BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU

ELEKTRONİK HABERLEŞME SEKTÖRÜNDE KİŞİSEL VERİLERİN İŞLENMESİ, SAKLANMASI VE GİZLİLİĞİNİN KORUNMASI

Osman ŞAHİN

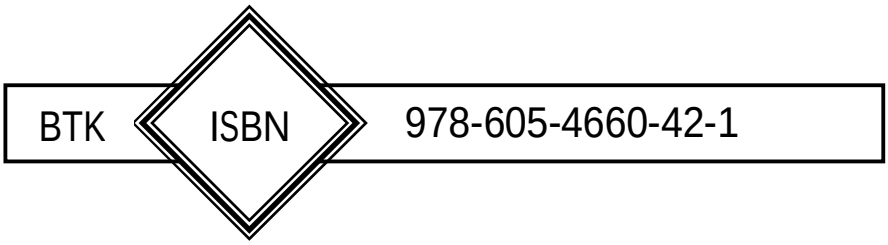
Bilişim Uzmanlığı Tezi

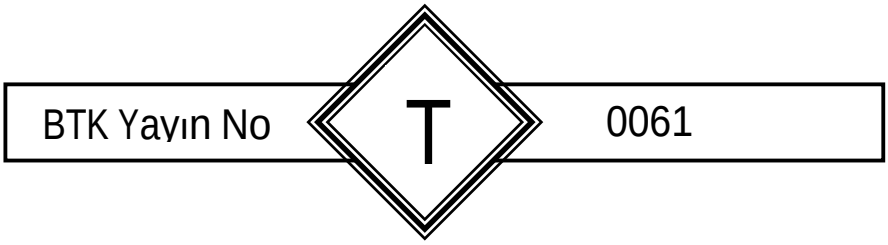
Haziran 2011

Ankara

Bu yayında öne sürülen fikirler eserin yazarına aittir;

Bilgi Teknolojileri ve İletişim Kurumunun görüşlerini yansıtmaz.





BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU

ELEKTRONİK HABERLEŞME SEKTÖRÜNDE KİŞİSEL VERİLERİN İŞLENMESİ, SAKLANMASI VE GİZLİLİĞİNİN KORUNMASI

Osman ŞAHİN

Bilişim Uzmanlığı Tezi

Haziran 2011

Ankara

Osman ŞAHİN tarafından hazırlanan "Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi, Saklanması ve Gizliliğinin Korunması" adlı bu tezin Bilişim Uzmanlığı tezi olarak uygun olduğunu onaylarım.

Doç. Dr. Mustafa İsmail KAYA
Tez Danışmanı

Bu çalışma, tez savunma komisyonumuz tarafından Bilişim Uzmanlığı tezi olarak kabul edilmiştir.

Başkan : Mehmet Selçuk NURSOY

Üye : Mehmet Bilal ÜNVER

Üye : Yasin BAKIRCI

Üye : Cafer CANBAY

Üye : Özgür Fatih AKPINAR

Üye : Doç. Dr. Mustafa İsmail KAYA

Üye : Niver Bengü KARABACAK

Bu tez, Bilgi Teknolojileri ve İletişim Kurumu tez yazım kurallarına uygundur.

İÇİNDEKİLER

ÖZET

BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU	
Tezin Adı	Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi, Saklanması ve Gizliliğinin Korunması
Türü	Bilişim Uzmanlığı Tezi
Yazar	Osman ŞAHİN
Teslim Tarihi	08.06.2011
Anahtar Kelimeler	Veri gizliliği, kişisel veriler, trafik ve konum verileri, veri işleme, veri saklama, istek dışı haberleşme, opt-in, opt-out, tasarımsal gizlilik, gizliliği artırıcı teknolojiler, kişisel veri ihlali
Tez danışmanı	Doç. Dr. Mustafa İsmail KAYA
Sayfa Adedi	xv + 198

Özet

Lizbon Antlaşmasının geçerlilik kazanmasıyla kişisel verilerin korunması artık temel haklar arasında sayılmaktadır. Ancak bilgi ve iletişim teknolojileri sayesinde kişisel verilerin daha kolay işlenebilmesi ve bu verilerin üçüncü taraflara aktarılması kişisel verilerin gizliliğine yönelik tehditleri artırmaktadır. Bu durum, bir yandan kişisel verilerin meşru amaçlarla ve hukuka uygun bir şekilde işlenmesini diğer yandan saklanması öngörülen verilerin korunmasında gerekli teknik ve idari tedbirlerin alınmasını gerekli kılmaktadır. Bu bağlamda son zamanlarda tartışılan tasarımsal gizlilik ilkesi ve gizliliği artırıcı teknolojiler kişisel verilerin korunmasında etkin rol oynayabilecektir. 2009/136/EC sayılı AB Direktifi kapsamında kişisel veri ihlallerinin yetkili otoritelere ve ihlalden etkilenen kişilere bildirilmesi ise gizlilik kültürünü artıracak, elektronik haberleşme sektöründe faaliyet gösteren işletmecilerin gizliliğin korunmasına daha fazla önem vermelerini sağlayacaktır. Bu çalışma kapsamında kişisel verilerin işlenmesi, saklanması ve korunması ile ilgili olarak AB uygulamaları ışığında Türkiye'de mevcut durum analizi ve ilgili düzenlemelere yer verilmektedir.

ABSTRACT

INFORMATION TECHNOLOGIES AND COMMUNICATIONS AUTHORITY	
Thesis	The processing of personal data, protection of privacy and data retention in electronic communications sector
Type	ICTA expert thesis
Author	Osman ŞAHİN
Submission Date	08.06.2011
Key Words	Data privacy, personal data, traffic and location data, data processing, data retention, unsolicited communications, opt-in, opt-out, privacy by design, privacy enhancing technologies, personal data breach
Advisor	Associate Professor Mustafa İsmail KAYA
Total Page	xv + 198

Abstract

The protection of personal data has become a fundamental right after entry into force of the Treaty of Lisbon. However, thanks to information and communication technologies processing of personal data easily and disclosing of such data to third parties have been increasing threats to privacy. On the one hand, this situation requires the processing of personal data fairly and lawfully and on the other hand taking appropriate technical and organizational measures for the protection of data retained. In this context, recently discussed issues such as privacy by design and privacy enhancing technologies will be able to play a significant role in personal data protection. Notification of personal data breaches to competent national authorities and individuals concerned under Directive 2009/136/EC will enhance culture of privacy and also ensure that electronic communications service providers pay more attention to privacy protection. In this study, relating to data processing, data retention and protection, current situation and related regulations for Turkey will be examined in the light of EU practices.

TEŞEKKÜR

Çalışmam boyunca değerli yardım ve katkılarıyla beni yönlendiren danışman hocam Doç. Dr. Mustafa İsmail KAYA'ya, sağlamış olduğu katkılardan dolayı Dr. Muhterem ÇÖL ve Özgür Fatih AKPINAR'a, yine kıymetli tecrübelerinden faydalandığım Güneş KOCA ve Mustafa ÖZDEMİR'e, gösterdikleri sabır ve anlayış için değerli mesai arkadaşlarıma, manevi desteklerini esirgemeyen Elif Şule ALMALI'ya, özveri ve fedakârlıklarından ötürü sevgili anne ve babama teşekkürü bir borç bilirim.

TABLOLAR LİSTESİ

ŞEKİLLER LİSTESİ

KISALTMALAR

AAD	Avrupa Adalet Divanı (European Court of Justice)
AB	Avrupa Birliği (European Union (EU))
ABA	Avrupa Birliği Antlaşması (European Union Treaty)
ABD	Amerika Birleşik Devletleri
ABİDA	Avrupa Birliğinin İşleyişine Dair Antlaşma (Treaty on the Functioning of the European Union)
ABTHŞ	Avrupa Birliği Temel Haklar Şartı (The Charter of Fundamental Rights of the European Union)
AEPD	İspanya Veri Koruma Kurumu
AGCOM	İtalya Telekomünikasyon Düzenleyici Kurumu
AİHM	Avrupa İnsan Hakları Mahkemesi
AİHS	Avrupa İnsan Hakları Sözleşmesi
AK	Avrupa Komisyonu (European Commission (EC))
APEC	Asya Pasifik Ekonomik İşbirliği Örgütü (Asia-Pacific Economic Cooperation)
ARCEP	Fransa Telekomünikasyon Düzenleyici Kurumu
AVKD	Avrupa Veri Koruma Denetçisi (European Data Protection Supervisor)
Bkz.	Bakınız
BNetzA	Almanya Posta ve Telekomünikasyon Düzenleyici Kurumu
BM	Birleşmiş Milletler (United Nations)
BTK	Bilgi Teknolojileri ve İletişim Kurumu
CDR	Çağrı Detay Kayıtları (Call Detail Records)
Cell ID	Mobil Telefon Çağrısının Başladığı veya Sonlandığı Hücrenin Kimliği
CLI	Arayan Hattın Kimliğinin Tanımlanması (Calling Line Identification)
CNIL	Fransa Veri Koruma Kurumu
COMREG	İrlanda Telekomünikasyon Düzenleyici Kurumu
EDRI	Avrupa Sayısal Hakları (Digital Civil Rights in Europe)

EHK	Elektronik Haberleşme Kanunu
ENISA	Avrupa Şebeke ve Bilgi Güvenliği Ajansı (European Network and Information Security Agency)
FCC	Amerika Birleşik Devletleri Haberleşme Komisyonu (Federal Communications Commission)
FEDMA	Avrupa Doğrudan ve İnteraktif Pazarlama Federasyonu (Federation of European Direct and Interactive Marketing)
GARANTE	İtalya Veri Koruma Kurumu
ICO	İngiltere Bilgi Komiserliği Ofisi (The Information Commissioner's Office)
IP	Internet Protokolü (Internet Protocol)
ISDN	Tümleşik Hizmetler Sayısal Şebekesi (Integrated Services Digital Network)
IT	Bilgi Teknolojisi (Information Technology)
KTS	Konum Tabanlı Servisler (Location Based Services)
KVKKT	Kişisel Verilerin Korunması Kanun Tasarısı
Md.	Madde
MMS	Çoklu Ortam Mesajlaşma Hizmeti (Multimedia Messaging Service)
ODPC	İrlanda Veri Koruma Kurumu
OECD	Ekonomik İşbirliği ve Kalkınma Teşkilatı (Organisation for Economic Co-operation and Development)
OFCOM	İngiltere İletişim Düzenleme Kurumu (Office of Communications)
OPTA	Hollanda Posta ve Telekomünikasyon Düzenleyici Kurumu
PET	Gizliliği Artırıcı Teknolojiler (Privacy Enhancing Technologies)
RFID	Radyo frekanslı tanımlama (Radio Frequency Identification)
SMS	Kısa Mesaj Hizmeti (Short Message Service)
URL	Tekbiçimli Kaynak Konumlayıcı (Uniform Resource Locator)
VKÇG	29. Madde Veri Koruma Çalışma Grubu (Article 29 Data Protection Working Party)

GİRİŞ

Son yıllarda elektronik haberleşme sektöründe yaşanan gelişmeler hayatımızın birçok alanına yenilik getirmiş, e-imza, e-devlet, e-ticaret gibi terimler sıklıkla kullanılmaya başlanmıştır. Bununla birlikte elektronik ortamda yapılan işlemlerde özel hayatla ilgili bilgilerin veya kişisel verilerin hukuka ve dürüstlük kurallarına aykırı olarak kullanılması; bu verilerin kişinin rızası alınmadan ifşa edilmesi ve bilginin bulunduğu yerden başka yerlere kolaylıkla aktarılması riskini de artırmıştır. Bu durum, kişisel verilerin korunmasına yönelik birtakım düzenlemeleri de kaçınılmaz kılmaktadır.

Veri koruma alanında Avrupa Birliği (AB) mevzuatının uluslararası alanda öncü konumda olduğu söylenebilir. Örnek vermek gerekirse 95/46/EC sayılı Veri Koruma Direktifi kişisel verilerin korunmasına yönelik genel bir çerçeve çizerken; 2002/58/EC sayılı E-Gizlilik Direktifi elektronik haberleşme sektörüne özgü kurallar içermektedir. Direktiflerde yer alan kişisel veriler ile trafik ve konum verilerinin hangi koşullarda kimler tarafından işlenebileceği ve ne şekilde üçüncü taraflarla paylaşılacağı kişisel verilerin gizliliği açısından önem taşımaktadır.

Üçüncü taraflar tarafından elde edilen kişisel iletişim bilgileri doğrudan pazarlama amaçlı haberleşme için kullanıldığında istek dışı haberleşme gerçekleşmektedir. Bu tür haberleşme için abonelere en kolay ulaşma mecrası olarak görülen e-posta ve kısa mesaj hizmeti (SMS); ürün veya hizmetlerin tanıtımında yoğun bir şekilde kullanılmaktadır. 2011 yılı birinci çeyreği itibarıyla[1] Türkiye'de yaklaşık 9 milyon internet abonesi ve 62 milyon mobil abone olduğu göz önüne alındığında istek dışı haberleşmeyle ilgili düzenlemelerin önemi daha iyi anlaşılacaktır.

---

[1] http://www.btk.gov.tr/kutuphane_ve_veribankasi/pazar_verileri/pazar_verileri.php

2000'li yıllarda ABD başta olmak üzere İspanya ve İngiltere'de yaşanan terör olayları, elektronik haberleşme araçları kullanılarak yapılan iletişime ilişkin trafik verilerinin suç araştırması ve tespitinde kullanılması konusunu gündeme getirmiş, bu çerçevede 2006/24/EC sayılı Veri Saklama Direktifi yayımlanmıştır. Ancak bu durum, trafik verilerinin saklanmasını özel hayatın gizliliğine müdahale olarak değerlendirerek Direktifin yürürlükten kaldırılmasını talep edenler ile suç tespiti amacıyla söz konusu verilerin saklanmasının gerekli olduğunu düşünenler arasındaki tartışmaları da beraberinde getirmiştir.

Elektronik haberleşme sektöründe faaliyet gösteren işletmecilerin[2] kişisel verilerin gizliliğini ihlal ettikleri yönünde haberler basın ve yayın organlarında zaman zaman yer almaktadır. Ancak söz konusu ihlallerin sadece ülkemizde yaşanmadığı unutulmamalıdır. Nitekim bu konuda AB tarafından yayımlanan 2009/136/EC sayılı Vatandaş Hakları Direktifi, kişisel veri ihlallerinin engellenmesi için işletmecilere çeşitli yükümlülükler getirmektedir.

Bu çerçevede, tez çalışmamızda AB düzenlemeleri ve uygulamalarını da göz önüne alarak farklı bir bakış açısı sağlayabilecek öneri ve sonuçlar ortaya konulacaktır.

Altı bölümden oluşan çalışmamızın birinci bölümünde kişisel veri kavramından bahsedilecek, kişisel verilerin işlenmesi, saklanması ve korunmasının önemi aktarıldıktan sonra kişisel verilerin gizliliğine yönelik tehditlere ve bu tehditler karşısında kişisel verilerin korunmasında kullanılan yöntemlere yer verilecektir.

---

[2] 5809 sayılı Elektronik Haberleşme Kanununda işletmeci, "Yetkilendirme çerçevesinde elektronik haberleşme hizmeti sunan ve/veya elektronik haberleşme şebekesi sağlayan ve alt yapısını işleten Şirket" olarak tanımlanmıştır. http://www.btk.gov.tr/mevzuat/kanunlar/dosyalar/elektronik_haberlesme_kanunu.pdf.
Bu bağlamda kavram karmaşası oluşturmaması adına AB Direktiflerinde yer alan "kamu haberleşme şebekesi veya kamuya açık elektronik haberleşme hizmeti sağlayıcıları" ifadesi için çalışmamızda işletmeci kavramı kullanılabilecektir.

İkinci bölümde kişisel verilerin işlenmesi, saklanması ve korunması alanında uluslararası kuruluşların yaptıkları çalışmalar ele alınacaktır. AB mevzuatı kapsamında yer alan Antlaşma, Tüzük ve Direktifler incelenecek; özellikle elektronik haberleşme sektörüne yönelik 2002/58/EC, 2006/24/EC ve 2009/136/EC sayılı Direktifler genel hatlarıyla aktarılacaktır.

Üçüncü bölümde AB Direktifleri doğrultusunda kişisel verilerin işlenmesi saklanması ve gizliliğinin korunması konusu işlenecektir. Bu çerçevede, kişisel veriler ile trafik ve konum verileri hakkında genel bilgi verildikten sonra veri türleri arasındaki ilişki ortaya konulacak, bu verilerin hangi koşullarda ve kimler tarafından işlenebileceği hususu anlatılacaktır. Ardından, istek dışı haberleşme konusu incelenecek ve verilerin saklanmasına ilişkin olarak 2006/24/EC sayılı Direktifte yer alan işletmeci yükümlülüklerinden bahsedilecektir. Son kısımda ise tasarımsal gizlilik kavramı ile gizliliği artırıcı teknolojilere yer verilecek, örnek uygulamalar ile konu pekiştirilecektir.

Dördüncü bölümde elektronik haberleşme sektöründe kişisel verilerin işlenmesi, saklanması ve korunmasına yönelik AB üyesi ülke uygulamaları tartışılacaktır. Bu kapsamda, gelişmişlik düzeyleri ve düzenleyici otoritelerinin etkinliği gibi unsurlar da göz önüne alınarak İngiltere, Almanya, İspanya, Fransa, İtalya, Hollanda ve İrlanda örnekleri incelenecektir.

Çalışmamızın beşinci bölümünde kişisel verilerin işlenmesi, saklanması ve korunması alanında ülkemizdeki genel düzenlemeler ile elektronik haberleşme sektörüne ilişkin mevzuat ele alınacak, ardından "Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik Taslağı" ele alınarak Taslak Yönetmeliğin AB Direktifleriyle uyumu karşılaştırılacaktır. Çalışma, yapılan inceleme ve değerlendirmeler neticesinde ulaşılan sonuç ve önerilerin yer aldığı bölümle son bulacaktır.

1. KİŞİSEL VERİ KAVRAMI, KİŞİSEL VERİLERİN İŞLENMESİ SAKLANMASI VE KORUNMASININ ÖNEMİ, KİŞİSEL VERİLERİN GİZLİLİĞİNE YÖNELİK TEHDİTLER VE KİŞİSEL VERİLERİN KORUNMASI YÖNTEMLERİ

Bu bölümde öncelikle kişisel veri kavramına yer verilecek, ardından temel haklar açısından kişisel veriler incelenecektir. Kişisel verilerin işlenmesi, saklanması ve korunmasının önemine yer verildikten sonra ise kişisel verilerin gizliliğine yönelik tehditler ile kişisel verilerin korunmasına ilişkin yöntemlerden bahsedilecektir.

1.1 Kişisel Veri Kavramı

Kişisel verilerin gizliliği, mahremiyet[1] ile ilişkili olduğundan öncelikle mahremiyet kavramı üzerinde durmak yerinde olacaktır.

Mahremiyet kavramının anlamı ve kapsamına ilişkin bir uzlaşma bulunmamakla birlikte, çok anlamlılık ve belirsizlikler içermesi kavram hakkında genel geçer bir tanım yapmayı güçleştirmektedir (Yüksel, 2009). Birçok ülkede kişisel verilerin korunmasıyla ilişkilendirilen mahremiyeti 1890'lı yıllarda Warren ve Brandeis "*yalnız başına kalma veya yalnız bırakılma hakkı (the right to be left alone)*" olarak tanımlamış, mahremiyetin demokrasilerde en fazla beğenilen özgürlükler içerisinde yer aldığını ve kavramın Anayasa'da yer alması gerektiğini vurgulamışlardır (GILC, 2007). Warren ve Brandeis "Harward Law Review"da yayımlanan makalelerinde telefon, telgraf, ses kayıt cihazı gibi mekanik aletlerin icadına ilave olarak gazetecilik sektörünün gelişmesinin, kişisel bilgilerin elde edilmesi ve ifşa edilmesinde önemli bir tehdit unsuru oluşturduğunu, bu tehdide karşı bireyin korunması için

---

[1]Privacy kelimesinin karşılığı olarak mahremiyet, gizlilik, özel hayatın gizliliği gibi kavramlar kullanılabilmektedir.

mahremiyet hakkının ilke olarak benimsenmesi gerektiğini belirtmişlerdir (Glancy, 1979).

Garfinkel ve Spafford (2002)'a göre, Warren ve Brandeis'in makalesi birçok yasal düzenlemeye temel oluşturmasına rağmen günümüz bilgi çağına uzanan bir çerçeve çizememiş, mahremiyeti *"birey, grup ya da kuruluşların kendileri hakkındaki bilgileri ne zaman, nasıl ve ne ölçüde başkalarına ifşa edeceklerini belirleme talebi"* olarak tanımlayan Alan Westin, kavram için bilgi çağına daha uygun olan yeni bir tanım geliştirmiştir.

Mahremiyetin tarih boyunca bireylerin özel hayatları ve haberleşmesiyle ilişkilendirildiğini ifade eden Holvast (2007) ise 19 uncu yüzyılın sonundan itibaren kişisel bilgilere doğru eğilimin arttığını vurgulamaktadır. Nitekim mahremiyetin unsurları arasında sayılan bilgisel mahremiyet (*informational privacy*), kişisel verilerin ne şekilde toplanacağı, kaydedileceği, işleneceği ve ifşa edileceğinin kontrol edilmesi olarak tanımlanmaktadır (Gritzalis, 2006). Bu kapsamda, özellikle elektronik haberleşme sektörünün gelişmesi ile birlikte bilgisel mahremiyet çerçevesinde kişisel veri kavramının ön plana çıktığı görülmektedir.

Kişisel veri[2], "Kişisel Verilerin Otomatik Olarak İşlenmesi Karşısında Bireylerin Korunmasına Dair 108 Sayılı Sözleşme"de, *"belirli veya belirlenebilir bir kişiyle ilgili bütün bilgiler"* olarak tanımlanmış, 95/46/EC sayılı Veri Koruma Direktifinde de benzer bir tanım yapılmıştır. "Kişi" ve "belirlenebilirlik" tanımda göze çarpan en önemli iki husustur. Buna göre, verinin öncelikle bir kişiyle ilişkili olması, sonrasında ise bu kişiyi belirlemeye imkân sağlaması gerekmektedir. Kişiyi belirleme ise kimlik numarası ile doğrudan; fiziki, psikolojik, zihinsel, ekonomik, kültürel veya sosyal kimlik gibi faktörlerin bir ya da birkaçıyla dolaylı olarak mümkün olabilmektedir (Karanja,

---

[2] Detaylı bilgi için bkz. 3.1.1

2008). Kişisel veri, yazılı bilgiler dışında bir kişinin ses kayıtları, görüntüleri ve fotoğraflarını da kapsamaktadır (Cate, 1979).

Trafik ve konum verileri[3] bireylerle ilişkilendirildiği takdirde kişisel veri olarak değerlendirilmektedir. Bu çerçevede, elektronik haberleşme alanında kişisel veri kapsamına tüketicilerin[4] işletmecilerle paylaştığı kişisel bilgilere ilave olarak trafik ve konum verilerinin de dâhil edildiği anlaşılmaktadır. Bu nedenle, çalışmamızda kişisel verilere ilave olarak trafik ve konum verileri hakkında yapılan düzenlemelere de yer verilecektir.

1.2 Temel Haklar Açısından Kişisel Veri Kavramının Doğuşu

Teknolojinin gelişmesi, dijital dünyaya geçişin hızlanması, iletişim araçlarındaki hızlı değişimler ve bilgisayar sistemlerinin güçlü bir denetim-gözetim aracı olarak kullanılması; kişisel verilerin toplanması ve ele alınmasında bazı özel kuralların getirilmesini ve kanunlar çıkarılmasını gerekli kılmakta, böylece sosyal hayatta olduğu gibi dijital dünyada da kişisel verilerin korunması en temel insan hakkı olarak ortaya çıkmaktadır (Ahmad, 2009).

Kişisel verilerin korunmasının hak olarak tanınması 4 Haziran 1999'da yapılan Köln Zirvesinde Avrupa vatandaşları ve AB'de ikamet eden herkesin medeni, siyasi, ekonomik ve sosyal haklarını belirleyecek AB Temel Haklar Şartının (ABTHŞ) bir Konvansiyon nezdinde oluşturulması kararıyla başlamıştır. Bu karar sonrasında 29. madde veri koruma çalışma grubu[5] (VKÇG) 4/99 sayılı tavsiye kararıyla, kişisel verilerin korunmasının temel haklar arasında yer almasının, verilerin korunması yönünde yasal bir gerekçe

---

[3] Detaylı bilgi için bkz. 3.1.2-3.1.3

[4] Elektronik Haberleşme Kanununda tüketici, "Elektronik haberleşme hizmetini ticari veya mesleki olmayan amaçlarla kullanan veya talep eden gerçek veya tüzel kişi" olarak tanımlanmıştır.

[5] 95/46/EC sayılı Direktifin 29. maddesi kapsamında kurulan veri koruma çalışma grubu kişisel verilerin korunması alanında tavsiye ve görüş niteliğinde kararlar almakta ve çeşitli çalışma dokümanları yayımlamaktadır.

oluşturacağını ve bilgi toplumunda kişisel verilerin korunmasının gittikçe artan önemini yansıtacağını bildirmiş (VKÇG, 1999), Konvansiyon tarafından hazırlanan metinde kişisel verilerin korunması temel hak olarak yer almıştır.

Avrupa vatandaşlarının anayasal haklarını belirleme konusunda ilk girişim olarak değerlendirilen ABTHŞ'nin *"Herkes, kendisini ilgilendiren kişisel verilerin korunması hakkına sahiptir."* şeklindeki 8 inci maddesi ile, her bir bireye sadece hassas verilerin değil bütün kişisel verilerin korunması hakkı sağlanmıştır (Buellesbach, 2010).

7 Aralık 2000 tarihinde Nice Zirvesi'nde ilan edilen ABTHŞ, yasal bağlayıcılık içermemesine rağmen AB kurucu antlaşmalarının sadeleştirilmesi ve üye ülkelerin bütünleşmesi amacıyla hazırlanan Taslak AB Anayasasının ikinci bölümüne aktarılarak yasal bağlayıcılığa kavuşması amaçlanmıştır. AB Anayasasının Fransa ve Hollanda'da yapılan referandumla reddedilmesinden sonra ise yeni bir metin oluşturulmuştur. Temelde AB Anayasasını koruyan, diğer yandan anayasa ifadesi ile AB sembolleri ve AB marşına yapılan atıfların kaldırılması gibi küçük değişiklikler içeren metin, 1 Aralık 2009 tarihinde 27 ülkenin onayıyla Lizbon Antlaşması olarak yürürlüğe girmiş (DTM, 2010), böylece kişisel verilerin korunması hakkı hukuki bağlayıcılık kazanmıştır.

1.3 Kişisel Verilerin İşlenmesi, Saklanması ve Korunmasının Önemi

Kişisel verilerin toplanması, depolanması, değiştirilmesi, silinmesi, üçüncü taraflara aktarılması gibi, veriler üzerinde gerçekleştirilen işlemler kişisel verilerin işlenmesi[6] kapsamında değerlendirilmektedir. Bu çerçevede, gerek kamusal alanda gerekse özel sektörde veri işleme faaliyetinin yoğun bir şekilde yapıldığı söylenebilir. Örneğin, Bilgi Edinme Hakkı Kanunu kapsamında kamu kurumlarına yapılacak bilgi edinme başvurularında

---

[6] Detaylı bilgi için bkz. 3.2

başvuru sahibinin adı ve soyadı, oturma yeri ve adresi, kimlik numarası, elektronik posta adresi gibi kişisel veriler talep edilmektedir.

Elektronik haberleşme sektöründe faaliyet gösteren işletmeciler ise abonelik sözleşmeleri veya internet siteleri aracılığıyla müşterilerinin kişisel verilerini elde etmekte ve bu verileri kullanmaktadır. Diğer taraftan, trafik ve konum verileri de faturalandırma ve katma değerli hizmetler sunma gibi amaçlarla işletmeciler tarafından işlenmektedir. Bu bağlamda, elektronik haberleşme sektöründe kişisel verilerin işlenmesi, tüketicilerin elektronik haberleşme hizmeti almak için işletmecilerle paylaştıkları bilgiler ile elektronik haberleşme hizmetini kullanmaları esnasında üretilen verilerin kaydedilmesi, değiştirilmesi, silinmesi, üçüncü taraflara aktarılması gibi işlemleri içermektedir.

Elektronik haberleşme hizmetinin sunulması esnasında üretilen veya işlenen trafik ve konum verileri fatura uzlaşmazlıklarının çözümünde, suç soruşturması ve kovuşturmasında kullanılmak üzere işletmeciler tarafından belirli süre saklanabilmektedir. Ancak bu verilerin saklanması ve güvenlik birimlerine verilmesi sırasında veri gizliliğine saygı gösterilmesi, elde edilen kişisel verilerin amaç ve kapsam dışında kullanılmaması son derece önemlidir. Zira kişisel verilerin işlenmesi ve saklanması sürecinde işletmeciler tarafından elde edilen veriler güvenli bir şekilde kontrol edilmezse bu veriler işletmeciler de dâhil olmak üzere pazarlama şirketleri tarafından kişiler üzerinde bir denetim-gözetim aracı olarak kullanılabilmekte ve alışkanlıkların profili çıkarılabilmektedir.

Tüm bunlara bağlı olarak kişisel verilerin işlenmesi, saklanması ve korunması konusu ülkemizde ve dünyada önem kazanmıştır. Bu çerçevede, kişisel verilerin gizliliği ve bu verilerin insan haklarına saygılı bir şekilde tutulması veya gerektiğinde kullanılmasının sağlanması devletin en önemli görevlerindendir. Elektronik haberleşme alanında kişisel verilerin işlenmesi ve gizliliğinin korunmasına ilişkin düzenleme ve denetleme yapma görevi,

AB'ye üye ülkelerde ve ülkemizde telekomünikasyon otoritelerine düşmektedir. Bu nedenle, telekomünikasyon otoriteleri tarafından yapılacak düzenlemelerin kişisel verilerin korunmasında mihenk taşı olacağı kuşku götürmez bir gerçektir.

1.4 Kişisel Verilerin Gizliliğine Yönelik Tehditler

Bilgisayar sistemleri ve ağlarının gelişmesi, kişisel verilerin toplanması, analiz edilmesi ve yayılmasını kolaylaştırırken kişisel verilerin gizliliğine yönelik artan tehditler ve saldırılar karşısında yasal düzenlemelere olan ihtiyaç da bu nispette artmaktadır. Veri akışının coğrafi sınırlandırmalarını kaldıran küreselleşme, sistemler arasındaki teknolojik engelleri ortadan kaldıran yakınsama (convergence), belirli formda toplanan bilginin başka formlara kolaylıkla dönüştürülmesini sağlayan çoklu ortam (multimedia) gibi unsurlar veri gizliliği ihlalini kolaylaştırmaktadır (GILC, 2007).

Kanada Veri Gizliliği Komitesi veri gizliliğinin en çok tehdit edildiği 10 yöntemi şöyle sıralamaktadır (PRIV, 2009):

- Kameralar, internette yapılan aramalar (elektronik ortamda bırakılan verilerin kişilerin rızası ve bilgisi olmadan toplanması, analiz edilmesi, satılması),
- Çevrimiçi alışveriş ve oyunlar,
- Kişilerin kendileri, aileleri ve arkadaşları hakkındaki kişisel bilgileri gönderdikleri sosyal paylaşım siteleri,
- Kamu güvenliği ve ulusal güvenlik adı altında birçok kişisel veriyi elde eden hükümetler,
- Kişisel verilerin korunması veya kullanılmasında yeterli koruma tedbirlerine sahip olmayan ancak birçok kişinin verilerini toplayan ticari kuruluşlar,
- Kamusal alan ve özel sektörde yaşanan veri ihlalleri,

- Kişisel verileri çalan dolandırıcılar,
- Çalınan kimlik kartları,
- Bilginin dünya üzerinde kolaylıkla dolaşabildiği küresel toplum,
- Mahremiyet hakkı kavramının erozyona uğradığı kişiler.

Foss (2008)'a göre veri gizliliğine yönelik olarak belirtilen tehditler karşısında sınırlandırma ve kontrol mekanizması iki önemli faktör olarak karşımıza çıkmaktadır. Doğru ve güncel kanunlarla bireylere sınırlandırma getirilmeli, olası sistem açıklarının tespiti ve gözetimi için ise sistemler üzerinde kontrol mekanizması sağlanmalıdır.

1.5 Kişisel Verilerin Korunmasında Kullanılan Yöntemler

Kişisel verilerin korunmasına yönelik uluslararası uygulamalarda 4 temel model bulunmakta, bazı ülkelerde ise birkaç modelin aynı anda kullanıldığı görülmektedir. Ülkeler arasındaki kültürel farklılıklar kişisel verilerin korunmasında tercih edilecek modeli etkilese de veri korumada etkin ve başarılı olan ülkelerin muhtemelen 4 modeli de kullanacakları aşikârdır (Holvast, 2007).

1.5.1 Genel düzenlemeler (comprehensive laws)

Bu modelde, kamusal alanda ve özel sektörde kişisel bilgilerin toplanma, kullanılma ve aktarılma yöntemlerini belirleyen genel bir düzenleme bulunmakta, akabinde denetleyici bir kurum (Komisyon, Ombudsman vb.) düzenlemeye uygunluğu denetlemektedir (Marcella ve Stucki, 2003). Bu yaklaşım, AB tarafından da kabul edilen ve birçok ülkede tercih edilen bir model olmakla birlikte, denetleyici kurumların yetkileri farklılık göstermekte ve düzenlemelerin gerektiği gibi uygulanması hususunda kaynakların yetersizliğinden bahsedilmektedir (Rodrigues vd, 2001).

Kişisel verilerin korunmasına ilişkin olarak genel düzenlemelerin kabul edilmesinin ardında yatan 3 temel faktörün; veri gizliliği ihlallerine çözüm üretmek, elektronik ticareti teşvik etmek ve özellikle ticari alanda yaşanabilecek problemlerin önüne geçmek için Pan-Avrupa yasalarına uyum sağlamak olduğu belirtilmektedir (GILC, 2007).

AB tarafından yayımlanan ve gerek kamusal alan gerekse özel sektörü kapsayan Veri Koruma Direktifi ile, üye ülkelerin Direktife uyum sağlamaları için yasa çıkarmaları ya da mevcut kanunlarında değişiklik yapmaları zorunlu kılınmış, kanunlarda yer alan hükümlerin uygulanmasını denetleyen bağımsız bir veri koruma kurumu kurmaları istenmiştir (Holvast, 2007).

Genel düzenleme modelinin varyantı olarak değerlendirilen ortak düzenleyici modelde ise kişisel verilerin korunmasına yönelik kurallar sektör aktörleri tarafından belirlenerek işlerlik kazandırılmakta, kuralların uygulanıp uygulanmadığı denetleyici bir kurum tarafından kontrol edilmektedir. Bireylerin, kuruluşların, endüstri temsilcilerinin ve hükümetlerin katılımlarını hedefleyen bu yaklaşım Avustralya ve Kanada'da kabul görmektedir (Cippguide, 2010).

1.5.2 Sektörel düzenlemeler (sectoral laws)

ABD gibi bazı ülkelerde genel düzenlemeler yerine sektörel düzenlemeler uygulanmakta ancak bu model yeni gelişen teknolojilerin her biri için mevcut düzenlemelerin yenilenmesini gerektirdiğinden, düzenlemeler teknolojinin gerisinde kalabilmektedir (GILC, 2007). Marcella ve Stucki (2003), tıbbi ve genetik bilgilerin korunmasında yasal eksikliklerin görüldüğü ABD'de sektörel düzenlemelerin sınırlı kaldığını ve denetleyici bir kurumun olmamasının da problem oluşturduğunu, buna karşılık birçok ülkede sektörel düzenlemelerin telekomünikasyon, tüketici kredi kayıtları gibi çeşitli kategorilerde yer alan bilgiler için detaylı koruma tedbirleri sağlayarak genel düzenlemelerin tamamlayıcı bir unsur olduğunu ifade etmektedir.

Holvast (2007) Strazburg Sözleşmesinde belirtilen tavsiyeler ışığında 1997 yılında Telekomünikasyon Sektöründe Gizliliğin Korunması Hakkında 97/66/EC sayılı Direktifin (ISDN Direktifi) kabul edildiğini, 95/46/EC sayılı Veri Koruma Direktifinin kişisel verilerin korumasına yönelik genel ilkeler belirlerken ISDN Direktifinin kamu haberleşme şebekelerinde ve özellikle internette yeni gelişen teknolojilerin kullanımında kişisel verilerin korunmasına ilişkin hükümler getirdiğini vurgulamaktadır.

Her ne kadar Anayasa değişikliği kapsamında kişisel verilerin korunmasını isteme hakkı Anayasada yer almış olsa da Bilgi Teknolojileri ve İletişim Kurumu (BTK) tarafından yayımlanan ve sektörel bir düzenleme sayılabilecek "Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik"in daha etkin olabilmesi için 95/46/EC sayılı Veri Koruma Direktifi doğrultusunda Adalet Bakanlığı Kanunlar Genel Müdürlüğü tarafından hazırlanan Kişisel Verilerin Korunması Kanun Tasarısı (KVKKT)'nın yasalaşmasının bir gereklilik olduğu değerlendirilmektedir.

1.5.3 Öz düzenleme (self regulation)

Endüstri kuruluşları ve şirketlerin mesleki davranış kurallarını (*code of conducts*) belirledikleri, yasalara alternatif veya yasaları tamamlayıcı bir düzenleme olarak görülen bir modeldir. Uygulanabilirlik ve yeterlilik açısından çoğu zaman yetersiz kalan model Singapur, Japonya ve ABD gibi ülkelerde uygulanmaktadır (Marcella ve Stucki, 2003).

Latin Amerika Veri Koruma Örgütü RedIPD tarafından 2005 yılında yayımlanan Meksika Deklarasyonunda, kişisel verilerin öz düzenleme mekanizmasıyla korunmasının önemli olduğu ve mevcut veri koruma yasalarına katkıda bulunacağı ancak kamu otoritelerini dışarıda bırakan bir öz düzenlemenin, temel bir hakkı korumak için başlı başına yeterli bir koruma sistemi sağlayamayacağı belirtilmiştir (AEPD, 2010).

ABD'de yasalara alternatif olarak görülen öz düzenleme Avrupa'da ise mevcut yasalara ek bir düzenleme olarak kabul edilmekte, Veri Koruma Direktifinde de üye ülkelerin ulusal düzenlemelerinde yer alan hükümlerin tam olarak uygulanmasına katkıda bulunması için farklı sektörler de göz önünde bulundurularak mesleki davranış kurallarının düzenlenmesi teşvik edilmektedir (Holvast, 2007). Örneğin, Veri Koruma Direktifi uyarınca VKÇG (1998) ilgili taraflarca hazırlanacak mesleki davranış kurallarının; Direktiflere uygun olup olmadığını, söz konusu kuralların Veri Koruma Direktiflerine ve yasalarına katma değer sağlayıp sağlamadığını değerlendirmekte ve ilgili taraflara görüş bildirmektedir. Bu kapsamda, VKÇG (2003) Avrupa Doğrudan ve İnteraktif Pazarlama Federasyonu (FEDMA) tarafından hazırlanan "Doğrudan Pazarlamada Kişisel Verilerin Kullanımına İlişkin FEDMA Davranış Kuralları" metninin doğrudan pazarlama sektöründe kişisel veriler hakkında ortaya çıkabilecek problemler için uygun çözüm önerileri sunduğunu belirterek metnin Veri Koruma Direktifinin 27 nci maddesine uygun olduğu yönünde görüş beyan etmiştir.

1.5.4 Teknolojik yöntemler

Teknoloji tabanlı sistemlerin gelişmesi, iletişimin güvenliği ve gizliliğinin çeşitli sistemler ve programlar (kriptolama, güvenlik duvarları, HTML filtreleme vb.) aracılığıyla sağlanmasına imkân tanımakta ancak sistemlerin güvenliği ve güvenilirliği tartışılmaktadır (GILC, 2007).

Gizliliği artırıcı teknolojiler[7] (PET), son zamanlarda tartışılan konular arasında yer almaktadır. Bygrave (2002) kişisel verilerin ve gizliliğin korunması amacıyla belirlenen ilkelerde yapılacak değişikliklerde, yaygınlaşması ve uygulanmasında karşılaşılan problemler de göz önüne alınarak PET'in özellikle AB enstrümanlarıyla yasal olarak desteklenmesi gerektiğini ifade etmektedir.

---

[7] Detaylı bilgi için bkz. 3.4.2

9 Temmuz 2009 tarihli "Kişisel Verilerin Korunması Temel Hakkına İlişkin Yasal Çerçeve Dokümanı" kapsamında VKÇG (2009)'nin Avrupa Komisyonu'na (AK) verdiği görüşte, kişisel verilerin korunması ilkelerinin yeni teknolojilerin gelişmesine rağmen geçerliliğini sürdürdüğü ancak bunun düzenlemelerde herhangi bir değişikliğe ihtiyaç olmadığı anlamına gelmeyeceği, bilakis tasarımsal gizlilik (*privacy by design*) gibi ilave ilkelerin eklenmesi suretiyle yasal çerçevenin geliştirilmesi fırsatının kullanılması gerektiği hususlarına yer verilmiştir. Tasarımsal gizlilik ilkesinin benimsenmesi durumunda,

- Kişisel verilerin korunmasının bilgi ve iletişim teknolojilerine uyarlanması,
- Bilgi ve iletişim teknolojilerinin, sadece güvenliğin sağlanmasına değil kişisel verilerin gerektirdiği ölçüde işlenmesine imkân verecek biçimde tasarlanması

gerektiği de VKÇG tarafından ifade edilmiştir.

Teknolojik yöntemlerin genel ve sektörel düzenleme modelleriyle birlikte uygulandığında tamamlayıcı bir unsur olacağı, yasal yükümlülüklerin uygulanmasında karşılaşılabilecek sorunlar karşısında bilgi ve iletişim teknolojilerinin uygun olarak tasarlanmasıyla kişisel verilerin korunmasına önemli katkılar sağlayacağı değerlendirilmektedir. Ayrıca yakınsama teknolojisinin gelişmesi ve yaygınlaşması, teknolojik yöntemlerin ulusal ve uluslararası düzeyde diğer modellere göre daha kolay uygulanabilmesini mümkün hale getirmektedir.

2. KİŞİSEL VERİLERİN İŞLENMESİ, SAKLANMASI VE KORUNMASINA YÖNELİK ULUSLARARASI ALANDA YAPILAN ÇALIŞMA VE DÜZENLEMELER

Çalışmamızın bu bölümünde özellikle AB üyesi ülkelerin uygulamalarına yön veren Birleşmiş Milletler, Ekonomik İşbirliği ve Kalkınma Teşkilatı, Avrupa Birliği, Avrupa Konseyi, Asya Pasifik Ekonomik İşbirliği Örgütü gibi uluslararası kuruluşlar nezdinde kişisel verilerin işlenmesi, saklanması ve korunmasına yönelik yapılan çalışmalara ve alınana kararlara yer verilecektir.

2.1 Birleşmiş Milletler (BM)

Mahremiyetin birey hakkı olarak uluslararası alanda tanınması ikinci dünya savaşını takip eden dönemlere dayanmaktadır. BM İnsan Hakları Komisyonu tarafından hazırlanan ve 10 Aralık 1948'de kabul edilen İnsan Hakları Evrensel Beyannamesinin 12 nci maddesi,

> *"Hiç kimse özel hayatı, ailesi, meskeni veya haberleşmesi hususlarında keyfi müdahalelere, şeref ve şöhretine karşı tecavüzlere maruz bırakılamaz. Herkesin bu karışma ve tecavüzlere karşı kanun ile korunmaya hakkı vardır."*

şeklindedir. Beyanname, mahremiyet hakkını ele alan ilk uluslararası belge özelliğini taşımaktadır (Holvast, 2007).

BM Genel Kurulu tarafından 16 Aralık 1966'da kabul edilen ve 23 Mart 1976'da yürürlüğe giren Kişisel ve Siyasal Haklar Uluslararası Sözleşmesi'nin 17 nci maddesi de şu şekilde düzenlenmiştir:

> *"Hiç kimsenin özel ve aile yaşamına, konutuna veya haberleşmesine keyfi veya hukuka aykırı olarak müdahale edilemez; onuru veya itibarı hukuka aykırı saldırılara maruz bırakılamaz.*
> *Herkes bu tür saldırılara veya müdahalelere karşı hukuk tarafından korunma hakkına sahiptir."*

BM İnsan Hakları Komitesi tarafından 17 nci maddenin kapsamına ilişkin yapılan yorumda, kişisel verilerin korunması hakkının mahremiyet hakkı kapsamında değerlendirildiği belirtilmiştir (Küzeci, 2010).

İki maddede de verilerin korunmasına doğrudan değinilmemiş ancak 14 Aralık 1990'da BM tarafından yayımlanan ve bağlayıcı nitelikte olmayan "*Bilgisayarla İşlenen Kişisel Veri Dosyalarına İlişkin Rehber İlkeler*" metninde verilerin korunması açıkça yer almıştır (Kuner, 2009). Söz konusu metin ile aşağıda yer alan 10 ilke belirlenmiştir (UN General Assembly, 1990):

- Hukuka uygunluk ve dürüstlük,
- Doğruluk,
- Amacın belirliliği,
- İlgili kişinin erişimi,
- Ayrım gözetmeme,
- İstisna oluşturma yetkisi,
- Güvenlik,
- Denetim ve yaptırımlar,
- Verilerin sınır ötesi akışı,
- Uygulama alanı.

Metinde yer alan ilkeler, OECD rehber ilkelerini büyük ölçüde yansıtmakta, ilave olarak 5 inci maddede yer alan ayrım gözetmeme ilkesi kapsamında hassas verilerin[1] toplanmasına sınırlama getirilmektedir. 8 inci maddeyle de gizlilik ilkelerinin uygulanmasının gözlenmesi amacıyla her ülkenin bağımsız bir kurum kurması tavsiye edilmektedir (OECD, 2003).

BM rehber ilkeleri resmi ve gayrı resmi uluslararası kuruluşların kişisel verileri güvenilir, adil ve gizlilik dostu bir tarzda işlemelerini teşvik etmesine rağmen,

---

[1] Bir kişinin ırkını, etnik kökenini, siyasi düşüncelerini, dini ya da felsefi inançlarını, sendika üyeliğini açığa çıkaran kişisel veriler ile sağlık ve cinsel yaşamına ilişkin veriler.

uygulamadaki etkisi OECD rehber ilkelerine göre daha az olmuştur (Bygrave, 2004).

2.2 Ekonomik İşbirliği ve Kalkınma Teşkilatı (OECD)

1960'lı yıllarda yayımlanan akademik çalışma ve resmi raporlarda, otomatik veri işleme teknolojisinin gelişmesiyle birlikte gizliliğe yönelik bazı problemlerin varlığının ortaya konulması (Kirby, 2010), diğer yandan OECD'ye üye bazı ülkelerde 1970'li yıllarda çıkarılan kanunlarda ülkeler arasındaki veri akışını engelleyebilecek farklılıkların bulunması, OECD'yi kişisel verilerin korunması ve sınır ötesi akışına ilişkin rehber ilkeler geliştirmeye yöneltmiş, yapılan çalışma neticesinde 23 Eylül 1980 tarihli "Gizliliğin Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkeler" yayımlanmıştır (OECD, 1980). Metnin birinci kısmında 3 kavrama ilişkin tanım göze çarpmaktadır (md. 1):

- *Veri kontrolörü: Kişisel verilerin toplanması, kaydedilmesi, işlenmesi ya da ifşa edilmesi işlemlerinin, kendisi veya adına iş yapan temsilcisi tarafından gerçekleştirilip gerçekleştirilmeyeceğine bakılmaksızın kişisel verilerin kullanımı ve içerikleri hakkında ulusal hukuka göre karar vermeye yetkili taraf,*
- *Kişisel veri: Belirli veya belirlenebilir bir kişiyle ilgili bütün bilgiler,*
- *Kişisel verilerin sınır ötesi akışı: Kişisel verilerin ulusal sınırlar arasında dolaşımı.*

Metnin ikinci kısmında ise kişisel verilerin korunmasına ilişkin aşağıda belirtilen 8 temel ilkeden bahsedilmektedir:

- ***Veri toplamanın sınırlandırılması**: Kişisel verilerin toplanmasında sınırlamanın olması, verilerin hukuka ve dürüstlük kurallarına uygun biçimde ve gerektiğinde ilgili kişinin rızası veya bilgisi dâhilinde elde edilmesi (md. 7),*

- ***Veri kalitesi (niteliği)**: Kişisel verilerin kullanım amaçlarıyla ilgili olması ve bu amaçların gerektirdiği ölçüde doğru, tam ve güncel olması (md. 8),*
- ***Amacın belirliliği:** Kişisel verilerin toplanması esnasında ya da öncesinde verilerin toplanma amaçlarının belirlenmiş olması, verilerin sonraki kullanımlarının bu amaçların sağlanmasıyla sınırlı olması (md. 9),*
- ***Kullanımın sınırlandırılması:** Kişisel verilerin yasal düzenleme veya ilgili kişinin rızası halleri dışında madde 9'da belirlenen amaç dışında kullanılmaması, ifşa edilmemesi ve erişilebilir hale getirilmemesi (md. 10),*
- ***Güvenlik tedbirleri:** Kişisel verilerin kaybolma, yetkisiz erişim, tahrip edilme, kullanılma, değiştirilme ve ifşa edilme gibi risklere karşı uygun güvenlik tedbirleriyle korunması (md. 11),*
- ***Açıklık:** Kişisel verilere ilişkin gelişme, uygulama ve ilkeler hakkında genel bir açıklık politikası olması, veri kontrolörünün adresi ve kimliği yanında kişisel verilerin mevcudiyeti, niteliği ve temel kullanım amaçlarını ortaya koyan vasıtaların kolayca bulunabilmesi (md. 12),*
- ***Bireysel katılım:** Bir bireyin aşağıdaki haklara sahip olması (md. 13),*
    a. *Veri kontrolörünün kendisiyle ilgili verilere sahip olup olmadığı teyidinin veri kontrolöründen ya da başka yöntemlerle elde edilmesi,*
    b. *Kendisiyle ilgili verilerin makul bir zamanda, gerekirse fahiş olmayan bir ücretle, makul bir yöntem ve kolayca anlaşılabilir bir biçimde kendisine bildirilmesi,*
    c. *(a) ve (b) bentleri kapsamında yapılan bir başvurunun reddi halinde ret gerekçelerinin gösterilmesi, bireyin redde itiraz edebilmesi,*
    d. *Kendisiyle ilgili verilere itiraz edebilmesi, itirazın kabulü halinde verilerin silinmesi, düzeltilmesi, tamamlanması ve değiştirilmesini sağlayabilmesi,*

- ***Sorumlu tutulabilirlik:*** *Bir veri kontrolörünün yukarıda belirtilen esasları yürürlüğe koyan tedbirlere riayet etme açısından sorumlu olması (md. 14).*

OECD rehber ilkeleri tavsiye niteliği taşımasına rağmen üye ülkelerin ulusal kanunlarında yer almış, Veri Koruma Direktifine de temel oluşturmuştur. Uluslararası düzeyde gizlilik esaslarında uzlaşma sağlanan ilk metin olma özelliğini de taşıyan rehber ilkeler yayımlanma tarihinden itibaren 30 yıl geçmesine rağmen,

- Teknolojik tarafsız ele alınması,
- Bağlayıcılık içermemesi,
- Kamusal alan ya da özel sektöre hasredilmeyerek kapsamın geniş tutulması,
- Sınırlar ötesi veri akışının önemini vurgulaması,
- Sorumlu tutulabilirlik ilkesini eklemesi

hususlarını içermesi sayesinde etkisini günümüze kadar sürdürebilmiştir (Kirby, 2010).

2.3 Asya Pasifik Ekonomik İşbirliği Örgütü (APEC)

Asya Pasifik bölgesinde ekonomik gelişme, işbirliği, ticaret ve yatırımın kolaylaştırılması amacıyla 1989 yılında kurulan ve hâlihazırda 21 üye ülkesi bulunan bir örgüttür. Örgütün bağlayıcı nitelikte olmayan kararları uzlaşma sağlanarak alınmakta, yükümlülükler ise gönüllülük esasına dayalı olarak yürütülmektedir (APEC, 2010). Örgüt'ün 2004 yılında yayımladığı "Gizlilik Çerçeve Dokümanı"nda[2] 9 temel veri koruma ilkesi şu şekilde sıralanmaktadır:

---

[2] APEC Privacy Framework

- Zararın önlenmesi,
- Bildirim,
- Veri toplamanın sınırlandırılması,
- Kişisel verinin kullanımı,
- Tercih hakkı,
- Kişisel verilerin bütünlüğü,
- Güvenlik tedbirleri,
- Erişim-düzeltme,
- Sorumluluk.

APEC veri koruma ilkelerine bakıldığında diğer uluslararası veri koruma ilkelerinden farklı olarak "zararın önlenmesi" ilkesi göze çarpmaktadır. İlke kişisel verilerin korunmasının, verilerin amaç dışı kullanılmasını önleyecek biçimde tasarlanmasını öngörmektedir. Ayrıca kişisel verilerin amaç dışı kullanımından kaynaklanacak zarara ilişkin riski bildirirken yükümlülüklerin, anılan riski göz önünde bulundurması ve çözüm tedbirlerinin kişisel verilerin aktarılması, kullanılması ve toplanmasından kaynaklanabilecek zararın büyüklüğü ve olasılığıyla orantılı olması gerekmektedir (APEC, 2005).

Greenleaf (2009) APEC ilkelerinin, OECD ilkelerini çok az geliştirmesi, temel ilkelerinin ve özellikle uygulama kısmının zayıf olması, AB standartlarını göz ardı etmesi, bölge ülkelerinin yasalarında yer alan bazı ilkelere (verinin saklanması, kişisel verilerde yapılan düzeltmelerin üçüncü taraflara bildirilmesi, anonim hale getirme, hassas veri vb.) yer vermemesi gibi nedenlerle kişisel verilerin korunmasında ancak minimum standartları sağlayabildiğini; bununla birlikte belgenin gözden geçirilerek önceliklerinin yeniden düzenlenmesi halinde gizliliğin korunmasına ilişkin standartların gelişmesinde önemli bir rol üstlenebileceğini belirtmektedir. Waters (2008) ise APEC ilkelerinin bazı eksiklikleri olmasına rağmen mahremiyetin korunmasında minimum standart sağladığı değerlendirmesini hak etmediğini, uluslararası veri koruma belgelerinden, söz konusu belgelerde yer alan

ilkelerin bağlayıcı yükümlülüklere dönüştürülürken önemli ölçüde yorumlanması bağlamında küçük bir farklılık gösterdiğini, sağlam bir yürütme mekanizmasıyla uygulandığı takdirde mahremiyetin etkin bir şekilde korunmasını sağlayabileceğini vurgulamaktadır.

2.4 Avrupa Konseyi

Merkezi Strazburg'da bulunan ve mevcutta 47 üyesi bulunan Konsey'in başlıca hedefi, demokrasi, insan hakları ve yasa düzenini güvence altına almak olarak belirtilmektedir. Konsey'in mahremiyetin korunmasına ilişkin atmış olduğu ilk adım, 3 Eylül 1953'de yürürlüğe giren Avrupa İnsan Hakları Sözleşmesidir (AİHS). AİHS'nin 8 inci maddesinde,

> *"Herkesin özel hayatına, aile hayatına, konutuna ve haberleşmesine saygı gösterilmesi hakkına sahip olduğu, bu hakkın kullanılmasına bir kamu otoritesinin müdahalesinin, 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 olabileceği"*

hususları yer almaktadır.

2.4.1 Avrupa insan hakları mahkemesi kararları

Avrupa Konseyi bünyesinde bulunan Avrupa İnsan Hakları Mahkemesi (AİHM), haberleşmenin gizliliği, kişisel verilerin toplanması, saklanması ve ifşa edilmesi ile kişisel verilere erişim gibi konularda AİHS 8 inci madde kapsamında içtihatlarda bulunmaktadır.

2.4.1.1 Haberleşmenin gizliliği

Şimşek (2008) kişisel verilerin korunması ile ilgili olarak AİHM'in ilk önemli içtihadının 6 Eylül 1978 tarihli Klass-Almanya kararı olduğunu belirtmektedir. Federal Almanya Cumhuriyetinin 1968 yılında çıkardığı yasayla mektup, posta ve telekomünikasyon yoluyla yapılan haberleşmenin gizliliği kısıtlanarak İdare'ye, belirli durumlarda ilgili kişiyi bilgilendirmeksizin gizli gözetim yapma imkânı tanınmıştır. Bunun üzerine Klass ve arkadaşları söz konusu yasanın AİHS'nin 6, 8 ve 13 üncü maddelerini ihlal ettiği gerekçesiyle 1971 yılında Avrupa İnsan Hakları Komisyonuna başvurmuştur (Council of Europe, 1979).

AİHM başvuruyu, AİHS 8(1) maddesinde güvence altına alınan haklara müdahalenin var olup olmadığı açısından değerlendirmiş, Alman yasasının bütün kişileri izlenme tehdidi altında bırakması, posta ve telekomünikasyon hizmetlerini kullananların haberleşme özgürlüklerini etkilemesi gerekçeleriyle başvuran kişilerin özel yaşamlarına ve haberleşme haklarını kullanmalarına kamu müdahalesi olduğunu belirlemiştir (AİHM Kararı, 1978).

Mahkeme, tespit edilen müdahalenin AİHS 8(2) maddesi kapsamında uygunluğuna karar verirken istisna getiren fıkranın dar anlamda yorumlanması gerektiğini ifade ettikten sonra müdahalenin hukuka uygun olduğunu, ulusal güvenlik ve kamu güvenliği açısından meşru amaçlarla yapıldığını ifade etmiştir (AİHM Kararı, 1978).

Mahkeme son tahlilde müdahalenin demokratik toplumda gerekliliğini sorgulamış, gelişen teknolojiyle paralel olarak artan terör tehdidine karşı ulusal güvenlik ve/veya suçların önlenmesi gerekçeleriyle devletin haberleşme alanında gizli gözetim faaliyetlerine imkân tanıyan yasa çıkarmasını demokratik toplumda gerekli görmüştür. Ancak bu durumun devletlere sınırsız takdir yetkisi tanındığı anlamına gelmeyeceği, gözetim sistemlerinin kötüye kullanımlarının engellenmesi için etkin ve yeterli

tedbirlerin alınması gerektiği de Mahkeme tarafından vurgulanmış, sonuç olarak Klass ve diğerlerinin yaptığı başvuru AİHS 8 inci madde ihlali olarak değerlendirilmemiştir (AİHM Kararı, 1978).

2.4.1.2 Kişisel verilerin işlenmesi, saklanması ve ilgili makamlara verilmesi

Leander-İsveç davası AİHM'in, kişisel verilerin işlenmesi ve saklanmasıyla ilgili olarak özel yaşama saygı hakkının ihlal edilip edilmediğini değerlendirdiği bir davadır. Leander, bir deniz müzesinde tekniker kadrosunda geçici olarak çalışmaya başlamış ancak güvenlik soruşturmasının olumsuz neticelenmesi nedeniyle müze müdürlüğü tarafından işine son verilmiştir. Leander, işe alınmama gerekçesi olarak gösterilen gizli polis sicilindeki bilgilere erişmek istemiş ancak bu mümkün olmamış, bu itibarla İsveç Personel Kontrol Sisteminin uygulanma şeklinin AİHS'nin 8 inci maddesini ihlal ettiği gerekçesiyle AİHM'e başvurmuştur. Mahkeme,

- İsveç Personel Kontrol Sisteminin milli güvenlik amacıyla yapıldığını (meşru amaç),
- İlgili mevzuatın kişisel verilerin toplanması, saklanması ve ilgili makamlara verilmesi açısından Milli Polis Kuruluna yetki verdiğini (hukuka uygunluk),
- Kötü amaçlı kullanıma mahal vermemek adına İsveç Personel Kontrol Sisteminin yeterli seviyede koruma sağladığı, mevcut olayda milli güvenliğin bireyin menfaatinin üzerinde olduğu ve bu çerçevede müdahalenin orantılı olduğunu (demokratik toplumda gereklilik)

belirterek AİHS 8 inci madde kapsamında ihlal tespit etmemiştir (AİHM Kararı, 1987).

Kilkelly (2001), Leander örneğinde İsveç Personel Kontrol Sisteminde yer alan koruma tedbirlerinin AİHS 8(2) maddesinin şartlarını karşılamada Mahkeme tarafından yeterli görüldüğünü, diğer yandan Mahkeme'nin her bir davayı genellikle ayrı ayrı değerlendirdiğini bu nedenle mevcut davada Mahkeme'nin, incelenen sistemin AİHS'de belirtilen eşik değeri aşıp aşmadığını ve demokratik toplumu korumanın gereksinimleri ile bireyin hakları arasında orta yolu bulup bulmadığını belirleme gibi bir rol üstlendiğini ifade etmektedir.

2.4.1.3 Kişisel verilere erişim

Bu tür şikâyetler, çoğunlukla kişisel verilerin devletin elinde bulundurulmasından çok bu tür verilere bireylerin erişememesinden kaynaklanmaktadır (Kilkelly, 2001). Gaskin-Birleşik Krallık davasında annesinin ölümünden sonra küçük yaşta devletin koruması altına alınan Gaskin, reşit olduktan sonra devletin koruması altında olduğu süre zarfında kötü muamele gördüğünü iddia ederek kendisine ilişkin dosyanın bütününe erişmek istemiş ancak yetkili makamlarca buna izin verilmemiştir (AİHM Kararı, 1989).

Konuyu Birleşik Krallık Mahkemelerine taşıyan davacı, dosyanın verilmesi ve açıklanmasının kamu yararına aykırı olacağı, dosyanın hazırlanmasına katkıda bulunan kişilerin bilgilerinin açıklanması halinde çocuk koruma faaliyetlerinin tehlikeye girebileceği yönünde alınan kararlar akabinde AİHS 8 inci madde kapsamında özel hayatına saygı gösterilmesi hakkının ihlal edildiği gerekçesiyle 17 Şubat 1983'te AİHM'e başvurmuştur (AİHM Kararı, 1989).

Mahkeme, bu davada çocuk koruma sisteminin etkin biçimde sürdürülmesi (kamu yararı) ile özel hayat hakkında kişisel verilere erişim (başvuranın menfaati) arasında adil bir denge gözetilip gözetilmediğini değerlendirmiş; bir kimsenin, çocukluğunu ve gelişiminin erken dönemlerini bilmesi ve anlaması

için gerekli bilgileri almasında hayati bir menfaati olduğuna dikkat çekmiştir. Mahkeme, özel yaşamıyla ilgili dosya bilgilerine ulaşmak isteyen davacının bireysel menfaatinin, ilgilinin dosyasına katkıda bulunan kişilerin mevcut olmadığı ya da gereksiz yere rıza göstermeyi reddettiği durumlarda korunması gerektiğini belirterek AİHS 8 inci maddenin ihlal edildiğini tespit etmiştir (AİHM Kararı, 1989).

Uslu-Türkiye davasında ise cezaevinde hükümlü bulunan Uslu, 14 Ocak 2004'te cezaevi revirinde yapılan muayeneye ilişkin doktor raporuna erişmek istemiş, her ne kadar raporun sureti kendisine verilmiş olsa da İnebolu Ağır Ceza Mahkemesinin asayiş ve güvenlik nedeniyle cezaevi dokümanlarının hükümlülere verilmesini yasaklama kararı almasının ardından söz konusu belgeler hükümlüden geri istenmiştir. Ağır Ceza Mahkemesinin kararının bozulması yönünde Adalet Bakanlığına başvuruda bulunan Uslu, talebi reddedilince AİHS 8 inci madde kapsamında AİHM'e başvurmuştur (AİHM Kararı, 2009).

Mahkeme, AİHS 8 inci maddenin temelinde bireyi devletin keyfi müdahalelerine karşı korumanın yer aldığını, bireyin ve devletin çatışan menfaatleri arasında adil bir denge gözetilmesi gerektiğini, mevcut davada davacının muayene raporunun suretini elde ederek tedavi seçiminde söz hakkına sahip olacağını belirtmiş, İnebolu Ağır Ceza Mahkemesi tarafından alınan kararın Adalet Bakanlığının Genelgesine dayanılarak alındığını tespit etmiş ancak hükümlüye getirilen kısıtlamanın orantılılığını değerlendirmek için Hükümet tarafından herhangi bir savunma sunulmaması üzerine, bireyin ve devletin çatışan menfaatleri arasında adil bir denge gözetilmediğine ve 8 inci maddenin ihlal edildiğine karar vermiştir (AİHM Kararı, 2009).

2.4.1.4 Kişisel verilerin kamuya ya da üçüncü taraflara ifşa edilmesi

Kişisel verilerin kamuya ifşa edilmesine ilişkin olarak MS-İsveç davası örnek verilebilir (AİHM Kararı, 1997). Bir anaokulunda öğretmen olan MS, 1981

yılında geçirdiği iş kazası sonrasında şiddetli sırt ağrıları nedeniyle meslek hayatına devam edememiş, 1994 yılından itibaren malul aylığı almaya hak kazanmıştır. MS, 1991 yılında İş Kazası Sigorta Kanunu kapsamında Sosyal Sigorta Kurumu'ndan tazminat talebinde bulunmuştur. Kurum, MS'nin tıbbi geçmişine ait verileri tedavi olduğu hastaneden temin etmiş ve hastanın sırt ağrılarının iş kazası nedeniyle olmadığını gösteren rapor üzerine tazminat talebini reddetmiştir. MS, tıbbi geçmişine ait verilerinin onayı alınmadan başka kamu kurumuna aktarıldığı gerekçesiyle AİHM'e başvurmuştur (AİHM Kararı, 1997).

Mahkeme, verilerin aktarılmasının yasayla öngörülmüş olduğunu, Sosyal Sigorta Kurumu'nun davacının iş kazası kapsamında talep ettiği tazminat için gerekli şartları taşıyıp taşımadığını belirlemek amacıyla söz konusu verileri talep ettiğini, verilerin paylaşılmasının kamu bütçesinden tahsis edilecek bir tutarın belirlenmesinde etkili olduğunu, bu nedenle mevcut davada ülkenin ekonomik refahını koruma amacı güdüldüğünü vurgulamış ve bireyin özel hayatına orantısız bir müdahale olmadığına karar vermiştir (AİHM Kararı, 1997).

Kilkelly (2001) kişisel verilerin korunmasının bireyin gerek özel hayatında gerekse aile hayatında temel bir öneme sahip olması nedeniyle, söz konusu verilerin kamuya ya da üçüncü taraflara ifşa edilmesinin bireyin özel hayatına, haklı gösterilmesi kolay olmayan bir müdahale anlamına geleceğini, bu kapsamda kişisel verilerin ifşa edilmesinde kullanıma ilişkin tedbirler ve hedeflenen amaç göz önünde bulundurularak kamu menfaatinin bireyin mahremiyet hakkından daha önde olması gerektiğini ifade etmektedir.

Avrupa Konseyi, bilgilerin dijital ortamlarda saklanması ve işlenmesine imkân tanıyan teknolojinin gelişmesiyle birlikte kişisel verilerin otomatik işlenme oranının artış göstermesi neticesinde kişisel verilerin korunmasını güçlendirmek istemiştir (Neuwirt, 2008). Bu amaçla ilk etapta, 1973 ve 1974 tarihlerinde kamusal alan ve özel sektördeki elektronik bilgi bankalarında yer

alan kişisel verilerin korunması için iki karar alınmıştır (Council of Europe, 2011). Bu kararlara bağlı olarak ulusal yasaların geliştirilmesi hedeflense de kararların hazırlanması sürecinde kişisel verilerin etkin korunmasının bağlayıcı uluslararası normlarla sağlanabileceğinin anlaşılması akabinde Konsey, 28 Ocak 1981 tarihinde "Kişisel Verilerin Otomatik Olarak İşlenmesi Karşısında Bireylerin Korunmasına Dair 108 Sayılı Sözleşme"yi kabul etmiştir (Council of Europe, 2011).

Kamusal alanı ve özel sektörü kapsayan 108 Sayılı Sözleşme'nin 5 inci maddesinde verilerin niteliğine ilişkin ilkelerden bahsedilmektedir. Buna göre, otomatik olarak işlenen kişisel veriler,

- *Hukuka ve dürüstlük kurallarına uygun olarak elde edilmeli ve İşlenmelidir,*
- *Meşru ve önceden belirlenmiş amaçlar için kaydedilmeli ve bu amaçlara aykırı biçimde kullanılmamalıdır,*
- *Elverişli ve amaca uygun olmalı, kaydedildikleri amaca göre ölçüsüz olmamalıdır,*
- *Doğru ve gerektiğinde güncel olmalıdır,*
- *İlgili kişinin kimliğinin belirlenmesine izin verecek biçimde ve kaydedildikleri amaç için gerekli olan süre kadar saklanmalıdır.*

108 Sayılı Sözleşme'nin diğer maddelerinde ise özel kategoriye giren verilerin (cinsel yaşam, sağlık, ırk, siyasi düşünce, dini inanç) iç hukukta yeterli koruma mekanizması sağlanmadıkça otomatik olarak işlenilmemesi (md. 6), kişisel verilerin güvenliğinin sağlanması (md. 7), ilgili kişinin hakları (md. 8), verilerin sınır ötesi akışı (md. 12) hususlarına yer verilmektedir (Council of Europe, 1981).

108 Sayılı Sözleşme kişisel verilerin işlenmesine ilişkin olarak Avrupa'daki bütün veri koruma kanunlarında yer alan temel ilkeleri belirlemiş, 95/46/EC

sayılı Veri Koruma Direktifini de önemli ölçüde etkilemiştir. Belge, toplanan ve işlenen verilerin kötü amaçlı kullanımlarını engellemek amacıyla kişisel verilerin korunmasını sağlayan ilk uluslararası bağlayıcı sözleşme olarak değerlendirilmektedir (Klosek, 2000).

2.5 Avrupa Birliği (AB)

AB'nin veri koruma alanındaki çalışma ve düzenlemelerini temel olarak Antlaşma, Tüzük[3], Direktif, Karar[4] gibi başlıklarda incelemek mümkündür.

2.5.1 Antlaşmalar

Ulusal düzeyde Anayasa hukukuna benzeyen ve AB'nin birincil mevzuatı kapsamında değerlendirilen Antlaşmalar, Birliğin temel özelliklerini, karar alma sürecinde çeşitli aktörlerin sorumluluklarını, yasal prosedürleri belirlemektedir. Üye ülkeler arasında yapılan müzakereler neticesinde kabul edilmesi ve ulusal parlamentolar tarafından onaylanması halinde Antlaşmalar geçerlik kazanmaktadır (Duke, 2010).

2.5.1.1 Avrupa Birliği Antlaşması (ABA)

7 Şubat 1992'de imzalanan ve 1 Kasım 1993'te yürürlüğe giren Maastricht Antlaşmasıyla (resmi adıyla Avrupa Birliği Antlaşması) AB bünyesinde, Avrupa Toplulukları, Ortak Dış Politika ve Güvenlik Politikası, Adalet ve İçişleri ile Kriminal Konularda Kolluk ve Adli İşbirliği olmak üzere üç sütunlu (*three pillars*) bir yapı oluşturulmuş, akabinde Amsterdam (1997) ve Nice Antlaşmalarıyla (2001) ABA'da değişiklikler yapılmıştır (EU, 2007). Lizbon

---

[3]AB hukuki düzenlemelerinin Türkçeye çevrilmesinde kullanılacak rehber için bkz. http://www.abgs.gov.tr/files/ceb/ab_nin_bazi_hukuki_duzenlemelerinin_turkce_ye_cevrilmesinde_kullanilacak_rehber.pdf

[4]AB'nin karar niteliğindeki düzenlemeleri tez kapsamında yer almamakla birlikte kriminal konularda polis ve adli işbirliği kapsamında işlenen kişisel verilerin korunması hakkında 2008/977/JHA sayılı kararı için bkz. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:350:0060:0071:EN:PDF

Antlaşması'nın yürürlüğe girmesiyle 2 nci ve 3 üncü sütundaki hukuksal araçlar kaldırılarak 1 inci sütundaki hukuki kaynakların diğer sütunlar için de kullanılabilmesi sağlanmıştır (Bilçen, 2010).

ABA'nın konsolide versiyonunun[5] 39 uncu maddesinde Ortak Dış Politika ve Güvenlik Politikası alanlarında, üye ülkelerde kişisel verilerin işlenmesi bağlamında bireylerin korunması ve söz konusu verilerin serbest dolaşımına ilişkin kuralların belirlenmesinde Konsey'e tek başına yetki verilmiştir (Cooper vd., 2010).

2.5.1.2 Avrupa Birliğinin İşleyişine Dair Antlaşma (ABİDA)

Temeli, 25 Mart 1957'de imzalanan ve 1 Ocak 1958'de yürürlüğe giren Avrupa Ekonomik Topluluğu (Roma) Antlaşmasına dayanan ABİDA, Maastricht ve Amsterdam Antlaşmalarıyla değişikliğe[6] uğramış (Bilçen, 2010), Lizbon Antlaşmasıyla son halini almıştır.

ABTHŞ'nin 8(1) maddesinde yer alan "*Herkes kendisini ilgilendiren kişisel verilerin korunması hakkına sahiptir*" ifadesi ABİDA'nın konsolide versiyonunun[7] 16(1) maddesine aynen alınmıştır. 16(2) maddesi ise Birlik bünyesindeki kurum, kuruluş ve organlar ile üye ülkelerde, bireylerin korunması amacıyla kişisel verilerin işlenmesine ve bu verilerin serbest dolaşımına ilişkin kuralların Avrupa Parlamentosu ve Konsey tarafından belirlenmesini ve kuralların denetlenmesinin bağımsız otoritelerin kontrolü altında olmasını öngörmektedir.

---

[5] Tam metin için bkz. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0013:0046:EN:PDF

[6] 1992 Maastricht Antlaşmasıyla Avrupa Ekonomik Topluluğu Anlaşmasının adı Avrupa Topluluğu Anlaşması olarak değiştirilmiştir.

[7] Tam metin için bkz. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0047:0200:EN:PDF

2.5.1.3 Lizbon Antlaşması

1 Aralık 2009 tarihinden itibaren yürürlüğe giren Lizbon Antlaşmasıyla, "Avrupa Topluluğu[8]" ifadesi "Avrupa Birliği", Avrupa Topluluğunu kuran antlaşmanın adı da "Avrupa Birliği'nin İşleyişine Dair Antlaşma" olarak değiştirilmiş, AB düzenlemelerinde yer alan mevcut temel haklar korunurken bunlara yenileri ilave edilmiştir (Bilçen, 2010).

AB'nin yasal temellerini oluşturan ABA ve ABİDA'da değişiklikler yapan Lizbon Antlaşması, ABA'nın 6 ncı maddesinin "*Birlik, Antlaşmalarla aynı yasal değere sahip 7 Aralık 2000 tarihli Avrupa Birliği Temel Hakları Şartında belirlenen ilke, özgürlük ve hakları tanımaktadır.*" şeklinde değiştirilmesini öngörerek ABTHŞ'ye yasal bağlayıcılık kazandırmıştır (Cooper vd., 2010).

Hustinx (2009) ABTHŞ'nin 8(2) maddesinde yer alan,

- Kişisel verilerin belirli amaçlar için ve dürüstlük kurallarına uygun bir şekilde işlenmesi,
- İlgili kişinin rızasına veya yasa ile öngörülmüş diğer meşru bir temele dayanarak işlenmesi,
- Herkesin kendisi hakkında toplanan verilere erişme ve bu verileri düzeltme hakkına sahip olması

hükümlerinin veri korumanın temel unsurlarını ortaya koyduğunu ifade etmektedir.

---

[8] Kavramlara ilişkin detaylı bilgi için bkz. http://ekutup.dpt.gov.tr/ab/

2.5.2 Tüzükler

AB'nin ikincil mevzuatı kapsamında değerlendirilen Tüzükler, doğrudan bağlayıcı olan ve doğrudan uygulanan, Birlik vatandaşları için ulusal kanunlar gibi hak ve yükümlülükler getiren hukuki tasarruflardır (Bilçen, 2010).

Tüzüğün doğrudan uygulanması, yürürlüğe girdiği tarihten itibaren üye ülkelerde bir iç hukuka aktarma işlemine gerek olmadığı; bütünüyle bağlayıcı olması ise üye ülkelerin, Tüzüğün amacının gerçekleşmesine yönelik tüm hükümlerini uygulamak zorunda oldukları anlamına gelmektedir. Tüzükleri, Türk hukuk düzenindeki kanunlara benzetmek mümkündür (Özdemir, 2001).

18 Aralık 2000 yılında Avrupa Konseyi ve Parlamentosu tarafından onaylanan 2001/45 sayılı Tüzük, AB antlaşmaları kapsamında Birlik bünyesinde kurulan kurum ve organların bireylerin korunması amacıyla kişisel verilerin işlenmesi sırasında uyacakları kuralları belirlerken bu çerçevede, bağımsız bir denetleyici otorite olarak Avrupa Veri Koruma Denetçisi[9] (AVKD) kurulmasını öngörmekte ve Denetçiye Birliğin kurum ve organları tarafından gerçekleştirilen bütün veri işleme faaliyetlerinin Tüzüğe uygun olup olmadığını denetleme görevi vermektedir (md. 1). Driessen (2008) Tüzüğün üç hususta garanti sağladığını belirtmektedir:

- İlgili kişiye kişisel verilere ilişkin olarak; erişim, düzeltme, engelleme, sildirme ve itiraz etme haklarının verilmesi ile ilgili kişinin veri işleme faaliyetleri hakkında bilgilendirilmesi,
- AVKD'nin veri işleme faaliyetlerini gözetlemesi,
- İlgili kişinin herhangi bir ihlal durumunda AVKD'ye başvuruda bulunması.

---

[9] European Data Protection Supervisor, AVKD hakkında detaylı bilgi için bkz. http://www.edps.europa.eu/EDPSWEB/edps/EDPS?lang=en

Bu haklara ilave olarak Veri Koruma Direktifinde olduğu gibi Tüzükte de kişisel verilerin hukuka ve dürüstlük kuralına uygun, amaca bağlı ve bu amaçla sınırlı biçimde işlenmesi öngörülerek AB bünyesinde hem üye ülkelere hem de Birlik kurum ve organlarına bireylerin temel hak ve özgürlüklerine ve özellikle de özel hayatın gizliliği hakkına riayet etmeleri hususunda yükümlülük getirilmiştir (Şimşek, 2008).

2.5.3 Direktifler

AB'nin ikincil mevzuatı kapsamında değerlendirilen Direktifler, üye ülkeler tarafından yerine getirilmesi gereken hukuki yükümlülükleri belirlemekte, üye ülkelerin iç hukukunda ilke olarak doğrudan uygulanmasa da seçilen hukuki araçtan bağımsız olarak Direktifte öngörülen amaçların gerçekleştirilmesi açısından üye ülkeler için bağlayıcı olmaktadır (Özdemir, 2001). Kişisel verilerin işlenmesi, saklanması ve korunması alanında yayımlanan Direktifler 4 başlıkta incelenmektedir.

2.5.3.1 95/46/EC sayılı Veri Koruma Direktifi

"Kişisel Verilerin İşlenmesi ve Bu Verilerin Serbest Dolaşımı Bağlamında Bireylerin Korunması Hakkında 95/46/EC sayılı Direktif"in kökeni, AK'nın "Kişisel Verilerin Otomatik Olarak İşlenmesi Karşısında Bireylerin Korunmasına Dair 108 Sayılı Sözleşme"nin üye ülkeler tarafından kabul edilmesi yönünde öneri sunmayı düşündüğü 1981 yılına dayanmaktadır. Ancak AK'nın tavsiye kararlarının hukuki açıdan bağlayıcı olmayacağının anlaşılması ve özellikle Avrupa Parlamentosunun, üye ülkelerde kişisel verilerin korunmasına ilişkin düzenlemelerin uyumlaştırılması amacıyla taslak bir Direktif hazırlanmasına yönelik çağrısı akabinde AK tarafından 1990 yılında kişisel verilerin korunmasına ilişkin Direktif Taslağı hazırlanmış ve Taslak çeşitli değişikliklerle birlikte 24 Ekim 1995 yılında nihai halini almıştır (Buellesbach, 2010).

Gerçek kişilerin temel hak ve özgürlükleri ile kişisel verilerin işlenmesi konusunda gizliliği korumak ve üye ülkeler arasında kişisel verilerin serbest dolaşımına imkân sağlamak amaçlarını (md. 1) taşıyan Direktif[10] 34 madde ve 7 bölümden oluşmaktadır.

Birinci bölümde amaç ve kapsam belirlenmiş, Direktifte geçen bazı terimlerin tanımı yapıldıktan sonra Direktif doğrultusunda kabul edilen hükümlerin üye ülkelerin ulusal mevzuatlarında uygulanmasına yer verilmiştir.

İkinci bölümde kişisel verilerin niteliğine ilişkin ilkeler, kişisel verilerin işlenmesinde hukuka uygunluk sebepleri, özel nitelikteki kişisel verilerin işlenmesi, ilgili kişiye (*data subject*[11]) yapılacak bilgilendirme, ilgili kişinin verilere erişme ve itiraz hakkı, istisnai hükümler, kişisel verilerin işlenmesinde gizlilik ve güvenlik, denetleyici otoriteyi bilgilendirme yükümlülüğü ve bilgilendirmenin içeriği, ön inceleme konuları düzenlenmiştir.

Üçüncü bölümde yükümlülükler ve yaptırımlar; dördüncü bölümde kişisel verilerin yabancı ülkelere transferi; beşinci bölümde mesleki davranış kuralları; altıncı bölümde kişisel verilerin korunması konularında denetleyici kurum ve çalışma grubu kurulması, yedinci bölümde ise uygulamaya ilişkin tedbirler düzenlenmiştir.

Direktifin kapsamı, herhangi bir dosyalama siteminin (*filing system*) parçasını oluşturacak biçimde kişisel verilerin kısmen veya tamamen, otomatik ve otomatik olmayan yöntemlerle işlenmesi olarak belirtilirken kişisel verilerin kamu güvenliği, milli güvenlik gibi amaçlarla veya gerçek kişiler tarafından sadece kişisel ve ailevi faaliyetler kapsamında işlenmesi durumları kapsam dışı tutulmuştur (md. 3).

---

[10] Direktifin tam metni için bkz. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:NOT

[11] Veri konusu kişi olarak da kullanılabilmektedir.

Kişisel verilerin işlenmesine yönelik ilkeler, 108 Sayılı Sözleşmeyle paralel biçimde ele alınmış olmakla birlikte üye ülkeler tarafından yeterli güvenlik tedbirleri alındığı takdirde kişisel verilerin tarihi, istatistikî ve bilimsel amaçlarla yeniden işlenebileceği hususu düzenlenmiştir (md. 4).

Kişisel verilerin ancak ilgili kişinin açık rızasıyla veya,

- İlgili kişinin taraf olduğu bir sözleşmenin ifası,
- Veri kontrolörünün bir yasal yükümlülüğü yerine getirmesi,
- İlgili kişinin meşru çıkarlarının korunması,
- Kamu yararına bir görevin yerine getirilmesi,
- Veri kontrolörünün kendi haklı çıkarlarının korunması

hususlarında veri işlemenin gerekli olması koşuluyla işlenebileceği (md. 7) Direktifte düzenlenen önemli hususlardan birisidir.

Özel kategorideki veriler (hassas veriler) kapsamında, bir kişinin ırkını, etnik kökenini, siyasi düşüncelerini, dini ya da felsefi inançlarını, sendika üyeliğini açığa çıkaran kişisel veriler ile sağlık ve cinsel yaşama ilişkin verilerin işlenmesi yasaklanmış ancak anılan verilerin tıbbi teşhis, tedavi veya sağlık hizmetlerinin yürütülmesi, suç soruşturulması için gerekli olması gibi sebeplerle ilgili kanunlarda yeterli koruma tedbirleri sağlanarak işlenebileceği belirtilmiştir (md. 8).

Veri kontrolörü, hakkında kişisel verileri toplanan ilgili kişiye, kendisinin ve varsa temsilcisinin kimliği, verilerin işlenme amacı, verilerin kimlere aktarılabileceği, verilere erişim ve veriler üzerinde düzeltme haklarının bulunduğu bilgilerini aktarmak durumundadır (md. 10). Kişisel verilerin, ilgili kişiden toplanmaması hâlinde de ilgili kişiye yukarıdaki bilgiler ve işleme konu olan veri kategorileri hakkında bilgi verilir (md. 11). İlgili kişilerin kişisel

verilere erişim ve itiraz hakları da üye ülkeler tarafından sağlanmalıdır (md. 12,14).

Veri kontrolörü, kişisel verilerin istem dışı veya hukuka aykırı biçimde yok edilmesi, kaybolması, değiştirilmesi ve verilere yetkisiz erişilmesi durumlarına karşı kişisel verilerin korunması amacıyla gerekli teknik ve idari tedbirleri almakla yükümlü kılınmış (md. 17), kişisel verilerin üçüncü ülkelere aktarılması ise söz konusu ülkelerde kişisel verilere ilişkin yeterli koruma düzeyinin sağlanması şartına bağlanmıştır (md. 25). Direktif kapsamında üye ülkelerin ulusal mevzuatlarına aktarılacak maddelerin uygulanmasına katkıda bulunacak mesleki davranış kurallarının çeşitli sektörlerin özellikleri dikkate alınarak hazırlanması teşvik edilmektedir (md. 27).

Direktifte üye ülkeler tarafından çıkarılan yasal düzenlemelerin uygulanmasını kontrol etmekle görevli bir ya da daha fazla bağımsız denetim organlarının kurulması (md. 28), ayrıca bağımsız hareket eden ve danışma niteliğinde olan bir çalışma grubu kurulması (md. 29) öngörülmüştür.

AK tarafından 2004 yılında Avrupa Konseyi ve Parlamentosuna sunulan raporda, Direktifin üye ülkelerin tamamında uygulanamamasına rağmen veri koruma alanında yüksek bir standarda ulaşıldığı ve üye ülkeler arasında veri akışına ilişkin engellerin kalktığı, bu nedenle yakın gelecekte Direktifte değişiklik yapılmasına gerek olmadığı belirtilmiş ancak Direktifin daha iyi uygulanabilmesi için çalışma programları oluşturulması yönünde karar alınmıştır. Müteakiben AK tarafından 7 Mart 2007'de Konsey ve Parlamentoya yapılan bildirimde ise çalışma programlarının özellikle VKÇG'nin katkılarıyla Direktifin daha iyi uygulanmasına büyük ölçüde katkı sağladığı, Direktifin bazı ülkelerde bütünüyle uygulanamasa da bu durumun iç pazar için önemli bir sorun teşkil etmediği belirtilmiş, diğer yandan üye ülkeler arasındaki farklılıkların en aza indirilmesi için çalışma programlarına devam edilmesi tavsiye edilmiştir (Buellesbach, 2010).

Küreselleşme ve yeni gelişen teknolojilerle birlikte kişisel verilerin korunmasında karşılaşılan zorluklar hakkında görüş toplama amacıyla AK tarafından 2009 yılında "Kişisel Verilerin Korunması Hakkına İlişkin Yasal Çerçeve" adlı konsültasyon dokümanı yayımlanmıştır. Dokümanda, mevcut yasal çerçevenin belirtilen zorlukları aşıp aşmadığı ve zorlukların çözümünde ne gibi önlemler alınabileceği hususları da yer almıştır (Buellesbach, 2010).

2.5.3.2 2002/58/EC sayılı E-Gizlilik Direktifi

Telekomünikasyon sektöründe kişisel verilerin işlenmesi ve gizliliğin korunması hakkında 15 Aralık 1997 tarihinde yayımlanan ISDN Direktifi, Veri Koruma Direktifinde belirlenen ilkelerin telekomünikasyon sektöründe özel kurallara dönüştürülmesini sağlamış ancak teknolojik gelişmelere (kablolu haberleşmeden kablosuz haberleşmeye, ses hizmetinden veri hizmetlerine geçiş vb.) uyum sağlamak amacıyla ISDN Direktifinin yenilenmesi öngörülmüştür. Bu kapsamda, AK tarafından 1999'da hazırlanan Taslak, 12 Temmuz 2002'de kabul edilerek 2002/58/EC sayılı E-Gizlilik Direktifi[12] yürürlüğe girmiş, ISDN Direktifi ise yürürlükten kaldırılmıştır (Gratton, 2003).

Kroes (2009) E-Gizlilik Direktifinin ISDN Direktifinde belirtilen hükümlere ilave olarak teknolojiden bağımsız yeni yükümlülükler getirmeyi amaçlarken Veri Koruma Direktifinde sağlanan veri koruma düzeyini de güvence altına almayı hedeflediğini, bu bağlamda örneğin çerez[13] (*cookie*) ve mobil şebekelerde konum belirleme hizmetleri gibi yeni teknolojiler karşısında gizlilikle ilgili ortaya çıkan problemlerin E-Gizlilik Direktifiyle giderilebileceğini belirtmektedir.

---

[12] Direktifin tam metni için bkz. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:EN:PDF

[13] Çerezlerle ilgili bilgi için bkz. http://www.bidb.itu.edu.tr/?d=834

2.5.3.2.1 Kapsam

E-Gizlilik Direktifinin, kamu haberleşme şebekelerinde kamuya açık elektronik haberleşme hizmetlerinin sağlanmasıyla ilgili olarak kişisel verilerin işlenmesi konusunda uygulanması (md. 3/1) ancak AB kurucu antlaşmalarının kapsamına girmeyen faaliyetler ile kamu güvenliği, milli güvenlik, savunma ve kriminal suçların soruşturulması alanlarında uygulanmaması (md. 1/3) öngörülmüştür. Ayrıca 8, 10 ve 11 inci maddelerin sayısal santrallere bağlı abone hatları ile -teknik imkânların elvermesi ve yüksek maliyet gerektirmemesi halinde- analog santrallere bağlı abone hatlarına uygulanması (md. 3/2) Direktifte belirtilmiştir. Veri Koruma Direktifinden farklı olarak gerçek kişiler yanında tüzel kişilerin de temel haklarını koruyan E-Gizlilik Direktifi aboneler[14] yanında kullanıcıları[15] da korumayı amaçlamaktadır (Koenig vd., 2009).

Veri Koruma Direktifinin 29 uncu maddesi uyarınca kurulan VKÇG'nin, aynı Direktifin 30 uncu maddesinde belirtilen görevlerini elektronik haberleşme sektöründe temel hak ve özgürlükler ile meşru çıkarların korunması hususlarında da yerine getirmesi düzenlenmiştir (md. 15/3).

2.5.3.2.2 Tanımlar

Kullanıcı, trafik verisi, konum verisi, haberleşme, abone veya kullanıcının rızası, arama, katma değerli hizmet ve elektronik ileti E-Gizlilik Direktifinde tanımlanan başlıca kavramlardır.

Trafik verisi, elektronik haberleşme şebekesinde bir haberleşmenin iletilmesi ya da faturalandırılması amacıyla işlenen her türlü veri olarak tanımlanırken;

---

[14] EHK'da abone tanımı, "Bir işletmeci ile elektronik haberleşme hizmetinin sunumuna yönelik olarak yapılan bir sözleşmeye taraf olan gerçek ya da tüzel kişi"şeklindedir.

[15] EHK'da kullanıcı, "Aboneliği olup olmamasına bakılmaksızın elektronik haberleşme hizmetlerinden yararlanan gerçek veya tüzel kişi" olarak tanımlanmıştır.

(md. 2/b) konum verisi, kamuya açık bir elektronik haberleşme hizmeti kullanıcısına ait bir terminal cihazının coğrafi konumunu belirleyen ve elektronik haberleşme şebekesinde işlenen her türlü veri olarak tanımlanmaktadır (md. 2/c).

Abone veya kullanıcının rızasının ise Veri Koruma Direktifinde belirtilen, verileri işlenen ilgili kişinin rızasına karşılık gelmektedir (md. 2/f). Buna göre, rıza ilgili kişinin özgürce, konu hakkında yeterince bilgilendirilmiş olarak kendisiyle ilgili verilerin işlenmesine verdiği irade beyanıdır. Bu çerçevede, ilgili kişinin susmasının rıza olarak değerlendirilmeyeceği, rızanın somut bir olaya ilişkin olması, baskı altında verilmemesi ve ayrıca kişinin kendisiyle ilgili verilerinin hangi faaliyetlerde kullanılacağını bilmesi gerektiği belirtilmektedir (Şimşek, 2008). Rıza tanımında[16] yer alan "specific" ifadesinin bazı veri koruma otoriteleri tarafından kişinin verdiği rızanın işaret kutucuğu (*tick box*) gibi bir mecrayla ayrıca belirtilmesi şeklinde yorumlandığı görülmektedir (Brunger ve Watts, 2010).

Elektronik ileti kavramı; alıcı tarafından toplanıncaya kadar alıcının terminal cihazında ya da şebekede saklanabilen ve bir kamu haberleşme şebekesi üzerinden gönderilen yazılı, sesli, görüntülü her türlü mesaj anlamına gelmektedir (md. 2/h). Teknolojik tarafsızlığı sağlamak amacıyla tanımın geniş tutulduğunu ve gönderici ile alıcının eş zamanlı katılımını gerektirmeyen her türlü mesajın tanıma dâhil edildiğini belirten VKÇG (2004) e-posta, SMS, MMS, arama cihazlarına bırakılan mesajlar, mobil hizmetlerde de kullanılan sesli mesaj sistemleri gibi vasıtaları elektronik iletiye örnek olarak vermektedir. Açılır pencere (*pop-up*) mesajları ise AK tarafından elektronik ileti olarak görülmemektedir (Buellesbach, 2010).

---

[16] 95/46/EC sayılı Veri Koruma Direktifinde rıza tanımı "the data subject's consent shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed" şeklinde yer almaktadır.

2.5.3.2.3 Genel hususlar

İstek dışı haberleşme, trafik verisi ve konum verisinin hangi hallerde ve kimler tarafından işleneceği hususları bir sonraki bölümde işlenirken E-Gizlilik Direktifinde yer alan diğer konular aşağıda özetlenmektedir:

a) **Güvenlik:** İşletmeciler sundukları hizmetlerin güvenliğini garanti altına almak için uygun teknik ve idari tedbirleri almak (md. 4/1) ve şebeke güvenliğini ihlal eden belirli bir risk olması durumunda bu risk hakkında abonelerini bilgilendirmekle yükümlü kılınmaktadır (md. 4/2).

b) **Haberleşmenin gizliliği:** Üye ülkelerin, yasaların öngördüğü durumlar hariç olmak üzere kullanıcının rızası olmadan bir başkası tarafından haberleşmenin ve ilgili trafik verisinin dinlenmesi, kaydedilmesi, saklanması ve gizlice gözetlenmesini yasaklamaları istenmektedir (md. 5/1). Buellesbach (2010) haberleşmenin ve trafik verisinin gizliliği ilkelerinin temelde AİHS 8 inci maddeye dayandığını, Direktif maddesinde "haberleşme" ve "trafik verisi" şeklinde bir ayrıştırmaya gidildiğini, ancak bu durumun gizliliğin sağlanması yükümlülüğüne ilişkin olarak trafik verisi konusunda haberleşmeye göre daha fazla istisna getirilmesini sağladığını belirtmektedir.

   Elektronik haberleşme şebekesi kullanıcılarının terminal cihazları ile bu cihazlarda saklanan bilgiler kullanıcıların özel alanına girdiğinden AİHS kapsamında koruma gerektirmektedir. Casus yazılımlar (*spyware*), internet virüsleri (*web bug*), gizli tanımlayıcılar (*hidden identifiers*) ve benzeri cihazlar kullanıcıların terminal cihazlarına girerek gizli bilgilere erişebilmekte ya da kullanıcı aktivitelerini takip edebilmektedir. Bu tür cihazların kullanımına kullanıcıların bilgisi dâhilinde meşru amaçlarla izin verilmelidir (E-Gizlilik Direktifi, dibace 24).

Diğer yandan çerez adı verilen cihazlar reklamcılıkta, çevrimiçi işlemlerde, kullanıcıları tanımlama ve doğrulamada faydalı ve meşru bir araç olabilmektedir. Çerezlerin bilgi toplumu hizmetlerinin sunumunu kolaylaştırmak gibi yasal bir amaçla kullanılması durumunda kullanımlarına, Veri Koruma Direktifi kapsamında kullanıcıların, cihazların kullanım amaçları hakkında açık ve anlaşılır biçimde bilgilendirilmeleri kaydıyla izin verilmelidir (E-Gizlilik Direktifi, dibace 25). Bu bağlamda, üye ülkeler bilgi saklamak veya abone/kullanıcının terminal cihazında saklanan bilgiye erişim sağlamak amacıyla elektronik haberleşme şebekelerinin kullanılmasına ancak ilgili kullanıcı/abonelerin açık ve kapsamlı olarak bilgilendirilmesi ve abone/kullanıcılara verilerinin işlenmesini reddetme hakkı verilmesi kaydıyla izin vereceklerdir (md. 5/3).

c) **Ayrıntılı faturalar:** Üye ülkeler, ayrıntılı fatura alan aboneler ile arayan ve aranan abonelerin mahremiyet haklarını bağdaştırmak amacıyla ulusal mevzuat hükümlerini uygulayacaklar, kullanıcı ve abonelere gizliliği artırıcı haberleşme yöntemleri sağlayabileceklerdir (md. 7). Bu çerçevede, ayrıntılı faturalar elektronik haberleşme hizmeti kullanıcılarının mahremiyetini tehdit edebildiğinden abonelere, ayrıntılı faturalarda aranan numaraların belirli sayıdaki hanelerinin silindiği farklı türde bir detaylı fatura sunulması işletmecilerden istenebilecektir (E-Gizlilik Direktifi, dibace 33). Örneğin, Alman Anayasa Mahkemesi aranan numaraların tam olarak gösterilmesi durumunda bireyin anayasal haberleşme özgürlüğünün ihlal edildiğine hükmettiğinden Almanya'da 1994 yılından itibaren faturalarda bütün telefon numaralarının son rakamları kısaltılarak gösterilmektedir (Özdemir, 2009).

d) **Arayan ve bağlanılan hattın kimliğinin gösterilmesi ve kısıtlanması:** Analog şebekelerde arayan tarafa ait bilgilerin aranan tarafa gönderilmesinin teknik olarak mümkün olmaması ve aynı zamanda bu duruma ihtiyaç duyulmamasına rağmen, sayısal telefon şebekelerinin ortaya çıkması ve ekranı olan telefon cihazlarının kullanılmaya

başlamasıyla birlikte arayan ve bağlanılan hattın kimliğinin gösterilmesi ve kısıtlanması hususlarında düzenleme ihtiyacı ortaya çıkmıştır (Buellesbach, 2010).

Arayan tarafa kimliğini gizleme, aranan tarafa ise kimliği belli olmayan hatlardan gelen aramaları reddetme imkânı sağlanması ve özellikle yönlendirilen aramalarda aranan tarafın yasal çıkarının korunması gerekli görüldüğünden (E-Gizlilik Direktifi, dibace 34) işletmeciler, arayan hattın kimliğinin görünmesine imkân sağlandığı durumlarda,

- Arayan kullanıcıya her bir arama için basit bir yöntemle ve ücretsiz olarak kimliğini gizleme (md. 8/1),
- Aranan aboneye basit bir yöntemle ve ücretsiz olarak gelen aramalarda arayan hattın kimliğinin gösterilmesini engelleme (md. 8/2),
- Arayan kullanıcının kimliğini gizlemesi halinde aranan abonenin isteğine bağlı ve ücretsiz olarak gelen aramaların abone tarafından reddedilmesi (md. 8/3)

imkânı sağlamakla yükümlüdür.

Bağlanılan numaranın kimliğinin görünmesine imkân sağlandığı durumlarda aranan aboneye, bağlanılan hattın kimliğinin arayan kullanıcıya gösterilmesinin engellenmesi imkânı da sağlanacak (md. 8/4), böylece bağlanılan hattın numarasının aranan numaradan farklı olduğu durumlarda hattına çağrı yönlendirilen bireyin mahremiyeti korunmuş olacaktır (ICO, 2006).

Abone ve kullanıcılara sağlanan imkânlara Direktifin 10 uncu maddesiyle istisna getirilmektedir. Buna göre, abone tarafından yapılan başvuru üzerine rahatsız edici veya kötü niyetli aramaların takip edilebilmesi için

arayan hattın kimliğinin gizlenmesi geçici olarak engellenebilir. Benzer şekilde, acil aramalara ilişkin çağrılara cevap vermeleri amacıyla kolluk güçleri, ambülâns ve itfaiye gibi organizasyonlar için arayan hattın kimliğinin gizlenmesi engellenebilir; abone/kullanıcının konum verisi, rızası olmasa veya geçici olarak reddetse dahi işlenebilir.

e) **Otomatik çağrı yönlendirme:** Başkaları tarafından otomatik çağrı yönlendirmesiyle abonelerin rahatsız edilmemesi için gerekli önlemler alınmalı, abonelerin işletmecilere talepte bulunmaları halinde terminal cihazlarına yönlendirilen çağrılar durdurulmalıdır (E-Gizlilik Direktifi, dibace 37). Bu kapsamda, üye ülkeler kullanıcıların terminal cihazlarına üçüncü bir parti tarafından yapılan otomatik çağrı yönlendirmelerinin ücretsiz ve basit bir yöntemle engellenmesine imkân sağlayacaklardır (md. 11).

f) **Abone rehberleri:** Üye ülkeler abonelerin kişisel verilerinin yer alabileceği basılı veya elektronik abone rehberlerinin amaçları ve bu rehberlerin elektronik sürümlerindeki arama fonksiyonlarına bağlı ilave kullanım imkânları hakkında rehbere kaydedilmeden önce ve ücretsiz olarak abonelerin bilgilendirilmelerini sağlayacaklardır (md. 12/1). Aboneler kişisel verilerinin kamuya açık bir rehberde yer alıp almamasını belirleyebilmeli, aynı zamanda kişisel verilerinin düzeltilmesini, teyit edilmesini ve/veya rehberden çıkarılmasını ücretsiz olarak talep edebilmelidir (md. 12/2).

Abonenin adı ve gerektiğinde aboneyi tanımlayan minimum bilgileri kullanılarak yapılacak sorgulamalar dışındaki rehberlik hizmetleri için abonenin ek rızası aranır (md. 12/3). Aboneden veri toplayan taraf ya da verilerin iletildiği üçüncü tarafın, verileri ilave amaçlar için kullanmak istemesi durumunda verileri toplayan ilk taraf ya da verilerin iletildiği üçüncü taraf abonenin rızasını yeniden almalıdır (E-Gizlilik Direktifi, dibace 39).

İstek dışı haberleşme, trafik ve konum verilerinin işlenmesi gibi hususların[17] da düzenlendiği Direktifin 31 Ekim 2003 tarihine kadar üye ülkelerin ulusal mevzuatlarına aktarılması öngörülmüştür (md. 17). Bu kapsamda, Direktifin mevcut durumda üye ülkelerin tamamında iç hukuka aktarıldığı görülmektedir[18].

Kuner (2007), Veri Koruma Direktifi ile E-Gizlilik Direktifinin kesişme ve ayrışma alanlarını ayırt etmenin zor olduğunu, E-Gizlilik Direktifinde "kamu haberleşme şebekesi" ile "kamuya açık elektronik haberleşme hizmetleri"nin kişisel verilerin işlenmesi uygulamalarında gereklilik olduğunu, Veri Koruma Direktifinin uygulanmasının ise "kişisel verilerin işlenme yöntemlerini ve amaçlarını belirleyen" bir "veri kontrolörü"nün varlığını tespit etmeye bağlı olduğunu ifade etmektedir.

2.5.3.3 2006/24/EC sayılı Veri Saklama Direktifi

Suç soruşturmalarında kullanılacak trafik verilerinin saklanması konusu uzun süre Avrupa'da tartışılmış, Veri Koruma Direktifi yürürlüğe girmeden önce bazı üye ülkelerin ulusal mevzuatında verilerin saklanmasına ilişkin hükümler yer almıştır. Örneğin İrlanda telefon haberleşmesinde trafik verilerinin 3 yıl süreyle saklanmasını zorunlu kılarken İtalya'da bu süre 4 yıl olarak belirlenmiş, sonrasında yükümlülük internet servis sağlayıcılarını ve internet kafeleri de kapsayacak şekilde genişletilmiştir (EECKE, 2006).

2001'de ABD, 2004 yılında Madrid ve 2005'te Londra'da meydana gelen terörist saldırılar veri saklama konusunda etkili tedbirler alınmasını gerekli kılmıştır (FEILER, 2008). Bu çerçevede Fransa, İngiltere, İrlanda ve İsveç tarafından hazırlanan ve AK tarafından Taslak haline getirilen metin Avrupa

---

[17] Bir sonraki bölümde detaylı olarak incelenmektedir.
[18] Detaylı bilgi için bkz. http://ec.europa.eu/information_society/policy/ecomm/library/national_transposition/index_en.htm

Parlamentosunda onaylanmasının ardından 3 Mayıs 2006'da yürürlüğe girmiştir (EECKE, 2006).

2.5.3.3.1 Kapsam

Direktif, işletmeciler tarafından işlenen ya da üretilen belirli verilerin ciddi suçların araştırılması, soruşturulması ve kovuşturulmasında kullanılmak üzere saklanmasına ilişkin yükümlülükler getirmektedir (md. 1/1). Bununla birlikte gerçek ve tüzel kişilere ilişkin trafik ve konum verileri ile abone veya kayıtlı kullanıcıların belirlenmesi için gerekli olan veriler Direktif kapsamında ele alınırken haberleşmenin içeriği kapsam dışı tutulmaktadır (md. 1/2).

Direktifin gerekçe kısmında sadece elektronik haberleşme hizmetinin sunumu esnasında üretilen ya da işlenen verilerin saklanmasının öngörüldüğü ancak işletmeciler tarafından işlenmeyen ya da üretilmeyen veriler için saklama yükümlülüğü getirilmediği, diğer yandan saklanacak verilerin erişilebilir olması gerektiği belirtilmektedir (Feiler, 2008).

2.5.3.3.2 Tanımlar

Direktifte tanımlanan başlıca kavramlar aşağıda belirtilmektedir (md. 2):

- Veri: Abone ya da kullanıcıyı tanımlamak için gerekli olan trafik verisi, konum verisi ya da ilgili veriler,
- Telefon hizmeti: Arama, mesaj, tamamlayıcı hizmet (çağrı yönlendirme vb) ve çoklu ortam hizmetleri,
- Kullanıcı kimliği: İnternet erişim veya internet haberleşme hizmetlerine abonelik ya da kayıt esnasında kişilere tahsis edilen özel tanımlama,
- Hücre kimliği: Mobil telefon çağrısının başladığı ya da sonlandığı hücrenin kimliği,

- Başarısız çağrı girişimi: Bağlantının başarılı bir şekilde kurulmasına rağmen çağrının cevaplanmadığı ya da şebeke yönetimine müdahalenin olduğu haberleşme.

2.5.3.3.3 Genel hususlar

Veri Saklama Direktifinde yer alan genel hususlara aşağıda yer verilmekle birlikte saklanacak veri kategorileri, veri saklama süreleri ve saklanan verilerin korunması ve güvenliği konuları bir sonraki bölümde daha detaylı olarak ele alınacaktır.

a) **Veri saklama yükümlülüğü ve verilere erişim:** E-Gizlilik Direktifinin 5, 6 ve 9 uncu maddelerinde elektronik haberleşme hizmetlerinin sunumunda üretilen trafik ve konum verilerinin ne zaman silinmesi veya anonim hale getirilmesi gerektiği hususları belirtilmekte (Veri Saklama Direktifi, dibace 3) ancak bu maddelere ulusal güvenlik, kamu güvenliği, kriminal suçların tespiti, araştırılması ve soruşturulması gibi belirli durumlarda sınırlama getirilebileceği aynı Direktifin 15 inci maddesinde dile getirilmektedir. Bu çerçevede, üye ülkeler Veri Saklama Direktifinde belirlenen verilerin saklanmasına ilişkin gerekli düzenlemeleri yapacaklardır. Veri saklama yükümlülüğü başarısız çağrı girişimlerini de kapsayacaktır (md. 3). Üye ülkeler Direktif kapsamında saklanması istenen verilerin yasalar çerçevesinde ve sadece yetkili otoritelere iletilmesini garanti altına alacaklardır (md. 4).

   Trafik verisinin, niteliği gereği hassas olduğunu bu çerçevede, trafik verilerine erişim ve bu verilerin yasa uygulayıcı makamlara transfer edilmesi konularına ekstra önem verilmesi gerektiğini belirten VKÇG (2010), saklanan verilere nasıl erişileceğine ve söz konusu verilerin nasıl transfer edileceğine ilişkin koşulların yasalarda açıkça yer alması gerektiğini ancak bunun öz düzenlemeyle gerçekleştirilemeyeceğini ifade etmektedir.

b) **Saklanacak veri kategorileri**: Üye ülkeler haberleşmenin takibi ve kaynağının tanımlanması, haberleşmenin sonlanacağı noktanın belirlenmesi, haberleşmenin tarihi, zamanı ve süresinin belirlenmesi, haberleşmenin türünün tanımlanması, kullanıcıların haberleşme cihazlarının veya bunların ekipmanlarının tanımlanması, mobil haberleşme cihazının konumunun belirlenmesi amacıyla sabit ve mobil telefon hizmeti ile internet hizmetlerine ilişkin veri kategorilerinin[19] saklanmasını temin edeceklerdir (md. 5). Söz konusu veriler haberleşmenin gerçekleştiği andan itibaren 6 aydan az 24 aydan fazla olmamak üzere saklanacaktır (md. 6).

c) **Verilerin korunması ve güvenliği:** Kişisel verilerin işlenmesi ile veri işleme faaliyetlerinin güvenliği ve gizliliğinin garanti altına alınmasına dair Veri Koruma Direktifi ile işletmecilere getirilen yükümlülükler, Veri Saklama Direktifi kapsamında saklanacak veriler için de geçerli olacak; bu verilere ilişkin olarak asgari aşağıda belirtilen veri güvenliği ilkeleri sağlanacaktır (md. 7):

- Saklanan veriler, şebekedeki diğer verilerle aynı kalitede olmalı, aynı güvenlik ve koruma tabirlerine tabi tutulmalıdır,
- Saklanan verilerin tedbirsizlikle, hukuka aykırı veya yetkisiz olarak erişim, tahrip, kayıp, değişiklik, depolama, işleme ve ifşa fiillerine karşı korunması için uygun teknik ve idari tedbirler alınmalıdır,
- Verilerin sadece özel yetkilendirilmiş personel tarafından erişilebilir olmasının sağlanması için uygun teknik ve idari tedbirler alınmalıdır,
- Veriler saklama süresi sonunda imha edilmelidir.

Üye ülkeler, saklanan verilerin güvenliğine ilişkin uygulamaların izlenmesi amacıyla denetleyici bir otorite belirleyecek (md. 9), ayrıca saklanan

---

[19] Saklanacak veri kategorilerine ilişkin detaylı bilgiler bir sonraki bölümde incelenmektedir.

verilerin ve söz konusu verilere ilişkin gerekli tüm bilgilerin yetkili otoritelere gecikme olmadan iletilebilecek biçimde muhafaza edilmesini sağlayacaklardır (md. 8).

d) **İstatistikler:** Üye ülkeler saklanan verilere ilişkin istatistikleri yıllık bazda AK'ya sunacaklardır (md. 10). Bu istatistikler aşağıdaki hususları içermelidir:

- Yürürlükte bulunan ulusal mevzuat çerçevesinde yetkili otoritelere bilgi sunulan vakalar,
- Verilerin saklanmaya başlandığı tarih ile yetkili otoriteler tarafından talep edildiği tarih arasında geçen süre,
- Veri talebinin karşılanamadığı vakalar.

Direktifin 15 Eylül 2007 tarihine kadar üye ülkelerin ulusal mevzuatlarına aktarılması öngörülmüş ancak internet erişimi, internet telefonu ve internet e-postasına ilişkin verileri saklama yükümlülüğünün 15 Mart 2009 tarihine kadar ertelenebileceği belirtilmiştir (md. 15).

Mevcut durumda AB ülkelerinin genelinde Direktif hükümleri iç hukuka aktarılırken Almanya, Çek Cumhuriyeti ve Romanya'da Anayasa Mahkemeleri, çıkarılan yasaların özel hayatın gizliliği ilkesine aykırı olduğuna hükmetmiştir. Buradaki itirazın Direktifin kendisine değil Direktife uyum amacıyla çıkarılan yasalara ilişkin olduğu önemli bir husustur (Ersoy, 2011).

2.5.3.4 2009/136/EC sayılı Vatandaş Hakları Direktifi

Elektronik haberleşme sektörüne ilişkin 2002 Avrupa düzenleyici çerçevesinde geçtiğimiz yıllarda değişiklikler olmuş, 2007 yılında ulusal düzenleyici otoriteler tarafından analiz edilecek piyasa sayısı 18'den 7'ye düşürülürken 2009 yılında iki yeni Direktif ve bir Tüzük yayımlanmıştır.

2009/140/EC sayılı Direktif, 2002/19/EC, 2002/20/EC ve 2002/21/EC sayılı Direktiflerde; 2009/136/EC sayılı Direktif ise 2002/22/EC ve 2002/58/EC sayılı Direktiflerde değişiklik öngörmüş, 1211/2009 sayılı Tüzük kapsamında ise Avrupa Elektronik Haberleşme Düzenleyicileri Grubu[20] kurulması kararlaştırılmıştır (Stevens, 2009).

Anılan Direktifler, rekabetin artması, düzenlemelerin iyileştirilmesi, tüketicilerin korunması ve iç pazarın güçlendirilmesi gibi hedeflerin birlikte gerçekleştirilmesi için 12 konuda reform öngörmektedir (Tsatsou, 2011). Kişisel verilerin ihlali ve spam karşısında tüketicilerin korunması başlıklı reform önerisinde, internet oturumu ve telefon aramalarına ilişkin veriler başta olmak üzere müşterilere ait kimlik bilgileri, e-posta adresleri ve banka hesap numaralarının başka kişilerin eline geçmemesi için işletmeciler tarafından gerekli güvenlik tedbirlerinin alınması gerektiği vurgulanarak işletmeciler, kişisel verileri etkileyen güvenlik ihlalleri hakkında yetkili otoriteleri ve tüketicileri bilgilendirmekle yükümlü kılınmaktadır (EU, 2010b).

2009/136/EC sayılı Vatandaş Hakları Direktifi ile, E-Gizlilik Direktifinde yer alan konum verisi tanımı genişletilerek, "elektronik haberleşme hizmeti aracılığıyla" işlenen veriler de konum verisi kapsamına dâhil edilmekte, ayrıca "kişisel veri ihlali" adıyla yeni bir tanım getirilmektedir. Buna göre, saklanan veya elektronik haberleşme hizmetinin teminiyle bağlantılı olarak başka şekilde işlenen kişisel verilere yetkisiz erişim ya da söz konusu verilerin tedbirsizlikle veya hukuka aykırı olarak yok edilmesi, kaybolması, değiştirilmesi ve yetkisiz olarak açıklanmasına neden olan güvenlik ihlali, kişisel veri ihlali olarak değerlendirilecektir (md. 2).

E-Gizlilik Direktifinin kapsamına veri toplayabilen ve nesne tanımlayabilen (örneğin RFID[21]) cihazları destekleyen kamu haberleşme şebekeleri dâhil

---

[20] BEREC (Body of European Regulators for Electronic Communications)
[21] Detaylı bilgi için bkz. http://www.hho.edu.tr/hutendergi/2011OCAK/12_OZMEN_BIRGUN.pdf

edilmekte (md. 3), güvenlikle ilgili birçok yenilik getirilmektedir. Şebeke güvenliği için teknik ve idari tedbirler alınırken işletmecilerin sağlaması gereken bazı koşullar şu şekilde sıralanmaktadır (md. 4/b):

- Kişisel verilere yetkili personelin yasal amaçlarla erişmesi,
- Kaydedilen veya aktarılan kişisel verilerin tedbirsizlik sonucu veya hukuka aykırı olarak yok edilmesi, tedbirsizlik sonucu kaybolması veya değiştirilmesi, yetkisiz veya hukuka aykırı olarak işlenmesi, erişilmesi, açıklanması durumlarına karşı korunması,
- Kişisel verilerin işlenmesine yönelik güvenlik politikasının gerektiği gibi uygulanması.

Kişisel veri ihlali durumunda işletmecilere, söz konusu ihlalin yetkili otoritelere bildirilmesi yükümlülüğü getirilmektedir. Eğer ihlal abone veya bireyin kişisel verilerini ya da mahremiyetini olumsuz yönde etkileyecekse abone ve bireylere de ihlalin bildirilmesi zorunlu kılınmakta ancak işletmeci bu ihlalin olmaması için şebekede gerekli güvenlik tedbirlerini aldığını yetkili otoriteye ispat ederse abone ya da bireyleri bilgilendirme zorunluluğu getirilmemektedir (md. 4/c). AB mevzuatına dâhil edilmesi uzun süre alsa da, kişisel veri ihlali durumunda bireylere ve yetkili otoritelere bildirim yükümlülüğü getirilmesi önemli bir gelişme olarak görülmektedir (Barcelo ve Traung, 2010).

Kişisel veri ihlallerine ilişkin olarak işletmecilerin kayıt kütüğü tutmakla yükümlü kılınması Direktifte düzenlenen bir diğer konudur. İhlali oluşturan sebepler, ihlalin etkileri ve ihlalin çözümüne yönelik alınan tedbirlerin yer alacağı kayıt kütüğü, sadece bu amaç için gerekli olan bilgileri içerecektir (md. 4/c). Avrupa Komisyonu ENISA, VKÇG ve AVKD'ye danışarak kişisel veri ihlali bildiriminin hangi durumlarda yapılacağı, formatı ve yapılış biçimi konularında teknik ilkeler belirleyebilecektir.

E-Gizlilik Direktifinde yapılan önemli bir değişiklik de çerezlerle ilgilidir. Bir bilgi toplumu hizmetinin sağlanması amacıyla kullanıcı tarafından talep edilmesi veya elektronik haberleşme şebekesi üzerinden bir haberleşmenin iletilmesi halleri saklı kalmak üzere, abone ve kullanıcıların terminal cihazında bilgi saklanması veya saklanan bilgiye erişim sağlanması için ilgili abone ve kullanıcıların veri işleme hakkında açık ve kapsamlı olarak bilgilendirilmeleri ve verilerin işlenmesine rıza vermeleri gerekmektedir. (md. 5). Böylece çerezler konusunda daha önceden uygulanan opt-out[22] sistemi yerine opt-in sistemi getirilmektedir.

Orrick (2009)'e göre çerezlere ilişkin hükümlerin katı bir şekilde uygulanması, kullanıcıların açılır pencerelerle ya da diğer araçlarla rızalarının alınmasını gerektireceğinden özellikle internet üzerinden reklam yapan yayıncıların gelirlerini azaltacak, bu durum ise internet üzerindeki gezintilerin birçok kullanıcı açısından sıkıcı olmasına neden olacaktır. Ayrıca çerezlere getirilen istisnaların nasıl uygulanacağı konusunda da bir belirsizlik bulunmaktadır.

İstek dışı haberleşmeyle ilgili olarak E-Gizlilik Direktifinde yapılan değişiklik ile, aboneler yanında kullanıcılar da kapsama dâhil edilmiştir (md. 7).

---

[22] Detaylı bilgi için bkz. 3.1.5.2

3. AB DİREKTİFLERİ KAPSAMINDA KİŞİSEL VERİLERİN İŞLENMESİ, SAKLANMASI VE GİZLİLİĞİNİN KORUNMASI

4 kısımdan oluşan bu bölümde, öncelikle AB Direktiflerinde yer alan kişisel veri, trafik verisi ve konum verisi gibi veri türleri ve bu veriler arasındaki ilişki açıklandıktan sonra kişisel verilerin doğrudan pazarlama amaçlı kullanımıyla ilişkilendirilen istek dışı haberleşmeye yer verilecektir. İkinci kısımda, kişisel verilerin işlenmesine ilişkin ilkelere değinilecek, trafik veya konum verilerinin hangi koşullarda ve kimler tarafından işlenebileceği ele alınacaktır. Üçüncü kısımda kişisel verilerin saklanmasına yönelik olarak işletmecilere getirilen yükümlülüklerin aktarılmasının ardından son kısımda, kişisel verilerin korunmasında son dönemde tartışılan tasarımsal gizlilik ve PET üzerinde durulacaktır.

3.1 Veri Türleri, Veri Türleri Arasındaki İlişki ve İstek Dışı Haberleşme

Kişisel verilerin işlenmesi saklanması ve korunması ile ilgili AB Direktiflerinde genel olarak 3 tür verinin ele alındığı görülmektedir. Trafik ve konum verisi elektronik haberleşme alanında kullanılan kavramlar olmakla birlikte bireylerle ilişkilendirildiği ölçüde kişisel veri kapsamında değerlendirilmektedir. Ancak kişisel veri niteliği taşımayan trafik veya konum verileri söz konusu olabildiğinden veri türlerini kişisel veriler, trafik ve konum verileri başlıkları altında incelemek yerinde olacaktır.

3.1.1 Kişisel veriler

Kişisel veriler Veri Koruma Direktifinde, "*Doğrudan veya dolaylı olarak; kimlik numarası ya da fiziksel, psikolojik, zihinsel, ekonomik, kültürel ya da sosyal kimliğin bir ya da birden fazla unsuruna dayanılarak kimliği belirlenebilen veya belirli gerçek kişilere ilişkin bütün bilgiler*" olarak tanımlanmaktadır. AB üyesi ülke uygulamaları ışığında kişisel veri kavramına ilişkin bazı belirsizlikler ve farklılıklar olduğunu belirten VKÇG, kavrama yönelik detaylı

bir analizi gerekli görmüş ve 2007/4 sayılı görüş dokümanı ile kişisel veri tanımında yer alan "belirli veya belirlenebilir olmak", "ilişkin olmak" ve "bütün bilgiler" unsurları hakkında görüş bildirmiştir. Bu çerçevede VKÇG'ye göre (VKÇG, 2007),

- Kişisel veri kavramı herhangi türde bir bilgiyi barındırabilir. Hassas veriler, kişinin iş ilişkileri, sosyal ve ekonomik davranışları bu kapsamdadır.
- Bilgilerin yer aldığı araç ya da bilginin formatına ilişkin olarak kişisel veri kavramı akustik, foto grafik, sayısal ve alfabetik formatta bilgileri içerdiği gibi videokaset veya kâğıt üzerinde saklanan bilgiler ile ikili kod (*binary kod*) şeklinde bilgisayar hafızasında depolanan bilgileri de kapsamaktadır.
- Bir kişinin belirlenebilir olması Veri Koruma Direktifinin tanım kısmında da belirtildiği üzere kişinin adı, boyu, saç rengi, mesleği gibi tanımlayıcılar aracılığıyla gerçekleşebilir.
- Bir kişi adıyla doğrudan; telefon numarası, araç plaka numarası, sosyal güvenlik numarası, pasaport numarası veya kişinin tanınmasına imkân verecek yaş, meslek, oturduğu yer gibi bilgilerin kombinasyonu aracılığıyla dolaylı olarak belirlenebilir.
- Ad ve adres gibi tanımlayıcılar çoğu zaman kişileri belirlemede yeterli olsa da kişisel verilerin tutulduğu elektronik dosyalar kişilere, özgün tanımlayıcılar (*unique identifiers*) atayabilmekte, dolayısıyla kişiyi belirlemek için ad ve adres bilgilerine gerek olmayabilmektedir.
- İnternet erişim sağlayıcıları dinamik IP adresi, tarih, zaman ve süre bilgilerini sistematik olarak bir dosyada tuttukları için, IP adresi verilen internet kullanıcılarını belirleyebilmektedir. Aynı durum HTTP[1] sunucu üzerinde bir kayıt defteri (*logbook*) tutan internet servis sağlayıcıları için de geçerlidir. Bu nedenle, IP adresleri belirlenebilir bir kişiye ilişkin veriler olarak değerlendirilmektedir.

---

[1] Hyper Text Transfer Protocol, http://tr.wikipedia.org/wiki/HTTP

IP adreslerinin kişisel veri olup olmadığı konusunda bazı AB üyesi ülke uygulamalarının incelendiği bir çalışmada, araştırmaya konu ülkelerin genelinde veri koruma otoriteleri ve mahkemeler tarafından IP adreslerinin kişisel veri olarak değerlendirildiği belirtilmektedir. Araştırmaya göre, Avusturya, Belçika, İspanya, Almanya ve İsveç IP adreslerinin kişisel veri olarak görüldüğü ülkelerdir. Fransa'da ise veri koruma otoritesi CNIL, IP adreslerini kişisel veri olarak yorumlarken konu hakkında çelişkili mahkeme kararlarına da rastlanmaktadır. Diğer yandan, Fransız Anayasa Konseyinin 2009 yılında aldığı kararın yanı sıra Fransız Senatosu'nun IP adreslerinin açık bir şekilde kişisel veri olduğunu belirtecek yasal düzenlemelerin yapılmasına ilişkin hazırladığı rapor, IP adreslerinin Fransa'da kişisel veri olarak kabul edileceğini ortaya koyan gelişmelerdir (EC, 2009).

Veri Koruma Direktifinde yer alan kişisel veri tanımı gerçek kişilere hasredilse de AAD'nin "Direktif hükümlerinin kapsamının üye ülkelerin ulusal mevzuatlarında genişletilebileceği" görüşü doğrultusunda örneğin İtalya, Avusturya ve Lüksemburg gibi ülkelerde verilerin işlenmesine ilişkin hükümlerin tüzel kişileri de kapsamakta olduğu VKÇG'nin 2007/4 sayılı görüş dokümanında ifade edilmektedir. Ülkemizde de KVKKT'de kişisel veri tanımının tüzel kişileri kapsayacak şekilde ele alındığı görülmektedir.

Veri Koruma Direktifi normal veri ile özel nitelikteki veri arasında ayrıma giderek kişilerin ırki ya da etnik kökenleri, siyasî düşünceleri, dini ya da felsefî inançları, sendika üyelikleri, sağlık yaşamları ve cinsel eğilimleri ile ilgili kişisel verilerin işlenmesini ilgili kişinin açık rızası veya veri işleme için yasal dayanak olmadıkça engellemektedir. Kişinin özel hayatına daha derin müdahale anlamına geldiğinden hassas verilerin işlenmesi daha katı kurallara bağlanmakta, kişiye sonraki bir aşamada veri işlemenin durdurulması imkânının sağlanması, açık rıza şartını yerine getirmemektedir (Chatziliassi, 2009).

İsveç'te bir kilisenin aktif üyesi olan Lindqvist kişisel bir internet sayfası oluşturmuş, sayfada kendisi ve 18 kilise gönüllüsü arkadaşı hakkında ad, telefon numarası, meslek ve hobi gibi çeşitli bilgiler yayımlamıştır. Lindqvist aynı sayfada bir arkadaşının ayağının sakatlandığı ve tıbbi gerekçelerle yarı zamanlı çalıştığı bilgisine de yer vermiştir. Lindqvist, İsveç Veri Koruma Kurumu'nun bilgilendirilmediği, bireylerin kişisel verilerinin yeterli veri koruma düzeyi olmayan ülkelere aktarılmasına olanak sağlandığı ve bireylerin hassas verilerinin rızaları olmadan işlendiği gerekçeleriyle 4000 İsveç Kronu para cezası almıştır. Lindqvist, Kararı İsveç Temyiz Mahkemesine götürmüş; Mahkeme de AAD'den, davalının aktivitelerinin Veri Koruma Direktifine aykırılık teşkil edip etmediğine ilişkin görüş talep etmiştir. AAD,

> *Bir internet sayfasında çeşitli kişilere atıfta bulunulması ve kişilerin adlarıyla veya başka vasıtalarla kimliklerinin belirlenmesinin, Veri Koruma Direktifi kapsamında kişisel verilerin tamamen veya kısmen otomatik vasıtalarla işlenmesi fiilini oluşturduğuna*

hükmetmiş ayrıca internet sayfasında sakatlık ya da tıbbi gerekçelerle yarı zamanlı çalışma gibi sağlıkla ilgili bilgilere atıfta bulunulmasının hassas veriler hakkındaki hükümlerin de ihlali anlamına geldiğini beyan etmiştir (OUT-LAW, 2003).

3.1.2 Trafik verileri

AB mevzuatında trafik verisi ilk olarak ISDN Direktifinde çağrıların kurulumu için işlenen veriler olarak kullanılmış ancak cep telefonları ve internetin hızlı gelişimiyle birlikte anılan Direktifin yenilenme ihtiyacı ortaya çıkmıştır. Bu çerçevede, ISDN Direktifini yürürlükten kaldıran E-Gizlilik Direktifi trafik verisi için sadece telefona bağımlı olmayan bir tanım getirmiştir (FISCHER, 2010). Buna göre trafik verisi, "*Bir elektronik haberleşme şebekesinde haberleşmenin iletimi veya bu haberleşmenin faturalandırılması amacıyla işlenen veri*" olarak tanımlanmaktadır (E-Gizlilik Direktifi, md. 2/b).

Trafik verisi, bir haberleşmenin zamanı, süresi, boyutu, yönlendirilmesi; kullanılan protokol; gönderici ve alıcının terminal cihazının konumu; haberleşmenin başladığı ve sonlandığı şebeke; bir bağlantının başlangıcı, bitişi, süresi ve ayrıca bir şebeke tarafından haberleşmenin iletildiği format hakkında bilgiler içerebilmektedir (E-Gizlilik Direktifi, dibace 15).

Abone ve kullanıcılara ilişkin trafik verileri bir haberleşmenin iletimi için gerekli olmadıkları takdirde silinmeli ya da anonim hale getirilmelidir (E-gizlilik Direktifi, md. 6/1). Haberleşme iletiminin tamamlandığı ve trafik verisinin -işlenmesine izin verildiği haller dışında- silinmesi gereken zaman dilimi, sağlanan hizmet türüne bağlı olmaktadır. Örneğin bir telefon görüşmesi için iletim, kullanıcılardan birinin bağlantıyı sonlandırmasıyla tamamlanırken e-posta için iletim, alıcı kişilerin hizmet sağlayıcının sunucusundan mesajları almasıyla sonlanmaktadır (E-Gizlilik Direktifi, dibace 27).

3.1.3 Konum verileri

Konum verileri E-Gizlilik Direktifinde, "*Kamuya açık bir elektronik haberleşme hizmeti kullanıcısına ait bir terminal cihazının coğrafi konumunu belirleyen ve elektronik haberleşme şebekesinde işlenen her türlü veri*" olarak tanımlanmış, Vatandaş Hakları Direktifinde ise tanım, "*elektronik haberleşme hizmeti aracılığıyla*" işlenen verileri de kapsayacak şekilde genişletilmiştir. Kullanıcı terminal cihazının enlem, boylam ve yükseklik değeri, konum bilgisinin hassasiyet düzeyi, kullanıcının hareket yönü, belirli bir zamanda terminal cihazının konumlandırıldığı şebeke hücresinin kimliği, konum bilgisinin kaydedildiği zaman gibi bilgiler konum verileri olarak değerlendirilebilmektedir (E-Gizlilik Direktifi, dibace 14).

Mobil şebekelerde haberleşmenin iletiminin sağlanması amacıyla işlenen ve mobil kullanıcının terminal cihazının coğrafi konumunu gösteren veriler, trafik verisi kapsamına dâhil edilirken haberleşmenin iletimi için gerekli olandan

daha fazla hassasiyet sağlayan veriler konum verisi olarak değerlendirilmektedir (E-Gizlilik Direktifi, dibace 35).

Örneğin, mobil haberleşmenin faturalandırmasında kullanılan çağrı detay kayıtlarında (CDR) hücre kimliği (*cell ID*) bilgisi yer almaktadır. Burada hücre kimliği bilgisi, çağrının kurulması ve dolayısıyla haberleşmenin sağlanması için gerekli bir veri olduğundan trafik verisi niteliğindedir. Diğer taraftan, çeşitli konum belirleme yöntemleri[2] kullanılarak daha hassas konum verisi değerleri elde edilmesi halinde, söz konusu veriler haberleşmenin iletimi için gerekli olmamakla birlikte trafik yol desteği, çocuk takibi, acil sağlık, filo takibi, çalıntı araç izleme gibi birçok katma değerli servis[3] sunumunda kullanılabilmektedir (FISCHER, 2010). Bu bağlamda, trafik verisi özelliği taşımayan konum verileri E-Gizlilik Direktifinin 9 uncu maddesinde, trafik verisi niteliğindeki konum verileri ise E-Gizlilik Direktifinin 6 ncı maddesinde düzenlenmiştir.

3.1.4 Veri türleri arasındaki ilişki

AB mevzuatında kişisel veri tanımının yer aldığı Veri Koruma Direktifi yanında elektronik haberleşme sektörüne özel Direktif hazırlanması ve trafik/konum verileri gibi veri türlerinin tanımlanmasının altında bu verilerin gizlilik karşısında belirli bir risk barındırmaları yatmaktadır. Bu nedenle, anonim hale getirme ve rıza alma gibi önlemleri teşvik etmek ve gizliliğin korunmasını sağlamak için trafik ve konum verilerinde ekstra koruma gerekli görülmektedir (Rannenberg vd., 2009).

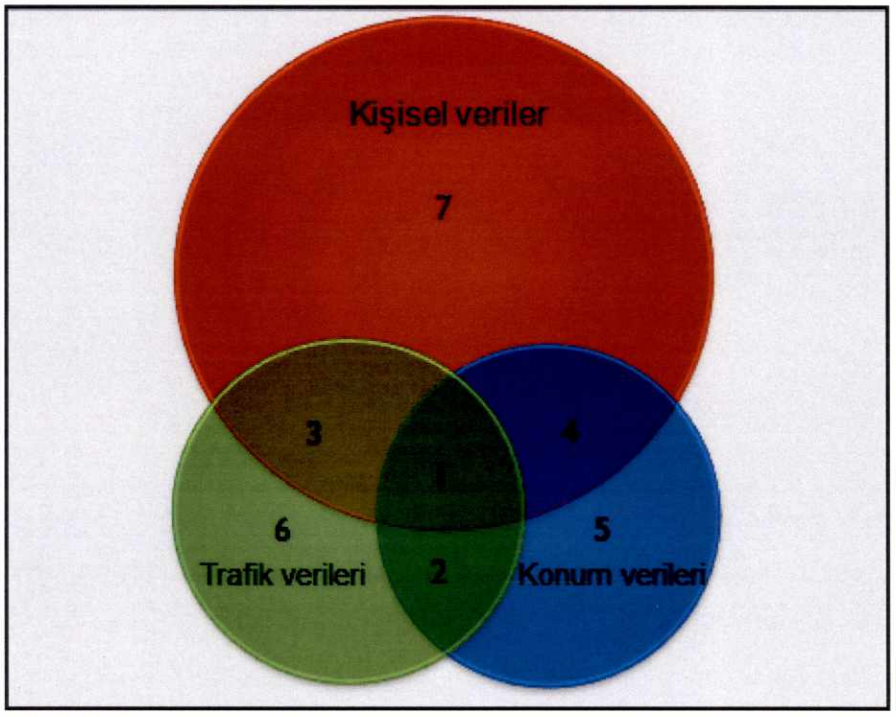
VKÇG (2005)'ye göre konum verileri belirli ya da kimliği belirlenebilir gerçek kişilerle ilişkilendirilebildiğinden Veri Koruma Direktifinde yer alan hükümlere tabi olmalıdır. Ancak bu tanımın geniş olduğu ve kişisel veri olarak değerlendirilmeyecek konum verilerinin bulunduğuna ilişkin görüşler de

---

[2] http://www.ericsson.com/ericsson/corpinfo/publications/review/1999_04/files/19990406.pdf
[3] http://www.basari.com.tr/btelekom/urunler/cepyerbelirleme/basari_trueposition.pdf (s.12).

mevcuttur (FIDIS, 2007). Bu görüşe göre, AB Direktiflerinde yer alan veri türleri arasındaki ilişki aşağıdaki şekilde sınıflandırılmaktadır (Şekil 3.1):

Şekil 3.1. Veri türleri arasındaki ilişki



Kaynak: 2007, FIDIS

1) Kişisel veri ve trafik verisi olarak değerlendirilen konum verisi (bir cep telefonu çağrısının başlatıldığı veya sonlandırıldığı hücrenin kimlik numarası),
2) Kişisel veri olmayan trafik ve konum verisi (çağrı yapılabilen bir telefon kulübesinin konum bilgisi),
3) Konum verisi olmayan kişisel veri ve trafik verisi (bir cep telefonu abonesi tarafından yapılan çağrının tarih ve saati),
4) Trafik verisi olmayan kişisel veri ve konum verisi (bir kişinin sabit telefon adresi),
5) Trafik verisi veya kişisel veri olmayan konum verisi (gerçek sürücü adı kaydedilmeyen bir şirket arabasının GPS konumu),

6) Konum verisi veya kişisel veri olmayan trafik verisi (bir internet kullanıcısının anonim internet servisleri kullanarak bir şirketin internet sayfasına eriştiği tarih ve saat),
7) Trafik veya konum verisi olmayan kişisel veri (bir kişinin sosyal güvenlik numarası).

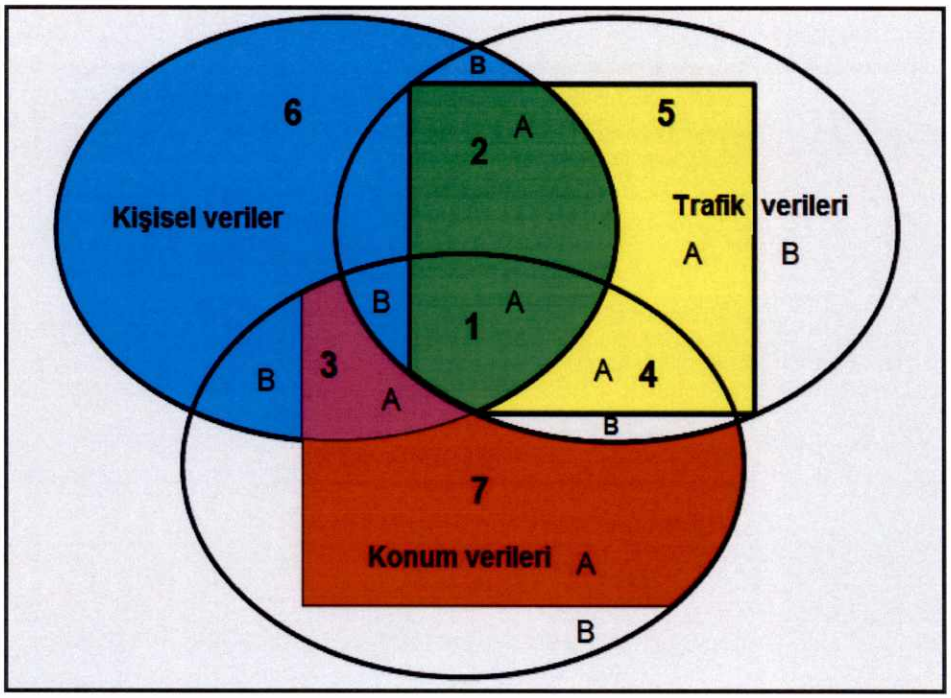
Trafik ve konum verilerinde genel olarak E-Gizlilik Direktifi, Veri Koruma Direktifine göre önceliğe sahiptir. Ancak E-Gizlilik Direktifinde yer almayan hükümler karşısında trafik ve konum verilerinin korunmasında Veri Koruma Direktifi tamamlayıcı rol üstlenmektedir. Bu kapsamda, kamuya açık haberleşmede E-Gizlilik Direktifinin 5 ve 6 ncı maddeleri trafik verilerine, 9 uncu maddesi ise konum verilerine uygulanmaktadır. Trafik ve konum verilerinin özel şebeke veya servisler aracılığıyla üretilmesi ve söz konusu verilerin kişilerle ilişkilendirilebilmesi durumunda ise Veri Koruma Direktifi göz önüne alınmaktadır (FIDIS, 2007).

Hangi Direktifin hangi tür verilere uygulanacağını gösteren Şekil 3.2'de,

- Mavili alan Veri Koruma Direktifinin,
- Sarılı alan E-Gizlilik Direktifinin 5 ve 6 ncı maddelerinin,
- Kırmızılı alan E-Gizlilik Direktifinin 9 uncu maddesinin,
- Mor ve yeşil alanlar ise bazı veri türleri için her iki Direktifin

uygulama alanını ifade etmektedir. Ayrıca elektronik haberleşme şebekeleri veya hizmetleri aracılığıyla üretilen veriler için "A" sembolü kullanılırken "B" sembolü, özel şebekelerde üretilen veya E-Gizlilik Direktifi dışında kalan verileri belirtmektedir.

Şekil 3.2. AB Direktiflerinin veri türlerine uygulanması



Kaynak: FIDIS, 2007

Bu kapsamda örneğin,

- 1A bölgesinde, elektronik haberleşme şebekeleri veya hizmetleri aracılığıyla üretilen veriler için E-Gizlilik Direktifinin 5 ve 6 ncı maddeleri ile Veri Koruma Direktifinin veri güvenliği maddesi,
- 1B bölgesinde özel şebeke veya servisler aracılığıyla üretilen veriler için sadece Veri Koruma Direktifinin ilgili maddeleri,
- 7A bölgesinde E-Gizlilik Direktifinin 9 uncu maddesi

uygulanacak ancak 7B bölgesindeki veriler herhangi bir mevzuat kapsamına dahil olmayacaktır (FIDIS, 2007).

3.1.5 Kişisel verilerin istek dışı haberleşme amacıyla kullanılması

Günümüz haberleşme teknolojileri zaman ve mekândan bağımsız olarak düşük maliyetlerle iletişimi kolaylaştırmıştır. Haberleşme teknolojileri birçok şirket tarafından doğrudan pazarlama amacıyla kullanıldığında ise kişiler rahatsız edilmekte ve kendileriyle bu tür haberleşmenin yapılmasından kaçınmaktadır (Fina, 2009).

Son yıllarda özellikle mobil iletişim ve internet alanında yaşanan gelişmelerle birlikte doğrudan pazarlama amacıyla yapılan haberleşme de artış göstermiştir. Elektronik haberleşme sektörü ile farklı sektörlerde faaliyette bulunan işletmeler, ürün ve servislerini pazarlamak amacıyla telefon, e-posta, faks, SMS gibi haberleşme vasıtalarını kullanarak bireylere ulaşmaktadır. Bu noktada, telefon numaraları ve e-posta adresi gibi iletişim bilgilerine ihtiyaç duyulduğundan söz konusu kişisel verilerin hukuka ve dürüstlük kurallarına uygun işlenmesi, bireylerin bilgisi ve rızası olmadan üçüncü taraflara aktarılmaması ve pazarlama amacıyla kullanılmaması gerekmektedir.

İtalya'da 2009 yılında kamuya açık abone rehberlerinde yer alan iletişim bilgilerinin kullanılması suretiyle tele pazarlama amaçlı veritabanları oluşturulabileceği düzenlenmiştir. AK abonelerin, kişisel verilerinin rehberlerden veritabanlarına aktarılması konusunda bilgilendirilmedikleri gibi bu verilerin pazarlama amacıyla veritabanlarında bulunmasına rıza vermediklerini belirterek düzenlemeyle E-Gizlilik Direktifinde yer alan *"Üye devletler abonelerin kişisel verilerinin yer alabileceği basılı veya elektronik abone rehberlerinin amaçları ve bu rehberlerin elektronik sürümlerindeki arama fonksiyonlarına bağlı ilave kullanım imkânları hakkında rehbere kaydedilmeden önce ve ücretsiz olarak abonelerin bilgilendirilmelerini sağlayacaklardır"* ve *"abonelerin rızası olmadan istek dışı haberleşme yapılamaz"* hükümlerinin ihlal edildiğini üye ülkeye bildirmiştir (EU, 2010c).

İtalya, numaraları abone rehberlerinde yer alan vatandaşların doğrudan pazarlama amacıyla yapılan istek dışı telefon çağrısı almamaları için opt-out sisteminin uygulanması konusunda işletmecilere yükümlülükler getirerek E-Gizlilik Direktifine uyum sağlamıştır. Bu çerçevede, tele pazarlama amaçlı çağrıları almak istemeyen abonelerin listelerinin yer aldığı bir kayıt bürosu kurulmuştur (EU, 2011).

3.1.5.1 Doğrudan pazarlama

Tüketiciler için daima baş ağrısı olarak görülen doğrudan pazarlama Avrupa Konseyinde ilk olarak 1985 yılında gündeme gelmiş ve "toplum bireylerine posta, telefon ya da diğer araçlarla ürün ve hizmetlerin sunulması veya herhangi bir mesajın iletilmesine imkân tanıyan tüm faaliyetler" olarak tanımlanmıştır. 1990'lı yılların başında internetin gelişmesiyle birlikte genelde spam olarak adlandırılan istenmeyen e-postalar ortaya çıkmış, sonrasında ise faks, SMS ve MMS gibi elektronik haberleşme araçlarıyla istek dışı haberleşme yaygınlaşmıştır. Bunun sonucunda istek dışı haberleşme E-Gizlilik Direktifinin 13 üncü maddesiyle düzenlenmiştir (Kosta vd, 2009).

VKÇG (2004)'ye göre Direktiflerde doğrudan pazarlama tanımı olmamakla birlikte FEDMA tarafından *"Herhangi bir reklam veya pazarlama aracıyla pazarlamacının bizzat kendisi ya da adına iş yapan temsilcisi tarafından belirli bireylere yönelik olarak yapılan haberleşme"* şeklinde yapılan tanım uygun görülmektedir. Ayrıca siyasi kuruluşlar veya yardım kuruluşları tarafından yapılan bağış toplama kampanyaları da doğrudan pazarlamaya dâhil olarak kabul edilmiştir.

Doğrudan pazarlamanın karakteristiği, televizyon, radyo, gazete ve dergi gibi kitle iletişim araçları kullanılmadan potansiyel alıcılarla doğrudan iletişim kurulabilmesidir. Kitle iletişim araçlarıyla yapılan reklamcılık, pahalı olması yanında mesajların hedef kitleye kesin olarak ulaştırılması yönünde bir garanti sağlamazken doğrudan pazarlama reklamcılara, hedef gruptaki

alıcıların seçilmesi ve bu kişilerle doğrudan temas kurulması imkânı tanımaktadır. Doğrudan pazarlama faaliyetlerinde kişilerle doğrudan iletişim sağlanabilecek telefon, faks, e-posta, SMS veya geleneksel posta gibi herhangi bir haberleşme teknolojisi kullanılabilmektedir (Fina, 2009).

3.1.5.2 Opt-in ve opt-out

İstek dışı haberleşmeyle ilgili olarak Avrupa'da düzenleyici otorite, sorunun öz düzenlemeyle çözüme kavuşturulmasına imkân tanımamış ve konuya müdahale etme gereği duymuştur. Bu çerçevede opt-in ve opt-out gibi iki sistemden bahsedilebilir. Opt-in sistemi, alıcının rızasının alınmadığı durumlarda doğrudan pazarlama amaçlı haberleşmenin engellenmesini gerektirirken opt-out sisteminde gönderici, alıcının önceden onayını almasa dahi alıcı istek dışı haberleşme yapılmasına itiraz etmediği sürece doğrudan pazarlama amacıyla haberleşme teknolojilerini kullanabilir (Fina, 2009).

Abonelik sözleşmelerinde yer alan genel hüküm ve koşulların kabul edilmesi, doğrudan pazarlama amaçlı haberleşme yapabilmek amacıyla abonelerden onay alınmış olduğunu göstermemektedir. Veri Koruma Direktifine uygun olması durumunda onay, bir kutucuğu işaretlemek suretiyle verilebilir (VKÇG, 2004).

Opt-out sistemini de kendi içinde ikiye ayırmak mümkündür. Bireysel opt-out sisteminde alıcı kendisiyle yapılan her bir haberleşmeyi reddetmek ve dolayısıyla haberleşmeyi yapan bütün taraflara bundan sonrası için bu tür haberleşmeyi istemediğini bildirmek durumundadır. Bu nedenle, bireysel opt-out sisteminin kişiler için zaman alıcı olduğu ve kullanıcı dostu olmadığı görülmektedir. Opt-out kayıt kütüğü sisteminde ise alıcı, iletişim bilgilerini bir kez kütüğe kaydettirmek suretiyle bu tür haberleşmeyi almak istemediğini belirtmekte, doğrudan pazarlama amaçlı haberleşme yapmak isteyen taraflara düzenli olarak bu kütüğü kontrol etme yükümlülüğü getirilmektedir (Fina, 2009).

Elektronik ileti (e-posta, SMS, MMS vb.) aracılığıyla yapılacak doğrudan pazarlama amaçlı haberleşmede, iletişim bilgilerinin bir ürünün satılması sırasında elde edilmesi halinde "soft opt-in" adı verilen bir yöntem kullanılabilmektedir. Bu yöntemde, şirket ile tüketici arasında müşteri ilişkisi bulunması halinde şirketler müşterilerinden aldıkları iletişim bilgilerini benzer ürün ve hizmetlerin pazarlamasında kullanabilir. Ancak verilerin ilk kez elde edilmesi aşamasında şirketler, bu verilerin doğrudan pazarlama amaçlı haberleşmede kullanılabileceğini açıkça belirtmeli, müşterilere bu tür haberleşmeyi reddetme seçeneği sunmalıdır. Ayrıca müteakip iletilerin her biri için de opt-out seçeneği sunulmalıdır (EU, 2004).

3.1.5.3 Robinson listeleri

1970'li yıllarda ABD'de doğrudan pazarlama alanında tüketicilerin belirli türdeki pazarlama gereçlerini engellemek isteyebilecekleri düşüncesiyle tüketicilere, tercihlerine bağlı olarak opt-out seçeneği sunma fikri ortaya çıkmıştır. Bu çerçevede oluşturulan listeler, tercihe bağlı servis (*preference service*) adıyla anılmış; diğer ülkelerde ise Daniel Defoe'nun romanında ana karakter olan ve ıssız bir adaya düşen Robinson Crusoe'un komşularıyla iletişim kurmak istememesine atfen Robinson listesi olarak kabul görmüştür. Birçok ülkede doğrudan pazarlama federasyonu tarafından kurulan listelere kayıt olmak için tüketiciler genellikle yazılı ve ücretsiz olarak başvuru yapmaktadır. Diğer yandan, çevrimiçi kayıt imkânının sağlandığı listelerin sayısı da gittikçe artmaktadır. Bazı listeler için kaydın geçerliliği süreklilik arz ederken bazı listelerde 2-3 yılda bir kayıt yenileme gerekmektedir (Tempest, 2007).

Robinson listeleri maliyetleri kimin üstleneceği, listelerin ne zaman ve hangi sıklıkta kontrol edileceği hususlarındaki belirsizlikler nedeniyle eleştirilmekte, ayrıca yasal düzenlemeleri dikkate almayan tarafların, bu listeleri yeni e-posta adresi elde etme aracı olarak kullanabilecekleri belirtilmektedir (Mosing, 2007).

Posta, telefon, faks, e-posta, SMS ve mobil telefon gibi haberleşme vasıtalarına yönelik olarak uygulanabilen Robinson listeleri ülkeden ülkeye değişiklik göstermektedir (Tablo 3.1).

Tablo 3.1. Robinson listeleri

Ülke	Posta	Telefon	Faks	E-posta	SMS/Mobil Telefon
Avustralya	✓	✓		✓	✓
Avusturya	✓		✓		
Belçika	✓	✓		✓	✓
Kanada	✓	✓	✓		
Çek Cumhuriyeti	✓	✓			
Danimarka	✓				
Finlandiya	✓	✓			
Fransa	✓	✓		✓	
Almanya	✓	✓	✓	✓	✓
Yunanistan	✓	✓	✓	✓	✓
Macaristan					
İrlanda	✓	✓	✓		✓
İtalya	✓	✓	✓	✓	✓
Hollanda	✓	✓		✓	✓
Yeni Zelanda	✓	✓	✓		
Norveç	✓	✓			
Polonya	✓				
Portekiz	✓				
Romanya					
Rusya					
Slovakya	✓				
Slovenya	✓				

Tablo 3.1. (Devamı) Robinson listeleri

Ülke	Posta	Telefon	Faks	E-posta	SMS/Mobil Telefon
İspanya	✓				
İsveç	✓	✓		✓	
İsviçre	✓	✓			
İngiltere	✓	✓	✓	✓	
ABD	✓	✓		✓	

Kaynak: Tempest, 2007

Robinson listelerinin önemi, AB'de ulusal veri koruma otoriteleri tarafından kabul edilmektedir. Nitekim AB Direktiflerinde doğrudan pazarlama amaçlı faks haberleşmesi opt-in sistemini gerektirmesine rağmen bazı ülkelerde opt-out listeleri zorunlu kılınmıştır. Ancak ulusal mevzuatlarda yer alan bu farklılıklar Pan-Avrupa Robinson listelerinin oluşmamasının nedenlerinden biri olarak gösterilmektedir (Tempest, 2007).

Ülkemizde veri koruma kanununun olmaması, olası bir Robinson listesi uygulamasının önündeki en büyük engeldir. Sektörel bazda elektronik haberleşme alanında yapılacak bir düzenlemede ise bazı Avrupa ülkelerinde olduğu gibi bütün listelerin tek bir veritabanında yer alması yanında sistemin merkezi olması ve sorgulama esaslı çalışması daha uygun olacaktır. Bu durumda, tüketicilerle pazarlama amaçlı haberleşme yapmak isteyen telekomünikasyon şirketleri sadece kendilerinde iletişim bilgileri bulunan tüketicilere ilişkin olarak merkezi veritabanında sorgulama yapabilecek ve diğer şirketlerde bulunan tüketici iletişim bilgilerine erişim engellenmiş olacaktır.

3.1.5.4 AB mevzuatında istek dışı haberleşme

Veri Koruma Direktifi, elektronik haberleşme alanına özgü hükümler içermemektedir. Ancak Direktifin kişisel verilerin işlenmesiyle ilgili hükümleri

istek dışı haberleşmede göz önünde bulundurulmalıdır. Örneğin, kişisel veri olarak kabul edilen e-posta adreslerinin haber grupları, sohbet odaları, internet sayfaları gibi vasıtalarla dürüstlük kuralına uygun olmayan yöntemlerle elde edilmesi Direktife aykırılık teşkil etmekte, benzer şekilde rıza alınırken önceden işaretlenmiş kutucukların kullanılması Direktifin şeffaflık ve dürüstlükle ilgili gereksinimlerini karşılamamaktadır (Lugaresi, 2004).

İstek dışı haberleşmeyle ilgili düzenleme adımına ilk olarak 97/7/EC sayılı Direktifte[4] rastlanılmaktadır. Otomatik arama sistemleri ve faks makineleri aracılığıyla yapılacak haberleşme için önceden rıza şartı getirilirken e-posta gibi uzaktan haberleşme vasıtalarının tüketici tarafından açıkça reddedilmediği sürece kullanılabileceği belirtilmiş ve dolaylı olarak opt-out sistemi öngörülmüştür. ISDN Direktifi de 97/7/EC sayılı Direktife benzer hükümler getirirken 2000/31/EC sayılı Direktif[5], elektronik ileti vasıtasıyla ticari haberleşme yapan hizmet sağlayıcılara opt-out kayıt kütüklerini düzenli olarak kontrol etme yükümlülüğü getirmiştir. 2002/58/EC sayılı Direktifte ise e-posta için de opt-in yöntemi belirlenmiş; böylece bireylerin menfaati, opt-in sisteminin e-ticaretin gelişmesini engelleyeceği kaygısının önüne geçmiştir (Lugaresi, 2004).

Mosing (2007)'e göre E-Gizlilik Direktifinin en büyük başarısı istek dışı haberleşmeyle ilgili düzenlemelerde AB çapında homojenlik sağlamış olması ve teknolojik tarafsız ele alınarak Direktifin gelecekte istek dışı haberleşmede kullanılabilecek vasıtalara uygulanabilir olmasına zemin hazırlamasıdır. İstek dışı haberleşmeye ilişkin olarak E-Gizlilik Direktifinde yer alan hükümler aşağıda belirtilmektedir.

---

[4] Directive on the Protection of Consumers in Respect of Distance Contracts (Mesafeli Sözleşmelere İlişkin Olarak Tüketicinin Korunması Hakkında Direktif).
[5] Directive on electronic commerce (Elektronik Ticaret Direktifi).

E-Gizlilik Direktifi kapsamında, kişi müdahalesi olmadan çalışan otomatik arama makineleri, faks makineleri ve elektronik iletilerin (SMS, MMS, sesli mesaj, e-posta vb.) doğrudan pazarlama amacıyla kullanılması abone veya kullanıcıların önceden rıza vermesi halinde mümkündür (E-Gizlilik Direktifi, md. 13/1). Ancak tüketicilerin elektronik iletişim bilgilerinin bir ürünün ya da bir hizmetin satılması sırasında Veri Koruma Direktifine uygun olarak elde edilmesi halinde, bu bilgiler benzer ürün ya da hizmetlerin pazarlanmasında kullanılabilir. İletişim bilgilerinin elde edilmesi esnasında tüketicilere bu tür bilgilerin doğrudan pazarlama amacıyla kullanılacağı açık biçimde belirtilir ve bu tür iletileri reddetme hakkı sağlanır. Tüketici, iletişim bilgilerinin pazarlama amacıyla kullanılmasına izin verse bile bundan sonra pazarlama amaçlı iletileri engelleme imkânı tüketiciye sağlanır (E-Gizlilik Direktifi, md. 13/2). Bu hüküm kapsamında sadece veriyi toplayan gerçek veya tüzel kişi pazarlama amacıyla elektronik ileti gönderebildiği için örneğin bir şirketin bağlı olduğu ana şirket ya da sahip olduğu bağlı ortaklıklar bu veriyi pazarlama amacıyla kullanamayacaktır (VKÇG, 2004).

13 üncü maddenin birinci ve ikinci fıkrasında belirtilen haller dışında, opt-in veya opt-out sistemi kullanılmadan doğrudan pazarlama amacıyla istek dışı haberleşme yapılmasına izin verilmemelidir (E-Gizlilik Direktifi, md. 13/3). Bu çerçevede, örneğin otomatik arama makineleri dışında sabit ve mobil ses hizmeti kullanılarak yapılacak pazarlama faaliyetleri için üye ülkeler iki sistemden herhangi birisini tercih edebilir (VKÇG, 2004).

Diğer taraftan, alıcının talebini iletebileceği geçerli bir adres bilgisi bulunmayan veya göndericinin kimlik bilgisi yer almayan elektronik iletilerin doğrudan pazarlama amacıyla gönderilmesi engellenmelidir (E-Gizlilik Direktifi, md. 13/4). İngiltere'de ICO tarafından uygun görülen pazarlama mesajı örneği Şekil 3.3'te yer almaktadır. Buna göre, pazarlama amaçlı SMS'lerde gönderici kimliği, varsa iletişim bilgileri ve pazarlama mesajlarından çıkış seçeneği gibi hususlar bulunmalıdır (ICO, 2011).

Şekil 3.3. Pazarlama amaçlı SMS örneği 1

Kaynak: ICO, 2011

ICO tarafından uygun görülmeyen pazarlama mesajı örneği ise Şekil 3.4'te gösterilmektedir. Ad/iletişim bilgileri ve opt-out seçeneği bulunmayan mesaj, gizli ücretlendirme de içermektedir.

Şekil 3.4. Pazarlama amaçlı SMS örneği 2

Kaynak: ICO, 2011

3.1.5.5 İstek dışı haberleşme araçları

Doğrudan pazarlama amacıyla yapılan istek dışı haberleşmede genel olarak aşağıdaki vasıtalar kullanılabilmektedir.

3.1.5.5.1 Otomatik arama sistemleri

Otomatik arama sistemleri, ICO (2007) tarafından "*kayıtlı komutlar sayesinde birden fazla noktaya otomatik olarak çağrı başlatabilen ve canlı olmayan sesleri iletebilen sistemler*" olarak tanımlanmakta; canlı telefon aramaları, SMS, MMS, e-posta ve faks yoluyla yapılan haberleşme ise otomatik arama olarak değerlendirilmemektedir.

3.1.5.5.2 Faks makineleri

Faks aracılığıyla yapılan istek dışı haberleşme tüketiciler için rahatsız edici (gece yarısı telefonun çalması) ve maliyetli (kâğıt ve kartuş harcanması) olduğundan birçok ülkede yasalarla düzenlenmesi gerekli görülmüştür. ABD'de faks hizmeti sunan bir şirkete 1991 yılında çıkarılan kanuna aykırı hareket ettiği gerekçesiyle 5.379.000 Amerikan Doları para cezası verilmiştir. Federal Haberleşme Komisyonu[6] konuya ilişkin olarak şirketin,

- Tüketicilere istek dışı mesajlar gönderdiğini,
- Tüketicilerle belirli bir iş ilişkisi bulunmadığını,
- Gönderilecek mesajlar için tüketicilerden rıza alınmadığını

belirtmiştir. Benzer şekilde İngiltere'de faks aracılığıyla pazarlama faaliyetinde bulunan iki şirket, düzenlemelere aykırı davrandıkları gerekçesiyle ICO tarafından uyarılmıştır (Eisenhauer, 2008).

---

[6] Federal Communications Commission

3.1.5.5.3 Telefon

E-Gizlilik Direktifinde otomatik arama makineleri, fakslar ve elektronik iletiler dışında kişiden kişiye telefon aramaları gibi doğrudan pazarlama amacıyla kullanılacak yöntemler için opt-in veya opt-out sisteminin uygulanabileceği belirtilmektedir (E-Gizlilik Direktifi, dibace 42). Tele pazarlama faaliyetlerinde kullanılan telefon aramaları tüketicilerin özel hayatlarına müdahale anlamına geldiğinden bu tür aramalar için çeşitli düzenlemeler yapılmaktadır. Örneğin, İngiltere'de tele pazarlama aramalarını almak istemeyen tüketiciler için telefon tercih servisi (*telephone preference service*) bulunmaktadır. Opt-out yöntemiyle çalışan servis sayesinde, sisteme kaydolan tüketicilere tele pazarlama aramaları yapılamamaktadır.

Hong Kong'da bir uluslararası arama servisinin reklamını yapan bir telekomünikasyon şirketinin tele pazarlama aramaları hakkında Veri Gizliliği Koruma Komiserliğine şikâyet başvurusunda bulunan bir tüketici, aramaların engellenmesi talebine rağmen şirketin bu tür aramalara devam ettiğini bildirmiş, Kişisel Verilerin Gizliliği Yönetmeliğine aykırı hareket edildiği gerekçesiyle şirkete para cezası verilmiştir.

Hindistan'da ise cep telefonu operatörü Airtel şirketi hakkında, mobil telefon kullanıcılarına tele pazarlama aramaları yaptığı, istek dışı mesajlar gönderdiği ve kullanıcıların uluslararası dolaşım ücretleri nedeniyle bu mesajların maliyetlerine katlanmak zorunda kaldıkları gerekçesiyle Hindistan Tüketici Mahkemesine yapılan başvuruda Mahkeme, yapılan aramalar ve gönderilen mesajların rahatsız edici nitelikte olduklarını göz önünde bulundurarak tüketicilerin gizlilik haklarının ihlal edildiğini belirtmiş ve şirket 170.500 Amerikan Doları para cezasına çarptırılmıştır (Eisenhauer, 2008).

3.1.5.5.4 Elektronik iletiler

SMS, MMS, sesli mesajlar ve telesekreter mesajları, e-posta gibi kanallar da istek dışı haberleşmede kullanılabilmektedir.

Avustralya'da faaliyet gösteren bir pazarlama şirketi cep telefonlarına kısa süreli çağrılar bırakarak kullanıcıların, telefon ekranlarında "cevapsız arama" mesajları görmelerini sağlamaktaydı. Kullanıcılar ekranlarında görünen bu numaraları aradıklarında ise önceden kaydedilmiş pazarlama mesajlarına muhatap kalmaktaydı. Avustralya Medya ve İletişim Kurumu, pazarlama mesajlarının göndericinin kimliğini belirtmemesi ve kullanıcıya opt-out seçeneği sunmaması nedeniyle Spam Kanununa aykırı olduğunu belirtmiş, şirket 132.000 Amerikan Doları para cezası almıştır. Benzer biçimde, 231 milyon adet istek dışı e-posta gönderdiği gerekçesiyle Avustralya Federal Mahkemesi tarafından Mansfield şirketine 900.000 Amerikan Doları para cezası verilmiştir (Eisenhauer, 2008).

İstek dışı haberleşmede son dönemlerde bluespam kavramı tartışılmaktadır. Bluespam, cep telefonları, cep bilgisayarları (*PDA*) ve dizüstü bilgisayarları gibi bluetooth teknolojisini destekleyen cihazlarla istek dışı haberleşme yapılmasıdır. ICO, başlangıçta bluetooth mesajlarının WAP[7] mesajları gibi elektronik ileti olarak değerlendirilmesi gerektiği yönünde görüş beyan etmiş ancak 2007 yılında bu görüşü değiştirerek bluetooth teknolojisinin spamla ilgili düzenlemelere tabi olmadığını ifade etmiştir (Kosta vd., 2010).

VKÇG (2009)'ye göre ise Vatandaş Hakları Direktifi ile tadil edilen E-Gizlilik Direktifinin 13(1) maddesine "haberleşme", Direktifin gerekçe kısmına ise "benzer uygulamalar" ibarelerinin eklenmesi bluetooth yoluyla yapılacak pazarlama faaliyetlerinde de opt-in sistemini gerekli kılmaktadır.

---

[7] http://tr.wikipedia.org/wiki/Kablosuz_uygulama_protokol%C3%BC

3.2 Verilerin İşlenmesi

Veri Koruma Direktifinde "kişisel verileri işleme (işlenme)" tanımı yer alırken E-Gizlilik Direktifinde, trafik veya konum verilerinin işlenmesi şeklinde ayrı bir tanım yer almamakta, "işlenme" tanımı için Veri Koruma Direktifinde yapılan tanımın geçerli olduğu belirtilmektedir. Bu paralelde, E-Gizlilik Direktifinin 6 ncı maddesinde "trafik verilerinin işlenmesi", 9 uncu maddesinde ise "trafik verisi dışındaki konum verilerinin işlenmesi" tabiri kullanılırken, diğer maddelerin genelinde "kişisel verilerin işlenmesi" ifadesi geçmektedir. Verilerin işlenmesini, veri türlerinde olduğu gibi 3 başlıkta incelemek mümkündür.

3.2.1 Kişisel verilerin işlenmesi

Kişisel verilerin işlenmesi Veri Koruma Direktifinde,

> *"Kişisel verilerin otomatik olan veya olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, değiştirilmesi, silinmesi veya yok edilmesi, yeniden düzenlenmesi, açıklanması veya başka bir şekilde elde edilebilir hale getirilmesi, üçüncü kişilere aktarılması, kullanılmasının sınırlanması amacıyla işaretlenmesi veya tasniflenmesi veya kullanılmasının engellenmesi gibi bu veriler üzerinde gerçekleştirilen bir işlem ya da işlemler bütünü"*

şeklinde tanımlanmakta, kişisel verilerin niteliğine ilişkin ise 5 temel ilkeden bahsedilmektedir. KVKKT'de yer alan ve "Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik Taslağı"na da eklenen bu ilkeler aşağıda açıklanmaktadır.

3.2.1.1 Hukuka ve dürüstlük kurallarına uygunluk

Kişisel veriler, hukuka ve dürüstlük kurallarına uygun olarak elde edilmeli ve işlenmelidir. Hukuka uygunluk veri işlemede göz önünde bulundurulması gereken birinci adımdır. Özdemir (2009) dürüstlük kuralı açısından "amaca uygun davranma" ve "aldatılmama" gibi iki önemli unsur bulunduğunu, bu

çerçevede abonelere ait kişisel verilerin işletmeci tarafından toplanması sırasında bu iki unsura dikkat edilmesi gerektiğini aksi halde işletmeci sorumluluğunun söz konusu olacağını belirtmektedir.

Dürüstlük şeffaflık anlamına da geldiğinden ilgili kişinin bilgisi olmadan veri işleme yapılmamalı, işlenen verilerin hangi amaçla ve kim tarafından işlendiği ilgili kişi tarafından bilinmelidir.

3.2.1.2 Amacın belirli olması ve meşruluk

Kişisel veriler önceden belirlenmiş amaçlar için toplanabilir. Örneğin, ürün satışı esnasında müşterisinden cep telefonu bilgisi alan ancak bu bilginin hangi amaçla kullanılacağını belirtmeyen bir internet servis sağlayıcısının abonelere doğrudan pazarlama amacıyla SMS göndermesi amacın belirliliği ilkesine aykırıdır.

Amacın belirliliği, hâlihazırda bilinmeyen veya gelecekte ortaya çıkabilecek amaçları içermemektedir. Amacın değişmesi halinde ise verileri işlenecek kişinin rızasının yeniden alınması gereklidir. Bu çerçevede, kişisel verileri işleyen taraflar rızayı geniş yorumlayarak elde ettikleri verileri başka alanlarda kullanmamalıdır (Özdemir, 2009).
Kişisel verilerin işlenmesini meşru kılan ve Veri Koruma Direktifinde belirtilen ölçütlere göre veri işleme,

- *İşleme faaliyetinin,*
    - *İlgili kişinin taraf olduğu bir sözleşmenin ifası veya sözleşme yapmadan önce ilgili kişinin talepleri,*
    - *Veri kontrolörünün bir yasal yükümlülüğü yerine getirmesi,*
    - *İlgili kişinin meşru çıkarlarının korunması,*
    - *Kamu yararına bir görevin yerine getirilmesi,*
    - *Veri kontrolörünün -ilgili kişinin temel hak ve özgürlüklerine zarar vermediği sürece- kendi haklı çıkarlarının korunması*

için gerekli olması,

- *İlgili kişinin rızasına dayanması*

durumlarından bir ya da birkaçının bulunması halinde meşru sayılacaktır (Küzeci, 2010).

3.2.1.3 Amaca uygunluk, yeterlilik ve orantılılık

Kişisel verileri işleyen taraflar orantılılık ilkesine riayet etmeli, verinin işlendiği her durumda işlemenin amaca uygun olup olmadığını ve işlenen verilerin bu amacın gerçekleştirilmesinde yeterli olup olmadığını incelemelidir (Özdemir, 2009). Özellikle internet ortamında kullanıcıların bilgi taleplerinin karşılanması için üyelik gerektiren sitelerde gereksiz bilgiler toplanabildiği, gizlilik bildirimlerinin eksik olduğu sık karşılaşılan durumlardandır. Bu çerçevede, ICO tarafından yayımlanan mesleki davranış kuralları veri kontrolörlerinin internet sayfası üzerinden kişisel verileri elde ederken göz önünde bulundurmaları gereken hususları belirtmesi açısından önemlidir.

Şekil 3.5'te, veri işleyen tarafın tüketiciden birçok bilgi talebinde bulunduğu ancak bilgilerin hangi amaçla kullanılacağını belirtmediği ve bu nedenle ICO tarafından uygun görülmeyen veri toplama yöntemi gösterilmektedir.

Şekil 3.5. İnternet sayfası üzerinden kişisel veri toplanması 1

Kaynak: ICO, 2010

Şekil 3.6'da ise ICO tarafından uygun görülen veri toplama yöntemi gösterilmekte, gizlilik politikasına ilişkin bilgilendirme yapılmasının tüketici algısında güven unsuru oluşturması açısından önemli olduğu vurgulanmaktadır. Bu kapsamda, Taslak Yönetmeliğin yürürlüğe girmesiyle ülkemizde elektronik haberleşme alanında faaliyet gösteren işletmeciler tarafından tüketicilerle daha kolay iletişim kurulmasında olmazsa olmaz bir gereklilik olarak görülen internet mecrasının kullanımında, kişisel verilerin işlenmesine ilişkin ilkelerin göz önünde bulundurulması gerekecektir.

Şekil 3.6. İnternet sayfası üzerinden kişisel veri toplanması 2

Kaynak: ICO, 2010

3.2.1.4 Doğruluk ve güncellik

Kişisel verilerin doğru olması ve gerektiğinde güncel tutulması gerek verileri işlenen kişi gerekse verileri işleyen taraf açısından önem arz etmektedir. Kişisel verilerin yanlış işlenmesi, kişilerden kaynaklanabileceği gibi teknik nedenlerle de gerçekleşebilir. Bu nedenle, sorumluluğun doğmaması için veri işlemenin her aşamasında verilerin doğru ve güncel olduğunun kontrol edilmesi gerekir (Özdemir, 2009).

Doğruluk ve güncellik ilkesi ile yakın ilişkisi bulunan kişisel verilere erişim hakkı, yanlış işlenen veya güncel olmayan verilerin düzeltilmesinde önemli bir rol oynamaktadır. Bu kapsamda, veri kontrolörleri kişisel verilere erişim ve bu verilerde düzeltme imkânı sağlayan sistemleri oluşturarak kendi sorumluluklarını yerine getirmiş olacaklardır (Küzeci, 2010). Bu tür bir sistemin kurulması, örneğin fatura adresleri değişen tüketicilerin yanlış adrese gönderilen faturalar nedeniyle yaşayabilecekleri olası mağduriyetleri engelleyebilecektir.

3.2.1.5 Kişisel verileri gerektiği kadar muhafaza etme

Kişisel veriler ile verilerin işlenme amacı arasındaki illiyet bağının sona ermesi ve dolayısıyla kişisel verilere gereksinim duyulmadığı durumlarda kişisel verilerin silinmesi veya anonim hale getirilmesi yöntemlerinden biri uygulanmaktadır. Ancak bu yöntemler de veri işleme kapsamında değerlendirildiğinden söz konusu yöntemler uygulanırken veri işleme ilkelerine riayet edilmelidir (Küzeci, 2010).

Elektronik haberleşme sektöründe faaliyet gösteren bir işletmeci, abonelik sözleşmesi devam ettiği sürece haberleşmenin iletilmesi veya faturalandırılması amacıyla abonenin trafik verilerini işleyebilir. Aranan numaraların yer aldığı bu veriler, abonelik sözleşmesi feshedildikten sonra mevzuatın öngördüğü saklama süresinin sonunda silinmeli ya da anonim hale getirilmelidir. Aksi halde bu verilerin pazarlama amaçlı kullanılması ve üçüncü tarafların eline geçmesi riski söz konusu olacaktır. Bu bağlamda, veri işleme faaliyetinin verilerin toplanma aşamasından silinme anına kadar devam eden kapsamlı bir süreç olduğu unutulmamalıdır.

3.2.2 Trafik verilerinin işlenmesi

Kişisel verilerin işlenmesinde hâkim olan ilkelerin, kişisel veri niteliği taşıması durumunda trafik verilerinin işlenmesinde de geçerli olacağı şüphesizdir. E-Gizlilik Direktifinde trafik verilerinin işlenebildiği durumlara ise aşağıda yer verilmektedir:

a) Arabağlantı[8] ödemeleri ve abonelerin faturalandırılması: Trafik verilerinin bu amaçla işlenmesi, yasal olarak faturaya itirazların yapılabileceği

---

[8] 08.09.2009 tarih ve 27343 sayılı Resmi Gazete'de yayımlanan Erişim ve Arabağlantı Yönetmeliğinde arabağlantı, "*bir işletmecinin kullanıcılarının aynı veya farklı bir işletmecinin kullanıcılarıyla irtibatının veya başka bir işletmeci tarafından sunulan hizmetlere erişiminin sağlanmasını teminen, aynı veya farklı bir işletmeci tarafından kullanılan elektronik haberleşme şebekelerinin birbirlerine fiziksel ve mantıksal olarak bağlantısı*" olarak tanımlanmaktadır.

veya ödemelerin takip edilebileceği süre kadar olmalıdır (E-Gizlilik Direktifi, md. 6/2). Nitekim kişisel verilerin korunması ilkelerinin beşincisi, kişisel verilerin işlenme amaçlarının gerektirdiği süreden daha uzun saklanmaması gerektiğini vurgulamaktadır (ICO, 2006).

b) Elektronik haberleşme hizmetlerinin pazarlanması veya katma değerli hizmetlerin sunulması: Verinin ilgili olduğu abone veya kullanıcının rıza vermesi durumunda trafik verileri, elektronik haberleşme hizmetlerinin pazarlanması veya katma değerli hizmetlerin sunulması için gerekli olan kapsam ve sürede işlenebilir. Abone veya kullanıcılara söz konusu verilerin işlenmesi için verdikleri rızayı geri alma imkânı her zaman sağlanmalıdır (E-Gizlilik Direktifi, md. 6/3). İşletmeciler, abone veya kullanıcıları belirtilen amaçlar için işlenecek trafik verilerinin türü ve işlenme süreleri hakkında bilgilendirmelidir. Elektronik haberleşme hizmetlerinin pazarlanması veya katma değerli hizmetlerin sunulması amacıyla yapılacak bu bilgilendirme, abone veya kullanıcıların rızaları alınmadan önce yapılmalıdır (E-Gizlilik Direktifi, md. 6/4).

ICO (2006)'ya göre düzenlemelerde işletmecilerin bu rızayı nasıl alacaklarına dair belirli bir yöntem yer almasa da abone veya kullanıcıların, bu tür verilerin nasıl kullanılacağı ile verilen rızanın muhtemel sonuçları hakkında değerlendirme yapabilmeleri için yeterli biçimde bilgilendirilmeleri, geçerli ve bilgilendirilmeye dayalı bir rıza alınması için gerekli olmaktadır. Bu çerçevede, işletmeciler internet sayfalarında ya da faturalarda örtülü biçimde yer alan bilgilendirmelere güvenemeyecek, katma değerli hizmetlerin temini ve elektronik haberleşme hizmetlerinin pazarlanması için abone veya kullanıcılardan gerekli şartları taşıyan bir rıza alma ihtiyacı duyacaktır.

Katma değerli hizmetler, haberleşmenin iletimi veya faturalandırılması için gerekli olanın ötesinde trafik verisi veya trafik verisi dışındaki konum verisi işlenmesini gerektiren hizmetlerdir (E-Gizlilik Direktifi, md. 2/g). En az maliyetli tarife paketlerine ilişkin öneri, yol rehberi, trafik bilgisi, hava tahmin

raporu, turizm danışma katma değerli hizmetler arasında sayılmaktadır (E-Gizlilik Direktifi, dibace 18). Örneğin, tüketicilere çeşitli tarife ve paket seçenekleri sunan bir mobil telefon işletmecisi abonelerinin CDR bilgilerini analiz etmek suretiyle her bir abone için en uygun tarife seçeneğini hesaplayabilir ve bu doğrultuda abonelere uygun tarife seçenekleri önerebilir. Ancak bu tür bir veri işleme faaliyeti abonelerin önceden bilgilendirilmesi ve rızalarının alınması koşuluyla gerçekleştirilebilecektir. Ayrıca trafik verileri, işletmecinin sadece kendi hizmetlerini pazarlaması amacıyla kullanılabileceğinden bu verilerin ticari amaçlı alım satımına izin verilmemelidir (FISCHER, 2010).

Haberleşme hizmetlerinin pazarlanması veya katma değerli hizmetlerin sunulması amacıyla işlenen trafik verileri bu hizmetlerin temininden sonra silinmeli veya anonim hale getirilmelidir (E-Gizlilik Direktifi, dibace 26). Trafik verileri özellikle arabağlantı ve faturalandırma konularındaki uzlaşmazlıkların çözümünde ilgili mevzuata uygun olarak yetkili makamlara bildirilebilir (E-Gizlilik Direktifi, md. 6/6).

Trafik verisini işleme yetkisi ise faturalandırma veya trafik yönetimi, tüketici talepleri, dolandırıcılık tespiti, elektronik haberleşme hizmetlerinin pazarlanması veya katma değerli hizmetlerin sunulması işlemlerini yürüten işletmecilerin yetkisi altında bulunan kişilerle ve ilgili faaliyetlerin gerektirdiği kapsamla sınırlandırılmalıdır (E-Gizlilik Direktifi, md. 6/5).

Trafik verilerini işlemekle görevli kişilerin yetki ve sorumluluklarının açıkça belirtilmesi ve yetkilerin sadece ilgili faaliyetin gerektirdiği kapsamda kullanılması veri gizliliği açısından son derece önemlidir. Nitekim yasal olmayan yollarla yapılan telefon dinlemeleri ile ilgili ülkemiz basınında yer alan haberler kapsamında veri gizliliği ihlali olup olmadığı hususunda BTK tarafından Turkcell İletişim Hizmetleri A.Ş hakkında soruşturma açılmış ve yapılan inceleme sonucunda aşağıdaki tespitlere yer verilmiştir (BTK, 2011b):

> *"Turkcell İletişim Hizmetleri AŞ'nin kişisel verilerin gizliliğine ve korunmasına yönelik olarak kişisel bilgilere erişimlerin işlem kayıtlarını tuttuğu, ancak bu işlem kayıtlarının ve personelin eriştiği bilgilerin görev tanımı çerçevesinde gerekli olup olmadığının incelemesini de içeren denetim faaliyetlerinin yapılmasında zafiyeti bulunduğu tespit edilmiştir. Bu durumun faturalandırma biriminde çalışan personel tarafından abonelere ait kişisel verilerin üçüncü kişilerle paylaşılarak ilgili mevzuat kapsamında haberleşmenin gizliliğini ihlal etmesi ile sonuçlandığı görülmüştür. Fatura bilgilerine erişen personelin yetkilerinin abonelerin kişisel bilgilerine erişimlerinde kötü amaçlarla kullanımını engelleyecek şekilde yeterli bir tedbirin alınmaması ve yetkilerin sınırlandırılmaması; maddi menfaat karşılığı üçüncü kişilere kişisel bilgileri pazarlayan bir suç şebekesinin bazı fatura detaylarını elde edebilmesine olanak sağlamıştır."*

Veri gizliliği ihlali nedeniyle ise işletmeci hakkında yaklaşık 12.250.000 TL tutarında para cezası uygulanmasına karar verilmiştir (BTK, 2011b).

VKÇG (2010) hassas nitelikte olmalarından dolayı trafik verilerinin, Veri Koruma Direktifinde belirtilen hassas verilerle kıyaslanabilir biçimde değerlendirilmesi gerektiğini belirtmektedir. Benzer biçimde PI (2001) raporunda, trafik verisinin birçok açıdan içerik verisi kadar hassas olduğu, modern haberleşme altyapılarının bireylerin profili hakkında büyük miktarda veri sağladığı hususlarına yer verilerek örneğin, internet üzerinde gezinen bir kişinin www.google.com arama motorunda sadece birkaç dakika içinde yaptığı sorgulardan kişinin sosyal, ekonomik, tıbbi ilgi alanları hakkında bir çıkarımda bulunulabildiği ifade edilmektedir.

3.2.3 Konum verilerinin işlenmesi

Son yıllarda özellikle uydusal konum belirleme sistemleriyle mobil telefonların gelişmesi konum verilerinin kullanımını arttırmış, başlangıçta sadece bir mobil telefondan çağrı yapmak veya almak için gerekli teknik veri olarak değerlendirilen konum verileri bireylere ilişkin önemli bilgiler sağladığından katma değerli hizmetler açısından potansiyel gelir kazancı olarak görülmeye başlamıştır. Böylece firmalar bu verilere dayalı birçok hizmet geliştirmiştir. En

yakın eczane veya restoran gibi bilgilerin bireylere sunulduğu hizmetleri, konum verisinin bir defaya mahsus kullanıldığı (belirli bir zamanda nerede olunduğu bilgisi) hizmetler ve verilerin sürekli kullanıldığı hizmetler (navigasyon desteği) takip etmiştir (VKÇG, 2005). Wi-Fi, RFID, bluetooth gibi teknolojiler kullanılarak yapılan veri işleme faaliyetlerinin kişisel verilerin işlenmesi ilkelerine uygunluğu ve söz konusu teknolojilerin veri koruma direktifleri kapsamında olup olmadıkları da günümüzün tartışma konuları arasındadır.

E-Gizlilik Direktifi kapsamında, kamu haberleşme şebekesi veya kamuya açık elektronik haberleşme hizmeti kullanıcı veya abonelerine ait konum verileri, anonim hale getirildikleri takdirde ya da abone ve kullanıcıların rıza vermeleri halinde katma değerli bir hizmetin sunulması için gerekli olan kapsam ve süre boyunca işlenebilir. Bu durumda hizmet sağlayıcı, rızaları alınmadan önce abone ve kullanıcıları şu hususlarda bilgilendirmelidir (E-Gizlilik Direktifi, md. 9/1):

- İşlenecek konum verisinin türü,
- Veri işlenmesinin amacı ve süresi,
- Verilerin katma değerli hizmet sunulması amacıyla üçüncü taraflara aktarılıp aktarılmayacağı.

Abone veya kullanıcıların konum verilerinin işlenmesi için verdikleri rızayı her zaman geri alabilmelerine de imkân sağlanmalıdır.

Konum verisinin işlenmesine rıza verildiği durumlarda abone ve kullanıcıya, ücretsiz ve basit bir yöntemle şebekeye her bağlanışta veya haberleşmenin her bir iletiminde veri işlenmesini reddetme olanağı sağlanır (E-Gizlilik Direktifi, md. 9/2). Ancak bu maddenin uygulanmasında problemler ortaya çıkabilir, zira yeni haberleşme teknolojileri sayesinde kapalı oldukları halde sinyal iletimi aracılığıyla cep telefonlarının yerleri tespit edilebilmektedir. Bu

durumda bir kullanıcının konum verisinin işlenmemesi yönündeki talebinin karşılanması tartışmaya açık olacaktır (FIDIS, 2007).

Konum verilerine bağlı katma değerli servisler üçüncü taraflarca veriliyorsa abone veya kullanıcı rızasının da üçüncü taraflarca alınması gerekir. Konum verisi sağlayan işletmecilerin ise katma değerli servisler için merkezi bir yapı kurmaları ve verileri üçüncü taraflara müşterinin tanımlanamayacağı şekilde (takma ad kullanımı gibi) iletmeleri önemlidir. Böylece üçüncü taraflar örneğin, en yakın restoran bilgisini talep eden tüketiciyi tanımlamadan servis sunmuş olacaklardır (VKÇG, 2005).

Konum verisini işleme yetkisi sadece, işletmecinin veya katma değerli elektronik haberleşme hizmetleri sağlayan üçüncü tarafın yetkisi altında bulunan kişilerle sınırlı olup, bu yetki söz konusu hizmetlerin sağlanmasının gerektirdiği kapsamda kullanılmalıdır (E-Gizlilik Direktifi, md. 9/3).

3.3 Verilerin Saklanması

Veri Saklama Direktifi ciddi suçların tespiti, soruşturulması ve kovuşturulmasında kullanılmak üzere gerçek ve tüzel kişilere ilişkin trafik ve konum verilerinin belirli bir süre saklanmasına yönelik olarak üye ülkelere yükümlülük getirmektedir.

Veri saklama yükümlülüğü E-Gizlilik Direktifinde oiduğu gibi kamu haberleşme şebekesi veya kamuya açık elektronik haberleşme hizmet sağlayıcılarını kapsamasına rağmen Finlandiya ve İngiltere gibi ülkelerde, küçük işletmecilere veri saklama yükümlülüğü getirilmemiştir. Zira küçük işletmeciler, bu yükümlülüğü yerine getirmek amacıyla veri saklama konusunda uzmanlaşan şirketlerle iş ortaklığı kurabilmekte ya da hizmeti dış kaynaktan temin edebilmektedir. Bu durum ise veri işleme faaliyetlerinin denetlenmesi ve gerekli güvenlik tedbirlerinin alınması gibi yükümlülüklerde küçük işletmeciler için sorun oluşturabilmektedir. Bu nedenle, veri güvenliği

konularının küçük ve orta ölçekli işletmeler üzerindeki etkileri göz önüne alınarak Veri Saklama Direktifinin tadil edilmesinin değerlendirileceği, AK tarafından dile getirilmektedir (EC, 2011).

Ciddi suç kavramının Veri Saklama Direktifinde tanımlanmamış olması, Direktif hükümlerini ulusal mevzuata aktaracak AB üyesi ülkelerin uygulamalarında farklılıklara neden olmuştur. Bu kapsamda, bazı ülkelerde ciddi suç kavramı hapis cezası gerektiren suçlara veya ulusal kanunlarda belirtilen suçlara hasredilirken bazı ülkelerde ise sadece ciddi suçlar hakkında değil ulusal güvenlik veya kamu güvenliğinin sağlanması gibi amaçlar için de veri saklama yükümlülüğü getirilmiştir (EC, 2011). AB ülkelerindeki uygulamaya ilişkin detaylara Tablo 3.2'de yer verilmektedir.

Tablo 3.2. AB ülkelerinde veri saklama amacının sınırlandırılması

Ülke	**Ulusal mevzuatta veri saklama gerekçeleri**
Belçika	Kriminal suçların soruşturulması ve kovuşturulması, acil yardım çağrı numaralarının suiistimali ile elektronik haberleşme şebeke veya hizmetlerinin art niyetli kullanımının soruşturulması, istihbarat veya güvenlik birimlerinin görevleri kapsamındaki amaçlar
Bulgaristan	Ciddi suçlar ile ceza kanunu kapsamındaki suçların araştırılması ve soruşturulması,
Çek Cumhuriyeti	Direktif mevzuata aktarılmadı.
Danimarka	Kriminal suçların soruşturulması ve kovuşturulması
Almanya	Direktif mevzuata aktarılmadı.
Estonya	Ciddi suçların soruşturulması
İrlanda	Ciddi suçların engellenmesi, devletin güvenliğinin sağlanması, insan hayatının kurtarılması
Yunanistan	Ciddi suçların tespit edilmesi
İspanya	Ceza kanunlarında öngörülen ciddi suçların tespiti, soruşturulması ve kovuşturulması

Tablo 3.2. (Devamı) AB ülkelerinde veri saklama amacının sınırlandırılması

Ülke	Ulusal mevzuatta veri saklama gerekçeleri
Fransa	Kriminal suçların tespiti, soruşturulması ve kovuşturulması, adli makamlara gerekli bilgilerin sağlanması, terörist eylemlerin engellenmesi, fikri hakların korunması
İtalya	Kriminal suçların tespiti ve önlenmesi
Kıbrıs	Kriminal suçların soruşturulması
Letonya	Ulusal güvenlik ve kamu güvenliğinin korunması, kriminal suçların soruşturulması
Litvanya	Ceza kanununda tanımlanan ciddi suçların tespiti, soruşturulması ve kovuşturulması
Lüksemburg	Kriminal suçların tespiti, soruşturulması ve kovuşturulması
Macaristan	Mahkeme, savcılık ve ulusal güvenlik birimlerinin görevleri kapsamındaki amaçlar, vergi ve gümrük idaresi ile polis birimleri tarafından kasıtlı işlenen ve 2 ya da daha fazla süre hapis cezası gerektiren suçların araştırılması
Malta	Ciddi suçların tespiti, soruşturulması ve kovuşturulması
Hollanda	Ciddi suçların tespiti, soruşturulması ve kovuşturulması
Avusturya	Direktif mevzuata aktarılmadı.
Polonya	Mahkeme talepleri, mali suçların engellenmesi, ulusal güvenlik ve istihbarat birimlerinin görevlerini yerine getirmesi
Portekiz	Ciddi suçların tespiti, soruşturulması ve kovuşturulması
Romanya	Direktif mevzuata aktarılmadı.
Slovenya	Anayasal düzen ve ulusal güvenliğin sağlanması, devletin politik ve ekonomik çıkarları, ulusal savunma
Slovakya	Kriminal suçların tespiti, soruşturulması ve kovuşturulması
Finlandiya	Ciddi suçların tespiti, soruşturulması ve kovuşturulması
İsveç	Direktif mevzuata aktarılmadı.
İngiltere	Ciddi suçların tespiti, soruşturulması ve kovuşturulması

Kaynak: EC, 2011

AB üyesi ülkelerin ulusal mevzuatlarında yer alan veri saklama amaçları Taslak Yönetmelikte ele alınmamıştır. Bu kapsamda Taslak Yönetmelikte,

verilerin hangi amaçlarla saklanacağı hususuna yer verilmesi amacın belirliliği ve sınırlandırılması ilkeleri gereği daha uygun olacaktır.

3.3.1 Saklanacak veri kategorileri

Veri Saklama Direktifi kapsamında saklanması öngörülen verilere ilişkin olarak,

- Sadece üretilmiş veya işlenmiş veriler için geçerli olması,
- Erişilebilir olması,
- Haberleşmenin içeriğine dair bilgi içermemesi

gibi birtakım sınırlandırmalar getirilmiş (Feiler, 2008), saklanacak veri kategorileri için sabit ve mobil telefon hizmetleri ile internet hizmetleri şeklinde bir ayrıma gidilmiştir.

3.3.1.1 Sabit ve mobil telefon hizmetleri

Sabit ve mobil telefon hizmetleri için saklanması gereken veriler şu şekilde sıralanmaktadır (Veri Saklama Direktifi, md. 5):

1) Haberleşmenin takibi ve kaynağının belirlenmesi için; arayan tarafın telefon numarası, adı ve adresi.
2) Haberleşmenin sonlandırılacağı noktayı belirlemek için aranan tarafın adı, adresi, numarası, çağrı iletme ve çağrı transferi gibi ek hizmetlerin olması durumunda çağrının yönlendirildiği numara veya numaralar.
3) Haberleşmenin tarihi, zamanı ve süresini belirlemek için haberleşmenin başlangıç ve bitiş tarih ve saati.
4) Haberleşmenin türünü tanımlamak için kullanılan telefon hizmeti. Kullanıcıların haberleşme cihazlarını veya bunların ekipmanlarını tanımlamak için sabit şebeke telefonu ile ilgili olarak arayan ve aranan

telefon numaraları. Mobil telefonla ilgili olarak aranan ve arayan telefon numaraları, arayan ve aranan tarafa ait IMSI ve IMEI; abone kaydı olmayan arama kartlı hizmetlerin olması durumunda hizmetin aktif hale getirildiği tarih ve zaman ile hizmetin aktif hale getirildiği hücre kimliği.

5) Mobil haberleşme cihazının konumunu tespit etmek için haberleşmenin başladığı hücre kimliği, haberleşme verilerinin saklandığı süre boyunca hücre kimlikleri ile ilgili olarak hücrelerin coğrafi konumlarını tanımlayan veriler.

3.3.1.2 İnternet hizmetleri

İnternet hizmetleri için saklanması öngörülen veriler ise şu şekildedir (Veri Saklama Direktifi, md. 5):

1) Haberleşmenin takibi ve kaynağının belirlenmesi için internet ortamına erişim, internet e-posta ve internet telefonu ile ilgili olarak kullanıcı kimliği ve/veya telefon numarası, haberleşmenin gerçekleştiği zaman diliminde kendisine IP adresi, telefon numarası veya kullanıcı kimliği tahsis edilen abonenin adı ve adresi.
2) Haberleşmenin sonlandırılacağı noktayı belirlemek için internet e-posta ve internet telefonu ile ilgili olarak aranan/alıcı tarafa ait telefon numarası ve/veya kullanıcı kimliği, adı ve adresi.
3) Haberleşmenin tarihi, zamanı ve süresini belirlemek için internet erişimi ile ilgili olarak oturum açma, kapatma tarih ve saati, internet servis sağlayıcısı tarafından tahsis edilen dinamik veya statik internet protokol adresi, abone ve kullanıcı kimliği, elektronik posta veya internet telefonu ile ilgili olarak oturum açma ve kapatma tarih ve saati.
4) Haberleşmenin türünü tanımlamak için internet ortamına erişim ve internet telefonu ile ilgili olarak kullanılan internet hizmeti.
5) Kullanıcıların haberleşme cihazlarını veya bunların ekipmanlarını tanımlamak için sayısal abone hattı numarası ya da haberleşmenin

kaynaklandığı diğer son noktalar ile çevirmeli ağ erişimi için arayan telefon numarası.

AB üyesi ülke uygulamaları incelendiğinde sabit ve mobil telefon hizmetlerine ilişkin saklanan trafik verilerinin genel olarak Veri Saklama Direktifi ile uyumlu olduğu dile getirilmektedir. Öte yandan, internet hizmetlerine yönelik saklanan trafik verilerinde farklılıklar olduğu örneğin internet sayfalarının URL adresi gibi haberleşmenin içeriği ile ilgili verilerin saklanabildiği VKÇG (2010) tarafından ifade edilerek Veri Saklama Direktifinin 5 inci maddesinde yer alan verilerin yeterince kapsamlı olduğu ve bu nedenle Direktif kapsamında işletmecilere ilave veri saklama yükümlülüğü getirilmemesi gerektiği belirtilmektedir

Trafik verisinden ziyade içerik verisi sağladığı göz önüne alındığında internet arama motorlarının Veri Saklama Direktifi kapsamında değerlendirilmemesi gerektiği VKÇG tarafından ifade edilmiş olmasına rağmen, Avrupa Parlamentosu AK'ya gönderdiği yazılı bildirimde çocuk pornografisi ve cinsel suçlarla mücadele etmek için Direktifin arama motorlarını da içerecek şekilde genişletilmesini talep etmiştir. AK, bu görüşleri değerlendirerek saklanacak veri türlerinde değişikliğe ihtiyaç olup olmadığını belirleyecektir (EC, 2011).

3.3.2 Veri saklama süreleri

AB üyesi ülkeler Veri Saklama Direktifinde belirtilen veri kategorilerini 6 aydan az 2 yıldan fazla olmamak üzere saklayacaklardır. 6 aylık sürenin kısaltılabileceğine dair bir hüküm bulunmazken özel durumlarda AK'nın onaylaması halinde 2 yıllık süre uzatılabilecektir (Veri Saklama Direktifi, md. 12/1). Direktifi iç hukuka aktaran AB ülkelerinin biri hariç tamamında Direktifte belirtilen sınırlar dâhilinde veri saklama süreleri uygulanmakta ancak bu süreler ülkeden ülkeye farklılık göstermektedir (EC, 2011). Tablo 3.3'te veri saklama sürelerine ilişkin ülke uygulamaları yer almaktadır.

Tablo 3.3. AB ülkelerinde veri saklama süreleri

Ülke	Veri saklama periyodu
Belçika	Kamuya açık telefon hizmetlerinde 1 yıldan 3 yıla kadar, internet hizmetlerine ilişkin bir hüküm mevcut değil.
Bulgaristan	1 yıl. Erişilen veriler talep olması halinde 6 ay daha saklanabilir.
Çek Cumhuriyeti	Direktif mevzuata aktarılmadı.
Danimarka	1 yıl
Almanya	Direktif mevzuata aktarılmadı.
Estonya	1 yıl
İrlanda	Sabit ve mobil telefon hizmetleri için 2 yıl, internet hizmetleri için 1 yıl.
Yunanistan	1 yıl
İspanya	1 yıl
Fransa	1 yıl
İtalya	Sabit ve mobil telefon hizmetleri için 2 yıl, internet hizmetleri için 1 yıl.
Kıbrıs	6 ay
Letonya	18 ay
Litvanya	6 ay
Lüksemburg	6 ay
Macaristan	Başarısız aramalar için 6 ay, diğer veriler için 1 yıl.
Malta	İnternet erişimi ve e-posta için 6 ay, diğer veriler için 1 yıl.
Hollanda	1 yıl
Avusturya	Direktif mevzuata aktarılmadı.
Polonya	2 yıl
Portekiz	1 yıl
Romanya	Direktif mevzuata aktarılmadı.
Slovenya	Sabit ve mobil telefon hizmetleri için 14 ay, internet hizmetleri için 8 ay.
Slovakya	Sabit ve mobil telefon hizmetleri için 2 yıl, internet hizmetleri için 6 ay.

Tablo 3.3. (Devamı) AB ülkelerinde veri saklama süreleri

Ülke	Veri saklama periyodu
Finlandiya	1 yıl
İsveç	Direktif mevzuata aktarılmadı.
İngiltere	1 yıl

Kaynak: EC, 2011

AB ülkeleri arasında tam bir uyum olmamakla birlikte veri saklama süresini 1 yıl olarak belirleyen ülkelerin çoğunluğu teşkil ettiği görülmektedir. Bu kapsamda, Taslak Yönetmelikte de 1 yıllık veri saklama süresine yer verilmiş olması AB üyesi ülke uygulamalarıyla paralellik arz etmektedir.

VKÇG (2010)'ye göre AB ülkeleri arasında veri saklama süreleri konusundaki uyumsuzluk rekabet ve maliyet açısından piyasa aktörlerini etkileyebileceğinden maksimum veri saklama süresinin azaltılması ve tek değerin belirlenmesi faydalı olacaktır. Nitekim Tablo 3.4'te yer alan ve 9 AB ülkesinde yetkili makamlar tarafından erişilen verilerin yaşını gösteren istatistikî bilgiler VKÇG'nin görüşünü destekler niteliktedir. Buna göre, yetkili makamlar tarafından erişilen verilerin yaklaşık %90'ını 6 aylık ya da daha kısa sürelik veriler oluşturmaktadır (EC, 2011).

Tablo 3.4. Yetkili makamlarca erişim talebinde bulunulan verilerin yaşı

Veri yaşı	Sabit telefon	Mobil telefon	İnternet
0 - 3 ay	% 61	%70	%56
3 - 6 ay	%28	%18	%19
6 - 12 ay	%8	%11	%18
1 yıl üzeri	%3	%1	%7

Kaynak: EC, 2011

Veri işlemenin uluslararası niteliğinin artması ve dış kaynaklı veri depolamanın gelişmesini göz önüne alarak AB bünyesinde veri saklama sürelerine ilişkin uyumun artırılması gerektiğini belirten AK ise farklı kategorideki veriler için farklı süreler öngörmeyi planlamaktadır. Nitekim 2005

yılında Komisyonun veri saklama süresine ilişkin önerisi sabit ve mobil telefon hizmetleri için 12 ay, internet hizmetleri için ise 6 ay şeklinde olmuştur (EC, 2011).

3.3.3 Saklanan verilerin korunması ve güvenliği

Veri Saklama Direktifi kapsamında saklanan verilere ulaşılabilirlik, kişilerin tercihleri, düşünceleri ve davranışları hakkında fikir verebildiğinden kişilerin özel hayatlarına müdahale edilme riskini içermekte ve haberleşmenin gizliliğini zedeleyebilmektedir. Örneğin, elektronik haberleşme ile ilgili konum verilerine yetkisiz erişim sağlanması ve/veya bu verilerin yetkisiz biçimde ifşa edilmesi ilgili kişilerin mahremiyetlerini önemli ölçüde etkilemektedir. Bu yüksek risk karşısında, uygun teknik ve idari tedbirlerin alınması gerekli olmaktadır (VKÇG, 2010).

Veri Saklama Direktifinde saklanan verilere ilişkin olarak işletmeciler tarafından yerine getirilmesi gereken 4 veri güvenliği ilkesi şu şekilde sıralanmaktadır:

1) *Saklanan veriler, şebekedeki diğer verilerle aynı kalitede olmalı, aynı güvenlik ve koruma tabirlerine tabi tutulmalıdır,*
2) *Saklanan verilerin istem dışı, yetki dışı ya da yasa dışı, erişim, tahrip, kayıp, değişiklik, depolama, işleme ve ifşa fiillerine karşı korunması için uygun teknik ve idari tedbirler alınmalıdır,*
3) *Verilerin sadece özel yetkilendirilmiş personel tarafından erişilebilir olmasının sağlanması için uygun teknik ve idari tedbirler alınmalıdır,*
4) *Veriler saklama süresi sonunda imha edilmelidir.*

Üçüncü maddede belirtilen veri güvenliği ilkesinin sağlanması için VKÇG (2010) tarafından tavsiye edilen ancak mevcut durumda bütün işletmeciler tarafından uygulanmadığı belirtilen teknik ve idari tedbirlerin bir kısmı aşağıda yer almaktadır:

- *Kullanıcı sorumlulukları ve profillerinin tanımlanmasıyla, saklanan verilere güçlü erişim kontrolü,*
- *Sisteme erişim için şifre+biyometri, şifre+simge (token) gibi çift kimlik denetimi mekanizmalarının kullanılması,*
- *En az, kullanıcı kimliği, erişim zamanı ve erişilen dosya bilgilerinden oluşan log kayıtlarının saklanmasıyla, veri işleme ve sisteme erişim faaliyetlerinin ayrıntılı olarak takip edilebilmesi,*
- *Log bütünlüğünün sağlanması için log yönetim sistemi kurulması,*
- *Veri saklama sisteminin, trafik verilerini ticari amaçlı işleyen sistemlerden mantıksal olarak ayrılması,*
- *Veri gizliliğini sağlayacak ilave tedbirler,*
- *İdari tedbirler açısından trafik verilerinin saklandığı sistemden sorumlu yöneticilere özel önem verilmesi, bu yöneticilerin görevlerinin detaylandırılması ve sistem üzerinde gerçekleştirilen faaliyetlerin kapsamlı biçimde denetlenmesi.*

Avrupa Komisyonu,

- 15 üye ülkenin Veri Saklama Direktifinde belirtilen veri güvenliği ilkelerinin tamamını iç hukuka aktardığını,
- Belçika, Estonya, İspanya ve Letonya'nın bu ilkelerin 2 veya 3'ünü iç hukuka aktardığını ancak veri saklama süresi sonunda verilerin yok edilmesine ilişkin doğrudan bir hükme yer verilmediğini,
- İtalya ve Finlandiya'da ise sadece verilerin yok edilmesine ilişkin veri güvenliği ilkesinin mevzuatta yer aldığını

belirtmekte ancak bu ülkelerde çift kimlik denetimi mekanizması, detaylı log yönetim sistemi gibi teknik tedbirlerin uygulanıp uygulanmadığı konusunda bir açıklık olmadığına dikkat çekmektedir. Ayrıca 21 ülkede veri güvenliği ilkelerinin uygulanmasını denetlemekle görevli bir otorite bulunduğu ve bunun

da genellikle veri koruma otoritesi tarafından yerine getirildiği Komisyon tarafından ifade edilmektedir (EC, 2011).

AB üyesi ülke uygulamalarına işletmeciler açısından bakıldığında ise büyük ölçekli işletmelerin uygun güvenlik seviyesi sağlamak için gerekli teknik ve idari tedbirleri almaya çalıştıkları ancak küçük ölçekli işletmelerin maliyet stratejileri nedeniyle daha düşük güvenlik standartları sağladıkları, bu kapsamda trafik verilerinin saklanmasına ilişkin risklerin farkındalığı hakkında bir standart olmadığı belirtilmektedir (VKÇG, 2010).

AK, saklanan verilerin kişisel ve hassas niteliği nedeniyle depolanması, elde edilmesi ve kullanılması sürecinde, veri ihlali riskini en aza indirmek ve AB vatandaşlarının güvenliğini sağlamak amacıyla yüksek standartlarda veri koruma ve güvenliğinin sağlanması gerektiğini, bu kapsamda VKÇG'nin tavsiyelerini de göz önüne alarak tasarımsal gizlilik ilkesinin benimsenmesi dâhil veri koruma ve veri güvenliği standartlarının güçlendirilmesine ilişkin seçeneklerin değerlendirileceğini beyan etmiştir (EC, 2011).

3.4 Kişisel Verilerin Korunmasında Teknolojik Yaklaşımlar

Kişisel verilerin korunmasında yasal düzenlemelerin önemi tartışılmaz olmakla birlikte teknik yöntemlerin yasal düzenlemelere dâhil edilmesinin gizliliğin korunmasında tamamlayıcı bir rol üstleneceği değerlendirilmektedir. Bu çerçevede tasarımsal gizlilik ilkesi ile gizliliği artırıcı teknolojilerden bahsetmek yerinde olacaktır.

3.4.1 Tasarımsal gizlilik

Tasarımsal gizlilik, "*Teknolojilerin tasarım, kurulum, kullanım ve kaldırılma safhalarını içeren yaşam döngülerinin tamamında kişisel verilerin ve gizliliğin tümleşik olarak bulunması*" olarak tanımlanmaktadır (EU, 2010a).

İnternet, mobil telefonlar, RFID, sosyal ağ siteleri, biyometri, bulut bilişimi (*cloud computing*) gibi araçlarla sayısal ayak izlerinin bırakılabildiği bir ortamda her türlü verinin işlenip depolanabilmesi ihtimaline karşın alınabilecek en önemli önlemlerden birisi teknolojik yeniliklerle bir bireyin mahremiyetinin ihlal edilme olasılığını en aza indirmektir. Örneğin, bir takside kilometre ölçmek amacıyla yer alan ve aracın konum verisini sürekli olarak merkezi bir veritabanına ileten cihazla, konum verileri sürücünün kontrolünde olacak şekilde tasarlanan bir cihaz arasında bireyin mahremiyeti açısından farklılık bulunmaktadır (DUTCHDPA, 2009).

E-Gizlilik Direktifinde işletmeciler, sundukları hizmetlerin güvenliğini garanti altına almak için uygun teknik ve idari tedbirleri almakla yükümlü kılınırken Veri Saklama Direktifinin 7 nci maddesinde ise saklanan verilerin tedbirsizlikle, hukuka aykırı veya yetkisiz olarak; tahrip edilmesi, kaybolması, değiştirilmesi, depolanması, işlenmesi, ifşa edilmesi ve belirtilen verilere erişilmesine karşı uygun teknik ve idari tedbirlerin alınması gerekli görülmektedir. Bununla birlikte Veri Koruma Direktifinde teknik ve idari tedbirlerin, gerek sistemlerin tasarım aşamasında gerekse veri işleme esnasında alınması gereken tedbirleri kapsayacağı belirtilmektedir (Veri Koruma Direktifi, dibace 46).

Her ne kadar AB düzeyinde kişisel verilerin ve gizliliğin korunmasına yönelik güçlü bir yasal çerçeve bulunuyor olsa da bilgi ve iletişim teknolojilerindeki gelişmeler bireylerin haklarının korunması için yeni aksiyonların alınmasını gerekli kılmaktadır. Bunun için tasarımsal gizliliğin bir ilke olarak benimsenmesi ve mevcut yasal çerçeveye dâhil edilmesi gizliliğin korunmasında önemli bir adım olacaktır (EDPS, 2010).

Bu ilke, veri kontrolörleri yanında teknoloji tasarımcıları ve üreticileri için de bağlayıcı olmalı, bilgi ve iletişim teknolojilerinin sadece güvenliği sağlamaları değil aynı zamanda kişisel verilerin gerekli kapsam ve ölçüde işlenmelerine imkân sağlamalıdır. Bu ilkenin gerekliliği, Almanya'da yaşanan örnekle

desteklenmektedir (VKÇG, 2009). Alman Federal Anayasa Mahkemesinin istihbarat birimlerince teknik araçların kullanılarak bilgi teknoloji sistemlerine gizlice erişmelerine olanak sağlayan kanun hakkında 27 Şubat 2008 tarihinde verdiği kararda "bilgi teknoloji sistemlerinin bütünlüğü ve gizliliğinin sağlanmasının" temel haklar arasında olduğu ve bu hakkın kanunla ihlal edildiği belirtilmiştir (Hornung, 2009).

Tasarımsal gizliliğin ilke olarak benimsenmesi, gizliliği artırıcı teknolojilere olan ihtiyacın önemini artıracak olmakla birlikte kişisel verilerin korunmasını sağlayan araçların (örneğin varsayılan gizlilik ayarları[9], şifreleme, erişim kontrolleri) uygulanmasını sağlayacak aynı zamanda sosyal ağlar, arama motorları, Wi-Fi yönlendiricileri gibi üçüncü taraflara ve bireysel müşterilere sağlanan ürün ve hizmetler için kritik bir gereklilik olacaktır (VKÇG, 2009).

Tasarımsal gizlilik ilkesi hızlı gelişen teknolojik ve sosyal çevre karşısında sürdürülebilirliğini sağlamak için teknolojiden bağımsız tanımlanmalı, ayrıca "mümkün olan en kısa zaman" özelliğini barındırdığı vurgulanmalıdır (VKÇG, 2009). Zira gizlilik ilkeleri sistem geliştirmelerinin başlangıç aşamasında düşünülmezse ortaya çıkacak zararların bertaraf edilmesi için geç kalınmakta ve sistemlerin onarılması ekonomik açıdan da maliyetli olabilmektedir. Son yıllarda artan sayıda yaşanan veri ihlalleri bu görüşü doğrularken tasarımsal gizliliğe olan gereksinimi de ortaya koymaktadır. (EDPS, 2010). Ülkemiz elektronik haberleşme sektöründe faaliyet gösteren işletmecilerden Vodafone Telekomünikasyon AŞ'nin resmi internet sayfası[10] üzerinden abonelere sunduğu "MyVodafone Servisi"ne ilişkin veri gizliliği ihlali buna örnek verilebilir.

İşletmecinin internet sayfasında Mart 2009 ve Ekim 2010 tarihleri arasında oluşan güvenlik açığı, abonelere ait kişisel bilgilerin başkaları tarafından

---

[9] Privacy by default settings.
[10] https://www.vodafone.com.tr/MyVodafone/myvodafone.home.php

görüntülenebilmesine neden olmuş, bu durumun şirketin gerekli güvenlik tedbirlerini almamasından kaynaklandığı ortaya çıkmıştır. Yapılan inceleme ve denetimin ardından BTK, şirket hakkında yaklaşık 1.270.000 TL tutarında idari para cezası uygulanmasına karar vermiştir (BTK, 2011a).

Tasarımsal gizlilik yerine göre,

- Kişisel verilerin en aza indirgenmesi veya bertaraf edilmesini,
- Gerekli olmayan ya da istenmeyen veri işlemenin engellenmesini,
- Bireylere, kişisel verilerini kontrol edebilmelerini sağlayan araçların sunulmasını,
- Kişisel veri işleyebilen bilgi ve iletişim teknolojilerinin mimarisine entegre edilmeyi

içerebilmektedir (EDPS, 2010).

Cavoukian (2011) tasarımsal gizliliğin hedeflerinin 7 temel unsur sayesinde gerçekleştirilebileceğini belirtmektedir:

- *Proaktiflik: Gizliliğe aykırılık teşkil edebilecek vakalar, gerçekleşmeden önce engellenir,*
- *Varsayılan ayarlar: Herhangi bir IT sisteminde kişisel veriler otomatik olarak korunmalıdır. Bireylerin kişisel verilerini korumaları için ilave önlem almalarına gerek yoktur zira bu önlemlerin sistem içinde zaten var olmaları beklenmektedir,*
- *Tasarıma eklenme: Tasarımsal gizlilik IT sistemlerine tasarım aşamasında yerleştirilir, bu durumda gizlilik ihlalleri gerçekleştikten sonra sisteme ilave edilen bir eklenti olmaz,*
- *Tam işlevsellik: Tasarımsal gizlilik bütün meşru menfaatleri ve hedefleri (gizlilik ve güvenliğin aynı anda sağlanması gibi) barındırır,*

- *Baştan sona güvenlik: Veriler elde edilmeden önce sisteme gömülen tasarımsal gizlilik, verinin yaşam döngüsü boyunca güvenli biçimde saklanmasını ve sürecin bitiminde silinmesini sağlar,*
- *Görünürlük ve şeffaflık: Tasarımsal gizlilik, ilgili tarafların belirlenen amaçlar doğrultusunda işlem yapıp yapmadıklarını garanti altına almayı hedefler. Yapılan işlemler hem kullanıcılara hem de hizmet sağlayıcılara açıktır,*
- *Bireyin mahremiyetine saygı: Tasarımsal gizlilik, ilgili aktörlerin bireylerin menfaatlerini en üstte tutmalarını gerektirir.*

VKÇG (2009)'ye göre ise veri işleme özelliğine sahip sistemlerin tasarımı esnasında ve bu sistemleri çalıştırırken aşağıdaki özellikler göz önünde bulundurulmalıdır:

- *Verinin en aza indirilmesi: Veri işleme sistemleri gerekli olandan daha fazla kişisel veri içermeyecek biçimde tasarlanmalıdır,*
- *Kontrol edilebilirlik: IT sistemleri, kişisel verilerini kontrol edebilmeleri için bireylere etkili mekanizma sunmalı, bireylerin rıza ve ret durumları bu mekanizmalar tarafından desteklenmelidir,*
- *Şeffaflık: Sistemlerin etkinliği hakkında bireyler yeterince bilgilendirilmeli, elektronik erişim veya bilgilendirilme sağlanmalıdır,*
- *Kullanıcı dostu sistemler: Her seviyede kullanıcıya hitap etmeleri için sistemler basit arayüzler sağlamalıdır,*
- *Verinin gizliliği: IT sistemleri kişisel verilere sadece yetkili kişiler erişecek şekilde tasarlanmalı ve güvenliği sağlanmalıdır,*
- *Veri kalitesi: Veri kontrolörleri gerektiğinde ilgili verilere yasal amaçlarla erişilebilmesini sağlamalıdır,*
- *Kullanımın sınırlandırılması: Farklı amaçlara hizmet eden (bulut bilişimi vb) işlem ve veriler güvenli biçimde birbirlerinden ayırt edilmelidir,*

Bu kapsamda, tasarımsal gizlilik ilkesinin yasal düzenlemelerde yer alması işletmecilerin yeterli koruma tedbirleri almalarını tetikleyecek, olası veri ihlallerinin önüne geçilerek gerek tüketiciler gerekse işletmeciler açısından fayda sağlanmış olacaktır.

3.4.2 Gizliliği artırıcı teknolojiler (PET)

PET hakkında birçok farklı tanım olmakla birlikte AB tarafından kabul gören tanım şu şekildedir:

> *"Sistemlerin işlevselliğine halel getirmeden, kişisel verilerin bertaraf edilmesi ya da gerektiği kadar kullanılması suretiyle kişisel verilerin gereksiz biçimde ya da istek dışı işlenmesini engelleyerek gizliliğin korunmasını sağlayan bilgi ve iletişim teknolojileri sistemlerine yönelik önlemler (Borking vd., 2003)."*

Teşebbüslerin, gizliliğin korunması amacıyla aldıkları önlemlere bakıldığında verilerin güvenliğinin sağlanması için sarf edilen çabaya vurgu yapıldığı görülmektedir. Ne var ki kişisel verilere yetkisiz erişimin engellenmesi amacıyla alınan güvenlik tedbirleri gizliliğin önemli bir unsuru olmasına rağmen gizliliğin korunmasıyla aynı anlama gelmemektedir. Zira gizlilik, verilerin gereken ölçüde toplanması, belirlenen amaçlar doğrultusunda kullanılması, ilgili kişinin rızası olmadan ikincil kullanımlarının engellenmesi gibi daha geniş alanları kapsamaktadır (Wright ve Hustinx, 1995). Aşağıda yer alan uygulamalar, tasarımsal gizliliğin ve PET'in kişisel verilerin ve gizliliğin korunmasına nasıl katkıda bulunduğunu örneklendirmektedir.

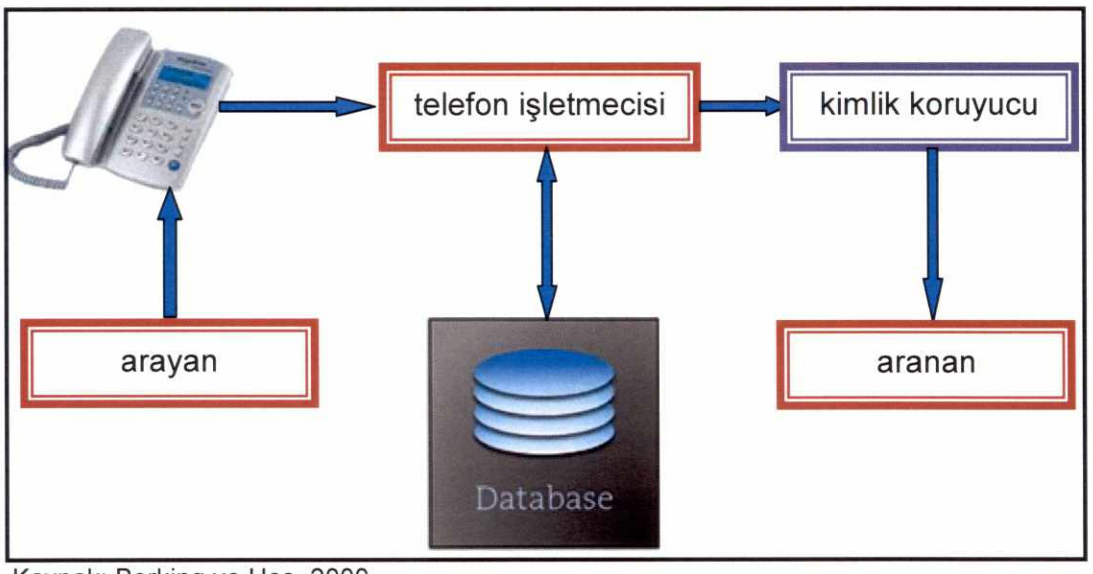
3.4.2.1 Örnek uygulama 1: arayan hattın kimliğinin tanımlanması

Bilgi sistemlerinin bir unsuru olarak görülen kimlik koruyucular (*identity protectors*) kullanıcıların gerçek kimliklerini takma kimliklere (*pseudo-identites*) dönüştürerek kullanıcıların menfaatlerini korumaktadır. Bir kimlik koruyucu bir bilgi sistemine entegre edildiğinde kullanıcı, hizmetleri anonim

olarak kullanabilmekte bu sayede hem belirtilen hizmet açısından hem de diğer kullanıcılarla ilişki anlamında gizliliğin korunması sağlanmaktadır. Örneğin, analog telefon şebekelerinde arayanın kimliği, aranan tarafından telefona cevap verilmeden önce bilinememekteydi. Sayısal telefon şebekeleri ise arayanın numarasının aranan tarafta görünmesine imkân tanımaktadır. Arayan tarafın numarasının görüntülenmesini sağlayan bu fonksiyon, arayan hattın kimliğinin tanımlanması (CLI) olarak bilinmektedir (Borking ve Hes, 2000).

Şekil 3.7'de kullanıcılara sağlanan telefon hizmetine ilişkin bilgi sistemi gösterilmektedir. Telefon çağrısı yapan/alan taraflar bilgi sisteminin kullanıcılarıdır. CLI fonksiyonunun içerisine entegre edilen ve kullanıcıya birtakım engelleme seçenekleri sunan bir kimlik koruyucu sayesinde arayan taraf, numarasını gizli tutabilmekte böylece CLI bir kimlik koruyucu rolü üstlenmektedir. Burada kimlik koruyucu, hizmet sağlayıcı ile hizmet arasında yer almaktadır (Borking ve Hes, 2000).

Şekil 3.7. CLI ve kimlik koruyucu işlevselliği



Kaynak: Borking ve Hes, 2000

Sonuç olarak CLI ve ona eşlik eden arayan hattın kimliğinin engellenmesine ilişkin seçenekler sayısal telefon şebekesinde bir kimlik koruyucunun fonksiyonunu ortaya koymaktadır. Burada gizliliğin korunmasına dair en önemli husus, numarasının aranan tarafa gösterilip gösterilmemesi konusunda arayan tarafın karar verebilmesidir. Benzer şekilde, aranan tarafa da gizli numaralardan gelecek aramaları reddederek tanımadığı kişilerden kendini koruma imkânı da sağlanmış olmaktadır.

3.4.2.2 Örnek uygulama 2: konum tabanlı servisler

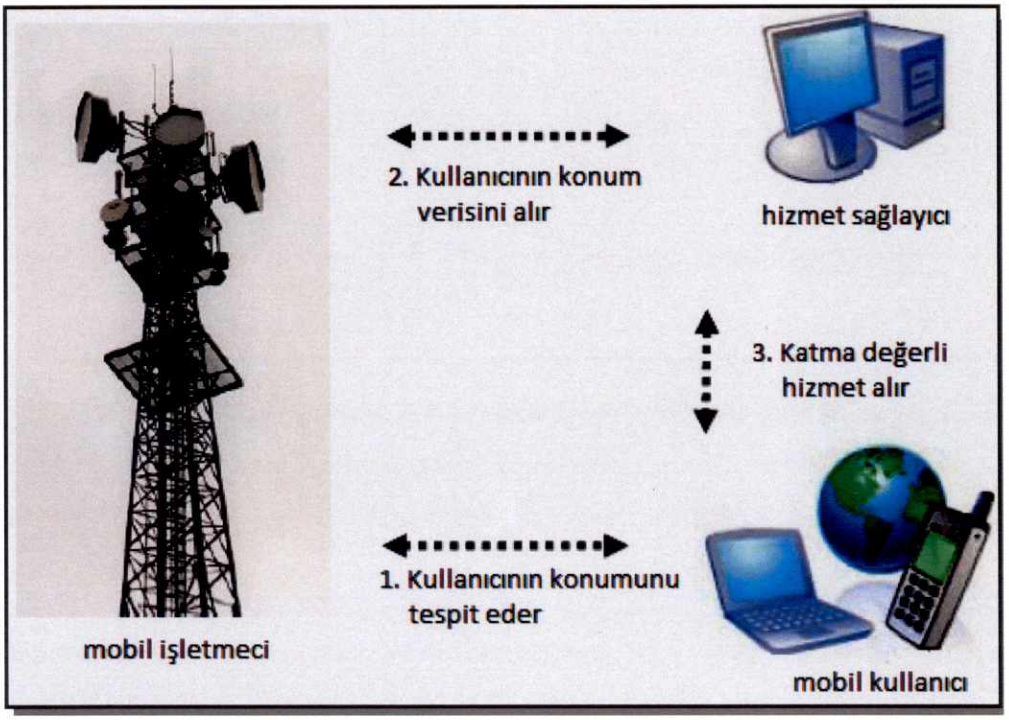
Son yıllarda konum tabanlı servislerin (KTS) artış göstermesi, mobil şebeke işletmecileri veya hizmet sağlayıcıların gizlilik ihlallerine neden olup olmadıkları sorununu da beraberinde getirmektedir. Bu sorun özellikle fazla miktarda kişisel verilerin ihtiyaç duyulduğu gelişmiş KTS hizmetlerinde ortaya çıktığından söz konusu verilerin gizliliğinin korunmasını sağlayacak PET'in önemi daha da artmaktadır (London Economics, 2010).

Bir KTS hizmeti uygulamasında ilgili tarafların genellikle mobil işletmeci ve KTS uygulama sağlayıcısından oluşması, karmaşık gizlilik politikalarının uygulanmasını gerektirmektedir. Ayrıca veriler ilgili taraflar arasında serbestçe iletilebildiğinden bu veri akışı mobil işletmecilerin kullanıcıların alışkanlıkları hakkında bilgi sahibi olmalarına, uygulama sağlayıcılarının ise kullanıcıların kimlik bilgilerini öğrenebilmelerine imkân tanımaktadır (Kosta vd, 2008).

Şekil 3.8'de yer alan klasik KTS senaryosunda mobil işletmeci, kullanıcının konum verilerini ve ilgili verileri uygulama sağlayıcısına iletirken bunun karşılığında kullanıcı talepleri, uygulama sağlayıcısı tarafından mobil işletmeci aracılığıyla yerine getirilmekte ancak KTS kullanımı gizli bilgilerin kötüye kullanılması ihtimalini içermektedir. Örneğin, bir veri hırsızı KTS'den faydalanmak isteyen bir kişinin kimliğini tespit edebilmek için kamuya açık bir adres kütüğünü kullanabilir. Böylece kişinin iletişim detayları ve

alışkanlıklarına ilişkin bilgiler pazarlama faaliyetleri yürüten üçüncü taraflara satılabilir. Bu nedenle, veri gizliliğinin korunmasına ilişkin düzenlemelere uyum sağlamak amacıyla KTS'nin işlevselliğine halel getirmeyecek ancak işlenen kişisel verileri en aza indirecek teknolojiler gerekli görülmektedir (London Economics, 2010).

Şekil 3.8. Klasik KTS senaryosu

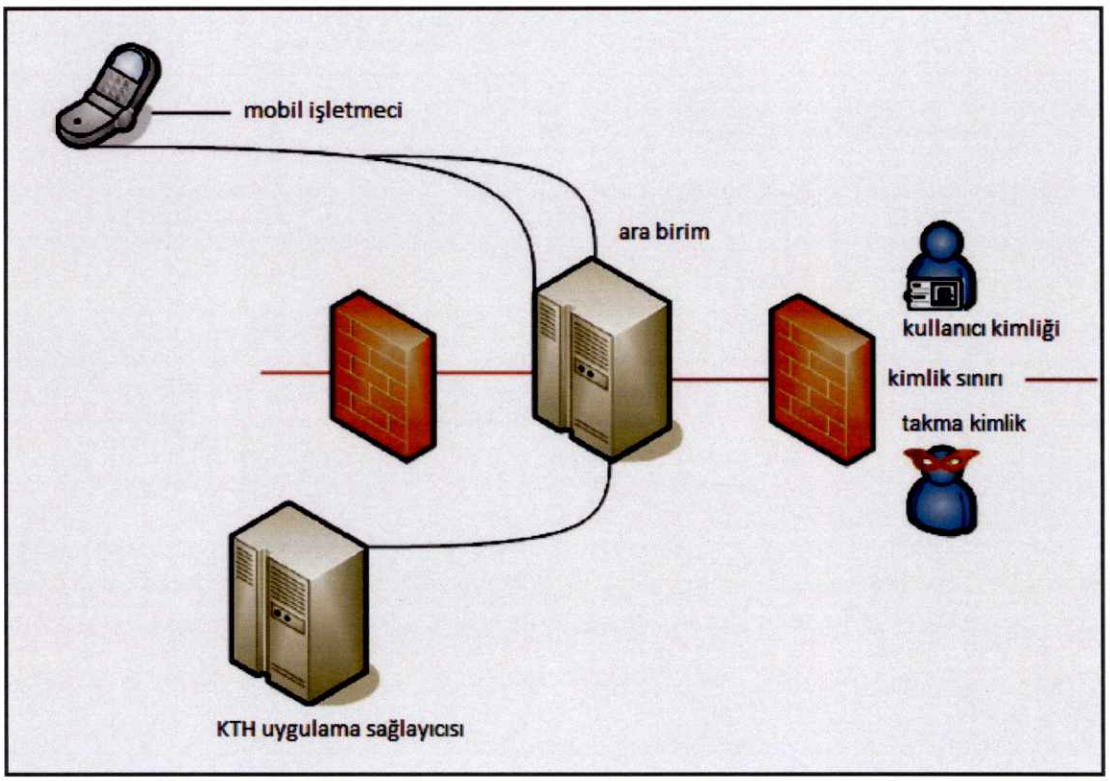


Kaynak: Prime, 2008

KTS hizmetleri için geliştirilen PET, mobil işletmeci ile KTS uygulama sağlayıcısı arasında oluşturulan bir ara birimi (intermediary) içermektedir. Ara birimin mobil işletmecinin sistemlerine kurulması durumunda gerekli idari tedbirlerin alınması gereklidir. Ancak ara birimin genellikle bağımsız bir tarafça kurulması örneğin sanal mobil şebeke işletmecileri açısından daha uygun olmaktadır. Klasik KTS senaryosunun aksine ara birim senaryosunda (Şekil 3.9) mobil işletmeci ile uygulama sağlayıcı sadece hizmetlerin sunumu için gerekli bilgileri görmektedir. Mobil işletmeci, aboneleri hakkında herhangi ilave bilgiye (kullanım profili gibi) sahip olmadan konum verilerini ara birime

iletmekte, KTS uygulama sağlayıcısı ise kullanıcının tanımlanmasına gerek olmadan KTS hizmetini sağlayabilmektedir (Kosta vd, 2008).

Şekil 3.9. KTS ara birim senaryosu



Kaynak: Kosta vd., 2008

PET'in özellikle veri kontrolörleri açısından getireceği ekonomik faydanın belirlenmesi tam olarak mümkün görünmemekle birlikte uygulama bazında veya kullanılacak teknolojiye göre getireceği fayda ve maliyetler değişmektedir (London Economics, 2010).

4. ÜLKE UYGULAMALARI

Tezin bu bölümünde elektronik haberleşme alanında kişisel verilerin işlenmesi, saklanması ve korunmasına yönelik olarak ülke örneklerine yer verilecektir. Çalışmamızın genelinde AB mevzuatı ve Direktifleri üzerinde durulduğundan Avrupa dışındaki ülke uygulamaları incelenmemiş, seçilen örneklerde ise ülkelerin gelişmişlik düzeyleri, coğrafi büyüklükleri ve elektronik haberleşme sektöründe düzenleyici otoritelerinin etkinliği gibi hususlar göz önünde bulundurulmuştur.

Öte yandan, çalışmamızda Veri Koruma Direktifine yer verilmiş olsa da genel olarak elektronik haberleşme sektörü esas alındığından bu bölümde E-Gizlilik Direktifi, Veri Saklama Direktifi ve Vatandaş Hakları Direktifine yönelik ülke uygulamaları ele alınacaktır. Bu kapsamda, AB ülkelerinden İngiltere, Almanya, Fransa, İspanya, Hollanda, İtalya ve İrlanda incelenerek söz konusu ülkelerde AB Direktiflerine uyum çerçevesinde yapılan çalışma ve düzenlemeler ortaya konulacaktır.

4.1 İngiltere

İngiltere'de E-Gizlilik Direktifinin ulusal mevzuata aktarılması 11 Aralık 2003 tarihinde yürürlüğe giren "Elektronik Haberleşme ve Gizlilik Yönetmeliği[1]" ile olmuştur. Yönetmelik, Direktif maddeleriyle genel olarak paralel biçimde ele alınmış ancak haberleşmenin ve ilgili trafik verisinin izlenmesi ile ilgili hükümler Yönetmelikte yer almamıştır. Kullanıcıların internet trafiği analizine bağlı olarak internet servis sağlayıcıları tarafından kullanılan davranışsal reklam[2] (*behavioral advertising*) uygulamaları hakkında AK'ya gelen

---

[1] http://www.legislation.gov.uk/uksi/2003/2426/pdfs/uksi_20032426_en.pdf

[2] Davranışsal reklam uygulamaları sayesinde kullanıcının internet üzerinde ziyaret ettiği sayfalar kayıt altına alınmakta ve bu bilgiye göre kullanıcının ilgi alanına yönelik reklam yayımlanabilmektedir. Örneğin bir internet sayfasından uçak bileti alan bir kullanıcıya başka bir internet sayfasına girdiğinde seyahat reklamları gösterilmektedir. Ayrıntılı bilgi için bkz.

şikâyetler üzerine AK, ulusal mevzuatında bulunan hükümlerin Direktife tam uyum sağlamadığı gerekçesiyle İngiltere'yi AAD'ye sevk etmiştir (EU, 2010d).

Yönetmelikte istek dışı haberleşmeyle ilgili detaylı hükümler yer almaktadır. Doğrudan pazarlama amaçlı istek dışı aramalar ile faks makineleri kullanılarak yapılacak haberleşme için düzenleyici otorite olan OFCOM'un kayıt kütüğü tutması ve kütükte yer alan verilerin güncelliğini sağlaması düzenlenmektedir (md. 25-26). Bu kayıt kütükleri opt-out esasına dayalı olarak çalışmaktadır. 25 Haziran 2004'te yürürlüğe giren Yönetmelik[3] ise tüzel kişilerin de telefon kayıt kütüğüne kaydolmalarına imkân tanımıştır.

İngiltere'de 6 Nisan 2009 tarihinde yürürlüğe giren Veri Saklama Yönetmeliği ile, Veri Saklama Direktifi ulusal mevzuata aktarılmıştır. Yönetmelikte sabit ve mobil telefon ile internet hizmetlerine ilişkin haberleşme verilerinin haberleşmenin yapıldığı andan itibaren 12 ay süre ile saklanması öngörülmektedir. Yönetmelikte yer alan haberleşme verisi Veri Saklama Direktifinde geçen "veri" kavramı yerine kullanılmaktadır. Bu kapsamda haberleşme verisi, trafik ve konum verileri ile abone veya kullanıcıyı tanımlamak için gerekli olan diğer ilgili verilerdir.

Vatandaş Hakları Direktifi hükümlerinin mevzuata aynen aktarılması öngörülürken ICO'nun kişisel veri ihlalinin bildirimiyle ilgili bir kılavuz yayımlaması ve bu maddenin hizmet sağlayıcılar tarafından uygulanıp uygulanmadığını denetlemesi istenmektedir (BIS, 2010).

---

http://www.radikal.com.tr/Default.aspx?aType=Detay&VersionID=7520&Date=16.06.2008&ArticleID=1047076

[3] http://www.legislation.gov.uk/uksi/2004/1039/pdfs/uksi_20041039_en.pdf

4.2 Almanya

22 Haziran 2004 tarihli Telekomünikasyon Kanunu[4] (TK) ve 3 Temmuz 2004 tarihli Haksız Rekabet Kanunu[5] (HRK) ile, E-Gizlilik Direktifi Almanya ulusal mevzuatına aktarılmaya çalışılmıştır.

HRK'nın 7 nci kısmında istek dışı haberleşmeyle ilgili hükümler yer almaktadır. Buna göre, telefon aramaları, otomatik arama makineleri, fakslar ve elektronik iletilerle yapılacak istek dışı haberleşmede tüketicilerin önceden onay vermesi şartı aranmaktadır. Elektronik iletilerde istisna olarak müşteri ilişkisi bulunması, benzer ürün ve hizmetlerin pazarlanması, iletişim bilgilerinin elde edilme aşamasında müşteriye doğrudan pazarlama amaçlı haberleşmeyi reddetme imkânı tanınması halinde önceden onay şartı aranmamaktadır (Finger and Schmieder, 2005).

2007 yılında TK'yı tadil eden düzenlemeyle de Veri Saklama Direktifi iç hukuka aktarılmış, 1 Ocak 2008 tarihinden itibaren sabit ve mobil telefon hizmet sağlayıcıları, 1 Ocak 2009 tarihinden itibaren de internet servis sağlayıcıları trafik verilerini 6 ay süre ile saklamakla yükümlü kılınmıştır (Arnoldi, 2009). Ancak düzenlemeye karşı Federal Anayasa Mahkemesine yapılan itiraz başvurusu neticesinde Yüksek Mahkeme, 2 Mart 2010 tarihli kararıyla yasanın, telekomünikasyonun gizliliğinin korunması temel hakkını ihlal ettiğini bildirmiştir. Kararda, veri depolanmasında güvenlik sorunları bulunduğu ve düzenlemenin bireyler üzerinde gözetim altında oldukları yönünde bir endişe oluşturduğu vurgulanmış, TK'nın 113a kısmında belirtilen hükümler uyarınca telekom şirketleri tarafından saklanan verilerin silinmesi ve yasada gerekli değişikliklerin yapılması istenmiştir (EDRI, 2010).

---

[4] http://www.bfdi.bund.de/cae/servlet/contentblob/411286/publicationFile/25386/TelecommunicationsAct-TKG.pdf

[5] http://www.gesetze-im-internet.de/englisch_uwg/englisch_uwg.html#fdt_1

Vatandaş Hakları Direktifinin yayımlanmasından önce Almanya'da veri ihlali bildirimine ilişkin olarak Federal Veri Koruma Kanunu (FVKK) 42a maddesiyle genel, Tele Medya Kanunu (TMK) 15a ve TK 93(3) maddeleriyle ise sektörel düzenleme getirilmiştir (Runte, 2010). Bildirim yükümlülüğünün uygulanacağı veri türleri arasında FVKK'da,

- Hassas veriler,
- Mesleki ya da resmi gizliliği gerektiren kişisel veriler (doktorlar tarafından hastalara ilişkin tutulan veriler),
- İdari veya kriminal suçlara ilişkin veriler,
- Kredi kartı veya banka hesap detayları

yer alırken TK'da hizmet sağlayıcılar tarafından tutulan müşteri verileri veya trafik verileri sayılmıştır. Düzenlemelere göre bildirim yükümlülüğü, yasa dışı veri transferinin veya üçüncü taraflar tarafından verilere yetkisiz erişimin bireylerin hak ve menfaatleri üzerinde ciddi bir etki oluşturma ihtimali bulunması halinde gerçekleşecektir. Veri ihlalinden çok sayıda kişinin etkilenmesi halinde bildirim, günlük ulusal gazetelerde en az yarım sayfalık ilan şeklinde yapılacaktır (Hladjk, 2009).

Alman Ceza Mahkemeleri tarafından görülen bir dava, veri gizliliği yasalarının artan önemini göstermesi açısından önemlidir. 2005 yılında Alman magazin dergisi Kapital'de, telekomünikasyon şirketi Deutsche Telekom (DT)'un orta vadeli planları hakkında bilgi veren bir makalenin yayımlanmasının ardından DT, şirket içi bilgileri sızdıran kişileri tespit etmek amacıyla Güvenlik Departmanını görevlendirmiştir. Veri sızıntısını tespit etmek amacıyla 2005 ve 2006 yıllarında Güvenlik Departmanı tarafından 40'tan fazla gazeteci, sendikacı ve kurul üyesinin telefon verileri elde edilmiş ve bu veriler analiz edilmiştir. Bu tür bir tespitin yapıldığı ortaya çıktıktan sonra yapılan ceza soruşturmasında Bonn Bölge Mahkemesi, Güvenlik Departmanı Müdürü Trzeschan'ın telefon verilerini elde etmesi ve kullanmasının

telekomünikasyonun gizliliği düzenlemesine aykırı olduğuna hükmetmiş ve Trzeschan'ı 3,5 yıl hapis cezasına çarptırmıştır (Linklaters, 2011).

2 Mart 2011 tarihinde Alman Hükümeti, Vatandaş Hakları Direktifi doğrultusunda TK'nın ilgili maddelerini revize eden kanun tasarısını kabul etmiştir. Tasarıya göre telekomünikasyon şirketleri, veri ihlallerini telekomünikasyon düzenleyici otoritesi BNetzA ile Alman Bilgi Özgürlüğü ve Veri Koruma Komiserliği'ne bildirecektir. Bildirim yükümlülüğünün içeriğine ilişkin detaylı bilgilerin de yer aldığı tasarıda, şirketlerin veri ihlallerini kayıt altına almaları da düzenlenmektedir (Hunton-Williams, 2011).

4.3 Fransa

Fransa'da E-Gizlilik Direktifi, 21 Haziran 2004 tarihli Dijital Ekonomide Güven Kanunu (DEGK) ve 9 Temmuz 2004 tarihli Elektronik Haberleşme Kanunu ile ulusal mevzuata aktarılmıştır (Ylouses ve Gay, 2011).

15 Kasım 2001 tarihli Günlük Güvenlik Kanunu (GKK) ile Fransa'da internet servis sağlayıcılarının, müşterilerine ait trafik verilerini 1 yıla kadar saklamaları ve adli otoritelerin bu verilere erişimlerine izin vermeleri düzenlenmiştir. DEGK'da da veri saklama ile hükümler yer almış, internet servis sağlayıcılarına trafik verileri yanında abonelerin ad ve adres gibi tanımlama verilerini de muhafaza etmeleri yükümlülüğü getirilmiştir (PI, 2011a).

23 Ocak 2006 tarihli Anti-terör Kanununda polis güçleri ve istihbarat birimlerinin terör olaylarının engellenmesi amacıyla yargı kararı olmadan, internet servis sağlayıcıları tarafından saklanan verilere erişebilecekleri belirtilmiş (PI, 2011a), Fransız Anayasa Komisyonu (Mahkeme), kanunun ilgili maddelerinin yeterli güvenlik tedbirleri öngördüğünü belirterek anayasaya aykırılık olmadığına hükmetmiştir (EDRI, 2006). Telekomünikasyon verilerinin saklanmasına ilişkin 24 Mart 2006 tarihli

Kararnameyle ise telekomünikasyon işletmecileri tarafından içerik hariç telefon ve internet haberleşmesine ilişkin verilerin 1 yıl süreyle saklanması düzenlenmiştir (PI, 2011a). Bu çerçevede Fransa'da veri saklama yükümlülüğü internet servis sağlayıcıları ile başlayıp telefon hizmet sağlayıcılarıyla genişletilmiş ve Veri Saklama Direktifine uyum sağlanmıştır.

Fransa'da Paris toplu taşıma sistemi için oluşturulan platformun internet sayfasında kimlik numarası girilerek binlerce kişinin kişisel bilgilerine kolaylıkla erişilebildiği anlaşılınca, platforma erişim kapatılmıştır. Benzer şekilde, internet servis sağlayıcısı Orange, şirketin internet sayfasında yer alan URL adresinin son kısmındaki numaralarının değiştirilmesiyle 400.000 abonenin kişisel verilerine kolaylıkla erişebileceğini fark etmesi üzerine internet sayfasını erişime kapatmak zorunda kalmıştır. Bu tür olaylar Fransa'da veri kontrolörlerine, yetkili otoritelere veya etkilenen bireylere veri ihlallerinin bildirilmesi yönünde bir yükümlülük getirilip getirilmemesi hususunu gündeme getirmiştir (Proust, 2009a).

Mevcut durumda güvenlik ihlallerinin yetkili otoritelere (CNIL veya ARCEP[6]) veya bireylere bildirilmesine yönelik doğrudan bir yükümlülük bulunmamakla birlikte Fransa Veri Koruma Kanunu'nun (FVKK) 34 üncü maddesiyle güvenlik ihlali yaşanmaması için veri kontrolörleri/işleyicilerinin gerekli tedbirleri almaları istenmektedir. FVKK'nın 2004 yılında tadil edilmesiyle CNIL'in, kişisel verilerin FVKK'ya uygun biçimde işlenmesinin sağlanması yönündeki yetkisi güçlendirilmiştir. Bu çerçevede CNIL uyarı, para cezası, veri işlemenin durdurulması, yetkilendirmenin geri alınması gibi yaptırımlar uygulayabilmektedir.

2006 yılında internet servis sağlayıcısı Free SAS, telefon rehberinde yer almak istemeyen 120.000 abonesinin iletişim bilgilerini rehberlik hizmeti sağlayıcılarına aktarmış, abonelerden gelen yoğun şikâyetler üzerine CNIL

---

[6] Fransa Elektronik Haberleşme ve Posta Düzenleyici Otoritesi

tarafından yapılan incelemede sorunun veri transferinde kullanılan yazılımdaki hatadan kaynaklandığı tespit edilmiştir. CNIL, FVKK 34 üncü maddenin ihlal edildiğini belirterek bu tür bir ihlalin gelecekte yaşanmamasını teminen gerekli teknik ve idari tedbirlerin alınması konusunda şirketi uyarmıştır (Proust, 2009a).

Fransa'da 6 Kasım 2009 tarihinde dijital çağda özel hayatın gizliliğinin daha iyi korunması hakkında bir kanun tasarısı hazırlanmıştır. Tasarıda kişisel veri tanımına, "*bir şebekeye bağlanan terminal cihazı tanımlayan adres veya numara*" ifadesi eklenerek IP adreslerinin de kişisel veri kapsamına dâhil edilmesi amaçlanmaktadır. Tasarı ayrıca veri güvenliği ihlali durumunda CNIL'e bildirim yapmaları konusunda işletmecilere yükümlülük getirmektedir. İhlalin kişisel verileri etkilemesi durumunda veri kontrolörleri, ihlalden etkilenen bireylere de bildirimde bulunacaktır. Böylece sadece telekomünikasyon şirketleri ve internet servis sağlayıcıları için değil bütün veri kontrolörleri için bildirim yükümlülüğü getirilerek Vatandaş Hakları Direktifinin bir adım ilerisine geçilmiş olacaktır (Proust, 2009b). Tasarı, kişisel veri işleyen veya kişisel verilere erişen personel sayısı 50 den fazla olan organizasyonların veri koruma direktörlüğü kurmalarını da öngörmektedir. Senato bu işlevin, kişisel verilerin ve gizliliğinin korunmasında bilinçlenmenin artması ve gizlilik kültürünün gelişmesinde önemli bir rol oynayacağını düşünmektedir (Proust, 2010). Fransız Ulusal Meclisi tarafından gözden geçirilmekte olan tasarı henüz yürürlüğe girmemiştir (PI, 2011a).

Diğer yandan, AB tarafından yayımlanan Telekom reform paketinin ulusal mevzuata aktarılması çalışmalarını sürdüren Fransa Ekonomi, Sanayi ve Çalışma Bakanlığının hazırladığı kanun tasarısında da elektronik haberleşme hizmeti sağlayıcılarına kişisel veri ihlallerini, ihlalden etkilenen bireylere ve CNIL'e bildirme yükümlülüğü getirilmektedir (PI, 2011a).

4.4 İspanya

E-Gizlilik Direktifi, 3 Kasım 2003 tarihli Genel Telekomünikasyon Kanunu (GTK) ve 424/2005 sayılı Kraliyet Kararnamesi ile İspanya ulusal mevzuatına aktarılmış (Coast, 2011), 34/2002 sayılı Bilgi Toplumu Hizmetleri ve Elektronik Ticaret Kanunu'nda (BTHETK) ise istek dışı haberleşmeyle ilgili hükümler yer almıştır (Linklaters, 2010).

BTHETK'nın 21 inci maddesiyle alıcıların onayı alınmadan e-posta veya benzeri elektronik haberleşme vasıtalarıyla reklam veya promosyon amaçlı haberleşme yasaklanmaktadır. Gönderici ile alıcı arasında sözleşmeye dayalı bir ilişki bulunması ve benzeri ürünlerin reklamının yapılması halinde ise önceden onay şartı aranmamaktadır. İstek dışı haberleşmeyle ilgili hükümlerin ihlal edilmesi halinde İspanya Veri Koruma Otoritesi AEPD'ye yaptırım uygulama yetkisi verilmiştir (AEPD, 2005).

2004 yılında, bir İspanyol hukuk Şirketi 2670 müşterisine lisansüstü eğitim reklamı içeren bir e-posta göndermiş; bir e-posta alıcısı Şirketten, iletişim bilgilerinin veritabanından silinmesini talep etmesine rağmen birkaç gün içinde ikinci bir e-posta almıştır. Bunun üzerine BTHETK'nın ihlal edildiği gerekçesiyle müşteki AEPD'ye başvurmuştur. Özel bir firmada çalışan müşteki, 2003 yılında yasal danışmanlık için şirketten tahmini ücret değeri talep etmiş ve iletişim bilgilerinin yer aldığı kartvizitini şirket temsilcisine vermiştir. Şirket, müştekinin fiyat teklifi talep etmesi ve kartvizitini vermesinin dolaylı olarak sözleşme ilişkisi anlamına geleceğini beyan etmiş ancak AEPD, müştekinin talep ettiği hizmetle şirketin yaptığı reklamın benzer ürün ve hizmet kapsamında değerlendirilemeyeceğini, ayrıca müştekinin açık, belirli ve bilgilendirilmeye dayalı rızasının alınmadığını, üstelik gönderilen e-postalarda opt-out seçeneğinin sunulmadığını belirterek şirkete 30.000 Euro para cezası vermiştir (Benalal ve Rodriguez, 2006).

Veri Saklama Direktifinin iç hukuka aktarılması kapsamında 25/2007 sayılı Kanunla, elektronik haberleşme hizmetlerine ilişkin verilerin operatörler tarafından 12 ay süre ile saklanması ve verilerin yetkili otoriteye ancak yargı kararı ile verilebilmesi düzenlenmiştir. (Aldama ve Cruz, 2009).

Vatandaş Hakları Direktifinin AB üyesi ülkelerde mevzuata aktarılma çalışmaları devam ederken bazı ülkelerde, veri ihlalleri hakkında yetkili otoritelere ve/veya ilgili kişilere bildirimde bulunulması ya da bir inceleme/soruşturma aşamasında düzenleyici otoriteler tarafından ulaşılabilecek veri ihlalleri kayıt kütüğü tutulmasına ilişkin düzenlemelerin yer aldığı görülmektedir. Nitekim İspanya'da 1720/2007 sayılı Kraliyet Kararnamesi ile veri kontrolörlerine güvenlik politikaları kapsamında yükümlülükler getirilmekte, örneğin kişisel verileri etkileyen vakaların yönetilmesi ve bildirilmesi için bir prosedür oluşturulması; vakanın türü, gerçekleşme zamanı, kime bildirim yapıldığı gibi hususların bir kayıt kütüğünde tutulması istenmektedir (ENISA, 2011).

4.5 Hollanda

E-Gizlilik Direktifinin 13(4) maddesi Ekonomik Suçlar Kanunu, diğer maddeleri ise 19 Mayıs 2004 tarihinde yürürlüğe giren Telekomünikasyon Kanunu (TK) ile Hollanda ulusal mevzuatına aktarılmıştır (EU, 2005).

İstek dışı haberleşmeyle ilgili mevzuat hükümleri sadece gerçek kişileri kapsarken 22 Ocak 2008 yılında TK'da yapılan değişiklikle tüzel kişiler de kapsama dâhil edilmiştir. Ancak tüzel kişilerle yapılacak haberleşme açık rızayı gerektirmemekte, örneğin tüzel kişinin elektronik iletişim bilgilerini vermesi rızayla eşdeğer olarak kabul edilmektedir (IBLS, 2009). Ayrıca 1 Ekim 2009 tarihinden itibaren, tele pazarlama amaçlı yapılacak her bir telefon çağrısında aranan tarafa opt-out kayıt kütüğü hakkında bilgi verilmesi zorunlu kılınmıştır (PI, 2011b).

2008 yılında Hollanda'da Abodata şirketiyle resmi ortaklığı bulunan Calldata adlı şirket Abodata'da bulunan boş iş pozisyonları hakkında tüketicilere gönderici adı Abodata olan e-postalar göndermiş ve ilanla ilgilenenlerin 0900' lü numaraları aramaları istenmiştir. Posta ve Telekomünikasyon Otoritesi OPTA'ya gelen şikâyetler üzerine yapılan inceleme sonrasında iki şirkete toplam 510.000 Euro para cezası verilmiştir. Calldata kendisine verilen 270.000 Euro para cezasına itiraz etmemiş ancak Abodata istek dışı e-postaların kendisi tarafından gönderilmediğini ve diğer şirketle doğrudan pazarlama faaliyetlerinde bir ortaklığı bulunmadığını belirterek Mahkemeye başvurmuştur. Mahkeme, Abodata şirketini haklı bulurken Calldata'ya verilen ceza onanmıştır (Stibbe, 2010).

2009 yılında da SMS hizmet sağlayıcısı SD&P adlı bir şirket tüketicilere gönderdiği mesajlarda, bir kısa mesaj numarasına mesaj atarak servise kaydolan tüketicilerin iPhone veya dizüstü bilgisayar kazanabileceklerini belirtmiş ancak belirtilen numaraya mesaj atan tüketicilerin ücretli bir servise abone oldukları ortaya çıkmıştır. Servis kapsamında tüketiciler aldıkları her bir SMS için ise 1,5 euro ücretlendirilmiştir. OPTA yaptığı incelemede şikâyet konusu SMS'lere ilişkin olarak alıcıların açık rızalarının alınmadığını ve tüketicilere mesajların sonunda opt-out seçeneği sunulmadığını belirterek mevzuat aykırılığı tespit etmiş ve şirkete 550.000 Euro para cezası vermiştir (OPTA, 2011).

Veri Saklama Direktifinin uygulanması kapsamında Hollanda Hükümeti 2007 yılında bir yasa tasarısı hazırlamış, tasarıda telefon ve internet trafik verilerinin polis birimleri ve adli otoritelerin ihtiyaçları doğrultusunda 18 ay süre ile saklanması öngörülmüştür. Hollanda Veri Koruma Kurumu tasarıyı eleştirerek veri saklama süresinin tartışmaya mahal bırakmayacak şekilde gerekçelendirilmesi gerektiğini beyan etmiştir. Bu çerçevede, Temsilciler Meclisi tarafından 22 Mayıs 2008 tarihinde kabul edilen ve veri saklama süresinin 12 ay olarak düzenlendiği Telekomünikasyon Veri Saklama Kanunu Senato'ya sevk edilmiştir (PI, 2011b). Senato tarafından onaylanan Kanun 1

Eylül 2009 tarihinde yürürlüğe girmiş olmakla birlikte internet servis sağlayıcıları için veri saklama süresi yükümlülüğünün 6 aya indirilmesi düşünülmektedir (Koops, 2010).

TK'ya göre hizmet sağlayıcıların, şebekelerinin veya sundukları hizmetlerin güvenliğini sağlamak için gerekli teknik ve idari tedbirleri almaları, güvenliği ihlal edecek bir risk olması durumunda da aboneleri bilgilendirmeleri gerekmektedir. Vatandaş Hakları Direktifinin mevzuata aktarılması kapsamında TK'yı tadil eden ve 3 Kasım 2010 tarihinde Parlamento'ya gönderilen yasa tasarısı ile hizmet sağlayıcılara, güvenlik ihlallerinde alınacak önlemlere abonelik sözleşmelerinde yer verilmesi ve güvenlik ihlallerinin kişisel verilerin korunmasında olumsuz etkileri bulunacaksa OPTA'ya ve abonelere bildirilmesi konularında yükümlülük getirilmektedir. Bu yükümlük ise sadece elektronik haberleşme hizmeti sağlayıcılarını kapsamaktadır (Gloudemans ve Lindenkamp, 2010).

4.6 İtalya

İtalya'da elektronik haberleşme sektöründe düzenleyici otorite AGCOM olmakla birlikte kişisel verilerin korunması hususunda GARANTE yetkili otorite konumundadır. 2002 yılında yayımlanan AB Direktiflerinden dördü 1 Ağustos 2003 Elektronik Haberleşme Kanunu ile, E-Gizlilik Direktifi ise 30 Haziran 2003 tarihli Veri Koruma Kanunu (VKK) ile iç hukuka aktarılmıştır. VKK genel olarak 3 bölümden oluşurken ilk bölümde veri koruma ilkeleri, ikinci bölümde sağlık, bankacılık ve finans, telekomünikasyon gibi belirli sektörlerde verilerin korunmasına yönelik alınması gereken önlemler, son bölümde ise yaptırımlar ve yasal haklara ilişkin hükümler yer almaktadır (ENISA, 2010).

VKK'nın 130 uncu paragrafında otomatik arama makineleri, faks ve elektronik iletilerle yapılacak istek dışı haberleşme için opt-in şartı getirilmiş, ancak elektronik iletilerle yapılacak haberleşmede soft-opt-in seçeneği

benimsenmiştir. Telefon rehberlik hizmetleri için oluşturulan veritabanlarının abonelerin bilgisi olmadan tele pazarlama amacıyla birçok şirket tarafından kullanılması abonelerin istek dışı telefon çağrıları almalarına neden olmuş, AK'nın İtalya hakkında başlattığı yasal süreç çerçevesinde, 7 Eylül 2010 tarihli Kararname ile, Ekonomi Bakanlığı denetiminde oluşturulacak kayıt bürosuna kaydolan abonelere tele pazarlama amaçlı aramalar yapılamayacağı düzenlenmiştir.

GARANTE istek dışı haberleşme yapılması halinde veri kontrolörlerine yaptırım uygulayabilmektedir. Örneğin 2008 yılında İtalya'da istek dışı SMS gönderimine ilişkin verilen 570.000 euro para cezası AB üyesi ülkelerde rastlanan en yüksek para cezalarından biridir (SMART, 2009).

30 Mayıs 2008 tarihli ve 109 sayılı Kanun Hükmünde Kararname ile Veri Saklama Direktifi uygulamaya geçirilmiş, saklanacak veri türleri ile veri saklama periyodu için yasal zemin oluşturulmuştur. Bu çerçevede, telefon trafik verileri için 24, internet trafik verileri için ise 12 aylık saklama süresi belirlenmiştir (PI, 2011c). Diğer AB üyesi ülkelerden farklı olarak İtalya'da, başarısız çağrı girişimi için de ayrı bir süre öngörülmüştür. Buna göre, başarısız çağrı girişimlerine ilişkin veriler işletmeciler tarafından 30 gün süre ile saklanacaktır (Cellere ve Mezzapesa, 2010).

Öte yandan, GARANTE tarafından 24 Temmuz 2008 tarihine alınan "İnternet ve telefon trafik verilerinde güvenlik" konulu karar kapsamında elektronik haberleşme hizmeti sağlayıcıları, kişisel verileri işlenen ilgili kişileri korumak amacıyla etkili kimlik doğrulama, yetki verme, şifreleme teknikleri gibi önlemleri almakla yükümlü kılınmıştır (Giampaolo ve Santorsola, 2011). İtalya'da kişisel veri ihlallerinin GARANTE'ye ya da ilgili kişilere bildirilmesi yönünde bir yükümlülük ise henüz getirilmemiştir (Parrillo ve Mezzetti, 2011).

4.7 İrlanda

E-Gizlilik Direktifi genel olarak İrlanda ulusal mevzuatına 6 Kasım 2003 tarihinde yürürlüğe giren 535 sayılı Verilerin Gizliliği ve Korunması Hakkında Yönetmelik (VKGY) ile aktarılmış, Direktifin haberleşmenin gizliliğine ilişkin 5(1) maddesi ise Posta ve Telekomünikasyon Kanununda düzenlenmiştir (ODPC, 2003). İrlanda'da Veri Koruma Komisyonu ODPC, veri koruma alanındaki düzenlemelere uygunluğu denetlerken teknik özellik içeren düzenlemelerde elektronik haberleşme sektöründe düzenleyici otorite ComReg ile koordineli olarak çalışmaktadır (ODPC, 2011a).

VKGY'de istek dışı haberleşmeyle ilgili kapsamlı hükümler yer almaktadır. Ulusal rehberlik veritabanında (URV) kayıtlı bulunan abonelerle telefon aramaları vasıtasıyla doğrudan pazarlama amaçlı haberleşme yapılamayacağı belirtilmiş, URV'de yer almayan aboneler için ise opt-out sistemi benimsenmiştir. (ODPC, 2011b).

URV, evrensel hizmet yükümlüsü işletmeci tarafından oluşturulan ve kamuya açık rehberlerde yer almak isteyen abonelere ait sabit ve mobil numaraların kaydedildiği bir veritabanıdır. 2005 yılında ComReg ve ODPC tarafından doğrudan pazarlama amaçlı aramalar için URV'de yer alan bir opt-out kayıt kütüğü (OKK) faaliyete geçirilmiştir. Ücretsiz bir servis olan OKK, istek dışı telefon aramaları ile tüzel kişilerle yapılacak faks aramalarının engellenmesinde önemli bir rol üstlenmektedir. Numaralarının rehberlerde yer almasını istemeyen abonelere ilişkin bilgiler ise otomatik olarak OKK'ya kaydedilmektedir. Bu çerçevede, telefon veya faks aracılığıyla abonelerle doğrudan pazarlama amaçlı haberleşme yapmak isteyen şirketlerin URV'de sorgulama yapmaları gerekmektedir (ComReg, 2011).

Otomatik arama makineleri veya fakslarla yapılacak doğrudan pazarlama amaçlı haberleşmede opt-in, bu haberleşmenin tüzel kişilerle yapılması halinde ise opt-out yöntemi benimsenmiştir. Bununla birlikte URV'de kayıtlı

tüzel kişilerle yapılacak haberleşmede de opt-in yöntemi kullanılmaktadır. Elektronik iletilerle yapılacak doğrudan pazarlama amaçlı haberleşmede ise gerçek kişiler için opt-in tüzel kişiler için opt-out yöntemi uygulanmakta, gerçek kişilerle şirketler arasında müşteri ilişkisi olması halinde E-Gizlilik Direktifinde belirtilen soft-opt-in yöntemi kullanılmaktadır (ODPC, 2011b).

13 Aralık 2008 tarihli ve 526 sayılı Yönetmelikle VKGY tadil edilmiş ve özellikle istek dışı haberleşmeye ilişkin yeni hükümler getirilmiştir. Bu kapsamda (Neylon, 2009),

- İstek dışı haberleşmeye ilişkin hükümlerin,
  - ✓ Gerçek kişiler tarafından ihlal edilmesi halinde hafif suç için 5.000 Euro ağır suç için 50000 Euro'ya kadar para cezası,
  - ✓ Tüzel kişiler tarafından ihlal edilmesi halinde 250.000 Euro'ya kadar ya da cironun % 10'unun bu miktardan yüksek olması durumunda %10 oranında para cezası,

  verilebilecek, ağır suç soruşturması Savcılık tarafından yürütülebilecektir.
- Cezalar her bir istek dışı arama/mesaj için uygulanacaktır.
- İhlale ilişkin kanuni soruşturmalarda bir abonenin istek dışı haberleşme için verdiği onayın ispat zorunluluğu davalı tarafta olacaktır.

2001 yılında İrlanda'da mobil telefon işletmecilerinin tüketicilerin bilgilerini (konum verileri dâhil) yasal dayanak olmaksızın 6 yıl boyunca sakladıklarının ortaya çıkarılması OPDC'nin söz konusu bilgilerin silinmesi yönünde müdahalesini gerekli kılmıştır. ODCP, İrlanda Hükümeti'nin trafik verilerinin saklanmasına yönelik yasal düzenleme yapmaması üzerine 2005 yılında telekom şirketlerinin söz konusu verileri 12 ay sonunda silmesi yönünde bir karar almış, bu karar Hükümetin Terör Suçları Kanunu (TSK) çıkarmasını tetiklemiştir. TSK'nın 7 nci kısmında sabit/mobil telefon trafik verilerinin 3 yıl süre ile saklanması yükümlülüğü getirilmiş ancak orantılılık ilkesi gözetilmeyerek sadece ciddi suçların değil herhangi bir suçun önlenmesi,

tespit edilmesi, araştırılması ve soruşturulması için söz konusu verilere erişilme imkânı sağlanmıştır (PI, 2011d).

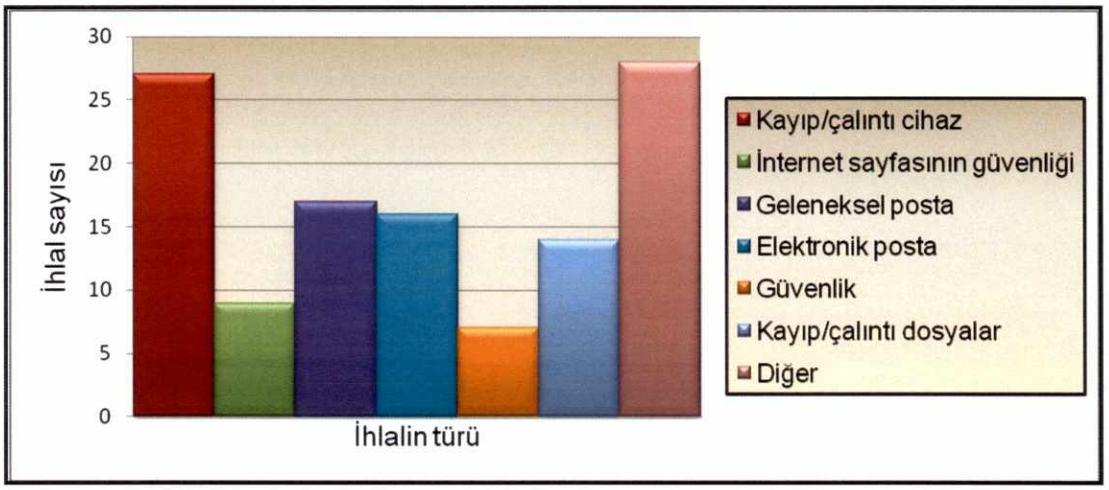
Yasal dayanağının geçersiz olduğu gerekçesiyle İrlanda, Veri Saklama Direktifinin iptali için ADD'ye başvurmuş ancak 2009 yılında bu başvuru reddedilmiştir (PI, 2011d). Direktif, 26 Ocak 2011 tarihli Verilerin Saklanmasına İlişkin Haberleşme Kanunu (VSHK) ile İrlanda mevzuatına aktarılmıştır. VSHK'ya göre, trafik verileri sabit ve mobil telefon işletmecileri tarafından 2 yıl, internet servis sağlayıcıları tarafında ise 12 ay süre ile saklanacaktır. Saklanan verilere ilişkin bilgi talebi ise polis teşkilatı, savunma kuvvetleri ve maliye yetkililerince sadece ciddi suçların (örneğin 5 yıl ve üzeri hapis cezası gerektiren suçlar) önlenmesi, tespit edilmesi, araştırılması ve soruşturulması amacıyla yapılabilecektir (Brennan, 2011).

İrlanda'da son yıllarda veri güvenliği ihlalleri artış göstermiş, örneğin 2007 yılında İrlanda'da bir bankanın 10.000 müşterisine ait şifrelenmemiş kişisel verilerin yer aldığı 4 diz üstü bilgisayar çalınmış, banka ODPC'yi olayın üzerinden 8 ay geçtikten sonra bilgilendirmiş ancak o tarihe kadar kişisel verileri risk altında olan müşterilerine herhangi bir bildirimde bulunmamıştır (EDRI, 2008).

ODPC'ye 2008 yılında 81, 2009 yılında ise 119 adet veri güvenliği ihlali bildirimi yapılmıştır. Bir cihazın çalınması veya kaybolması en fazla bildirilen ihlal türüdür. Diz üstü bilgisayarlar veya flash bellekler yüksek miktarda veri depolayabildiğinden şirketler ve kuruluşlar tarafından bu tür cihazlar üzerinde kişisel verilerin saklanma gerekliliğinin belirlenmesi ve uygun güvenlik tedbirlerinin alınması istenmektedir. Geleneksel posta yoluyla yapılan ihlaller ODPC'ye yapılan veri güvenliği ihlali bildirimi arasında ikinci sırada yer almaktadır. Zarfın yanlış adrese gönderilmesi veya zarfın içinde başka kişilere ait bilgilerin yer alması bireylerin mahremiyetine zarar verebilmektedir. E-posta yoluyla yapılan ihlallerde ise e-posta alıcılarına başka kişilere ait e-posta adresleri gönderilebilmektedir. Bu çerçevede, şirket

ve kuruluşların çok sayıda kişiye gönderilecek e-postalarda gizli karbon kopya (*BCC*) kullanılması ve bütün personelin bu konuda bilinçlendirilmesi gibi tedbirleri almaları bahse konu ihlali engelleyebilecektir (ODPC, 2010). Veri güvenliği ihlali bildirimlerinde rastlanan ihlal türleri Şekil 4.1'de gösterilmektedir.

Şekil 4.1. Veri ihlali türleri



Kaynak: ODPC, 2010

ODPC, 2003 yılında Veri Koruma Kanununda yapılan değişikliklerle birlikte uygulama esasları (*code of practice*) düzenleyebilmekte, bu esaslar İrlanda Parlamentosu tarafından onaylanması halinde hukuki bağlayıcılık kazanmaktadır. Bu kapsamda ODPC, telekomünikasyon sektörüne yönelik olarak 2010 yılı temmuz ayında kişisel verilerin güvenliğinin ihlaline ilişkin uygulama esasları[7] yayımlamıştır. Buna göre (PI, 2011d),

- *Elektronik ya da manüel yöntemle kişisel verilerin güvenliğinin ihlal edilmesi halinde veri kontrolörü ihlalin ilgili kişilere bildirilmesini değerlendirmeli ve gerekirse polis teşkilatı ve finans kurumlarını ihlal hakkında bilgilendirmelidir,*

[7] Detaylı bilgi için bkz. http://www.dataprotection.ie/viewdoc.asp?DocID=901&ad=1

- *Verilerin yüksek standartlarda şifrelenmiş olması halinde veri kontrolörü, risk bulunmadığı ve dolayısıyla ilgili kişileri bilgilendirme gereği olmadığı sonucuna varabilir,*
- *Kişisel veri işleyen taraflar veri ihlali olduğunu tespit eder etmez ilgili veri kontrolörlerini bilgilendirmelidir,*
- *100 den fazla kişiyi etkilememesi, ilgili kişilerin gecikme olmadan bilgilendirilmesi ve hassas kişisel veri veya finansal veri içermemesi halinde bütün veri ihlalleri tespit edildiği andan itibaren iki iş günü içinde ODPC'ye bildirilmelidir,*
- *ODPC, veri ihlalleri hakkında ayrıntılı rapor isteyebilir ve soruşturma yapabilir,*
- *ODPC'ye bildirim yapılmasa dahi, veri kontrolörü her bir veri ihlaline ilişkin kayıt kütüğü tutmalıdır. Kayıt kütüğünde ihlalin niteliği, ODPC'ye bildirim yapılmama gerekçeleri yer almalı, belirtilen kayıt kütükleri talep halinde ODPC'ye iletilmelidir.*

Uygulama esasları mevcut durumda İrlanda Parlamentosu tarafından henüz onaylanmadığı için hukuki bağlayıcılığı bulunmamakta sadece güçlü bir tavsiye niteliği taşımaktadır (Edwards, 2011).

2009 yılında Adalet Bakanlığı bünyesinde Veri Koruma Araştırma Grubu (VKAG) kurulmuştur. Genel olarak veri ihlalleriyle ilgili mevzuatın tadil edilmesi, veri ihlallerinin bildirim formatı, zorunlu bildirim halinde cezaların rolü gibi konularda çalışan grup 2010 yılında bir rapor yayımlamıştır (PI, 2011d). Raporda, veri ihlallerinin ODPC'ye veya ilgili kişilere bildirilip bildirilmeyeceği konusunda şirketlerin karar verdiği öz düzenleme rejiminin pratik bir çözüm olmayacağı, ilgili kişilere doğrudan bildirim yükümlülüğünün yasal düzenlemede yer almayabileceği ancak ODPC'nin kendisine yapılacak bildirim çerçevesinde veri kontrolörlerine, veri ihlallerinin ilgili kişilere bildirilmesi yönünde yaptırım uygulayabileceği belirtilmiş ve şu tavsiyelerde bulunulmuştur (Justice, 2010):

- *Yasal düzenlemelerde genel veri koruma ilkelerinin (güvenlik ilkesi dâhil) ihlal edilmesine ilişkin kriminal hükümlerin yer alması,*
- *Veri ihlallerinin bildirilmesine ilişkin yükümlülüklerin yasal bağlayıcılık içerecek uygulama esasları ile getirilmesi, uygulama esaslarında ODPC tarafından yayımlanan kılavuz esas alınarak veri ihlali bildiriminin zorunlu olacağı koşulların belirlenmesi,*
- *Uygulama esaslarının ODPC tarafından düzenli aralıklarla gözden geçirilmesi,*
- *ODPC tarafından toplumu bilinçlendirme faaliyetlerinin sürdürülmesi.*

5. TÜRKİYE İNCELEMESİ

Çalışmamızın bu bölümünde öncelikle kişisel verilerin işlenmesi, saklanması ve gizliliğinin korunmasına ilişkin Türkiye'deki genel düzenlemeler ele alınacaktır. Müteakiben elektronik haberleşme sektörüne yönelik düzenlemelere yer verilecek ve "Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik[1]" ile "Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik Taslağı"nın AB Direktifleriyle uyumu değerlendirilecektir.

5.1 Genel Düzenlemeler

Ülkemizde kişisel verilerin işlenmesi, saklanması ve gizliliğinin korunması hususu sadece elektronik haberleşme sektörüne özgü düzenlemelerde değil Anayasada ve çeşitli kanunlarda da yer almaktadır.

5.1.1 Anayasa

2010 yılında yapılan referandumda kabul edilen Anayasa değişikliği paketiyle 1982 Anayasasının[2] kişinin hakları ve ödevlerini düzenleyen ikinci bölümünün "Özel hayatın gizliliği" başlıklı 20 nci maddesinde,

> *"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."*

---

[1] 6 Şubat 2004 tarihli ve 25365 sayılı Resmi Gazete.
[2] 13 Mayıs 2010 tarihli ve 27580 sayılı Resmi Gazete.

hükmüne yer verilerek kişisel verilerin korunmasını isteme, ülkemizde temel hak olarak tanınmıştır. Söz konusu maddede kişisel verilerin korunmasını isteme hakkının kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsadığı belirtilmek suretiyle, kişisel verilerin korunması amacıyla kişilerin talep haklarının çerçevesi çizilerek bu hususun anayasal güvence altına alındığı görülmektedir. Diğer taraftan kişisel verilerin korunmasına yönelik usul ve esasların kanunla düzenleneceği belirtilerek kişisel verilerin ancak kanunda öngörülen hallerde veya kişinin açık rızasının bulunması kaydıyla işlenebileceği hükme bağlanmıştır.

Bu kapsamda, AB'nin 2010 yılı Türkiye ilerleme raporunda kişisel verilerin korunması ve bilgiye erişim konularında ilerleme kaydedildiği belirtilmiştir (ABGS, 2010).

5.1.2 Türk Ceza Kanunu

12 Ekim 2004 tarihli ve 25611 sayılı Resmi Gazete'de yayımlanan 5237 sayılı Türk Ceza Kanunu'nun (TCK) "Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar" başlıklı dokuzuncu bölümünde haberleşmenin gizliliği yanında kişisel verilerle ilgili hükümlere yer verilmektedir. TCK'nın 135, 136 ve 138 inci maddeleri kapsamında kişisel verilerin kaydedilmesi, hukuka aykırı olarak verilmesi ya da ele geçirilmesi ile yok edilmemesi halleri suç olarak kabul edilmiş ve hapis cezası öngörülmüştür. Nitekim TCK'nın,

- *135 inci maddesinde kişisel verileri hukuka aykırı olarak kaydeden kimse ile kişilerin siyasî, felsefî veya dinî görüşlerine, ırkî kökenlerine; hukuka aykırı olarak ahlâkî eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgileri kişisel veri olarak kaydeden kimseler hakkında altı aydan üç yıla kadar,*

- *136 ncı maddesinde kişisel verileri hukuka aykırı olarak elde eden, yayan veya bir başkasına aktaran kimse hakkında bir yıldan dört yıla kadar,*
- *138 inci maddesinde Kanunlarda öngörülen süreler bitmiş olmasına rağmen kişisel verileri silmekle yükümlü olanların görevlerini yerine getirmemeleri durumunda altı aydan bir yıla kadar*

hapis cezası öngörülmektedir. TCK'nın "Bilişim Alanında Suçlar" başlıklı onuncu bölümünde yer alan 243 ve 244 üncü maddelerinde bilişim sistemine girme, sistemi engelleme, bozma, verileri yok etme veya değiştirme suçları için çeşitli cezalar ile bu cezaların ağırlaştırıcı hallerine yer verilmektedir. Bahse konu suçlar için TCK 140 ve 246 ncı maddelerinde ise tüzel kişiler hakkında güvenlik tedbirleri uygulanacağı belirtilmektedir.

5.1.3 Türk Medeni Kanunu ve Borçlar Kanunu

Kişisel verilerin hukuka aykırı olarak işlenmesi TCK kapsamında suç oluşturmakla birlikte kişilik haklarının ihlali anlamına da gelmektedir. Bu kapsamda, kişisel verileri hukuka aykırı olarak işlenen kişilerin Türk Medeni Kanunu (TMK) ve Borçlar Kanunu'nda düzenlenen kişilik haklarını koruyan davalara başvurması mümkündür. Nitekim kişisel verileri hukuka aykırı bir şekilde işlenen kimse TMK'nın 25 inci maddesi uyarınca, bu işlemenin önlenmesi, kaldırılması ve tespiti talebiyle dava açma hakkı bulunduğu gibi (Iscturkey, 2010) zarara uğramış ise maddî ve manevî tazminat istemleri ile hukuka aykırı saldırı dolayısıyla elde edilmiş olan kazancın kendisine verilmesine ilişkin istemde bulunma hakkına da sahiptir.

Diğer taraftan, 6098 sayılı Türk Borçlar Kanunu'nun (TBK) 58 inci maddesi kapsamında, kişilik hakkının zedelenmesinden zarar gören kişinin manevi tazminat talep edebilmesi mümkündür. Bu çerçevede, otomatik ya da geleneksel metotlarla kişisel verileri hukuka aykırı olarak işleyen kişiler,

kusurun ağırlığına bakılmaksızın manevi tazminat yükümlüsü olacaklardır (Iscturkey, 2010).

5.1.4 Elektronik İmza Kanunu

Elle atılan imza ile aynı hukukî sonucu doğuran güvenli elektronik imzanın kullanımına ilişkin esasları düzenleyen 5070 sayılı Elektronik İmza Kanununun "Bilgilerin korunması" başlıklı 12 nci maddesi,

> *"Elektronik sertifika hizmet sağlayıcısı;*
> *a) Elektronik sertifika talep eden kişiden, elektronik sertifika vermek için gerekli bilgiler hariç bilgi talep edemez ve bu bilgileri kişinin rızası dışında elde edemez,*
> *b) Elektronik sertifika sahibinin izni olmaksızın sertifikayı üçüncü kişilerin ulaşabileceği ortamlarda bulunduramaz,*
> *c) Elektronik sertifika talep eden kişinin yazılı rızası olmaksızın üçüncü kişilerin kişisel verileri elde etmesini engeller. Bu bilgileri sertifika sahibinin onayı olmaksızın üçüncü kişilere iletemez ve başka amaçlarla kullanamaz."*

hükmünü içermektedir. Söz konusu kanun hükmü ile, kişisel verilerin hizmetin gerektirdiği kapsamda ve rızaya dayalı olarak elde edilmesi, bu verilerin kişilerin rızası olmadan üçüncü taraflara aktarılmaması ve başka amaçlarla işlenmemesi hususları düzenlenmiştir.

5.1.5 Bilgi Edinme Hakkı Kanunu

4982 sayılı Bilgi Edinme Hakkı Kanununda özel hayatın ve haberleşmenin gizliliğine ilişkin hükümlere yer verilmektedir. Buna göre,

- *Kişinin izin verdiği hâller saklı kalmak üzere, özel hayatın gizliliği kapsamında, açıklanması hâlinde kişinin sağlık bilgileri ile özel ve aile*

hayatına, şeref ve haysiyetine, meslekî ve ekonomik değerlerine haksız müdahale oluşturacak bilgi veya belgeler, bilgi edinme hakkı kapsamı dışındadır. Kamu yararının gerektirdiği hâllerde, kişisel bilgi veya belgeler, kurum ve kuruluşlar tarafından, ilgili kişiye en az yedi gün önceden haber verilerek yazılı rızası alınmak koşuluyla açıklanabilir (md. 21),

- *Haberleşmenin gizliliği esasını ihlâl edecek bilgi veya belgeler, bu Kanun kapsamı dışındadır (md. 22).*

Bu çerçevede, kişisel verilerin ilgilinin rızası olmaksızın üçüncü taraflara ifşa edilmesinin önüne geçebilmek amacıyla *açıklanması hâlinde kişinin sağlık bilgileri ile özel ve aile hayatına, şeref ve haysiyetine, meslekî ve ekonomik değerlerine haksız müdahale oluşturacak bilgi veya belgelerin bilgi edinme hakkı kapsamında bulunmadığı* belirtilmek suretiyle bireyin mahremiyetinin korunmaya çalışıldığı görülmektedir.

5.1.6 Kişisel Verilerin Korunması Kanun Tasarısı

AB uyum sürecinde 95/46/EC sayılı Veri Koruma Direktifi kapsamında kişisel verilerin korunmasına ilişkin kanun tasarısını hazırlamak üzere ilk komisyon 13 Eylül 1995 tarihinde oluşturulmuş, çalışmasını tamamlayamayan komisyonun 18 Eylül 2000 tarihinde yeniden oluşturulmasını müteakiben 2003 yılında KVKKT hazırlanmıştır. Biri geçici toplam 42 maddeden oluşan tasarı 22 Nisan 2008 tarihinde Türkiye Büyük Millet Meclisi Başkanlığına gönderilmiştir (Gülmez, 2008).

KVKKT'nin henüz yasalaşmamış olması kişisel verilerin korunması alanında büyük bir boşluk oluşturmaktadır. Nitekim 2010 yılında düzenlenen Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansının sonuç bildirgesinde söz konusu tasarının bir an önce yasalaşmasının önemli bir boşluğu dolduracağı hususuna yer verilmiştir (Iscturkey, 2010). Diğer taraftan kişisel verilerin korunmasına yönelik usul ve esasların düzenlendiği söz konusu

kanun tasarısının bir an evvel yasalaşması Anayasa'nın 20 nci maddesi gereğinin yerine getirilmesi bakımından faydalı olacaktır.

AB'nin 2009 yılı Türkiye ilerleme raporunda da kişisel verilerin korunması alanındaki mevzuatın yetersizliğine vurgu yapılarak kişisel verilerin korunması alanındaki düzenlemelerin, başta Veri Koruma Direktifi olmak üzere verilerin korunmasına dair diğer AB mevzuatı ile uyumlaştırılması ve bu kapsamda tam bağımsız bir veri koruma denetçisinin kurulması gerektiği belirtilmektedir (ABGS, 2009).

5.1.7 Elektronik Ticaretin Düzenlenmesi Hakkında Kanun Tasarısı

AB'nin 2000/31/EC sayılı Elektronik Ticaret Direktifine uyum kapsamında Adalet Bakanlığı tarafından hazırlanan Elektronik Ticaretin Düzenlenmesi Hakkında Kanun Tasarısı 26 Temmuz 2010 tarihinde Türkiye Büyük Millet Meclisi Başkanlığına gönderilmiştir.

Tasarı, elektronik araçlarla yapılan sözleşmelerde bilgi verme ve hizmeti sunanlar için getirilen yükümlülükler ile istenmeyen elektronik postalara ilişkin hükümler olmak üzere genel itibarıyla iki alanda düzenleme yapmaktadır (KGM, 2010). Tasarının 6 ncı maddesi birinci fıkrasında *"Ticarî elektronik iletiler, alıcılara ancak önceden onayları alınmak kaydıyla gönderilebilir. Bu onay, yazılı olarak veya her türlü elektronik iletişim araçlarıyla alınabilir."* hükmüne yer verilerek opt-in sistemi öngörülmüştür. Aynı maddenin ikinci fıkrasında ise esnaf ve tacirlere önceden onay alınmaksızın ticari elektronik ileti gönderilebileceği belirtilmektedir. Böylece esnaf ve tacirlere gönderilecek ticari iletiler için opt-out sisteminin benimsendiği görülmektedir.

Tasarıda kişisel verilerin korunması ile ilgili hükümler de yer almaktadır. Buna göre hizmet sağlayıcılar,

- *Kanun çerçevesinde yapmış olduğu işlemler nedeniyle elde ettiği kişisel verilerin saklanmasından ve güvenliğinden sorumludur,*
- *Kişisel verileri ilgili kişinin onayı olmaksızın üçüncü kişilere iletemez ve başka amaçlarla kullanamaz.*

5.2 Elektronik Haberleşme Sektörüne Yönelik Düzenlemeler

Elektronik haberleşme sektöründe kişisel verilerin korunmasına yönelik çerçeveyi şu başlıklar altında incelemek mümkündür:

- Elektronik Haberleşme Kanunu,
- Elektronik Haberleşme Sektöründe Tüketici Hakları Yönetmeliği,
- Elektronik Haberleşme Sektörüne İlişkin Yetkilendirme Yönetmeliği,
- Elektronik Haberleşme Güvenliği Yönetmeliği,
- Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik.

5.2.1 Elektronik Haberleşme Kanunu

10 Kasım 2008 tarihli ve 27050 (Mükerrer) sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren Elektronik Haberleşme Kanunu (EHK) veri gizliliğine ilişkin hükümler getirmektedir. EHK'nın "Kurumun görev ve yetkileri" başlıklı 6 ncı maddesinin birinci fıkrası (c) bendinde,

> *"Abone, kullanıcı, tüketici ve son kullanıcıların hakları ile kişisel bilgilerin işlenmesi ve gizliliğinin korunmasına ilişkin gerekli düzenlemeleri ve denetlemeleri yapmak."*

hükmü yer almaktadır. Aynı Kanunun "İşletmecilerin hak ve yükümlülükleri" başlıklı 12 nci maddesinin ikinci fıkrası (d) bendiyle; BTK'nın sektörün ihtiyaçları, uluslararası düzenlemeler, teknolojide meydana gelen gelişmeler

gibi hususları gözeterek işletmecilere kişisel veri ve gizliliğin korunması hususunda yükümlülük getirebileceği düzenlenmiştir.

EHK'nın "Kişisel verilerin işlenmesi ve gizliliğin korunması" başlıklı 51 inci maddesinin birinci fıkrasıyla ise BTK'ya, elektronik haberleşme sektörüyle ilgili kişisel verilerin işlenmesi ve gizliliğinin korunmasına yönelik usul ve esasları belirleme yetkisi verilmiştir. Ancak EHK'da istek dışı haberleşme dışında kişisel verilerle ilgili hükümlere yer verilmediği, kişisel verilerin korunması ile ilgili diğer düzenlemelerin ise ikincil mevzuata bırakıldığı görülmektedir. Daha önce izah edildiği üzere Anayasanın, "*Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir.*" şeklindeki 20 nci maddesi uyarınca kişisel verilerin işlenmesi ve gizliliğin korunması ile ilgili usul ve esasların kanununla düzenlenmesi gerekmektedir. Bu nedenle, Anayasa'nın ilgili hükmüne uygun olarak elektronik haberleşme sektöründe de kişisel verilerin işlenmesi ve gizliliğinin korunmasına ilişkin usul ve esasları içeren hükümlerin ikincil düzenlemelere bırakılmaksızın kanunda yer alması uygun olacaktır. Bu çerçevede, EHK'da gerekli değişikliklerin yapılarak elektronik haberleşme sektöründe kişisel verilerin işlenmesi ve gizliliğinin korunması hususu kanuni güvence altına alınmalıdır.

İstek dışı haberleşmeyle ilgili olarak EHK'nın 50 nci maddesi beşinci fıkrasında,

> *"Abonenin önceden izni alınmadan otomatik arama makineleri, fakslar, elektronik posta, kısa mesaj gibi elektronik haberleşme vasıtalarının kullanılması suretiyle doğrudan pazarlama, siyasi propaganda veya cinsel içerik iletimi gibi maksatlarla istek dışı haberleşme yapılması halinde, abone ve kullanıcılara gelen her bir mesajı bundan sonrası için almayı reddetme hakkı kolay bir yolla ve ücretsiz olarak sağlanır."*

hükmü yer almaktadır. Maddede, doğrudan pazarlama dışında siyasi propaganda veya cinsel içerik iletimi maksadıyla yapılacak haberleşmeye de yer verilerek istek dışı haberleşmenin kapsamı, E-Gizlilik Direktifine göre daha geniş tutulmuştur. Ancak herhangi bir elektronik haberleşme vasıtasıyla yapılacak istek dışı haberleşme için opt-out sisteminin benimsendiği, bu sistemin ise E-Gizlilik Direktifine benimsenen opt-in sistemine uygun olmadığı görülmektedir.

Bu kapsamda, Elektronik Ticaretin Düzenlenmesi Hakkında Kanun Tasarısında,

> *"5/11/2008 tarihli ve 5809 sayılı Elektronik Haberleşme Kanununun 50 nci maddesinin beşinci fıkrası aşağıdaki şekilde değiştirilmiştir: Abone ve kullanıcılarla, önceden izinleri alınmaksızın otomatik arama makineleri, fakslar, elektronik posta, kısa mesaj gibi elektronik haberleşme vasıtalarının kullanılması suretiyle doğrudan pazarlama, siyasi propaganda veya cinsel içerik iletimi gibi maksatlarla istek dışı haberleşme yapılamaz. Abone ve kullanıcılara, verdikleri izni geri alma hakkı kolay ve ücretsiz bir şekilde sağlanır."*

hükmüne yer verilerek E-Gizlilik Direktifine uyum sağlanmaya çalışıldığı görülmektedir.

5.2.2 Elektronik Haberleşme Sektöründe Tüketici Hakları Yönetmeliği

5809 sayılı EHK'ya dayanılarak hazırlanan ve elektronik haberleşme hizmetlerinden yararlanan tüketicilerin haklarını ve menfaatlerini korumaya yönelik usul ve esasları düzenleyen Elektronik Haberleşme Sektöründe Tüketici Hakları Yönetmeliği 28 Temmuz 2010 tarihli ve 27655 sayılı Resmi Gazete'de yayımlanarak yürürlüğe girmiştir.

Yönetmeliğin 4 üncü maddesinde kişisel veri tanımına yer verilmekte, kavram "*Belirli veya kimliği belirlenebilir gerçek veya tüzel şahıslara ilişkin bütün bilgiler*" olarak tanımlanmaktadır.

Yönetmeliğin 5 inci maddesinde *"abonelerin kişisel verilerinin kamuya açık rehberlerde yer alıp almamasını talep etmeleri"* tüketici hakları arasında sayılırken 15 inci maddenin dördüncü fıkrasında ise "*Telefon hizmetlerinde, sunulan elektronik ve/veya yazılı rehber hizmetleri için abonelik sözleşmesi imzalanırken, aboneden bu rehberlerde kişisel verilerinin yer alıp almayacağı hususunda onayı alınır.*" hükmüne yer verilmektedir. Böylece E-Gizlilik Direktifinin abone rehberleriyle ilgili maddesi (12/2) doğrultusunda, abonelik sözleşmesi imzalanırken aboneler kişisel verilerinin kamuya açık bir rehberde yer alıp almamasını belirleyebilmektedir.

Yönetmeliğin 15 inci maddesinin ikinci fıkrası,

> *"İşletmecinin kendisi ya da üçüncü şahıslar tarafından otomatik arama makineleri, fakslar, elektronik posta, kısa mesaj gibi elektronik haberleşme vasıtaları kullanılmak suretiyle, doğrudan pazarlama, siyasi propaganda veya cinsel içerik iletimi gibi maksatlarla haberleşme yapılması halinde, gelen her bir mesajı ya da iletiyi bundan sonrası için almayı reddetme hakkı işletmeciler tarafından kısa mesaj, çağrı merkezi ve benzeri yollarla kolay bir usulle ücretsiz olarak sağlanır."*

hükmünü amirdir. Burada da EHK ile benzer biçimde opt-out sistemi benimsenmiştir. Ancak fıkranın AB Direktifleriyle uyumlu hale getirilmesi yerinde olacaktır[3].

---

[3] Detaylı bilgi için bkz. 5.2.6

5.2.3 Elektronik Haberleşme Sektörüne İlişkin Yetkilendirme Yönetmeliği

5809 sayılı EHK'ya dayanılarak hazırlanan ve elektronik haberleşme hizmet, şebeke ve altyapılarına ilişkin yetkilendirmeye[4] yönelik usul ve esasları belirleyen Elektronik Haberleşme Sektöründe Yetkilendirme Yönetmeliği 28 Mayıs 2009 tarihli ve 27241 sayılı Resmi Gazete'de yayımlanarak yürürlüğe girmiştir. Yönetmeliğin 19 uncu maddesinin ikinci fıkrasının (ç) bendiyle işletmeciler, kişisel verilerin gizliliğinin korunmasına ilişkin düzenlemelere uymakla yükümlü kılınmaktadır. Aynı maddenin birinci fıkrasının (p) bendiyle ise

- *Haberleşme mahremiyeti ve güvenliği ile şebeke güvenliğinin sağlanması ve korunması için, her türlü tedbirin alınması, altyapı ve sistemlerinde teknolojik uyumun sağlanması,*
- *Elektronik haberleşmeye ilişkin bilgi, belge ve verilerin gerek korunmasında gerekse iletilmesinde gizlilik hükümlerine uyulması,*
- *Kanunla yetkilendirilmiş merci dışında başkasının bu bilgileri elde etmesinin önlenmesi,*
- *Elektronik haberleşme hizmeti, şebeke ve altyapısında kullanılacak cihazlara, yetkisiz kişilerin erişimini ve bozucu/değiştirici müdahalelerini önlemek amacıyla gerekli tedbirlerin alınması*

işletmecilerin hak ve yükümlülükleri arasında sayılmaktadır.

Yönetmelikte trafik bilgilerinin muhafaza edilmesine ilişkin bir hüküm de yer almaktadır. Buna göre, erişim sağlayıcı olan veya telefon hizmeti sunan işletmeci, kullanıcı sayısı, kimlik bilgileri ve görüşme süreleri ile altyapısı üzerinden gerçekleşen görüşmelere ait trafik bilgilerini bir yıl süreyle

---

[4]Yetkilendirme: Elektronik haberleşme hizmetlerinin sunulması ve/veya elektronik haberleşme şebekesi sağlanmasını teminen Şirketlerin, Kurum nezdinde kayıtlanmasını veya kayıtlanmasıyla birlikte bu Şirketlere elektronik haberleşme hizmetlerine özel, belirli hak ve yükümlülükler verilmesi olarak tanımlanmaktadır. Ayrıntılı bilgi için http://www.btk.gov.tr/Duzenlemeler/Hukuki/yonetmelikler/2009/ehsiyy.pdf

muhafaza etmekle yükümlüdür. Bu kapsamda, trafik bilgilerini 1 yıl süreyle saklama yükümlülüğünün Veri Saklama Direktifi ve Taslak Yönetmeliğe uygun olduğu değerlendirilmektedir.

5.2.4 Elektronik Haberleşme Güvenliği Yönetmeliği

5809 sayılı EHK'nın 4 üncü maddesinin birinci fıkrasının (l) bendi ve 12 nci maddesinin ikinci fıkrasının (j) bendine dayanılarak hazırlanan Yönetmeliğin[5] kapsam maddesi,

> 1) *İşletmecilerin fiziksel alan güvenliği, veri güvenliği, donanım-yazılım güvenliği ve güvenilirliği ile personel güvenilirliğinin sağlanması için tehditlerden ve/veya zafiyetlerden kaynaklanan risklerin bertaraf edilmesi veya azaltılmasına ilişkin olarak alacakları tedbirlere yönelik usul ve esasları kapsar.*
> 2) *Kişisel bilgilerin işlenmesi ve gizliliğinin korunması, bu Yönetmelik kapsamı dışındadır.*

şeklindedir. Yönetmelikte yer alan bazı tanımlara ise aşağıda yer verilmektedir:

> ***Veri:*** *Abone ya da kullanıcının elektronik haberleşme şebekesi üzerindeki konum, zaman, trafik bilgileri ile elektronik haberleşmenin içeriği.*
> ***Veri güvenliği:*** *Verinin gizliliği, bütünlüğü ve devamlılığının sağlanması.*

Her ne kadar kişisel bilgilerin işlenmesi ve gizliliğinin korunması Yönetmelik kapsamı dışında tutulmuş olsa da, "abonelerin elektronik haberleşme şebekesi üzerindeki trafik ve konum bilgileri" kişilerle ilişkilendirildiği takdirde

---

[5] http://www.btk.gov.tr/mevzuat/yonetmelikler/dosyalar/elektronikhaberlesmeguvenligi.pdf

kişisel veri olarak değerlendirileceğinden ve veri tanımı kapsamından hareketle veri güvenliği tanımı da kişisel verilerin gizliliği, bütünlüğü ve devamlılığının sağlanması anlamını taşıyacağından bu hususlar dikkate alınarak kapsam maddesinin ikinci fıkrasının gözden geçirilmesi yerinde olacaktır.

Yönetmelikte, elektronik haberleşmeye ilişkin tehdit ve zafiyetlerin bertaraf edilmesi veya en aza indirilmesi amacıyla alınması gereken güvenlik önlemleri,

- Fiziksel alan güvenliği (md. 7),
- Personel güvenilirliği (md. 8),
- Veri güvenliği (md. 9),
- Donanım yazılım güvenliği ve güvenilirliği (md. 10).

başlıklarında incelenmekte, ayrıca işletmecilere TS ISO/IEC 27001 veya ISO/IEC 27001 bilgi güvenliği yönetim sistemi standartlarına uyum sağlama yükümlülüğü getirilmektedir.

Kişisel verilerin işlenmesine ilişkin ilkelerle birlikte veri güvenliği açısından yukarıda belirtilen yükümlülüklerin yerine getirilmesinin kişisel verilerin ve gizliliğin korunmasında etkin bir rol oynayacağı değerlendirilmektedir.

5.2.5 Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik

406 sayılı Telgraf ve Telefon Kanunu ile 2813 sayılı Telsiz Kanununa dayanılarak hazırlanan Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik[6], 6 Şubat 2004 tarihli ve 25365 sayılı Resmi Gazete'de yayımlanarak yürürlüğe girmiştir.

---

[6] http://www.tk.gov.tr/mevzuat/yonetmelikler/dosyalar/Kisisel_Bil_Yon_06_02_04.pdf

Yönetmeliğin genel olarak E-Gizlilik Direktifi kapsamında ele alındığı görülmekle beraber E-Gizlilik Direktifinde yer alan,

- İşletmeciler tarafından elektronik haberleşme şebekelerinin; haberleşme iletiminin sağlanması amacı dışında abone ve kullanıcıların terminal cihazlarında bilgi saklamak veya saklanan bilgilere erişim sağlamak amacıyla ancak ilgili abone ve kullanıcıların, verilerin işlenmesi hakkında açık ve kapsamlı olarak bilgilendirilmeleri, abone ve kullanıcılara verilerin işlenmesini reddetme seçeneği sunulması kaydıyla kullanılabilmesi[7]
- Abone ve kullanıcıların işlenen ve saklanan trafik verilerinin, haberleşmenin iletimi için gerekli olmadığı takdirde silinmesi veya anonim hale getirilmesi[8]
- Trafik verilerinin abonelerin faturalandırılması ve arabağlantı ödemeleri amacıyla işlenebileceği[9],
- Faturalandırma ve arabağlantı ödemeleri amacıyla işlenecek trafik verileri ile bu verilerin işlenme süresi hakkında abone ve kullanıcıların bilgilendirilmesi[10],
- Ayrıntılı fatura alan aboneler ile arayan ve aranan abonelerin mahremiyet haklarını bağdaştırmak amacıyla kullanıcı ve abonelere gizliliği artırıcı haberleşme yöntemlerinin sağlanması[11],
- Aranan aboneye basit bir yöntemle ve ücretsiz olarak gelen aramalarda arayan hattın kimliğinin gösterilmesini engelleme imkânının sağlanması[12],
- Bağlanılan numaranın kimliğinin görünmesine imkân sağlandığı durumlarda aranan aboneye, bağlanılan hattın kimliğinin arayan kullanıcıya gösterilmesinin engellenmesi imkânının sağlanması[13],

---

[7] 2002/58/EC Direktifi madde 5(3)
[8] 2002/58/EC Direktifi madde 6(1)
[9] 2002/58/EC Direktifi madde 6(2)
[10] 2002/58/EC Direktifi madde 6(4)
[11] 2002/58/EC Direktifi madde 7(2)
[12] 2002/58/EC Direktifi madde 8(2)

- Kullanıcıların terminal cihazlarına üçüncü bir parti tarafından yapılan otomatik çağrı yönlendirmelerinin ücretsiz ve basit bir yöntemle engellenmesine imkân sağlanması[14]

hususlarına Yönetmelikte yer verilmediği görülmektedir. İstek dışı haberleşme ise Yönetmeliğin 20 nci maddesinde düzenlenmektedir. Buna göre,

> *"İşletmeciler kişi müdahalesi olmadan çalışan fakslar, elektronik posta, kısa mesaj gibi otomatik arama sistemlerini, abonenin önceden izni olmadan siyasi propaganda amacıyla kullanamazlar. Söz konusu otomatik arama sistemlerinin doğrudan pazarlama amacıyla kullanılması halinde kullanıcılara gelen her bir mesajı bundan sonrası için almayı reddetme hakkı ücretsiz ve kolay bir yolla sağlanır. Doğrudan pazarlama amacıyla gönderilen ve kimin adına haberleşme yapıldığı hususunda göndericinin kimliğini saklayan veya alıcının bu iletişimin sonlandırılması konusunda talepte bulunacağı bir adres bulunmayan elektronik mektupların gönderilmesi abonenin bu yöndeki talebi halinde engellenir".*

E-Gizlilik Direktifinde düzenlenmeyen siyasi propaganda amaçlı haberleşme Yönetmelik kapsamına alınmış ve bu tür haberleşme için opt-in sistemi getirilmiştir. Doğrudan pazarlama amaçlı haberleşmede ise opt-out yöntemi benimsenmiştir. Ancak mezkûr Yönetmelik hükmünün, siyasi propaganda amaçlı haberleşmede opt-out sistemini öngören EHK'nın 50 nci maddesi ile çeliştiği görülmektedir.

Mevcut Yönetmeliğin yukarıda izah edilen hususlar açısından 2002/58/EC Direktifine uyumlu olmadığı ancak "Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik Taslağı"nın hazırlanması suretiyle mevcut Yönetmelikteki eksikliklerin

---

[13] 2002/58/EC Direktifi madde 8(4)
[14] 2002/58/EC Direktifi madde 11

giderilmeye çalışıldığı ve aynı zamanda 2006/24/EC sayılı Direktifin dikkate alındığı görülmektedir. Bu çerçevede, Taslak Yönetmelik ile mevcut Yönetmeliğin karşılaştırmalı tablosuna Ek'te yer verilmektedir.

5.2.6 Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik Taslağı

5809 sayılı EHK'ya dayanılarak hazırlanan "Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik Taslağı" (Taslak Yönetmelik) BTK tarafından 25.12.2009 tarihinde kamuoyu görüşüne açılmıştır.

Taslak Yönetmeliğin hazırlanmasında 2002/58/EC ve 2006/24/EC sayılı Direktiflerin esas alındığı ancak 2009/136/EC sayılı Direktif hükümlerine yer verilmediği görülmektedir. Bu kapsamda, Taslak Yönetmeliğin bazı yönleri ile 2009/136/EC Direktifine uyumlaştırılması amacıyla 2009/136/EC sayılı Direktifte yer alan "kişisel veri ihlali" tanımının aşağıda yer verilen şekilde Taslak Yönetmeliğe eklenmesi uygun olacaktır:

> *Kişisel veri ihlali: İletilen, kaydedilen veya kamuya açık elektronik haberleşeme hizmetinin teminiyle bağlantılı olarak başka şekilde işlenen kişisel verilere yetkisiz erişilmesine ya da söz konusu verilerin tedbirsizlikle veya hukuka aykırı olarak yok edilmesi, kaybolması, değiştirilmesi, yetkisiz olarak ifşa edilmesine neden olan güvenlik ihlali*

2009/136/EC Direktifi ile konum verisi tanımına *"elektronik haberleşme hizmeti aracılığıyla"* ifadesi eklendiğinden, konum verisi tanımının da bu doğrultuda değiştirilmesi yerinde olacaktır.

Taslak Yönetmeliğin 4 üncü maddesinde KVKKT'de düzenlenen kişisel verilerin işlenmesine ilişkin ilkelere yer verilmektedir. Bu çerçevede kişisel verilerin,

- Hukuka ve dürüstlük kurallarına uygun olarak ancak ilgili kişinin rızasına dayalı olarak işlenmesi,
- Yönetmelik hükümleri dâhilinde toplanması ve bu hükümlere aykırı olarak yeniden işlenmemesi,
- Toplandıkları amaçla bağlantılı, yeterli ve orantılı olması,
- Doğru olması ve gerektiğinde güncellenmesi,
- İlgili kişilerin kimliklerini belirtecek biçimde ve kaydedildikleri veya yeniden işlenecekleri amaç için gerekli olan süre kadar muhafaza edilmesi

esastır. Madde, elektronik haberleşme sektöründe faaliyet gösteren işletmecilerin kişisel verileri işlerken uyacakları ilkeleri belirlemiş olması açısından önemlidir. Ayrıca madde hükmü ile, Veri Koruma Direktifinde belirtilen verilerin niteliğine ilişkin ilkeler Taslak Yönetmeliğe dâhil edilmiş olmaktadır.

"Güvenlik" ve "Riskin bildirilmesi" başlıklı 5 ve 6 ncı maddeler mevcut Yönetmelikle paralel ele alınmış olmakla birlikte 2009/136/EC Direktifiyle kişisel verilerin ihlali konusunda işletmecilere getirilen yükümlülüklerin düzenlenmediği görülmektedir. Bu itibarla, 5 inci maddenin birinci fıkrasından sonra aşağıdaki hüküm yer almalıdır:

Birinci fıkrada belirtilen tedbirler asgari,

a) Kişisel verilere sadece yetkili personelin yasal amaçlarla erişmesinin garanti altına alınmasını,

b) Kişisel verilerin tedbirsizlikle, hukuka aykırı veya yetkisiz olarak; tahrip edilmesi, kaybolması, değiştirilmesi, depolanması veya başka bir ortama kaydedilmesi, işlenmesi, ifşa edilmesi ve söz konusu verilere erişilmesine karşı korunmasını,

c) Kişisel verilerin işlenmesine yönelik bir güvenlik politikası uygulamasının garanti altına alınmasını

içermelidir.

Böylece kişisel verilerin işlenmesi ve korunmasında güvenlik tedbirlerinin artırılması sağlanmış olacaktır.

Casus yazılımlar, internet virüsleri (*web bug*) ve gizli tanımlayıcılar (*hidden identifiers*) gibi vasıtalarla kullanıcıların terminal cihazlarına girilerek gizli bilgilere erişilmesi ya da kullanıcı aktivitelerini takip edilmesinin önlenmesi amacıyla,

> *İşletmeciler tarafından elektronik haberleşme şebekeleri; haberleşme iletiminin sağlanması amacı dışında abone ve kullanıcıların terminal cihazlarında bilgi saklamak veya saklanan bilgilere erişim sağlamak amacıyla ancak ilgili kullanıcı ve abonelerin verilerin işlenmesi hakkında açık ve kapsamlı olarak bilgilendirilmeleri ve rızalarının alınması kaydıyla kullanılabilir.*

şeklinde bir maddenin Taslak Yönetmeliğe eklenmesi tüketiciler açısından faydalı olacaktır.

Taslak Yönetmelikte 2009/136/EC sayılı Direktifle getirilen kişisel veri ihlallerinin bildirimine ilişkin herhangi bir hüküm yer almamaktadır. Bu kapsamda, 6 ncı maddeye kişisel verilerin ihlali durumunda işletmeciler tarafından yerine getirilmesi gereken yükümlülüklerin belirtildiği ve kişisel verilerin gizliliğinin korunmasında son derece önemli rol oynayacağı değerlendirilen aşağıdaki hususlar ilave edilmelidir:

1) *Kişisel veri ihlali durumunda işletmeciler, söz konusu ihlali gecikmeksizin Kuruma bildirir. İşletmeciler, kişisel veri ihlallerinin yer aldığı bir dosya tutmakla yükümlüdür. Dosyada, ihlali oluşturan sebepler, ihlalin etkileri ve ihlalin çözümüne yönelik alınan tedbirler yer almalı ve dosya sadece gerekli olan bilgileri içermelidir.*

2) *Kişisel veri ihlalinin abone veya bireyin kişisel verilerini ya da mahremiyetini olumsuz yönde etkileme ihtimali bulunması halinde işletmeci, abone ve bireyleri de ihlal hakkında bilgilendirir.*
3) *İşletmeci kişisel veri ihlalinin olmaması için şebekede gerekli koruma tedbirlerini aldığını ve söz konusu tedbirlerin ihlale konu verilere uygulandığını ispat ederse abone ya da bireylere bildirim yükümlülüğü ortadan kalkar. Belirtilen koruma tedbirleri, verilere erişim yetkisi bulunmayan herhangi bir kişi tarafından verilerin anlaşılamaz nitelikte olmasını sağlamalıdır.*
4) *İşletmecinin abone veya bireye bildirim yükümlülüğünü yerine getirmemesi durumunda Kurum, kişisel veri ihlalinin olumsuz etkilerini göz önüne alarak işletmecilere, bireyleri ve aboneleri ihlal hakkında bilgilendirmesi konusunda yükümlülük getirebilir.*
5) *Abone veya bireylere yapılacak bildirim, kişisel veri ihlalinin niteliğini, daha fazla bilginin elde edilebileceği iletişim noktalarını ve ihlalin olumsuz etkilerini azaltmak için alınabilecek önlemleri içermelidir. Kuruma yapılan bildirimde ise ilave olarak kişisel veri ihlalini çözümlemek için işletmeci tarafından alınan tedbirler ve ihlalin sonuçları hakkında bilgiler yer almalıdır.*

Mevcut Yönetmelikte yer almayan, "*trafik verilerinin abonelerin faturalandırılması ve arabağlantı ödemeleri amacıyla işlenebileceği*" hususu Taslak Yönetmeliğin 7(2) maddesine eklenerek trafik verilerinin işlenmesi konusunda AB Direktifiyle uyum sağlanmıştır.

13 üncü maddede sabit ve mobil telefon hizmeti ile internet hizmetlerine ilişkin olarak işletmecilerin saklaması gereken veri kategorileri belirtilmekte, haberleşmenin içeriği kapsam dışında tutulmaktadır. Verilerin ise haberleşmenin gerçekleştiği andan itibaren 1 yıl süreyle saklanması öngörülmektedir (md. 14). Öngörülen sürenin Veri Saklama Direktifiyle ve üye ülke uygulamalarıyla paralel olduğu değerlendirilmektedir.

Taslak Yönetmelikte saklanan verilerin korunması ve güvenliği ile ilgili hususlar da düzenlenmektedir. Bu çerçevede, işletmecilere getirilen yükümlülükler arasında (md. 15):

- Saklanan veriler ile şebekedeki diğer verilerin aynı kalite, güvenlik ve koruma özelliklerine tabi olması,
- Saklanan verilerin, istem dışı veya yasadışı tahrip, istem dışı kayıp ya da değişiklik veya yetki dışı ya da yasa dışı depolama, işleme, erişim ve ifşa olaylarına karşı uygun teknik ve idari tedbirlerin alınması,
- Verilerin sadece özel yetkilendirilmiş kişiler tarafından erişilebilir olmasının sağlanması için uygun teknik ve idari tedbirlerin alınması,
- İşlenen ve saklanan verinin saklama süresi sonunda imha edilmesi,
- Yasaların yetkili kıldığı makamlarca talep edilmesi halinde, saklanan veri ve söz konusu veriye ilişkin gerekli tüm bilgilere erişimin, ilgili makam tarafından belirtilen süre içinde sağlanması

sayılmaktadır. Madde ile getirilen yükümlülüklerin saklanan verilere ilişkin olası güvenlik ihlallerinin engellenmesinde önemli bir rol oynayacağı değerlendirilmektedir.

Kişisel veri içermeyen istatistikî bilgilerin BTK'ya gönderilmesi de Taslak Yönetmelikte düzenlenen bir diğer hususdur (md. 16). Söz konusu bilgiler,

- Yetkili makamlar tarafından talep edilen hususları,
- Verinin saklandığı tarih ile yetkili makamlar tarafından talep edildiği tarih arasında geçen süreyi,
- Veri talebinin karşılanamadığı durumları

kapsayacaktır. Madde hükmü ile, yetkili makamların suçun araştırılması, soruşturulması ve kovuşturulmasında ne kadar sıklıkta bilgi talep ettiklerinin anlaşılabilmesi amaçlanmakta olup, bu doğrultuda 1 yıl olarak düzenlenen

veri saklama süresinin söz konusu talepleri karşılamada yeterli olup olmadığı hususlarında değerlendirme yapma imkânı sağlanabilecektir.

17 nci maddede numaranın gizlenmesi ve gösterilmesi konularında abonelere sağlanan imkânlar yer almaktadır. Ancak mevcut Yönetmelikteki eksikliğin Taslak Yönetmelikte de devam ettiği, bu çerçevede 17 nci maddeye aşağıda belirtilen hususların ilave edilmesinin uygun olacağı değerlendirilmektedir:

Arayan hattın kimliğinin görünmesine imkân sağlandığı durumlarda işletmeci, aranan aboneye gelen aramalarda basit bir yöntemle ve ücretsiz olarak arayan hattın kimliğinin gösterilmesini engelleme imkânını sağlamakla yükümlüdür.

Bağlanılan hattın kimliğinin görünmesine imkân sağlandığı durumlarda işletmeci, aranan aboneye bağlanılan hattın kimliğinin arayan kullanıcıya gösterilmesinin engellenmesi imkânını sağlamakla yükümlüdür.

18 inci madde otomatik çağrı yönlendirmeleriyle ilgili olarak mevcut Yönetmelikteki eksikliği gidermektedir. Nitekim söz konusu düzenlemeyle işletmeciler, abone veya kullanıcının telefon cihazına üçüncü kişiler tarafından yapılan yönlendirmeleri abonenin ücretsiz ve basit bir yöntemle engellemesine imkân sağlayacak, ayrıca abone veya kullanıcının rızası olmaksızın aboneye veya kullanıcıya doğru yapılan aramaları başka bir numaraya veya otomatik mesaj sistemine yönlendirmeyecektir. Bu kapsamda örneğin, cevapsız çağrılar için telesekreter servisine yönlendirme yapmak isteyen bir işletmeci söz konusu yönlendirme için abone veya kullanıcının rızasını alacaktır.

İstek dışı haberleşmeyle ilgili olarak Taslak Yönetmeliğin 20 nci maddesi,

> *"Bir ürünün satılması ya da bir hizmetin sağlanması sırasında edinilen tüketiciye ait iletişim bilgileri, tüketicinin rızasının alınması koşuluyla, doğrudan pazarlanma amacıyla kullanılabilir ve bu tür elektronik mesajlarda, göndericinin kimliği ve erişim bilgisinin yer alması zorunludur. İşletmeciler, istenmeyen mesajların haberleşmenin her aşamasında abone tarafından basit ve ücretsiz bir işlemle reddedilebilir olmasına imkân sağlar ve bu mesajların engellenmesi yöntemlerine ilişkin olarak kullanıcıları açık ve detaylı bir şekilde ücretsiz olarak bilgilendirir"*

hükmünü içermektedir. Ancak maddenin E-Gizlilik Direktifinde yer alan hususları karşılamadığı görülmekte olup, istek dışı haberleşmeyle ilgili eksikliğin Taslak Yönetmelik de devam ettiği değerlendirilmektedir. Bu çerçevede, Taslak Yönetmelikte istek dışı haberleşmeyle ilgili maddenin AB Direktiflerine uygun olarak aşağıdaki şekilde düzenlenmesi yerinde olacaktır:

1) *Kişi müdahalesi olmadan çalışan otomatik arama ve haberleşme sistemleri, faks makineleri ve elektronik iletilerin doğrudan pazarlama amacıyla kullanılması abone veya kullanıcıların önceden rıza vermesi halinde mümkündür.*
2) *Abone veya kullanıcıların elektronik iletişim bilgilerinin bir ürünün ya da bir hizmetin satılması sırasında elde edilmesi halinde, bu bilgiler benzer ürün ya da hizmetlerin doğrudan pazarlanmasında kullanılabilir. Ancak, iletişim bilgilerinin elde edilmesi esnasında abone veya kullanıcılara bu tür bilgilerin doğrudan pazarlama amacıyla kullanılacağı açık biçimde belirtilir ve bu tür iletileri kolay bir yolla ve ücretsiz olarak reddetme imkânı sağlanır. İletişim bilgilerinin doğrudan pazarlama amacıyla kullanılmasına önceden rıza verilse bile bundan sonraki her bir iletiyi engelleme imkânı abone veya kullanıcıya sağlanır.*

3) *Birinci ve ikinci fıkrada belirtilen durumlar dışında, abone veya kullanıcılarla önceden rızaları alınmadan doğrudan pazarlama amaçlı istek dışı haberleşme yapılamaz.*
4) *Gerçek kişi dışındaki abonelerle önceden rızaları alınmadan otomatik arama ve haberleşme sistemleri, faks makineleri ve elektronik iletilerle doğrudan pazarlama amacıyla istek dışı haberleşme yapılması halinde, söz konusu abonelere bundan sonrası için istek dışı haberleşmeyi reddetme hakkı kolay bir yolla ve ücretsiz olarak sağlanır.*
5) *Alıcının talebini iletebileceği geçerli bir adres bilgisi bulunmayan veya kimin adına haberleşme yapıldığına dair gönderici kimlik bilgisi yer almayan doğrudan pazarlama amaçlı elektronik iletilerin gönderilmesi engellenmelidir.*

Böylece birinci fıkra ile opt-in, iknci fıkra ile soft-opt-in, üçüncü fıkra ile örneğin tele pazarlama aramaları için opt-in, dördüncü fıkra ile de gerçek kişi dışındaki abonelerle yapılacak istek dışı haberleşmede opt-out yöntemleri benimsenmiş ve AB Direktifleriyle uyum sağlanmış olacaktır.

Mevcut Yönetmelikte yer almayan gizliliği artırıcı haberleşme yöntemlerinin sağlanması hususuna ilişkin olarak, örneğin ayrıntılı faturalarda arayan ve aranan numaraların bazı hanelerinin gösterilmemesinin sağlanmasına yönelik bir maddenin Taslak Yönetmeliğe eklenmesi yerinde olacaktır.

Mevcut Yönetmeliğin *"Kötü niyetli veya rahatsızlık verici aramaların takibi amacıyla, abone tarafından yapılan başvuru üzerine, arayan abonenin kimliğini içeren bilgiler, 1 (bir) yıl süreyle saklanmalı ve ilgili mevzuata göre erişilebilir olmalıdır."* hükmünün Taslak Yönetmelikten çıkarıldığı görülmektedir. Tüketiciler için faydalı olabileceği değerlendirilen söz konusu hükmün Taslak Yönetmelikte yer alması daha uygun olacaktır.
Bu çerçevede, Taslak Yönetmeliğin genel olarak 2002/58/EC ve 2006/24/EC sayılı AB Direktifleri doğrultusunda hazırlandığı ve mevcut Yönetmelikteki

eksikliklerin giderilmeye çalışıldığı ancak bazı maddelerde mezkûr Direktiflere uyumun istenilen seviyede sağlanamadığı, ayrıca 2009/136/EC sayılı Direktifle getirilen hükümlere Taslak Yönetmelikte yer verilmediği görülmektedir. Bu bölümde yer alan değişiklik önerilerinin Taslak Yönetmeliğe derç edilmesiyle elektronik haberleşme sektöründe kişisel verilerin işlenmesi, saklanması ve gizliliğinin korunması hususunda AB mevzuatına büyük ölçüde uyum sağlanacağı değerlendirilmektedir. Bununla birlikte Anayasa değişikliği ile kişisel verilerin korunmasına ilişkin usul ve esasların kanunla düzenleneceği hüküm altına alındığından, elektronik haberleşme sektöründe kişisel verilerin işlenmesi, saklanması ve gizliliğinin korunmasına yönelik hususlara EHK'da yer verilmesi ya da söz konusu hususların başka bir yasa ile düzenlenmesinin daha uygun olacağı değerlendirilmektedir.

SONUÇ ve ÖNERİLER

Tarih boyunca bireylerin özel hayatları ve haberleşmeleriyle ilişkilendirilen mahremiyet bir başka deyişle özel hayatın gizliliği 19 uncu yüzyılın sonundan itibaren kişisel bilgiler bağlamında ele alınmaya başlanmış, mahremiyet unsurları arasında sayılan bilgisel mahremiyet çerçevesinde de kişisel veri kavramı ön plana çıkmıştır.

1970'lı yıllarda bilgi ve iletişim teknolojilerinin gelişmesi, bilgisayar ağlarında coğrafi sınırların kalkması ve veri işleme yeteneği olan güçlü sistemlerin varlığı, kişisel verilerin işlenmesi ve saklanmasında bazı kurallar getirilmesini ve yasal düzenlemeler yapılmasını gerekli kılmış, kişisel verilerin gizliliğine yönelik artan tehditler ve saldırılar karşısında ise dijital dünyada kişisel verilerin korunması en temel insan hakkı olarak ortaya çıkmıştır.

Kişisel verilerin korunmasında 4 temel model göze çarpmaktadır. Kamusal alan ve özel sektörü kapsayan genel kuralların belirlendiği ve bu kuralların yasaya uygunluğunun bağımsız bir kurum tarafından denetlendiği "Genel Düzenleme" modeli AB tarafından kabul edilen ve birçok ülkede uygulanan bir yöntemdir. Genel düzenleme yerine sektörlere özgü düzenlemelerin yapıldığı "Sektörel Düzenleme" modeli, ABD gibi ülkelerde uygulanmakta ancak birçok ülkede "Genel Düzenleme" modelinin alternatifi olarak değil genel düzenlemeleri tamamlayıcı bir unsur olarak uygulanmaktadır. Bu çerçevede, AB tarafından yayımlanan 95/46/EC sayılı Veri Koruma Direktifi "Genel Düzenleme", 2002/58/EC sayılı E-Gizlilik Direktifi ise "Sektörel Düzenleme" modeli altında değerlendirilmektedir. Şirketlerin mesleki davranış kurallarını kendilerinin belirledikleri ancak genel ve sektörel düzenleme modellerine göre yetersiz kalabilen öz düzenleme modeline Singapur ve Japonya gibi ülkelerde rastlanmaktadır. Teknolojik yöntemler de kişisel verilerin korunmasında kullanılabilecek modellerden biridir. Bu meyanda, PET ve söz konusu teknolojilerin kişisel verilerin korunmasına sağlayacağı katkı, son dönemde tartışılan konular arasındadır. Ülkemizde veri koruma

alanında sektörel düzenleme bulunsa da genel bir veri koruma yasasının bulunmaması önemli bir eksiklik olarak görülmektedir.

Avrupa Konseyi tarafından yayımlanan 28 Ocak 1981 tarihli "Kişisel Verilerin Otomatik Olarak İşlenmesi Karşısında Bireylerin Korunmasına Dair 108 Sayılı Sözleşme" ile OECD'nin yayımladığı 23 Eylül 1980 tarihli "Gizliliğin Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkeler"in birçok ülkede kişisel verilerin korunmasına ilişkin yasaların temelini oluşturduğu görülmektedir. Öte yandan AİHM, AİHS 8 inci madde kapsamında önemli içtihatlarda bulunmaktadır. Kişisel verilere erişilmesi, kişisel verilerin kamuya ya da üçüncü taraflara ifşa edilmesi ile kişisel verilerin toplanması ve saklanmasına ilişkin bu içtihatlarda meşru amaç, hukuka uygunluk ve demokratik toplumda gereklilik Mahkeme tarafından gözetilen temel unsurlardır.

Avrupa Birliğini kurucu antlaşmaları tadil eden ve ABTHŞ'ye yasal bağlayıcılık kazandıran Lizbon Antlaşması, 1 Aralık 2009 tarihinden itibaren yürürlüğe girmiş ve AB'de kişisel verilerin korunması temel hak olarak kabul edilmiştir. Ülkemizde ise 2010 yılında yapılan Anayasa değişikliğiyle 1982 Anayasasının 20 nci maddesine "*Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir.*" hükmü eklenerek kişisel verilerin korunmasını isteme hakkı, temel bir hak olarak tanınmıştır.

Kişisel verilerin işlenmesi konusunda gizliliğin korunması ve AB'ye üye ülkeler arasında kişisel verilerin serbest dolaşımına imkân sağlanması amaçlarını taşıyan 95/46/EC sayılı Veri Koruma Direktifi, üye ülkelerin ulusal mevzuatına aktarılmış olmasına rağmen, söz konusu Direktif doğrultusunda hazırlanan KVKKT'nin ülkemizde halen yasalaşmamış olması kişisel verilerin korunması alanında büyük bir boşluk oluşturmaktadır. Bu durum, ülkemizde kamusal alan ile özel sektördeki veri işleme faaliyetlerinin gelişigüzel olması ve bu alandaki yeterli koruma tedbirlerinin sağlanamaması riskini artırmaktadır.

2002/58/EC sayılı E-Gizlilik Direktifi, kişisel verilerin işlenmesi konusunda elektronik haberleşme sektörüne özgü kurallar getirmiştir. Direktif teknolojik tarafsızlık temelinde; haberleşmenin ve ilgili trafik verisinin gizliliği, trafik ve konum verilerinin işlenmesi, istek dışı haberleşme, ayrıntılı faturalar, arayan ve bağlanılan hattın kimliğinin gösterilmesi ve engellenmesi, abone rehberleri ve otomatik çağrı yönlendirme gibi konularda abonelerin yanı sıra kullanıcıları da korumayı hedefleyen hükümler içermektedir. Direktif AB üyesi ülkelerin tamamında iç hukuka aktarılmış ve bu ülkelerde kapsamlı veri koruma kanunlarını tamamlayıcı bir rol üstlenmiştir.

2006/24/EC sayılı Veri Saklama Direktifi, işletmeciler tarafından işlenen ya da üretilen trafik ve konum verilerinin ciddi suçların araştırılması, soruşturulması ve kovuşturulmasında kullanılmak üzere saklanmasına ilişkin yükümlülükler getirmiş, haberleşmenin içeriği kapsam dışı tutulmuştur. Direktifin AB üyesi ülkelerde iç hukuka aktarılmasında sorunlar yaşandığı, örneğin Almanya, Çek Cumhuriyeti ve Romanya Anayasa Mahkemelerinin Veri Saklama Direktifine uyum amacıyla çıkarılan yasaların, yeterli koruma tedbiri sağlamadığı gerekçesiyle özel hayatın gizliliği ilkesine aykırı olduğuna hükmettiği görülmektedir. Bu çerçevede, Veri Saklama Direktifine uyum amacıyla yapılacak yasal düzenlemelerde meşru amaç ve orantılılık unsurlarıyla birlikte saklanan verilere ilişkin yeterli koruma tedbirlerinin sağlanması önemlidir.

E-Gizlilik Direktifini tadil eden 2009/136/EC sayılı Vatandaş Hakları Direktifi, özellikle veri işlemenin güvenliği konusunda önemli yenilikler içermektedir. Kişisel veri ihlallerinin yetkili otoritelere ve gerekli hallerde ihlalden etkilenen abonelere bildirilmesi yönünde işletmecilere yükümlülük getirilmesi, gizlilik kültürünün gelişmesine ve veri ihlallerine yönelik şeffaflığın artmasına katkıda bulunacak; işletmecilerin itibar kaybı yaşamamaları ve maddi zarara uğramamaları için kişisel verilerin işlenmesi ve korunmasında güçlü güvenlik tedbirleri almalarını tetikleyecektir.

Elektronik haberleşme alanında kullanılan trafik veya konum verileri, kişilerle ilişkilendirilebildikleri takdirde kişisel veri olarak değerlendirilmekle birlikte her bir trafik veya konum verisini kişisel veri olarak nitelendirmek mümkün görünmemektedir. Bu bağlamda, AB Direktiflerinde rastlanan veri türlerini 3 başlık altında incelemek uygun olacaktır.

Ürün veya hizmetlerin pazarlanması amacıyla kişisel iletişim bilgileri kullanılarak telefon, SMS, MMS, faks ve e-posta gibi vasıtalarla yapılan istek dışı haberleşmenin yaygınlaşması karşısında, E-Gizlilik Direktifinin 13 üncü maddesinde kapsamlı düzenleme yapılmıştır. Söz konusu madde ile, istek dışı haberleşmenin engellenmesinde kullanılabilecek 3 yöntemden bahsedilmektedir. Opt-in, istek dışı haberleşme konusunda abone ve kullanıcıların önceden onaylarının alınmasını gerektiren bir yöntem iken opt-out, önceden onay gerektirmeyen ancak abone ve kullanıcılara istek dışı haberleşmeyi reddetme imkânının sağlandığı bir yöntemdir. Soft-opt-in ise tüketicilere ait iletişim bilgilerinin bir ürünün ya da bir hizmetin satılması sırasında Veri Koruma Direktifine uygun olarak elde edilmesi halinde, bu bilgilerin benzer ürün ya da hizmetlerin pazarlanmasında kullanılmasına imkân tanıyan bir sistemdir. Bu çerçevede otomatik arama makineleri, fakslar ve elektronik iletilerle (e-posta, sesli mesaj, SMS, MMS vb.) yapılacak doğrudan pazarlama amaçlı haberleşmede opt-in sistemi benimsenmiş olmakla birlikte -gerekli şartların taşınması halinde- elektronik iletiler için soft-opt-in yöntemi kullanılabilecektir. Başka vasıtalarla yapılacak haberleşme ile tüzel kişilere uygulanacak yöntem ise üye ülkelere bırakılmıştır. Bu nedenle, söz konusu madde uygulamaları üye ülkeler arasında farklılık göstermektedir. Ülkemizde ise istek dışı haberleşme konusunda EHK'da opt-out sistemi benimsenmiş ancak AB Direktifleriyle istenilen seviyede uyum sağlanamamıştır. Zira AB Direktiflerinde çeşitli elektronik haberleşme araçlarıyla yapılacak istek dışı haberleşmede opt-in ve soft-opt-in yöntemlerinin kullanılması öngörülmektedir.

Kişisel verilerin niteliğine ilişkin temel ilkelerin 25.12.2009 tarihinde BTK tarafından kamuoyu görüşüne açılan "Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik Taslağı"nda yer alması önemli bir adımdır. Bu anlamda, Taslak Yönetmeliğin yürürlüğe girmesiyle işletmecilerin abonelik sözleşmeleri, taahhütname, çağrı merkezleri, tele pazarlama aramaları, internet gibi mecraları kullanarak yapacakları veri işleme faaliyetlerinde söz konusu ilkeleri göz önünde bulundurmaları gerekecektir.

Trafik verilerinin haberleşmenin iletilmesi, faturalandırılması ve arabağlantı ödemeleri gibi amaçlarla işlenmesi, işletmecinin aboneye hizmet sunabilmesi açısından bir gereklilikse abonelerin bilgilendirilmesi koşuluyla bu tür veriler işlenebilir. Ancak trafik verilerinin işlenmesi, CDR bilgilerinin analiz edilmesi suretiyle abonelere en uygun tarife seçeneğinin sunulması gibi haberleşme hizmetlerinin pazarlanması amacını taşıyorsa bu tür veri işleme faaliyetinden önce aboneler bilgilendirilmeli ve rızaları alınmalıdır.

Trafik verilerini işlemekle görevli personelin yetki ve sorumluluk sınırlarının tam olarak belirlenmesi veri gizliliği ihlallerinin önlenmesi ve herhangi bir cezai yaptırımla karşılaşılmaması açısından işletmeciler tarafından hassasiyet gösterilmesi gereken bir diğer husustur. Çeşitli konum belirleme yöntemleri kullanılarak üretilen ve trafik verisi niteliği taşımayan konum verilerinin işlenmesi için de abonelerin önceden bilgilendirilmesi, rızalarının alınması, verilerin katma değerli hizmetlerin sunumu için gerekli kapsam ve süre boyunca işlenmesi gereklidir.

Veri Saklama Direktifinde sabit ve mobil telefon ile internet hizmetlerine ilişkin verilerin 6 ila 24 ay arasında saklanabileceği öngörülmektedir. AB üyesi ülkeler arasında veri saklama süreleri farklılık arz etmekle beraber bu süre genellikle 1 yıl olarak belirlenmiştir. Taslak Yönetmelikte de veri saklanmasına ilişkin 1 yıllık sürenin öngörülmesi AB üyesi ülke uygulamalarıyla paralellik arz edecektir.

Tasarımsal gizlilik ilkesi, "*teknolojilerin tasarım, kurulum, kullanım ve kaldırılma safhalarını içeren yaşam döngülerinin tamamında kişisel verilerin ve gizliliğin tümleşik olarak bulunması*" olarak tanımlanmaktadır. AB Direktiflerinde yer alan "teknik ve idari tedbirlerin alınması" ifadesi, işletmecilerin bu yükümlülüğü istedikleri şekilde yorumlamaları ve gerekli güvenlik tedbirlerini almamaları riskini barındırırken diğer yandan kişisel verilerin korunmasında hukuki düzenlemelerin teknik yöntemlerle desteklenmesi yönünde tetikleyici bir unsur olabilmektedir. Veri Koruma Direktifinin 46 numaralı dibacesinde teknik ve idari tedbirlerin, gerek sistemlerin tasarım aşamasında gerekse veri işleme esnasında alınması gereken tedbirleri kapsayacağı belirtilmektedir. Bu çerçevede, tasarımsal gizliliğin bir ilke olarak belirlenmesi ve yasal düzenlemelere dâhil edilmesi hususu VKÇG ve AVKD gibi önemli organlar tarafından dile getirilmektedir. Nitekim son yıllarda veri ihlallerinde yaşanan artışlar ve Alman Federal Anayasa Mahkemesinin 2008 tarihli kararında yer alan, "*bilgi teknoloji sistemlerinin bütünlüğü ve gizliliğinin sağlanmasının*" temel haklar arasında olduğu görüşü bu ilkenin gerekliliğini destekler niteliktedir.

Tasarımsal gizlilik ilkesinin benimsenmesi PET uygulamalarını beraberinde getirecektir. PET, arayan hattın kimliğinin tanımlanması (CLI) örneğinde olduğu gibi basit bir uygulama olabilirken konum tabanlı servisler için geliştirilen sistemde daha karmaşık bir yapı içerebilmektedir.

İşletmeciler tarafından veri güvenliğini sağlamaya yönelik alınan tedbirler, gizliliğin korunmasında gerekli olmakla birlikte yeterli görülmemektedir. Zira gizlilik, kişisel verilerin hukuka uygun olarak yeterli ve orantılı biçimde toplanması, toplanma amacına uygun kullanılması, ilgili kişinin rızası olmadan yeniden işlenmemesi ve üçüncü taraflara aktarılmaması gibi daha geniş alanları kapsamaktadır.

AB Direktiflerinin üye ülkelerin ulusal mevzuatlarına aktarılmasına ilişkin bilgiler aşağıda özetlenmektedir:

- 2002/58/EC sayılı E-Gizlilik Direktifi üye ülkelerin tamamında iç hukuka aktarılmıştır. Genellikle, istek dışı haberleşmeye ilişkin uygulamalar ise farklılık gösterebilmektedir.
- 2006/24/EC sayılı Veri Saklama Direktifi Avusturya ve İsveç'te taslak düzenleme halinde iken Çek Cumhuriyeti, Romanya ve Almanya'da çıkarılan yasalar Anayasa Mahkemeleri tarafından iptal edilmiş kalan 22 ülkede ise Direktif iç hukuka aktarılmıştır.
- 2009/136/EC sayılı Vatandaş Hakları Direktifinin iç hukuka aktarılma çalışmaları devam etmektedir. Kişisel veri ihlallerinin yetkili otoritelere veya ilgili kişilere bildirilmesi konusunda İrlanda, Almanya, İspanya ve İngiltere gibi ülkelerde daha somut düzenlemeler yer almaktadır.

Ülkemizde Anayasa ve çeşitli kanunlarda kişisel verilerle ilgili hükümler yer almakla birlikte elektronik haberleşme sektöründe daha detaylı düzenlemeler bulunmaktadır. "Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik" genel olarak 2002/58/EC sayılı Direktif doğrultusunda ele alınmış olmakla birlikte Direktifte yer alan bazı hususlar Yönetmeliğe aktarılmamıştır. Bu çerçevede, "Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik Taslağı" ile söz konusu eksikliklerin giderilmeye çalışıldığı ancak 2009/136/EC sayılı Direktif hükümlerinin Taslak Yönetmeliğe aktarılmadığı görülmektedir.

Ülkemizde veri koruma alanında genel bir düzenlemenin olmaması, elektronik haberleşme şebekeleri veya hizmetleri aracılığıyla işlenen kişisel verilerin gizliliğine olan tehditleri artırmakta, kişisel verilerin korunmasını daha da önemli hale getirmektedir. Bu kapsamda, Lizbon Antlaşmasının yürürlüğe girmesiyle yasal bağlayıcılık kazanan ABTHŞ'de, temel haklar arasında sayılan kişisel verilerin korunması hakkının ülkemiz elektronik haberleşme

mevzuatında yer alan tüketici hakları arasına dâhil edilebileceği değerlendirilmektedir.

Kişisel verilerin işlenmesinde gerekli olan ilkelerin EHK'da ve/veya ikincil mevzuatta yer almaması işletmecilerin veri işleme faaliyetlerini orantısız biçimde yapmaları, verilerin üçüncü taraflarla paylaşımında yeterli ve gerekli tedbirleri almamaları gibi riskleri artırmakta; düzenleyici otoritenin, işletmecilerin veri işleme faaliyetlerini değerlendirirken kullanabileceği hukuki dayanakları da önemli oranda kısıtlamaktadır. Bu nedenle, belirtilen ilkelerin Taslak Yönetmelikte yer alması uygun görülmekle birlikte AB mevzuatına dâhil edilmesi beklenen tasarımsal gizlilik ve sorumlu tutulabilirlik gibi yeni ilkelerin düzenlemelere ilave edilebileceği düşünülmektedir.

Tüketicilerin kişisel verilerin işlenmesi konusunda tam ve eksiksiz olarak bilgilendirilmeleri önem arz etmektedir. Bu bağlamda, Veri Koruma Direktifine uygun olarak kişisel verilerin elde edilmesi sırasında ilgili kişiye,

- İşletmecinin ve varsa temsilcisinin kimliği,
- Kişisel verilerin hangi amaçla işleneceği,
- Kişisel verilerin kimlere aktarılacağı,
- Kendisi hakkındaki kişisel verileri öğrenme ve gerekiyorsa bunları düzeltme hakkına sahip olduğu

hususlarında bilgilendirme yapılmalıdır. Ancak "*Kişisel verileriniz üçüncü taraflarla paylaşılabilir.*" şeklindeki ifadeler çok genel bir anlam taşıdığından ve kişisel verilerin hangi amaçlarla (doğrudan pazarlama amaçlı haberleşme, adli soruşturma vb) paylaşılacağı hususunda açık bir bilgi içermediğinden, kişisel veriler ile trafik veya konum verilerinin işlenmesi, iletişim bilgilerinin doğrudan pazarlama amacıyla kullanılması gibi abonenin rızasını gerektirebilecek hususlarda tüketicilere yapılacak bilgilendirmeler açık ve anlaşılır olmalı, örtülü ifadeler içermemelidir.

EHK ve ikincil mevzuatta yer alan istek dışı haberleşmeye ilişkin hükümlerde, 2002/58/EC ve 2009/136/EC Direktifleri doğrultusunda gerekli değişiklikler yapılmalıdır. Bu çerçevede, doğrudan pazarlama amaçlı istek dışı haberleşmede opt-in ve soft-opt-in yöntemlerinin tercih edilebileceği, elektronik ticaret kanun tasarısı ile paralellik sağlanması amacıyla gerçek kişi dışındaki abonelerle yapılacak istek dışı haberleşmede ise opt-out sisteminin benimsenebileceği değerlendirilmektedir.

Düzenlemelerde abonelerin istek dışı haberleşmeyi basit ve ücretsiz bir yöntemle engelleyebilecekleri belirtilmesine rağmen, bu yöntemlerin açıkça ifade edilmesi uygulamaları tüketiciler açısından kolaylaştıracaktır. Bu bağlamda örneğin, doğrudan pazarlama amacıyla tüketicilere gönderilecek SMS metinlerinin sonunda bu tür mesajları almak istemeyen tüketiciler için bir çıkış seçeneğinin yer alması uygun olacaktır.

Kişisel verilerin elde edilmesi sırasında abonelere opt-out seçeneğinin sunulmasına örnek olarak tüketicilerle akdedilen abonelik sözleşmeleri verilebilir. Bir mobil telefon işletmecisinin abonelik sözleşmesinde bir işaret kutucuğu ve "*Şirketimizin kampanya ve tarifelerine ilişkin duyurular SMS ile gelmesin*" ifadesinin yer alması, SMS kanalıyla yapılacak istek dışı haberleşme için abonelere opt-out seçeneğinin sunulmuş olduğu anlamını taşıyacaktır. Bu çerçevede, abonelik sözleşmeleri başta olmak üzere ilgili metinlerde bu hususa dikkat edilmelidir.

Tele pazarlama amaçlı aramalara yönelik olarak opt-out sisteminin tercih edilmesi halinde elektronik haberleşme sektörüne özgü Robinson listeleri oluşturulabilir. Ancak bu durumda, bütün listelerin tek bir veritabanında yer alması, sistemin merkezi olması ve sorgulama esaslı çalışması kişisel verilerin korunması açısından daha uygun olan yöntemdir.

Veri Saklama Direktifi kapsamında Taslak Yönetmelikte, işletmeciler tarafından saklanması öngörülen veri kategorileri belirlenmiştir. Saklanacak

veri türleri, veri saklama süreleri, saklanan verilerin korunması ve güvenliği gibi konularda Direktife uyum sağlandığı görülmekle birlikte veri kategorilerinin hangi gerekçelerle saklanacağına ilişkin bir hükmün Taslak Yönetmelikte yer almadığı görülmektedir. Bu nedenle, AİHM içtihatları da göz önüne alındığında işletmecilere hangi gerekçelerle veri saklama yükümlülüğü getirildiğinin belirtilmesi yerinde olacaktır.

Tüketiciler tarafından internet mecrası kullanılarak elektronik haberleşme hizmetlerine ilişkin yapılacak çeşitli sorgulama işlemlerinde kişisel verilerin üçüncü kişiler tarafından elde edilmesi veya görülmesi riskine karşı yeterli güvenlik tedbirleri alınmalıdır. Bu çerçevede, sundukları hizmetlerin güvenliğini sağlamak için işletmecilerin alacakları teknik ve idari tedbirlerin, internet sayfaları üzerinden sunulan hizmetleri de kapsaması gerektiği değerlendirilmektedir.

Elektronik Haberleşme Güvenliği Yönetmeliği ile işletmecilere getirilen birtakım yükümlülükler veri koruma alanında teknik ve idari tedbirler öngörmektedir. Ancak Yönetmelikte yer alan veri tanımının kişisel veri tanımıyla paralel olduğu göz önüne alındığında *"kişisel bilgilerin işlenmesi ve gizliliğinin korunması"* hususunun kapsam dışı bırakılması bir çelişki oluşturmaktadır. Bu husus gözetilerek Yönetmeliğin ilgili maddelerinin gözden geçirilmesi uygun olacaktır.

Kişisel veri ihlallerine ilişkin bildirimlerin hem yetkili otoriteye hem de ilgili kişilere yapılmasının ülkemizde gizlilik kültürünün gelişmesine katkı sağlayacağı bir gerçektir. Buradan hareketle 2009/136/EC Direktifinin kişisel veri ihlallerine ilişkin hükümlerinin ikincil mevzuata aktarılması önemli bir adım olacak, işletmecilerin gizliliğin korunmasına yönelik koruma tedbirlerini artırmaları ve bu yönde politika belirlemeleri sağlanmış olacaktır.
Çalışmamızda yer alan tespit ve öneriler doğrultusunda Taslak Yönetmelikte değişiklik yapılması halinde AB Direktiflerine büyük ölçüde uyum sağlanacağı değerlendirilmekle birlikte, Anayasa'nın 20 nci maddesinde düzenlenen

kişisel verilerin korunmasına ilişkin usul ve esasların kanunla düzenleneceği hususu göz önünde bulundurularak elektronik haberleşme sektöründe kişisel verilerin işlenmesi, saklanması ve gizliliğinin korunmasına yönelik usul ve esasların EHK ya da başka bir yasa ile düzenlenmesi daha uygun olacaktır.

Kişisel verilerin korunmasında işletmecilerin olduğu kadar kamu kurum ve kuruluşları ile tüketicilerin sağlayacağı katkılar da göz ardı edilmemelidir. Örneğin, kamu kurumları kanundan doğan görevlerini icra ederken işletmecilerden orantısız bilgi talebinde bulunabilmektedir. Bu çerçevede kamu kurumları tarafından kişisel bilgilerin talep edilmesi, toplanması, depolanması ve silinmesi aşamalarında kişisel verilerin gizliliğine zarar verebilecek durumlara mahal verilmemelidir. Tüketicilerin ise gerek abonelik tesis edilmesi gerekse işletmecilerden ürün veya hizmet satın alınması esnasında kişisel verilerini bilinçli bir şekilde paylaşmaları son derece önemlidir. Bu itibarla, gizlilik kültürünün tam olarak gelişmesi ve toplumun tamamına yaygınlaştırılmış kişisel verilerin korunmasına ilişkin saygı kültürünün oluşturulmasında kamu kurum ve kuruluşları, işletmeciler ve tüketicilerden oluşan üçlü sacayağının önemi ve katkısı büyüktür.

KAYNAKLAR

ABGS, 2009, Türkiye 2009 Yılı İlerleme Raporu, http://www.abgs.gov.tr/files/AB_Iliskileri/AdaylikSureci/IlerlemeRaporlari/turkiye_ilerleme_rap_2009.pdf (18.04.2011).

ABGS, 2010, Türkiye 2010 Yılı İlerleme Raporu, http://www.abgs.gov.tr/files/AB_Iliskileri/AdaylikSureci/IlerlemeRaporlari/turkiye_ilerleme_rap_2010.pdf (18.04.2011).

AEPD, 2005, Guide for the Fight Against Spam, https://www.agpd.es/portalwebAGPD/english_resources/regulations/common/pdfs/INFORMACION_SPAM.INGLES_V.30-mayo.pdf (05.05.2011).

AEPD 2010, Mexico Declaration, http://www.agpd.es/portalwebAGPD/english_resources/regulations/common/pdfs/Mexico_declaration.pdf (20.01.2011).

AHMAD Tabrez, 2009, Technology Convergence and Protection of Data Privacy, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1480718 (19.01.2011)

AİHM Kararı, 1978, Çev. Osman DOĞRU, 2011, Klass ve Diğerleri-Almanya Davası, http://ihami.anadolu.edu.tr/aihmgoster.asp?id=30, (02.01.2011).

AİHM Kararı, 1987, Çev. Osman DOĞRU, 2011, Leander-İsveç Davası, http://ihami.anadolu.edu.tr/aihmgoster.asp?id=126 , (07.01.2011).

AİHM Kararı, 1989, Çev. Osman DOĞRU, 2011, Gaskin-Birleşik Krallık Davası, http://ihami.anadolu.edu.tr/aihmgoster.asp?id=192 , (07.01.2011).

AİHM Kararı, 1997, MS-İsveç Davası, http://www.humanrights.is/the-human-rights rpoject/humanrightscasesandmaterials/cases/regionalcases/europeancourtofhumanrights/nr/2627, (06.01.2011).

AİHM Kararı, 2009, Uslu-Türkiye Davası, http://www.yargitay.gov.tr/aihm/upload/23815-04.pdf , (07.01.2011).

ALDAMA Almudena, CRUZ Eduardo, 2009, Telecommunication Laws and Regulations, http://www.iclg.co.uk/khadmin/Publications/pdf/2967.pdf (05.05.2011).

ARNOLDI Thomas, 2009, Report of the Data Retention Conference, 'Towards the Evaluation of the Data Retention Directive', Brussels, Mayıs 2009, http://ec.europa.eu/home-affairs/doc_centre/police/docs/meeting_report_09_07_14_en.pdf (27.04.2011).

APEC, 2005, Apec Privacy Framework, http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx (30.12.2010).

APEC, 2010, Asia-Pacific Economic Cooperation, About APEC, http://www.apec.org/About-Us/About-APEC.aspx (30.12.2010).

Article 29 Data Protection Working Party, 1998, Future Work on Codes of Conduct, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1998/wp13_en.pdf (20.01.2011).

Article 29 Data Protection Working Party, 1999, Recommendation on the Inclusion of the Fundamental Right to Data Protection in the European Catalogue of Fundamental Rights. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1999/wp26en.pdf (19.01.2011).

Article 29 Data Protection Working Party, 2004, Opinion 5/2004 on Unsolicited Communications for Marketing Purposes under Article 13 of Directive 2002/58/EC, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp90_en.pdf (20.02.2011).

Article 29 Data Protection Working Party, 2005, Opinion on the Use of Location Data With a View to Providing Value-Added Services, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp115_en.pdf (22.03.2011).

Article 29 Data Protection Working Party, 2007, Opinion 4/2007 on the Concept of Personal Data,http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf (10.03.2011).

Article 29 Data Protection Working Party, 2009, The Future of Privacy, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf (22.01.2011).

Article 29 Data Protection Working Party, 2010, Report on Compliance at National Level of Telecom Providers and ISPs with the Obligations Required from National Traffic Data Retention Legislation on the

Legal Basis of Articles 6 and 9 of the E-Privacy Directive 2002/58/EC and the Data Retention Directive 2006/24/EC Amending the E-Privacy Directive, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp172_en.pdf (19.03.2011).

BARCELO Rosa, TRAUNG Peter, 2010, The Emerging European Security Breach Legal Framework. Data Protection in a Profile World, GUTWIRTH Serge, POULLET Yves, DE HERT Paul. (der.), Springer, ISBN 978-90-481-8864-2, p. 77-105.

BENALAL Alexander, RODRIGUEZ Maria G, 2006, The Spanish Data Protection Agency Imposes a Fine on a Law Firm for Spam, http://www.twobirds.com/Finnish/News/Articles/Sivut/The-Spanish-Data-Protection-Agency-imposes-a-fine-on-a-law-firm-for-spam.aspx (05.05.2011).

BİLÇEN Sumru, 2010, AB'de Önemli Bir Adım: Lizbon Antlaşması, http://www.tbmm.gov.tr/ul_kom/kpk/docs/lizbonsumru24032010.pdf (26.01.2011).

Bilgi Teknolojileri ve İletişim Kurulu Kararı, 22.02.2011 tarihli ve 2011/DK-10/83 sayılı "MY Vodafone Servisindeki Güvenlik Açığına İlişkin Denetim" konulu karar.

Bilgi Teknolojileri ve İletişim Kurulu Kararı, 19.04.2011 tarihli ve 2011/DK-10/198 sayılı "Kişisel Veri Gizliliğinin İhlali" konulu karar.

BIS, 2010, Implementing the Revised EU Electronic Communications Framework, http://www.culture.gov.uk/images/consultations/10-1132-implementing-revised-electronic-communications-framework-consultation.pdf (26.04.2011).

BORKING John, BLARKOM Van G.W, OLK J.G.E, 2003, Handbook of Privacy and Privacy-Enhancing Technologies, College bescherming persoonsgegevens, The Hague. http://www.andrewpatrick.ca/pisa/handbook/Handbook_Privacy_and_PET_final.pdf (31.03.2011).

BORKING John, HES Ronald, 2000, Privacy-Enhancing Technologies: Path to Anonymity, Registratiekamer, The Hague.

BRENNAN Davinia, 2011, President Signs Communications (Retention of Data) Act 2011 into Law, http://www.irelandip.com/2011/02/articles/privacy-1/president-signs-communications-retention-of-data-act-2011-into-law/ (06.05.2011).

BRUNGER James, WATTS Mark, 2010, Changes to the European E-Privacy Directive, Consequences for Online Advertising, http://www.bristows.com/?pid=46&level=2&nid=1494 (19.02.2011).

BUELLESBACH, 2010, Concise European It Law, Kluwer Law International, Alphen Aan Den Rijn, Netherlands.

BYGRAVE Lee A, 1998, Data Protection Pursuant to the Right to Privacy in Human Rights Treaties, Volume 6, p. 247–284 http://folk.uio.no/lee/oldpage/articles/Human_rights.pdf (18.01.2011).

BYGRAVE Lee A, 2002, Privacy-Enhancing Technologies - Caught between a Rock and a Hard Place, Privacy Law & Policy Reporter, Volume 9, p.135-137,http://folk.uio.no/lee/publications/PETs_speech.pdf (22.01.2011).

BYGRAVE Lee A, 2004, Privacy Protection in a Global Context, Scandinavian Studies in Law, Volume 47, p.319-348, http://folk.uio.no/lee/publications/ (27.12.2010).

CATE Fred H, 1979, Privacy In Perspective, The AEI Press, Washington.

CAVOUKIAN Ann, 2011, Privacy By Design: The 7 Foundational Principles, http://www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf (30.03.2011).

CELLERE Macchi S, MEZZAPESA Giuseppe, 2010, The Technology, Media and Telecommunications Review, http://www.jonesday.com/files/Publication/72e14e57-99a1-43bb-b721-c1d73e43b082/Presentation/PublicationAttachment/43ad8c72-a7bb-4788-9a09-8516549fa109/Italy.pdf (06.05.2011).

CHATZILIASSI Evi, 2009, Legal Issues on the Protection of Personal Data on the Internet. Handbook of Electronic Security and Digital Forensics. JAHANKHANI Hamid, WATSON David L, LEONHARDT Frank, (der.). World Scientific Publication, Singapur, s. 497-513.

CIPPGUIDE, 2010, Comparing the Co-Regulatory Model Comprehensive Laws and the Sectoral Approach, https://www.cippguide.org/2010/06/01/comparing-the-co-regulatory-model-comprehensive-laws-and-the-sectoral-approach/ (21.01.2011).

COAST, 2011, DPI Specification and High Level Complexity Evaluation of Algorithms,http://www.coast-fp7.eu/public/COAST_D4_1_POLITO_FF_20110204.pdf (04.05.2011).

COMREG, 2011, Direct Marketing Opt-Out Register, http://www.comreg.ie/consumer_initiatives/direct_marketing_opt-out_register.492.566.html (06.06.2011).

COOPER Daniel, TIELEMANS Henriette, FINK David, 2010, The Lisbon Treaty and Data Protection: What's Next for Europe's Privacy Rules? http://www.cov.com/publications/?pubtype=1&archiveyear=2010 (27.01.2011).

Council of Europe, 1979, Yearbook of the European Convention on Human Rights, Martinus Nijhoff Publishers, Netherlands.

Council of Europe, 1981, Convention for the Protection of Individuals With Regard to Automatic Processing of Personal Data http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm (01.01.2011).

Council of Europe, 2011, Data Protection History, http://www.coe.int/t/dghl/standardsetting/dataprotection/History_en.asp (04.01.2011).

DIŞ TİCARET MÜSTEŞARLIĞI (DTM), 2010, Lizbon Antlaşması (Reform Antlaşması), http://www.dtm.gov.tr/dtmweb/index.cfm?action=detay&yayinID=2157&icerikID=2316&dil=TR (19.01.2010).

DRIESSEN Bart, 2008, Transparency in EU Institutional Law - A Practitioner's Handbook, Cameron May, London.

Duke, 2010, Duke University Libraries: International Governmental Organizations, http://library.duke.edu/research/subject/guides/igo_guide/eu_guide/eu_system/eu_treaties.html (26.01.2011).

DUTCHDPA, 2009, Summary of the Annual Report 2009 of the Dutch DPA, http://www.dutchdpa.nl/downloads_jv/jv_2009_sv.pdf (28.03.2011).

EC, 2009, Study on Online Copyright Enforcement and Data Protection in Selected Member States, http://ec.europa.eu/internal_market/iprenforcement/docs/study-online-enforcement_en.pdf (06.04.2011).

EC, 2011, Evaluation Report on the Data Retention Directive (Directive 2006/24/EC), Nisan 2011, http://ec.europa.eu/commission_2010-2014/malmstrom/archive/20110418_data_retention_evaluation_en.pdf (01.05.2011).

EDRI, 2006, French Anti-terrorism Law Not Anti-constitutional, http://www.edri.org/edrigram/number4.2/frenchlaw (03.05.2011).

EDRI, 2008, Important Personal Data Lost by the Bank of Ireland, http://www.edri.org/edrigram/number6.9/personal-data-bank-ireland (06.05.2011).

EDRI, 2010, German Federal Constitutional Court Rejects Data Retention Law, http://www.edri.org/edrigram/number8.5/german-decision-data-retention-unconstitutional (27.04.2011).

EDPS, 2010, Opinion of the European Data Protection Supervisor on Promoting Trust in the Information Society by Fostering Data Protection and Privacy, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:280:0001:0015:EN:PDF (29.03.2011).

EDWARDS Elaine, 2011, Data Breach Code 'Not Signed Off', http://www.irishtimes.com/newspaper/breaking/2011/0301/breaking26.html (06.05.2011).

EECKE Van P, 2006, Scope and Impact of the European Data Retention Directive, http://www.netutils.com/documentation/sensage/WhitePapers/EuropeanDataRetention_wp.pdf (02.03.2011).

ENISA, 2010, Italy Country Report, http://www.enisa.europa.eu/act/sr/files/country-reports/Italy.pdf (06.05.2011).

ENISA, 2011, Data Breach Notifications in the EU, http://www.enisa.europa.eu/act/it/library/deliverables/dbn (05.05.2011).

ERSOY Ömer, AB'de Özel Hayat Risk Altında mı?, http://www.sde.org.tr/tr/haberler/1350/abde-ozel-hayat-risk-altinda-mi.aspx (04.02.2011).

EU, 2004, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Unsolicited Commercial Communications or 'Spam', http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2004:0028:FIN:EN:PDF (10.05.2011).

EU, 2005, Seventh Annual Report on the Situation Regarding the Protection of Individuals with Regard to the Processing of Personal Data and Privacy in the European Union and in Third Countries

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/7th_report_prot_individs_en.pdf (06.05.2011).

EU, 2007, Treaty of Maastricht on European Union, http://europa.eu/legislation_summaries/economic_and_monetary_affairs/institutional_and_economic_framework/treaties_maastricht_en.htm (26.01.2011).

EU, 2010a, A Comprehensive Approach on Personal Data Protection in the European Union, http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf (01.02.2011).

EU, 2010b, Information Society: Main Elements of the Reform, http://ec.europa.eu/information_society/policy/ecomm/tomorrow/reform/index_en.htm (05.02.2011).

EU, 2010c, Telecoms: European Commission Launches Legal Action Against Italy over Databases for Telemarketing Purposes, http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/64 (07.04.2011).

EU, 2010d, Digital Agenda: Commission Refers UK to Court over Privacy and Personal Data Protection, http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/1215&format=HTML&aged=0&language=EN&guiLanguage=en (25.04.2011).

EU, 2011, Digital Agenda: Better Protection of Italian Consumers Against Unwanted Telemarketing Calls; European Commission Closes Legal Action, http://europa.eu/rapid/pressReleasesAction.do?reference=IP/11/411&format=HTML&aged=0&language=en&guiLanguage=en (07.04.2011).

FEILER Lukas, 2008, The Data Retention Directive, http://www.rechtsprobleme.at/doks/feiler-DataRetentionDirective.pdf (03.3.2011).

FIDIS, 2007, Future of Identity in the Information Society, Haziran 2007, http://www.fidis.net/fileadmin/fidis/deliverables/fidis-WP11-del11.5-legal_framework_for_LBS.pdf (21.03.2011).

FINA Siegfried, 2009, The Legal Framework for Unsolicited Commercial Communications in the European Union, http://unternehmensrecht.univie.ac.at/fileadmin/user_upload/privat_fina/Fina_FS_Straube.pdf (13.04.2011).

FINGER Manuela, SANDRA Schmieder, 2005, The New Law Against Unfair Competition: An Assessment, German Law Journal, Volume 6 No 1, p 201-216. http://www.germanlawjournal.com/pdfs/Vol06No01/PDF_Vol_06_No_01_201-216_Developments_Finger_Schmieder.pdf (29.04.2011).

FISHCER Hans, 2010, Communications Network Traffic Data - Technical and Legal Aspects, PrintService TU/e, Amsterdam, ISBN: 978-90-386-2339-9.

FOSS Marek, 2008, Information Technologies Bring New and Substantive Threats to Privacy, www.marekfoss.org/misc/Threats_to_Privacy.pdf (20.01.2011).

GARFINKEL Simson, SPAFFORD Gene, 2002, Web Security, Privacy and Commerce, O'Reilly Media Inc, Sebastopol.

GIAMPAOLO Silvia, SANTORSOLA Cugia F, 2011, Telecommunication Laws and Regulations 2011, http://www.iclg.co.uk/khadmin/Publications/pdf/3881.pdf (06.05.2011).

GILC, 2007, An International Survey of Privacy Laws and Practice http://gilc.org/privacy/survey/intro.html#fnlnk0017 (18.01.2011).

GLANCY Dorothy J, 1979, The Invention of the Right to Privacy, Arizona Law Review, Volume 21, Number 1, p.1-39, http://law.scu.edu/site/dorothy-glancy/File/Privacy.pdf (12.01.2011).

GLOUDEMANS Nathalie, LINDENKAMP Robichon, 2010, More Obligations for Electronic Communication Providers by Implementation of New European Framework in Telecommunications Act, http://www.mondaq.com/article.asp?articleid=121876 (06.05.2011).

GRATTON Eloise 2003, Internet and Wireless Privacy: A Legal Guide to Global Business Practices, CCH Canadian Limited, ISBN 1- 55367-180-5.

GREENLEAF Graham, 2009, Five Years of the APEC Privacy Framework: Failure or Promise Computer Law & Security Review, Volume 25, Issue 1, p.28-43.

GRITZALIS Stefanos, 2006, Privacy and Anonymity in the Digital Era, Internet Research, Volume 16, Number 2, p.117-119.

GÜLMEZ Cihan L, 2008, Kişisel Verilerin Korunması Kapsamında AB Mevzuatı ile İç Hukukumuzdaki Düzenlemelerin Karşılaştırılması,

http://www.teftis.gov.tr/dosyagoster.ashx?id=45e1f3c5-1ca1-432e-b432-471d33d4f1bf (18.04.2011).

HLADJK Jörg, 2009, Germany Adopts Stricter Data Protection Law—Impact on Financial Services Companies, http://www.hunton.com/files/tbl_s47Details/FileUpload265/2642/Germany_adopts_stricter_data_protection_law.pdf (01.05.2011).

HOLVAST Jan, 2007, The History of Information Security, Chapter 27, p.737-769.

HORNUNG Gerrit, 2009, The Federal Constitutional Court and the Online Searching Judgement, http://www.cpdpconferences.org/Resources/HornungGerrit.pdf (29.03.2011).

HUNTON&WILLIAMS, 2011, German Government Adopts Security Breach Notification Requirement in Telecommunications Act, http://www.huntonprivacyblog.com/2011/03/articles/european-union-1/german-government-adopts-security-breach-notification-requirement-in-telecommunications-act/index.html (02.05.2011).

HUSTINX Peter, 2009, Data Protection in the Light of the Lisbon Treaty and the Consequences for Present Regulations, 11th Conference on Data Protection and Data Security, Berlin, 8 June 2009, http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2009/09-06 08_Berlin_DP_Lisbon_Treaty_EN.pdf (26.01.2011).

IBLS, 2009, Holland's Telecommunication Act: the Fight Against Spam, http://www.ibls.com/internet_law_news_portal_view.aspx?s=latestnews&id=2289 (06.05.2011).

ICO, 2006, Guidance on the Privacy and Electronic Communications (EC Directive) Regulations 2003 Part 2: Security, Confidentiality, Traffic and Location Data, Itemised Billing, CLI and Directories, http://www.ico.gov.uk/upload/documents/library/privacy_and_electronic/detailed_specialist_guides/pecr_guidance_part2_1206.pdf (20.02.2011).

ICO, 2007, Guidance for Marketers on the Privacy and Electronic Communications (EC Directive) Regulations 2003 Part 1: Marketing by Electronic Means, http://www.ico.gov.uk/upload/documents/library/privacy_and_electronic/detailed_specialist_guides/guidance_part_1_for_marketers_v3.1_081007.pdf

ICO, 2010, Privacy Notices Code of Practice, http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/~/media/documents/library/Data_Protection/Detailed_specialist_guides/PRIVACY_NOTICES_COP_FINAL.ashx (20.05.2011).

ICO, 2011, Privacy Notices For Organizations, http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/privacy_notices.aspx (20.05.2011).

ISCTURKEY, 2010, Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı Sonuç Bildirgesi, http://www.iscturkey.org/2010/full.pdf (18.04.2011).

JUSTICE, 2010, Report of the Data Protection Review Group, Mart 2010, http://www.justice.ie/en/jelr/dprgfinalwithcover.pdf/Files/dprgfinalwithcover.pdf (06.05.2011).

KARANJA Stephen K, 2008, Transparency and Proportionality in the Schengen Information System and Border Control Co-Operation, Martinus Nijhoff Publishers, Netherlands.

KANUNLAR GENEL MÜDÜRLÜĞÜ (KGM), 2010, Elektronik Ticaretin Düzenlenmesi Hakkında Kanun Tasarısı, http://www.kgm.adalet.gov.tr/tbmmkom/eticaret.doc (17.04.2011).

KILKELLY Ursula, 2001, A guide to the Implementation of Article 8 of the European Convention on Human Rights, Almanya. http://www.coe.int/T/E/Human_rights/hrhb1.pdf (06.01.2011).

KIRBY Micheal, 2010, The History, Achievement and Future of the 1980 OECD Guidelines on Privacy, International Data Privacy Law, Volume 1, p.1-9, http://idpl.oxfordjournals.org/content/early/2010/09/16/idpl.ipq002.abtract, (25.12.2010)

KLOSEK Jacqueline, 2000, Data Privacy in the Information Age, Greenwood Publishing Group, United States of America.

KOENIG Christian, BARTOSCH Andreas, BRAUN Jens-Daniel, 2009, EC Competition and Telecommunications Law, Kluwer Law İnternational, Netherlands.

KOOPS Bert-Jaap, 2010, Cybercrime Legislation in the Netherlands, http://akgul.bilkent.edu.tr/oii/SSRN/cybercrime-legislation-netherlands.pdf (06.05.2011).

KOSTA Eleni, ZIBUSCHKA Jan, SCHERNER Tobias, 2008, Legal Considerations on Privacy-Enhancing Location Based Services

Using PRIME Technology, Computer Law & Security Review, Volume 24, Issue 2, p.139-146.

KOSTA Eleni, VALCKE Peggy, STEVENS David, 2009, Spam, spam, spam, spam ... Lovely spam!' Why is Bluespam different?, International Review of Law, Computers & Technology, Volume 23, Issue 1, p. 89-97.

KROES Quinten R, 2009, E-Business Law of the European Union, Kluwer Law İnternational, Netherlands.

KUNER Christopher, 2007, European Data Protection Law: Corporate Compliance and Regulation, Oxford University Press, ISBN 978-0-19-928385-9.

KUNER Christopher, 2009, An International Legal Framework for Data Protection: Issues and Prospects, Computer Law & Security Review, Volume 25, Issue 4, p.307-317.

KÜZECİ Elif, 2010, Kişisel Verilerin Korunması, Turhan, Ankara.

LINKLATERS, 2010, Report on the Status of Data Protection Legislation in Europe, Ekim 2010, http://www.linklaters.com/pdfs/extranet/DataProtected/2009_2010.pdf (02.05.2011).

LINKLATERS, 2011, Germany - Three and a Half Years' Imprisonment for Privacy Breach, Technology, Media and Telecommunications News, Ocak 2011, http://www.linklaters.com/Publications/Publication1403Newsletter/20110119/Pages/03_Germany_Three_Half_Years_Imprisonment_Privacy_Breach.aspx (02.05.2011).

LONDON ECONOMICS, 2010, Study on the Economic Benefits of Privacy-Enhancing Technologies (PETs), Temmuz 2010, http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_pets_16_07_10_en.pdf (07.04.2011).

LUCARESI Nicola, 2004, European Union vs. Spam: A Legal Response, http://research.microsoft.com/en-us/um/people/joshuago/conference/papers-2004/145.pdf (15.05.2011).

MARCELLA Albert J, STUCKI Carol G, 2003, Privacy Handbook: Guidelines, Exposures, Policy Implementation and International Issues, John Wiley&Sons Inc, New Jersey.

MOSING Max W, 2007, The Ups and Downs in the History of Eu-Spam-Regulations and Their Practical Impact, http://spamsymposium.eu/files/spamsymposium-eu-mosing.pdf (15.05.2011).

NEUWIRT Karel, 2008, New Challenge for Data Protection in Non-European States, Mexico City, http://www.infodf.org.mx/web/participantes/neuwirt/Abstract%20Karel%20Neuwirt.pdf (31.12.2010)

NEYLON Gemma, 2009, Increased Penalties for Direct Marketing, http://www.mhc.ie/fs/doc/publications/Increased_Penalties_for_Direct_Marketing_Gemma_NeylonMarch_09.pdf (06.06.2011).

ODPC, 2003, European Communities (Electronic Communications Networks and Services) (Data Protection and Privacy) Regulations, http://www.dataprotection.ie/viewdoc.asp?DocID=799&ad=1 (06.06.2011).

ODPC, 2010, Twenty First Annual Report of the Data Protection Commissioner 2009, Nisan 2010, http://www.dataprotection.ie/viewdoc.asp?DocID=906&ad=1 (06.06.2011).

ODPC, 2011a, A Guide to the European Communities (Electronic Communications Networks and Services)/(Data Protection and Privacy) Regulations 2003 as Amended by SI 526 of 2008, http://www.dataprotection.ie/viewdoc.asp?DocID=906&ad=1 (06.06.2011).

ODPC, 2011b, Direct Marketing – A General Guide for Data Controllers, http://www.dataprotection.ie/viewdoc.asp?DocID=905&ad=1#4 (06.06.2011).

OECD, 1980, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html , (25.12.2010)

OECD, 2003, Privacy Online: OECD Guidance on Policy and Practice, OECD Publishing, ISBN: 9264101624.

OPTA, 2011, Annual Report 2010, Nisan 2011, http://www.opta.nl/en/news/all-publications/publication/?id=3389 (06.05.2011).

OUT-LAW, 2003, Identifying People On-Line Violates Data Protection Laws, Says European Court, Out-Law News, 07.11.2003. http://www.out-law.com/page-4051 (12.03.2011).

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

ÖZDEMİR Sarih, 2001, Avrupa Topluluğunda İkincil Mevzuat ve Karar Alma Usulleri, http://www.dpt.gov.tr/DocObjects/Download/1007/ATIkincilMevzuatKAU.pdf (27.01.2011).

PARRILLO Giovanni, MEZZETTI Andrea, 2011, Data Protection:Italy, http://www.practicallaw.com/9-502-4794?q=*&qp=&qo=&qe= (06.05.2011).

Privacy International, 2001, Report to EU Forum on Data Retention, Kasım 2001, https://www.privacyinternational.org/article/report-eu-forum-data-retention (19.03.2011).

Privacy International, 2011a, France Privacy Profile, https://www.privacyinternational.org/article/france-privacy-profile (03.05.2011).

Privacy International, 2011b, Netherlands Privacy Profile, https://www.privacyinternational.org/article/netherlands-privacy-profile (06.05.2011).

Privacy International, 2011c, Italy Privacy Profile, https://www.privacyinternational.org/article/italy-privacy-profile#regulator (06.05.2011).

Privacy International, 2011d, Ireland Privacy Profile, https://www.privacyinternational.org/article/ireland-privacy-profile (06.06.2011).

PRIV, 2009, Top 10 Ways Your Privacy is Threatened. http://www.priv.gc.ca/resource/dpd/top10_e.cfm (20.01.2010).

PROUST Olivier, 2009a, Notification of Data Security Breaches in France, http://www.jdsupra.com/post/documentViewer.aspx?fid=8b566d08-de56-4de7-b181-7058d8fd92e5 (04.05.2011).

PROUST Olivier, 2009b, French Senate Proposes Amendments to the Data Protection Act http://www.jdsupra.com/post/documentViewer.aspx?fid=45a5b43f-64d4-4217-9a1d-a3b4e124673f (04.05.2011).

PROUST Olivier, 2010, French Senate's proposed Bill to amend Data Protection Act, http://www.jdsupra.com/post/documentViewer.aspx?fid=6f2c9135-11dc-4064-8c54-5a09dd65a0fe (04.05.2011).

RANNENBERG Kai, ROYER Denis, Deuker Andre, Future of Identity in the Information Society, 2009, Springer, Almanya.

RODRIGUES Roberto J, WILSON Petra, SCHANZ Stephen J, 2001, The Regulation of Privacy and Data Protection in the Use of Electronic Health Information, Pan American Health Org, Washington.

RUNTE Christian M, 2010, Data Breach Laws: EU Framework and Implementation, European Card Acquiring Forum – Berlin, 25 Şubat 2010.

SMART, 2009, Spam and Spyware Study Final Report, Nisan 2009, http://ec.europa.eu/information_society/policy/ecomm/doc/library/ext_studies/privacy_trust_policies/spam_spyware_legal_study2009final.pdf (06.05.2011).

STEVENS David, 2009, The Revised European Framework for the Electronic Communications Sector: Promoting Investment in Infrastructure and EuropeanHarmonisation?http://didactiek.edm.uhasselt.be/jurinf/uploads/Main/ecommunications_2009.pdf (05.02.2011).

STIBBE, 2010, EU – New European E-Privacy Rules, ICT Law Newsletter, Sayı 37, Şubat 2010, http://www.stibbe.com/upload/1438c6f980127235104740l3bcc.pdf (06.05.2011).

ŞİMŞEK Oğuz, 2008, Anayasa Hukukunda Kişisel Verilerin Korunması, Beta, İstanbul.

TEMPEST Alastair, 2007, Robinson Lists for Efficient Direct Marketing, International Direct Marketing, KRAFFT Manfred, HESSE Jürgen (der.), Springer, Germany, p. 128-153.

TSATSOU Panayiota, 2011, EU Regulations on Telecommunications: The Role of Subsidiarity and Mediation, First Monday, Volume 16, Number 1-3, http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/issue/view/330 (06.03.2011).

UN General Assembly, Guidelines for the Regulation of Computerized Personal Data Files, 14 December 1990, http://www.unhcr.org/refworld/docid/3ddcafaac.html ,(27.12.2010).

WATERS Nigel, 2009, The APEC Asia-Pacific Privacy Initiative – A New Route to Effective Data Protection or a Trojan Horse for Self-Regulation, SCRIPTed, Volume 6, Issue 1, p.75-89.

WRIGHT Tom, HUSTINX Peter, 1995, Privacy-Enhancing Technologies: The Path to Anonymity Volume 1, Ağustos 1995, http://www.ontla.on.ca/library/repository/mon/10000/184530.pdf

YLOUSES Laure, GAY Solene, 2011, A Practical Insight to Cross-Border Telecommunication Laws and Regulations: France, http://www.iclg.co.uk/index.php?area=4&country_results=1&kh_publications_id=157&chapters_id=3877 (03.05.2011).

YÜKSEL Mehmet, 2003, Mahremiyet Hakkı ve Sosyo-Tarihsel Gelişimi, Ankara Üniversitesi SBF Dergisi, C.58 S.1 http://www.politics.ankara.edu.tr/eski/dergi/pdf/58/1/9_mehmet_yuksel.pdf (12.01.2011)

YÜKSEL Mehmet, 2009, Mahremiyet Hakkına ve Bireysel Özgürlüklere Felsefi Yaklaşımlar, Ankara Üniversitesi SBF Dergisi, C.64 S.1. http://www.politics.ankara.edu.tr/eski/dergi/pdf/64/1/10-yuksel_mehmet.pdf (12.01.2011).

EK

Karşılaştırmalı Tablo

Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik (06.02.2004 Tarih ve 25365 Sayılı Resmi Gazete)	Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik Taslağı (25.12.2009)
BİRİNCİ BÖLÜM **Genel Hükümler** **Amaç ve Kapsam** **Madde 1** — Bu Yönetmeliğin amacı, telekomünikasyon sektöründe kişisel bilgilerin işlenmesi ve gizliliğinin korunmasının güvence altına alınmasına ilişkin usul ve esasları düzenlemektir. Bu Yönetmelik, telekomünikasyon sektöründe hizmet veren ve alan gerçek ve tüzel kişileri kapsar.	**BİRİNCİ BÖLÜM** **Genel Hükümler** **Amaç ve kapsam** **MADDE 1** — Bu Yönetmeliğin amacı, elektronik haberleşme sektöründe kişisel verilerin işlenmesi, saklanması ve gizliliğinin korunması amacıyla elektronik haberleşme sektöründe hizmet veren işletmeciler ile hizmet alan gerçek ve tüzel kişilerin uyacakları usul ve esasları düzenlemektir.
Hukuki Dayanak **Madde 2** — Bu Yönetmelik, 4/2/1924 tarihli 406 sayılı Telgraf ve Telefon Kanunu ile 5/4/1983 tarihli 2813 sayılı Telsiz Kanununa dayanılarak hazırlanmıştır.	**Hukuki dayanak** **MADDE 2** — (1) Yönetmelik, 05/11/2008 tarih ve 5809 sayılı Elektronik Haberleşme Kanununun 4, 6 ve 51 inci maddelerine dayanılarak hazırlanmıştır.

Tanımlar	Tanımlar ve kısaltmalar
Madde 3 — Bu Yönetmelikte geçen; Kurul: Telekomünikasyon Kurulunu, Kurum: Telekomünikasyon Kurumunu, Abone: Telekomünikasyon hizmeti sunan bir işletmeci ile ilgili hizmetten yararlanmaya ilişkin sözleşme yapan gerçek veya tüzel kişiyi, Alıcı: Resmi görevi çerçevesinde bilgileri elde edebilecek makamların dışında kalan ve kişisel bilgilerine erişebilen kamu kurum ve kuruluşları ile her türlü gerçek ya da tüzel kişiyi, Arama: Haberleşmeye imkân tanıyan kamuya açık bir telekomünikasyon hizmeti yoluyla kurulan bir bağlantıyı, Ara bağlantı: İki ayrı telekomünikasyon şebekesi arasındaki telekomünikasyon trafiğinin gerçekleştirilmesini teminen iki şebekenin birbirine irtibatlandırılmasını, Elektronik mektup: Telekomünikasyon hizmetini kullanan tarafından toplanacağı ana kadar şebekede veya alıcının terminal cihazında depolanabilir nitelikteki şebeke üzerinden gönderilen yazılı, sesli, görüntülü mesajı, İşletmeci: Türk Telekom da dâhil olmak üzere, Kurum ile yapılan bir görev sözleşmesi, imtiyaz sözleşmesi ve/veya Kurumdan alınan bir	**MADDE 3** — (1) Bu Yönetmelikte geçen; a) Abone: Bir işletmeci ile elektronik haberleşme hizmetinin sunumuna yönelik olarak yapılan bir sözleşmeye taraf olan gerçek ya da tüzel kişiyi, b) Acil yardım çağrıları: Ulusal ve uluslararası düzenlemelerde kabul görmüş yangın, sağlık, doğal afetler ve güvenlik gibi acil durumlarla ilgili olarak itfaiye, polis, jandarma, sağlık ve benzeri kuruluşlara yardım talebiyle yapılan aramaları, c) Arama: Kamuya açık bir telefon hizmeti yoluyla kurulan ve çift yönlü haberleşmeye imkân sağlayan gerçek zamanlı bağlantıyı, ç) Gerçekleşmeyen arama: Başarılı bir şekilde bağlantı kurulmasına rağmen, aranan tarafın cevap vermemesi ya da şebeke yönetiminden kaynaklanan bir nedenle görüşmenin gerçekleşmemesini, d) Hücre kimliği: Mobil telefon çağrısının başladığı ya da sona erdiği hücrenin kimliğini,

telekomünikasyon ruhsatı veya genel izin uyarınca telekomünikasyon hizmetleri yürüten ve/veya telekomünikasyon altyapısı işleten bir sermaye Şirketini, İsimsizleştirme: Arayan veya aranan numara veya kişiye ait özel bilgilerin görüntüsünün veya bilgisinin görünürlüğünün ortadan kaldırılmasını, Katma değerli telekomünikasyon hizmetleri: Aboneler arasında iletilen ses ve veri dâhil her türlü mesajın formu, muhtevası, kodu, protokolü veya benzer hususları üzerinde bilgisayar işlemleri veya başka surette işlem yapıp, aboneye veya kullanıcıya ilave, farklı veya yeniden yapılandırılmış bir mesaj ileten veya yüklenilmiş, kaydedilmiş mesaj ve veriler ile aboneler arası iletimi sağlayan telekomünikasyon hizmetlerini, Kişisel bilgiler/veriler: Tanımlanmış ya da doğrudan veya dolaylı olarak, bir kimlik numarası ya da fiziksel, psikolojik, zihinsel, ekonomik, kültürel ya da sosyal kimliğinin, sağlık, genetik, etnik, dini, ailevi ve siyasi bilgilerinin bir ya da birden fazla unsuruna dayanarak tanımlanabilen gerçek ve/veya tüzel kişilere ilişkin herhangi bir bilgiyi, Kişisel bilgilerin işlenmesi: Otomatik olsun olmasın, toplama, kaydetme, hazırlama, yükleme, uyarlama, değiştirme, geri çağırma, danışma, kullanma, aktarma yoluyla açığa vurma, yayma ya da	e) IMSI: Uluslararası mobil abone kimliğini, f) IMEI: Uluslararası mobil cihaz kimliğini, g) İsimsizleştirme: Kişisel verilerin, belirli veya kimliği belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek veya kaynağı belirlenemeyecek hale getirilmek suretiyle işlenmesini, ğ) Kişisel veri: Belirli veya kimliği belirlenebilir gerçek ve tüzel kişilere ilişkin bütün bilgileri, h) Kişisel verilerin işlenmesi: Kişisel verilerin otomatik olan veya olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, değiştirilmesi, silinmesi veya yok edilmesi, yeniden düzenlenmesi, açıklanması veya başka bir şekilde elde edilebilir hale getirilmesi, üçüncü kişilere aktarılması, kullanılmasının sınırlanması amacıyla işaretlenmesi, tasniflenmesi veya kullanılmasının engellenmesi gibi bu veriler üzerinde gerçekleştirilen işlem ya da işlemler bütününü,

bunların dışında erişilebilir hale getirme, düzenleme, birleştirme, engelleme, silme gibi yollardan, kişisel bilgiler üzerinden yürütülmekte olan herhangi bir işlem ya da işlemler bütününü, Kısa mesaj: Kullanıcıya, herhangi bir telekomünikasyon cihazı aracılığıyla kısa yazılı mesaj alma ve gönderme imkânı sağlayan hizmeti, Kullanıcı: Aboneliği olup olmamasına bakılmadan telekomünikasyon hizmetlerinden yararlanan gerçek kişiyi, Şebeke: Bir veya birden fazla noktada telekomünikasyonu sağlamak için bu noktalar arası bağlantıyı teşkil eden anahtarlama teçhizatı ve hatlar da dâhil olmak üzere her türlü iletişim sistemleri ağını, Trafik verisi: Bir şebekede haberleşmenin iletimi veya faturalama amacıyla işlenen her türlü veriyi, Telekomünikasyon: Her türlü işaret, sembol, ses ve görüntünün ve elektrik sinyallerine dönüştürülebilen her türlü verinin kablo, telsiz, optik, elektrik, manyetik, elektro manyetik, elektrokimyasal, elektromekanik ve diğer iletim sistemleri vasıtasıyla iletilmesi, gönderilmesi ve alınmasını, Telekomünikasyon hizmeti: Telekomünikasyon tanımına giren faaliyetlerin bir kısmının veya tümünün hizmet olarak sunulmasını, Üçüncü şahıs: Kamu kurum ve kuruluşları ile her türlü özel ve tüzel	ı) Konum verisi: Kamuya açık elektronik haberleşme hizmeti kullanıcısına ait bir cihazın coğrafi konumunu belirleyen ve elektronik haberleşme şebekesinde işlenen belirli veriyi, i) Kullanıcı: Aboneliği olup olmamasına bakılmaksızın elektronik haberleşme hizmetlerinden yararlanan gerçek veya tüzel kişiyi, j) Kullanıcı Kimliği: Kişilere, abonelik işlemi sırasında, internet erişimi hizmetlerine ya da internet haberleşme hizmetlerine kayıt yaparken tahsis edilen, tek ve kişiye özel tanımlamayı, k) Kurul: Bilgi Teknolojileri ve İletişim Kurulunu, l) Kurum: Bilgi Teknolojileri ve İletişim Kurumunu, m) Rıza: İlgili kişinin özgür kararı ile, kendisine ait kişisel verinin işlenmesine yönelik, verinin işlenmesi kapsam ve amacı dâhilinde ve verinin işlenmesi öncesinde verdiği kabulü gösterir

kişileri ya da verilerin ilgili olduğu kişi, Kurum veya işlemcinin doğrudan yetkisi altında verileri işlemekle yetkilendirilen kişiler dışındaki herhangi bir kurum veya kişiyi, Yer verisi: Kamuya açık telekomünikasyon hizmeti kullanıcısına ait bir telekomünikasyon cihazının coğrafi konumunu belirleyen şebekede işlenen her türlü veriyi, ifade eder.	irade beyanını, n) Tanımlayıcı veri: Rehberlik hizmetinin sunumu için mecburi olan ve aynı ad ve soyada sahip kişilerin ayrıştırılmasını sağlayacak en genel kişisel bilgiyi, o) Trafik verisi: Bir elektronik haberleşme şebekesinde haberleşmenin sağlanması veya faturalama amacıyla işlenen her türlü veriyi, ö) Veri: Abone ya da kullanıcıyı teşhis etmek için yararlanılan trafik verisi, konum verisi ya da ilgili diğer bilgileri, ifade eder. (2) Bu Yönetmelikte geçen ve yukarıda yer almayan tanımlar ve kavramlar için ilgili mevzuatta yer alan tanımlar geçerlidir.

İKİNCİ BÖLÜM Uygulama Esasları	İKİNCİ BÖLÜM Uygulama Esasları
Uygulama **Madde 4** — Bu Yönetmelik, şebekelerde telekomünikasyon hizmetlerinin sağlanmasına ilişkin kişisel bilgilerin işlenmesi ve gizliliğinin korunması konusunda uygulanır.	**Kişisel verilerin işlenmesine ilişkin ilkeler** **MADDE 4** — (1) Kişisel verilerin; a) Hukuka ve dürüstlük kurallarına uygun olarak ancak ilgili kişinin rızasına dayalı olarak işlenmesi, b) Bu Yönetmelik hükümleri dâhilinde toplanması ve bu hükümlere aykırı olarak yeniden işlenmemesi, c) Toplandıkları amaçla bağlantılı, yeterli ve orantılı olması, ç) Doğru olması ve gerektiğinde güncellenmesi, d) İlgili kişilerin kimliklerini belirtecek biçimde ve kaydedildikleri veya yeniden işlenecekleri amaç için gerekli olan süre kadar muhafaza edilmesi, esastır.
Uygulama Kapsamı **Madde 5** — Yönetmeliğin, 12,13, 14 ve 18 inci maddeleri yalnızca sayısal ve uygun işaretleşme sistemine sahip santrallerde hizmet	

alan aboneler için uygulanır. Bu maddenin uygulanmasının teknik olarak mümkün olmadığı durumlar ile aşırı mali yük getirdiği durumlar, işletmeciler tarafından gerekçeli olarak Kuruma bildirilir. Kurum tarafından teknik imkânsızlık veya aşırı mali yük getirdiğinin tespit edildiği durumlarda bu maddeler uygulanmaz	
Güvenlik **Madde 6** — İşletmeciler verdikleri hizmetlerin güvenliğini sağlamak amacıyla, hizmetin gerektirdiği hallerde şebekenin güvenliğine ilişkin alacakları tüm gerekli teknik ve yapısal önlemleri Kurumun onayına sunar.	**Güvenlik** **MADDE 5** — (1) İşletmeciler, şebekelerinin ve sundukları hizmetlerin güvenliğini sağlamak amacıyla uygun teknik ve idari tedbirleri alır. Söz konusu güvenlik tedbirleri, teknolojik imkânlar ve uygulama maliyetleri de göz önünde bulundurularak muhtemel riske uygun bir düzeyde sağlanır. (2) Kurum, gerekli gördüğü hallerde işletmecilerden, aldıkları güvenlik tedbirlerine ilişkin bilgileri isteme ve söz konusu güvenlik tedbirlerinde değişiklik talep etme hakkını haizdir.

Riski Haber Verme **Madde 7** — İşletmecinin verdiği hizmetlerle ilgili olarak şebeke güvenliğinin ihlaline ilişkin, işletmeci tarafından alınan önlemlerin dışında olağanüstü bir risk söz konusu olduğunda işletmeci, riskler ve riskin giderilme yolları konusunda derhal abonelerini uyarır.	**Riskin bildirilmesi** **MADDE 6** — (1) İşletmeci, şebekesinin güvenliğini ihlal eden belirli bir risk olması durumunda bu risk hakkında Kurumu ve abonelerini bilgilendirmekle yükümlüdür. (2) Bu riskin işletmeci tarafından şebeke güvenliğini sağlamaya yönelik olarak alınan tedbirlerin dışında kalması halinde söz konusu riskin içeriği ve giderilme yolları hakkında abonelerin etkin ve hızlı bir şekilde bilgilendirilmesi sağlanır.
Telekomünikasyonun Gizliliği **Madde 8** — Yasaların ve yargı kararlarının öngördüğü durumlar haricinde, haberleşmeye taraf olanların tamamının izni olmaksızın, telekomünikasyonun üçüncü şahıs tarafından dinlenmesi, kaydedilmesi, saklanması, kesilmesi veya gözetimi yasaktır. İlgili trafik verilerinin ise işletmeci tarafından hizmet amaçları dışında kaydedilmesi, saklanması ve gözetimi yasaktır.	

ÜÇÜNCÜ BÖLÜM **Trafik Verisi** **İzin ve Süre** **Madde 9** — Telekomünikasyon hizmetlerini pazarlamak ya da katma değerli hizmetleri sağlamak amacıyla; abone veya kullanıcı kişisel bilgilerinin kullanılmasına izin verirse, işletmeci bu tür hizmetler ve pazarlama için gerekli kapsam ve sürede veriyi işleyebilir. Kullanıcı ve aboneler, kişisel bilgilerinin işlenmesi için verdikleri izinleri her zaman geri alabilirler. İşletmeci; abonenin veya kullanıcının onayını almak koşuluyla, telekomünikasyon hizmetlerinin pazarlanması ya da katma değerli hizmetlerin sağlanması amacıyla, işlenen kişisel bilgileri ve bu tür işlemin süresini abone ve kullanıcılara bildirecektir.	**ÜÇÜNCÜ BÖLÜM** **Verilerin İşlenmesi ve Saklanması** **Trafik verisinin işlenmesi** **MADDE 7** — (1) İşletmeci tarafından abonelere ve kullanıcılara ait işlenen ve saklanan trafik verilerinin, bu verilerin işlenmesi ve saklanmasını gerekli kılan faaliyetin tamamlanmasından sonra silinmesi veya isimsizleştirilmesi esastır. (2) Trafik verisi ancak, ilgili mevzuat hükümlerine uygun olarak, trafiğin yönetimi, arabağlantı, faturalandırma ve benzeri işlemleri gerçekleştirmek veya tüketici şikâyetleri ile arabağlantı ve faturalandırma anlaşmazlıkları başta olmak üzere uzlaşmazlıkların çözümü amacıyla işlenir. (3) Elektronik haberleşme hizmetlerini pazarlamak veya katma değerli hizmetler sunmak amacıyla ihtiyaç duyulan trafik verileri, ilgili abonelerin veya kullanıcıların işlenecek trafik verisinin türü ve süresi hakkında bilgilendirilmelerinden sonra rızasının alınması kaydıyla ve sadece söz konusu hizmetlerin

	veya pazarlamaların gerektirdiği ölçüde ve süre boyunca işlenebilir. Aboneler veya kullanıcılar, trafik verilerinin işlenmesi için vermiş oldukları rızayı her zaman geri alabilirler. **Trafik verisini işleme yetkisi** **MADDE 8** — (1) Trafik verisi işleme yetkisi sadece, faturalandırma veya trafik yönetimi, tüketici şikâyetleri, elektronik haberleşme hizmetlerinin pazarlanması veya katma değerli hizmetlerin sunulması ile görevli, işletmecinin kendi bünyesindeki ve işletmeci tarafından yetkilendirilmiş kişiler tarafından, görevin gerektirdiği kapsamda kullanılır.
Trafik Verisi İşleme Yetkisi **Madde 10** — Trafik verilerinin işlenmesi yetkisi; işletmecinin yetkisi altındaki kişiler ile telekomünikasyon hizmetlerinin faturalama ve trafik idaresi, müşteri hizmetleri, yolsuzluk tespitleri, elektronik telekomünikasyon hizmetleri pazarlama veya katma değerli hizmet ile görevli kişilere münhasırdır.	**Trafik verisinin bildirilmesi** **MADDE 9** — (1) Bu Yönetmelik kapsamında, trafik verisi ancak arabağlantı ve faturalandırma uzlaşmazlıkları başta olmak üzere uzlaşmazlıkların çözümü amacıyla talep edilmesi halinde mevzuat uyarınca yetkilendirilmiş taraflara bildirilir.
Yetkili Makama Bildirim **Madde 11** — Trafik verisi; arabağlantı, faturalama veya benzeri anlaşmazlıkları çözmek amacıyla mahkeme veya uyuşmazlığı	**Trafik verisinin gizliliği** **MADDE 10** — (1) Elektronik haberleşme hizmetleri ve/veya şebekesi aracılığıyla gerçekleştirilen

çözmekle yetkili gerçek ve tüzel kişilere bildirilebilir.	elektronik haberleşme ve ilgili trafik verisinin gizliliği esas olup, yasaların ve yargı kararlarının öngördüğü durumlar haricinde, haberleşmeye taraf olanların tamamının rızası olmaksızın, ilgili trafik verisinin üçüncü kişiler tarafından kaydedilmesi, saklanması, izlenmesi yasaktır. (2) Elektronik haberleşme sektöründe faaliyette bulunan işletmeciler tarafından hizmetin kapsamı dışındaki amaçlar için ilgili trafik verisinin, kaydedilmesi, saklanması, izlenmesi yasaktır.
Ayrıntılı Faturalar **Madde 12** — Aboneler taleplerine uygun olarak ayrıntılı veya ayrıntısız fatura alma hakkına sahiptir.	
Arayan Hattın Kimliğinin Açıklanmasının Engellenmesi **Madde 13** — İşletmeci, aramayı yapan abonesine basit bir yöntemle ve ücretsiz olarak her arama için arayan hattın kimliğinin açıklanmasını engelleme olanağını tanır. İşletmeci söz konusu imkândan abonelerini ücretsiz olarak haberdar etmekle yükümlüdür.	
Arayan Hattın Bağlanmasının Engellenmesi **Madde 14** — Arayan hattın kimliğinin gizlendiği durumlarda; işletmeci abonenin isteğine bağlı ve ücretsiz olarak gelecek	

aramaların aboneye ulaşmasını engeller. İşletmeci söz konusu imkândan abonelerini ücretsiz olarak haberdar etmekle yükümlüdür.	
Yer Verisi **Madde 15** — Abone ve kullanıcılarla ilgili yer verileri sadece abone ve kullanıcıların isimsizleştirildiği veya katma değerli bir hizmetin sağlanması için gereken kapsam ve sürede abonelerin aksi başvuruları olmadığı hallerde işlenebilir. İşletmeciler, işlenecek yer verisi tipini, işlemenin amaç ve süresi ile bu bilgilerin üçüncü şahıslara katma değerli hizmet sağlama amacıyla gönderilip gönderilmeyeceği hususlarında, aboneleri bilgilendirir. Aboneler, yer verilerinin işlenmemesi için her zaman başvuru yapabilirler. **Geçici Red** **Madde 16** — İşletmeciler kullanıcı veya abonelere yer verilerinin	**Konum verisinin işlenmesi** **MADDE 11** — (1) İşletmeciler, abone/kullanıcının konum verisini ancak, katma değerli elektronik haberleşme hizmetlerinin sağlanması için gerekli olan ölçü ve süre dâhilinde abone/kullanıcıların rızasıyla veya abone/kullanıcı verisinin isimsizleştirilmesi halinde işleyebilir. (2) Söz konusu işleme ilişkin olarak işletmeciler; abone/kullanıcıların rızasını almadan önce, işlenecek konum verisinin türü, işlenme amacı, süresi ve katma değerli elektronik haberleşme hizmetlerinin sağlanması amacıyla üçüncü kişilere iletilip iletilmeyeceği hakkında abone/kullanıcıları bilgilendirir. Abone/kullanıcılar konum verisinin işlenmesi için verdikleri rızayı her zaman geri alabilirler. (3) Konum verisinin işlenmesine rıza verildiği durumlarda; abone/kullanıcıya, ücretsiz ve basit bir

işlenmesini geçici olarak reddetme olanağını, basit bir yöntemle ve ücretsiz olarak, şebekeye her bağlantı için sağlarlar.	yöntemle şebekeye her bağlanışta veya her bir veri iletiminde geçici olarak veri işlenmesini reddetme olanağı sağlanır. (4) Abone/kullanıcının rızası dışında konum verisine ilgili mevzuat çerçevesinde ancak acil yardım çağrıları kapsamında yetkili makamların erişmesi mümkündür.
Kişi Sınırlandırması **Madde 17** — Yer verilerinin işlenmesi yetkisi, şebeke ve/veya işletmecinin veya katma değerli hizmet sağlayan üçüncü kişilerin yetkisi altındaki kişilere münhasırdır. Ancak bu yetki, telekomünikasyon hizmetinin sağlanması amacının gerektirdiği ölçüde yapılmalıdır.	**Konum verisini işleme yetkisi** **MADDE 12** — (1) Konum verisini işleme yetkisi sadece, işletmecinin kendi bünyesinde görevli ve işletmeci tarafından yetkilendirilmiş olan ve katma değerli hizmetleri sağlayan üçüncü kişilerle sınırlı olup, bu yetki söz konusu hizmetlerin gerektirdiği kapsamda kullanılır.
İstisnai Durumlar **Madde 18** — Kötü niyetli veya rahatsızlık verici aramaların takibi amacıyla, abone tarafından yapılan başvuru üzerine, arayan abonenin kimliğini içeren bilgiler, 1 (bir) yıl süreyle saklanmalı ve ilgili mevzuata göre erişilebilir olmalıdır. Kolluk güçleri, ambülâns ve itfaiye hizmetleri dâhil tüm acil aramalara	

ilişkin çağrılara cevap verme amacıyla; abonenin veya kullanıcının rızası olmasa bile abonenin yer verisini ve kimliğini, kullanıcının ise yer verisini içeren bilgilere erişilebilir olmalıdır.	
	Saklanacak veri kategorileri **MADDE 13** — (1) Bu Yönetmelik kapsamında saklanması öngörülen veri kategorileri, aşağıda belirtilmiştir. a) Haberleşmenin takibi ve kaynağının tanımlanması için: 1. Sabit telefon şebekeleri ve mobil telefon şebekeleriyle ilgili olarak; gerçekleşmeyen aramalar da dâhil olmak üzere arayan hatta ait telefon numarası, abonenin veya kullanıcının adı ve adresi, arayan hattın hangi tarihte hangi aboneye tahsis edildiğine ait bilgi. 2. İnternet ortamına erişim ve internet telefonu ile ilgili olarak; tahsis edilmiş kullanıcı kimliği, telefon şebekesine erişim

	için tahsis edilmiş kullanıcı kimliği veya telefon numarası, haberleşmenin gerçekleştiği andaki internet protokol adresi, kullanıcı kimliği veya telefon numarasının tahsis edildiği abonenin adı ve adresi. b) Haberleşmenin son bulacağı noktayı belirlemek için: 1. Sabit şebeke telefonları ve mobil telefonlarla ilgili olarak; aranan numaralar, çağrı iletme ve çağrı transferi gibi ek hizmetlerin olması durumunda çağrının yönlendirildiği numara veya numaralar, abonelerin adı ve adresi. 2. İnternet ortamına erişim ve internet telefonu ile ilgili olarak; internet telefonu ile aranmak istenen alıcılara ait kullanıcı kimliği veya telefon numarası, abonelerin adı ve adresi ve haberleşme için aranmak istenen alıcılara ait kullanıcı kimliği. c) Haberleşmenin tarihi, zamanı ve süresini belirlemek için:

	1. Sabit ve mobil telefon hizmeti ile ilişkin; haberleşmenin başlangıç ve bitiş tarih ve zamanı. 2. İnternet erişimi, elektronik posta ve internet telefon hizmetine ilişkin; İnternet erişimi ile ilgili oturum açma ve kapatma tarihi ve zamanı, internet servis sağlayıcısı tarafından tahsis edilen dinamik veya statik İnternet Protokol adresi, abone / kullanıcı kimliği, elektronik posta veya İnternet telefonu ile ilgili oturum açma ve kapatma tarihi ve zamanı. ç) Haberleşmenin türünü tanımlamak için: 1. Sabit telefon hizmeti ve mobil telefon hizmeti ile ilgili olarak; kullanılan telefon hizmeti. 2. İnternet ortamına erişim ve internet telefonu ile ilgili olarak kullanılan internet hizmeti. d) Kullanıcıların haberleşme cihazlarını veya bunların ekipmanlarını tanımlamak için:

	1. Sabit telefon hizmeti ile ilgili olarak; arayan ve aranan telefon numaraları 2. Mobil telefonla ilgili olarak; aranan ve arayan telefon numaraları, arayan tarafa ait IMSI, arayan tarafa ait uluslararası mobil cihaz kimliği IMEI, aranan tarafa ait IMSI, aranan tarafa ait IMEI, abone kaydı olmayan arama kartlı hizmetlerin olması durumunda hizmetin aktif hale getirildiği tarih ve zaman ile hizmetin aktif hale getirildiği hücre kimliği. 3. İnternet ortamına erişim ve internet telefonu ile ilgili olarak; çevirmeli ağ erişimi için arayan telefon numarası, sayısal abone hattı numarası ya da haberleşmenin kaynaklandığı diğer nokta. e) İlgili mevzuatın öngördüğü hallerde mobil haberleşme cihazının konumunu tespit etmek için; haberleşmenin başladığı hücre kimliği, haberleşme verilerinin saklandığı sürede hücre kimlikleri ile ilgili olarak hücrelerin coğrafik

	konumlarını tanımlayan veri, hücre adresi ve hücre kimliğinin o adrese atanma ve kaldırılma tarihleri. (2) Haberleşmenin içeriğine ilişkin verilerin saklanması bu Yönetmeliğin kapsamına dâhil değildir.
	Veri saklama süresi **MADDE 14** — (1) 13 üncü madde kapsamında tanımlanan veri kategorileri, haberleşmenin gerçekleştiği tarihten itibaren işletmeciler tarafından 1 (bir) yıl süre ile saklanır.
	Saklanan verinin korunması ve güvenliği **MADDE 15** — (1) Bu Yönetmelik kapsamında saklanması öngörülen veriler için işletmeciler asgari olarak aşağıdaki şartları yerine getirmekle yükümlüdür: a) Saklanan veriler ile şebekedeki diğer verilerin aynı kalite, güvenlik ve koruma özelliklerine tabi olmasını, b) Saklanan verilerin, istem dışı veya yasadışı tahrip, istem dışı kayıp ya da değişiklik veya yetki dışı ya da yasadışı depolama, işleme,

	erişim ve ifşa olaylarına karşı uygun teknik ve idari tedbirlerin alınması, c) Verilerin sadece özel yetkilendirilmiş kişiler tarafından erişilebilir olmasının sağlanması için uygun teknik ve idari tedbirlerin alınması, ç) İşlenen ve saklanan verinin saklama süresi sonunda imha edilmesi. (2) İşletmeciler sundukları hizmetler kapsamında elde ettikleri verilerin gizliliği ve güvenliğini her aşamada sağlamakla yükümlü olup, bu yükümlülük bazı işlemlerin işletmeci tarafından yetkilendirilmiş kişiler marifetiyle yapılması halini de kapsar. (3) İşletmeciler, yasaların yetkili kıldığı makamlarca talep edilmesi halinde, saklanan veri ve söz konusu veriye ilişkin gerekli tüm bilgilere erişimi, ilgili makam tarafından belirtilen süre içinde sağlamakla yükümlüdür.

	İstatistikî bilgilerin verilmesi **MADDE 16** — (1) Bu Yönetmelik kapsamında saklanması öngörülen kişisel verileri içermeyen istatistikî bilgiler, her yılın Ocak ayı içerisinde bir önceki yılın bilgilerini kapsayacak şekilde Kuruma gönderilir. Bu istatistikî bilgiler; a) Yürürlükteki mevzuat çerçevesinde yetkili makamlar tarafından talep edilen hususları, b) Verinin saklandığı tarih ile yetkili makamlar tarafından talep edildiği tarih arasında geçen süreyi, c) Veri talebinin karşılanamadığı durumları, kapsar.

	DÖRDÜNCÜ BÖLÜM **Sağlanan İmkânlar** **Numaranın gizlenmesi** **MADDE 17** — (1) İşletmeci tarafından arayan numaranın görünmesine imkân verildiği durumlarda, işletmeci aynı zamanda; a) Arayan kullanıcıya her bir arama için basit bir yöntemle ve ücretsiz olarak numarasını gizleme olanağı sağlamakla, b) Arayan kişinin numarasını gizlediği durumlarda, aranan abonenin isteğine bağlı ve ücretsiz olarak, gelecek aramaların abone tarafından reddedilmesini sağlamakla yükümlüdür. (2) Ayrıca, bağlanan hattın numarasının görünebilir olduğu durumlarda, aranan abonenin talep etmesi halinde işletmeci tarafından, ücretsiz ve basit bir

	yöntemle aramanın gerçekleştiğinin arayan tarafından bilinmesi engellenir. (3) İşletmeciler, yukarıda belirtilen hizmet imkânları hakkında abonelerini ve kamuoyunu kısa mesaj, internet, basın, yayın organları, posta veya benzeri araçlarla ücretsiz olarak bilgilendirmekle yükümlüdür.
	Otomatik çağrı yönlendirme **MADDE 18** — (1) İşletmeciler, abone veya kullanıcının telefon cihazına üçüncü kişiler tarafından yapılan yönlendirmeleri abonenin ücretsiz ve basit bir yöntemle engellemesine imkân sağlarlar. (2) İşletmeciler abone veya kullanıcının rızası olmaksızın aboneye veya kullanıcıya doğru yapılan aramaları başka bir numaraya veya otomatik mesaj sistemine yönlendiremez.

Aboneler İçin Hazırlanan Rehberler **Madde 19** — Aboneler, yazılı ve elektronik abone rehberlerinin, yayınlanma amaçları hakkında rehbere kayıt edilmeden önce ücretsiz olarak bilgilendirilirler. Aboneler istedikleri zaman, abonelik bilgilerinin rehberlerde düzeltilmesini, teyit edilmesini ve/veya çıkarılmasını ücretsiz olarak talep edebilirler. Abonelerin ad ve soyadlarına dayalı kişisel bilgilerine erişim dışındaki rehberlik hizmetleri için abonenin ek onayı alınır.	**Aboneler için hazırlanan rehberler** **MADDE 19** — (1) Aboneler, yazılı ve/veya elektronik abone rehberlerinin, yayımlanma amaçları ve bu rehberlerde yer alacak kişisel veriler ile bu rehberlerin elektronik sürümlerinde olabilecek arama fonksiyonları ve kullanım imkânları hakkında rehbere kayıt edilmeden önce ücretsiz olarak bilgilendirilirler. (2) Kamuya açık rehberlerde yer alan kişisel veriler, rehberlik hizmeti sağlayıcısının rehberin amacına uygun olarak belirlediği kapsamda verilecek olup, aboneler istedikleri zaman, rehberde yer alan kişisel verilerinin düzeltilmesini, teyit edilmesini ve/veya çıkarılmasını ücretsiz olarak talep edebilirler. (3) Abonelerin ad ve soyadları ile rehberlik hizmetinin sunumu için mecburi olan tanımlayıcı veriler dışındaki kişisel bilgileri kullanılarak yapılacak sorgulamalar için abonenin ilave rızası aranır.

İstek Dışı Haberleşme **Madde 20** — İşletmeciler kişi müdahalesi olmadan çalışan fakslar, elektronik posta, kısa mesaj gibi otomatik arama sistemlerini, abonenin önceden izni olmadan siyasi propaganda amacıyla kullanamazlar. Söz konusu otomatik arama sistemlerinin doğrudan pazarlama amacıyla kullanılması halinde kullanıcılara gelen her bir mesajı bundan sonrası için almayı reddetme hakkı ücretsiz ve kolay bir yolla sağlanır. Doğrudan pazarlama amacıyla gönderilen ve kimin adına haberleşme yapıldığı hususunda göndericinin kimliğini saklayan veya alıcının bu iletişimin sonlandırılması konusunda talepte bulunacağı bir adres bulunmayan elektronik mektupların gönderilmesi abonenin bu yöndeki talebi halinde engellenir.	**İstenmeyen mesajlar** **MADDE 20** — (1) Bir ürünün satılması ya da bir hizmetin sağlanması sırasında edinilen tüketiciye ait iletişim bilgileri, tüketicinin rızasının alınması koşuluyla, doğrudan pazarlanma amacıyla kullanılabilir ve bu tür elektronik mesajlarda, göndericinin kimliği ve erişim bilgisinin yer alması zorunludur. (2) İşletmeciler, istenmeyen mesajların haberleşmenin her aşamasında abone tarafından basit ve ücretsiz bir işlemle reddedilebilir olmasına imkân sağlar ve bu mesajların engellenmesi yöntemlerine ilişkin olarak kullanıcıları açık ve detaylı bir şekilde ücretsiz olarak bilgilendirir.
Teknik Özellikler ve Düzenlemeler **Madde 21** — İşletmeciler kişisel bilgilerinin işlenmesi ve gizliliğinin korunması için gerekli terminal cihazlarını temin ederler.	

DÖRDÜNCÜ BÖLÜM Diğer Hükümler	BEŞİNCİ BÖLÜM Diğer Hükümler
	İdari para cezaları ve diğer yaptırımlar **MADDE 21** — (1) İşletmeciler tarafından bu Yönetmelik hükümlerine aykırı davranılması halinde işletmecinin bir önceki takvim yılındaki cirosunun % 3 (yüzde üç)'üne kadar idari para cezası uygulanır. (2) Bu Yönetmelikte öngörülen idari para cezasının uygulanmasından önce ilgili işletmeciye, Kurum tarafından verilen bir süre içerisinde yükümlülüğünü yerine getirmesi konusunda ihtarda bulunulur. Bu süre içerisinde yükümlülüğünü yerine getirmeyen işletmeciye Kurul kararıyla belirlenen oranda idari para cezası uygulanır. (3) Bu madde uyarınca idarî para cezalarının uygulanması, bu Yönetmelikle getirilen yükümlülükleri ortadan kaldırmaz. İhlal konusu fiilin tekrarı veya devamı halinde işletmecinin bir önceki takvim yılındaki cirosunun % 3 (yüzde üç)'ünü aşmamak kaydıyla idarî

	para cezası uygulanır. (4) 05/09/2004 tarihli ve 25574 sayılı Resmî Gazete'de yayımlanan Telekomünikasyon Kurumu Tarafından İşletmecilere Uygulanacak İdari Para Cezaları ile Diğer Müeyyide ve Tedbirler Hakkında Yönetmelik hükümleri saklıdır.
	Hüküm bulunmayan haller **MADDE 22** — (1) Bu Yönetmelikte hüküm bulunmayan hallerde, tebliğ veya Kurul Kararı ile düzenleme yapılır.
	Yürürlükten kaldırılan yönetmelik **MADDE 23** – (1) Bu Yönetmelikle, 06/02/2004 tarihli ve 25365 sayılı Resmi Gazete'de yayımlanan "Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik" yürürlükten kaldırılmıştır.
Geçici Madde 1 — Bu Yönetmeliğin yayımından önce halka açık abone rehberlerinde kişisel bilgileri bulunan sabit veya mobil telefon hizmeti abonelerinin kişisel bilgileri, elektronik veya basılmış rehberlerde	**Atıflar** **MADDE 24** - (1) Diğer mevzuatta 06/02/2004 tarih ve 25365 sayılı Resmî Gazete'de yayımlanan "Telekomünikasyon Sektöründe Kişisel Bilgilerin

bulunmaya devam eder.	İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik"e yapılan atıflar bu Yönetmeliğe yapılmış sayılır.
Yürürlük **Madde 22** — Bu Yönetmelik, yayımı tarihinde yürürlüğe girer.	**Yürürlük** **MADDE 25** – (1) Bu Yönetmelik yayımlandığı tarihte yürürlüğe girer.
Yürütme **Madde 23** — Bu Yönetmelik hükümlerini, Telekomünikasyon Kurulu Başkanı yürütür.	**Yürütme** **MADDE 26** — (1) Bu Yönetmelik hükümlerini, Bilgi Teknolojileri ve İletişim Kurulu Başkanı yürütür.

ÖZGÜNLÜK BİLDİRİMİ

Uzmanlık tezi olarak sunduğum bu çalışmayı, bilimsel ahlak ve geleneklere aykırı düşecek bir yol ve yardıma başvurmaksızın yazdığımı, yararlandığım eserlerin kaynakçada gösterilenlerden oluştuğunu, bunlardan her seferinde değinme yaparak yararlandığımı ve Bilgi Teknolojileri ve İletişim Kurumu Meslek Personeli Sınav, Görev, Çalışma Usul ve Esasları Hakkında Yönetmeliğe uygun olarak hazırladığımı belirtir, bunu onurumla doğrularım.

Bilgi Teknolojileri ve İletişim Kurumu tarafından belli bir zamana bağlı olmaksızın, tezimle ilgili yaptığım bu beyana aykırı bir durumun saptanması durumunda, ortaya çıkacak tüm ahlaki ve hukuki sonuçlara katlanacağımı bildiririm.

08/06/2011

Osman ŞAHİN

ÖZGEÇMİŞ

1982 yılında Trabzon'da doğdu. İlköğrenimini Eskişehir'de, ortaöğrenimini Samsun'da tamamladı. 2007 yılında Orta Doğu Teknik Üniversitesi Bilgisayar Mühendisliği Bölümünden mezun oldu. Nisan 2008'de Bilgi Teknolojileri ve İletişim Kurumunda Bilişim Uzman Yardımcısı olarak göreve başladı. Halen Bilgi Teknolojileri ve İletişim Kurumu, Tüketici Hakları Dairesinde çalışmalarına devam etmektedir.