sürecinin sonucunda gerçek kişilerin temel hak ve özgürlüklerini korumak ve özellikle de kişisel verilerin işlenmesi nedeniyle özel yaşam hakkı alanında ortaya çıkabilecek hak ihlallerini önlemek, bu sırada üye devletlerin, kişilerin temel hak ve özgürlüklerini korumak gerekçesiyle, Birlik içinde kişisel verilerin özgür akışını sınırlamalarının ya da yasaklamalarının önüne geçilmek amacı ile temel hak ve özgürlükler ihlal edilmeksizin kişisel veri akışının sağlanabilmesi için üye devletlerin uyması gereken temel ilkeleri belirlemiştir[50].

Birlik düzeyinde üye Devletlerarasında verilerin korunması düzeyinin uyumlu hale getirilmesi ve sorunsuz bir şekilde işlev görmesi amacı ile aşağıda belirtilen iki ana yönerge kabul edilmiştir[51].

- Avrupa Parlamentosu ve Konseyinin 24 Ekim 1995 tarihli "Kişisel Verilerin İşlenmesi Sırasında Gerçek Kişilerin Korunması ve Serbest Veri Trafiğine İlişkin Yönergesi" (AT Verilerin Korunması Yönergesi, 95/46/AT).

- Avrupa Parlamentosu ve Konseyinin 12 Temmuz 2002 tarihli "Elektronik Komünikasyon Alanında Kişisel Özel Alanın Korunması ve Kişisel Verilerin İşlenmesi Hakkındaki Yönergesi" (Elektronik Komünikasyon Verilerin Korunması Yönergesi, 2002/58/AT).

Ayrıca kişisel verilerin korunması konusunda Avrupa Konseyi Bakanlar Komitesi'nin çok sayıda kararı ve tavsiye kararı mevcuttur. Bu amaçla Avrupa Konseyi Bakanlar Komitesi, 26.09.1973 tarih ve (73) 22 sayılı "Özel Kesimdeki Elektronik Veri Bankalarına Karşı Bireylerin Gizliliğinin Korunması" ve 20.09.1974 tarih ve (74) 29 sayılı "Kamu Kesimindeki Elektronik Veri Bankalarına Karşı Bireylerin Gizliliğinin Korunması" kararlarını kabul etmiştir. Ardından da 25.10.1985 tarih ve (85) 20 sayılı "Doğrudan Pazarlama Amacıyla Kullanılan Kişisel Verilerin Korunması"; 23.01.1986 tarih ve (86) 1 sayılı "Sosyal Güvenlik Amacıyla Kişisel Verilerin Korunması"; 17.09.1987 tarih ve (87) 15 sayılı "Güvenlik Alanında Kişisel Verilerin Kullanılmasının

[50] Atak, **108 Sayılı Sözleşme,** a.g.m. s. 204.

[51] Şimşek, a.g.e. s. 36.

Düzenlenmesi";18.01.1989 tarih ve (89) 2 sayılı "İstihdam Amacıyla Kullanılan Kişisel Verilerin Korunması"; 13.09.1990 tarih ve (90) 19 sayılı "Ödeme ve Diğer Muameleler İçin Kullanılan Kişisel Verilerin Korunması"; 09.09.1991 tarih ve (91) 10 sayılı "Kamu Otoritelerinin Sahip Olduğu Kişisel Verilerin Üçüncü Kişilere Bildirilmesi;7.02.1995 tarih ve (95) 4 sayılı "İletişim Hizmetleri Alanında Kişisel Verilerin Korunması (özellikle de telefon hizmetleri alanında)", 13.02.1997 tarih ve (97) 5sayılı "Tıbbi Verilerin Korunması"; 30.09.1997 tarih ve (97) 18 sayılı "İstatistik Amaçlarla Toplanan ve İşlenen Kişisel Verilerin Korunması"; 23.02.1999 tarih ve(99) 5 sayılı "İnternette Gizliliğin Korunması"; 18.09.2002 tarih ve (2002) 9 sayılı "Sigorta Amacıyla Toplanan ve İşlenen Kişisel Verilerin Korunması" hakkında tavsiye kararlarını kabul etmiştir[52].

b. Avrupa Parlamentosu ve Konseyinin 24 Ekim 1995 tarihli "Kişisel Verilerin İşlenmesi Sırasında Gerçek Kişilerin Korunması ve Serbest Veri Trafiğine İlişkin Yönergesi (VKY)

Teknolojide yaşanan hızlı gelişmeler karşısında, 108 No.lu Sözleşme, günün ihtiyaçlarına cevap veremez hale gelmiş, bu nedenle bireyin özel alanının ve kişisel verilerinin korunması için kapsamlı ve güncel bir hukuk metnine ihtiyaç duyulmuştur. Ayrıca 108 No.lu Sözleşmenin 4. maddesine rağmen, imzacı devletlerin iç hukuk sistemlerindeki hukuki düzenlemeler arasında farklılıklar bulunması nedeniyle bu farklılıkların giderilmesi ve kişisel verilerin korunması konusunda AB içerisinde uyumlu bir sistem oluşturulması ihtiyacı da doğmuştur[53]. Komisyon, bu çeşitliliği "tek pazar" düşüncesine karşı ciddi bir engel olarak görmüştür. Bu nedenle AB Komisyonu'nun hazırladığı Yönerge'nin birincil amacı, üye devletlerarasındaki veri korunmasına ilişkin farklılıkların ortadan kaldırılmasıdır. Nitekim AB'yi kuran Antlaşmanın 7/a maddesi uyarınca malların, kişilerin, hizmetlerin ve sermayenin serbest dolaşımına olanak tanıyan bir iç pazar oluşturulmalı ve işleyebilmelidir. Ancak kişisel verilerin bir üye devletten diğerine serbestçe dolaşımının yanında bireylerin temel

[52] KAYA Cemil., **İdare Hukukunda Bilgi Edinme Hakkı**, Seçkin Yayıncılık, Ankara, Mayıs 2005. s. 94.

[53] Küzeci, a.g.e. s. 164.

haklarının korunması gerektiği de unutulmamalıdır. 95/46/AT Yönergesi, bu ihtiyaçlara cevap vermek üzere hazırlanmıştır[54].

Yönergenin hazırlanması sürecinde değişik menfaat gruplarının, özellikle de bankacılık ve doğrudan pazarlama sektörlerinin yoğun tepkileriyle karşılanmıştır. Bunlar kişisel verileri kullanmaları konusuna getirilen sınırlamaların derecesi ve bu kurallara uyulmasının yaratacağı potansiyel maliyet konusundaki endişelerini dile getirmişlerdir. Yönerge bu alanda yapılan uzun tartışmalardan sonra ancak Ekim 1995'te kabul edilmiştir[55].

Yönergenin 1. maddesinde Yönergenin amacının, üye devletler içerisinde uyumlu bir hukuksal düzen yaratılması ve kişisel verilerin korunması sırasında kişi hak ve özgürlüklerinin ve özellikle kişisel verilerin korunması konusunda, üye devletlerde geçerli olacak asgari veri koruma ölçütlerinin belirlenmesi olduğu vurgulanmıştır. Aynı maddenin ikinci fıkrasında yer alan ve üye devletler arasında serbest veri trafiğinin yasaklanamayacağını ve sınırlandırılamayacağını da öngören düzenleme ise Yönerge'nin gerçek amacını ortaya koymaktadır. Yönergenin gerçek amacı; gerçek kişilerin korunması, özellikle özel hayatın korunması gibi sebeplerle veri trafiğinin engellenmesinin önüne geçmek, veri akışının önündeki engelleri kaldırmak, serbest veri akışını sağlamaktır[56].

Yönergede belirtilen bu amaçlara, Birliğe üye bütün devletlerin iç hukuklarında Yönergede belirlenen ilkeler doğrultusunda düzenleme yapılması ile ulaşılacaktır. Üye devletler iç hukuklarını Yönerge ile uyumlu hale getirmek zorundadırlar. Bunun önemi Yönergenin 7 No'lu gerekçesinde belirtilmiştir. Bu gerekçeye göre, üye devletlerde kişisel verilerin işlenmesi konusunda farklı koruma düzeylerinin olması, verinin bir üye devletten diğerine akışını engelleyebilir. Bu durum Birlik düzeyinde belli ekonomik faaliyetlerin izlenmesinde bir engel oluşturabilir. Bu riskin önüne geçilebilmesi için ne yapılması gerektiği de Yönergenin 8 No'lu gerekçesinde şöyle belirtilmiştir; kişisel verilerin akışının önündeki engelleri kaldırmak için, kişisel verilerin işlenmesi

[54] Küzeci, a.g.e. s. 164.

[55] Atak, **Veri Koruma Yönergesi,** a.g.m. s, 204.

[56] BAŞALP, Nilgün., **Kişisel Verilerin Korunması ve Saklanması**, Yetkin Yay., Ankara, 2004, s.30.

konusunda temel hak ve özgürlükler açısından sağlanan korumanın düzeyi tüm üye devletlerde eşit olmalıdır[57].

Veri Koruma Yönergesi'nin kapsamı Yönerge'nin 3. maddesinde açıklanmıştır.

Buna göre Yönerge; tamamı ya da bir bölümü otomatik olarak işlenen kişisel verilere ve otomatik olmayan yollarla işlenen verilerden bir dosyalama sistemine kaydedilenler veya kaydedilebilecek olanlar için uygulanır. Günümüzde hemen hemen tüm verilerin, bilgisayar ortamına kaydedilip işlendiği, eski kayıtların da bilgisayar sistemlerine aktarıldığı dikkate alındığında, Yönerge'nin bütün kişisel verileri kapsadığı söylenebilir.

AB veri koruma modelinin kilit özelliği *zorlayıcılığıdır.* AB üyesi devletlerin tamamında kişisel verilerin korunmasını güvence altına alan kuralların uygulanmasını sağlayacak birimler bulunmaktadır. Yönerge ile özellikle önleyici bir korumanın sağlanması hedeflenmektedir[58].

Veri koruma hukukunun temel ilkeleri bölümünde konu ayrıntılı olarak inceleneceğinden dolayı burada konuyu kısaca özetlemek ile iktifa ediyoruz.

c. Avrupa Parlamentosu ve Konseyinin 12 Temmuz 2002 tarihli "Elektronik Komünikasyon Alanında Kişisel Özel Alanın Korunması ve Kişisel Verilerin İşlenmesi Hakkındaki Yönergesi" (Elektronik Komünikasyon Verilerin Korunması Yönergesi, (2002/58/AT)

Avrupa Parlamentosu ve Konseyi 2002 yılı ortalarında Elektronik Komünikasyon alanında Özel Alanın Korunması ve Kişisel Verilerin İşlenmesine İlişkin Yönergeyi (2002/58/AT) kabul etmiştir. 2002 yılında kabul edilen Elektronik Komünikasyon Verilerin Korunması Yönergesi Avrupa Topluluklarının 1995 tarihli genel Verilerin Korunması Yönergesini elektronik komünikasyon alanında tamamlamaktadır. Yönergesinin amacı, özellikle elektronik komünikasyon alanında temel hak ve özgürlüklere riayet etmektir. Yönerge özellikle Avrupa Birliği Temel

[57] Atak, **Veri Koruma Yönergesi,** a.g.m. s. 204.

[58] Küzeci, a.g.e. s. 180.

Haklar Şartında yer alan özel yaşamın gizliliği ve verilerin korunması haklarına saygı gösterilmesi gerekliliğini vurgulamaktadır. Yönergede ayrıca uluslararası sözleşmelerde ve özellikle Avrupa İnsan Haklan Sözleşmesindeki haberleşmenin gizliliği hakkına da yollamada bulunulmaktadır. Yine Elektronik Komünikasyon Yönergesinde özel olarak düzenlenmeyen konularda 95/46/AT Verilerin Korunması Yönergesinin geçerli olacağı belirtilmektedir[59].

[59] Şimşek, a.g.e. s. 53.

II. BÖLÜM

KİŞİSEL VERİLERİN KORUNMASI HUKUKUNUN TEMEL İLKELERİ

A. GENEL OLARAK

Küreselleşme çağında teknoloji ve bilgi alanında meydana gelen bu gelişmeler, devletler üstü alanda da kişisel verilerin korunması gereğini ortaya çıkarmıştır. Bu düşüncenin temelinde ise, esas olarak devletin bireyin kişisel verilerine sınırsız olarak müdahale edebilme imkânı karşısında bireyin korunması düşüncesi ve yine bireyin bilgi toplumuna katılma hakkı bulunmaktadır[60]. Bu nedenle veri işleme sistemleri insana hizmet etmek üzere tasarlanmalı; başta kişisel mahremiyet olmak üzere, temel haklarını ve özgürlüklerini korumalı ve bireylerin ekonomik ve sosyal ilerlemesine, refahına ve ticari genişlemeye katkıda bulunmalıdır.

Kişisel verilerin korunmasına ilişkin uluslararası alanda yapılan çeşitli düzenlemelerde yer alan yaklaşımlardaki farklılığa rağmen konuya ilişkin düzenlemelerde ortak olan bazı temel ilkeler bulunmaktadır[61]. Bu ilkeler birçok metinde yer almakla birlikte söz konusu ilkelerin belirlenmesinde temel metin AB Veri Koruması Yönergesi (VKY) kabul edilmektedir. Çünkü bu alanda kabul edilen ilk önemli belge, Avrupa Birliğinin iki önemli organı olan Avrupa Parlamentosu ve Konseyinin kabul etmiş olduğu, "Kişisel Verilerin İşlenmesi Sürecinde Kişilerin Korunması ve Bu Verilerin Özgür Dolaşımına İlişkin Yönerge"dir[62].

---

[60] Şimşek, a.g.e. s. 35.

[61] Küzeci, a.g.e. s.225.

[62] Atak, **Veri Koruma Yönergesi,** a.g.m. s.201.

Bu ilkelerin birbirlerinden kesin çizgilerle ayrılması oldukça zordur. Kimi ilkeler diğerlerine kaynaklık eden genel bir nitelik sergilerken, pek çoğu da birbirini tamamlamaktadır. Bu nedenle yapılan açıklamalar değerlendirilirken bu ilkelerin birbirleri ile olan yakın ilişkisi unutulmamalıdır[63].

B. VERİLERİN KALİTELİ OLMASI İLKESİ

Verilerin kaliteli olması ilkesinin kriterlerini belirleyen 95/46/ AT sayılı Yönerge'nin 6. maddesi kişisel verilerin;

- Hukuka ve dürüstlük kurallarına uygun işlenmesini,

-Belirli, açık ve meşru amaçlar için toplanmasını,

- Toplanma ve daha sonrasında işlenme amaçlarına uygun, ilgili ve aşırı olmamasını,

-Doğru ve eğer gerekli ise güncel olarak tutulmasını,

- Amacın gerektirdiğinden daha uzun bir süre tutulmamasını öngörmektedir[64].

1. Hukuka ve Dürüstlük Kuralına Uygun Olma

Hukuka uygun olma kişisel verilerin işlenmesinde yasalarla ve diğer hukuksal düzenlemelerle getirilen ilkelere uygun hareket edilmesi zorunluluğunu, dürüstlük kuralına uygun olma ilkesi (dürüstlük kuralı, sadece Türk Medeni Kanunu'nun değil hukuk düzeninin tamamını kapsayan genel ilkedir[65].) ise veri denetçilerinin, veri işlemedeki hedeflerine ulaşmaya çalışırken, ilgili kişilerin çıkarlarını ve makul beklentilerini dikkate almalarını ve şeffaf olmalarını kapsar[66].

Bu ilke ile Yönerge'de işleme olarak tanımlanan; toplama, kaydetme, silme veya tahrip etme, engelleme, birleştirme veya sıralama, sağlama ya da dağıtma, iletmeyle

[63] Küzeci, a.g.e. s.226.

[64] Küzeci, a.g.e. s.212.

[65] http://www.turkhukuksitesi.com/mevzuat.php?mid=678 , (E.T. 04.06.2014)

[66] Küzeci, a.g.e. s.213.

açıklama, organizasyon, depolama, adaptasyon veya değiştirme, kurtarma, danışma gibi otomatik ya da otomatik olmayan araçlarla yapılan herhangi bir faaliyet veya faaliyet dizisini kasteden tüm faaliyetler esnasında hukuka ve dürüstlük kurallarına uygun hareket edilmesi hedeflenmiştir[67].

Hukuka ve dürüstlük kurallarına uygun işleme ilkesi, verilerin işlenmesinin saydamlığı açısından kişisel verilerin işlenmesi sürecinin başından sonuna kadar var olması gereken bir ilkedir. Dürüstlük kuralının hukuki işlemler açısından uygulanması, söz konusu *işlemenin* öncesi ve sonrasında, tarafların birbirinden beklemeye haklı oldukları konularda aldatılmamalarını olarak yorumlanmaktadır[68].

2. Amaca Uygun Toplanma

Verilerin kaliteli olması ilkesi, her şeyden önce verilerin işlenmesinde veri toplama amacına bağlı kalınmasını ve kullanım amacının önceden belirli olmasını ifade etmektedir. *Kişisel verilerin kullanılma amacının önceden ilgili tarafından bilinmesi, ilgilinin kendi verileri üzerinde kontrol imkânını vermekte ve kişisel veriler bakımından önleyici korumayı sağlamaktadır*[69].

Bütün temel veri koruma düzenlemelerinde kabul edilen bu ilkenin üç parçadan oluştuğu görülmektedir[70]:

-Verilerin toplanma amacının belirli ve açık olması;

-Verilerin toplanma amacının meşru olması;

- Verilerin daha sonra işlenme amaçlarının, toplanma amacı ile uyumlu olması.

Verilerin toplanma amacının belirli ve açık olması, her şeyden önce bu konuya ilişkin hukuksal düzenlemelerde belirsiz ifadelerden kaçınılmasını gerektirir. Ayrıca

[67] http://www.ihop.org.tr/dosya/coe/EC_DIRECTIVE_95_46_Kisisel_Veriler.pdf , (E.T. 04.06.2014).

[68] ÖZDEMİR Hayrünnisa., **Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması,** Seçkin ANKARA 2009, s.137.

[69] Şimşek, a.g.e. s.83.

[70] Küzeci, a.g.e. s.214.

verilerin anonimleştirilmeden yalnızca depolanmak üzere, bir başka anlatımla olası kullanımdan hareketle tutulması da bu ilkeye aykırılık oluşturur.

Bu ilke gereğince kişisel verilerin toplanma ve kullanma amacının mümkün olduğunca tam olarak tanımlanması ve açıkça belirlenmesi zorunludur. Bireye ilişkin kişisel veriler toplanırken, veri işlem sorumlusunun belirli bir amacının bulunup bulunmadığı veya hangi amaçlara sahip olduğu hususunda herhangi bir tereddüt bulunmamalıdır. Bu itibarla verilerin korunmasına izin veren yasal düzenlemelerdeki somut olmayan genel veya belirsiz ifadelerden kaçınılmalıdır. Çünkü bu tür düzenlemeler, kişisel verilerin toplanma amacının belirli ve sınırlı olması ilkesi ile bağdaşmamaktadır. Aynı şekilde kişisel bir verinin anonim olmayan bir şekilde stok yapmak üzere veya somut bir amaç olmaksızın işlenmesi de genel kişilik hakkıyla bağdaşmadığı gibi, kullanım amacının önceden yasayla somut olarak ve açıkça belirlenmiş olması ilkeleri ile de bağdaşmamaktadır. Bu nedenle belirli ve somut bir yasal amaçtan yoksun olarak kişisel verileri toplamak üzere oluşturulan veri depoları amaca bağlılık ilkesine aykırıdır[71].

Yönerge 7. maddede aşağıda belirtilen veri işlemeyi meşru kılan ölçütler belirlenmiştir[72].

- Veri öznesi açık, kesin ve net bir biçimde rızasını vermişse,

- İşleme, bir sözleşme yapmadan önce veri öznesinin talebi üzerine önlem almak için ya da veri öznesinin taraf olduğu bir sözleşmenin yerine getirilmesi için gerekliyse,

- İşleme denetleyicinin konusu olan bir yasal yükümlülüğe uyum için gerekirse,

- İşleme, veri öznesinin hayati menfaatlerini korumak için gerekliyse,

- İşleme, verilerin açıklandığı üçüncü bir şahıs veya denetleyiciye yetki veren kamu makamının uygulamasında veya kamu menfaatine yapılan bir görevin yerine getirilmesi için gerekliyse,

[71] Şimşek, a.g.e. s.84.

[72] http://www.ihop.org.tr/dosya/coe/EC_DIRECTIVE_95_46_Kisisel_Veriler.pdf , (E.T. 04.06.2014).

- İşleme, bu tür menfaatlerin, 1. madde kapsamında koruma gerektiren veri öznesinin temel hak ve özgürlükleriyle ilgili menfaatleri çiğnemesi haricinde, verilerin açıklandığı üçüncü şahıs veya şahıslar tarafından ya da denetleyici tarafından takip edilen meşru menfaatlerin amaçları için gerekliyse işlenebilecektir.

Kişisel verilerin belirli bir amaç olmaksızın "bir gün gerekli olursa" düşüncesiyle tutulması, bütün bir toplumu potansiyel suçlu konumuna sokar. Bu, kişileri kendilerini özgürce ifade etmekten alıkoyabilir. Sonuçta zarar görecek olan kişinin maddi ve manevi bütünlüğü, kişiliğini geliştirme hakkı, bireysel özerkliği ve masumiyet karinesi gibi çağdaş demokratik toplumun temel değerleridir. AB Veri Koruma Yönergesi 'ne göre veri denetçileri, kişisel verilerin işlenme amacını tam olarak belirlemeli ve bunu ilgili kişi ile ulusal denetim birimine bildirmelidir. Dolayısıyla bu gereklilik ilgili kişinin bilgilere erişim hakkı ve veri koruma görevlisinin bildirim yükümlülüğü ile de yakından ilişkilidir. Bu nedenle örneğin kullanıcılarının kişisel bilgilerini toplayan bir web sitesi, onları toplama amacı konusunda bilgilendirmeli ve verileri bu amaç dışında kullanmamalıdır. Bu kapsamda web sitesinin bilgileri pazarlama amacıyla kullanacağını belirtmediği durumlarda, kullanıcılarına e-posta reklamları göndermesi ilkenin ihlali anlamına gelecektir[73].

3. Toplanma ve Sonrasında İşlenme Amaçlarına Uygun, İlgili Bulunma, Aşırı Olmama

AB Yönerge'sinin 6/1,c bendi "toplandığı ve/veya ayrıca işlendiği amaçlara ilişkin olarak yeterlidir, ilgilidir ve bu amacı aşmaz" hükmünü düzenlemektedir. Verilerin yaratılması, kaydedilmesi ve kullanılması, esas olarak kullanma amacı için gerekli olan minimum düzeyle sınırlı olmalıdır[74].

Bu ilke uyarınca veri denetçisi, öncelikle amaçlarına ulaşabilmek için kişisel verilerin mutlaka gerekli olup olmadığını saptamalıdır. Eğer kişisel veriler kullanılmadan da hedefe ulaşılabilecekse öncelikle bu yol tercih edilmelidir. Ancak elbette kişisel verilerin kullanımının hedefe ulaşılması için zorunlu olacağı durumlarda

[73] Küzeci, a.g.e. s.215.

[74] Şimşek, a.g.e. s.85.

bulunacaktır. Böylesi durumlarda ise veri denetçisi amaca ulaşmak için gerekli olan en az sayı da veriyi kullanmalıdır. "Veri ekonomisi" olarak da ifade edebileceğimiz bu yaklaşımla gerekli olandan fazla miktardaki kişisel verinin kullanımı önlenmektedir. Eğer aynı veri birden fazla amaç için kullanılıyorsa yine bunların gerekli olan kadarıyla sınırlandırılması gerekir. Örneğin iş başvurusu formları, müşteri bilgi kartları ya da internet ortamında kayıt sayfaları hazırlanırken bu ilkeye dikkat edilmeli ve amaca ulaşmak için gerekli olandan fazla bilgi istenmemelidir[75].

4. Doğru ve Eğer Gerekli İse Güncel Olarak Tutulma

Yönerge 6/1/d maddesi üye devletlerin, kişisel verilerin doğru ve gerektiği yerde güncel tutulmasını, toplanma ve sonrasındaki işlenme, silinme veya düzeltilme amaçlarını göz önünde tutarak verilerin yanlış veya eksik olmamasını sağlayacak tüm makul önlemleri alması gerektiğini belirtmiştir[76].

Burada işaret edilmesi gereken belki de ilk husus: belirtilen ilkenin erişim hakkı ile yakın ilişkisidir. Nitekim aşağıda da üzerinde durulacağı gibi, bilgilere erişilememesi durumunda, kişisel verilerin doğruluğunun saptanması da hemen hemen olanaksızdır. Kişisel veriler, bağlantılı olduğu kişiyi niteleyen, onun kişiliği ile sıkı sıkıya bağlı bilgiler olduğuna göre şurası açıktır: bu bilgilerin doğruluğunu en iyi şekilde denetleyebilecek taraf yine ilgili kişi olacaktır. Bilgilerine ulaşamayan kişinin ise bunların doğruluğunu denetleyebilmesi olanak dışıdır. İkinci olarak kişisel verilerin güncel tutulmasının ne zaman "gerekli" olacağı belirlenmelidir. Bu saptamayı yaparken şu nokta gözden kaçmamalıdır: kişisel verilerin doğru ve güncel tutulması veri denetçisine yönelik bir yükümlülüktür ve devredilemez. Ancak bu ilkeyi kişisel verilerin güncelliğini saptayabilmek için veri denetçilerinin zorla ve sürekli olarak ilgili kişilerin içinde bulunduğu yeni durumları araştırması olarak algılamak makul değildir. Bu durumda ilgilinin kişisel bilgilerine ilişkin bir değişiklik oluştuğunda veri denetçisini bilgilendirmesi gerektiğini söylemeliyiz. Bu ilkeye uyumluluğu sağlayabilmek için veri denetçileri ilgili kişilerin bilgilerine ulaşabileceği ve onları denetleyebileceği bir sistem

[75] Küzeci, a.g.e. s.220.

[76] http://www.ihop.org.tr/dosya/coe/EC_DIRECTIVE_95_46_Kisisel_Veriler.pdf, (E.T. 04.06.2014).

oluşturabilirler[77].

5. Amacın Gerektirdiğinden Daha Uzun Süre Tutulmama

Kişisel verilerin gerektiğinden uzun süre tutulmaması gerekir. AB Veri Koruma Yönergesi'nin 6/1,e hükmü uyarınca, ilgili kişinin teşhis edilmesine olanak tanıyacak şekilde, kişisel verilerin toplandığı veya daha sonra işlendiği amaçlar için gerekli olandan daha uzun süre tutulmaması gerekir. Bu, kişilerin *unutulma hakkı (unutulma hakkı, bireyin başta internet olmak üzere dijital dünyadaki izlerinin başka bir ifadeyle geçmişinin kendi talebiyle silinip silinemeyeceği tartışmasının bir sonucu olarak değerlendirilmelidir[78].)* olarak nitelendirilebilir. Her şeyden önce kişisel verilerin tutulmasının kendi başına potansiyel bir risk yarattığı unutulmamalıdır. Aşağıda da değinileceği üzere veri güvenliği sağlanması zorunlu, ancak pek de kolay olmayan bir gerekliliktir. Bu durumda verilerin tutulduğu sürecin tamamında veri güvenliğine ilişkin tehlikeler varlığını sürdürecektir. AİHM de çeşitli kararlarında verilerin gerekenden uzun süre tutulmasının sakıncalarına dikkat çekmiştir. Şüphelilerin parmak izi, DNA profili ve hücre örneklerinin ulusal bir veri tabanına aktarılmasına ilişkin bir başvuruyu değerlendirdiği kararında Mahkeme, herhangi bir kayıt altına alınabilir suç dolayısıyla herhangi bir yaştaki herhangi bir kişinin parmak izi ve DNA örneklerinin belirsiz bir süre saklanmasına izin veren uygulamayı Sözleşme'nin 8/1 hükmüne aykırı bulmuştur[79].

C. ÖZEL KATEGORİLERDEKİ VERİLERİN (HASSAS VERİLERİN) ÖZEL OLARAK KORUNMASI İLKESİ

Yönerge, kişisel veriler içinde yer alan hassas nitelikteki verileri ayrı bir başlık altında ele almış ve bunların işlenmesini yasaklamıştır. Ancak bu yasak mutlak değildir. Yasağın istisnaları madde içinde açıklanmıştır[80]. Bu ilke, ilgili kişi açısından "hassas" sayılan bazı veri türlerinin işlenmesini diğerlerine göre daha sıkı bir denetim altına alma

[77] Küzeci, a.g.e. s.226.

[78] GÜLENER Serdar., **Dijital Hafızadan Silinmeyi İstemek: Temel Bir İnsan Hakkı Olarak "Unutulma Hakkı"** http://tbbdergisi.barobirlik.org.tr/m2012-102-1218 (E.T. 04.06.2014).

[79] Küzeci, a.g.e. s.228.

[80] Atak, **Veri Koruma Yönergesi,** a.g.m. s.208.

düşüncesine dayanır. Pek çok uluslararası ve ulusal metinde hassas verilerin özel olarak korunması yaklaşımı benimsenmiştir. AB Yönergesi, AK Sözleşmesi, BM Rehber İlkeleri hassas verilere özel koruma öngörürken, OECD Rehber İlkeleri ve APEC Çerçeve Belgesi'nde belirli türdeki verilere yönelik özel bir koruma geliştirilmemiştir.

AB Yönergesi'nin 8. maddesine göre özel kategorideki kişisel verilerin işlenmesi kural olarak yasaktır. Bunlar ilgili kişinin,

- ırksal veya etnik kökenini,

- siyasal görüşünü,

- dinsel ya da felsefi inancını,

- sendika üyeliğini,

- sağlık ya da cinsel yaşamını belirli eden verilerdir.

Bunun yanında kişilerin ceza mahkûmiyetine ilişkin veriler de her durumda korumadan yararlanırken, idari ve adli mahkûmiyetlere ilişkin verilerin bu kapsamda sayılıp sayılmayacağı üye devletin takdirine bırakılmıştır. Çeşitli metinlerde bu sayımda farklılıklar dikkat çekse de genel olarak bu konulara ilişkin bilgilerin hassas veriler olarak kabul edildiği görülür[81].

Özellikle ilgili kişi hakkında ayrımcılık yapılmasına yol açabilecek hassas verilerin toplanamaması ya da sınırlı koşullar altında işlenebilmesi ilkesi, kişisel verilerinin toplanması ve işlenmesi sırasında bireyin özel olarak korunmasına hizmet etmektedir. Bu nedenle kişinin etnik kökeni, politik düşünceleri, ideolojik kanaatleri, dinsel veya felsefi inançları, sendikaya aidiyeti, sağlık veya cinsel durumu gibi hassas verileri özel olarak korunmak zorundadır. Bu tür verilerin işlenmesi kural olarak yasak olup bunlar ancak yasal bir temelle veya ilgilinin rızası ile işlenebilecektir[82].

Veri işlem sorumluları hem hassas nitelikteki verileri hem de bu niteliği taşımayan verileri her durumda dürüstlük kuralına ve hukuka uygun olarak işlemek

[81] Küzeci, a.g.e. s. 250.

[82] Şimşek., a.g.e. s. 86.

zorunda oldukları için verilerin iki farklı kategori içinde ele alınması gereksiz bir zorlaştırma olarak değerlendirilebilir. Ancak bu yöndeki düzenleme ile hassas veriler açısından daha güçlü bir koruma sağlanmış olmaktadır[83].

İçinde bulunduğumuz bilgi çağında pek çok alanda, hatta belki hemen hemen her alanda, verilere gereksinim duyulduğu açıktır. O halde verilerin işlenmesinden doğacak zarar ile yarar arasında bir dengenin kurulması gerekir. Nitekim çeşitli yerlerde belirttiğimiz üzere, kişisel verilerin korunması hukukunun temeli de bu düşüncedir. Bu saptamadan hareketle, kişisel verilerin mutlak olarak korunmasından söz edilemez. Dengenin sağlanabilmesi, yararın derecesi ve tehlikenin şiddetini de dikkate almayı gerektirdiğinden, bazı verilerin diğerlerine göre daha yüksek oranda korunmasını yadırgamamak gerekir[84].

Özel nitelikteki (hassas) verilerin işlenmesi kural olarak yasak olmakla birlikte, bu kurala Yönergede (95/46/AT) bir takım istisnalar getirildiği görülmektedir. Bu çerçevede;

- İlgili kişinin açıkça bu tür verilerin işlenme rıza göstermesi durumunda bu veriler işlenebilir.

- İlgili Devlet hukuku tarafından yeterli garantilerin öngörülmesi kaydıyla iş hukuku alanında veri işlem sorumlusunun hak ve yükümlülüklerine riayet etmek için gerekli olması halinde bu veriler işlenebilir.

- Fiziksel veya hukuksal nedenlerle ilgili kişi rıza verebilecek durumda değilse, ilgili kişinin veya üçüncü kişinin hayati önem taşıyan menfaatlerinin korunmasının zorunlu olduğu durumlarda söz konusu veriler işlenebilir.

- Ticari amaca yönelmemiş, politik, felsefi dinsel veya sendikal nitelikteki vakıf dernek veya diğer organlar vasıtasıyla kendi faaliyet alanları içerisinde olmak ve uygun garantiler sağlanmak kaydıyla bu verilerin işlenmesi mümkündür. Burada ancak söz

[83] Atak, **Veri Koruma Yönergesi,** a.g.m. s. 209.

[84] Küzeci, a.g.e. s. 251.

konusu kuruluşların üyesi olan veya kuruluşun faaliyet amaçlan çerçevesinde sürekli ilişki içinde bulunduğu kişiler hakkındaki verilerin ilgilinin rızası olmadan üçüncü kişilere devredilebilmesi söz konusudur.

- Özel kategorilerdeki veriler, şayet ilgili tarafından açık bir şekilde kamuya açılmışsa veya hukuksal taleplerin mahkeme önünde kullanılması veya savunma yapılması için zorunluluk bulunuyorsa işlenebilirler.

- Yine suçlara, ceza mahkûmiyetlerine ve güvenlik tedbirlerine ilişkin verilerin işlenmesi ancak resmi makamların gözetimi altında veya yeterli garantileri öngören ulusal düzenleme çerçevesinde mümkündür. Ceza hukukuna ilişkin mahkûmiyetlerin bütün halinde kaydedilmesi ise ancak resmi makamların denetimi altında söz konusu olabilir[85].

- Sağlığın korunması, tıbbi teşhis, tedavi veya sağlık hizmetlerinin yönetimi için gerekli ise bu veriler, münferit devletlerin yasal düzenlemeleri çerçevesinde meslek yükümlülüğüne tâbi hekimler veya sır saklama yükümlülüğü altındaki diğer personel tarafından yapılan faaliyetler bakımından işlenme yasağına tabi değildir.

11.10.2011 tarihli ve 663 sayılı Sağlık Bakanlığı ve Bağlı Kuruluşlarının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname'nin 47'nci maddesi ile Sağlık Bakanlığının bilgi toplama, işleme ve paylaşma yetkisine yönelik düzenleme yapılmıştır. Buna göre; 47. maddenin 1. fıkrasıyla, Bakanlık ve bağlı kuruluşlarına, mevzuatla kendilerine verilen görevleri, e-devlet uygulamalarına uygun olarak daha etkin ve hızlı biçimde yerine getirebilmek için, bütün kamu ve özel sağlık kurum ve kuruluşlarından; sağlık hizmeti alanların, aldıkları sağlık hizmetinin gereği olarak ilgili sağlık kurum ve kuruluşuna vermek zorunda oldukları kişisel bilgileri ve bu kimselere verilen hizmete ilişkin bilgileri her türlü vasıtayla toplama, işleme ve paylaşma yetkisi verilmiştir. Maddenin 2. fıkrasında, Bakanlık ve bağlı kuruluşlarının işlediği kişisel sağlık verilerini ilgili üçüncü kişiler ve kamu kurum ve kuruluşları ile ancak bu kişi ve kurumların bu verilere erişebileceği hususunda kanunen yetkili olması halinde ve görevlerini yapmalarına yetecek derecede paylaşabilecekleri belirtilmiştir. Maddenin 3.

[85] Şimşek, a.g.e. s. 87.

fıkrasında ise, *"Bakanlık ve bağlı kuruluşları, mevzuatla kendilerine verilen görevleri yerine getirebilmek için gereken bilgileri, kamu ve özel ilgili bütün kişi ve kuruluşlardan istemeye yetkilidir. İlgili kişi ve kuruluşlar istenilen bilgileri vermekle yükümlüdür."* hükmüne yer verilmiştir[86].

Anayasa Mahkemesi[87], 663 sayılı KHK'nin 47. maddesinin; Anayasa'nın 20. maddesinde düzenlenen ve "Kişinin Hakları ve Ödevleri" başlıklı ikinci bölümünde yer alan özel hayatın gizliliği ve kişisel verilerin korunması hakkına ilişkin olarak kanun hükmünde kararname ile düzenleme yapılmasının mümkün olmadığı; Anayasa'nın 20. maddesiyle güvenceye bağlanan özel hayatın gizliliği ve kişisel verilerin korunması hakkına ilişkin düzenlemeler içeren dava konusu kuralların Anayasa'nın 91. maddesinin birinci fıkrasına aykırı olduğu gerekçesiyle iptaline karar vermiştir[88].

Kişisel sağlık verileriyle ilgili Z./Finlandiya kararında AİHM, HIV enfeksiyonu nedeniyle bir kişinin HIV testinin pozitif olduğunun açıklanmasının, onun özel hayatını ve toplumda bulunduğu yeri ağır bir şekilde zedeleyeceğini belirtmiştir[89]. Anılan kararında AİHM, hastanın sağlık verilerinin korunacağı hususunda kuşkusunun bulunmaması gerektiğini vurgulamıştır. Mahkemeye göre; *"Tıbbi verilerin gizliliğine saygı göstermek, AİHS'ye taraf olan bütün Sözleşmeci devletlerin yasal sistemlerinin temel prensibidir. Sadece hastanın özel hayatına saygı göstermek değil, hastanın tıp mesleğine ve genel olarak sağlık hizmetlerine duyduğu güveni de korumak şarttır. Böyle bir koruma olmazsa, tıbbi yardıma ihtiyacı olanlar doğru tedavi görmek için ve hatta tıbbi yardım almak için gerekli olan kişisel veya mahrem bilgileri açıklamaktan cayabilir; bu durum da hem kendi sağlıklarını, hem de bulaşıcı hastalıklar söz konusu olduğunda toplum sağlığını tehlikeye atar[90]."*

Gerçekten de özel kategorilerdeki (hassas) verilerin özel olarak korunması,

---

[86] AKGÜL Aydın., Danıştay Kararları Işığında Kişisel Sağlık Verilerinin Korunması, **Danıştay Dergisi,** Sayı 133, 2013, s.28-29.

[87] Anayasa Mahkemesi, 14.2.2013, E:2011/150, K:2013/30 (25.6.2013 tarihli ve 28688 sayılı Resmi Gazete)

[88] Akgül, **Danıştay Dergisi**, a.g.m. s. 29.

[89] POLATER, Yusuf Ziya., **Türk Hukukunda ve Avrupa İnsan Hakları Sözleşmesinde Özel Hayatın Gizliliği ve Korunması**, Adalet Yayınları, Ankara 2010, s.126.

[90] Küzeci, **a.g.e.** s. 237.

insanın aynı zamanda kişilik haklarının da korunmasına hizmet etmektedir. Hassas veri olarak korunan değerlerin genellikle kişilik değerleri içerisinde bulunduğu ve işlendikleri takdirde kişi bakımından ayrımcılık yaratmaya müsait oldukları görülmektedir. Bu çerçevede insanın örneğin sağlık durumu, politik veya dinsel görüşleri gibi verilerinin toplanması veya açıklanması onun kişilik haklarının korunmasına da ağır bir müdahaledir. Bu nedenle bu tür müdahalelerin ancak ağırlıklı kamu yararının söz konusu olduğu istisnai durumlarda mümkün olması gerekmektedir[91].

D. KİŞİSEL VERİLERİN İŞLENMESİ SIRASINDA İLGİLİNİN BİLGİLENDİRİLMESİ İLKESİ

Kişisel verilerin işlenmesi sırasında kişinin bilgilendirilmesi, onun kişisel verilerinin korunması bakımından son derece önemlidir. İlgili kişi kendisi hakkında veri işlendiğini bilmeden kişisel verilerinin korunmasına yönelik haklarını gerçek anlamda kullanamaz. Bu ilke aynı zamanda hukuk devleti içerisinde kamusal organların kişisel verilerin işlenmesine yönelik faaliyetlerinin şeffaf olması gereğinin de bir ifadesidir.

Bireyin kişisel verilerinin işlendiğinden haberdar edilmesi ya da veri toplamanın koşulları hakkında düzenli ve kapsamlı olarak bilgilendirilmesi ilkesi, aynı zamanda verilerin işlenmesinde dürüstlük ilkesine uyulmasının da bir gereğidir. Kişinin ancak kendisi hakkında veri toplandığını anlayabilmesi durumunda davranışlarını akılcı bir şekilde belirleyebilmesi mümkündür. Yine veri işlem faaliyetlerinin hukuka uygun şekilde yürütülebilmesi için de bireyin veri işlem faaliyeti konusunda bilgilendirilmesi gerekmektedir.

Kamusal organlar tarafından bireyin kişisel verileri doğrudan ilgili birey nezdinde elde edildiğinde veri işlem sorumlusu veya temsilcisi tarafından ilgili kişinin en azından aşağıdaki hususlarda bilgilendirilmesi gerekmektedir;

- Veri işlem sorumlusunun ve duruma göre temsilcisinin kimliği,

- Veriler için belirli olan veri işlemenin amacı,

- Verileri kabul eden veya edenlerin kategorisi,

[91] Şimşek, **a.g.e**. s. 88.

- Sorulara cevap vermenin zorunlu veya isteğe bağlı olduğu ve yine olası bir cevap vermeme durumunun sonuçları,

- Kendisini ilgilendiren veriler hakkında bilgi alma ve düzeltme haklarının mevcut olduğu.

Buna karşılık şayet bireye ilişkin kişisel veriler doğrudan ilgili kişi nezdinde değil de üçüncü bir kişiden elde ediliyorsa, bu durumda da veri işlem sorumlusunun veya temsilcisinin kişisel verilerin toplandığı veya işlendiği hususunda ilgili kişiyi bilgilendirmesi yükümlülüğü vardır. Bu durumda hakkında üçüncü kişi nezdinde kişisel veri toplanan bireye en azından şu hususlarda bilgi verilmesi gerekmektedir;

- Veri işlemin sorumlusunun ve gerektiği takdirde temsilcisinin kimliği,

- Veri işlemin amacı, işlenen verilerin kategorisi,

- Verileri kabul eden veya edenlerin kategorisi,

- Kişiyi ilgilendiren veriler hakkında bilgi edinme ve düzeltme haklarının bulunduğu[92].

Elektronik Haberleşme Sektöründe Kişisel Vergilerin İşlenmesi ve Gizliliğinin Korunması Hakkındaki Yönetmeliğin 3'üncü maddesinde yer alan ve "İlgili kişinin kendisine ait kişisel verisinin işlenmesine yönelik, verinin işlenme amaç ve kapsamı dâhilinde, verinin işlenmesi öncesinde özgür iradesiyle verdiği ispatlanabilir kabul beyanı[93]" şeklinde tanımlanan rıza beyanı alınmadan veri sahibinin dürüstlük kuralları çerçevesinde bilgilendirilmesi gereklidir.

Somut olayın özelliklerine göre kişisel veriler toplanırken veri toplama, işleme ve kullanma için öngörülen amaç ve yine istek durumunda rıza vermemenin sonuçlan hakkında da ilgili kişiye bilgi verilmelidir. Aynı şekilde veri işleme sorumlusu, toplanan verilerin aktarılabileceği konusunu ilgili kişi hesaba katamıyorsa ona bu konuda da bilgi

[92] Şimşek, a.g.e. s.88-89.

[93] Resmi Gazete Tarihi: 24.07.2012 Resmi Gazete Sayısı: 28363
http://tk.gov.tr/mevzuat/yonetmelikler/dosyalar/EHSKVIGKHak_Yon_Konsolide_Metin_2013.pdf
(E.T. 04.06.2014)

vermelidir. Şayet toplanan verilerin açıklanması konusunda hukuki bir yükümlülük bulunuyorsa bu durumun hukuksal temelleri konusunda da ilgili kişinin bilgilendirilmesi gerekmektedir. Bilgilendirme yükümlülüğü çerçevesinde sadece soyut olarak bireyin kendisi hakkında veri işlendiği konusunda bilgilendirilmesi yeterli olmayıp, aynı zamanda fiili olarak ilgili kişi hakkında işlenecek veriler, bu verilerin kökeni, verileri kabul eden veya kabul edenlerin kategorisi ve veri kaydetmenin amacı konusunda da bilgi verilmelidir. Bu bilgilendirme yükümlülüğünün veri toplama yetkisi bulunan hem kamusal hem de kamusal olmayan organlar için geçerli olduğu ifade edilmektedir[94].

Kişisel verilerin ilgili kişiden alınmadığı, başka kaynaklardan elde edildiği durumlarda da ilgili kişinin bu kapsamda bilgilendirilmesi, eğer ilgili kişiden elde edilen bilgiler üçüncü kişiyle paylaşılmışsa bu konuda da haberdar edilmesi gerekir. Ancak bu kurala karşın, eğer bu bilgilerin sağlanması olanaksız ise, oransız bir çaba gerektiriyor ise ya da işlem açıkça yasadan kaynaklanıyorsa bu bilgilerin sağlanması gerekmeyecektir. İlgili kişinin bilgilendirilmesi özellikle İnternet ortamında kullanılan çeşitli araçlar ve iletişim şekilleri açısından tartışılan bazı konuları beraberinde getirir. Nitekim pek çok donanım ve yazılım kişisel bilgileri toplamakta, değerlendirmekte ve çeşitli amaçlar için kullanmaktadır. Hiperbağlar (Hyperlinks), çerezler (cookies) ya da tarayıcıların (browser) karşılıklı iletişimi bu kapsamda düşünülebilir. Bu gibi uygulamalar, yukarıdaki açıklamalar ışığında, servis sağlayıcıların ilgili kişinin yapılan işlemin farkında olduğunu kanıtlaması hariç, kullanıcının yeterli oranda bilgilendirilmediği durumlarda kabul edilemez. Ancak ilgili kişinin durumun farkında olduğunu ispatlamanın hemen hemen olanaksız olduğu da belirtilmelidir. 29. Madde Veri Koruma Grubu da İnternet yazılım ve donanım ürünlerinin kullanıcılara hangi bilgilerin toplanma, saklanma ve aktarılma niyetinde olunduğu ve hangi amaçlarla bu verilerin gerekli olduğu konusunda bilgilendirilmelerini sağlayacak bir sistemin gerekliliğine işaret etmektedir[95].

Hakkında kişisel veri toplanan ilgili kişiye bilgi vermek mümkün değilse, çok aşırı masrafı gerektiriyorsa veya verileri kaydetme ve işleme yasada açıkça

[94] Şimşek, a.g.e. s. 89-90.

[95] Küzeci, a.g.e. s. 231-232.

öngörülmüşse ve yine istatistikî, tarihi veya bilimsel amaçlarla veri işlenmesi durumunda yasal düzenlemelerde belirtmek ve bireyi koruyucu gerekli önlemleri almak şartıyla bildirim yükümlülüğü ortadan kalkabilecektir.

E. İLGİLİ KİŞİNİN KATILIMI VE DENETİMİNE YÖNELİK İLKELER

1. İlgilinin Bilgilendirilmesi

Bireyin kişisel verilerinin işlenmesi durumunda kendisi hakkında kimin, ne zaman, hangi nedenle, hangi verilerini işlediğini bilme hakkı, kişisel verilerin korunmasının "altın kuralı veya "Manga Charta"sı olarak ifade edilmektedir. Her bireyin kendisi hakkında kimin, hangi verileri işlediğini bilme hakkı bulunmaktadır. Bu hak aynı zamanda veri işlem faaliyetlerinin şeffaflığı ya da açıklığı ilkesinin de bir uzantısıdır[96]. Kişinin bilgilendirilmesi dürüstlük kuralı ile de yakından ilişkilidir. Bütün bu nedenlerden ötürü, ilgilinin bilgilendirilmesi veri koruma hukukunda merkezi öneme sahiptir[97].

Yönerge, hakkında veri toplanan ve verileri işlenen ilgili kişilere önemli haklar sağlamıştır. Öncelikle ilgili kişilere veri işlem sorumlusu tarafından şu bilgilerin verilmesini zorunlu kılmıştır: Veri işlem sorumlusunun kimliği, verinin işlenme amaçları; veriyi kimin alacağı; kendisine yöneltilen soruları cevaplamak zorunda olup olmadığı ve cevaplamamasının olası sonuçları hakkında bilgi; kendisi ile ilgili verilere ulaşma ve onları düzeltme hakkının varlığı (md.10, 11)[98].

Bireyin kendisi hakkında kimin hangi verileri ve ne sebeple işlediğini bilme hakkı, kendisi hakkında veri işleyen kamusal organın ilgiliyi bilgilendirme yükümlülüğünden ayırt edilmelidir. Veri işlem faaliyeti hakkında ilgiliyi bilgilendirmek kamusal organlarının bir yükümlülüğü iken, kendisi hakkında veri işlenip işlenmediği konusunda bilgi almak ilgili bakımından bir haktır. Ancak bu iki husus da birbirini tamamlamaktadır. Veri işlem sorumlusu ilgiliyi veri işleme konusunda

[96] Şimşek, a.g.e. s.90.

[97] Küzeci, a.g.e. s. 230.

[98] Atak, **Veri Koruma Yönergesi,** a.g.m. s. 212.

bilgilendirmeden, ilgilinin henüz haberi olmadığı bir veri işlem faaliyeti hakkında bilgi alma, düzeltme, sildirme, engelleme gibi haklarını kullanmasına pek mümkün olmayacaktır. Bu nedenle ilgilinin bilgi alma hakkı veri işlem sorumlusunun bilgilendirme yükümlülüğü ile birlikte düşünülmelidir[99].

OECD Verilerin Korunması İlkelerinde (md. 13) ilgilinin bilgi edinme hakkı açıkça düzenlenmiştir. Buna göre ilgili, bir veri ya da veri topluluğu için sorumlu olan organdan kendisi hakkında veri toplanıp toplanmadığını öğrenme hakkına sahiptir. Ayrıca bireyin kendisine ilişkin verileri, makul bir sürede, ücretsiz ya da makul bir ücretle, kendisinin anlayabileceği uygun bir şekilde öğrenme hakkı bulunmaktadır[100].

2. İlgilinin Bilgilerine Erişim Hakkı

Pek çok metinde ilgili kişinin başka kişi ve kurumların elinde bulunan kişisel verilere ulaşma hakkı kabul edilmiştir. Ancak özellikle AB Yönergesi'ndeki düzenleme dikkat çekicidir. Nitekim benzer hükümler, AK Sözleşmesi, OECD Rehber İlkeleri ve BM Rehber İlkeleri'nde bulunsa da Yönerge'deki düzenleme daha geniş kapsamlıdır[101]. Bu hak Yönergenin 12. maddesinde düzenlenmiştir. Bu düzenlemeye göre, veri işlem sorumlusu verilerin işlenip işlenmediği hakkında ilgili kişiye uygun aralıklarla ve aşırı gecikme olmaksızın anlaşılabilir bir şekilde bilgi verme yükümlülüğü altındadır[102].

Burada şu noktaya dikkat çekmek gerekir: belirtilen hükümde kişiye yalnızca kendisine ilişkin verilere ulaşma hakkı tanınmamış, bunun yanında verilerin nasıl kullanıldığı, işleme amaçları, verinin kaynağı ve alıcıları gibi başka bilgilerin alınmasına da olanak verilmiştir. Bu bilgilerin ilgili kişiye gereksiz yere geciktirilmeden ve gereksiz masraflardan kaçınılarak bildirilmesi gerekir[103].

---

[99] Şimşek, a.g.e. s. 90.

[100] Şimşek, a.g.e. s. 91.

[101] Küzeci, a.g.e. s. 232.

[102] Atak, **Veri Koruma Yönergesi,** a.g.m. s. 212.

[103] Küzeci, a.g.e. s. 233.

AİHM de kişinin bilgilerine erişim hakkını Sözleşme'nin 8. maddesinin güvence alanı kapsamında görmektedir[104].

3. İlgilinin Verilerini Düzeltme Hakkı

Ayrıca bireyin verilerin işlenmesinin Yönergenin hükümlerine uymaması halinde (özellikle verilerin tam olmaması veya yanlış olması gibi), duruma göre bu verilerin düzeltilmesini, silinmesini veya engellenmesini isteme hakkı bulunmaktadır. Yine belirlenen ilkelere aykırı olarak yanlış veya eksik verilerin işlenmesi durumunda düzeltme, sildirme veya engelleme yapılmışsa, imkân dâhilinde olmak ve aşın masrafı gerektirmemek kaydıyla, bireyin kendilerine daha önceden veri aktarılan üçüncü kişilere bu durumun bildirilmesini isteme hakkı da bulunmaktadır. İlgilinin kişisel verilerinin düzeltilmesi, silinmesi veya engellenmesi hakkı aynı zamanda bilgi alma hakkının da bir uzantısıdır. Tüm bu haklar bireyin kişisel verilerin korunması hakkına hizmet etmektedir. Ancak düzeltme, sildirme ve engelleme hakkının kullanılması bilgi alma hakkının kullanılması ön şartına bağlı değildir. Bu haklar bilgi alma hakkı

[104] Bilgilere erişim hakkına ilişkin Mahkeme'nin ilk kararı Leander'in İsveç'e karşı yaptığı başvuru (Başvuru No: 9248/81, k.t. 26 Mart 1987)üzerine verilmiştir. Başvuruya konu olan olayda, hakkındaki güvenlik soruşturması nedeniyle İsveç'li bir marangoz olan Leander'in askeri bir deniz üssü yakınındaki müzedeki işine son verilmesi söz konusudur. Ayrıca Leander'in kendisine ilişkin güvenlik kayıtlarına ulaşmasına da izin verilmemiştir. Mahkeme'ye göre başvuranın kişisel verilerinin ulusal güvenlik gerekçeleriyle gizli olarak tutulması ve yayımı özel yaşama müdahale oluşturmaktadır. Bu nedenle 8. maddenin kapsamında değerlendirilmelidir(par.48). Nitekim Leander'e ilişkin bilgi, yalnızca güvenlik güçlerince tutulmakla kalmamış, ayrıca kendisi hakkındaki güvenlik soruşturması nedeniyle ilgili birime de aktarılmıştır. Ancak Mahkeme'nin ve K o m i s y o n ' u n bu olaya ilişkin açıklamaları oldukça belirsizdir. Burada M a h k e m e ' n i n bilgilerin gizliliği ile tutulmaları ve aktarılmalarına ilişkin sorunlara değinmediği görülmektedir. Mahkeme, Sözleşme'nin düşünceyi açıklama özgürlüğüne ilişkin10.maddesi çerçevesinde yaptığı değerlendirmede, bu hükmün, somut olaydakine benzer şartlarda, bireye kendi kişisel durumuna ilişkin kayıtlara erişim hakkı tanımadığı gibi, devlete de bu tür bilgileri bireye iletme yükümlülüğü getirmediğine karar vermiştir(par.74). Mahkeme, 10.madde çerçevesinde Sözleşmeci Devletlerin böylesine bir pozitif yükümlülüğünün bulunmadığı belirtilse de, bu hakkın 8.madde kapsamında değerlendirilebileceğine hükmetmiştir. İlk kez Gaskin Birleşik Karalık'a karşı, kararında (Başvuru No: 10454/83,k.t.7Temmuz1989) dile getirilen bu yaklaşım, daha sonraki başka kararlarda da tekrarlanmış ve devlet tarafından tutulan kişisel verilere erişim talepleri 8. maddenin kapsamında görülmüştür.

kullanılmamış olsa da kullanılabilir. Başka bir anlatımla kamusal organlar ilgiliyi bilgilendirmemiş olsalar bile, ilgili kişi başka bir surette kendisine ilişkin olarak kamusal organlarda doğru olmayan, eksik veya hukuka aykırı bir veri bulunduğunu öğrenmişse bu durumda da düzeltme, sildirme ve bu verilerin kullanılmasının engellenmesi haklarını kullanabilir. Zira bireyin kişisel verilerinin işlenmesi karşısında bilgi alma hakkı gibi düzeltme, sildirme ve engelleme hakları da hukuka aykırı olarak veri işlenmesi durumunda kişinin özgürlüklerinin korunmasını amaçlamaktadır[105].

Sildirme hakkı ise, veri işlem sorumlusunun kişisel veriler üzerinde artık tasarruf edememesi sonucunu doğuran bir önlemin alınmasını sağlamayı amaçlamaktadır. Kişisel verilerin hukuka aykırı olarak toplanıp, işlenmesi durumunda verinin veri taşıyıcısının (örneğin kâğıt üzerindeki bilginin) yok edilmesi vasıtasıyla silme gerçekleşebileceği gibi verinin kişinin kimliğini ortaya çıkartacak kişisel bağlantısının kaldırılması yoluyla da silmenin gerçekleşmesi mümkündür. Sildirme hakkı, özellikle veri işleme yetkisinin bulunmaması ve verilerin kaliteli olması ilkesine aykırılık durumlarında söz konusu olmaktadır [106].

F. VERİ GÜVENLİĞİ İLKESİ

Kişisel verilerin korunması ile veri güvenliği eş anlamlı değildir. İlkinde amaç, bireylerin korunması iken, ikincisinde verilerin korunması hedeflenmektedir. Ancak bunlar kişisel nitelikte olduğunda veri güvenliği kişisel verilerin korunmasının bir aracı haline gelmektedir. Verilere yetkisiz erişim ve bunların yetkisiz kullanımının önüne geçilmesinde kurum ve kuruluşların da çıkarı bulunur. Bu, bankacılık, sigortacılık ve sağlık hizmetleri gibi güven ilişkisinin önemli olduğu alanlarda daha da açıkça görülebilir[107].

Bir bankaya parasını yatırmayı, sigorta şirketiyle sözleşme yapmayı ya da tanı ve tedavi için bir sağlık kuruluşuna başvurmayı düşünen kişi verilerinin güvende olduğunu bilmek isteyecektir. Bu konuda endişe duyması halinde ise belirtilen hizmetleri almamayı tercih edebilir. Bunun ilgili kişi açısından yaratacağı sorunlar

[105] Şimşek, a.g.e. s. 92-93.

[106] Şimşek, a.g.e. s. 93.

[107] Aktaran Küzeci, a.g.e. s. 262.

yanında, kurumun ekonomik kaybına neden olacağı da açıktır. Bu durum, veri güvenliğinin ekonomik olarak ölçülebilir çıkarları da güvence altına aldığını ortaya koymaktadır[108].

Verilerin güvenliğinin amacı kişisel nitelikli verilerin korunması için gerekli olan bütün idari ve teknik tedbirlerin alınmasının sağlanmasıdır. Kişisel verilerin korunması ve verilerin güvenliği kavramları birbirinden farklıdır. Kişisel verilerin korunması ile esas olarak kişisel verilerin işlenmesi sırasında bireyin hak ve özgürlüklerinin korunması ve veri işleme faaliyetlerinin hukuksal sınırları ifade edilirken, verilerin güvenliği ile verilerin bizatihi kendisinin korunmasına yönelik olarak alınması gereken teknik ve idari tedbirlerin anlaşılması gerekmektedir. Verilerin güvenliği ilkesi, verilerin kaybedilmesi, yetkisiz kişilerin verilere ulaşması, tesadüfen veya yetkisiz kişilerce verilerin tahrip edilmesi, değiştirilmesi veya alenileştirilmesi gibi rizikolar karşısında uygun güvenlik önlemleriyle verilerin korunmasına hizmet etmektedir[109].

Verilerin güvenliği ilkesi günümüzde modern veri koruma hukukunun önemli bir parçası olarak kabul edilmektedir. Bu çerçevede verilerin güvenliğine yönelik olası tehlikeler karşısında alınabilecek bütün idari ve teknik tedbirler veri güvenliği ilkesi içerisinde değerlendirilmelidir. Bu ilke aynı zamanda olası tehlikeler karşısında verinin güvenliğinin sağlanması yoluyla kişisel verilerin korunması temel hakkının korunmasına da hizmet etmektedir. Kişisel verilerin korunması temel hakkı kapsamında garantilerin anlam kazanabilmesi ve veri işlem faaliyetleri sırasında bireyin ortaya çıkabilecek tehlikelerden korunabilmesi için her şeyden önce teknik ve idari önlemlerin de alması gereklidir. Verilerin korunmasının güvence altına alınması için zorunlu olan bu idari ve teknik önlemler, özgürlüğün maddi olarak korunmasını tamamlayıcı düzenlemeler olarak anlaşılmaktadır. Bu anlamda idari ve teknik önlemler, kişisel verilerin işlenmesi sırasında kişiliğin ihlal edilmesini önlemek amacıyla gerekli önlemlerin alınmasını ifade etmektedir. Bu önlemler, teknik ve kurumsal tedbirlerin yanı sıra, genel olarak veri sırrının korunması, ilgilinin haklan, haber verme

[108] Küzeci, a.g.e. s. 262.

[109] Aktaran Şimşek, a.g.e. s. 94.

yükümlülüğü, veri koruma görevlisine başvurma gibi önlemleri de kapsamaktadır[110].

AB Veri Koruma Yönergesi'nde ise şu düzenleme yer alır: "Üye Devletler denetçinin, kişisel verilerin kazara veya hukuka aykırı tahribine veya kazara kaybolmasına, değiştirilmesine, yetkisiz yayımı veya erişimine, özellikle işlemin bir şebeke ağı üzerinden nakli yoluyla yapılması durumunda ve hukuka aykırı diğer hukuka aykırı işleme biçimlerinden korunması için gerekli teknik ve örgütsel önlemleri almasını sağlayacaklardır". Bu önlemler hem ilgili sistem kurulurken, hem de daha sonra veriler işlenirken alınmalıdır. Bu sırada teknik olanaklar ve uygulama masrafları göz önünde tutularak işlemeden kaynaklı riske ve korunan verinin niteliğine uygun düzeyde güvenlik sağlanmalıdır. Veri denetçisi ayrıca, bir sözleşme veya yasal hüküm uyarınca, veri işleyen çalıştırdığında teknik ve örgütsel güvenlik önlemleri bağlamında yeterli güvenceyi sağlamalıdır. Bunun yanında belirtilen hükümlere uygun olarak alınan önlemlerin belgelendirilmesi de gerekir[111].

Veri güvenliği önemli ancak hızla gelişen teknoloji dolayısıyla sağlanması zor bir konudur. Veri güvenliğini sağlayan araçlar ile bunların aşılmasını sağlayan yöntemler paralel bir şekilde gelişmektedir. Bu nedenle alınan teknik önlemlerin sürekli güncellenmesi, yenilenmesi bir zorunluluktur. Veri güvenliğinin yeteri düzeyde sağlan(a)maması dünyanın pek çok yerinde yankı uyandıran skandalların yaşanmasına neden olmuştur. Hatta ABD'de özellikle müşteri veri tabanlarından çeşitli bilgilerin çalınması olayları, ülkenin kişisel verilerin korunması politikasını çeşitli zamanlarda önemli bir tartışma konusu haline getirmiştir. Kişisel verilerin yetkisiz kişilerin eline geçmesi ekonomik, siyasal, sosyal ve hatta fiziksel zararlara neden olabilir. Yaklaşık on yıl önce Cambridge Üniversitesi'nde çalışanların adres bilgilerinin sızması sonucunda, evlerinin hayvan hakları savunucularınca hedef alındığı bilinmektedir. Birkaç yıl önce yine İngiltere'de kredi kartı verilerinin basına sızması sonucunda politikacıların iddia edilen ölçüsüz alkol tüketimlerine ilişkin kişilik haklarına zarar verici bilgiler basında yayınlanmıştır. Kimlik bilgileri, banka hesap numaraları gibi bilgilerin çalınması sonucunda oluşan ekonomik zararın boyutu ise her geçen gün artmaktadır. Bu noktada şu hususa da işaret etmek gerekir: veri güvenliğinin hem verileri işleyen kişiler

[110] Şimşek, a.g.e. s. 95.

[111] Küzeci, a.g.e. s. 263.

tarafından, hem de verilerin öznesi tarafından sağlanması gerekir. Verileri toplayan ve işleyen sistemlerin korunması yanında, bireyler de kendilerini korumalıdır. Teknoloji tabanlı güvencelerin kişisel verilerin etkin korunması için oldukça önemli olduğu unutulmamalıdır. Bireylerin kendi özel bilgisayarlarında ya da kullandıkları başka elektronik araçlarda gereken önlemleri almaları, hem temel hak ve özgürlüklerine hem bütçelerine yönelecek pek çok saldırının önlenmesine yardımcı olacaktır[112].

G. VERİLERİN İŞLENMESİNDE ÖN KONTROL İLKESİ

Üye Devletler, veri öznelerinin haklarına ve özgürlüklerine özel riskler sunması, olası işleme faaliyetlerini belirleyecektir ve bu işleme faaliyetlerinin başlatılmasından önce incelenmesini kontrol edecektir. Bu tür ön kontroller, şüphe durumunda denetim makamına danışması gereken bir veri koruma görevlisi tarafından veya denetleyiciden bir bildirimin alınmasını takiben denetleme makamı tarafından yerine getirilecektir. Üye Devletler ya ulusal parlamentonun bir tedbiri ya da işlemenin yapısını tanımlayan ve uygun korunma önlemlerini belirten bu tür bir yasama tedbirine dayalı bir tedbirin hazırlanması bağlamında, bu tür kontrolleri de yapabilir[113].

Kişisel verilerin işlenmesinde ön kontrol ilkesi çerçevesinde veri işlem faaliyetlerinin kişilerin hak ve özgürlükleri için özel rizikolar taşıması durumunda bu hususun belirlenmesi ve bu tür veri işleme faaliyetleri daha başlamadan önce ön kontrole tabi tutulması gerekmektedir. Veri işlenmesi faaliyetinden önce yapılacak ön kontrol, veri işlem faaliyetlilerinin kişisel verilerin korunması hukukunun gereklerine uygun olup olmadığının ve ilgilinin hak ve özgürlükleri bakımından özel rizikolar taşıyıp taşımadığının önceden incelenmesi anlamına gelmektedir. Ön kontrol her şeyden önce veri işlem faaliyetlerinin hukuka uygunluğu açısından yapılan bir denetimdir[114].

Belirli veri işleme türlerinin kapsam ve amaçlarıyla birlikte, örneğin ilgilinin bir hakkını kullanması, bir hizmeti veya sözleşmeyi yapması gibi, teknolojilerin özel surette kullanılması sebebiyle ilgilinin hak ve özgürlükleri bakımından özel rizikolar ortaya çıkarabilmesi mümkündür. Bu nedenle bu tür rizikoların önlenmesi için kontrol

[112] Küzeci, a.g.e. s.264-265.

[113] http://www.ihop.org.tr/dosya/coe/EC_DIRECTIVE_95_46_Kisisel_Veriler.pdf , (E.T. 04.06.2014).

[114] Aktaran Şimşek, a.g.e. s.97.

organları vasıtasıyla bir ön kontrol öngörülmelidir. Ön kontrol, veri işlemenin türüne uygun garantileri belirleyen bir yasama işlemi şeklinde öngörülebileceği gibi bu tür bir yasal düzenlemeye dayanan tedbirlerin uygulanması sırasında da öngörülebilir. İlgilinin hak ve özgürlükleri bakımından ortaya çıkabilecek riziko kavramı ise, modern teknolojilere bağlı hataları ve kötüye kullanmaları da kapsayacak şekilde geniş şekilde anlaşılmalıdır. Bu çerçevede şayet veri işleme faaliyeti bireyin hak ve özgürlükleri için özel rizikolar yaratabilecek nitelikte ise, veri işlemeden önce bu konuda geniş ve yoğun bir incelemenin yapılması ön kontrol için yeterli olacaktır. Bu nedenle bireylerin hak ve özgürlüklerinin korunması bakımından özel rizikolar doğurabilecek nitelikteki verilerin (örneğin hassas verilerin) işlenmesinden önce ön kontrol organları oluşturulmalıdır[115].

H. HAK ARAMA, SORUMLULUK VE YAPTIRIMLARA İLİŞKİN DÜZENLEMELERİN GEREKLİLİĞİ İLKESİ

Denetleyici veri öznelerinin haklarını gözetmezse, ulusal mevzuat bir yargı yolu sağlamalıdır. Yasadışı işlemenin bir sonucu olarak bir kişinin maruz kalabileceği herhangi bir zarar; mücbir sebepler durumunda ya da hatanın veri öznesinin tarafında olduğunu saptadığı durumlarda; zarardan sorumlu olmadığını kanıtlarsa yükümlülükten muaf tutulacak olan denetleyici tarafından tazmin edilmelidir. Yaptırımlar, Yönerge kapsamında alınan ulusal tedbirlere uymayanın kamu veya özel hukuk tarafından yönetilen herhangi bir kişi olduğuna bakılmaksızın uygulanmalıdır[116].

Kişisel verilerin işlenmesi sırasında hukuka aykırılıklar durumunda bireyin kişisel verilerinin korunması için aynı zamanda idari, cezai ve hukuki bir takım yaptırımların da öngörülmesi gerekmektedir. Bu husus, kişisel verilerin etkin bir şekilde korunabilmesi için bir zorunluluktur. Bu çerçevede AT Verilerin Korunması Yönergesi de yasa koyuculara veri işlemeye yönelik düzenlemelere uyulamaması durumunda yaptırım uygulama konusunda gerekli önlemleri alma yükümlülüğünü getirmektedir[117].

---

[115] Aktaran Şimşek, a.g.e. s.98.

[116] http://www.ihop.org.tr/dosya/coe/EC_DIRECTIVE_95_46_Kisisel_Veriler.pdf , (E.T. 04.06.2014).

[117] Şimşek, a.g.e. s.102.

İ. YETKİSİZ VERİ İŞLENEMEMESİ YA DA KİŞİSEL VERİLERİN İŞLENEBİLMESİ İÇİN YASAL TEMELİN VEYA İLGİLİNİN RIZASININ GEREKLİLİĞİ İLKESİ

Kişisel verilerin kamusal organlar tarafından işlenebilmesi için bu organların yasal bir düzenleme ile yetkilendirilmiş olması veya ilgilinin veri işlemeye rıza göstermesi gerekmektedir. Bu ilke, hem kendisi için veri toplayan hem de talep üzerine veri toplayan organlar bakımından geçerlidir. Genellikle verilerin korunmasına ilişkin hukuksal düzenlemeler kamusal organların kişisel verileri işleyebilmesi için yasal bir yetkilendirmenin veya ilgilinin rızasının gerekliliğini öngörmektedir. Buna *"izin kaydı"* adı verilmektedir[118].

Nitekim ilgilinin rızası, verilerin işlenmesinin en önemli meşruluk temellerinden biridir. Bu bağlamda "rıza" ilgili kişinin kendisiyle ilgili veriler üzerinde denetimini sağlamasının önemli bir aracı ve "bilgilerin geleceğini belirleme" düşüncesinin bir yansımasıdır. Ancak bu noktada hemen belirtmek gerekir: kişisel verilerin korunmasına ilişkin düzenlemelerden bir bölümünde bireyin rıza vermesi koşulu yer almadığı gibi, AB Yönergesi gibi başka metinlerde verilerin işlenmesinin tek meşru koşulu olarak değerlendirilmemiş, yalnızca veri işlemeyi meşru kılan durumlar içerisinde sayılmıştır. Bunun yanında diğer koşulların geniş yorumlara olanak veren yapısı, rızanın aranmasının zorunlu olduğu durumların oldukça sınırlı kalmasına neden olmaktadır[119].

Uygulama bakımından ilk önce somut veri işlem faaliyetinde ilgilinin bu işlemeye rızasının bulunup bulunmadığı araştırılmalıdır. Fakat rızanın soyut olarak tek başına var olması yeterli olmayıp, rızanın aynı zamanda verilerin toplanmasının ve işlenmesinin somut amacı ile verilerin kullanılması durumunda ortaya çıkacak sonuçlar hakkında ilgilinin bilgilendirilmesinden sonra verilmiş olmalıdır. Bunun yanı sıra rızanın bireyin özgür iradesine dayanması ve kural olarak yazılı şekilde verilmesi gerekmektedir. Şayet rıza elektronik ortamda, örneğin tele hizmetler sırasında alınıyorsa bu durumda da tele hizmetler hukukunda rızanın alınmasına ilişkin ilkelere de

[118] Aktaran Şimşek, a.g.e. s. 106.

[119] Aktaran Küzeci, a.g.e. s. 238.

uyulmalıdır. Bireye ilişkin hassas verilerin işlenmesi söz konusu ise, bu konuda verilen rızanın açıkça işlenmesi söz konusu olan ilgili verinin belirtilmesi suretiyle alınması gerekmektedir. Bu çerçevede ilgiliye kişisel verilerin toplanma amacı, veri işlem sorumlusunun kimliği ve adresinin bildirilmesi gerekir. Burada veri işlem sorumlusunun sadece internet veya e-posta adresinin verilmesi yeterli olmayıp, kişisel verileri toplanan bireyin haklarını takip edebilmesini mümkün kılacak şekilde veri işlem sorumlusunun kimliğinin ve adresinin bildirilmesi gerekmektedir. Aynı şekilde kişisel veriler birden fazla amaç için veriliyorsa ilgili kişiye bu amaçlar da açıkça bildirilmelidir. Kişisel verilerin işlenmesinin yasal bir temele veya ilgilinin rızasına bağlı olmasının bir sonucu olarak birey, kişisel verilerinin işlenmesine neden rıza vermediğini gerekçelendirmek zorunda değildir. Bu çerçevede kişisel verilerinin işlenmesi karşısında bireyin susmasının bir nedene bağlanması değil bilakis her türlü kişisel veri işleme faaliyetlerinin yasal olarak haklı gösterilmesi gerekmektedir. Bireyin kişisel verilerinin işlenmesine rıza göstermemesini haklı çıkartmak için bir gerekçe göstermek zorunda bırakılması söz konusu olmayıp kamusal organların kişisel verileri işleyebilmek için mutlaka yasal temele sahip olması gerekmektedir[120].

Kişisel verilerin hukuka uygun olarak işlenebilmesi için Yönerge'ye göre kişisel verilerin toplanabilmesi için şu koşullardan en az birisinin varlığı gerekli öngörülmüştür;

- İlgili kişinin her türlü şüpheden uzak bir şekilde rızasının bulunması,

- İlgili kişinin taraf olduğu bir sözleşmenin uygulanması veya ilgili kişinin talebi üzerine yapılan sözleşme öncesi önlemlerin alınması,

- Veri işlemin veri işlem sorumlusunun hukuksal bir yükümlülüğünün yerine getirilmesi için zorunlu olması,

- Kişisel verilerin işlenmesinin ilgili kişinin yaşamsal menfaatlerinin korunması için gerekli olması,

[120] Aktaran Şimşek, a.g.e. s.107.

- Veri işlemin kamu yararı bulunan bir görevin yerine getirilmesi için gerekli olması,

- Veri işlemin, ilgili kişinin menfaatlerinin veya temel hak ve özgürlüklerinin ağır basmaması durumunda kendisine veri aktarılacak veri işlem sorumlusunun veya gerektiğinde üçüncü kişinin haklı menfaatlerinin korunması için gerekli olması[121].

K. KİŞİSEL VERİLERİN İŞLENMESİNİN BAĞIMSIZ KONTROL ORGANLARI TARAFINDAN DENETLENMESİ İLKESİ

Denetim makamına ilişkin Üye Devletlerdeki tam bağımsız olarak işlevlerini yerine getiren kuruluşlar, kişisel verilerin işlenmesine dair bireylerin korunmasında, *zorunlu bir bileşendir*[122].

Kişisel verilerin korunması açısından oldukça önemli bir güvence, veri koruma yasaları ile belirlenen ilkelere uygun hareket edilip edilmediğini denetleyen bağımsız bir organın oluşturulmasıdır. Kimi yazarlarca bu, kişisel verilerin korumasına ilişkin düzenlemeleri diğerlerinden ayırt edici bir özellik olarak bile değerlendirilir. Diğer uluslararası metinler ile karşılaştırıldığında, bağımsız denetim organına ilişkin en ayrıntılı düzenlemenin AB Veri Koruma Yönergesi'nde bulunduğu görülür. Yönerge'ye göre her üye devlet, Yönerge'de belirlenen hükümlerin uygulamasını izlemek üzere bir ya da birden çok resmi makam oluşturacaktır[123].

Her bir Üye Devlet, bu Direktif uyarınca Üye Devletler tarafından kabul edilen hükümlerin kendi ülkesindeki uygulamasını izlemekten, bir veya daha fazla kamu makamının sorumlu olmasını sağlayacaktır. Bu makamlar, onlara tevdi edilen işlevleri yerine getirmede tam bağımsız olarak hareket edeceklerdir. Her bir Üye Devlet, kişisel verilerin işlenmesine dair bireylerin hak ve özgürlüklerinin korunmasına ilişkin idari tedbirleri veya yönetmelikleri hazırlarken, denetim makamına danışılmasını sağlayacaktır. Her bir makama özellikle sağlanacaktır:

[121] http://www.ihop.org.tr/dosya/coe/EC_DIRECTIVE_95_46_Kisisel_Veriler.pdf , (E.T. 04.06.2014).

[122] http://www.ihop.org.tr/dosya/coe/EC_DIRECTIVE_95_46_Kisisel_Veriler.pdf , (E.T. 04.06.2014).

[123] Küzeci, a.g.e. s. 271.

- Denetim görevlerinin yerine getirilmesi için gerekli tüm bilgileri toplama yetkileri ve işleme faaliyetlerinin konusunu oluşturan verilere erişim yetkileri gibi araştırma yetkileri.

- Örneğin ulusal parlamentolar veya diğer siyasi kuruluşlara konuyu havale etme veya denetleyiciye ihtar verme veya uyarma, işleme üzerinde geçici veya kesin yasaklama koyma, verilerin yok edilmesini veya silinmesini, engellenmesini emretme, bu tür görüşlerin uygun şekilde yayınlanmasını sağlama ve madde 20'e uygun olarak işleme faaliyetlerinin yerine getirilmesinden önce görüş bildirme gibi etkin müdahale yetkileri.

- Bu Direktif uyarınca kabul edilen ulusal hükümler ihlal edildiğinde veya bu ihlalleri yargı makamlarının dikkatine sunma için kanuni kovuşturmaya girişme yetkisi.

Denetleme makamının şikâyetlere yol açan kararları; mahkemelerde temyiz edilebilir. Her bir denetim makamı, kişisel verilerin işlenmesine dair hak ve özgürlüklerin korunmasına ilişkin o kişiyi temsil eden bir dernek veya herhangi bir kişi tarafından arz edilen iddiaları dinleyecektir. Her bir denetim makamı, özellikle, bu Direktifin 13. maddesi uyarınca kabul edilen ulusal hükümler uygulandığında, herhangi bir kişi tarafından arz edilen veri işlemenin yasallığı hakkındaki kontroller için iddiaları dinleyecektir. Kişi, bir kontrolün yapıldığından her halükarda bilgilendirilecektir. Her denetleme makamı, faaliyetleri hakkında düzenli aralıklarla bir rapor hazırlayacaktır. Rapor, kamuoyuna açıklanacaktır.

Her denetleme makamı, söz konusu işlemeye uygulanan ulusal kanun her ne olursa olsun, paragraf 3'e uygun olarak verilen yetkileri kendi Üye Devletinin toprağında uygulamaya yetkilidir. Her bir makamdan, diğer bir Üye Devletin makamı ile yetkilerini uygulaması istenebilir.

Denetleme makamları, özellikle tüm yararlı bilgileri takas ederek, kendi görevlerini yerine getirmek için gerekli ölçüde birbirleriyle iş birliği yapacaklardır. Üye Devletler, görevlerinin bitiminden sonra bile, denetleme makamının personellerinin ve mensuplarının, eriştikleri gizli bilgilere dair mesleki gizlilik

görevine tabi olmalarını sağlayacaktır.

L. KİŞİSEL VERİLERİN HUKUKA AYKIRI İŞLENMESİ DURUMUNDA TAZMİNAT HAKKI

Üye Devletler, hem kişisel verilerin işlenmesi hususunda bireylerin korunması hakkındaki genel kanunlar, hem de örneğin istatistik enstitülerine ilişkin olanlar gibi sektörel kanunlar yoluyla bireylerin korunmasını uygulamayı temin etmek üzere yetkilendirilmişlerdir. Denetleyici veri öznelerinin haklarını gözetmezse, ulusal mevzuat bir yargı yolu sağlamalıdır. İşlemenin bir sonucu olarak bir kişinin maruz kalabileceği herhangi bir zarar; mücbir sebepler durumunda ya da hatanın veri öznesinin tarafında olduğunu saptadığı durumlarda; zarardan sorumlu olmadığını kanıtlarsa yükümlülükten muaf tutulacak olan denetleyici tarafından tazmin edilmelidir. Yaptırımlar, Yönerge kapsamında alınan ulusal tedbirlere uymayanın kamu veya özel hukuk tarafından yönetilen herhangi bir kişi olduğuna bakılmaksızın uygulanmalıdır[124].

Hukuka aykırı veya yetkisiz bir şekilde kişisel verilerin işlenmesi sebebiyle bir zarara uğrayan herkesin veri işlem sorumlusundan tazminat talep etme hakkı da verilerin korunması hukukunun temel gereklerindendir. Veri işlem faaliyetleri sırasında ilgili kişinin haklarının ihlal edilmesi durumunda yargısal yolların öngörülmesi zorunlu olduğu gibi ortaya çıkabilecek zararların da tazmin edilmesi de gerekmektedir. Tazminat talebi maddi zararları kapsadığı gibi ağır kişilik hakkı ihlallerinde manevi zararları da kapsamaktadır. Buna karşılık veri işlem sorumlusunun zararın kendisine kusur yüklenemeyecek bir nedenden dolayı meydana geldiğini kanıtlaması durumunda tazminat talebi karşısındaki sorumluluğundan kurtulması mümkündür[125].

[124] http://www.ihop.org.tr/dosya/coe/EC_DIRECTIVE_95_46_Kisisel_Veriler.pdf , (E.T. 04.06.2014).

[125] Şimşek, a.g.e., s.109.

III. BÖLÜM

TÜRK HUKUKUNDA KİŞİSEL VERİLERİN KORUNMASIYLA İLGİLİ HUKUKSAL DÜZENLEMELER

A. ANAYASA

Anayasa'nın 2010 yılında 5982 sayılı kanun ile değiştirilen 20. maddesinin 3. fıkrası şu şekildedir;

"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." Madde ile kişilere kendileriyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenme dâhil olmak üzere kişisel verilerin korunması anayasal hak olarak tanınmaktadır. Madde ayrıca kişisel veriler ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebileceğini belirtmektedir. Ancak bunun yanında kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenleneceği de belirtilmiştir. Bahsedilen anayasal hüküm her ne kadar bu konudaki esas ve usullerin kanunla düzenleneceğini vurgulasa da, ülkemizde kişisel verilerin korunması konusuna özgülenmiş çerçeve bir düzenleme henüz bulunmamaktadır[126].

[126] Türkiye'de Kişisel Verilerin Korunmasının Hukuki ve Ekonomik Analizi, Türkiye Ekonomi Politikaları Araştırma Vakfı (TEPAV), İstanbul Bilgi Üniversitesi Bilişim Ve Teknoloji Hukuku Enstitüsü, 21.05.2014, http://www.nocistanbul.com/pdf/Turkiyedeki-Kisisel-Verilerin-Korunmasinin-Hukuki-ve-Ekonomik-Analizi.pdf s.43. (E.T. 04.06.2014)

Anayasada kişisel verilerin korunmasına yönelik hükümler bulunmakla birlikte yeterli değildir. Mukayeseli hukukta ve tarafı olduğumuz uluslararası belgelerde de kişisel verilerin korunması önemle vurgulanmaktadır. Maddeyle, herkesin, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkı, anayasal bir hak olarak teminat altına alınmaktadır. Bu bağlamda, bireylerin kendilerini ilgilendiren kişisel veriler üzerinde hangi hak ve yetkilere sahip olduğu ve kişisel verilerin hangi hallerde işlenebileceği hükme bağlanırken, kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenleneceği öngörülmektedir.

Kişisel verilerin korunması anayasal temelden yoksun değildir. Aksine oldukça sağlam normatif temellerini Türkiye Cumhuriyeti Anayasasında bulmak olanaklıdır. Daha önce de belirtildiği üzere kişisel verilerin korunmasını anayasalarında ayrı bir hak alanı olarak yer vermemiş çeşitli devletlerin yargı organları, geliştirdikleri içtihatlar ile bu normatif temeli belirlemiştir. AİHM de kişisel verilerin korunmasında hâkim olan pek çok temel ilkeyi Sözleşme'nin özel yaşamın gizliliği hakkını düzenleyen 8. maddesinin kapsamında görmüştür. Türkiye'de Anayasa Mahkemesinin de benzer bir anlayışı benimsediği söylenebilir. Mahkeme, her ne kadar geçmişte verdiği bazı kararlarda konuya ilişkin temel ilkeleri Anayasanın 20. maddesi çerçevesinde yorumlamada biraz isteksiz görünse de yakın zamanda verdiği bir karar kişisel verilerin korunmasını özel yaşamın gizliliği hakkı ve düşünce özgürlüğü çerçevesinde değerlendirdiğini açıkça ortaya koymaktadır. Mahkeme 2008 yılında, 5429 sayılı Türkiye İstatistik Kanunu'nun istatistiksel birimlerin (yani haklarında veri toplanacak gerçek ve tüzel kişiler ile kurum ve kuruluşların yetkilerinin) kendilerinden istenen veri veya bilgileri, vermekle yükümlü olduklarına ve bu yükümlülüğe uymayanların para cezası ile cezalandırılacaklarına[127] ilişkin hükmün iptaline ona karşı bir oyla karar vermiştir[128].

[127] http://www.alomaliye.com/kasim_05/5429_sayili_kanun_istatistik.htm (E.T. 04.06.2014).

[128] Küzeci, a.g.e. s.293.

Mahkeme 2006/167 Esas ve 2008/86 Karar Sayılı 20.3.2008 tarihli kararında:

5429 sayılı Yasa'nın 2. maddesinin (h) bendine göre istatistiki birim, yapılan sayım veya örnekleme çalışmalarına konu olan, hakkında veri toplanacak gerçek ve tüzel kişiler ile kurum ve kuruluşları ifade etmektedir.

İtiraza konu 8. madde hükmüyle sayım ve örnekleme çalışmalarına konu olan, hakkında veri toplanacak gerçek ve tüzel kişiler ile kurum ve kuruluşların yetkililerine cevap verme yükümlülüğü getirilmiş, bu yükümlülüğe uymayanların da 54. maddede gösterilen biçimde idari para cezasıyla cezalandırılması öngörülmüştür.

Maddede açıklayıcı bir düzenleme bulunmadığı için, "kişisel veri" veya "isteme bağlı veri" olarak adlandırılan, belirli veya belirlenebilir kişilerle ilgili her türlü bilgilerin istenebileceği kuşkusuzdur.

İstatistiki birimlerin kendilerinden istenen bilgileri belirlenen şekil ve sürede eksiksiz ve hatasız olarak vermek zorunluluğuna uyulmaması idari para cezası yaptırımına bağlanmış olmasına karşın, istenilecek veri ve bilgilerin kapsamı ya da sınırlarının ne/neler olacağına, başka bir anlatımla, temel hak ve özgürlüklere müdahale niteliğinde olan veri ve bilgilerin bu zorunluluk kapsamında bulunup bulunmadığına ilişkin herhangi bir düzenlemeye rastlanmamaktadır. Dolayısıyla, istatistiki birimler kendilerinden istenildiği takdirde her türlü bilgiyi temel hak ve özgürlüklerine müdahale niteliğinde olsa bile vermek zorundadırlar.

AİHM kararlarında da belirtildiği gibi, özel hayat bütün unsurlarıyla tanımlanamayacak kadar geniş bir kavram olup devletin yetkili temsilcileri tarafından ilgililer hakkında rızası olmaksızın bilgi toplamasının her zaman söz konusu kişinin özel hayatını ilgilendireceği kuşkusuzdur.

Anayasa'nın 20. ve 25. maddelerinde yer alan güvencelere rağmen itiraza konu 8. madde hükmüyle kişiler, bilgi toplama, saklama, işleme ve değiştirme tekeli olan idareye ve diğer kişilere karşı korumasız bırakılmış, veri toplamanın sınırlarına yasal düzenlemede yer verilmemiştir.

Açıklanan nedenlerle itiraz konusu kuralların Anayasa'nın 20. ve 25. maddelerine aykırı olduğundan iptali gerekir[129]*."*

Anayasa Mahkemesinin konuya ilişkin bir diğer önemli kararı ise 1774 sayılı Kimlik Bildirme Kanununa eklenen bir hüküm ile genel kolluk kuvvetlerinin bilgisayarlarında kişisel bilgilerin toplanması yetkisini, bu yetki kullanılırken hangi kurallara uyulması gerektiği belirlenmeden, tanıyan hükmüne ilişkindir. Anayasa Mahkemesinin kararda kullandığı ifadeden kişisel verilerin korunmasının Anayasanın 20. maddesi kapsamında değerlendirdiği anlaşılmaktadır[130].

"Anayasa Mahkemesi'nin 31.3.1987 gün ve E: 1986/24, K: 1987/8 sayılı kararı özel hayatın gizliliği ve korunması konusundadır (RG. 28.5.1987). Bu kararın ilgili bölümü şöyledir:

Özel hayatın korunması her şeyden önce bu hayatın gizliliğinin korunması, başkalarının gözleri önüne serilmemesi demektir. Orada cereyan edenlerin yalnız kendisi veya kendisinin bilmesini istediği kimseler tarafından bilinmesini istemek hakkı, kişinin temel haklarından biridir. Bu niteliği sebebiyledir ki, özel hayatın gizliliğine dokunulmaması, insan haklarına ilişkin beyanname ve sözleşmelerde korunması istenilmiş, ayrıca tüm demokratik ülke mevzuatında açıkça belirlenen istisnalar dışında bu hak devlet organlarına, topluma ve diğer kişilere karşı korunmuştur.

1981 tarihli "Otomatik İşlemden Geçirilen Kişisel Verilerin Korunması ve Aktarımı Hakkındaki Sözleşme"ye göre, kişi hakkındaki verilerin toplanmasında dürüst davranılmalı, yasaya uygun yöntem kullanılmalıdır. Kişi adına veriler, belli amaçlar doğrultusunda kayda geçmeli, bu amaçlar yasa ile tanınmalı ve verilerin kullanılması ancak bu amaçlar doğrultusunda olmalıdır. Verilerin kullanılmasında amaç dışına çıkılmamasına, uygunluk ve dengeye özen gösterilmesi gerekir. Tutulan veriler gerektirdiği takdirde düzeltilebilmelidir. Veriler gerçeğe uygun olmalıdır. Kişisel veriler ancak gerekli olduğu ölçüde ve amaca hizmet ettiği süre için saklanmalıdır.

---

[129] http://www.resmigazete.gov.tr/eskiler/2008/06/20080625.htm , (E.T. 04.06.2014).

[130] Küzeci, a.g.e. s. 294.

Sözleşmede "duyarlı veriler"e özel önem verilmiştir. Kişilerin ırk/soy kökeni, siyasal kanıları, dini inançları, öteki kişisel kanıları, sağlık ve cinsel yaşam verileri özel güvenceler getirilmedikçe bilgi işlem konusu olamaz. Bireylerin özellikle kişilik haklarına aykırı buldukları verileri düzeltme ve kayıttan sildirme hakları, verilere itiraz ve düzeltme hakkı, verilerin işlemden geçirilme ve değişimine karşı itiraz hakkı iç hukukta düzenlenmesi gereken güvencelerin başında gelmektedir[131]*."*

B. TÜRK CEZA KANUNU

1. Genel Olarak

5237 sayılı Türk Ceza Kanunu'nun (TCK) 135 ve devamı maddelerine göre, kişisel verilerin hukuka aykırı olarak; elde edilmesi, kaydedilmesi veya ifşa edilmesi fiilleri suç olarak düzenlenmiş ve yaptırıma bağlanmıştır[132].

TCK'nin "kişisel verilerin kaydedilmesi" başlıklı 135. maddesi kişisel verilerin ve hassas kişisel verilerin hukuka aykırı kaydedilmesini suç saymıştır. Maddeye göre;

"(1) Hukuka aykırı olarak kişisel verileri kaydeden kimseye bir yıldan üç yıla kadar hapis cezası verilir.

(2) Kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgileri kişisel veri olarak kaydeden kimse, yukarıdaki fıkra hükmüne göre cezalandırılır."

Bu maddenin devamı olan 136. madde de, kişisel verilerin hukuka aykırı olarak ele geçirilmesi ve yayılmasını aşağıdaki şekilde suç saymıştır;

"Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, iki yıldan dört yıla kadar hapis cezası ile cezalandırılır."

---

[131] http://www.kararlaryeni.anayasa.gov.tr/Karar/Content/9f7b3df0-e060-4c61-9dc8-f9e43a52adf4?excludeGerekce=False&wordsOnly=False , (E.T. 04.06.2014).

[132] TEPAV Analizi, s.44,

TCK, aynı zamanda, kişisel verilerin bu şekilde hukuka aykırı olarak kaydedilmesi, verilmesi, yayılması, ele geçirilmesi fiillerinin kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle ve belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle işlenmesi hallerini nitelikli hal olarak saymış ve bu durumlarda verilecek cezanın yarı oranında artırılacağını düzenlemiştir.

TCK, aynı zamanda silinmesi gereken kişisel verilerin silinmemesini de suç saymış ve 138. madde ile "kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde bir yıldan iki yıla kadar hapis cezası verilir" hükmü getirmiştir.

Ülkemizde kişisel verilerin korunması ile ilgili bir çerçeve kanunu bulunmaması dolayısıyla, TCK'da düzenlenen bu fillerin ne zaman hukuka aykırı, ne zaman hukuka uygun olduğunun belirlenmesi, hangi verilerin kişisel veri olduğunun belirlenmesi ya da yukarıda sayılan fiillerin tanımları ve kapsamları gibi konularda uygulamada tereddütler ortaya çıkmaktadır. Bu tereddütler, Raporun ilerleyen kısımlarında da görülebileceği gibi, çeşitli mahkeme kararlarında da görülebilmektedir. Veri koruması hukukunun ve bu konudaki farkındalığın eksikliği Türk Ceza Kanununun 135. maddesinin 1. ve 2. fıkralarında açıkça görülmektedir. Zira 135. Maddeye göre normal kişisel veriler ile özel niteliği olan (hassas) verilerin hukuka aykırı olarak işlenmesi halinde verilecek faile ceza arasında bir fark mevcut değildir. TCK'nın bu maddelerinin tam olarak yürürlüğe konabilmesi ve konu ile ilgili mahkeme kararlarındaki tereddütlerin ortadan kaldırılabilmesi için kişisel verinin ve hukuka uygun / hukuka aykırı kişisel veri işlemenin ne olduğunun, kişisel verilerin korunmasına özgü bir kanun ile belirlenmesi gerekmektedir[133].

[133] http://www.nocistanbul.com/pdf/Turkiyedeki-Kisisel-Verilerin-Korunmasinin-Hukuki-ve-Ekonomik-Analizi.pdf s.45 , (E.T. 04.06.2014).

2. Mahkeme Kararlarında Kişisel Verilerin Korunması

a. Yargıtay 12. Ceza Dairesinin 2011/20072 E. ve 2012/12126 K. Sayılı Kararı

"Türk Ceza Kanunu'nun 135.maddesinde kişisel verilerin hukuka aykırı olarak kaydedilmesi ve 136.maddesinde ise verileri hukuka aykırı olarak verme, yayma ve ele geçirme suçları düzenlenmiştir. Bugüne kadar kişisel verilerin neler olduğuna dair kanunun çıkarılmaması nedeniyle TCK'daki 135 ve 136. maddelerindeki hukuka aykırılığın hangi hallerde oluştuğuna ilişkin başvurulabilecek kapsayıcı bir kaynak ya da norm olmaması nedeniyle bu iki madde eksik norm sayılırlar. Belki zamanın ihtiyaçlarına cevap verecek "Kişisel Verilerin Korunması Kanunu" Meclisten geçtiğinde bu "çerçeve düzenleme" tamamlanmış olacaktır. Bununla beraber adı geçen ceza maddeleri yürürlükte olduğundan uygulanması sırasında çok dikkatli olunması gerekir. Doktrinde birçok tanım ve kapsam belirlemesi yapılmaktadır. Bu bilimsel görüşlerden hareketle kişisel verilerin hangileri olabileceğini belirlemek gerekir. Şu da bir gerçek ki bu verilerin tamamının da ceza normları ile korunması gerektiği düşünülmemelidir. Bu tasnifin esasını genel yaşam mahremiyetinden hareketle özel hayatın gizli alanını korumayı amaçlayan ve sağlayan bilgiler olarak anlamak gerekir.

Bilimsel görüşlerden hareketle kişisel verilerin neler olabileceğini şu başlıkları altında sınıflandırabiliriz.

a- Yaşam şekline ilişkin kişisel veriler: Kişilerin üçüncü kişiler tarafından ayırımcılığa uğramaması ve haysiyetinin korunmasıyla ilişkili olarak, dini inançları, cinsel tercihleri, etnik kökeni, suç geçmişi, politik eğilimleri ve kişisel özel aktivitelere ilişkin bilgiler bu bağlamda sayılabilecektir.

b- Ekonomik ve finansal kişisel veriler: Suçlular tarafından suiistimale ve kimlik hırsızlığına hedef olmamak için kişinin mali varlığı, sahip olduğu hisse ve hesaplar, borçları, yaptığı alış verişler, kredi kartlarına ilişkin veriler. Ayrıca sayılan bu bilgiler ile kişinin nerede ve kimlerle bulunduğuna, sağlık bilgilerine ilişkin bilgiler de ortaya çıkarabileceğinden ve varlık bilgisinin toplumsal açıdan da özel sayılmasından dolayı önemi artmaktadır.

c- Bilişim alanına ilişkin kişisel veriler: e-postaların bizzat adresleri veya şifreleri, internet ortamında paylaşılan kişisel veriler mahrem olarak değerlendirilebilir. Bunun önemi şu bakımdan artmaktadır. İnternette gezinti yapan kişi birçok kişisel bilgileri paylaşmakta, bu bilgiler kayıt altına alınmakta, yine internet erişimine ilişkin iz kayıtlarının hizmet sağlayıcı ve sunucu sahipleri tarafından tutulabiliyor olması nedenleriyle artmaktadır.

d- Sağlıkla ilgili kişisel veriler: Sağlık verileri kişilerin iş güvenliğini, toplum içindeki statüsünü ve sigorta kapsamını etkileyen hassas bilgilerdir. Ayrıca sağlık verileri kişilerin sosyal yaşantısı ve psikolojik durumları hakkında bilgi edinilmesine neden olabilir. Biyometrik (Kişinin kendine özgü fiziksel veya biyolojik niteliklerine dayalı olarak insanların kimliğini tespit için dijital teknolojiden faydalanma bilimi) veriler de kişisel veriler arasındadır.

e- Politik kişisel veriler: Toplum içinde yaşayan kişilerin siyasi tercihleri toplum katmanları arasında bilinme halinde ayırımcılığa maruz kalma ihtimali bulunduğundan bu bilgilerde kişisel veridir[134].”

b. Yargıtay 12. Ceza Dairesinin 2012/17703 E. ve 2012/18222 K. Sayılı Kararı

“5237 sayılı TCK'nın 135. maddesinde düzenlenen Kişisel verilerin kaydedilmesi suçunun oluşabilmesi için belirli veya belirlenebilir bir kişiye ait her türlü bilginin, hukuka aykırı olarak kaydedilmesi gerekmekte olup; suçun maddi konusunu oluşturan kişisel veri kavramından, kişinin, yetkisiz üçüncü kişilerin bilgisine sunmadığı, istediğinde başka kişilere açıklayarak ancak sınırlı bir çevre ile paylaştığı, herkes tarafından bilinmeyen ve/veya kolaylıkla ulaşılması ve bilinmesi mümkün olmayan, kişinin kimliğini belirleyen veya belirlenebilir kılan, kişiyi toplumda yer alan diğer bireylerden ayıran ve onun niteliklerini ortaya koymaya elverişli, gerçek kişiye ait her türlü bilginin anlaşılması gerektiği; bir özel hayat görüntüsü ya da sesinin, kişisel veri olduğunda kuşku bulunmamakta ise de, kişinin özel hayatına ilişkin görüntüsü ya

[134]http://legalbank.net/belge/y-12-cd-e-2011-20072-k-2012-12126-t-15-05-2012/1351930/K%c4%b0%c5%9e%c4%b0SEL+VER%c4%b0LER%c4%b0N+KORUNMASI (E.T. 04.05.2014)

da sesinin, bilgisi dışında, resim çekme veya kaydetme özelliğine sahip aletle belli bir elektronik, dijital, manyetik yere sabitlenmesi eyleminin, 5237 sayılı TCK'nın 134/1. maddesinin 2. cümlesinde tanımlanan özel hayatın gizliliğini ihlal suçu kapsamında değerlendirilmesi gerektiği, kişinin özel hayatına ilişkin görüntü, fotoğraf ya da sesin, 5237 sayılı TCK'nın 135. maddesi kapsamında kişisel veri olarak kabul edilemeyeceği [135] ."

c. Yargıtay 12. Ceza Dairesinin 2013/9912 E. ve 2014/4422 K. Sayılı Kararı

" Belirli veya belirlenebilir bir kişiye ait her türlü bilginin, başkasına verilmesi, yayılması ya da ele geçirilmesi, TCK'nın 136/1. maddesinde "Verileri hukuka aykırı olarak verme veya ele geçirme" başlığı altında suç olarak tanımlanmış olup, eylemin; kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak ya da belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle gerçekleşmesi hali, aynı Kanunun 137. maddesinde cezada artırım nedeni olarak öngörülmüştür.

Verileri hukuka aykırı olarak verme veya ele geçirme suçunun maddi konusunu oluşturan "kişisel veri" kavramından, kişinin, yetkisiz üçüncü kişilerin bilgisine sunmadığı, istediğinde başka kişilere açıklayarak ancak sınırlı bir çevre ile paylaştığı nüfus bilgileri (T.C. kimlik numarası, adı, soyadı, doğum yeri ve tarihi, anne ve baba adı gibi), adli sicil kaydı, yerleşim yeri, eğitim durumu, mesleği, banka hesap bilgileri, telefon numarası, elektronik posta adresi, kan grubu, medeni hali, parmak izi, DNA'sı, saç, tükürük, tırnak gibi biyolojik örnekleri, cinsel ve ahlaki eğilimi, sağlık bilgileri, etnik kökeni, siyasi, felsefi ve dini görüşü, sendikal bağlantıları gibi kişinin kimliğini belirleyen veya belirlenebilir kılan, kişiyi toplumda yer alan diğer bireylerden ayıran ve onun niteliklerini ortaya koymaya elverişli, gerçek kişiye ait her türlü bilginin anlaşılması gerekir; ancak, herkes tarafından bilinen ve/veya kolaylıkla ulaşılması ve bilinmesi mümkün olan kişisel bilgiler, yasal anlamda "kişisel veri" olarak değerlendirilemez, aksinin kabulü; anılan maddenin uygulama alanının amaçlanandan fazla genişletilerek, uygulamada belirsizlik ve hemen her eylemin suç oluşturması gibi olumsuz sonuçlar doğurur, bu nedenle, bir kişisel bilginin, açıklanan anlamda "kişisel veri" kabul edilip edilmeyeceğine karar verilirken, somut olayın özellikleri dikkate

[135] http://www.kararara.com/forum/viewtopic.php?f=46&t=9880 , (E.T. 04.05.2014)

alınarak titizlikle değerlendirme yapılması, sanığın eylemiyle hukuka aykırı hareket ettiğini bildiği ya da bilebilecek durumda olduğunun da ayrıca tespit edilmesi gerekir."

d. Yargıtay 12. Ceza Dairesinin 2012/16872 E. ve 2012/18221 K. Sayılı Kararı

TCK'da "özel hayatın gizliliğini ihlal" ve "kişisel verilerin kaydedilmesi" suçlarının iki ayrı suç olarak düzenlenmesi ve kişisel verilerin korunması ile ilgili özgül bir kanun bulunmaması dolayısıyla kapsamın tam olarak belirlenememesi durumu, Yargıtay'ın 2012/16872 E. Ve 2012/18221 K. numaralı kararında belirgindir. Yargıtay bu kararında TCK madde 135'de düzenlenen "kişisel verilerin kaydedilmesi" suçunun oluşabilmesi için, "belirli veya belirlenebilir bir kişiye ait her türlü bilginin, hukuka aykırı olarak kaydedilmesinin gerekmekte" olduğunu belirtmiştir. Bunun ardından kişisel verinin ne olduğunu tartışmış ve "'kişisel veri' kavramından, kişinin, yetkisiz üçüncü kişilerin bilgisine sunmadığı, istediğinde başka kişilere açıklayarak ancak sınırlı bir çevre ile paylaştığı, herkes tarafından bilinmeyen ve/veya kolaylıkla ulaşılması ve bilinmesi mümkün olmayan, kişinin kimliğini belirleyen veya belirlenebilir kılan, kişiyi toplumda yer alan diğer bireylerden ayıran ve onun niteliklerini ortaya koymaya elverişli, gerçek kişiye ait her türlü bilginin anlaşılması gerektiği" sonucuna varmıştır. Ancak bunun ardından Yargıtay ilginç bir karara varmış ve "bir özel hayat görüntüsü ya da sesinin, 'kişisel veri' olduğunda kuşku bulunmamakta ise de, kişinin özel hayatına ilişkin görüntüsü ya da sesinin, bilgisi dışında, resim çekme veya kaydetme özelliğine sahip aletle belli bir elektronik, dijital, manyetik yere sabitlenmesi […] 5237 sayılı TCK'nın 134/2. maddesinde özel hayatın gizliliğini ihlal suçu kapsamında düzenlendiğinden, kişinin özel hayatına ilişkin görüntüsü, fotoğrafı ya da sesinin, yasal anlamda, 5237 sayılı TCK'nın 135. maddesi kapsamında kişisel veri olarak değerlendirilemeyeceğini söylemiştir. Yani Yargıtay, kişinin özel hayatına ilişkin görüntü ya da sesinin kişisel veri olduğunu, ancak kişilerin özel hayatına ilişkin görüntü veya sesleri hukuka aykırı olarak ifşa edilmesinin kişisel verilerin kaydedilmesinden ayrı bir suç olarak düzenlendiği, bu nedenle kişinin özel hayatına ilişkin görüntüsü, fotoğrafı ya da sesinin, yasal anlamda, 5237 sayılı TCK'nın 135. maddesi kapsamında kişisel veri olarak değerlendirilemeyeceği hükmüne varmıştır. Yani Yargıtay kişinin özel hayatına ilişkin görüntü ya da sesinin hem kişisel veri olduğunu hem de kişisel veri

kapsamında değerlendirilemeyeceğini söylemektedir. Buradaki karışıklığın nedenlerinden biri, kişisel verinin tanımının bir çerçeve kanunda tam olarak yapılamaması ve birbirleri ile çok benzer konuları düzenleyen maddelerin bu durumda karışıklığa yol açması olarak düşünülebilir[136].

e. Danıştay 10.D., 27.12.2011, E:2009/9151, K: 2011/5976 Sayılı Kararı[137]

"Bireyin sağlık kurumuna başvurduğu andan itibaren hastalık ve şikâyetlerine yönelik birçok kayıt tutulmaktadır. Yataklı Tedavi Kurumları İşletme Yönetmeliği'nin 66 ncı maddesinde; yatacak hastaların kabul şekli ve işlemlerine ilişkin düzenlemeye yer verilmiştir. Buna göre; polikliniklere başvuran veya hariçten gönderilen hastalar hakkında görevli tabiplerce muayene edilerek, hasta giriş kâğıdının doldurulacağı hükme bağlanmıştır. Yönetmeliğin 67 nci maddesinde ise yatırılan hastalar hakkında tutulan hasta dosyasında nelerin bulunacağına yönelik düzenleme yapılmış; hasta dosyalarının, tıbbi müşahede muayene kağıdı, derece kağıdı ve hasta tabelası olmak üzere üç esas kısımdan oluştuğu hükmüne yer verilmiştir. Etkili bir sağlık tedavisi için bilgi hayati bir öneme sahiptir. Hastalar, kendilerinin sağlık problemlerine uygulanacak tedaviyle ilgili alınacak kararların sağlam ve kesin bilgilere dayandığını bilmeye ihtiyaç duyarlar. Bu açıdan, hasta hakkında tutulacak hasta dosyasında yer alan bilgilerin doğru ve eksiksiz olması hayati öneme sahiptir. Danıştay, hasta hakkında tutulan tıbbi kayıtların, hasta hakkında uygulanan tedavinin ve tedavide meydana gelebilecek zararlı sonucun sebebinin öğrenilmesine yaradığını, dolayısıyla bu kayıtlardaki eksikliğin, "hastanın doğruyu öğrenme hakkına engel olacağını belirtmektedir. Şiddetli bel ağrısı şikayetiyle başvurduğu Devlet hastanesinde yapılan enjeksiyon sonucu sol bacağında his kaybı oluştuğundan bahisle, olay nedeniyle uğranıldığı ileri sürülen işgücü kaybı ve tedavi giderleri karşılığı zararın tazmini istemiyle açılan davada Yüksek Mahkeme; "davacının, hakkında uygulanan tedavileri ve zararlı sonucun sebebini öğrenmesine yarayacak tıbbi kayıtların noksan olması, dolayısıyla maddi gerçeğe (rahatsızlığının

[136] http://www.nocistanbul.com/pdf/Turkiyedeki-Kisisel-Verilerin-Korunmasinin-Hukuki-ve-Ekonomik-Analizi.pd f s. 57-58, (E.T. 04.06.2014).

[137] Akgül, Danıştay Dergisi, a.g.m., s.33-36.

nedenine) hiçbir zaman ulaşamayacak ve ömür boyu şüphe duyacak olması nedeniyle uğradığı manevi zararının tazmini gerektiğine" karar vermiştir.

Danıştay'a göre; hastanın sağlık kuruluşuna başvurduğu gün ve saatin, hastaya uygulanan tedavinin, tedaviyi uygulayan doktor ve sağlık personelinin adının, kullanılan ilaç gibi bilgilerin hasta dosyasında (poliklinik defterinde) yer alması hasta haklarının gereği olup, söz konusu kayıtların düzenli ve yeterli tutulmaması, kişinin doğruyu öğrenme hakkına engel olacağından hizmet kusurunu oluşturmakta, dolayısıyla davacının uğradığı manevi zararın tazmin edilmesi gerekmektedir."

IV. BÖLÜM

AVRUPA İNSAN HAKLARI MAHKEMESİ VE KİŞİSEL VERİLERİN KORUNMASI HAKKI

A. GENEL OLARAK

AİHS'nin en önemli özelliği, kapsadığı temel hakların ve özgürlüklerin korunmasını sağlamak için getirdiği denetim mekanizmasında kendini göstermektedir. Bu denetim mekanizmasının en önemli ayağından birisini ise AİHM oluşturmaktadır[138].

AİHM vermiş olduğu kararlarla, sistemin hukuksal karakterini güçlendirmiş, böylece AİHS sistemi ile birlikte tartışılan konuların insan haklarının korunması, İnsan Hakları Hukuku ve bu kapsamdaki konular olmasını sağlamıştır[139]. AİHM, 1980'li yılların ortalarından bu yana ve artan oranda, kişisel verilerin korunmasını, AİHS'nin sağladığı güvenceler kapsamı içinde değerlendirmiştir. Nitekim Mahkemenin, bireysel özerkliği ve bilgilerin geleceğini belirleme hakkını, Sözleşme'nin 8'inci maddesiyle getirilen güvencelerin yorumlanmasında önemli bir temel ilke olarak kabul ettiği görülmektedir. Bu bağlamda AİHM, kişisel verilerin kullanımı ve kayıt altına alınması konusunda bireylerin denetim hakkının olduğunu kabul etmektedir[140]. Bununla birlikte, AİHM, önüne gelen birkaç davada, kişisel verilerin korunmasını Sözleşme'nin 8'inci maddesi kapsamında görmüş iken, kişisel verilerin işlenmesinin bütün yönleriyle Sözleşme'nin koruması altında olmadığını ve kişisel verilerin özel yaşamın gizliliği çerçevesinde korumaya değer bulmadığını kabul etmiştir. Mahkeme, somut

[138] KAPANİ, Münci., **Kamu Hürriyetleri**, Yetkin Yayınları, 7. Baskı, Ankara 1993, s. 71.

[139] YOKUŞ, Sevtap**., Avrupa İnsan Hakları Sözleşmesi'nin Türkiye'de Olağanüstü Hal Rejimine Etkisi**, Beta Yayınları, İstanbul 1996, s.9.

[140] Küzeci, a.g.e. s. 136.

uyuşmazlıkta öncelikle, ihlal edildiği öne sürülen hakkın AİHS m.8/1'de sayılan dört alandan herhangi birisine girip girmediğine bakmaktadır. Bu tespitten sonra, ortada hakkın ihlaline yol açan bir müdahale veya sınırlama olup olmadığına, son olarak da müdahalenin veya sınırlamanın Sözleşme m.8/2'de sayılan haller nedeniyle yapılıp yapılmadığına bakarak karar vermektedir[141].

B. KİŞİSEL VERİLERİN KORUNMASI HAKKINA İLİŞKİN AİHM KARARLARI

Konuyla ilgili AİHM kararlarına bakıldığında, AİHM'nin kişisel verilerin korunması hakkını çoğunlukla özel hayatın gizliliği hakkı çerçevesinde değerlendirdiği; ancak kimi kararlarında kişisel verilerin korunması hakkına ilişkin temel ilkeleri de uyguladığı görülmektedir. Kişisel verilerin korunmasıyla ilgili AİHM kararları, Mahkemenin önüne gelen uyuşmazlıklar çerçevesinde aşağıda altı başlık altında toplanacaktır[142].

1. Özel Hayat

AİHM, Pretty/Birleşik Krallık kararında, 'özel hayat' kavramının, geniş bir kavram olduğunu ve sınırlı bir tanımı verilebilecek bir kavram olmadığını ve kişinin, fiziksel ve ruhsal bütünlüğünü kapsadığını belirtmiştir[143]. AİHM'nin özel hayata ilişkin değerlendirmesi şu şekildedir: *"Özel hayat kavramını, bireyin kişisel hayatını istediği gibi yaşayabileceği bir "iç alan" ile 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 içermektedir."*[144]. Kişisel verilerin korunması hakkı, özel hayatın gizliliğinin korunması hakkının en iyi biçimde değiştirilmiş biçimi olarak kabul edilmektedir[145]. Başka bir deyişle, kişisel verilerin korunması hakkının, özel hayatın

[141] AKGÜL A., Avrupa İnsan Hakları Mahkemesi Kararlarında Kişisel Verilerin Korunması Hakkı, **Terazi Hukuk Dergisi,** Cilt 9, Sayı 92, Nisan 2014, s.75.

[142] Akgül, **Terazi Hukuk Dergisi**, a.g.m. s.75.

[143] Akgül, **Terazi Hukuk Dergisi**, a.g.m. s.75.

[144] Polater, a.g.e. s. 122.

[145] Akgül, **Terazi Hukuk Dergisi**, a.g.m. s.75.

gizliliği hakkının kendine özgü özellikleri olan bir türü olduğu ve her iki alan arasında yakın bir ilişki bulunduğu belirtilmektedir. Nitekim özellikle Anglo-Amerikan sisteminin geçerli olduğu ABD, Yeni Zelanda, Avustralya, Kanada gibi ülkelerde konuya ilişkin düzenlemelerin özel hayatın gizliliği başlığı altında yapılması bunun en önemli belirtisidir[146]. Kişisel verilerin korunması hakkı ile özel hayatın gizliliği hakkı, aralarında kesin farklılıklar çizilmekle birlikte, açık olarak temel çıkış noktaları örtüşmektedir. Ancak, kişisel verilerin korunmasıyla ilgili içtihatlar, kaçınılmaz olarak bireyin özel hayatıyla ilgili konularda daha geniş soruların sorulmasına neden olmuştur. Örneğin, Alman Anayasa Mahkemesi, hükümete genel nüfus sayımında yetki veren kanunun anayasaya aykırı olduğuna karar verdiği meşhur nüfus sayımı kararında, her bir veri öznesinin kişisel verilerinin kullanılmasını ve açıklanmasını belirleme hakkının bulunduğunu belirtmiştir[147].

Yetkili kamu idareleri, bireyin özel yaşamı hakkında bilgiyi yalnızca yasal nedenler ve toplumun menfaati nedeniyle isteyebilir. Bu yasal nedenlere doğum, evlilik ve ölüm kayıtları gibi hususları içeren bilgiler örnek olarak verilebilir[148]. Ancak, AİHM'ye göre; devletin, bireyin özel yaşamı hakkındaki bilgileri talep etmesi halinde, kural olarak bu bilgileri başka amaçlarla değerlendirmemesi ve kayda almaması gerekir. Bunun istisnası ise, AİHS'nin 8'inci maddesinin ikinci fıkrasında belirtildiği üzere yasal bir dayanağının bulunmasıdır. Amann/İsviçre kararında (27798/95 Başvuru No.) AİHM, kişisel verilerin tutulup saklanılmasının *(Rus büyükelçiliği ile telefonla görüşen kişiler hakkında gizli bilgi tutma, bu müdahalenin hukuken öngörülebilir olmaması)* bireyin özel yaşamını ilgilendirdiğini ve AİHS'nin 8'inci maddesinin ihlal edildiğini kabul etmiştir[149]. AİHM, verdiği çeşitli kararlarında, kişisel verilere yetkisiz erişim, kişisel verilerin gereğinden uzun süre sistemlerde tutulması gibi, kişisel verilerin korunması hakkı kapsamında değerlendirilen alanlara özel hayatın gizliliği hakkına ilişkin ilkeleri uygulamıştır[150]. Yasal bir dayanağı bulunmaksızın bir kişiye ait kişisel

[146] Küzeci, a.g.e. s.70.

[147] Akgül, **Terazi Hukuk Dergisi**, a.g.m. s.75.

[148] Akgül, **Terazi Hukuk Dergisi**, a.g.m. s.75.

[149] Anadolu Üniversitesi Hukuk Fakültesi, İnsan Hakları Hukuku Projesi İnsan Hakları Avrupa Mahkemesi İçtihatları, http://ihami.anadolu.edu.tr/, (E.T. 04.06.2014)

[150] Küzeci, a.g.e. s.74.

verilerin tutulup saklanılması, AİHS'nin 8'inci maddesi bağlamında bir müdahale oluşturmaktadır. Mahkemeye göre, kişisel verilerin değerlendirilip değerlendirilmediği, içeriğinin önemli olup olmadığı ve ilgilinin bundan dolayı bir zorluğa düşüp düşmediği gibi hususlar bu noktada önemli değildir[151]. Kişiler hakkında bilgi toplama ve bu bilgileri saklama sistemine ilişkin Rotaru/Romanya davasında AİHM; kamuya açık bilgilerin, düzenli olarak toplanması ve yetkili makamlarca dosyalarda saklanması halinde özel hayat kapsamına girebileceğini, bu durumun özellikle söz konusu bilgilerin kişinin geçmişine aitse daha da geçerli olduğunu belirtmiştir. Başvurucuya ait toplanan kişisel verilerin bir kısmı, elli yıldan uzun bir süre önce toplanan ve başvurucunun özellikle eğitimi, siyasi faaliyetleri ve sabıka kaydıyla ilgili bilgilerdir. Kararda, başvurucunun kişisel bilgilerinin bir kısmının yanlış ve itibarını zedeleyebilecek olması nedeniyle, bu durumun daha da geçerli olduğu ve özel hayatın gizliliğinin ihlal edildiği vurgulanmıştır[152].

Bireyin fotoğrafına ve görüntüsüne ilişkin olarak AİHM; 2003 yılında verdiği Peck/Birleşik Krallık kararında (44647/98 Başvuru No.), depresyon sırasında et bıçağıyla caddeye inip bileklerini kesme teşebbüsünde bulunan başvurucunun caddedeki Belediyeye ait görüntü kameraları tarafından hareketlerinin tespit edilmesi üzerine uyarılan polisin başvurucuya müdahale ederek önce karakola götürmesi ve tıbbi muayene ve tedaviden sonra evine götürülmesi, daha sonra başvurucunun sokaktaki görüntülerinin belediyle tarafından bazı televizyon kuruluşlarına verilerek ve kamera ile polis işbirliğinin olumlu sonuç verdiğine dair açıklamalar yapılması, başvurucunun kimliğini açığa vurmasını engelleyecek bir tedbir almadan yapılan yayınlar sonunda başvurucunun tanınması[153]; 2004 yılında verdiği Von Hannover/Almanya kararında da, başvurucunun bir Fransız restoranında arkadaşıyla birlikte fotoğrafının alınmasının özel bilgi içerdiğini belirterek Sözleşme çerçevesinde korunmaya değer bulmuştur. Buna karşın, Friedl/Avusturya davasında, kamusal bir eylemde çekilmiş olan anonim fotoğrafların saklanmasının, özel yaşama müdahale anlamına gelmediğine karar verilmiştir. Ancak, AİHM tarafından bu sonuca varılırken; söz konusu fotoğrafların,

[151] Şimşek, a.g.e., s.34.

[152] Dutertre, a.g.e. s.288.

[153] Peck/Birleşik Krallık Kararı, http://ihami.anadolu.edu.tr/aihmgoster.asp?id=3485 , (E.T. 04.06.2014)

hiçbir işleme sisteminde kayıtlı olmadıkları ve resmi makamların, verileri işleyerek, fotoğrafı çekilen kişilerin kimliğini belirlemek için tedbirler almamış oldukları dikkate alınmıştır[154].

2. Haberleşme

AİHM değişik kararlarında, özel yaşamı, kişinin özel yaşamının iç çemberi dışında bulunan başkalarıyla ilişki kurduğu alanları da kapsayacak şekilde yorumlamaktadır. Bu yorum, kişisel verilerin korunması yönünden önemli sonuçlar doğurmaktadır. Mahkeme, özel yaşamı kişinin mahrem alanıyla sınırlı görmediğinden, kişinin ev telefonu yanında, iş telefonunun dinlenmesi, Sözleşmenin 8'inci maddesinin korumasından yararlanmasını sağlamaktadır[155].

Telefon konuşmalarının gizli olarak kaydedilmesinin, Sözleşmeyle güvence altına alınan özel yaşama ve haberleşmeye saygı hakları kapsamında olduğuna, birden fazla davada karar verilmiştir. Mahkeme bir başka davada, başvuruculaın seslerinin suç isnat edildiği sırada ve polis hücresindeyken kaydedilmesinin, özel yaşamın gizliliği hakkına müdahale oluşturduğu sonucuna varmıştır[156].

Avrupa İnsan Hakları Mahkemesinin verilerin korunması bakımından önem arz eden ilk önemli kararı 6 Eylül 1978 tarihli Klass Kararı'dır. Mahkeme bu kararında özel alana telefon dinleme gibi teknik araçlarla müdahale sırasında özel koruma tedbirlerinin, kontrol mekanizmalarının ve hukuksal araçların gerekliliğini ortaya koymuştur. Avrupa İnsan Hakları Mahkemesi vermiş olduğu kararda, gizli gözetleme tedbirlerinin demokratik bir toplumda kabul edilebilmesi için, esas olarak olağan üstü bir durumun gerekli olmasını (bunun her durumda Sözleşmenin 15. maddesindeki askıya alma durumları olması gerekmemektedir), müdahalenin sınırlarım belirleyen yasal bir temelin bulunmasını, elde edilen verilerin değerlendirilmesine hukuki sınırların getirilmesini ve kötüye kullanmayı engellemeye yönelik etkili kontrol mekanizmalarının varlığını gerekli görmüştür. Görüldüğü üzere AİHM bu kararı ile gizli gözetleme tedbirlerini tamamen Sözleşmeye aykırı görmemiş bilakis gözetleme ve gizliliğin

[154] Akgül, **Terazi Hukuk Dergisi**, a.g.m. s.76.

[155] Küzeci, a.g.e. s.140

[156] Dutertre, a.g.e. s.291,

Sözleşmenin 8. maddesinin 2. fıkrasına göre meşru gösterilmesi gerekliliğini öngörmüştür. Avrupa İnsan Hakları Mahkemesine göre, şayet devlet bireyin özel yaşamına ilişkin bilgileri talep ediyorsa, kural olarak bu bilgileri başka amaçlarla değerlendirmemeli ve kayda tabi tutmamalıdır. Bu temel ilkenin istisnası ise AİHS' in 8. maddesinin 2'inci fıkrasında da belirtildiği gibi yasal bir temelin bulunmasıdır. Gerçekten de AİHM vermiş olduğu bir kararda (Leander/İsveç), şikâyetçinin Denizcilik Müzesinde marangoz olarak istihdam edilmesine izin verilmemiştir. Divan kişinin verilerinin kaydedilmesinin ve değerlendirilmesinin Avrupa İnsan Hakları Sözleşmesinin 8.maddesinin 2. fıkrası anlamında "ulusal güvenliğe" hizmet ettiğini kabul etmiştir. Bu nedenle Divan olayda yapılan müdahaleyi özel yaşama yapılmış olan ölçülü bir müdahale olarak nitelemiştir. Divan, somut olayda örneğin kaydetmenin gerektiğinde ombudsman ve de parlamento komisyonu tarafından dahi kontrol edilebileceğini belirtmiştir. AİHM, Leander/İsveç kararında verilerin kaydedilmesi ve toplanması değil aynı zamanda verilerin devrinin ve ilgilinin bilgi edinme hakkından kaçınmanın da AİHS'nin 8. maddesine bir müdahale oluşturduğuna karar vermiştir. Kısaca Leander Kararında Mahkeme, mutlaka gerekli olması ve kötüye kullanmaya karşı belirli garantilerin alınması durumunda kişisel verilerin toplanmasının AİHS 8. maddesindeki özel yaşamın gizliliği hakkına müdahale teşkil etmeyeceğini belirtmiştir[157].

Anayasalar, yürütme organının yetkilerini keyfi kullanma eğilimine karşı, halkın temsilcilerine güven duymaları nedeniyle, özgürlüklerin, yasama organınca, ancak yasayla sınırlanabileceklerini kabul etmektedir[158].

Yasayla sınırlama kaydı, yasa koyucunun yasa ile temel haklara doğrudan müdahale etmesine, sınır çizmesine ya da idareyi, temel haklara müdahale etme konusunda yetkilendirmesine imkân vermektedir. Bağlamda, gizli telefon dinlemeleri, bireyin özel yaşamına ve iletişimine ciddi biçimde müdahale oluşturmaktadır ve mutlaka açık ve kesin bir kanuna dayanmalıdır[159].

---

[157] Şimşek, a.g.e. s. 33-34.

[158] KABOĞLU, İbrahim Ö., **Özgürlükler Hukuku**, İmge Kitabevi, 6. Baskı, İstanbul 2002, s. 89.

[159] Akgül, **Terazi Hukuk Dergisi**, a.g.m. s. 76-77.

Ancak AİHM içtihatlarında, telefon dinlenilmesiyle ilgili kanunun, dinleme öncesi etkili bir yargısal denetim mekanizmasını öngörmesi ve idarenin kişilerin haklarına müdahalesinin etkili bir denetime açık olması gerektiği belirtilmektedir. Bu denetim ise tarafsızlık, bağımsızlık ve usul güvenceleri sunan mahkemeler aracılığıyla yürütülür[160]. Diğer taraftan, telefon dinlemeye olanak veren bir kanunun varlığı bile, bu olanağı kullanan kişilerin denetimi ile ilgili bir hüküm içermemesi halinde, AİHS'nin 8. maddesinin ihlali sonucunu doğurur. Nitekim AİHM, Halford/Birleşik Krallık davasında verdiği kararında, başvurucuların haberleşmesinin ve telefon görüşmelerinin yetkililer tarafından gizli olarak izlenmesine imkân veren *"kanunun sadece varlığı"* ile bu kanunun uygulanabileceği kişiler için posta ve iletişim hizmetleri kullanıcıları arasında haberleşme özgürlüğüne zarar veren bir izlenme tehdidi oluşturduğunu; bu durumun da başvurucuların aile ve özel hayatına, haberleşmesine saygı gösterilmesi haklarına karşı kamu otoritesinin bir müdahalesi anlamına geldiğini belirtmiştir[161].

Bireye ait mektuplar ve yazışmalar da, bireyin kişisel verilerini oluşturmaktadır. AİHM, bireye ait mektupların açılmasını veya okunmasını Sözleşmenin 8. Maddesinin ihlali olarak görmektedir. Campell/Birleşik Krallık kararında (13590/88 Başvuru No.); *"Başvurucu ile avukatı arasındaki haberleşme konusunda, başvurucu hangi mektubunun açılıp okunduğundan söz etmediği halde hapishanedeki yetkililer yürürlükteki yönetmelik ve talimatların Komisyon'dan gelen mektupları açma ve avukatından gelen ve avukata gönderilen mektupları açma ve okuma yetkisi verdiğini belirtmişlerdir. Bu nedenle bu olayda müdahale bulunmakta olup, 8. maddenin uygulanabilir niteliktedir. İkinci derecedeki mevzuatın (yönetmeliğin) geçerliğini incelemek kural olarak Mahkeme'nin görevi olmayıp, bu sorun ulusal mahkemelerin görevidir. Olayda ulusal mahkemeler Komisyon'dan mahpusa gelen mektubun açılmasına ve avukatıyla yazışmaların açılıp okunmasına imkan veren hapishane yönetmeliğinin geçerliliğine karar verdikleri için müdahale hukuken öngörülebilir niteliktedir. Hapishane yönetmeliğinin verdiği müdahale yetkisi 'suçu veya düzensizliği önleme' meşru amacına sahiptir. Müdahalenin gerekli olup olmadığı konusuna gelince:*

---

[160] ALTIPARMAK, Kerem., "Büyük Biraderin Gözetiminden Çıkış: Telefonların İzlenmesinde Devletin Sorumluluğu", **TBB Dergisi,** Y: 2006, S: 63, s. 51-52.

[161] GÜNTÜRK, M. Serdar., **Türk Yüksek Mahkemeleri ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Özel Hayatın Gizliliğinin Korunması**, Seçkin Yayınları, Ankara 2012, s. 117-118.

'gereklilik' kavramı haberleşmeye yapılacak müdahale için toplumsal bir ihtiyaç baskısı bulunması gerektiğine işaret etmektedir. Ayrıca müdahale meşru amaçla orantılı olmadır. Hapisliğin makul gerekleri ve mahpusun dış dünya ile tek bağlantısı olan mektuplaşması üzerinde sınırlı bir denetim uygulamak Sözleşme'ye aykırı değildir. Ancak olayda başvurucunun avukatıyla mektuplaşması bakımından, kural olarak vekil-müvekkil ilişkisinin yararlı olabilmesi için denetimden muaf tutulması gerekir. Mahpusların avukatlarıyla yaptıkları görüşmelerin dinlenememesi gibi, özel ve gizli nitelikteki mektupların da okunamaması gerekir. Bu muafiyetin istismar edilmemesini sağlamak için makul bir denetim yöntemi uygulanabilir. Olayda avukatın dürüstlüğünden veya avukatlık meslek kurallarını çiğnediğinden kuşkulanmak için bir sebep bulunmamaktadır. Bu çerçevenin dışında devletin takdir alanı bulunmadığından, müdahale demokratik bir toplumda gerekli değildir."[162].

3. Sağlık Verileri

Kişisel sağlık verileri, bireyin kişisel verilerinden bir bölümünü oluşturmakta ve sağlığına ilişkin bilgiler içermektedir. Bu veriler, bireyin hastalıklı veya sağlıklı olduğuna ilişkin bilgi içerebileceği gibi, ölümüne ilişkin bilgi de içerebilir. İdare, sağlık hizmetinin sunumu sırasında birey hakkında birçok bilgi toplamakta, bu bilgileri değerlendirmekte ve kayıt altına almaktadır. Çünkü bireye uygulanacak sağlık tedavisinin başarıya ulaşmasında, bireye ait sağlık verilerinin hayati önemi bulunmaktadır. Bireyin sağlık verileri, Avrupa Birliği uygulamasında da hassas veriler içerisinde kabul edilmektedir. Hollanda Kişisel Verilerin Korunması Kanununda, İngiltere Kişisel Verilerin Korunması Kanununda, İsveç Kişisel Verilerin Korunması Kanununda ve Yunanistan Kişisel Verilerin Koruması Kanununda bireyin sağlık verileri, hassas verileri içerisinde sayılmıştır[163].

Kişisel sağlık verileriyle ilgili Z./Finlandiya kararında AİHM, bireyin HIV testinin pozitif olduğu hakkındaki bir bilginin açıklanmasının, onun yalnızca özel ve aile yaşamını değil; sosyal ve iş durumunu da büyük ölçüde etkileyebileceğini belirtmiştir. Anılan kararda; yalnızca sağlık verilerinin korunmasının değil; bireyin kişisel

[162] Campell/Birleşik Krallık Kararı, http://ihami.anadolu.edu.tr/aihmgoster.asp?id=348 (E.T. 04.06.2014).

[163] Akgül, **Terazi Hukuk Dergisi**, a.g.m. s. 22-27.

verilerinin korunmasının AİHS'nin 8'inci maddesinde güvence altına alınan bireyin özel ve aile hayatının gizliliğinin korunmasında hayati bir öneme sahip olduğu belirtildikten sonra, kişisel sağlık verilerinin gizliliğine saygı gösterilmesinin AİHS'ye taraf olan Sözleşmeci Devletlerin yasal sistemlerinin temel prensibi olduğuna vurgu yapılmıştır. Mahkemeye göre; kişisel sağlık verilerine yönelik bu tür bir koruma olmazsa, tıbbi yardıma ihtiyacı olanlar, uygun tedaviyi almak için ve hatta tıbbi yardımın araştırılması için gerekli olan kişisel veya özel bilgilerini açıklamaktan kaçınabilir; bu durum da kendi sağlıkları açısından ve bulaşıcı hastalık söz konusu olduğunda toplum sağlığı açısından tehlikeli sonuçlara yol açabilir[164].

Bireyin sağlık verilerinin, hassas verileri içinde yer alması ve bu konuda kural olarak kesin işlem yasağı içerisinde bulunması nedeniyle işlenmesi, yetkili sağlık personeli veya sır saklamakla yükümlü kişiler tarafından yapılması gerekmektedir. Bu nedenle, olayla ilgisi bulunmayan kişi veya kişiler tarafından hassas kişisel verilerin işlenmesi hukuka aykırı olur. Konuyla ilgili olarak AİHM, AIDS taşıyıcısı eşin intihara teşebbüs etmesi halinde, korunması gereken önemli kamusal yararların bulunmasından dolayı temel hakların kısıtlanabileceği yönünde karar vermiştir[165]. Benzer şekilde, Chave/Fransa kararında; başkalarının sağlığını ve haklarını ve özgürlüklerini korumak üzere tasarlanmış kişisel dosyaların, ilgili gizlilik ve erişim kurallarıyla korunduğu, başvuranın bir psikiyatri hastanesine zorla yatırılması hakkında bilgi içeren dosyanın, psikiyatri kliniği dışından sadece belirli kategorideki kişilerin erişimine açık olduğu belirtilmiştir[166]. AİHM, önüne gelen uyuşmazlıkların bir bölümünde davaların bir bölümünde Gaskin davasında olduğu gibi sağlık ve benzeri konulardaki kişisel veri talepleri söz konusu olmuştur. Mahkeme yine 8. madde kapsamında az önce sözünü ettiğimiz denge testini uygulamış ve bilginin saklanmasındaki ağır basan kamusal yararı değerlendirmiş, kişisel çıkara ağır basan kamusal yarar durumunda ihlal bulmamıştır. Ayrıca ağır basan kamusal yararın varlığına işaret ettiği davalarda da bu çıkar çatışmasını ölçecek iç hukukta bağımsız bir organın varlığını aramış, böyle bir mekanizmanın eksik olması durumunda da 8. madde yönünden ihlal bulmuştur. Bu

[164] Akgül, **Terazi Hukuk Dergisi**, a.g.m. s.77.

[165] Özdemir, a.g.e. s. 132.

[166] Akgül, **Terazi Hukuk Dergisi**, a.g.m. s.77.

türden davalara örnek olarak da M.G/Birlesik Krallık ve Roche/Birlesik Krallık davaları verilebilir[167].

Panteleyenko/Ukrayna davasında, ceza yargılaması için gerekli olmayan, kişinin psikiyatrik verilerinin kurumdan istenilmesini ve bu raporun açık duruşma sırasında okunmasını özel yaşamın gizliliğinin ihlali olarak kabul eden AİHM64; M.S./İsveç kararında, başvuranın geçirdiği kürtaj hakkında bilgi içeren tıbbi kayıtların sosyal güvenlik kurumuna iletilmesinde geçerli ve makul gerekçelerin bulunduğunu; zira, söz konusu kurumun, başvuranın sırt yaralanmasına yönelik tazminat talebini incelemekten hukuken sorumlu olduğunu, dolayısıyla alınan önlemin, izlenen meşru amaçla orantısız olmadığını belirterek Sözleşmenin 8'inci maddesinin ihlal edilmediğine karar vermiştir[168].

4. Bilgi Edinme

Bilgi edinme hakkının bir tanımı yapılacak olursa dar anlamda bilgi edinme hakkı, devletin elinde bulunan her türlü resmi veriye erişim hakkı olarak tanımlanabilir. Daha genel anlamda ise, herkesin hiç bir devlet müdahalesi olmaksızın kendi seçimi doğrultusunda veya basın ve diğer haberleşme imkânları ile her türlü bilgiyi elde edebilmesini, hiç bir devlet müdahalesi olmaksızın tüm özel kaynaklardaki bilgiye ulaşabilmesini ve devletin elinde tuttuğu kamuyu ilgilendiren her türlü veriye erişebilmesini ifade etmektedir[169].

Bilgi edinme hakkı, bireyleri idarenin işlemleri ve eylemleri, yetkileri konusunda bilgi sahibi yaparak, bireylerin toplumu ilgilendiren bilgilere ulaşmalarını, alınan kararları sorgulayabilmelerini sağlamakta ve kamu hizmetlerinin daha etkin bir şekilde yürütülmesini güvence altına almaktadır[170].

---

[167] SOYKAN, Cavidan., "Avrupa İnsan Hakları Mahkemesi İçtihatlarında Bilgi Edinme Hakkı". **Ankara Üniversitesi Hukuk Fakültesi Dergisi**, 2007, S: 2, C: 56, s. 70, http://auhf.ankara.edu.tr/dergiler/auhfd-arsiv/AUHF-2007-56-02/AUHF-2007-56-02-soykan.pdf (E.T. 04.06.2014)

[168] Akgül, **Terazi Hukuk Dergisi**, a.g.m. s.78.

[169] Soykan, a.g.m. s. 65.

[170] Kaya, a.g.e. s. 42.

Kişiler, bilgi edinme hakkı kapsamında haklarında tutulan veya işlenen bilgilere erişme ve bu şekilde kişisel verilerini kontrol etme hakkına sahiptir. Kişisel verilerin korunması hakkı ile bilgi edinme hakkı birbirleriyle yakından ilişkili olmakla birlikte, bu ilişki birbiriyle ters orantılı olarak iki alanda ortaya çıkmaktadır. Birincisi, kişisel veriler bilgi edinme hakkı kapsamında erişilebilecek bir bilgi kategorisini oluşturmaktadır. İkincisi ise, kişisel verilerin korunması, bilgi edinme hakkını sınırlayan özel yaşamın gizliliği kapsamında yer almaktadır[171].

İfade özgürlüğünün unsurları içerisinde sayılan bilgi edinme hakkı ile ilgili olarak AİHM, bu özgürlüğün bilgiyi araştırma, toplama ve bilgiye ulaşma haklarını da içerdiğini belirtmektedir. Yine bu özgürlük, bilgileri ve fikirleri açıklama özgürlüğü ile birbirini tamamlamaktadır. Mahkeme, bilgi edinme özgürlüğünün, halkın özellikle kamu çıkarını ilgilendiren konularda yeterince bilgilendirilmesi hakkını da kapsadığını; Devlet'in, bir kişinin başkalarının kendisine vermeyi istediği veya isteyebileceği bir bilgiyi almasını engellemesini yasakladığını belirtmiştir[172].

AİHM'ne göre, başta politikacılar olmak üzere, genel olarak kamuya mal olmuş kişiler hakkında kamunun bilgi edinme hakkı, söz konusu kişilerin özel yaşamlarına ilişkin hususlara kadar genişleyebilmektedir. Bununla birlikte, kamuya mal olmuş kişi kavramı, AİHM içtihatlarında dar şekilde yorumlanmaktadır. Örneğin, politikacılar, kamuya mal olmuş kişi olarak kabul edilmekte iken; Von Hannover kararında Prenses Caroline, kamuya mal olmuş kişi olarak kabul edilmemiştir. Politikacılar özelinde, AİHM'nin önüne gelen uyuşmazlıklardan Craxi davası burada örnek olarak verilebilir. Mahkeme, devam eden suç yargılamasıyla ilgili basının haber yapma ve kamunun da bilgi edinme hakkının bulunduğunu belirterek; kamunun bilgi edinme hakkının yalnızca başvurucunun aleyhindeki suçlamaya ilişkin olguları kapsadığı, kamuya mal olmuş kişilerinde mahremiyetlerine saygı gösterilmesi hakkının bulunduğu, basında yer alan telefon konuşmalarındaki bazı detayların ise tamamen özel nitelikteki hususlar olduğu ve başvurucunun aleyhindeki suçlamayla hiçbir ilgisi bulunmadığından, AİHS'nin

[171] Kaya, a.g.e. s. 89.

[172] TANJU, Erhan., **AİHM Kararları Işığında İfade ve Basın Özgürlüğü**, Seçkin Yayınları, Ankara 2012, s. 164.

8'inci maddesi çerçevesinde özel yaşamın gizliliği hakkına müdahale oluşturduğuna karar vermiştir[173].

Bilgi edinme hakkı kapsamında devlet tarafından tutulan kayıtlara erişim amacıyla açılan Gaskin/Birleşik Krallık davasında AİHM; Sözleşmeye taraf devletlerin, resmi makamlarının tuttuğu kişisel verilere, ilgili veri sahiplerinin erişim özgürlüğünü sağlayacak etkin usuller oluşturmaları gerektiğini belirtmiştir[174]. Söz konusu kararda, kişilik hakkının korunması nedenleriyle, belirli durumlarda bireyin kişisel verilerine ilişkin bilgi edinme hakkının bulunduğunu vurgulayan Mahkeme, kişinin kendi kimliği, ailesi ve doğumunun nasıl meydana geldiği hususları hakkında bilgi edinmesi hakkının, kişiliğinin gelişmesi kavramı içinde olması nedeniyle özel yaşamının bir parçası olduğunu, dolayısıyla bu hususta ki sınırlamaların AİHS'nin 8'inci maddesinin 2.fıkrasına göre gerekçelendirilmesinin gerektiğini, ancak sınırlamanın gerekliliği belirlenirken de kapsamlı şekilde bir menfaat tartımının yapılmasının şart olduğunu belirtmiştir[175].

Mahkeme'nin kişisel verilere erişim taleplerini de ifade özgürlüğü kapsamında değerlendirmesi, bilgi edinme hakkının iki işlevi düşünüldüğünde çok daha tutarlı olacaktır. Bilgi edinme hakkının ilk işlevi açıklığı sağlamak ise, ikinci işlevi de bireyin devlet karsısında korunmasıdır. Bu bağlamda bilgi edinme hakkının aslında su üç hakkın bir bütünü olduğu söylenebilir: *Kişisel verilere erişim hakkı, resmi verilere erişim hakkı ve kamu yararı taşıyan konularda bilgilendirilme hakkı*[176].

5. Güvenlik Kayıtları

İdareler tarafından, ulusal güvenlik açısından çok önemli bir göreve alınacak bireylere ait bilgilerin elde edilmesi amacıyla güvenlik soruşturmaları yapılarak kişisel veri toplanılmaktadır. Güvenlik soruşturması, bir kişi hakkında, bir kurumun veya

---

[173] ÖNCÜ, Gülay A., **Avrupa İnsan Hakları Sözleşmesinde Özel Yaşamın Korunması**, Beta Yayınları, İstanbul 2011, s. 184-185.

[174] AKSOY, Hüseyin Can., **Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması,** Çakmak Yayınevi, Ankara 2010, s. 184.

[175] Şimşek, a.g.e. s. 36.

[176] Soykan, a.g.e. s. 73.

makamın istemi üzerine, güvenlik ya da haber alma kuruluşları tarafından, belli bir amaçla kullanılmak için rapor düzenlenmesi ve ilgili makama iletilmesidir. Güvenlik soruşturmasında amaç, kişinin, bir kamu hürriyetini kullanmasının sakıncalı olup olmadığının saptanması ve bu hürriyeti kullanmasının buna göre izin verilmesidir. Güvenlik soruşturması oldukça geniş bir uygulama alanına sahiptir. Vatandaşların devletle olan ilişkilerinde, kimi haklarını kullanabilmesi, devletin hakkında yapacağı güvenlik soruşturmasının "temiz" çıkması koşuluna bağlanmıştır. Türkiye'de bireylerin, yaşamlarının hemen her alanında devletle ilişkiye girmek zorunda kalmaları ve devasa yapısıyla devletin en büyük işveren olması, güvenlik soruşturması uygulamasının yaygınlığını ve önemini artmaktadır[177].

Askeri deniz üssünde bulunan müzedeki görevine, güvenlik soruşturması sonucunda son verilen başvurucu tarafından açılan *Leander* davasında AİHM; bir kamu makamının bireyin özel hayatıyla ilgili bilgileri saklamasının, 8'inci maddenin ihlalini oluşturduğunu ve saklanan bilgilerin daha sonra kullanılıp kullanılmamasının buna bir etkisinin bulunmadığını vurgulamakla birlikte; bu müdahalenin demokratik bir toplumda, ulusal güvenlik gibi devlete geniş bir takdir yetkisi tanıyan bir konuda ağır basan sosyal ihtiyaç nedeniyle meşru olduğuna karar vermiştir. Kamu görevinde çalışmak için gerekli güvenlik soruşturmasını geçemeyen başvurucuya ilişkin Turek/Slovakya kararında; ulusal sistemde başvurucunun, özel hayatına saygı gösterilmesi hakkının etkin biçimde korunmasını talep edebileceği gerçekçi ve etkili bir prosedürün bulunmamasını Sözleşmenin 8'inci maddesinin ihlali olarak görmüştür. Öte yandan, idare, kamu düzeni ve güvenliği açısından suçları takip edebilmek ve önleyebilmek için bireylerin kişisel verilerine ihtiyaç duymaktadır. Şüphesiz, bu ihtiyaçla birlikte, idare tarafından söz konusu kamu hizmetinin yürütülmesi sırasında bireylerin temel haklarının ve özgürlüklerinin gözetilmesi gerekir. Başvurucu hakkında emniyet tarafından tutulan kayıtların açıklanmaması nedeniyle açılan Segerstedt-Wiberg ve Diğerleri/İsveç davasında; istihbarat servislerinin, kanunlara uygun olarak demokratik bir toplumda var olabileceği kabul edilirken, vatandaşların gözetim altında tutulmasına yönelik bu yetkinin kullanımının, ancak demokratik kurumları korumak için

[177] KARAHANOĞULLARI, Onur., "Güvenlik Soruşturması", **Ankara Üniversitesi Siyasal Bilgiler Fakültesi Dergisi,** C: 53, S: 1-4, 1998, s.165. http://acikarsiv.ankara.edu.tr/browse/2614/3387.pdf?show

kesinlikle gerekli olması halinde Sözleşme tarafından meşru ve makul görülebileceği vurgulanmıştır. Bu açıklamadan sonra Mahkeme; başvuruculara ait kişisel verilerin saklanması nedeniyle Sözleşmenin 8'inci maddesinin ihlal edildiğini belirtirken, başvuruculaların kişisel verilerinin tutulduğu dosyaların ya da bu dosyalardaki bilgilerin güvenli bir şekilde silinmesine ya da düzeltilmesine yönelik bir başvuru yolunun mevcut olmamasını da Sözleşmenin ihlali olarak kabul etmiştir. AİHM, bireylerin, emniyet tarafından kişisel verilerinin tutulduğu dosyalara erişememesine ilişkin ortaya konulan gerekçelerin makul olmamasını da Sözleşmenin 8'inci maddesinin ihlali olarak görmektedir. Buna ilişkin Haralambie/Romanya kararında; nakledilen dosyaların miktarının çokluğu ya da arşiv sistemindeki eksikliklerin, başvurucunun hakkındaki bilgilere ulaşmasına izin vermek için 6 yıl beklenmesini açıklayamayacağı belirtilmiştir. Bireyler hakkında haksız olarak uzun süre bilgi tutulmasını Sözleşmeye aykırı bulan AİHM; bir tecavüz olayıyla ilgili sorgulandıktan sonra kendisi hakkında bir suçlama yapılmadığı halde, adı tecavüz suçlusu olarak polis kayıtlarına giren ve daha sonra birçok kez tecavüz şikâyetleri nedeniyle polis tarafından kontrole tabi tutulan başvurucuya ilişkin Dimitrov-Kazakov/Bulgaristan kararında; başvuranın isminin polis kayıtlarından çıkarılmamasını ve buna ilişkin itiraz mekanizmasının bulunmamasını[178]; Khelili/İsviçre kararında; Fransız bir kadının Cenevre polisinin bilgisayar veri tabanında 5 yıl boyunca "fahişe" olarak kayıt edilmesini Sözleşmenin 8'inci maddesinin ihlali olarak kabul etmiştir[179].

Sözleşmeye taraf devletlerin, resmi makamlarının tuttuğu kişisel verilere, ilgili veri sahiplerinin erişim özgürlüğünü sağlayacak etkin usuller oluşturmaları gerektiğini belirten AİHM; kişinin kendi kimliği ve ailesi hakkında bilgi edinmesi hakkının, özel yaşamının bir parçası olduğunu belirtmiştir. Kamu düzeni ve güvenliği açısından suçları takip edebilmek ve önleyebilmek için bireylerin kişisel verilerine ihtiyaç duyan idare tarafından, söz konusu kamu hizmetinin yürütülmesi sırasında bireylerin temel haklarının ve özgürlüklerinin gözetilmesi gerekir. Bu bağlamda AİHM; bireylerin, emniyet tarafından kişisel verilerinin tutulduğu dosyalara erişememesine ilişkin ortaya konulan gerekçelerin makul olmaması; bireyler hakkında haksız olarak uzun süre bilgi

[178] Akgül, **Terazi Hukuk Dergisi**, a.g.m. s.79.

[179] Akgül, **Terazi Hukuk Dergisi**, a.g.m. s.79.

tutulması; kişisel verilerinin tutulduğu dosyaların ya da bu dosyalardaki bilgilerin güvenli bir şekilde silinmesine ya da düzeltilmesine yönelik bir başvuru yolunun mevcut olmaması durumlarında Sözleşmenin 8'inci maddesinin ihlal edildiğine karar vermiştir[180].

6. DNA Profili ve Parmak İzleri

Kişisel verilerin korunması, aynı zamanda bunların zaman yönünden sınırlı kaydedilmesini zorunlu kılmaktadır. Verilerin yaratılması, kaydedilmesi ve kullanılması, esas olarak kullanma amacı için gerekli olan minimum düzeyle sınırlı olmalıdır. Ayrıca kaydedilen her türlü verinin tür ve kapsamı, veri toplamanın temelinde bulunan yasal amacın gerçekleşmesine uygun olmalı amaca ulaşmayı sağlayacak ölçü aşılarak bundan daha fazla kişisel veri kaydedilmemeli ve işlenmemelidir. Verilerin korunması aynı zamanda kişisel verilerin zaman bakımından sınırlı kaydedilmesini de gerektirmektedir. Kişisel verilerin kullanımı gibi kişisel verilerin saklanmasında da amaca bağlılık ilkesine uyulmalıdır [181]. Zira kişisel verilerin korunması düşüncesinin özünde de bu yatmaktadır. Kişisel verilerin, bir kere tutulmasından sonra, ilgilinin yaşamı boyunca bir yerde gerektiğinde kullanılmak üzere tutulması, bireyin maddi ve manevi bütünlüğünü zedeler. AİHM, verdiği çeşitli kararlarında, kişisel verilerin olması gerekenden uzun süre tutulmasının olumsuz yanlarına işaret etmiştir[182].

Van der Velden/Hollanda davasında, Mahkeme, özellikle hücre örneklerinin gelecekte kullanılma olanağı göz önüne alındığında, bunların sistematik olarak muhafaza edilmelerinin, özel yaşama saygı gösterilmesi hakkına müdahale oluşturmak için yeterli olduğuna karar vermiştir. Amann/İsviçre kararında AİHM; hücre örneklerinde bulunan kişisel bilgilerin miktarını ve türünü dikkate alarak, bunların muhafaza edilmesinin, ilgili kişilerin özel yaşamlarına saygı gösterilmesi hakkına saldırı olarak görülmesi gerektiğini; bu bilgilerin yalnızca bir kısmının, gerçekte, resmi makamlar tarafından, DNA profillerinin yaratılması için çıkartılmış ve kullanılmış olmasının ve özel bir durumda, hemen zarara sebep olmamış olmalarının önemsiz

[180] Akgül, **Terazi Hukuk Dergisi**, a.g.m. s.81.

[181] Şimşek, a.g.e. s. 85.

[182] Küzeci, a.g.e. s. 210-211.

olduğunu belirtmiştir. AİHM, DNA profilinin tutulmasıyla ilgili olarak AİHS'nin ihlal edildiği iddiasıyla S. ve Marper tarafından Birleşik Krallık aleyhine yapılan başvuru sonucunda; resmi makamların muhafaza ettikleri parmak izi, DNA profili ve hücre örnekleri kayıtlarının, belirlenmiş ya da belirlenebilecek kişilerle ilgili olduklarından kişisel veri olduğunu kabul etmiştir. Bununla birlikte Mahkeme, DNA profillerindeki ve hücre örneklerindeki kişisel bilgilerin, sonradan daha fazla kullanılabilecek olması nedeniyle, parmak izlerine ait bilgilerin tutulmasından daha ağır sonuçlara yol açabileceğini; sonuç olarak, hem hücre örneklerinin hem de DNA profillerinin ileride kullanılabilecek olması nedeniyle muhafaza edilmesinin, AİHS m.8/1 kapsamında başvuranların özel yaşamlarına saygı gösterilmesi hakkına bir saldırı olduğuna karar vermiştir. Parmak izleriyle ilgili Kinnunen/Finlandiya davasında AİHM; başvuranın yakalandıktan sonra parmak izlerinin ve fotoğraflarının muhafaza edilmesinin, bu hususların itiraz edilebilecek hiçbir sübjektif değerlendirme barındırmamaları nedeniyle, özel yaşamına müdahale oluşturmadığına karar vermekle birlikte, söz konusu verilerin, başvuranın talebi üzerine, dokuz yıl sonra imha edildiklerini tespit etmiştir[183].

Hücre örneklerinde bulunan kişisel bilgilerin miktarı ve türünü dikkate alarak, bunların uzun süre muhafaza edilmesinin, ilgili kişilerin özel yaşamlarına saygı gösterilmesi hakkına saldırı olarak görülmesi gerektiğini belirten AİHM; DNA profillerindeki ve hücre örneklerindeki kişisel bilgilerin, sonradan daha fazla kullanılabilecek olması nedeniyle, parmak izlerine ait bilgilerin tutulmasından daha ağır sonuçlara yol açabileceğini kabul ederek, hem hücre örneklerinin hem de DNA profillerinin ileride kullanılabilecek olması nedeniyle muhafaza edilmesini, Sözleşmenin 8'inci maddesinin ihlali olarak görmüştür[184].

[183] Aktaran Akgül, **Terazi Hukuk Dergisi**, a.g.m. s. 79-80.

[184] Akgül, **Terazi Hukuk Dergisi**, a.g.m., s.81.

V. BÖLÜM

KOLLUK HİZMETLERİ ve KİŞİSEL VERİLERİN KORUNMASI

A. GENEL BİLGİLER

Genel olarak, kamu düzenini koruma, kollama, suç ve suçluları tespit etme, yakalama ve bu amaçla ilgili kurum ve kuruluşlara yardımcı olma görevlerine kolluk görevleri denilmektedir. Bu genel tanım esas alındığında kolluk kavramı, yukarı da sayılan görevleri yapan, teşkilat veya bu teşkilatta çalışan bu amaçla görevlendirilmiş görevliler için kullanılmaktadır[185]. Kolluk bir yandan kamu düzenini sağlayan, koruyan ya da bozulduğunda eski durumuna getiren yönetsel etkinlikler, diğer yandan da bu tür etkinlikleri yürüten görevliler anlamında kullanılır[186].

Kolluk; emniyet ve asayiş ile kamu düzenini koruyan, toplumsal düzenini sağlayan, bozulduğunda geri getiren, suç işlenmesini önleyen kanunların ve diğer düzenleyici işlemlerin verdiği görevleri yapan suç işlendikten sonra failleri ele geçirmek görev ve yetkilerine sahip olan görevliler olarak tanımlanabilir[187].

Kolluk, kamu düzenini ve güvenliğini koruma, kollama; suç ve suçluları bulmakla görevli ve gerektiğinde zor kullanma yetkisine sahip olan ve kanunlarla verilen yetkiler çerçevesinde görev yapan bir devlet kuruluşudur. Başka bir ifade ile polis, emniyet ve asayişi sağlayan hukuki mevzuatın verdiği görevleri yapan, yine kanunların kendisine verdiği yetkileri kullanan icra ve inzibat kuvvetidir. Ülkede asayişi

---

[185] DÜNDAR, A. Nihat., **Açıklamalı-İçtihatlı-Örnek Uygulamalı Emniyet Teşkilatı ve Hizmetleri**, Yiğit Ofset, Ankara, 1988, s.1.

[186] GÖZÜBÜYÜK, Şeref., **Yönetim Hukuku,** Sevinç Matbaası, Ankara, 1989, s.185.

[187] Gündoğan Kadir., Koç Cihan., Özbudak Coşkun., **Kolluk Hukuku,** Kartal Yayınevi Ankara, 2007 s. 445–446.

sağlama görevi hükümete aittir. Hükümet içerisinde bu görev İçişleri Bakanlığı tarafından yapılır[188].

B. KOLLUĞUN GÖREVLERİ

2559 sayılı Kolluk Vazife ve Salahiyet Kanunu[189] kolluğun görevini düzenlemiştir. Bu düzenlemeye göre kolluk; Kamu düzeni ve kamu güvenliğinin sağlanmasından sorumludur ve önleyici ve adli görevleri yerine getirir.

2803 sayılı Jandarma Teşkilat, Görev ve Yetkileri Kanunu[190] bir kolluk kuvveti olan jandarmanın görevlerini; Emniyet ve asayiş ile kamu düzenini sağlamak, korumak ve kollamak, suç işlenmesini önlemek için gerekli tedbirleri almak ve uygulamak, adli görevleri yerine getirmek şeklinde düzenlemiştir.

Kanaatimizce en kapsamlı tanım Jandarma Teşkilat, Görev ve Yetkileri Yönetmeliğinde[191] yapılan; Genel kolluk, emniyet asayiş ile kamu düzeninin korunmasını sağlayan, diğer kanun ve nizamların verdiği görevleri yerine getiren ve Silahlı bir kuvvet olan Jandarma tanımıdır.

Kolluğun iki temel görevi vardır, öncelikli görevi temel hak ve özgürleri korumak, diğer görevi ise kamu düzenini sağlamaktır. Esasen temel hak ve özgürlükler korunabilmiş ise zaten kamu düzeni de sağlanmış demektir.

Klasik bakış açısıyla bakıldığında; polis halen, "somut bir tehlikenin olduğu durumlarda yetkilidir" denir. Yeni bakış açısında ise, tehlikenin doğmasını önleyecek tedbir almak da polisin görevi olarak görülmektedir. Bu önleyici yetkiler polisin kişilerle ilgili pek çok veriyi toplamasının gerekliliğini doğurmaktadır. Aynı zamanda bu düşünce, ilerde suç işleyebilecek diye insanların özel hayatlarına müdahaleyi de doğurmaktadır. Bu düşünce, araçları durdurup arama yetkisi de verir. Kameralarla açık alanların (meydan, istasyon vb.) izlenmesi yetkisini de içerir. Günümüz hukukunda

[188]SÖNMEZ, Nevzat., **Emniyet Teşkilatı Polis Meslek Hukuku**, Ankara, EGM Yayınları, 2005, s.2.

[189] R. Gazete: Tarih: 14/7/1934 Sayı: 2751.

[190] R. Gazete: Tarih: 12/3/1983 Sayı: 17985.

[191] R. Gazetenin Tarihi: 17.12.1983, No: 18254.

polis sadece somut mevcut bir tehlikeyi önlemekle değil, tehlikenin doğmasını önleyecek tedbirler almakla da yetkilidir. Bu tedbirler kişiler hakkında veri toplamasına yöneliktir. Tehlikenin doğmasının engellenebilmesi için kolluğun kuvvetli bilgilere ihtiyacı vardır. Tehlikenin önlenebilmesi, tedbirlerin gizli olmasını gerektirir. Kolluğun gizli olarak veri toplaması, bireyin yaşam alanına girmesini ve özgürlüklerine müdahaleyi kapsayacaktır[192].

C. ADLİ KOLLUK – İDARİ KOLLUK

Polis, asayişi, kamu, birey, tasarruf güvenliğini ve konut dokunulmazlığını korur (PVSK m.1). Polis, halkın ırz, can ve malını koruma ve kamunun istirahatini sağlamakla yükümlüdür; yardım isteyenlere, yardıma muhtaç olan çocuklara ve engellilere yardım eder, yasaların ve tüzüklerin kendisine verdiği görevleri yapar. Bu faaliyetler, kolluğun önleyici görevlerinden sayılır. Kolluğun görevi, suç islenmesini önleyici tedbirler almaktır(PVSK m.2) Kolluğun önleyici görevinin temelinde, bir tehlikeyi önleme düşüncesi vardır[193].

Suçu önlemek demek, suç riskinin önceden sezilmesi, görülmesi, tanınması, değerlendirilmesi ve suçun önüne geçmek için de gerekli girişimlerin yapılması demektir. Yukarıda açıklamaya çalıştığımız görevler kolluğun suçun oluşmasından önce ve suçu önlemeye yönelik faaliyetleri içermektedir. Ön alıcı faaliyetler neticesinde toplumun güven ve huzur içinde yaşaması, hak ve özgürlüklerinin koruma altında olması sağlanmış olacaktır.

Kolluğun önleme yetkisinin amacı ileriye yöneliktir. Kolluğun suç öncesi görev ve suç sonrası görev olmak üzere iki büyük görevi vardır. Önleme görevi; hükümet emirlerine, hukuk normlarına ve kamu düzenine uygun olmayan hareketlerin işlenmesinden önce önünü almak şeklinde tanımlanmıştır.

Önleme görevi suç işleninceye kadar olan safhalardan oluşur. Önleme görevlerinin bir kısmı doğrudan doğruya konusu suç teşkil eden fiil ve hareketlere karşı

---

[192] WÜRTENBERGER T., **"Tehlike Kavramı" ve Alman Uygulaması Ekseninde Kolluk Hukuku**, Tercüme Eden: Prof. Dr. Feridun Y., Ankara 2008 , s.12.

[193] Koç Coşkun., **Avrupa Birliği Üyelik Sürecinin Kolluk Mevzuatı ve Uygulamaları Üzerine Etkisi** (yüksek lisans tezi) Ankara 2007 s.10. web sayfası

tedbirlerden oluşurken, diğer kısmı ise, konusu suç teşkil etmediği halde, kamu düzenini ve asayişi temine yönelik tedbirlerdir. Bu görevler sürekli olabildikleri gibi, belli zamanlarda ifa edilen görevler de olabilirler.

Son yıllarda soruşturma makamlarınca ve özellikle de polis tarafından ceza muhakemesi öncesinde yeni bir soruşturma devresine ve bu devrede başvurulabilen yeni soruşturma yöntemlerine ihtiyaç olduğu ileri sürülmektedir. Tartışmanın esasını "suçla önleyici mücadele" kavramı oluşturur. Zamanla polisin suçla önleyici mücadele kavramına verdiği anlam değişmiş, polisin tehlikeyi önlemek görevi suçun takibi için tedbir almak, suçu önlemek ve bunun yanında gelecekteki tehlikeleri önleyebilmek amacıyla hazırlıklar yapmak olarak anlaşılmaya başlanmıştır[194]. Bu durum ceza hukukunda failin topluma kazandırılması görüşünün yerini "suçun önlenmesi için korkutma" görüşüne bırakması sonucunu doğurmuştur[195].

Ön alan soruşturmasının anlamı polisin "gelecekteki tehlikeleri önleyebilmek amacıyla tedbir alması" ibaresi altında yatmaktadır. Polisin gelecekteki tehlikeleri önleyebilmek amacıyla tedbir alması, "veri (ya da bilgi) elde etme, saklama, değiştirme, yararlanma, aktarma ve verilerin karşılaştırılması" olarak kabul edilir. O halde burada söz konusu olan kısaca veri elde etmek ve kullanmaktır. Aslında bunu istihbarat olarak nitelemek ve polisin görevleri arasında gittikçe daha fazla önem kazandığını söylemek mümkündür. Burada dikkat çekici olan husus, veri ya da bilgi elde etmenin "önleme" niteliğine sahip olması, bu yönüyle polisin bu faaliyetinin bir şüphe ya da somut bir tehlikeye dayanmasının aranmamasıdır. Böyle olunca polisin bu faaliyetlerde bulunması zaman bakımından öne çekilmiş olmaktadır. Böylece şüphe ya da tehlikenin ön alanı da polisin müdahale alanı haline getirilmiş bulunmaktadır. İşte polisin suçla önleyici mücadelesine hizmet eden bilgi elde edilmesi yönündeki tedbirler ön alan tedbirleri olarak nitelenir[196].

---

[194] ÖZBEK Veli, Özer., **Organize Suçlulukla Mücadelede Ön Alan Soruşturmaları**, http://web.deu.edu.tr/hukuk/dergiler/DergiMiz4-2/PDF/ozbek3.pdf, s.57

[195] Kunter Nurullah/Yenisey Feridun, Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku, 11 Bası, İstanbul 2000, no.48.14; s.705. Yenisey F., Organize Suçlulukla Mücadelede Özel Ceza Muhakemesi Tedbirleri, **Hukuk Kurultayı 2000**, Ankara2000, s.105.

[196] Özbek, a.g.m. s.58.

Ön alan soruşturmaları bilgi elde etmeye yönelmiş operatif, yani gizli tedbirlerdir. Bu tedbirlerin uygulanması için ne işlenmiş bir suçun aydınlatılması, ne de önlenmesi gereken somut bir tehlikenin bulunması gerekmemektedir. Aşağıda da ortaya konmaya çalışılacağı üzere günümüz suçluluk türlerinin organize niteliği ön alan soruşturmalarının iki yönünü ön plana çıkarmaktadır: 1- Ön alan soruşturmaları gizlidir. 2- Ön alan soruşturmaları bilgi elde etmeye, yani istihbarata yöneliktir. Ön alan içinde başvurulan soruşturma tedbirleri bakımından amaç çoğu zaman toplanan istihbarat ile fail hakkında hazırlık soruşturmasına başlamaya yetecek güçte delillere ulaşmaktır[197].

Gizli olarak yürütülen ön alan araştırmasında bilgi toplama işlemi kişiye ait verilerin toplanması ve işlenmesidir. Gizli yollarla kişiye ait verilerin toplanması ve işlenmesi, kişinin haklarına müdahale oluşturup oluşturmadığı konusunda farklı görüşler mevcuttur. Bu görüşlerin temelinde Alman Anayasa Mahkemesi'nin elektronik veri işlemine ilişkin kararının farklı yorumlanması yatmaktadır. Alman Anayasa Mahkemesi, modern veri işlem teknolojisinin ortaya çıkardığı tehlikelere işaret etmektedir. Tehlike, modern bilgi teknolojisinin kendine özgü veri işlem ve bağlantı olanakları yaratmasından kaynaklanmaktadır. Bundan hareketle bazı yazarlar, kişinin kendisine ait verilerin kaderini belirleme hakkını, otomatik veri işlemle sınırlı görmüşlerdir, bu görüşe göre veri elde etmenin gizli olduğu durumlarda bu hakkın koruma alanına girilmiş olmayacaktır. Diğer görüşe göre ise, kararın can alıcı yanı, vatandaşların, kişiliğini geliştirme şansına sahip olmaları için kendisi hakkında kimin neyi, ne zaman bildiğini bilmek zorunda olduğu anlatımıdır. Alman Anayasa Mahkemesi bunu özellikle, otomatik işlem bakımından tehlike altında görmüştür. Bu durumda otomatik veri işlem dışında da, pekâlâ birey kimin tarafından kendisi hakkında kişisel nitelikli bilgi elde edildiğini bilemiyorsa aynı tehlike ortaya çıkabilir. Kişisel verinin korunması, bireyin kişiliğini geliştirmesi amacını kapsamaktadır. Devletin gizli olarak kişi hakkında veri toplaması, kanaatimce kişinin kişiliğini geliştirmesi açısından bir tehlike ihtiva etmektedir. Çünkü bireyin kişiliğini geliştirmesi, kendisi hakkında kimin neyi, ne zaman bildiğini bilmesini gerektirir, devletin gizli olarak kişi hakkında veri toplaması, kişinin bu hakkını sınırlamaktadır. Bu nedenle sınırlamanın koşul ve

[197] Özbek, a.g.m. s.63.

çerçevesini, açık ve bireylerin anlayabileceği biçimde ortaya koyan ve normun açıklığı ilkesine uygun yasal bir düzenlemeye dayanması gerekir[198].

Kişisel verilerin toplanması ve kaydedilmesinde amaca uygunluk ilkesi kabul edilmiştir. Bu ilkeye göre kişisel veri hangi amaçla toplanmış ise o amaç doğrultusunda kullanılır. Kolluğun kişisel veriyi suçun önlenmesi amacıyla mı, adli amaçla mı topladığı burada önem kazanmaktadır. Uygulanan hukuk normunun koruduğu menfaate bakılır. Eğer kişisel verinin başka bir amaçla kullanılması, "ölçülülük ilkesine" uygun ise bu takdirde amaç değişikliği yapılabilir. Verinin kullanma amacı değiştirilmesi söz konusu olduğunda hakkında kişisel veri toplanmış olan birey açısından "ikinci bir temel hak ihlali" oluşur.[199].

Bir suçun işlendiğinin öğrenilmesi anından sonra, CMK madde 160 "suç işlendiği izlenimini veren hal" in varlığı ile Cumhuriyet Savcısının araştırma mecburiyeti doğar ve adli yetkiler başlar. Cumhuriyet savcısı maddi gerçeğin araştırılması ve adil yargılamanın yapılabilmesi için emrindeki adli kolluk görevlileri marifetiyle şüphelinin lehine ve aleyhine olan delilleri toplayarak muhafaza altına almakla ve şüphelinin haklarını korumakla yükümlüdür. (CMK madde160/2) Ceza Muhakemesi kanunda "acele hallerde kendiliğinden suç araştırma" yetkisi kolluğa verilmemiştir. Yeni kanunla adli kolluk Cumhuriyet savcısının emri ile suç araştırması yapabilecektir. Adli Kolluk Yönetmeliği madde 6/2 adli kolluk görevlileri kendilerine yapılan bir suça ilişkin ihbar veya şikâyeti, el koydukları olayları yakalanan kişiler ile uygulanan tedbirleri derhal Cumhuriyet savcısına bildirir ve Cumhuriyet savcısının emri doğrultusunda işin aydınlatılması için gerekli soruşturma işlemlerine başlar. Alman Ceza Muhakemesi Kanunu acele hallerde polisin kendiliğinden suç araştırması yapmasını kabul etmiştir. Hırvatistan, İngiltere ve Galler, Kuzey İrlanda, İrlanda'da polis bütünüyle bağımsız olduğu için, savcının soruşturma hususunda polise doğrudan talimat vermek için yetkisi bulunmamaktadır. Bu nedenle bu ülkelerde savcı ve polis arasında doğrudan bir komuta zinciri bulunmamakta ve savcı polise herhangi bir konuda

[198] Erdem M. Ruhan., **Ceza Muhakemesinde, Organize Suçlulukla Mücadelede, Gizli Soruşturma Tedbirleri**, Ankara 2001 s.158-159.

[199] Aktaran BAYRAM, Z., **Kolluğun, Suç Öncesi Ve Sonrası Kişisel Veri Toplama Yetkisi** (yayımlanmamış yüksek lisans tezi) İstanbul-2009, s.13.

emir verme yetkisini elinde bulundurmamaktadır. Aynı nedenle polisin de doğrudan savcının taleplerine göre hareket etme zorunluluğu yoktur[200].

D. KOLLUĞUN BİLGİ TOPLAMASI

Suç öncesi, suçun önlenmesi amacıyla kolluğun bilgi toplaması konusunda kanunda ayrı bir düzenleme yapılmamıştır. Suçun önlenmesi amacıyla bilgi toplama, kolluğun istihbarat yetkisi kapsamında değerlendirilmektedir. Bu tür bir bilgi toplama polisin etrafı kollama konusundaki görevinden kaynaklanır. Bu göreve "istihbarat toplama" adı verilir[201]. Kolluğun istihbarat yetkisi Polis Vazife ve Salahiyet Kanunu ve Jandarma Teşkilatı Görev ve Yetkileri Yönetmeliğinde düzenlenmiştir. PVSK ek madde 7'de şu şekilde tanımlanmıştır;

"Polis, Devletin ülkesi ve milletiyle bölünmez bütünlüğüne, Anayasa düzenine ve genel güvenliğine dair önleyici ve koruyucu tedbirleri almak, emniyet ve asayişi sağlamak üzere, ülke seviyesinde istihbarat faaliyetlerinde bulunur, bu amaçla bilgi toplar, değerlendirir, yetkili mercilere veya kullanma alanına ulaştırır. Devletin diğer istihbarat kuruluşlarıyla işbirliği yapar". PVSK ek madde 7'de polise genel yetki verilmiştir. Polis, ülke ve milletin bütünlüğü, anayasa düzeni ve genel güvenlik için önleyici ve koruyucu tedbirleri uygulamada yasal kaynağını bu genel düzenlemeden almaktadır. İstihbarat ile ilgili çalışmalar açık bilgi veya gizli bilgi üzerinden yapılır. Açık bilginin kişi ile ilgili olan kısmının depolanması ve sonra bunların değerlendirilmesi kişilik hakları ile ilgili olduğundan yasa ile düzenlenmelidir. Gizli bilgilere ulaşılması için de yasal düzenlemeye ihtiyaç bulunduğu açıktır. Halen mevcut olan istihbarat yasalarımız hangi yetkinin kim tarafından, nasıl kullanılacağı ve nasıl denetleneceği konusunda ayrıntılı düzenleme içermemektedir. Bunların tamamlanması gerekir[202].

İleride suç işlenmesini önlemek amacıyla polisin bilgi toplama yetkisinin doğması için "belli olayların" ortaya çıkmış olması ve bu olaylara dayanan şüphenin

---

[200] Bayram, s.9-10.

[201] YENİSEY Feridun., **Uygulanan ve Olması Gereken Ceza Muhakemesi Hukuku Hazırlık Soruşturması ve Polis**, İstanbul 1993, s. 134.

[202] Bayram, a.g.e. s. 10-11.

belli kişiler üzerinde yoğunlaşmış olması şart olmalıdır. Çünkü istihbarat yoluyla kişinin özel hayatına, kişisel verilerine, haberleşme özgürlüğüne müdahale edilmektedir. Bu haklar temel hak ve özgürlüklerden olması nedeniyle ancak Anayasa ve Uluslararası sözleşmelere uygun olarak kanuni düzenlemeler doğrultusunda müdahale edilebilir[203].

Polisin topladığı istihbari bilginin delil olarak kullanılması konusunda kanunda açık bir düzenleme mevcut değildir. PVSK ek madde 7/7'de elde edilen kayıtların birinci fıkrada sayılan amaçlar dışında kullanılamayacağı ve elde edilen bilgi ve kayıtların saklanmasında ve korunmasında gizlilik ilkesi geçerlidir. Derdiman[204]'a göre polis istihbarat yöntemleri ile elde ettiği bilgiler de bizzat saklanamayacağından adli soruşturmaya zorunlu bir dayanak teşkil eder, mahkemelerde delil olarak kullanılabilirler. Alman Hukukunda terör eylemi niteliğinde suçlarda istihbarat sonucu elde edilen bilgiler delil olarak kullanılmaktadır. Ancak Anayasa ve Ceza Muhakemesi Kanunuyla posta ve telekomünikasyon yoluyla iletişimin denetlenmesi yetkisi sınırlandırılmış ve hangi şartlarda nasıl kullanılacağı belirtilmiştir[205]. Kolluğun istihbarat amaçlı gizli tedbirlere başvurulabileceğine ilişkin belirlilik ve normun açıklığı ilkelerine uygun yasal düzenlemelerin olması ve istihbarat amaçlı toplanan bilgilerin, toplandığı amaç doğrultusunda kullanılmalıdır. İstihbarat amaçlı bilgi toplamak amacıyla başvurulan tedbirler, temel hak ve hürriyetlere müdahale oluşturduğu için bu müdahalenin kaynağı yasal bir düzenlemeden alması gerekir[206].

Kişisel verilerin toplanması ve kaydedilmesinde amaca uygunluk ilkesi kabul edilmiştir. Bu ilkeye göre kişisel veri hangi amaçla toplanmış ise o amaç doğrultusunda kullanılır. Kolluğun kişisel veriyi suçun önlenmesi amacıyla mı, adli amaçla mı topladığı burada önem kazanmaktadır. Uygulanan hukuk normunun koruduğu menfaate bakılır. Eğer kişisel verinin başka bir amaçla kullanılması, "ölçülülük ilkesine" uygun ise bu takdirde amaç değişikliği yapılabilir. Verinin kullanma amacı değiştirilmesi söz konusu olduğunda hakkında kişisel veri toplanmış olan birey açısından "ikinci bir temel

[203] Bayram, a.g.e. s. 12.

[204] DERDİMAN R. Cengiz., **Polis Yönetimi ve Hukuku**, 3. Baskı, 2007, s. 216.

[205] SEMİZ Hasan., **Uluslararası Hukuk Bakımından Terör Suçlarında Kolluk Yetkileri**, (yüksek lisans tezi) İstanbul, 2007, s. 81.

[206] Bayram, a.g.e. s. 13.

hak ihlali" oluşur. Baden-Württemberg Polis Kanununda, amaç değişikliğinin hangi hallerde hukuka uygun olduğu düzenlenmiştir[207]. Baden-Württemberg Polis Kanununda "sadece önleme amacıyla" elde edilmiş kişisel veriler ceza muhakemesi amacıyla kullanılamaz. Fakat önleme amacıyla toplanmış bulunan kişisel verilerin ceza muhakemesinde kullanılması konusunda bir düzenleme varsa bu mümkündür[208].

1. Durdurma ve Kimlik Sorma Yoluyla Kişisel Veri Elde Edilmesi

PVSK durdurma nedenlerini, yani kişileri ve araçları durdurma hususunda makul bir şüpheye ulaşmış kolluğun hangi nedenlere dayanarak bu yetkisini kullanabileceği meselesini 4/A maddesinin birinci fıkrası hükmünde dört grup halinde düzenlemiştir. Buna göre kolluk, Adli ve Önleme Aramaları Yönetmeliği'nin "durdurma ve kontrol işlemlerini düzenleyen 27. maddesinin ikinci fıkrası hükmünden de hareketle somut olayda tecrübesine dayanarak, içinde bulunduğu durumdan ve izlediği davranışlardan[209] hareketle polis, kişileri ve araçları;

a) Bir suç veya kabahatin işlenmesini önlemek,

b) Suç işlendikten sonra kaçan faillerin yakalanmasını sağlamak, işlenen suç veya kabahatlerin faillerinin kimliklerini tespit etmek,

c) Hakkında yakalama emri ya da zorla getirme kararı verilmiş olan kişileri tespit etmek,

ç) Kişilerin hayatı, vücut bütünlüğü veya malvarlığı bakımından ya da topluma yönelik mevcut veya muhtemel bir tehlikeyi önlemek, amacıyla durdurabilir.

Kimlik sorma yetkisi bir suç veya kabahatin işlenmesini ya da kişilerin hayatı, vücut bütünlüğü veya malvarlığı bakımından ya da topluma yönelik mevcut veya muhtemel bir tehlikeyi önlemek amacıyla kullanıldığında önleme tedbiri niteliği

---

[207] Aktaran Bayram, a.g.e. s.3.

[208] Bayram, a.g.e. s. 14.

[209] Erdağ İhsan, Ali., **Kolluğun "Durdurma ve Kimlik Sorma" Yetkisi** (PVSK madde 4/A), http://www.ankarabarosu.org.tr/siteler/ankarabarosu/tekmakale/2010-4/2010-4-erdag.pdf (E.T. 25.05.2014)

taşırken, suç işlendikten sonra kaçan faillerin yakalanmasını sağlamak, işlenen suç veya kabahatlerin faillerinin kimliklerini ya da hakkında yakalama emri veya zorla getirme kararı verilmiş olan kişileri tespit etmek amacıyla yapılması halinde ise adli bir görev ve yetki olarak karşımıza çıkmaktadır. Ancak bu arada gözden kaçırmamak gerekir ki; kolluğun "kimlik sorması" ile "kimlik tespit etmesi" kurumları birbirinden esasen farklı işlemlerdir. Kimlik sorma işlemi sırasında kimliği sorulan kişi kayıtlara geçirilemezken, kimlik tespit etme işlemi, bir kişinin kayıtlara geçirilmesi, yaygın ifadesiyle ile "fişlenmesi "anlamına gelmektedir.[210].

Kolluğun kişisel veri toplama yetkisi açısından durdurma sonucu elde edilen veriler, kişiye kimlik sorulması, durdurulan bir araç ise plakası, durdurma sebebine ilişkin sorular karşısında aldığı bazı bilgiler, kişisel veri niteliğindedir[211].

2. Mobil Elektronik Sistem Entegrasyonu (MOBESE) Kameraları ile Kişisel Veri Elde Edilmesi

MOBESE; Emniyet Genel Müdürlüğünün Asayiş ve Trafik güvenliğinin sağlanması ile genel güvenliğe yönelik tehditleri bertaraf etmek ve denetim görevini daha etkin gerçekleştirmek üzere mevzuata uygun olarak elde edilen görüntü, ses ve konum verilerinin işlenerek, anlamlı sonuçlar üretilmesini ve bu sonuçların POLNET uygulamaları ile desteklenmesini sağlayan, Görüntüleme, Çağrı Yönetim ve Mobil Uygulamalar alt sistemlerinden oluşan modüler olarak geliştirilmiş bilişim sistemidir[212].

İstanbul Emniyet Müdürlüğü Bilgi İşlem Daire Başkanlığı'nda çalışan 7 polisin, görev yaptıkları yerlerde görüp geliştirdikleri sisteme kısaca MOBESE adı verildi. Bu ad, çalışmalarda görev alan Murat Nazmi Akman, Mustafa Harharcı, Osman Nihat Şen,

---

[210] Yenisey, Feridun., "Faili 'Tekrar Tanımaya Yarayan' Önleme ve Koruma Tedbirleri (Durdurma, Kimlik Sorma, Kimlik Tespiti, Parmak İzi Alma, Fotoğraf Çekme, Fizik Kimliğin Tespiti)", **Polise Görev, Yetki ve Sorumluluk Veren Mevzuat Uygulamaları Eğitim Projesi (MUYEP) Tebliğleri-II**, EGM Yayın Katalog No:444, Eğitim Dairesi Başkanlığı Yayın No: 43, Ankara, 2008, s.10.

[211] Bayram, a.g.e. s. 18.

[212] http://www.trabzon.pol.tr/Sayfalar/MOBESE.aspx (E.T. 25.05.2014)

Basri Aktepe, Erin Çoban, Süleyman Demirci, Erdoğan Toprakman'ın isimlerinin baş harfinden oluşmaktadır[213].

MOBESE eş zamanlı olarak elde edilen görsel bilgilerin; delil niteliğinde saklanmasını, izlenmesini, otomatik olarak veya izleme neticesinde elde edilen alarmlar hakkında gerekli kayıt ve işlemlerin yapılmasını sağlayan donanım ve yazılımlardır. Görüntüleme Sistemi Kabiliyetleri ise elde edilen görüntü verisinin; Delil niteliğini kaybetmeden kaydedilip saklanabilmesi, fotoğraf çıktısının alınabilmesi, eş zamanlı veya geçmişe yönelik izlenebilmesi, görüntü kalitesini arttırmak veya görünebilirliği sağlamak üzere işlenebilmesi ve ilgili alt uygulamaları içermektedir. MOBESE, kayıtları ile kişinin kimliğini belirleyici fotoğraf ve görüntü kaydı yapılabilmektedir. Bu sistem sayesinde kişinin görüntü kayıtları ile kolluk, kişisel veri elde etmiş ve kaydetmiş olmaktadır. Kanun koyucunun aleni alanlara açıkça görülebilir bir şekilde denetleme kameraları koymasındaki amaç, potansiyel faillerin gözetlenen alanlarda suç işlemekten çekinecekleri beklentisidir. Ancak, bu tür kayıtların suçların aydınlatılmasında ve faillerin teşhisinde önemli bir rol oynadığı ve halktaki emniyet duygusunu güçlendirdiği de bir gerçektir. Video ile denetleme çifte karakterli bir idari işlemdir; bir taraftan suçun işlenmesi önlenirken, diğer taraftan da işlenecek olan suçun kovuşturulması kolaylaştırılmaktadır[214].

Kamusal ulaşılabilir alanlarda video gözetlemeleri ile elde edilen kişisel veriler, örneğin kişinin resmi, bireyin kişisel verilerinin akıbetini belirleme hakkıyla yakından ilgilidir. Bu resmin ilgilinin rızası dışında devredilmesi de yine kişinin resmi üzerindeki hakkım kapsayan genel kişilik hakkını ihlal edebilir. Bunun yanı sıra belirli bir kişiyi hedef almadan yapılan video gözetlemeleri de temel haklar açısından önemli olabilir. Aykırı davranış tarzı sergileyen kişilerin her zaman not edildiği ve bunların bilgi olarak kaydedildiği, kullanıldığı ve devredildiği konusundaki güvensizlik, basit olarak sadece gözlemleme amacıyla yapılan gözetlemeler karşısında dahi insanları temel hak ve özgürlüklerini kullanmaktan alıkoyabilmektedir[215]. Kamusal ulaşılabilir alanların video

[213] http://www.milliyet.com.tr/2005/06/18/guncel/gun02.html (E.T. 25.05.2014)

[214] Bayram, a.g.e. s. 31.

[215] Şimşek, a.g.e. s.145.

ile gözetlenmesi mutlaka hukuksal bir temele sahip olmalıdır. Bu hukuksal temel ise açık, anlaşılır ve meşru olmalı, video gözetlemeler sırasında ve sonrasında kişisel verilerin korunmasına ilişkin etkin bir kontrol sistemi öngörülmelidir. Kişisel verilerin korunması bakımından video gözetlemeler sırasında ve sonrasında bireyin haklarının korunmasını ve gözetlemelerin hukuksal ilke ve temellerinin belirlenmesini sağlayacak yasal düzenlemelerin yapılması bir zorunluluktur[216].

3. Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi Yolu İle Kişisel Verilerin Elde Edilmesi

Suçun işlenmesi tehlikesinin ortadan kaldırılması bu yönde bilginin elde edilmesine bağlıdır. Bu açıdan suç öncesi araştırma evresinde tehlikenin varlığı aranmadan kolluğun bilgi toplaması değerlendirmesi öngörülmektedir. Önleme dinlemesi ön alan araştırması kapsamındadır. Bu nedenle ön alan araştırmasındaki koşulların varlığının aranması gerekmektedir. Ön alan soruşturmasının hareket noktası soruşturulmaya değer bir olay ya da yasal bir şüphe kategorisi altında kabul edilmeyecek olan şüpheli hareketlerdir. Yoksa hiçbir şüphenin bulunmaması önalan soruşturmasına girişmek için yeterli olmadığı gibi belirli vakıalarla temellenmiş şüphenin varlığı da şart değildir. Adından da anlaşılacağı üzere önleme dinlemesi, iletişimlerinin denetlenmelerini gerekli kılacak makul şüphelerin oluştuğu, bu konuda ciddi bilgi aktarımlarının, üzerlerinde suç işleyeceklerine dair tereddütler oluşturduğu ve güçlendirdiği kişilerin yaptığı iletişimlerin denetlenmesi olarak yapılabilir. Aksi halde, hem Anayasanın koruması altındaki kişi hak ve hürriyetinin özüne dokunulmuş olacağı gibi, hem de yapılan bu tür işlem ve faaliyetler hukuka aykırı sayılacaktır[217].

İletişim anayasal bir özgürlük olarak tanınan ve anayasa üstü evrensel hukuk normları ile de korunan düşünce ve ifade özgürlüğünün bir uzantısı olmakla birlikte, özel hayatın sınırları içerisinde de yer almaktadır. İletişimin korunmasındaki bu çift yönlü gereklilik, iletişim özgürlüğünün de anayasal ve evrensel platformda tanınmasını sağlamıştır. İletişime yapılacak haksız müdahaleler sadece iletişim özgürlüğünü ihlal etmekle kalmayacak, hakkın doğasındaki ikili yapı nedeniyle düşünce ve ifade

[216] Şimşek, a.g.e. s.157.

[217] Bayram, a.g.e. s. 41.

özgürlüğü ile özel hayatın korunması ilkelerinin de aynı zamanda ihlal edilmesine yol açacaktır[218]. Önleme dinlemesinde elde edilen telefon numarası, ses kaydı, konuşma içeriğindeki veriler kişisel veridir. Bu verilerin elde edilmesi ve işlenmesi ancak yasal düzenleme ile mümkündür[219].

CMK' da birinci kitap, dördüncü kısım beşinci bölümde "Telekomünikasyon yoluyla yapılan iletişimin denetlenmesi" başlığı ile konu düzenlenmiştir. CMK madde 135 başlığı ise "iletişimin tespiti, dinlenmesi, kayda alınması" olarak düzenlenmiştir. Maddede üç kavram öne çıkmaktadır. Tespit, dinleme, kayda alma ve sinyal bilgilerinin değerlendirilmesidir[220].

AİHM kararlarında uygulandığı gibi telekomünikasyon araçlarıyla yapılan iletişimin denetlenmesi tedbirine "ancak demokratik kurumları korumak bakımından mutlak zorunluluk bulunması" koşuluyla başvurulabilir. Nitekim AİHM Klass ve diğerleri davasında " demokratik toplum kurumlarının korunması amacıyla" bu tedbirlere başvurulabilir demiştir. Dolayısıyla bu tedbirin uygulama amacıyla girecek suçların sınırlı olması gerekmektedir. Avrupa ülkelerinde bu tedbire başvurmak için belirli suç grupları veya fiilen ağırlığı veya işleme biçimi bakımından belirli koşullar göz önüne alınarak düzenleme yapılmıştır[221]. CMK madde 135'te bu tedbirin hangi suçlar için uygulanacağı katalog suç düzenlemesi ile belirlenmiştir. Bu suçlar belirli ağırlıkta olan ve işleniş şekilleri itibarıyla, iletişimin denetlenmesi tedbirine en çok ihtiyaç duyulacak suçlar olarak belirlenmiştir. Bu katalog tespit edilmek suretiyle, bunların dışındaki suçlarla ilgili olarak bu tedbire başvurulması engellenmiştir. Bu noktada belirli ağırlıktaki suçlarla ilgili olarak bu tedbire imkân veren hükümet tasarısından ayrılmıştır[222]. CMK madde 135'te iletişimin tespiti, dinlenmesi, kayda alınması ve sinyal bilgilerinin değerlendirilmesi dışında maddenin 4. fıkrasında sanığın

---

[218] UÇKAN Özgür., Bilgi Ekonomisi, Bilgi Toplumu, Mahremiyet ve Güvenlik, **Ankara Barosu Hukuk Kurultayı, Bilişim ve Hukuk**, 2006, s.37.

[219] Bayram, a.g.e. s. 40.

[220] Bayram, a.g.e. , s. 54.

[221] ŞİRİN Osman., **Gizli Ceza Muhakemesi Tedbirleri (Gizli Koruma Tedbirleri)** http://www.ceza-bb.adalet.gov.tr/makale/145.doc (E.T. 25.05.2014)

[222] HAKERİ Hakan., Yeni Ceza Muhakemesi Hukukunda İletişimin Tespiti, Dinlenmesi ve Kayda Alınması, **Erciyes Üniversitesi Hukuk Fakültesi Dergisi**, C.1, Sayı 1 Yıl:2006, s.22.

veya şüphelinin yakalanması için mobil telefonun yerinin hâkim veya gecikmesinde sakınca olan hallerde Cumhuriyet savcısının kararı ile tespit edilebileceği düzenlenmiştir. CMK madde 137'de kovuşturmaya yer olmadığı veya hâkim onayının alınamaması halinde kayıtların en geç on beş gün içinde yok edileceği belirtilmiştir[223].

Elde edilen bilgilerin ceza muhakemesinde kullanılmasının değil de örneğin toplanan verilerin başka yollarla elde edilen bilgilerle bağlantı kurulmasının söz konusu olduğu durumlarda haberleşme özgürlüğünün mekân itibariyle genişletilmiş koruma alanının dışına çıkmaktadır. Artık bu durumda kişinin kendisine ait verilerin kaderini belirleme hakkının sağladığı koruma devreye girer[224]. Bu özgürlük iletişimi bir bütün olarak kapsamaktadır. Gizliliğin kapsamına sadece haberleşme içeriği değil, aynı zamanda şekli, süresi, zamanı ve yerine ilişkin bilgiler de dâhildir[225].

E. KOLLUK TARAFINDAN KİŞİSEL VERİLERİN İŞLENMESİ VE KULLANILMASI

Hukukumuzda kolluk tarafından kişisel verilerin toplanması, kaydedilmesi, işlenmesi, değerlendirilmesi ve kullanılması ile ilgili olarak yasal düzenleme bulunmamaktadır.

Alman Hukukunda, belli bir amaç doğrultusunda ve hukuka uygun olarak elde edilmiş olmaları halinde kişisel verilerin bilgisayara kaydedilerek saklanması mümkündür [226].

Baden Württemberg Polis Kanununda kişisel veri toplama konusundaki genel kurallar Madde 23'de;

---

[223] Bayram, a.g.e. s. 55.

[224] Bayram, a.g.e. s. 56.

[225] SÖZÜER Adem., Türkiye'de ve Karşılaştırmalı Hukuk'ta ,Telefon, Teleks, Faks ve Benzeri Araçlarla Yapılan Özel Haberleşmenin Bir Ceza Yargılaması Önlemi Olarak Denetlenmesi, Prof. Dr. Türkan Rado'ya Armağan, **İHFM** C.IV Sayı:3 İstanbul, 1997 s. 72.

[226] **Baden-Württemberg Polis Kanunu** Tercüme eden: Prof. Dr. YENİSEY F., Bahçeşehir Üniversitesi, www.hukukturk.com/fractal/hukukTurk/pages/dwnldCntHT.jsp?...131 (E.T. 20.05.2014)

(1) Herkesin kullanabileceği genel kaynaklardan alınmadığı takdirde kişiye ilişkin bir veri sadece ilgilinin bilgisi dâhilinde olmak koşulu ile elde edilebilir. İlgilinin bilgisi olmadan veya üçüncü kişilere ait kişisel veriler, ilgilisinden elde edildiği takdirde ulaşılamayacaksa veya orantısız derecede büyük bir işgücü kaybı gerektiriyorsa veya polise verilmiş olan görevin yerine getirilmesi tehlikeye düşecekse, bu takdirde kişisel veriler bilgi verilmeden elde edilebilir.

(2) Kişisel veriler, kural olarak, açık bir şekilde elde edilir. Kişisel veri elde etmenin polis tedbiri olduğu anlaşılmadan, gizlice veri toplanması, sadece orantısız derecede büyük bir işgücü kaybı gerektiriyorsa veya polise verilmiş olan görevin yerine getirilmesi tehlikeye düşecekse veya ilgilinin üstün basan yararı bunu gerektiriyorsa, bu gibi hallerde mümkündür.

(3) Kişisel veriler açık olarak elde ediliyorsa, yazılı olarak istendiğinde, daima; diğer hallerde ise, talebi üzerine, somut halde kişisel bilgi vermesini gerektiren hukuk kuralı veya rızaya dayalı olarak kişisel veri verebileceği, ilgili kişiye bildirilir. İlgili kişinin açıkça korunması gerekli olduğu anlaşılan hukuki yararları ihlal edilebilecekse, üçüncü kişilere bildirim yapılmaz, şeklinde düzenlenmiştir.[227].

Kişisel verilerin değerlendirilmesinde polis elinde bulundurduğu verileri örnek verilerle karşılaştırma yetkisine sahiptir. Kanun maddesinde belirtilen kişilere ait verilerin polisin bilgisayarında bulunan veriler ile karşılaştırılarak tespit yapılması mecburidir. Bu kişiler dışında kalan kişilerin kişisel verilerinin polis bilgisayarında sorgulanabilmesi için, bu sorgulamanın polise verilmiş olan belli bir görevin ifası için gerekli olması şarttır.

Bavyera Polis Kanununda veri toplama konusundaki temel hükümler Madde 30'da;

(1) Polis sadece bu kanun veya özel hukuk kuralları ile polisin veri toplamasına izin verilen hallerde kişi ile ilişkili verileri toplayabilir.

[227] Baden-Württemberg Polis Kanunu Tercüme eden: Prof. Dr. YENİSEY F., Bahçeşehir Üniversitesi, www.hukukturk.com/fractal/hukukTurk/pages/dwnldCntHT.jsp?...131 (E.T. 20.05.2014)

(2) Kişisel veriler kural olarak sadece ilgiliden alınan bilgilerden oluşur. Ancak ilgili kişinin kendisinden veri almak mümkün değil ise veya bilgileri ondan almak yüksek miktarda masrafı gerektirecek veya polisin kendisine yüklenen görevleri yerine getirmesini tehlikeye düşürecek ise, ilgiliye ait kişisel veriler diğer makamlardan resmi yerlerden veya üçüncü kişilerden alınarak elde edilebilir.

(3) Kural olarak, polis tarafından toplanan kişisel veriler açıkça belli edilerek elde edilir. Bununla birlikte dış görünüş itibarıyla polis tedbiri olarak algılanmaması gereken bir veri elde etme de, eğer polisin kendisine verilmiş olan görevi başka türlü yerine getirmesi tehlikeli olacaksa veya önemli ölçüde zorlaşacaksa veya bu tür bir yöntem ilgilinin kendi menfaatleri açısından ağır bir sakınca meydana getirecek ise, bu gibi hallerde kapalı bir şekilde veri toplanabilir.

(4) Kişisel veriler ilgilisinden veya üçüncü bir kişiden açık bir şekilde elde ediliyorsa bu gibi durumlarda talep üzerine uygun bir şekilde kişiye veri elde etmenin dayandığı hukuk kuralı, somut olay içerisinde mevcut bilgi verme mükellefiyeti veya bilgi verip vermeme konusunda özgür olduğu kişiye açıklanır.

Şayet bilgi verildiği takdirde polis kendisine yüklenmiş olan görevi yerine getiremeyecekse veya üçüncü kişilerin korunmaya değer yararları zarar görecek veya tehlikeye girecekse bilgi vermekten vazgeçilebilir, şeklinde düzenlenmiştir[228].

[228] BAVYERA POLİS KANUNU, Tercüme eden: Prof. Dr. YENİSEY F.,
www.hukukturk.com/fractal/hukukTurk/pages/dwnldCntHT.jsp?...120 (E.T. 28.05.2014)

SONUÇ

Ülkemizde kamu gücünün en yoğun ve etkili olarak kullanıldığı alan kolluk faaliyetlerinin icra edildiği alandır. Bu güç kullanılırken özellikle anayasamızda düzenlenen temel hak ve özgürlüklerimiz kimi zaman kısıtlanmakta kimi zaman ise nerede ise tamamen kullanılamaz hale gelmektedir.

Anayasada belirtilen ve hür bir insan olmamızın gereği olarak sahip olduğumuz hak ve özgürlüklerin kullanılması; ***"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"*** şeklinde bir olasılıklar zincirine bağlanmıştır.

Elbette ki kolluğun görevi millî güvenlik ve kamu düzeninin korunması, suç işlenmesinin önlenmesidir. Ancak emniyet ve asayişin temini sağlanması için öncelikle onu bozacak ve suç işlenmesine neden olacak sebeplerin tespit edilerek, ortadan kaldırılmasına yönelik faaliyetlerin planlanması ve uygulanması gereklidir. Bunun yerine emniyet ve asayişin temini için kolay yol olan hak ve özgürlüklere müdahale edilmesi kalıcı bir çözüm getirmeyecektir.

Ayrıca kolluk faaliyetleri esnasında yoğun olarak kişiler verilerimiz çeşitli işlemlere tabi tutulmasına rağmen kişisel verilerin korunması konusunda mevcut bir yasal düzenleme bulunmamaktadır.

Başta anayasamız ve ceza kanunumuz olmak üzere mevzuatımızda kapsamlı bir düzenleme yapılarak kişisel verilerin korunması öncelikli olarak zihinsel ikincil olarak ise yasal bir koruma kalkanı altına alınmalıdır.

Özellikle kolluk faaliyetleri alanında kişisel verilerin toplanması, kaydedilmesi ve değerlendirilmesi başta olmak üzere kişisel verilerimizin kullanıldığı tüm işlemler yasal olarak düzenlenmelidir. Bu düzenlemeler yapılırken de kamu güvenliği veya emniyet ve asayişin sağlanması gibi genel geçer nedenlerle değil daha somut ve dar kapsamlı düzenlemeler ile kişisel verilerin işleme tabi tutulması sıkı kurallara bağlanmalıdır.

Bizi biz yapan ve kendimizi tanımlamamızı sağlayan veriler kişisel verilerimizdir. Kişisel verilerimiz korunmadığı takdirde özel hayatımız ve kişiliğimiz de anonim hale gelmiş olacaktır. İnternet ve sosyal medya olarak tanımladığımız sanal dünya zaten bize özel alanı olabildiğine daralmışken yasa koyucunun bu alanın korunmasında daha hızlı ve çözüm odaklı adımlar atması gereklidir.

Nihayetinde her konuda olduğu gibi kişisel verilerin korunması konusunda da öncelikli olarak toplumsal bir bilinç düzeyi oluşturulmalıdır. Bu algıyı toplumsal düzeyde oluşturamadığımız takdirde çabalarımız ve önerilerimiz, "*kişisel verilerin korunması hakkında yapacağımız yasal düzenlemede olduğu gibi"* sadece kâğıt üzerinde ve *"tasarı olarak"* kalacaktır.

Kolluk kuvvetlerinin adli ve önleyici olmak üzere iki ana görevi vardır. Kamu düzenini korunmasını amaçlayan ve emniyet ve asayişi sağlamanın ana hedef olarak belirlendiği suçun önlenmesine yönelik faaliyetler önleyici hizmetlerdir, genellikle de idari faaliyetlerden oluşur.

Suç şüphesinin ortaya çıkması ile başlayan faaliyetler ise adli görevlerdir ve adli işlemlerden oluşur. Kolluk kuvvetleri adli görevlerini yerine getirir iken Cumhuriyet Savcılarının talimatları ile hareket ederler ve hareket sahalarını, yetki ve sorumlulukların belirleyen düzenlemelere sahiptirler, ancak önleyici faaliyetlerde bu durum farklıdır.

Kolluğun suç işlenmesinin önlenmesini amaçlayan faaliyetleri kısmen de olsa kendi inisiyatifi ile hareket edebildiği alandır. Çünkü bu görevler tam ve ayrıntılı olarak düzenlenmemiştir. Özellikle de önleyici kapsamda yaptığı bilgi toplama ya da istihbarat

faaliyeti olarak adlandırabileceğimiz faaliyetleri esnasında kimin güdümünde olacağı ve hangi yetkileri nasıl kullanacağı açık değildir ve sınırları belirlenmemiştir.

Cumhuriyet savcısı, ihbar veya başka bir suretle bir suçun işlendiği izlenimini veren bir hâli öğrenir öğrenmez kamu davasını açmaya yer olup olmadığına karar vermek üzere hemen işin gerçeğini araştırmaya başlar. Cumhuriyet savcısı, doğrudan doğruya veya emrindeki adlî kolluk görevlileri aracılığı ile her türlü araştırmayı yapabilir, bu araştırma bütün kamu görevlilerinden her türlü bilgiyi isteyebilir.

Adli kolluk görevlileri Cumhuriyet savcısı tarafından verilen görevleri yerine getirir. Adli kolluk görevlileri ayrıca el koydukları olayları, yakalanan kişiler ile uygulanan tedbirleri emrinde çalıştıkları Cumhuriyet savcısına derhâl bildirmek ve bu Cumhuriyet savcısının adliyeye ilişkin bütün emirlerini gecikmeksizin yerine getirmekle yükümlüdür.

Kolluk görevlileri Cumhuriyet savcısının suça ilişkin yaptığı araştırma faaliyetlerinde kullandığı en önemli enstrümandır ve buraya kadar açıkladığımız konular tamamen suç şüphesinin ortaya çıkmasından itibaren başlayan sürece ilişkindir.

Kolluk görevlileri kanunların kendilerine verdiği yetki ve sorumluluklar çerçevesinde suçu önlemek, emniyet ve asayişi sağlayabilmek için bir takım önleyici faaliyetler icra etmek zorundadır. Suçun önlenmesine yönelik faaliyetlerin başında ise önleyici istihbarat faaliyeti diyeceğimiz suç işlenmeden önce suça ilişkin iz, emare ve bulguların araştırılması faaliyeti gelecektir. İngilizce ve Fransızcada “intelligence” kelimesi ile ifade edilen ve anlamı zekâ, akıl olan istihbarat kelimesinin Türkçedeki anlamı haberdir. Haber ham bir bilgidir amaca hizmet edecek bir istihbarat haline gelmesi için işlemlere tabi tutulması gereklidir. İstihbarat ise belirlenen bir amaca yönelik toplanan bilgi, belge ve dokümanların işleme tabi tutulmuş halidir. Kolluk görevlileri önleyici hizmetleri yerine getirmek için araştırma yapacak, bil-belge-doküman toplayacak, yaptığı araştırma neticesinde elde ettiği bulguları işleme tabi tutarak suçun önlenmesine yönelik istihbarat elde etmiş olacaktır.

Suçun işlenmesinden sonra soruşturma faaliyeti başladığından dolayı bu aşamada elde edilecek bilgiler istihbarat olmayacak ve yapılan araştırma faaliyetleri istihbarat faaliyeti alanına girmeyecektir.

Diğer önemli bir husus ise istihbarat faaliyetleri suç ve suçlunun varlığını ortaya çıkarmaya yönelik olduğundan ceza soruşturmasında delil olarak kullanılamayacak suçun aydınlatılmasında ve suçlunun yakalanmasında yol gösterici olacaktır. *Yapılan istihbarat faaliyetleri neticesinde suça ilişkin kuvvetli bir şüphenin ortaya çıkması durumunda Ceza Muhakemesi Kanunumuz gereğince Cumhuriyet savcısına bilgi verilecektir, suçun öğrenilmesi ile adli süreç başlamış ve ön araştırma faaliyetleri sona ermiş olacaktır.*

Çalışmamızda nihai hedef; kişisel verilerin korunması alanında yapılan ulusal ve uluslararası düzenlemeleri inceleyerek kolluğun önleyici hizmetleri esnasında hem kişisel verilerin korunmasını hem de suç ve suçlu ile etkin bir şekilde mücadele etmesini sağlamak yönünde bir katkı sağlamaktır. Bu amaçla;

. Kişisel Verilerin Korunması ile ilgili kanun tasarısının, uluslararası antlaşmalar ve veri koruma hukukunun genel ilkeleri göz önüne alınarak güncellenmesi ve yasalaşması,

. Kolluk hizmetleri esnasında kişisel verilerin kullanılmasının özel bir yasa ile düzenlenmesi gerektiği kanaatindeyiz.

KAYNAKÇA

AKGÜL, Aydın. Avrupa İnsan Hakları Mahkemesi Kararlarında Kişisel Verilerin Korunması Hakkı, **Terazi Hukuk Dergisi,** Cilt 9, Sayı 92, Nisan 2014

AKGÜL, Aydın. Danıştay Kararları Işığında Kişisel Sağlık Verilerinin Korunması, **Danıştay Dergisi,** Sayı 133, 2013.

ALTIPARMAK, Kerem. "Büyük Biraderin Gözetiminden Çıkış: Telefonların İzlenmesinde Devletin Sorumluluğu", **TBB Dergisi,** Y: 2006, S: 63.

ATAK, Songül. Avrupa Konseyinin Kişisel Veriler Açısından Sağladığı Temel Güvenceler, **TBB Dergisi,** 2010.

ATAK, Songül. Kişisel Verilerin Korunmasına İlişkin Avrupa Birliği Yönergesinin Temel Özellikleri, **Kazancı Hakemli Hukuk Dergisi** (sayı 59-60), 2009.

BAYRAM, Zeynep. Kolluğun, **Suç Öncesi ve Sonrası Kişisel Veri Toplama Yetkisi** (yayımlanmamış yüksek lisans tezi) İstanbul-2009.

BADEN-WÜRTTEMBERG POLİS KANUNU Tercüme eden: Prof. Dr. YENİSEY Feridun. Bahçeşehir Üniversitesi.

BAŞALP, Nilgün. **Kişisel Verilerin Korunması ve Saklanması,** Yetkin, Ankara 2004.

BAVYERA POLİS KANUNU, Tercüme eden: Prof. Dr. YENİSEY Feridun.

CİVELEK, Dilek Yüksel. **Kişisel Verilerin Korunması Ve Bir Kurumsal Yapılanma Önerisi** (Uzmanlık Tezi).

DERDİMAN, Ramazan Cengiz. **Polis Yönetimi ve Hukuku,** 3. Baskı, 2007.

DUTERTRE, Gilles. **Avrupa İnsan Hakları Mahkemesi Kararlarından Örnekler,** Avrupa Konseyi Yayınları, Ankara 2007.

DÜNDAR, Ahmet Nihat., **Açıklamalı-İçtihatlı-Örnek Uygulamalı Emniyet Teşkilatı ve Hizmetleri,** Yiğit Ofset, Ankara, 1988.

ERDAĞ, Ali İhsan. Kolluğun "Durdurma ve Kimlik Sorma" Yetkisi (PVSK madde 4/A).

ERDEM, Mustafa Ruhan., **Ceza Muhakemesinde, Organize Suçlulukla Mücadelede, Gizli Soruşturma Tedbirleri,** Ankara 2001.

ERSOY Uğur,. 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 2009

GÜNTÜRK, M. Serdar. **Türk Yüksek Mahkemeleri ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Özel Hayatın Gizliliğinin Korunması,** Seçkin Yayınları, Ankara 2012.

GEMALMAZ, Mehmet Semih. **Ulusal Üstü İnsan Hakları Hukukunun Genel Teorisine Giriş Cilt 1,** Legal, 2012 İstanbul.

GÜNDOĞAN Kadir., KOÇ Cihan., ÖZBUDAK Coşkun. **Kolluk Hukuku** Ankara Kartal Yayınevi 2007.

GÜLENER, Serdar. Dijital Hafızadan Silinmeyi İstemek: Temel Bir İnsan Hakkı Olarak "Unutulma Hakkı", **TBBD Sayı 102, 2012.**

GÖZÜBÜYÜK, Şeref. **Yönetim Hukuku,** Sevinç Matbaası, Ankara, 1989.

HAKERİ, Hakan**.** Yeni Ceza Muhakemesi Hukukunda İletişimin Tespiti, Dinlenmesi ve Kayda Alınması, **Erciyes Üniversitesi Hukuk Fakültesi Dergisi, C.1, Sayı 1 Yıl:2006.**

KABOĞLU, İbrahim ÖZDEN. **Özgürlükler Hukuku,** İmge Kitabevi, 6. Baskı, İstanbul 2002.

KAPANİ, Münci. **Kamu Hürriyetleri,** Yetkin Yayınları, 7. Baskı, Ankara 1993.

KARLIDAĞ, Serpil. **Amme İdaresi Dergisi, Cilt 46, Sayı 1,** Mart 2013.

KARAHANOĞULLARI, Onur. Güvenlik Soruşturması, **Ankara Üniversitesi Siyasal Bilgiler Fakültesi Dergisi,** C: 53, S: 1-4, 1998.

KAYA, Cemil. **İdare Hukukunda Bilgi Edinme Hakkı,** Seçkin Yayıncılık, Ankara, Mayıs 2005.

KETİZMEN, Muammer., **Türk Ceza Hukukunda Bilişim Suçları,** 1. Basım, Adalet Yayınları, Ankara, 2008.

KILINÇ, Doğan. Anayasal Bir Hak Olarak Kişisel Verilerin Korunması, **AÜHFD,** 61 (3), 2012.

KOÇ Coşkun. Avrupa Birliği Üyelik Sürecinin Kolluk Mevzuatı ve Uygulamaları Üzerine Etkisi **(yüksek lisans tezi)** Ankara 2007.

KÜZECİ, Elif. **Kişisel Verilerin Korunması,** Turhan Kitabevi, ANKARA 2010.

ÖNCÜ, Gülay Arslan. **Avrupa İnsan Hakları Sözleşmesinde Özel Yaşamın Korunması,** Beta Yayınları, İstanbul 2011.

ÖZBEK, Veli Özer. Organize Suçlulukla Mücadelede Ön Alan Soruşturmaları, **DEÜ Huk. Fak. Dergisi,** C.4, S. 2, 2002.

ÖZDEMİR, Hayrunnisa. **Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması,** Seçkin ANKARA 2009.

POLATER, Yusuf Ziya. **Türk Hukukunda ve Avrupa İnsan Hakları Sözleşmesinde Özel Hayatın Gizliliği ve Korunması,** Adalet Yayınları, Ankara 2010.

SEMİZ, Hasan. Uluslararası Hukuk Bakımından Terör Suçlarında Kolluk Yetkileri, **(yüksek lisans tezi)** İstanbul, 2007.

SOYKAN, Cavidan. "Avrupa İnsan Hakları Mahkemesi İçtihatlarında Bilgi Edinme Hakkı". **Ankara Üniversitesi Hukuk Fakültesi Dergisi,** S: 2, C: 56, 2007.

SOYKAN Cavidan, **Bireysel Gizlilik ve Kişisel Verilere Erişim Hakkı, XI. Türkiye'de İnternet Konferansı Bildirileri,** TOBB Ekonomi ve Teknoloji Üniversitesi, 21 - 23 Aralık 2006, Ankara.

SÖNMEZ, Nevzat. Emniyet Teşkilatı Polis Meslek Hukuku, **EGM Yayınları,** Ankara, 2005.

SÖZÜER Adem. Türkiye'de ve Karşılaştırmalı Hukuk'ta, Telefon, Teleks, Faks ve Benzeri Araçlarla Yapılan Özel Haberleşmenin Bir Ceza Yargılaması Önlemi Olarak Denetlenmesi, Prof. Dr. Türkan Rado'ya Armağan**, İHFM C.IV Sayı:3** İstanbul, 1997.

ŞİMŞEK, Osman. **Anayasa Hukukunda Kişisel Verilerin Korunması,** Beta, 2008 İSTANBUL.

ŞİRİN, Osman. **Gizli Ceza Muhakemesi Tedbirleri** (Gizli Koruma Tedbirleri).

TANJU, Erhan. **AİHM Kararları Işığında İfade ve Basın Özgürlüğü,** Seçkin Yayınları, Ankara 2012.

TBD Kamu-BİB Kamu Bilişim Platformu X, s. 24-25, Kişisel Verilerin Korunması 2. Çalışma Grubu, **Bilişim Dergisi,** Nisan 2008.

UÇKAN Özgür. Bilgi Ekonomisi, Bilgi Toplumu, Mahremiyet ve Güvenlik, Ankara Barosu Hukuk Kurultayı, **Bilişim ve Hukuk Dergisi,** 2006.

YOKUŞ, Sevtap**. Avrupa İnsan Hakları Sözleşmesi'nin Türkiye'de Olağanüstü Hal Rejimine Etkisi,** Beta Yayınları, İstanbul 1996.

WÜRTENBERGER, Thomas. **"Tehlike Kavramı" ve Alman Uygulaması Ekseninde Kolluk Hukuku,** Tercüme Eden: Prof. Dr. Feridun Yenisey. Ankara 2008.

YENİSEY, Feridun. **Uygulanan ve Olması Gereken Ceza Muhakemesi Hukuku Hazırlık Soruşturması ve Polis**, İstanbul 1993.

YENİSEY, Feridun. “Faili ‘Tekrar Tanımaya Yarayan’ Önleme ve Koruma Tedbirleri (Durdurma, Kimlik Sorma, Kimlik Tespiti, Parmak İzi Alma, Fotoğraf Çekme, Fizik Kimliğin Tespiti)”, **Polise Görev, Yetki ve Sorumluluk Veren Mevzuat Uygulamaları Eğitim Projesi (MUYEP) Tebliğleri-II,** EGM Yayın Katalog No:444, Eğitim Dairesi Başkanlığı Yayın No: 43, Ankara, 2008.

İNTERNET KAYNAKLARI

http://www.haberler.com/izmir-yargitay-baskani-alkan-dunya-perdesi-olmayan-4770413-haberi/

http://www.bilgitoplumu.gov.tr/Documents/1/tezler/Kisisel_Verilerin_Korunmasi-Dilek_Civelek-DPT_Uzmanlik_Tezi.pdf

http://www.ab.gov.tr/files/AB_Iliskileri/AdaylikSureci/IlerlemeRaporlari/2012_ilerleme_raporu_tr.pdf

www.idare.gen.tr/akkillioglu-idariusul.htm

http://www.tbd.org.tr/usr_img/cd/kamubib15/raporlarPDF/RP2-2008.pdf

http://web.deu.edu.tr/ab/MAKALE/deu%20MAK/0012.htm ,

https://yenianayasa.tbmm.gov.tr/docs/gerekceli_1982_anayasasi.pdf

http://www.kgmd.adalet.gov.tr/kisiselverilerinkorunmasikanunu.htm

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

http://www.ihop.org.tr/dosya/coe/EC_DIRECTIVE_95_46_Kisisel_Veriler.pdf

http://www2.tbmm.gov.tr/d23/1/1-0576.pdf

www.yargitay.gov.tr/abproje/belge/.../aihm_kararlarindan_ornekler.pdf

http://oecd.nedir.com/

http://www.oecd.org/document/18/0,2340, en_2649_34255_1815186_1_1_1_1,00.html

http://tr.wikipedia.org/wiki/Birle%C5%9Fmi%C5%9F_Milletler

http://dergiler.ankara.edu.tr/dergiler/38/1690/18020.pdf

http://www.alomaliye.com/kasim_05/5429_sayili_kanun_istatistik.htm

http://bilisimsurasi.org.tr/listeler/tbs-hukuk/Mar/att-0044/01-KİSEL_VER_LER_N_KORUNMASI.doc.

http://tbbdergisi.barobirlik.org.tr/m2012-102-1218

http://www.danistay.gov.tr/dergiler/133.pdf

http://tk.gov.tr/mevzuat/yonetmelikler/dosyalar/EHSKVIGKHak_Yon_Konsolide_Metin_2013.pdf

http://www.nocistanbul.com/pdf/Turkiyedeki-Kisisel-Verilerin-Korunmasinin-Hukuki-ve-Ekonomik-Analizi.pdf

http://www.resmigazete.gov.tr/main.aspx?home=http://www.resmigazete.gov.tr/eskiler/2008/06/20080625.htm&main=http://www.resmigazete.gov.tr/eskiler/2008/06/20080625.htm

http://www.kararlaryeni.anayasa.gov.tr/Karar/Content/9f7b3df0-e060-4c61-9dc8-f9e43a52adf4?excludeGerekce=False&wordsOnly=False

http://legalbank.net/belge/y-12-cd-e-2011-20072-k-2012-12126-t-15-05-2012/1351930/K%c4%b0%c5%9e%c4%b0SEL+VER%c4%b0LER%c4%b0N+KORUNMASI

http://www.kararara.com/forum/viewtopic.php?f=46&t=9880

http://www.yargitay.gov.tr/abproje/belge/kitaplar/aihm_kararlarindan_ornekler.pdf

http://tbbdergisi.barobirlik.org.tr/m2006-63-206

http://www.inhak.adalet.gov.tr/tematik/bilgi/kisisel_veriler.pdf

http://auhf.ankara.edu.tr/dergiler/auhfd-arsiv/AUHF-2007-56-02/AUHF-2007-56-02-soykan.pdf

http://acikarsiv.ankara.edu.tr/browse/2614/3387.pdf?show

http://www.inhak.adalet.gov.tr/tematik/bilgi/kisisel_veriler.pdf

http://web.deu.edu.tr/hukuk/dergiler/DergiMiz4-2/PDF/ozbek3.pdf

http://www.ankarabarosu.org.tr/siteler/ankarabarosu/tekmakale/2010-4/2010-4-erdag.pdf

http://www.trabzon.pol.tr/Sayfalar/MOBESE.aspx

http://www.milliyet.com.tr/2005/06/18/guncel/gun02.html

http://www.ceza-bb.adalet.gov.tr/makale/145.doc

www.hukukturk.com/fractal/hukukTurk/pages/dwnldCntHT.jsp?...131

www.hukukturk.com/fractal/hukukTurk/pages/dwnldCntHT.jsp?...120

http://www.kgm.adalet.gov.tr/Faaliyetler/Donemfa/24DonemFal/24.%20dönem%20faaliyet%20raporu.pdf

http://yayin.todaie.gov.tr/yazar.php?Yazar=1085

http://www.anayasa.gov.tr/files/bireysel_basvuru/AIHS_tr.pdf

http://ihami.anadolu.edu.tr/