T.C.
BAŞBAKANLIK
DEVLET PLANLAMA TEŞKİLATI
MÜSTEŞARLIĞI

KİŞİSEL VERİLERİN KORUNMASI ve BİR KURUMSAL YAPILANMA ÖNERİSİ

(Uzmanlık Tezi)

Dilek YÜKSEL CİVELEK

BİLGİ TOPLUMU DAİRESİ BAŞKANLIĞI

Nisan 2011

Yayın No : 2821

KİŞİSEL VERİLERİN KORUNMASI ve BİR KURUMSAL YAPILANMA ÖNERİSİ

(Uzmanlık Tezi)

Dilek YÜKSEL CİVELEK

BİLGİ TOPLUMU DAİRESİ BAŞKANLIĞI

Nisan 2011

ISBN 978-975-19-5018-5

Bu tez Müsteşar Yardımcısı Erhan USTA başkanlığında Timoçin SANALAN, Şevki EMİNKAHYAGİL, Mustafa DEMİREZEN, Doç. Dr. Adil TEMEL, Hayri MARAŞLIOĞLU, Bahaettin GÜLGÖR, Nihal ERCAN, Dr. Vedat ŞAHİN ve Mehmet Fatih LEBLEBİCİ'den oluşan Planlama Uzmanlığı Yeterlik Sınav Kurulu tarafından değerlendirilmiştir.

Bu yayın 500 adet basılmıştır.

TEŞEKKÜR

Bu çalışmanın hazırlanmasında;

Danışmanım olarak bana rehberlik yapan, bu çalışma ile ilgili ciddi ölçüde zaman harcayan ve bilgisini esirgemeyen Sayın Oğuz TURHAN'a,

Okunmasına ayırdıkları zaman ve olumlu eleştirileri ile çalışmanın olgunlaşmasına yaptıkları değerli katkılarından dolayı Sayın Recep ÇAKAL'a ve Sayın Murat İNCE'ye,

Desteklerinden dolayı Sayın Emin Sadık AYDIN'a ve tüm mesai arkadaşlarıma,

Her zaman olduğu gibi, bu süreçte de bana sevgi, moral ve destek veren sevgili anne ve babama,

Konuya yakın çalışmalarından kaynaklanan görüşlerini benimle paylaşan, bu süreci yakından izleyerek destek veren sevgili eşim Furkan CİVELEK'e ve sağladığı motivasyon ile küçük yolcumuza

en içten teşekkürlerimi sunmayı borç bilirim…

Dilek YÜKSEL CİVELEK

Ankara, 2011

ÖZET

Planlama Uzmanlığı Tezi

KİŞİSEL VERİLERİN KORUNMASI VE BİR KURUMSAL YAPILANMA ÖNERİSİ

Dilek YÜKSEL CİVELEK

Son yıllarda bilgi ve iletişim teknolojileri ve özellikle İnternet günlük hayatta artan şekilde kullanılmaya başlanmış, bunun doğal sonucu olarak ekonomik ve sosyal hayata ilişkin birçok iş ve işlem elektronik ortamda yapılır duruma gelmiştir. Bu teknolojilerin günlük hayatta giderek artan kullanımı, bireyi normal hayatta tanımlayan ve belirleyen kişisel verilerin elektronik izdüşümlerinin oluşmasına, bu verilerin elektronik ortamda çeşitlenmesine ve daha fazla işlenmesine sebep olmuştur.

Kişisel verilerin elektronik ortamda saklanıp işlenmesi bir yandan kullanıcı ihtiyaçları için özelleştirilmiş yenilikçi hizmetlerin sunulmasına imkan sağlamakta, öte yandan bu verilerin suistimali ile siber suçların artışını tetiklemekte ve söz konusu verilerin ticaretine ilişkin bir yeraltı ekonomisinin oluşmasına zemin hazırlamaktadır. Bu noktadan hareketle, dünyada pek çok ülke kişisel verilerin kullanıcıların isteği dışında ve onların zararına olacak şekilde saklanması ve işlenmesini önlemek amacıyla yasal düzenlemeler yapmaktadır. Bu tezin amacı da, bir taraftan kişisel verilerin işlenmesine dayalı ekonomik ve sosyal faaliyetlerin etkin şekilde yürütülmesine imkan sağlarken diğer taraftan kişisel verilerin uygunsuz şekilde saklanması ve işlenmesini önleyerek kişisel hakları korumayı hedefleyen hukuki düzenlemelere ışık tutmak ve dünyadaki gelişmelere paralel olarak Türkiye için öneriler geliştirmektir.

Bu çalışmada; kişisel veriler ve mahremiyet hakkı, kişisel verilerin siber suçlarla ilişkisi, uluslararası alanda ve karşılaştırmalı hukukta kişisel verilerin korunmasına yönelik yasal ve kurumsal yapılar ile Türkiye'de kişisel verilerin korunmasına ilişkin yasal ve kurumsal ihtiyaçlar bütünsel bir bakış açısıyla incelenmiştir. Çalışmada; Türkiye'de kişisel verilerin kullanımına ilişkin ilkeleri tespit edecek, kişisel verilerinin korunmasına yönelik olarak vatandaşların şikayet haklarını genişletecek ve veri işleyenlere çeşitli sorumluluklar getirecek çerçeve nitelikte bir Kanun ile bu Kanunun uygulanmasından sorumlu olacak bağımsız bir kurumsal yapıya ihtiyaç olduğu sonucuna varılmış ve bu çerçevede hukuki ve kurumsal yapıya ilişkin öneriler geliştirilmiştir. Çalışmanın hazırlanmasında literatür taraması, ülke örneklerinin incelenmesi ve ülkemizdeki mevcut mevzuatın değerlendirilmesi yöntemi kullanılmıştır.

Anahtar Kelimeler: Kişisel Verilerin Korunması, Mahremiyet, Siber Suç, Bilgi Toplumu, Bilgi ve İletişim Teknolojileri.

ABSTRACT

Thesis for Planning Expertise

PROTECTION OF PERSONAL DATA AND A SUGGESTION FOR THE INSTITUTIONAL BUILDING

Dilek YÜKSEL CİVELEK

In the last years, information and communication technologies and particularly the Internet have begun to be used increasingly in daily life and as a natural consequence; several transactions regarding economic and social life have started to be carried out in the electronic medium. Increasing usage of these technologies in daily life created fingerprints of personal data which identifies and determines the individual in his daily life and diversified and multiplied it in the digital environment.

Although storage and processing of personal data in the electronic medium enables provision of innovative services customized for user needs, this also triggers abuse of personal data and increase in cyber crimes and sets the ground for an underground economy related to trade of personal data. In this respect, several countries around the world are developing legal regulations in order to prevent storage and processing of personal data without the consent of the users and in a way detrimental to them. The aim of this thesis is to shed light on legal regulations which, on one side, enable carrying out economic and social transactions that rely on processing of personal data, and on the other, aim to prevent improper storage and processing of this data and protect personal rights and formulate proposals in line with developments in the world.

In this study; personal data and right to privacy, relation of personal data with cyber crimes, legal and institutional structures regarding protection of personal data in the international arena and comparative law and legal and institutional needs of Turkey regarding protection of personal data have been analyzed with a holistic point of view. It is concluded in the study that; a framework law which will establish principles regarding the use of personal data, enlarge complaint rights of citizens with respect to protection of personal data and set necessary obligations for data processing entities, and an independent authority that will be in charge of implementation of this law are needed. In this context, proposals regarding this framework law and institutional structure have been developed. With regards to methodology, literature survey and analysis, examination of other country cases and assessment of Turkey's current legal framework have been adopted.

Key Words: Protection of Personal Data, Privacy, Cyber Crime, Information Society, Information and Communication Technologies.

İÇİNDEKİLER

TABLOLAR

ŞEKİLLER

KISALTMALAR

AB	: Avrupa Birliği
ABD	: Amerika Birleşik Devletleri
AET	: Avrupa Ekonomik Topluluğu
a.g.e.	: Adı geçen eser
AİHM	: Avrupa İnsan Hakları Mahkemesi
AİHS	: Avrupa İnsan Hakları Sözleşmesi
APPA	: Asia Pacific Privacy Authorities (Asya Pasifik Mahremiyet Kurumları)
Ar-Ge	: Araştırma ve Geliştirme
A.Ş.	: Anonim Şirket
AT	: Avrupa Topluluğu
AY	: Anayasa
BİT	: Bilgi ve İletişim Teknolojileri
BK	: Borçlar Kanunu
Bkz.	: Bakınız
BM	: Birleşmiş Milletler
BTK	: Bilgi Teknolojileri ve İletişim Kurumu
BTS	: Bilgi Toplumu Stratejisi
CEN	: Committee for European Standardization
CNIL	: Commission Nationale de l'informatique et des Libertés (Fransa Enformatik ve Özgürlükler Milli Komisyonu)
e-DTr	: e-Dönüşüm Türkiye
e-Devlet	: Elektronik Devlet
e-Ticaret	: Elektronik Ticaret
GATS	: General Agreement on Trade in Services (Hizmet Ticareti Genel Anlaşması)
GPS	: Global Positioning System (Küresel Yer Belirleme Sistemi)

GSM	: Global System for Mobile Communication (Mobil İletişim için Küresel Sistem)
ICC	: International Chamber of Commerce (Uluslararası Ticaret Odası)
ITU	: International Telecommunication Union (Uluslararası Telekomünikasyon Birliği)
KDEP	: Kısa Dönem Eylem Planı
KOB	: Katılım Ortaklığı Belgesi
KVKK	: Kişisel Verilerin Korunması Kanunu
MAT	: Mahremiyet Artırıcı Teknoloji
MEB	: Milli Eğitim Bakanlığı
MERNIS	: Merkezi Nüfus İşletim Sistemi
md.	: Madde
MİT	: Milli İstihbarat Teşkilatı
MOBESE	: Mobil Elektronik Sistem Entegrasyonu
PANZA	: Privacy Agencies of New Zealand and Australia (Yeni Zelanda ve Avustralya Mahremiyet Kurumları)
PANZA+	: Privacy Agencies of New Zealand and Australia plus Hong Kong and Korea (Yeni Zelanda ve Avustralya Mahremiyet Kurumları artı Hong Kong ve Kore)
PIN	: Personal Identification Number (Kişisel Tanımlama Numarası)
POLNET	: Polis Bilgi Ağı
RFID	: Radio Frequency Identification (Radyo Frekans Tanımlama)
RG	: Resmi Gazete
SBS	: Schengen Bilgi Sistemi
STK	: Sivil Toplum Kuruluşu
TAKBİS	: Tapu ve Kadastro Bilgi Sistemi
TBD	: Türkiye Bilişim Derneği
TBMM	: Türkiye Büyük Millet Meclisi
T.C.	: Türkiye Cumhuriyeti
TCK	: Türk Ceza Kanunu
TİB	: Telekomünikasyon İletişim Başkanlığı
TL	: Türk Lirası

TMK	: Türk Medeni Kanunu
TUENA	: Türkiye Ulusal Enformasyon Altyapısı Anaplanı
OECD	*: Organization for Economic Co-operation and Development (Ekonomik □□birli□i ve Kalk‹nma Örgütü)*
vd.	*: ve devam‹*
VEDOP	*: Vergi Daireleri Otomasyon Projesi*
VKD	*: Veri Koruma Direktifi*
WTO	*: World Trade Organization (Dünya Ticaret Örgütü)*
YPK	: Yüksek Planlama Kurulu

BAZI İNGİLİZCE KAVRAMLAR İÇİN ÖNERİLEN TÜRKÇE KARŞILIKLAR

Bu çalışma yapılırken karşılaşılan bazı İngilizce teknik terimlerin bir kısmının karşılığı Türkçede henüz bulunmamaktadır. Kişisel verilerin korunması ile ilgili karşılaşılan bu terimler ve bu çalışma kapsamında önerilen Türkçe karşılıkları aşağıda verilmektedir.

Cookies : Çerezler
Crack(ing) : (Güvenlik duvarını) Kırmak
CID (Customer Card ID number)
veya CVV2 : Müşteri kart kimliği veya doğrulama kodu
Cyber crime : Siber suç (Bilişim suçu olarak da kullanılmaktadır.)
Data mining : Veri madenciliği
DDoS (Distributed Denial of Service) attack : Dağıtık olarak hizmet çökertme saldırısı
Dumpster diving : Çöp karıştırma
Hacker : Bilgisayar korsanı
Hacking : Bilgisayar korsanlığı
Hash : Özdeğer
Information : Bilgi[*]
Intrusion : İşgal
Mailer : Toplu e-posta gönderim hizmeti
Malware : Kötü niyetli yazılım
Off-line identity theft : Çevrimdışı kimlik hırsızlığı
On-line identity theft : Çevrimiçi kimlik hırsızlığı
Personal data : Kişisel veri
PET (Privacy enhancing technology) : MAT (Mahremiyet artırıcı teknoloji)
Pharming : Sahte internet sitesi kurma
Phishing : Oltalama
Pretexting : Bahane yaratma
Privacy : Mahremiyet
Proxy : Aracı site
Scams : Dolandırıcılık için üretilen mal ve hizmetler
Shoulder surfing : Omuz üstünden seyir
Skimming : Tarama
Spam : İstenmeyen ileti
Surveillance : Gözetleme, izleme
Trojan : Truva atı

[*] Bu çalışma kapsamında "veri" ve "bilgi" kavramları aynı anlamda, biri diğerinin yerine geçebilecek şekilde kullanılmıştır.

"Mahremiyete değer vermeyen ve kişisel verilere ucuz bir eşya muamelesi yapan toplumlar, er ya da geç, vatandaşlarına da aynı şekilde davranırlar."

John Grace, 1982

(Kanada'nın ilk Mahremiyet Komiseri)

GİRİŞ

Kristof Kolomb 1492 yılında, Hindistan'a daha kısa bir yol bulmak için Doğu Hint Adaları'na kadar uzanan açık bir deniz olduğunu varsaydığı Atlantik Okyanusu'nda gemilerle yola çıktı. Kolomb, sefere çıkarken dünyanın yuvarlak olduğu varsayımıyla hep batıya giderek Hindistan'a ulaşabileceğini düşünüyordu. Hindistan'a böyle kestirme bir yol bulunması hem Kolomb'u hem de İspanyol monarşisini zengin ve güçlü kılacaktı. Ama dünyayı olduğundan daha küçük sanarak mesafeyi yanlış hesaplayan Kolomb, yeni dünyada rastladığı halkları "Hintliler" olarak adlandırdı. Memleketine dönünce Kral ve Kraliçe'ye Hindistan'a ulaşamamış olsa da dünyanın "yuvarlak" olduğunu söyledi.

21'inci yüzyıla gelindiğinde ise, ünlü gazeteci Thomas L. Friedman, hizmetler ve bilişim teknolojisi alanlarında Amerika ve sanayileşmiş diğer ülkelere taşeronluk yapan Hindistan'ı göz önünde bulundurarak, bilgisayar ve teknolojinin "yuvarlak" olan dünyayı "düz"leştirdiğini ifade ediyordu. Friedman'a göre, gezegenimizdeki tüm bilgi merkezlerinin tek bir küresel şebekeye (network) bağlanması anlamına gelen İnternet ile birlikte, çok daha fazla sayıda insanın, daha fazla insanla, daha fazla iş süreçleri üzerinden, dünyanın pek çok köşesinde, daha eşit bir zeminde, gerçek zamanlı rekabette yer alması artık mümkün hale gelmişti. Bilgisayarlar, elektronik postalar, ağlar, telekonferanslar bu imkanları sağlamaktaydı. Dünya artık, küresel tedarik zincirini sanal toplantıya davet eden bir ekran kadar düzleşmişti. [2]

Hindistan ile sembolize edilen yapı, esasında bilgi ve iletişim teknolojilerinin (BİT) yaygınlaşmasıyla literatüre giren ve tüm dünyada ekonomik ve sosyal gelişmenin önemli itici güçlerinden biri olarak kabul edilen bilgi toplumunu ifade etmektedir. Her türlü ekonomik ve sosyal aktivitede bilginin artan şekilde girdi olarak kullanıldığı ekonomik ve sosyal yapıyı ifade eden bilgi toplumunda, söz konusu aktivitelerin etkin şekilde yürütülmesi açısından bilginin hızlı ve güvenli şekilde ve uygun maliyetlerle iletilmesi gerekmektedir. Bu iletimin gerçekleştirilmesinde temel role sahip olan bilgisayar ve bilgisayarların birbirleriyle

[2] Friedman, 2006:17,18

iletişimini sağlamada ağ altyapısı olan İnternetin[3] kullanımının gün geçtikçe artmasıyla birlikte, anılan iletişim vasıtalarıyla iletilen kişisel verilerin, güvenli bir şekilde aktarılması gittikçe zorlaşmaktadır. Daha önceki dönemlerde hayal edilmesi bile zor olan makine ve otomatik cihazların giderek vazgeçilmez hale geldiği günümüz dünyasında, kişisel verilerin çalınması, kişinin rızası olmaksızın profillerinin çıkartılarak ticari amaçlar için kullanılması da çok kolay bir hale gelmiştir. Hukuka aykırı eylemlerde bulunan siber suçlular ve terör suçluları da bilgi değişiminde İnterneti kullanmaktadırlar. Ağ etkisi, veri kayıplarını ve kimlik hırsızlığını artırdığı gibi, ticari amaçlara hizmet edecek profil oluşturma işlemlerine de hız kazandırmıştır. Kısacası, son yıllarda bilgi iletimi kolaylaşarak hayat daha sayısal hale gelirken, sanal dünyaya olan güven ve veri güvenliği azalmaya başlamıştır. Bu sebeple, sanal dünyanın hızla değişen yapısı sonucu ortaya çıkan "verilerin güvenliği problemi" karşısında hukuk dünyası da sanal dünyadaki gelişmelere ayak uydurmak, veri güvenliği ihlallerini ortadan kaldırmak veya en az seviyeye indirmek için gerekli mevzuat çalışmalarını yapmak durumundadır.

Yine, İkinci Dünya Savaşı yıllarında ayrımcılık içeren bazı kanunların uygulanmasında, kişisel veri kayıtları bireyleri "fişleme" aracı olarak kullanılmıştır. Bireyler, dönem itibarıyla kağıt ortamında elle tutulan bu kayıtlar üzerinden ayrımcı muameleye tabi tutulmuştur.

Günümüzde ise, neredeyse sınırsız büyüklükteki bilgi bankaları, toplumda herkesin açık ya da mahrem bilgilerini toplama, saklama, transfer etme, değiştirme, silme vb. şekillerde işleme yeteneği ile kişiler ve kişilik hakları üzerinde baskı unsuru olmaya başlamıştır. Bu nedenle, uzun yıllardan beri "öteki" ile ilgili bilgilerin cazibesi, günümüzde masum bir merakın dışına çıkmıştır. Kişilere ait kredi kartı bilgileri, şifreler, banka hesapları, etnik köken, din, sağlık bilgileri, siyasi görüşler, görüntüler, kısacası kişisel veriler mesafelerden bağımsız olarak edinilebilmekte; bu bilgiler yasa dışı birçok faaliyetin malzemesi haline getirilebilmektedir. Bu durum, maddi zararların yanında, kişilerde psikolojik buhranı da beraberinde getirmektedir.

[3] Sarıhan'a (1995:10) göre "İnternet" kelimesi özel isim olduğundan ilk harfi büyük olarak yazılmalıdır. Eğer küçük harfle yazılırsa birden çok ağı birleştiren bağlantıları ifade etmektedir.

Kısacası hayat, pek çoğumuz için artık, Büyük Birader'in[4] yarattığı paranoyanın gölgesinde geçmektedir.

Yaşadığımız her alana; eve, ofise, okula ve cebimize giren bilgisayar, mobil telefon, güvenlik kameraları vb. elektronik araçlar, Büyük Birader kadar aleni olmasa da, aslında kişilerin kolayca izlenmesini sağlayabilen araçlardır. Son yirmi yılda büyük bir hızla gelişen İnternet, gerçek hayatın dışında sanal bir alem yaratmış ve bu alem aynı zamanda insanların izlerinden oluşan profillerin de deposu haline gelmiştir. Gelişen uydu bağlantılı coğrafi bilgi sistemleri, taşıdığımız cep telefonları bizi izleyen ve yerimizi tespit etmeye yarayan birer araç olarak kullanılabilmektedir. Kısacası, tüm akıllı sistemler, bir yerlerde bıraktığımız küçük izlerin takipçisi konumuna geçebilmektedir. Yararları olduğu kadar, sanal korsanların istifadesinde çok tehlikeli olabilecek bu araçlara karşı, bireyin korunması ihtiyacı, hukuk alemini harekete geçirmiştir.

"Kişi" ve "kişilik", tüm hukuk sistemlerinde korunan hukuki kavramlardır. Bununla birlikte, sanal dünyanın kişilik kavramı üzerindeki olumsuz etkileriyle mücadelede klasik hukuki araçlar yeterli olamamaktadır.

Günümüzde uluslararası nitelikteki sorunlarla mücadelede, devletler etki ve sonuçları nedeniyle işbirliği yaparak yeni düzenlemeler ve uygulama modelleri ortaya koyma eğilimindedirler. Kamu ve özel hukukun etkilerini taşıyan "Veri Koruma Hukuku" da bu çerçevede ortaya çıkan bir disiplindir.

1980'li yıllarda kişi mahremiyetinin deşifre edilerek kötüye kullanılması sonucunda gelişmeye başlayan Veri Koruma Hukuku, bu hukukun uygulama aracı olarak veri koruma yasalarını gündeme getirmiş; böylece kişisel veriler ve bireyin mahremiyeti hukukun koruması altına alınmaya başlanmıştır.

Dünyada otuz yılı aşkın bir geçmişi olmasına karşın, Türkiye'de Veri Koruma Hukuku ile ilgili literatür oldukça kısıtlıdır. Mevcut çalışmalar, daha ziyade

[4] George Orwell'in "1984" adlı romanındaki Büyük Birader her an her yerde izlediği bireyin hayatını büyük bir paranoyaya dönüştürmekte; özel hayat, gizlilik gibi kişilik değerleri de birer birer yok olmaya başlamaktadır.

Veri Koruma Hukukunu ve kavramları açıklamaya yönelik olup; Türkiye için etkin bir işleyiş modeli henüz ortaya konulamamıştır.

Son dönemde yürütülen yasal düzenleme çalışmaları kapsamında hazırlanan Kişisel Verilerin Korunması Kanunu (KVKK) Tasarısı, 2008 yılı Nisan ayı sonu itibarıyla TBMM'ye sevk edilmiştir. Tasarı, bu çalışmanın yapıldığı dönemde halen TBMM Adalet Komisyonu'nda bulunmaktadır. Kişisel veri koruma hukuku ülkemiz için henüz yeni bir konu olup, bu konuda karar vermeyi destekleyecek nitelik ve sayıda çalışma bulunmamaktadır. Bu durumun, Tasarının yasalaşmasına ilişkin karar alıcıların çekimser davranmalarına sebep olduğu düşünülmektedir.

Dünyada yaşanan söz konusu gelişmeler ve Türkiye'deki son durumdan hareketle bu çalışmanın amacı; veri koruma hukuku ve kişisel veri kavramının uluslararası alanda ve özellikle Avrupa Birliği'ndeki (AB) durumu hakkında bilgi verilmesi, kişisel verilerin BİT aracılığıyla hızlı ve kolay paylaşılması nedeniyle giderek çoğalan siber suç ve diğer tehditler ile alınan önlemlerin incelenerek Türkiye için yasal ve kurumsal yapıya ilişkin öneriler geliştirilmesi ve ayrıca, mevcut Tasarıya ilişkin bazı değerlendirmeler yapılmasıdır. Bu yolla, Türkiye'de yapılan çalışmalara katkıda bulunulması amaçlanmaktadır.

Bu çerçevede, çalışmanın birinci bölümünde kişisel veri, mahremiyet hakkı ve veri koruma hukukuna yer verilmiştir. Bu kavramların hukuki gelişimi, kişisel verilerin özel bir çeşidi olan hassas veriler ve bilgi güvenliği kavramları kısaca açıklanmaya çalışılmıştır.

İkinci bölümde, sanal ortamda işlenen siber suçlar ile elde edilen haksız kazancın malzemesi olarak kullanılan kişisel verilerin yeraltı ekonomisindeki ticari değeri incelenmiştir. Bu bölümde, kişisel verilerin kötüye kullanılmasında ve siber suçlarla mücadelede alınacak tedbirlerden mahremiyet artırıcı teknolojiler, elektronik imza ve akıllı kartlar üzerinde durulmuştur.

Üçüncü bölümde, uluslararası alanda ve karşılaştırmalı hukukta kişisel verilerin korunmasına yönelik yapılan çalışmalar incelenmiştir. Bu bölümde, özellikle ülkemizin AB entegrasyon süreci nedeniyle uyumu öngördüğü kişisel verilerle ilgili AB düzenlemeleri ve bu düzenlemelerde yer alan temel kavramlar

tanıtılmış, bunların yanı sıra OECD, Avrupa Konseyi, Birleşmiş Milletler (BM) ve Dünya Ticaret Örgütü (DTÖ) nezdinde veri koruma hukuku ve mahremiyet hakkında yapılan çalışmalara yer verilmiştir. Daha sonra, karşılaştırmalı hukukta kişisel verilerin korunması alanındaki düzenlemeler verilmiş ve seçilen ülkelerde yaşanan sorunlar ile düzenleme örnekleri daha ayrıntılı olarak ele alınmıştır.

Dördüncü bölümde, veri koruma alanında kurumsal yapıya ilişkin incelemeler yapılmıştır. Bu bölümde, öncelikle kurumsal yapıya ilişkin teorik çerçeve ve alternatif veri koruma otorite modelleri ile bu modellerin avantaj ve dezavantajları tartışılmıştır. Ardından, seçilmiş ülkelerde veri koruma otoritelerinin kurumsal yapıları, görev ve özellikleri incelenmiştir.

Beşinci bölümde, Türkiye'de ve Türk hukukunda kişisel verilerin korunması ile ilgili politikalar, bu alandaki yasal boşluk nedeniyle yaşanan sorunlar ve sınırlı düzeydeki mevcut düzenlemeler ile KVKK Tasarısı ve içeriği incelenmektedir.

Son bölümde ise, çalışmada incelenen tüm veri ve değerlendirmeler ışığında, Türkiye için hukuki düzenleme ve kurumsal yapı ihtiyacına ilişkin öneriler geliştirilmiştir. Bu bölümde, Türkiye'nin ihtiyaç duyduğu kişisel verilerin korunması kanununda yer alması gereken temel özellikler ile ihtiyaç duyulan bağımsız veri koruma kurumunun kurumsal yapı ve işleyişine ilişkin ayrıntılı öneri ve değerlendirmelere yer verilmiş, elde edilen bulgularla mevcut Tasarıya ilişkin bazı değerlendirmeler yapılmıştır.

1. KİŞİ ve KİŞİSEL VERİ KAVRAMLARI ile KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN HUKUKUN TARİHSEL GELİŞİMİ

1.1. Genel Çerçeve

Bilgi ve iletişim teknolojilerinin yaygınlaşarak günlük hayatta daha fazla yer alması ile "bilgi" daha önceki dönemlere göre daha fazla değer kazanmaya başlamıştır. "Bilgi"nin, toplumun her tür ekonomik ve sosyal faaliyetinde artan şekilde kullanımı, bu bilgilerin hızlı, güvenli ve uygun maliyetlerle iletilmesini gerektirmiş, ekonomik ve sosyal alanda yaşanan bu değişim "bilgi toplumu" kavramı ile ifade edilmeye başlanmıştır. Söz konusu bilgilerin iletimi, saklanması, değiştirilmesi, sınıflandırılması ve aranmasına ilişkin alternatiflerin artışı ise özellikle bireyi tanımlayan ve belirleyen "kişisel bilgiler"in, temel hak ve özgürlüklere zarar vermeksizin nasıl korunması gerektiği sorusunu gündeme getirmiştir.

İnternetin ortaya çıkışıyla hızlanan küreselleşme olgusu ve ekonomik ve sosyal sebeplerle çok sayıda kişisel bilgi hızlı bir şekilde işlenmektedir. Kamu kurum ve kuruluşları görevlerini yerine getirmek; özel sektör ise mal ve hizmet pazarlamak ve tüketici taleplerinden haberdar olmak, bu taleplerin karşılanmasına yönelik araştırma ve analiz faaliyetlerinde bulunmak için kişisel verilere ihtiyaç duymaktadır. Yine herhangi bir mesleğin icrasında meslek mensupları, meslek birlikleri ve bunların üst kuruluşları, sivil toplum kuruluşları günlük hayatta birçok kişinin kişisel verilerini toplamakta, işlemekte ve depolamaktadır. Bu bilgiler, bazen birinci elden, bazen de bu bilgileri elde etmiş olanlardan ticari veya ticari olmayan farklı yöntemlerle edinilebilmektedir.

Kullanım amaçları ve edinim olanakları giderek artan kişisel bilgiler, tüm dünyada, erişim ve kullanma hakkı ile bireyin mahremiyet hakkı arasında bir dengenin kurulması ihtiyacını gündeme getirmiştir. Dünyada ve ülkemizde kişisel veriler, sadece üçüncü kişiler nezdinde bireyleri tanımlamakla kalmamakta; bu bilgiler, sayısal ortamın sunduğu işleme yetenekleri ile birey "hakkında" veya "onun gibi" işlem yapabilme olanağı sağlamaktadır. Küçük bir bilgi parçasıyla yola çıkan bir bilgisayar korsanı, kısa bir sürede bir kişinin bütün banka hesaplarını ele geçirebilmekte, onun adına sahte evraklar düzenleyebilmekte, bu şekilde klasik veya

sanal ortamda zincirleme suçlar işleyebilmektedir. Dolayısıyla, bu verilerin gelişigüzel kullanılması birçok suç faaliyetine aracılık etmekte ve ayrıca kişilerin mahremiyet hakkının da ihlal edilmesine sebep olmaktadır.

Hukuka aykırı çok sayıda fiilin ve failin yer aldığı yeni bir yeraltı ekonomisi oluşturan kişisel verileri İnternet ekonomisinin para birimi olarak tanımlamak[5] mümkündür. Bu değerin yeraltı ekonomisinde haksız kazanca dönüşmesini ve kişilerin mağdur edilmesini önlemek için yapılan hukuki düzenlemeler, kişilerin mahremiyet hakkı, veri güvenliğinin sağlanması ve Anayasayla güvence altına alınan özel hayatın korunmasına katkıda bulunacaktır. Kişisel verilerin kullanım esaslarının belirlenerek bireyin korunmasına ilişkin bu tür hukuki gereksinimler veri koruma hukukunu gündeme getirmiştir. Düzenlediği alanın yatay olması ve bu alanların genellikle BİT ile kesişmesi nedeniyle Kuner'e göre veri koruma hukuku, sürekli hareket halinde olan ve hızlı değişen bir konu durumundadır.[6]

Bununla birlikte, özel hayatın gizliliğine saygı ile kişisel veri koruması kavramları birbirlerinin tam karşılığı olarak kullanılabilecek kavramlar değildir. Genel anlamda veri koruma mevzuatının amacı kişilere kendilerine ilişkin verilerin nasıl işleneceği noktasında birtakım haklar tanımak ve kişisel veri işlemelerini birtakım kurallara tabi kılmaktır.[7]

İnsan onurunun[8] korunmasının bir uzantısı olarak kişisel verilerin korunması, bu verilerin işlenmesi sırasında, birey hak ve özgürlüklerini korumayı amaçlamaktadır. Bu çerçevede, kişisel verilerin korunması hakkı, kişinin hak ve özgürlüklerinden bağımsız olarak sadece verinin kendisini değil, bilakis birey özgürlüklerinin korunmasını amaçlamaktadır. Dolayısıyla kişisel verilerin

---

[5] OECD Genel Sekreteri Angel Gurría, 17 Haziran 2008 tarihinde Kore'de gerçekleştirilen "İnternet Ekonomisinin Geleceği Hakkında Bakanlar Toplantısı"nda, bireyin İnternet Ekonomisinin odağında olduğunu vurgulamış; kişisel verilerin ise bu ekonominin "para birimi" olduğu benzetmesini yapmıştır. Bu konuşmanın ayrıntıları için bkz.
<http://www.oecd.org/document/8/0,3343,en_2649_34487_40863240_1_1_1_1,00.html>

[6] Kuner, 2007: xii

[7] Gür, 2010:195

[8] İnsan onuru, insan hakları düşüncesinin temelinde yer almakta olup, II. Dünya Savaşı'ndan sonra uluslararası hukuk belgelerine girmiştir. 1945 tarihli Birleşmiş Milletler Şartı, 1948 tarihli İnsan Hakları Evrensel Beyannamesi, 1966 tarihli Birleşmiş Milletler Medeni ve Siyasi Haklar Sözleşmesi ile Ekonomik, Sosyal, ve Kültürel Haklar Sözleşmesinde ve Avrupa İnsan Hakları Sözleşmesinde insan onuru kişilik hakkıyla birlikte ele alınmakta ve korumaya değer bulunmaktadır.

korunması, (…) kamusal organlar tarafından kişisel verilerin sınırsız olarak toplanması, kaydedilmesi, kullanılması ve devredilmesi karşısında bireyin temel hak ve özgürlüklerinin korunmasına hizmet etmektedir.[9] Bu amaçla yapılan düzenlemeler ise en genel anlamda kişisel verilere erişim, bu verileri kullanma ve işleme ilkelerini belirlemekte; bu ilkelere aykırı kullanım durumlarında ise bireye çeşitli haklar sağlamaktadır.

1.2. Tarihsel Gelişim

Kişisel verilerin korunmasına ilişkin hukuksal sorunlar, özellikle kişisel verilerin elle yapılan işlemelerin dışında, otomatik araçlarla işleme tabi tutulmaya başlanmasıyla gündeme gelmiş olmakla birlikte, bireyin kendisine ait verilerin korunmasına ya da gizli kalmasına yönelik düşünceler oldukça eskiye gitmektedir. Günümüzden 2500 yıl kadar geriye uzanan susma (sır saklama) yükümlülükleri, esas olarak belirli meslek gruplarına güven ilişkisi çerçevesinde giz alanını açan bireylerin, bu alanların korunmasının bir gereği olarak ortaya çıkmıştır. Örneğin günümüzde de geçerli olan hekimin sır saklama yükümlülüğüne ilişkin Hipokrat yemini, hekime hastalarla ilişkisi içerisinde elde ettiği verileri saklama ve açıklamama yükümlülüğü getirmektedir. Benzer şekilde kiliselerde din adamlarının sır saklama yükümlülüğü, memurun görev sırrı, banka sırrı, avukatın sır saklama yükümlülüğü de sahip olunan bilgilerin yetkisiz ve hukuka aykırı şekilde üçüncü kişilere aktarılmamasını amaçlamaktadır.[10]

Sır saklama yükümlülüğünü gerektiren düşüncelerin yanı sıra, bilgisayar ve İnternetin tetiklediği ve artırdığı kişisel verilere ve dolayısıyla kişilere yönelik tehditler yeni değildir. 16'ncı yüzyılda modern devletin ortaya çıkardığı bürokrasi ile birlikte, devletlerin vatandaşları hakkında güvenlik nedeniyle tutmaya başladığı kütükler ve bu kütüklerde tutulan verilerin, halk tarafından fişlenmenin bir aracı olarak algılanması korku ve endişeye neden olmuştur. Buna karşın, modern devlette vatandaşlık kavramı olmadığı gibi, kişilerin devlete karşı ileri sürebilecekleri hakları da olmadığından, devlet kişilere istediği türde muamele edebilmiştir. Milliyetçilik akımının ortaya çıkardığı ulus devlet döneminde de düşman belirlemek ve kimin ne

[9] Şimşek, 2008:119
[10] Şimşek, 2008:6

tarafta olabileceğini anlamak için yapılan fişlemeler, II. Dünya Savaşı'nda Doğu Bloku ülkelerde zirveye çıkmış ve bu durum birçok zulüm ve kıyımla sonuçlanmıştır. 1935'te Almanya'da bir dizi ırk kanunu ile başlayan ve II. Dünya Savaşı başladıktan sonra, Alman ordusunun Yahudilerin kayıtlarını tutmaya başlaması ile kişisel verilerin üçüncü kişilerce ayrımcılık ve diğer olumsuz niyetlere hizmet edecek şekilde kullanılabileceği dikkat çekmeye başlamıştır.

Kıta Avrupası hukuk sisteminin kişisel verileri bireyin kişilik hakkı çerçevesinde ele alması işbu tarihsel temele dayanmaktadır. Nitekim özellikle Nazi Almanyası'nda hem kamu kurumlarınca, hem de özel sektör tarafından toplanan kişisel verilerin kötüye kullanılması, neticede bilgi mahremiyetinin bir yurttaşlık hakkı olarak Avrupa'da kabul edilmesine ve korunmasına yol açmıştır.[11]

Elektronik ortam aracılığıyla bilgi ölçeğinin büyümesi, bu bilgilere erişim ve paylaşım hızını da artırmıştır. Modern teknolojiler, arama ve araştırma yöntemlerini daha kolay ve etkin hale getirmiştir. Büyük veri setlerini elektronik ortamda paylaşmak, bu setlerde arama veya sorgulama yapmak kolaylaşmakla beraber bu işlemleri güvenli ve güvenilir olarak yapmak, sayısallaştırılmış veri setlerini iyi yönetmek, kaza veya kasıt karşısında mağduriyetleri azaltmak için dünyada çeşitli yasal düzenleme çalışmaları başlatılmıştır.

Verilerin korunması ile ilgili dünyada ilk yasal düzenleme 1970 yılında Federal Almanya'nın Hessen eyaletinde yapılmıştır. Bu düzenleme ile ilk veri koruma otoritesi olan Veri Güvenlik Ofisi (Datenschutzbeauftragter) kurulmuştur.[12] Bu tarihten sonra, dünyada ve AB üye ülkelerinde çok sayıda yaklaşımı yansıtan pek çok veri koruma kanunları ihdas edilmiştir. AB üyesi olan ülkelerde çıkarılan kanunlar içerik olarak ve uygulama alanında birbirlerinden farklı özellikler göstermektedir. Almanya örneği bu farklı yaklaşımlara en iyi örnek olarak gösterilebilir, zira bu ülkenin merkez düzeyinde Federal Veri Koruma Kanunu uygulanırken, eyaletlerde farklı kanunlar uygulanmaktadır.[13]

[11] Aksoy, 2010:56
[12] Caprioli at al, 2006:214
[13] Kuner, 2007:13

Almanya'dan sonra 1973'te İsveç'te elektronik ortamdaki kişisel verilerin korunmasına ilişkin ilk kapsamlı Kanun çıkartılmıştır. 1972 yılının başlarında, Amerika'da sosyal güvenlik numarasının kimlik tanımlayıcı olarak hayatın her alanında sıkça kullanılmaya başlanması ve kişilerin kredi verilebilirliğinin (güvenilirliğin) büyük bir sosyal değer olmaya başlaması, bilgisayarların hata yapmaması için birtakım çalışmalar yapılmasına sebep olmuştur. Bu dönemde ABD Hükümeti özel bir Danışma Komitesi kurarak sosyal güvenlik numarası gibi tanımlayıcı sayıların ve özellikle o dönemde yeni kullanılmaya başlanan otomatik kişisel veri işleme sistemlerinin kullanılmasının pratik etkilerini araştırmıştır. Komite'nin 1973 tarihli raporunda[14], devletin ve özel sektörün tuttuğu kişisel bilgileri içeren kayıtlara itiraz etme, bu kayıtları düzeltme ya da kişinin kendisiyle ilgili bilgileri kontrol etme şansının olmamasının kişiler üzerinde dezavantajlı bir durum yarattığı belirtilmektedir. Rapora göre, veriyi elinde tutan kurum ve kuruluşlar bu bilgiler üzerinde sınırsız yetki sahibi olmamalıdır. Bu tartışmalar üzerine, 1974'te ABD'de özel alanın korunmasına ilişkin Kanun (Privacy Act) kabul edilmiştir. Bu düzenlemeyi 1977 tarihli Kanada İnsan Hakları Kanunu ve Fransa'da çıkarılan 1978 tarihli Elektronik Veri İşlenmesi, Veriler ve Özgürlük Haklarına ilişkin Kanun izlemiştir. 1978 tarihli Fransız Kanunu da Fransa vatandaşlarının kişisel verilerini koruyacak bir ulusal Komisyon[15] kurmaktadır. Aynı dönemde Danimarka, Norveç ve İsviçre'de de verilerin korunmasına ilişkin yasal düzenlemeler yapılmıştır. 1970'li yılların sonunda ise Lüksemburg'ta kişisel verilerin korunmasını amaçlayan bir Kanun çıkartılmıştır.

Kişisel verilerin korunması ile ilgili kanunlaştırma faaliyetlerinin aşamalı olarak devam etmesi nedeniyle, bu düzenleme ve faaliyetlerin belirli ilke ve standartlara sahip olması için uluslararası kuruluşlar da çeşitli çalışmalarda bulunmuşlardır. Bu çalışmalar içinde Avrupa Konseyi, 1981 yılında "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunması Hakkında Sözleşme"yi (108 Sayılı Sözleşme) kabul etmiştir. Bu Sözleşme, kişisel

[14] EPIC, "Records, Computers and the Rights of Citizens". 31 Temmuz 1973. 9 Şubat 2010. <http://epic.org/privacy/hew1973report/>

[15] Kısa adı CNIL olan Komisyon, bu tezin Kurumsal Yapılanma başlıklı dördüncü bölümünde ayrıntılı olarak ele alınacaktır.

verilerin korunması ile ilgili ilk uluslararası hukuk belgesi niteliğini taşımakta olup, özellikle de kağıt ortamındaki elle işleme yerine, daha fazla veriyi, daha nitelikli şekillerde, çok daha kısa sürede otomatik olarak işleme yeteneğine sahip araçların ortaya çıkmasıyla başlayan endişeleri giderme çabasıyla da bir ilki teşkil etmektedir. 1980 yılında ise OECD mahremiyetin korunması ve sınır ötesi kişisel veri korunmasını teşvik eden tavsiye niteliğindeki "Mahremiyet Rehber İlkeleri"ni kabul etmiştir.

Doksanlı yılların başından itibaren, ekonomik ve sosyal nedenlerle tüm dünyada bilgi toplumu olma yolundaki çabaların arttığı gözlenmektedir. ABD'nin 1990'lı yıllardan itibaren, özellikle BİT'e dayalı olarak sağladığı verimlilik artışı ve ekonomik büyümenin etkisiyle yoğunlaşan bu çabalar içerisinde AB de önemli bir aktör olarak yerini almıştır.[16] Üretim maliyetlerinde sağladığı düşüş ve günlük hayatta sağladığı kolaylıklar nedeniyle, BİT tüm dünyada giderek önem kazanmaya başlamış, iktisadi alanda emek ya da doğal kaynakların yerini "teknolojik yetenek" ve "bilgi" almaya başlamıştır. Bilginin tüm ekonomik faaliyetlerde temel girdi olarak kullanılmasıyla ekonomileri tanımlamada "bilgi ekonomisi" veya "bilgiye dayalı ekonomi" kavramları kullanılmaya başlanmıştır. BİT alanında yaşanan gelişmeler, bireyin kişilik hakkının bir parçası olan kişisel verileri üzerinde kontrol imkanının artması ve bu verilerin kullanım sürecinde etkin olma istek ve gerekliliğini gündeme getirmiştir. Bu dönemde, Avrupa Birliği, 95/46 sayılı "Kişisel Verilerin Korunmasına İlişkin Direktif"i kabul etmiş (1995) ve üye devletler bu Direktifle uyumlu düzenlemeler yapmaya başlamışlardır.

Bilgi toplumu alanında yürütülen çalışmalar, bu çalışmaların günlük hayatta vatandaşa en belirgin yansımalarından biri olan e-devlet uygulamaları ile hız kazanmaya başlamıştır. Devletler, BİT'in yaygınlaşmasıyla, klasik devletten, birçok kamu hizmetinin elektronik araçlar kullanılmak suretiyle sunulduğu e-devlet uygulamalarını gerçekleştirecek önemli bir dönüşüm sürecine girmiştir. "Kağıtsız devlet" sloganıyla da özdeşleşen bu süreç, bürokrasinin ortadan kaldırılması, şeffaf ve katılımcı bir kamu yönetimi, vatandaş odaklı hizmet sunumu gibi paradigmalar

[16] DPT, Bilgi Toplumu Dairesi. "e-Dönüşüm Türkiye Projesi Kısa Dönem Eylem Planı (2003-2004)." 4 Aralık 2003. s.5. 17 Kasım 2009. <http://www.bilgitoplumu.gov.tr/kdep.asp>

üzerinde şekillenmektedir. İnternet tabanlı uygulamaların başarılı sayılabilmesinde verilerin toplanması ve iletimi, kullanıcıların bilgilendirilmesi, haberleşme olanakları ve bilginin paylaşılmasında kişisel verilere ve mahremiyete saygının gözetilmesi temel unsurlardandır.[17] Geleneksel devlet modelinde, kamu kurumlarıyla muhatap olan vatandaşlar, e-devlette kurumlar tarafından kontrol edilen bilgi sistemleriyle yüzleşmekte, böylece daha hızlı ve kaliteli hizmet sunumu sağlanabilmektedir.

Dünya Bankası'nın 1993 yılında yayımladığı "Türkiye, Bilişim ve Ekonomik Modernizasyon Raporu" ile Türkiye'de de bilgi toplumu süreci hareketlenmiş, bu süreç Ulaştırma Bakanlığı koordinasyonunda, TÜBİTAK tarafından hazırlanan Ulusal Enformasyon Altyapısı Ana Planı (TUENA), Vizyon 2023: Bilim ve Teknoloji Stratejileri Projesi, Dış Ticaret Müsteşarlığı (e-Ticaret Koordinasyon Kurulu) ve Başbakanlığın (KamuNET) çalışmaları ile devam etmiştir. Daha sonra, 2002/55 sayılı Başbakanlık Genelgesi kapsamındaki Acil Eylem Planı "e-Dönüşüm Türkiye Projesi" ile bilgi toplumu olma yolundaki çalışmaları daha bütüncül bir şekilde ele almış olup projenin koordinasyonu, izlenmesi, değerlendirilmesi ve yönlendirilmesi görevini Devlet Planlama Teşkilatı Müsteşarlığına vermiştir. 2003/12 sayılı Başbakanlık Genelgesi ile Projenin temel amacı vatandaşlara daha kaliteli ve hızlı kamu hizmeti sunabilmek; katılımcı, şeffaf, etkin ve basit iş süreçlerine sahip bir devlet yapısı oluşturmak olarak belirlenmiştir. Bu amaçla ortaya konulan Eylem Planları[18] ve Türkiye'nin ilk Bilgi Toplumu Stratejisi'nde (2006-2010) e-devlete önemli bir yer verilmektedir.

Dünyada olduğu gibi, Türkiye'de de e-devlet hizmetlerinde birçok iş ve işlem gerçekleştirilirken kişisel veriler kullanılmaktadır. e-Devlete geçiş sürecinde, 18 Aralık 2008 tarihinde pilot hizmetlerle hayata geçirilen e-Devlet Kapısı[19], devlet hizmetlerinin tek nokta sayılabilecek bir İnternet adresinde toplaması bakımından Türkiye için bir dönüm noktası teşkil etmektedir. e-Devlet Kapısının açılışında konuşma yapan Ulaştırma Bakanı'nın: "Kurumlarımız bu aşamadan sonra verileri paylaşırken kıskançlık yapmamalıdır." sözleri ile kişisel verilere bu süreçte duyulan

[17] OECD, "Shaping Policies for the Future of the Internet Economy". Ministerial Meeting. Seoul, Korea. s.9.17-18 Haziran 2008.
[18] 2003-2004 Kısa Dönem Eylem Planı ve 2005 Eylem Planı için bkz. DPT Bilgi Toplumu Dairesi. E-Dönüşüm Türkiye Projesi. 11 Kasım 2009. <http://www.bilgitoplumu.gov.tr/Strateji.asp>
[19] Devletin Kısayolu. <www.türkiye.gov.tr>

ihtiyaç vurgulanmaktadır. Zira hayatı zenginleştirmede kullanılabileceği gibi, kişileri mahkum ve kontrol edecek şekilde kötüye de kullanılabilen[20] kişisel veriler, e-devletin gelişmesi için hukuka uygun olarak ve insan haklarına saygı çerçevesinde kullanılmalı, paylaşılmalı ve işlenmelidir. Bilginin kamu kurumları arasında daha geniş bir çevrede iletiminin sağlanması ile elde edilecek fayda ile kişisel veri korumanın gerekliliği ve önemi arasındaki hassas dengenin sağlanmasına dikkat edilmelidir.

12 Eylül 2010 tarihinde yapılan halkoylaması ile Anayasa değişiklik paketinin kabulüne kadar T.C. Anayasasında kişisel verilerin korunmasına ilişkin bağımsız bir temel hak tanımı yer almamıştır. Kabul edilen Anayasa hükümlerinden birisi de kişisel verilerin korunmasına ilişkin olup, bu madde ile ilgili ayrıntılı bilgiler bu çalışmanın 5.4.1. nolu "Anayasa'da kişisel verilerin korunması" bölümünde daha ayrıntılı olarak ele alınmıştır. Bu çalışmanın hazırlandığı dönemde de ulusal hukukta kişisel verilerin korunmasına ilişkin özel bir kanun bulunmamaktadır. Ancak, bu konuda hazırlanan KVKK Tasarısı[21] TBMM'de bulunmakta olup, yasalaşmayı beklemektedir. Söz konusu Kanun Tasarısı daha sonra ayrıntılı olarak incelenecektir.

1.3. Kişi ve Kişilik Hakkı

Hukuk, kişiler arasındaki ilişkileri, toplu halde yaşamı düzenler. Bir diğer ifade ile hukuk, kişiler olduğu için vardır. Hukuk kuralları toplumdaki malları taksim eder; birtakım hak ve yükümlülükler öngörür ve bu yolla toplumda bir düzen yaratır. Hukukun öngördüğü bu hak ve yükümlülüklerin bir sahibinin olması gerekir. Hukuk bunları kişiye yöneltmiştir. *Kişi*, haklardan yararlanan, hak sahibi olan varlık demektir.[22] Sağ ve tam doğmak şartıyla kişi artık hak sujesi olmakta, yani hak ehliyetini kazanmaktadır. Hukukumuzda hak sujesi olan iki tür kişi bulunmaktadır, bunlar gerçek ve tüzel kişilerdir.

---

[20] Thomas and Walport. 2008:i
[21] Kişisel Verilerin Korunması Kanunu Tasarısı için bkz. <http://www2.tbmm.gov.tr/d23/1/1-0576.pdf> Erişim tarihi: 11 Kasım 2009.
[22] Öztan, 2005:221

4721 sayılı Türk Medeni Kanunu'nda kişiyle birlikte kişilik kavramına da yer verilmektedir. *Kişilik*, kişiye bağlı ve hukukça korunan bedeni, manevi, hukuki nitelikteki varlıkların tümünü ifade eder. Kişilik doğumla başlar ve ölümle sona erer.

Kişinin, kişiliğini oluşturan hayatı, sağlığı ve beden bütünlüğü gibi maddi (cismani) varlığı ile; özgürlüğü, dini ve vicdani inançları, şeref ve haysiyeti, itibarı, ismi, resmi, gizlilik ve sır çevresi gibi çeşitli manevi varlıklarının tamamı üzerinde hukuken korunan menfaatine ise *kişilik hakkı* denir. Kısaca kişilik hakkı, kişinin toplumda yer alabilmesi ve kişiliğini serbestçe geliştirebilmesi için tüm maddi ve manevi değerler üzerindeki hak olarak da tanımlanabilir. Bu hak, kişiye üçüncü kişilerden kişilik hakkına saygı gösterilmesini ve kişilik değerlerine dokunulmamasını isteme yetkisi verir. Kişilik hakkının içeriği yere ve zamana göre değişebileceğinden Türk Medeni Kanunu'nun 24 ve Borçlar Kanunu'nun 49'uncu maddelerinde kişilik hakkı çerçeve hüküm olarak düzenlenmiş ve içeriğinin doldurulması hakime bırakılmıştır.

Günümüzde teknolojide ve insanların yaşayış şekillerinde meydana gelen hızlı gelişim düşünülürse, kişiliğin mahiyeti ve kişiliğe saldırı çeşitlerinin değişmesi kaçınılmazdır.[23] Kişisel verilerin korunması da bu yönüyle kişilik hakkının korunmasının bir parçasıdır.

1.3.1. Kişisel veri koruma hukukunda kişi

Türk Medeni Kanunu'nun birinci kitabı olarak düzenlenmiş olan Kişiler Hukuku'na ilişkin üç temel ilke bulunmaktadır. Bunlar; kişilerin eşitliği, özgürlüğü ve kişinin korunması ilkeleridir.

Kişisel verilerin korunmasının özünde, "kişinin korunması" ilkesi bulunmaktadır. Bu ilkeye göre, herkesin diğer kişilerden saygı görmeyi isteme hakkı vardır. Kişi, kişilik değerlerinin zedelenmemesini talep hakkına sahiptir. Kişiler, hak ve fiil ehliyetlerinden kısmen de olsa vazgeçemeyeceği gibi, özgürlüklerinden de vazgeçemez veya onları hukuka veya ahlaka aykırı olarak sınırlayamaz (TMK, md. 23). Saldırılar karşısında en temel ilke ise belirli istisnaların gerçekleşmesi hali dışında kişilik haklarına yapılan her saldırının hukuka aykırı olduğudur. Bu

[23] Zevkliler, 1999:445

istisnalar, TMK md. 24'te sınırlandırılmış olup, kişilik hakkı zedelenen kimsenin rızası, daha üstün nitelikte özel veya kamusal yarar ya da kanunun verdiği yetkinin kullanılması sebeplerinden biriyle saldırının haklı olması olarak sayılmaktadır.[24]

TMK'nın kişiliğin korunmasına yönelik bu ilkeleri, hukukumuzun kişiliğe ne derece önem verdiğinin göstergeleri durumundadır.

1.3.2. Kişisel veri koruma hukukunda gerçek – tüzel kişi ayrımı

AB Direktifleri, OECD çalışmaları ve Avrupa Konseyi Sözleşmeleri kişisel verileri koruma alanını gerçek kişilerle sınırlamıştır. Kişisel verilerin korunması hukukunun genel ve öncelikli hedefi de gerçek kişileri ve onların mahremiyet ve kişilik haklarını korumaktır. Ancak günümüzde tüzel kişilere ait verilerden kişisel verilere ulaşmanın kolaylığı nedeniyle[25] tüzel kişilere ilişkin gerçek kişi bilgilerinin de dikkatle korunmasına özen gösterilmelidir.

1.4. Kişisel Veri ve İlgili Bazı Kavramlar

Kişisel veriler, bireylerin kimliklerini tespit etmeye yarayan bilgilerdir. Ad, soyad, adres, iş, meslek, araç, kredi kartı bilgileri ya da sağlık, istihdam, sendikal veya siyasi faaliyetler, sosyal güvenliğe ilişkin bilgiler ile bir kişiyi tanınabilir veya belirlenebilir kılmaya yarayacak nitelikte her tür bilgi kişisel veridir. Bu bilgiler, elektronik araçlar ve özellikle İnternet aracılığıyla çok kolay bir şekilde kaydedilmekte, transfer edilmekte ve sınıflandırılmaktadır.

AB'nin, kişisel verilerin korunmasına ilişkin çerçeve nitelikteki 95/46/AT sayılı Veri Koruma Direktifi (VKD) kişisel veriyi *"Kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkili her tür veri"* (md. 2/a) olarak tanımlamaktadır. Maddenin devamında kimliği belirlenebilir kişi, *"doğrudan veya dolaylı olarak özellikle bir kimlik numarasının veya kişinin fiziksel, fizyolojik, akli, ekonomik, kültürel veya*

---

[24] TMK, md. 24 "Hukuka aykırı olarak kişilik hakkına saldırılan kimse, hakimden, saldırıda bulunanlara karşı korunmasını isteyebilir.

Kişilik hakkı zedelenen kimsenin rızası, daha üstün nitelikte özel veya kamusal yarar ya da kanunun verdiği yetkinin kullanılması sebeplerinden biriyle haklı kılınmadıkça, kişilik haklarına yapılan her saldırı hukuka aykırıdır."

[25] Örneğin bir şirkete ait verilerden o şirketin ortaklarına ve onların kişisel verilerine, yine bir şirketin prim veya sigortalı işçi bildiriminden o şirketin sahibine, oradan da sahibinin malvarlığı bilgisine ulaşabilmek mümkündür.

sosyal kimliğine ait bir veya birden fazla spesifik faktörün referansına dayanılarak teşhis edilebilir olan kişi" olarak tanımlanmaktadır. Tanımlayıcı bir numara veya kişinin fiziksel, psikolojik, zihinsel, ekonomik, kültürel ve sosyal kimliğine ilişkin bir ya da birden fazla verinin bir araya getirilmesi ile bir kişinin kimliği doğrudan veya dolaylı olarak belirlenebilir duruma gelebilir. İşte tüm bu veriler, o kişiye ait kişisel verileri teşkil eder. Ülkemizde T.C. kimlik numarası, ad-soyad, sosyal güvenlik numarası, vergi numarası, kişinin malvarlığı, ailesi, okulu, çalıştığı işyeri, adresi vs. bilgiler belli başlı kişisel verilerdendir.

VKD'deki kişisel veri tanımı, üye ülkelerde farklı anlaşılarak uygulamalarda farklılıkların doğmasına yol açabilmektedir. Kişisel veri tanımına ilişkin uygulamadan kaynaklanabilecek bu farklılıkların azaltılması ve farkındalığın artırılması amacıyla Avrupa Komisyonu bünyesindeki Veri Koruma Çalışma Grubunun[26], kişisel veri tanımına ilişkin yaptığı bazı açıklamaları aşağıda incelenmektedir.

i) Her tür veri: Kanun koyucu, bu ifadeyle kişisel veri kavramını oldukça geniş tutarak bu kapsama nesnel (objektif) ve öznel (subjektif) bilgileri dahil etmiştir. Bu bilgi türlerinden kişinin kanında bulunan bir bileşen nesnel; kişinin inanç, düşünce ve değerleri öznel bilgilere örnek olarak verilebilir. Bankacılıkta kredi kullananların (borçluların) güvenilirliğinin ölçülmesinde, sigortacılıkta ve istihdam gibi alanlarda subjektif veriler, sözleşmenin kurulmasında kişiyi tanımlanabilir kılan asli verilerdendir.[27]

"Her tür veri" kavramı, kişisel verinin tutulduğu ortam veya verinin tutulma şeklinden bağımsızdır. Örneğin, bir okulda kayıtlı öğrencilerin kimlik bilgilerinin alfabetik, nümerik/sayısal veya fotoğraf bazlı olması o verilerin kişisel veri olmasını engellememektedir. Bir başka örnek olarak; istatistiklerle ilgilenen bir kurumda, herhangi bir araştırmaya ilişkin kişisel verilerin grafik veya şekil halinde bulunması

[26] Article 29 Data Protection Working Party. "Working Document on the processing of personal data relating to health in electronic health records (EHR)". 15 Şubat 2007. 28 Ocak 2009. <http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp131_en.pdf>

[27]Örneğin şu bilgiler sırasıyla bankacılık, sigortacılık ve istihdam alanında sözleşmenin kurulmasına etki eden kişisel bilgilerdir. "Ali borçların ifası konusunda güvenilirdir.", "Mehmet'in sağlık durumunda problem görülmediğinden ölümle sonuçlanabilecek riskli bir durumu bulunmamaktadır.", "Ayşe iyi bir çalışandır; ayrıca kurallara saygılıdır."

önem arz etmemektedir. Söz konusu verilerin kişilerin tanınabilir veya kimliğini belirleyebilir olmasını engelleyecek "anonimleştirme" işlemine tabi tutulması dışında, bu grafik veya şekiller kişisel veri olarak kabul edilmelidir. Yine bir konservatuar öğrencisinin akustik halde tutulan ses kayıtları ya da telefon bankacılığı ile işlem yapıldığı esnada müşterinin kaydedilmiş sesli talimatı da o kişiyi belirleyebilecek nitelikte ise kişisel verilerin kapsamına dahildir. Bireylerin kamera ile kayda alınan görüntüleri de birey, görüntü içinde fark edilir ve tanınabilir düzeyde ise kişisel veridir.

Biyolojik özelliklerden kaynaklanan biometrik veriler de kişisel verilerdendir. Parmak izi, retina, ses, yüz hatları, elin şekli, damarlar, değişik yetenekler, davranış karakteristiği (mesela elyazısıyla imza, tuşa dokunma biçimi, değişik yürüme veya konuşma tarzı gibi veriler) kişinin biometrik verileri olarak sınıflandırılabilecek kişisel verileridir.[28]

Psikolojik karakteristiği yansıtan bilgiler de yine kişisel veridir. İrlanda'da boşanma talebi ile mahkemeye başvuran bir çiftin yargılamasında hakim, bu çiftin çocuklarına, ailesini temsil eden çizgi çalışması yaptırmıştır. Bu nöro-psikiyatrik çalışma, psikolojik olarak analiz edildiğinde çocuğun ruh hali ve aile bireyleri hakkında hissettiklerini yansıtması sebebiyle, "kişisel veri" olarak kabul edilmiştir.[29]

Bir verinin kişisel veri olarak değerlendirilebilmesi için bilginin doğru veya kanıtlanmış olmasına gerek yoktur. Zira, VKD'ye göre veri sahibi, kendisine ilişkin bilgileri görme ve yanlışlığın düzeltilmesi için hukuki yollara başvurma hakkına sahiptir.

ii) Belirli ya da belirlenebilir gerçek kişi: VKD'nin kişisel veri tanımı içinde geçen bir diğer ifade de verinin, kimliği "belirli ya da belirlenebilir gerçek kişi" ile

[28] Belirli bir bireye özgü olması ve başka kimsede bulunmaması nedeniyle biometrik veriler kimlik doğrulayıcı (identifier) olarak kullanılabilirler. Ör: DNA verisi. Bununla birlikte, insan doku örneği biometrik verinin kaynağı olsa da biometrik veri değildir. Örneğin parmak izi biometrik veridir; ancak parmak tek başına değildir. Doku örneklerinin (kan örneği gibi) toplanması, depolanması ve bunların kullanılması Kişisel Veri Direktifi kapsamında değerlendirilmelidir. (Bkz. Council of Europe Recommendation No. Rec (2006) 4 of the Committee of Ministers to member states on research on biological materials of human origin, <https://wcd.coe.int/ViewDoc.jsp?id=977859>)

[29] Psikiyatrik bakış açısıyla resim çocuğun sağlık durumu hakkında da bilgi vermektedir; ayrıca anne ve babasının davranış biçimleri hakkında da bilgileri içerir. Sonuç olarak böyle bir durumda, haklarında bilgi veren bu resimler konusunda anne babanın da katılma haklarını (gerekli açıklamalar yapma, savunma hakkı gibi karşı hak bildirme durumu) kullanabilecekleri öne sürülebilir.

ilişkili olmasıdır. Belirli bir kişiyi diğerlerinden ayırt etmeyi ve o kişiyi betimlemeyi sağlayan bilgiler, bir kişiyi belirli ya da belirlenebilir kılmaktadır. Mesela kişinin dış görünüşü, boyu, saç rengi, giyimi veya kişinin hemen belirlenmesini sağlamasa da mesleği, adı, herhangi bir özelliği bu tür verilerin kapsamı içinde değerlendirilmektedir.

iii) İlişkili olma: Tanımda geçtiği üzere, kişi ile veriyi "ilişki"lendiren unsur, o verinin "içerik", "amaç" ya da "sonuç" unsurlarından en az birinin kişi ile bağlantılı olmasını gerektirmektedir. Örneğin; bir taşınmazın değeri normalde veri koruma yasalarına tabi değildir. Ancak bu taşınmazın değeri, malikine ait ad-soyad veya kimlik numarası gibi bilgilerden herhangi biri ile ilişkili olarak yan yana ya da birbirini tamamlayacak başka bir şekilde birlikte bulunuyorsa, verinin artık o kişinin malvarlığını, vergi mükellefiyetini tanımlaması nedeniyle, taşınmazın değeri bir kişisel veri haline gelmiş olacaktır. Kişinin davranışının bir sonucu olması nedeniyle, kredi kartı ile yapılan alışverişin faturası da kişiyle "ilişkili" bir kişisel veridir.

VKD'nin 2'nci maddesinin (b) fıkrasında ise *kişisel verilerin işlenmesi* tanımlanmaktadır. Buna göre,

"*Toplama, kaydetme, organize etme, saklama, uyarlama veya değiştirme, geri alma, danışma, kullanma, ileti ile açığa çıkarma, yayma veya başka şekilde mevcut hale getirme, sıraya koyma veya birleştirme, bloke etme, silme veya yok etme gibi otomatik olan veya olmayan araçlarla, kişisel veri üzerinde uygulanan her türden işlem veya işlem dizisi o veriyi işlemektir*."

Veri koruma hukukunda sıklıkla kullanılan ve veri işleme tanımı içinde kullanılan diğer bazı tanımlar ise şöyle yapılabilir:

Kişisel verilerin toplanması: Kişiye ait her tür bilginin herhangi bir şekilde edinilmesi ve tedarikini ifade etmektedir.[30]

Kişisel verilerin depolanması: Kağıt, resim veya elektronik veri taşıyıcıları kullanılarak kişisel bilgilerin kaydı veya koruma altına alınmasıdır.

[30] Peter 1995:90: Özdemir'den 2009:135

Kişisel verilerin değiştirilmesi: Toplanıp depolanan kişisel verilerin içeriğinin çeşitli sebep ve amaçlarla değiştirilmesidir.[31] Silme faaliyeti ise, değiştirme faaliyetinden farklı olarak, kişisel verilerin tutulduğu ortama göre teknik araçlar veya el ile okunamayacak hale getirilmesi işlemidir.

1.4.1. Bazı önemli kişisel veriler

Kişisel veriler, sınırlı sayıda değildir ve kapsamı genişletilebilir. Ancak günümüzde en yaygın kullanılan belli başlı kişisel veriler aşağıda verilmektedir.

Kimlik bilgileri: Kişilerin ad ve soyadı, kimlik numarası, doğum yeri, tarihi, anne-baba adı, anne kızlık soyadı, nüfusa kayıtlı olduğu yer vb. gibi kişinin tanımlanabilir olmasını sağlayan her tür vatandaşlık kimlik kartı, sürücü belgesi, sosyal güvenlik kayıtları, vergi kimlik bilgilerine ilişkin bilgileri, o kişinin kimlik bilgilerini oluşturmaktadır. Kişiye ait fotoğraf, resim, kamera kayıtları içinde o kişinin ayırt edilmesini sağlayacak görüntüler de kimlik bilgileri içinde değerlendirilebilir.

Adres bilgileri: Yerleşim yeri, bir kimsenin sürekli kalma niyetiyle oturduğu yerdir.[32] Kişinin kendisi veya ailesinin ikametine, işyerine ya da geçici yerleşkesine ait adres bilgileri o kişiye ait kişisel verilerdendir.

Kredi kartı bilgileri: Kişinin kredi kartına ilişkin şifre, güvenlik kodu gibi kişisel bilgiler sıklıkla kimlik hırsızlığına konu olmaktadır. Bu çalışmanın "Kişisel Verilerin Ticari Değeri ve Siber Suçlar" başlıklı ikinci bölümünde görüleceği üzere bu veriler, elektronik ortamda satışa konu olabilmektedir. Bununla birlikte, kredi kartı ile yapılan her harcamanın kaydı tutulmaktadır.[33] Bu kayıtlar yasal takiplerde hukuka uygun olarak kullanılabileceği gibi, hukuka uygun olmayan başka amaçlarla da kullanılabilir. Ayrıca, bu bilgilerin kişilerin alışveriş profilleri çıkarılarak pazarlama amacıyla kullanılması sıklıkla rastlanan bir olgudur.

---

[31] Özdemir, 2009:136
[32] Türk Medeni Kanunu (TMK), md. 19.
[33] Dinç, 2006:9

Telefon bilgileri: Günümüzde sabit telefonların yanında kişilerin bir veya birden fazla GSM hat ve numaraları bulunmaktadır. Bütün bu bilgiler ile kişiye ait faks numaraları kişiye erişimi sağlayan temel kişisel verilerdendir.

Ülkemizde Haziran 2009 tarihi itibarıyla GSM abone sayısı 63.614.157[34], sabit telefon abone sayısı ise 17.071.269[35] dir. Neredeyse kişi başına bir cep telefonu hattının düştüğü ülkemizde bu veriler zincirleme olarak kişi hakkında yer, adres, bölge verilerine ulaşabilmeyi mümkün kıldığından kritik önemi haizdir. Ayrıca telefon bilgilerinin en çok kullanıldığı alanlardan birisi de bir çok ülkenin gönderimini yasakladığı veya belli kurallara bağladığı istenmeyen iletilerin (spam) pazarlama amacıyla gönderilmesi için kullanılmasıdır.

Elektronik posta bilgileri: İnternet ortamında her tür mektup vb. yazışma ile özel bilgi ve belgelerin değişiminde kullanılan elektronik posta adresleri de kişinin haberleşme hakkı bağlamındaki kişisel bilgilerindendir. Kişilerin haberleşme bilgilerine bakılarak oluşturulabilen profiller[36] reklamcılar için önemli bir pazarlama aracı olarak kullanılmaktadır. Tüketicilerin alışveriş alışkanlıkları, tercihleri gibi bilgileri analiz etmek, kişisel veri koruma hukuku kapsamında olumlu bir değer yaratılması için kullanılabileceği gibi; bu veriler güvenli ve güvenilir olmayan şekillerde işlemeye konu olduğunda ise büyük zararların oluşması olasıdır.

Kamu kurumlarındaki bilgiler: Kamu kurum ve kuruluşları kanunla verilen görevlerini yerine getirirken çok sayıda kişisel veriye ihtiyaç duymaktadırlar. İstatistik, sosyal güvenlik ve kolluk alanında, içişleri ve vatandaşlık ile ilgili iş ve işlemlerde, tapu ve vergi kayıtlarında, adrese dayalı iş ve işlemlerde kişisel veriler kullanılmaktadır. Ülkemizde giderek gelişen ve yaygınlaşan e-devlet projelerinden MERNIS, VEDOP, POLNET, UYAP, TAKBİS projeleri ya da MOBESE, Adrese Dayalı Nüfus Kayıt Sistemi gibi sistemler bu verilerin paylaşılmasını, görülmesini ve kullanılmasını kolaylaştırmıştır. Bu nedenle, bu verilerin korunması ihtiyaç ve

[34] BTK. Yayınlar/ İstatistikler. İşletmecilerden alınan veriler sonrası hazırlanan istatistikler. GSM 2009. 17 Kasım 2009. <http://www.tk.gov.tr/Yayin/istatistikler/istatistik/2009/gsm2009.htm>
[35] Yukarıdaki kaynak. PSTN 2009. 17 Kasım 2009.
<http://www.tk.gov.tr/Yayin/istatistikler/istatistik/2009/pstn2009.htm>
[36] Bilgi parçalarıyla oluşturulan profiller, kişi hakkında tanımlanabilir olma özelliklerini taşıması ve o kişinin siyasi görüşü, okuduğu gazete, ilgilendiği konular üzerinde fikir vermesi ile kişisel veriler içerisinde yer almaktadır.

gereklilikleri daha fazla hissedilmeye başlanmıştır. Kağıt ortamında veya otomatik işlenebilir bilgisayar ortamında tutulan veriler, oy ve nüfus sahteciliklerinin yanı sıra, vergi borcunu silme, ölü birisinin yerine geçme, sınavı kazanmış gibi gösterme, emekli maaşı bağlama gibi birçok sahteciliğin konusunu oluşturabileceği gibi, kişilerin özel hayatlarını ifşa etmede de kullanılabilir.

1.4.2. Hassas veriler

Korunmaması halinde toplumda ayrımcılık yaratma riski yüksek olan kişisel verilere "hassas veriler" denilmektedir. Kural olarak bu veriler işlenemezler. Bu veriler, yalnızca kanunla belirlenmiş bazı istisnai durumlarda işlenebilirler. AB üyesi ülkeler, kamu yararı nedeniyle bu istisnaları kısmen genişletebilirler.

VKD'nin "Özel Veri Kategorilerinin İşlenmesi" başlığını taşıyan 8'inci maddesinde hassas veriler, ırki veya etnik köken, siyasi görüş, dini veya felsefi inanç, meslek birliğine üyelik, sağlık ve cinsel tercih bilgileri olarak sayılmaktadır. Bu Direktifte, hassas verilerin üye ülkelerde işlenmesinin yasak olması gerektiği belirtildikten sonra, bu kuralın uygulanmayacağı, hassas verilerin işlenmesinde hukuka uygunluk sebebi olan beş ayrı istisnai durum düzenlenmiştir. Buna göre hassas veriler : *i)* kişinin bu verilerin işlenmesine ilişkin açık rıza vermesi, *ii)* iş hukuku kapsamındaki zorunlu durumlarda yeterli yasal ve teknik önlemlerin sağlanması, *iii)* veri sahibinin, fiziksel olarak rıza verebilecek anlayış ve kudretinin olmaması ya da yasal olarak rıza vermeye ehliyetinin olmaması halinde veri işlemenin, veri sahibi veya üçüncü bir kişinin hayati çıkarlarının korunması için zorunlu olması, *iv)* kâr amacı gütmeyen herhangi vakıf, örgüt, siyasi, felsefi veya sendikal nitelikte bir kurumun hukuka uygun bir amacının gerçekleşebilmesi için, sadece düzenli olarak bağlantıda olduğu kişilerle ilgili olarak, bu kişilere uygun garantilerin sağlanması ve verilerin üçüncü kişilerle paylaşılması gerektiği her bir durum için bu kişilerin yeni rızalarının alınması şartıyla ve *v)* veri sahibinin aleni olarak ilan etmiş olduğu verilerinin, bir hakkın tesisi, kullanılması ve korunabilmesi için veri işlemenin zorunlu olduğu durumlarda işlenebilecektir.

1.5. Kişisel Verilerin Korunması Hukuku

1.5.1. Genel olarak

1953 yılında IBM'in "IBM 701" modeliyle başlayan elektronik veri işletim sistemlerinin gelişimi, 1983'te geliştirilen ilk veri bankalarından günümüz veri işletim sistemlerine ulaşmıştır. Banka ve sigorta şirketleri gibi geniş bir hizmet ağına ve müşteri portföyüne sahip kuruluşlar tarafından tercih edilen ana işlemciler ile, birçok işlemci bir ana işlemci üzerinden farklı işlemleri aynı anda gerçekleştirebilmektedir. Bu işlemlere, hesap sahiplerinin otomatik ödeme emirleri neticesinde faturalarını ödemesi ya da İnternet üzerinden müşterilerin "çevrimiçi" ya da "sanal" para transferi emirlerinin eşzamanlı yerine getirilmesi örnek gösterilebilir.[37]

Daha önce de ifade edildiği gibi, özellikle 1970'li yıllardan bu yana otomatik veri işleme araçları vasıtasıyla verilerin sınırsız olarak kaydedilebilme kapasitesi, bu verilere her zaman ulaşılabilir olması ve kişilik profillerinin oluşturulabilme olasılığı, insan davranışları üzerinde şimdiye kadar görülmeyen bir şekilde psikolojik baskı yaratmış ve insanın bu suretle kamusal yaşama katılmasını etkileyebilmiştir.[38] BİT'in yarattığı bu etki, kişisel verileri korumayı ve güvence altına almayı gerektiren politikaların geliştirilmesine sebep olmuştur.

Bu dönemde, birçok Avrupa ülkesi ve Amerika'da, gelişen teknolojilere ayak uydurabilmek, devletin tuttuğu kişisel bilgilere bireyin erişim sağlayarak bu bilgilerin doğruluğu ve uygun olup olmadığını kontrol edebilmesi imkanını sağlamak, bu şekilde devletin daha demokratik ve şeffaf olabilmesini temin etmek için bireylere *bilgiye erişim hakkı* sağlayan kanunlar ihdas edilmiştir. Bu dönemde yapılan kanunlar devletlerin yapılarına göre ulusal düzeyde olabildiği gibi bölgesel düzeyde de bulunabilmektedir. Birçok ülke mahremiyet ve veri koruma kanunlarına, bilgiye erişim (bilgi edinme) hakkının bir parçası olarak hukuk sistemlerinde yer vermiştir.

[37] Başalp, 2004:23
[38] Şimşek, 2008:115

Kıta Avrupasında söz konusu düzenlemeler "veri kanunları" ya da "veri koruma kanunları" (lois sur la protection des donnees) olarak adlandırılırken, İngilizce konuşan ülkelerde ise genellikle "mahremiyet koruma kanunları" (privacy protection laws) olarak adlandırılmaktadır.

Genel kanının aksine, kişisel veri koruma kanunları, kişisel veri tutan kurum, kuruluş, şirket veya bireylerin veri işlemesini yasaklamamaktadır. Bu kanunlar, veri işleme görev ve yetkisinin nerede biteceğine ve verinin tanımladığı ve ilişkisi olduğu veri sahibi kişinin (bundan böyle VKD ile uyumlu olarak "veri öznesi" kullanılacaktır) bu işleme neticesinde hak ve özgürlükleri ile mahremiyetine zarar verilmemesi, verilmişse buna ilişkin mekanizmaların işletilmesi ile ilgilenmektedir. Kısacası veri koruma kanunları, veri işleme ile elde edilecek yarar pahasına kişi onurunu ihmal etmemekte, kişilik hakkını korumaktadır. Bununla birlikte, bu korumanın, kişi lehine sınırsız olduğu düşünülmemelidir.

Günümüzde e-ticaretin yaygınlaşması ve bilgi teknolojileri kullanımının sağladığı maliyet avantajları nedeniyle, birçok şirket, iş ve işlemlerini elektronik ortama taşımıştır. Tüketici verilerini otomatik yollarla işleyerek müşteri profilleri oluşturan firma sayısının artması ile birlikte, kişisel verilerin hukuka uygun olarak işlenmesi ve bu verilerin toplandıkları amacın dışında kullanılmaması talebi, sadece devlete karşı ileri sürülebilecek bir hak olmaktan çıkmıştır. GSM şirketleri, bankalar, sigorta şirketleri, özel sağlık kuruluşları, oteller ve diğer turizm acenteleri gibi çok sayıda kişisel veri tutan özel sektör kuruluşları da kişisel verilerin korunması taleplerinin muhatabı durumundadırlar.

Kişisel verilerin kötüye kullanılmasıyla mücadelede güvenliğin ve tüketici güveninin sağlanması, kalıcı ve daha verimli ilişkiler kurulması ve bir insan hakkı olarak "mahremiyet hakkı"nın korunması için dünyada birçok ülke kanun yapma sürecini tamamlamış olup, bir kısım ülkelerde ise kanun hazırlıkları devam etmektedir. Halihazırda yasal düzenlemeye sahip ülkeler ya korumada yeni alanlara yönelmiştir ya da mevcut düzenlemelerini yeniden gözden geçirmekte ve eksiklerini tamamlamaktadır.[39] Ülkemizin de içinde bulunduğu bazı ülkelerde ise veri koruma

[39] OECD, 2002:24

ile ilgili mevzuat hazırlık çalışmaları devam etmektedir. Bu konuda Türkiye'de yürütülen çalışmalardan ileride bahsedilecektir.

1.5.2. Mahremiyet hakkı

Mahremiyet kavramı ilk kez 1890 yılında Amerikalı yargıç Brandeis tarafından "bireyin yalnız bırakılma hakkı" olarak tanımlanmıştır.[40] *Özel hayatın gizliliğinin korunması* ya da *mahremiyet* açısından bir dönüm noktası oluşturan bu yaklaşım önce ABD'de, sonra da uluslararası düzeyde kabullenilmiştir.[41] 1960 ve 1970'li yıllarda birçok ülke kişisel veri ve mahremiyet üzerinde çalışmalar başlatmıştır. Bu dönemlerde ABD'de mahremiyet ile ilgili olarak yapılan iki tanım literatüre önemli katkı sağlamıştır. Bu tanımlardan Westin mahremiyeti "bireyin kendisi hakkındaki bilgilerin ne zaman, nasıl ve ne oranda diğer kişilere paylaşılabileceği hakkındaki belirleme yetkisi" olarak tanımlarken[42]; Miller'in mahremiyet tanımı daha açık ve nettir. Miller'e göre mahremiyet, "bireyin kendisi ile ilgili bilginin dolaşımı üzerindeki kontrol imkanıdır"[43]. Bu kavram günümüzde evde, işyerinde kişisel tercihlere göre hareket etme ve karar alma, bağımsız bir şekilde hiçbir etki altında kalmadan haberleşme, kişisel bilgilerin ve haberleşme içeriğinin güvenilir olması gibi özel hayatın gizliliğine ilişkin fiziksel bir durum olarak kabul görmektedir.

Günün koşulları ve sosyo-ekonomik gelişime paralel olarak özel hayatın gizliliğinin kapsamı ve içeriği de değişmekte ve gelişmektedir. Günümüzde özel hayatın gizliliği şu başlıklar altında incelenmektedir:

- Kişinin üstünün, özel kağıtlarının, eşyasının ve konutunun dokunulmazlığı gibi hususları içeren *"bölgesel mahremiyet";*
- Kişinin mektuplarının, telefon görüşmelerinin, e-posta ve diğer iletişim olanaklarının içerdiği bilgilerin gizliliğinin ve güvenilirliğinin korunmasına ilişkin *"haberleşmenin gizliliği";*

[40] Beceni, 2004:9
[41] TBD, 2008:18
[42] Westin, 1967:7
[43] Miller, 1971:25

- Kişinin vücut bütünlüğüne yönelik olarak genetik ve uyuşturucu testleri gibi müdahaleleri içeren *"vücut bütünlüğüne ilişkin mahremiyet";*
- Kişisel verilerin her tür işlenmesi sürecini kapsayan *"veri mahremiyeti"*.[44]

Mahremiyet, temel bir "hak" ve "özgürlük"tür. Dolayısıyla mahremiyet, kişilerin kamusal alan ile özel hayatının ayrı kalmasını sağlayarak onların bu alanda diledikleri gibi tartışmalarını, konuşmalarını ve düşünmelerini garanti altına almaktadır. Bu hak, kişiye ait bilgilerin, kişinin kontrolünden çıkarak istenmeyen sonuçların oluşmasının önlenmesi için tedbir alınmasında kullanılır. Örneğin Alman hukukunda bu önlem, kişinin kendisi ile ilgili veriler üzerinde, o bilgilerin açıklanması ve kullanılmasına ilişkin belirleme yetkisinin (self-determinasyon hakkı) oldukça geniş tutulması ile sağlanmaktadır.

Mahremiyetin normatif temelleri birtakım uluslararası belgelere dayanmaktadır. Başta BM İnsan Hakları Evrensel Bildirisi (1948) ve Avrupa İnsan Hakları Sözleşmesi (AİHS) (1950) olmak üzere birçok hukuk belgesinde mahremiyet hakkı temel insan hakları arasında sayılmaktadır. İnsan Hakları Evrensel Bildirisi'nin 12'nci maddesine göre:

"Kimsenin özel yaşamı, ailesi, konutu ya da haberleşmesine keyfi olarak karışılamaz, şeref ve adına saldırılamaz. Herkesin, bu tür karışma ve saldırılara karşı yasa tarafından korunma hakkı vardır."

Ülkemizin de imzaladığı ve onaylamış olduğu AİHS'nin[45] "Özel hayatın ve aile hayatının korunması" başlıklı 8'inci maddesinde ise mahremiyet şöyle ifade edilmektedir:

"Herkes özel ve aile hayatına, konutuna ve haberleşmesine saygı gösterilmesi hakkına sahiptir. Bu hakkın kullanılmasına bir kamu otoritesinin müdahalesi, ancak

---

[44] TBD, 2008:18

[45] *Türkiye, AİHS'ni 1954 yılında 6366 sayılı kanunla onaylamış ve iç hukukun parçası haline getirmiştir. Daha sonra 28.1.1987 tarihinde Avrupa Komisyonunun ve 22.1.1990 tarihinde Adalet Divanının yargılama yetkisini tanımasıyla denetleme sistemine dahil olmuştur. Türkiye, yargı yetkisini tanıyan beyanında, bildirdiği bazı çekincelerini (sıkıyönetim ve olağanüstü hallerde, askeri personelin hukuki statüsü ve disiplin sistemiyle ilgili konularda) Bakanlar Kurulunun 1992 yılındaki kararıyla kaldırmış ve durum Konseye bildirilmiştir. Halihazırda AİHM kararlarıTürkiye için bağlayıcıdır.*

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

BM Siyasi ve Medeni Haklar Sözleşmesinin 17'nci maddesi[46] de mahremiyet hakkını düzenlemektedir. Yine AB Temel Haklar Bildirgesinin 7'nci maddesine göre herkes, özel ve aile yaşamına, konutuna ve haberleşmesine saygı gösterilmesini isteme hakkına sahiptir. Bu Bildirgenin 8'inci maddesi ise veri korumayı temel bir insan hakkı olarak kabul etmekte ve bu hakkın kullanımını tesis edecek bağımsız bir makamdan söz etmektedir:

Kişisel bilgilerin korunması

1. Herkes, kendisine ilişkin kişisel bilgilerin korunmasını isteme hakkına sahiptir.

2. Bu tür bilgiler, belirtilen amaçlar için ve ilgili kişinin muvafakatine veya yasada öngörülen başka meşru temele dayalı olarak adil şekilde kullanılmalıdır. Herkes, kendisi hakkında toplanmış olan bilgilere erişme ve bunlarda düzeltme yaptırma hakkına sahiptir.

3. Bu kurallara uyulması, bağımsız bir makam tarafından denetlenecektir.

Yukarıda bir kısmı ifade edilen uluslararası normatif belgeler ile çeşitli ulusal yasalara bakıldığında bu araçların bazı temel ilke ve koşullara dayandığı görülmektedir. Mahremiyetin korunmasına ilişkin söz konusu ilke ve koşulların ortak özellikleri aşağıdaki gibi özetlenebilir:

- Kişisel veriler toplandığında bireyler bu konuda haberdar edilmelidir.
- Verileri kimin, ne sebeple topladığını açıklaması gerekmektedir.

[46] Madde 17 - Mahremiyet hakkı
Hiç kimsenin özel ve aile ya□am‹na, konutuna veya haberle□mesine keyfi veya hukuka ayk‹r‹ olarak müdahale edilemez; onuru veya itibar‹ hukuka ayk‹r‹ sald‹r‹lara maruz b‹rak‹lamaz.
Herkes bu tür sald‹r‹lara veya müdahalelere kar□‹ hukuk taraf‹ndan korunma hakk‹na sahiptir.

- Bireylerin kendileri ile ilgili verilere nasıl erişebileceklerinin belirtilmesi ile bu bilgilerinin doğruluğunun görülebilmesinin sağlanması ve güncelleme taleplerinin yapılmasını sağlayacak yöntemler bildirilmelidir.
- Kişiler, kendileri ile ilgili verilerin kötüye kullanımlardan ne şekilde korunduğu hakkında bilgilendirilmelidir.[47]

Mahremiyet kavramının siber uzaydaki[48] açılımı "bilgi (enformasyon) mahremiyeti" terimi içinde somutlaşmaktadır. Bilgi mahremiyeti, bireyleri tanımlayabilir nitelikteki kişisel bilgilerin açıklanması, elde edilmesi ve kullanılması üzerinde, bireylerin hukuken kontrol ve denetim hakkının bulunması olarak tanımlanmaktadır[49]. Aynı şekilde, Amerika'da 1973 yılında yayımlanan Özel Komite raporuna[50] göre, bir kişiyi tanımlanabilir kılacak nitelikte veriyi içeren bir kayıt, ilişkin olduğu bireyin bu kayıtların içeriği ve ne şekilde açıklanabileceği konusunda karar vermeye katılmasını sağlayacak şekilde işletilmelidir. Kişiyi tanımlanabilir kılan bu tür verilerin, kanuni dayanağı olmaksızın her tür kullanımı, açıklanması ve kaydedilmesi hukuka aykırı addedilmelidir.

1.5.3. Gözetleme (İzleme) toplumu

Günümüzde ilkel veri edinme yöntemlerinin yerini alan cep telefonları, GPS cihazları, radyo frekansı ile tanımlama teknolojisi (RFID)[51] etiketleri vb. bilgi ve iletişim teknolojileri bireylerin zaman ve mekan bağlamındaki davranışları hakkında şimdiye kadar görülmemiş boyutlarda verinin toplanmasına olanak sağlamaktadır.[52] Bu sistemler, veri işleme kapasitesini artırdığı gibi, tek bir organizasyon ya da farklı

---

[47] Rand Europe, 2009:2

[48] Siber uzay (cyber space) kavramını ilk kez kullanan bilim kurgu yazarı William Gibson'dır. Gibson, Neuromancer isimli kitabında, bilginin eloktromanyetik formda oluşturulması ile başlayıp dünyanın dört bir yanını kuşatan sistemler vasıtasıyla (telefon hatları, uydular, internet gibi) bilgiye erişimin sağlandığı sanal ortamın bütününe bu adı vermektedir.

[49] Beceni, 2004:11

[50] EPIC, *Records, Computers and the Rights of Citizens*. 31 Temmuz 1973. 9 Şubat 2010. <http://epic.org/privacy/hew1973report/>

[51] Etiket yapıştırılmış objeleri tanımlamada radyo dalgalarını kullanan bir tür otomatik tanımlama teknolojisi olan bu teknolojiler, genellikle İngilizce kısaltması olan RFID (Radio Frequency Identification) ile bilinmektedir.

[52] TÜBİTAK–UEKAE, Sabancı Üniversitesi ve TBD eşgüdümünde, 1.Türkiye "Bilişim Çağında Kişisel ve Kurumsal Mahremiyet Çalıştayı" duyurusu. 8 Kasım 2007. 4 Aralık 2008. <http://istanbul.tbd.org.tr/mmdbfiles/TBD/MahremiyetCalistayiAyrintiliBilgi.pdf >

organizasyonlar arasında sınırların aşılarak kişisel verilere erişimi de kolaylaştırmıştır.

Toplumsal olarak, konunun hassasiyetiyle ilgilenen pek çok kişi, bu durumu Orwell'in 1984 romanındaki gözetleyiciye benzeterek, romandaki Büyük Birader karakterinin canlanması ile özdeşleştirmektedir. Bireysel özgürlüklerin artma eğilimine rağmen, devletlerin, bireylerin ve kurumların teknolojik ve sosyolojik gelişmelerle birlikte artan oranda özel hayata müdahale etme arzularının çatışması neticesinde, insanoğlunun içinde bulunduğu bu dönem literatürde "gözetleme toplumu" (*surveillance society*) olarak anılmaya başlanmıştır. (Stanley and Steinhardt, 2003:1)[53]

Gözetleme, genel itibarıyla toplumsal kontrolü gerçekleştirebilmek amacıyla bireylerin veya grupların kimliklerinin saptanması ve durumlarının takibi anlamında kullanılmaktadır. Böylece modern organizasyonlar etkin karar alma, alınan kararları uygulama, kontrol ve koordinasyon sürecinde gözetleme sonucu edinilen verileri bir karar destek sistemi aracı gibi kullanma eğilimindedir.

Westin (1972:52)'e göre gözetleme araçları; *fiziksel, psikolojik* ve *veri gözetlemesi* olmak üzere üç kısımda incelenmektedir. Bunlardan ilki, kişinin bulunduğu yerin, hareketlerinin, konuşmalarının ya da özel yazışmalarının kişinin bilgisi veya rızası dışında optik ya da akustik araçlarla ele geçirilmesidir. *Fiziksel izleme* olarak nitelendirilen bu alanda genellikle gizli kamera, ortam dinleme cihazları vb. kullanılmaktadır. İkinci tip izleme ise genellikle kişinin iradesinin yazılı veya sözlü testler ya da madde kullanımı suretiyle *psikolojik* olarak ortadan kaldırılarak, kişinin istemeden özel hayatı veya kişiliği bakımından önemli hususları açığa çıkarma şeklidir. Günümüzde en yaygın olarak kullanılan ve hukuki açıdan veri koruma hukukunun ana parçasını oluşturan *veri gözetlemesi* ise, veri işleme araçları ile kişi veya gruplar hakkında bilginin toplanması, değişimi ve kullanımı olarak tanımlanmaktadır.[54] Artık günümüzde veri gözetlemesini oluşturan otomatik veri işleme yöntemleri ve bilgisayarlar neredeyse sınırları ortadan kaldıracak boyutlarda veri işleme yeteneğine sahiptir.

[53] Beceni, 2004:9
[54] TBD, 2008:15

1.5.4. Bilgi ekonomisi

Bilgi ekonomisi genel olarak bilgiye dayalı, bilgiyi temel alan bir ekonomi olarak tanımlanabilir.[55] Hammadde, emek, zaman, mekan, sermaye ve öteki girdilere olan ihtiyacı azalttığı için bilgi pek çok şeyi ikame etmekte, ileri bir ekonominin kaynağı haline gelmektedir.[56] Yazılımlar, medya, ecza malzemeleri, elektronik ticaret, banka hizmetleri vs. bilgi ekonomisi ürün ve hizmetleridir. Bu ürünler her ne kadar fonksiyonları ve teknolojileri itibarıyla değişiklik gösterse de, bunların üretimlerindeki ortak nokta görece olarak yüksek fikri bilgi gerektirmesi ve işgücü ve sermaye bakımından geleneksel üretim faktörlerine daha az ihtiyaç duymalarıdır. Bununla birlikte, gıda, tekstil, turizm gibi geleneksel sektörlerdeki üretim ve pazarlama araçları da giderek daha yoğun bilgi içermeye başlamıştır.[57]

Bilgi ekonomisinde genel olarak teknolojik gelişmeler[58]; özelde ise, BİT ve beraberinde İnternet sürükleyici bir rol oynamaktadır. Bu süreçte, ekonomiler mal, hizmet, yatırım, insanlar ve fikirlerin uluslararası ortamda kolayca hareket etmesiyle dünya ekonomisine gittikçe entegre olmaktadır. Böylece bu süreç, firmalar arasında yeni rekabet ve işbirliği alanlarını artırırken, yeni fikir ve teknolojilerin yayılmasını da teşvik etmektedir.[59] ABD, İrlanda, Finlandiya gibi gelişmiş ülkeler bilgi ekonomisine geçmiş olup, bu ülkelerin üretim ve rekabet düzeyleri, yeni iş olanakları artmış ve böylece uzun vadede vatandaşlarının refah düzeylerini iyileştirici adımlar atılmıştır.[60]

Bilgi ekonomisinde, ekonomide; hangi malların ne miktarda üretileceğine karar vermek üretici firmalardan, bilgiye sahip olan dağıtıcı firma ve kuruluşlara geçmiştir.[61] Bütün gelişmiş ülkeler, gayri safı milli hasılalarının yaklaşık beşte birini

---

[55] Yıldırım, Süreyya. "Bilgi Ekonomisi ve Bilgi Ekonomisinin Türkiye Açısından Değerlendirilmesi". *Sosyal Bilimler Dergisi.* s.109. Erişim: 31 Mayıs 2010. http://sbe.balikesir.edu.tr/dergi/edergi/c7s12/makale/c7s12m6.pdf.
[56] Toffler, 1996:40
[57] The World Bank, 2004:4
[58] Burada, teknolojik gelişmeler kavramıyla yeni ürünler üretilmesi anlamında *ürün yeniliği*, yeni üretim süreçleri anlamında *süreç yeniliği* ve üretim birimlerinin örgütlenmesinde yenilik anlamında *organizasyonel yenilik* kavramlarının bütünü kastedilmektedir.
[59] Kelleci, 2003:2
[60] The World Bank, 2004:13
[61] Drucker, 1995:156

bilginin üretimine veya dağıtımına harcamaktadırlar.[62] Dolayısıyla, artık bilgi sahibi firmalar ekonomide söz sahibi olmaya başlamıştır.

Bilgi ekonomisinde yaygınlaşan BİT kullanımı, firmaların ağ üzerinden haberleşme kapasitelerini nitelikli bir seviyeye yükseltmiştir. Bilginin özellikle küresel ağ olan İnternet üzerinden transferi neticesinde, transfer edilen bu bilgiler BİT aracılığıyla işlenmekte ve anlamlı yeni bilgi setleri oluşturulmaktadır. Bu dönüşüm, bilgi ekonomisi içinde bir katma değer yaratmaktadır. Kişisel veriler de bu dönüşümde üretimin belirleyicilerinden biri olmaya başlamıştır. Zira, müşterilerin kişisel tercihleri, üretimin talep boyutunun nitelik kazanmasına ve arzın şekillenmesine büyük bir katkı yapmaktadır. Artık firmalar, kişisel verilerin işlenmiş türevlerinden, neyi ne zaman, hangi kitle için ve ne kadar üreteceklerini optimal düzeyde belirleyebilmektedir.

Bilgi ekonomisinin hukuki çerçevesi içinde elektronik imza, elektronik haberleşme, fikri mülkiyet hakları ile veri koruma ve mahremiyet ön plana çıkmaktadır.[63] Bu çalışmada bilgi ekonomisine geçiş sürecinin sağlıklı gelişiminde gerekli olan hukuki başlıklardan kişisel verileri korunması ve mahremiyet konuları incelenmektedir.

1.5.5. Bilgi güvenliği

Bilgi güvenliği, bir bilginin yetkisiz kişilerce ele geçirilmesini, yetkisiz kişilerce değiştirilmesini engelleme ve bilgiye yetkili kişilerin istenilen zamanda ve istenilen kalitede erişmesini sağlama anlamına gelmektedir.[64] Kaza veya kasta dayalı güvenlik risklerine karşı bir ağın ya da bilgi sisteminin karşı koyabilme kapasitesi, kişisel verilerin korunması ile sıkı sıkıya ilişkilidir. Zira kişisel veriler, devletlerin geliştirdikleri bilgi güvenliği strateji ve politikaları içinde korunması gerekli görülen en önemli bilgilerdendir.

---

[62] Drucker, 1993:259
[63] Vere, 2009:7
[64] "Bilgiçağı" dergisi, Hayrettin Bahşi ile röportaj. "Kolaylık, Güvenlik Riskini de Getiriyor". Kasım 2008. s.12.

Avrupa'da e-devlet uygulamasına geçen öncü ülkelerden olan Estonya'nın 2007 yılı Nisan ayında maruz kaldığı ve on üç gün süren siber saldırı[65], bilgi güvenliğini, günümüz sanal ortam savaşlarının engellenmesinde, dikkate alınması gereken konular içinde önemli bir yere taşımıştır. Estonya'ya yönelik saldırılarda, Estonya Hükümetine AB ile birlikte yardım amaçlı uzman tahsis eden NATO sözcüsü, bu saldırıyı normal bir savaştan ayıran tek farkın, tanklarla ve ağır silahlarla yapılmamış olması şeklinde ifade etmiştir.

İlerleyen dönemlerde, özellikle soğuk savaşın yaşandığı ülkeler arasında meydana gelmesi muhtemel görülen siber saldırılar ve güvenlik krizleri için bilgi sistemlerinin güvenliğinin öneminin farkına varan ülkeler çeşitli bilgi güvenliği tedbirleri almaya, stratejiler geliştirmeye başlamışlardır. AB ülkelerine ve doğrudan Avrupa Konseyi'ne danışmanlık faaliyetinde bulunan Avrupa Ağ ve Bilgi Güvenliği Ajansı (ENISA) bu tür güvenlik krizlerini çözmek ve tüketici güvenini kazanmak için kurulmuş bir kurum olarak 2004 yılından bu yana faaliyetlerde bulunmaktadır.

Ağ ve bilgi güvenliği konusu, pratikte siber suç, kişisel veri koruma yasaları ve telekomünikasyon alanında yapılan düzenlemelerle iç içe geçmiş durumda olduğundan, bu konuya ilişkin alınacak politika tedbirlerinin de mevcut telekomünikasyon, veri koruma ve siber suç politikalarından bağımsız düşünülmemesi gerekmektedir.

Dünyadaki mahremiyet ve veri koruma kanunlarında da ağ ve bilgi güvenliğine ilişkin hükümler bulunabilmektedir. Bu hükümler genellikle kişisel veri kontrolörü[66] veya işleyicisi olan kurum ve kuruluşların uymaları gereken yükümlülükleri belirtmektedir. Bu yükümlülüklere örnek olarak; ilgili kurum ve kuruluş içindeki birimlerin hangi verileri nasıl kullanacakları konusunun açıkça belirlenmesi, verilerin kullanılabilmesi için gereken talimatların açık ve net olması,

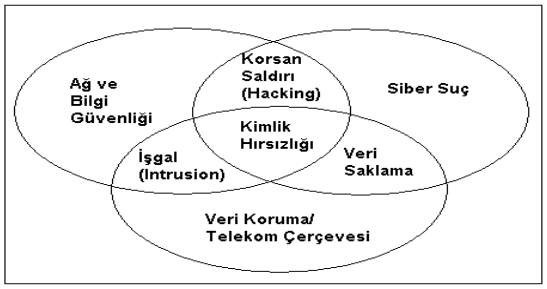
[65] Estonya'ya yönelik olarak gerçekleştirilen siber saldırıya sebep olarak, saldırının gerçekleşmesinden kısa bir süre önce Estonya ve Rusya arasında Bronz Asker Heykeli'nin sökülmesi ile başlayan gerginlik gösterilmektedir. Bu olaydan kısa bir süre sonra, Estonya'nın birçok önemli kuruluşunun bilgisayarlarına Rus bilgisayar korsanları tarafından saldırılmıştır. Estonya'ya yönelik düzenlenen bu saldırı, bir devlet tarafından bir başka ülkenin bilgisayar sistemlerine karşı siber ortamda yapılmış "ilk siber saldırı" ve "21. yüzyılın savaşı" olarak kayıtlara geçmiştir. Benzer şekilde, İsrail-Hamas mücadelesi de sanal ortama yansımış, İsrail'in önde gelen internet sitelerinden "Ynet" haber sitesi hacklenmiştir.

[66] Veri kontrolörünün tanımı, bu çalışmanın 3'üncü bölümündeki "Veri Koruma Direktifindeki temel kavramlar" kısmında yapılmıştır.

veri işleyenlerin veri koruma ve bilgi güvenliği kanunları hakkında bilgilendirilmeleri, bu kişilerin görev ve yetkilerinin düzenlenmesi ile veri işlemelerinin kaydının en fazla tutulacağı sürenin belirtilmesi sayılabilir.

AB Komisyonunun 2001 yılında Konsey'e yönelik bildirisinde bu durum, aşağıdaki şema ile izah edilmeye çalışılmış ve bu üç politika alanının nasıl bir ilişki içinde oldukları örneklendirilmiştir.

Şekil 1. 1. Bilgi Güvenliği Politika Alanları ve Etkileşim



Kaynak: Commission of the European Communities, COM (2001) 298 final, s. 3, <http://www.justice.gov/criminal/cybercrime/intl/netsec_comm.pdf>.

Bir veritabanında korunması gereken veriler değişik öncelik ve gruplara göre tasnif edilebilir. Bilgi güvenliğinin sağlanmasında teknik araçlar ve teknolojik güvenlik çözümlerinden genellikle virüsleri yok etme, ağ problemlerini giderme, yetkisiz kullanıcıların erişim yetkisini sınırlandırma yöntemleri kullanılmaktadır. Kişisel verilerin korunması hukuku ise, kişiye ait verilerin mümkün olduğunca teknik araçlarla korunması ile bu bilgilerin istenmeyen şekillerde kullanılmasının önüne geçecek hukuki ve sosyal tedbirlerin alınmasını ve nihayet bireyin kendisine ait verilerin kullanılması sürecinde söz sahibi olmasını hedeflemektedir. Kişisel verilerin kötüye kullanılması da genellikle bir bilgi güvenliği sorunudur. Eğer bir sistemde kişisel veri yoksa, sadece bilgi güvenliği önemli hale gelecektir.

Bilgi güvenliği kavramı, Kasım 2005 tarihinde Litvanya'nın Vilnius kentinde düzenlenen "Birinci Avrupa Bilgi ve Ağ Güvenliği Konferansı"nda[67] da "ağ ve bilgi güvenliği" ve "yenilikçi teknolojik çözümler" olmak üzere iki bölümde ele alınmıştır. Bunlardan kişisel veri hırsızlığı araçları, virüs ve truva atı gibi kötü niyetli

[67] Konferansa ilişkin ayrıntılı notlar için bkz. "Security Conference Held in Lithuania". <http://www.ebaltics.com/doc_upl/Korsakaite.pdf?PHPSESSID=184c660b4f48066e05317338f777dd75>

yazılımlar[68], istenmeyen ileti (spam) ve dağıtık olarak hizmet çökertme saldırıları (DDoS attack)[69] en bilinen ve sık rastlanan ağ ve bilgi güvenliği riskleridir. Bu risklerin kullanıcılar üzerinde en büyük etkisi, sanal ortamda mahremiyet, veri ve para kaybı olmaktadır. Ağ ve bilgi güvenliği sorunları, geleceğin, mobil ağ ve hizmetlerinin en önemli problemleri arasında gösterilmektedir.Vilnius'ta yapılan bu Konferans'ta, ağ ve bilgi güvenliği vak'alarının sayısını azaltmada farkındalığın artırılması, yasal ve teknik koruma araçlarının kullanılması ve iyi bir işbirliği etkili yöntemler arasında sayılmaktadır. Bu Konferansta yenilikçi teknolojik çözümler yoluyla bilgi güvenliğinin ve dolayısıyla İnternet güvenliğinin sağlanması da ele alınan bir diğer konudur. Yenilikçi teknolojik çözümler, saldırıya karşı tepki vermekten ziyade, ağ ve bilgi güvenliği vak'alarının önlenmesi esasına dayanmaktadır. Bu nedenle bu teknolojilere akıllı teknolojiler de denilmektedir. Akıllı teknolojilerin iyi tanımlanmış iş, hizmet ve ağ kurtarma planları çerçevesinde, zararların en az seviyeye çekilerek kullanılmasıyla sistemlerin istikrarı ve güvenliği temin edilmiş olacaktır.

[68] "Malware" kavramı bu çalışmada, "kötü niyetli yazılım" olarak Türkçe'ye çevrilmiştir.

[69] Herhangi bir sitenin normal ziyaretçilerine veya sanal müşterilerine geçici bile olsa hizmet verememesini sağlamak üzere, failin, yakalanmamak ve iz bırakmamak için "zombi" denilen aracı bilgisayarlar kullandığı saldırılara DoS saldırılaradı verilmektedir. Fail böylece kendi kimliğini ve IP adresini/numarasını gizlemiş olur. Bu şekilde birçok zombinin aynı anda saldırması ile yapılan DoS ataklarına Dağıtık DoS (DDoS) saldırı denilmektedir. Ayrıntılı bilgi için bkz. "Zavallı Savunmasız İnternet-DoS Atakları". Albert Levi. <http://www.teknoturk.org/docking/yazilar/tt000002-yazi.htm>

2. KİŞİSEL VERİLERİN TİCARİ DEĞERİ VE SİBER SUÇLAR

2.1. Genel Çerçeve

Dünyanın küresel bir köy olarak nitelendirildiği 21'inci yüzyılda, fiziki sınırlar daha belirsiz bir hal almış, para ve sermayenin dolaşımı eskisi kadar kolay kontrol edilebilir olmaktan çıkmıştır. BİT'teki gelişmeler, insan refahına olumlu katkılar sağlamışsa da, suç olgusu ve suçluların izlediği yöntemlerde de bir dizi değişimin yaşanmasına sebep olmuştur. Elektronik ortam, yeni suç türlerinin işlendiği bir alan haline gelmiştir. Bu nedenle bu bölümde kimlik hırsızlığı, banka hesapları ve aboneliklerin kötüye kullanılması ve diğer sahtecilik suçları gibi kişisel verilerin kötüye kullanılması suretiyle işlenen çeşitli suç tipleri ve kişisel verilerin ticari değeri incelenmektedir.

Günümüz ekonomik sisteminde, "veri" ya da "bilgi", mal ve hizmet üretim faktörlerinden birisi olarak algılanmaktadır. İnternetin küreselleşmenin hızlanmasına olan katkısı, rekabetin artması, kar marjlarının düşmesi ve müşteri memnuniyetinin daha önemli hale gelmesi nedenleriyle yanlış karar almak istemeyen karar mercileri, mümkün olduğunca fazla veriyi depolamak istemektedirler. Kişisel bilgilerin daha ziyade sayısal ortam kullanılarak depolanması ve işlenmesi ise bu verilerin kötüye kullanılma riskini artırmaktadır.

Kişisel verilerin türlü şekillerde kötüye kullanılması salt teknolojinin sonucu değildir. Bilgisayarlar ve İnternetin ağ etkisi, mahremiyetin ihlalinde ve kişilere ait veriler kullanılarak suç işlenmesinde hızlandıran etkiye sahiptir. Biometrik karakterlerle tanımlama yapılmasını sağlayan teknolojiler, DNA bankaları, gözetim araçlarındaki artış, sokakları bile gözlemleyen kameralar, veri madenciliği, RFID vb. araçlar bu bilgilerin manipülasyonu ve kötüye kullanılması risklerini de beraberinde getirmiştir. Günümüzde yaygın olarak kullanılan sosyal paylaşım siteleri kişisel verilerin elektronik ortam kullanılmak suretiyle tutulmasını sağlayarak, küresel ölçekte kişilerin iletişimini kolaylaştıran bir hizmet olmakla beraber, büyük bir iktisadi faaliyetin de kaynağı durumundadır. Bu sosyal siteler, barındırdıkları kişisel verilerin çalındığı, satıldığı, fotoğrafların kötüye kullanıldığı, yani kişiye ait bilgilerin kontrol edilemez olduğu bir ortam halini almaya başlamıştır. Bu ve benzer

ortamlarda kişisel verilere ve dolayısıyla kişiliğe yönelik saldırıların cezalandırılabilmesi ve kişi hak ve özgürlüğünün korunması için hukuk düzeninin söz konusu kötüye kullanmaları tanıması gerekmektedir. Kanunsuz suç ve ceza olmaz prensibi nedeniyle etkin bir suç ve ceza sisteminin öngörülmemesi halinde mağduriyetler giderek artacaktır.

Kişisel veriler, yukarıda ifade edildiği gibi, elektronik ortamda suç işlenmesinin önemli araçlarından biri haline gelmiştir.

2.2. Siber Suçlar

Türk yazınında kavramsal olarak henüz görüş birliğine varılamayan ve "bilgisayar suçları", "internet suçları", "siber suç" veya "bilişim suçları" olarak adlandırılan suçlar için, Dünya'daki tek düzenleme olan Avrupa Konseyi Siber Suç Sözleşmesi'nin adına uygun olması ve uluslararası hukukta yaygın olarak kullanılması nedeniyle bu çalışmada kavramsal olarak "siber suç" ifadesi tercih edilmiştir.[70]

Siber suç, bir bilgisayar, ağ veya donanım cihazı kullanılmak suretiyle, elektronik ortamda hukuka aykırı olarak gerçekleştirilen her tür fiil olarak tanımlanabilir.

1980'li yıllardan sonra bilgisayar ve İnternet kullanımının yaygınlaşması ile birlikte, siber suçların sadece ekonomik boyutlarının olmadığı ve bu tür suçların en az ekonomi kadar önemli, diğer bazı değerler aleyhine de işlenebileceği anlaşılmıştır. Bunun sonucu olarak da bu suçların ayrı bir disiplin altında incelenmesi gereği ortaya çıkmıştır.[71]

Bir kişiye ait isim, adres, telefon veya sosyal güvenlik numarası veya aile hayatına ilişkin kişisel veriler çoğu kez veri sahibinin bilgisi ve isteği dışında yayılabilmektedir. Böyle durumlarda, bilgilerin milyonlarca sayıda iletilmesi ya da çoğaltılması saniyelerle ifade edilmektedir. Klasik ceza hukukunda suç aracı olan herhangi bir vasıta gibi kişisel verilerin de, üçüncü kişilerin tasarrufuna girdiği anda suç aracı olarak kullanılma riski doğmuş olmaktadır. Klasik suça göre daha hızlı ve

[70] Turhan, 2006:28
[71] A.g.e., s.28

kolay işlenebilen siber suçun tespit edilmesi ve bu suç tespit edilse bile failin yakalanması her zaman mümkün olamamaktadır.

Siber suçları, geleneksel anlamdaki suçlardan ayıran özelliklerden en önemlisi, bu suçların işleniş şekillerinin (modus operandi) tespitinin zorluğudur. Söz konusu suçlar, yepyeni ve çok farklı yollarla işlenebilmektedirler.[72] Çoğu kez ilk etapta kişisel verilerin çalınması, ikinci etapta ise bu verilerin kullanılması suretiyle suç işlendiğinden siber suçlar genellikle zincirleme şekilde gelişmektedir. Kişisel verilerin elde edilmesi için işlenen hırsızlık suçu sanal veya fiziki ortamda gerçekleşebilmektedir.

Çalışmanın bu bölümünde kişisel verileri elde etmek için kullanılan yöntemler ve bazı siber suç türleri ile siber suçların ticari değeri incelenmektedir.

2.3. Kişisel Verileri Edinme Yöntemleri ve Siber Suç Türleri

2.3.1. Kimlik hırsızlığı

Kimlik hırsızlığı, gerçek veya tüzel kişilere ait kişisel bilgilerin yetkisiz kişilerce, dolandırıcılık veya diğer suçların işlenmesinde kullanılmak üzere ele geçirilmesi, iletilmesi (transferi), muhafaza edilmesi veya kullanılması olarak tanımlanabilir.[73] Son yıllarda sıkça rastlanmaya başlayan veri kayıpları, dikkatleri kamu ve özel sektörde teknolojik gelişmelerle artan kimlik hırsızlığı ve kişisel verilerin korunması kavramına çevirmiştir. Kimlik hırsızlığı konusunda farkındalık arttıkça, şüphesiz tüketicilerin de kişisel bilgilerini paylaşırken tereddütleri artmaktadır. Avrupa Komisyonu, bu nedenle Veri Koruma Direktifini yeniden gözden geçirme çalışmalarını başlattığını açıklamıştır.

Kimlik hırsızlığı, klasik veya çevrimiçi olmak üzere iki farklı ortamda işlenebilmektedir.

2.3.1.1. Klasik (off-line) kimlik hırsızlığı

Kimlik hırsızları veri elde etmek için her tür yola başvurmaktadırlar. Bu yollardan biri de insanlar arasındaki iletişim ve insan davranışındaki açıklardan

[72] Turhan, 2006:47
[73] OECD, "OECD Policy Guidance on Online Identity Theft". Haziran 2008

faydalanarak güvenlik süreçlerini atlatma olarak adlandırılan *sosyal mühendisliktir*. Bu kavram, kişileri gizli bilgilerini vermeleri için aldatmak olarak da tanımlanabilir. Etkileme, zorlama, aldatıcı ilişkiler geliştirme, sosyal mühendislik saldırı araçlarındandır. Kimlik hırsızlığında bu yöntemler sıkça kullanılmaktadır.

Klasik kimlik hırsızlığı yöntemleri:

i-Çöp karıştırma (dumpster diving): Çöpe atılmış her tür çek yaprağı, kredi kartı, banka sözleşmesi, fatura veya kişisel veri içeren ve elektronik ya da diğer araçlarda yer alan kayıtları elde etmek için bu kayıtları incelemeye çöp karıştırma denilmektedir. Hırsızlar bu iş için çöp toplayıcılarla menfaat karşılığı işbirliği yapmaktadır. ABD'de bu konuda hazırlanmış 1997 tarihli bir Kanun bulunmaktadır.[74]

ii-Bahane yaratma (pretexting): Bir banka, telefon şirketi veya diğer bir bilgi kaynağını arayarak, belli bir müşteri gibi davranıp herhangi bir şifre ya da başka bir bilgiyi elde etmek için kullanılan sosyal mühendislik yöntemidir.

iii- Omuz üstünden seyir (shoulder surfing): ATM cihazı veya diğer şifre girilen ekranları gizlice izleyerek şifre çalma yöntemidir.

iv-Tarama (Skimming): Kredi kartlarının arkasındaki manyetik verileri elde ederek sahte kartlara ekleme şeklinde yapılmaktadır.

v- İş kayıtları hırsızlığı: İşyerlerindeki bilgisayar veya dosyaların çalınması veya bu bilgilerin elde edilmesidir. Bu hırsızlık yönteminde, çalışanlara rüşvet vs. menfaat sağlayarak bilgi edinilebilmektedir.

2.3.1.2. Çevrimiçi (on-line) kimlik hırsızlığı

Çevrimiçi ortamda kullanılan kimlik hırsızlığı yöntemleri, belirli sayıyla sınırlı değildir. Zira bu yöntemler günden güne değişebilmektedir. Bu çalışmada örnekleyici olmak üzere çeşitli çevrimiçi kimlik hırsızlığı yöntemleri hakkında bilgi verilmektedir. Suç unsuru taşıyan yöntemlerle elde edilen bu veriler, elde edildikten

[74] Bkz. "An Act Concerning Dumpster Diving". June 6, 1997. 5 Ocak 2011.
< http://www.cga.ct.gov/ps97/Act/pa/1997PA-00110-R00HB-07030-PA.htm>

sonra başka suçların işlenmesinde de kullanılabilmektedir. Bu tür kimlik hırsızlığı, e-ticaret faaliyetleri sırasında tüketicilerin güvenlerinin sarsılmasına neden olmaktadır.

Günümüzde, çevrimiçi ortamda kişisel verileri elde etmek için;

i. Kötü niyetli yazılım veya programlar (malware)

ii. Aldatıcı nitelikte e-posta veya İnternet siteleri

iii. Sistem veya yazılımların açıkları (hacking) kullanılmaktadır.

2.3.1.2.1. Kötü niyetli yazılım veya programlar (malware)

Yaygın olarak virüs, truva atı, bukalemun, çerezler olarak karşılaşılan kimlik hırsızlığı yöntemlerinden cep telefonu, sabit telefon veya bilgisayarlara yüklenen yazılım veya programlar aşağıda incelenmektedir.

i) Virüsler:

Çalıştırılabilen bir programa kendisini ekleyerek veya bir kopyasını oluşturarak çoğalan ve bilgisayarın belleğine yerleşen gizli yazılım programıdır.

ii) Truva atı:

Yararlı ve yasal gibi görünen, ancak bilgisayarları uzaktan yönetmek için arka kapı açan programlardır. Bu programla bilgisayar korsanları, sistemin yapılanmasını değiştirebilir, kullanıcının şifre gibi hassas verileri ile diğer kişisel verilerine ulaşabilirler. Tipik truva programlarından olan bot'lar ise bir haberleşme kanalı aracılığıyla yerleştirildiği makineyi yetkisiz kişilerin kontrol etmesini sağlayabilmektedir.

iii) Bukalemun:

Çok kullanıcılı sistemlerde kullanıcı adları ve şifrelerini taklit yeteneği sayesinde kendisini gizli bir dosyaya kaydedebilen ve normal bir program gibi çalışan "bukalemun", sistemin bakım için bir süre kapatılacağına ilişkin bir uyarı verir. Bu sırada bukalemun programını yöneten kişi, bu gizli dosyaya ulaşarak kullanıcı adları ve şifrelerini ele geçirir.[75]

[75] Turhan, 2006:50

iv) Çerezler (Cookies):

İnternet kullanıcısının sabit diskinde bulunan ve kullanıcı her İnternete bağlandığında hangi siteleri dolaştığını kayıt altına alan, bu bilgileri kullanıcının sabit diskine yerleştiren metin dosyalarıdır. Bu araç, iyi niyetli olarak kullanılabileceği gibi, özellikle hukuka ve ahlaka aykırı yayın yapan İnternet siteleri tarafından bireylere şantaj ve baskı yapılması için de kullanılabilir. Bu yönüyle çerezler, mahremiyetin ihlalinde tehlikeli bir araç olarak kabul edilebilir. Ancak; çoğu kez çerezlerde tutulan bilgiler kişisel verilerin korunmasına zarar verici nitelikte değildir. Çerezler ile genellikle belirli bir kullanıcının belirli bir siteyi ne sıklıkta ziyaret ettiği izlenebilir. Bununla birlikte çerezlerdeki bilgi ile, sitenin tekrar kullanılması nedeniyle kullanıcıya teşekkür de edilebilmektedir. Bir bilgisayarın farklı kişilerce kullanılabileceği ofis ortamlarında bu bilgiler tanımlayıcı olarak kullanılabilir. e-Ticaret faaliyetleri için çerezlerin faydalı bir araç olduğu da söylenebilir.

2.3.1.2.2. Aldatıcı e-postalar ve İnternet siteleri

i) Oltalama (Phishing):

İngilizce "Balık tutma" anlamına gelen "Fishing" sözcüğündeki "f" harfinin yerine "ph" harflerinin konulmasıyla türetilen terim, oltayı attığınız zaman en azından bir balık yakalayabileceğiniz düşüncesinden esinlenilerek oluşturulmuştur.[76]

Phishing, bir işletme, banka ya da devlet kurumundan geliyormuş izlenimi yaratılan bir e-posta ya da aslını kopya eden bir İnternet sitesi (mirror web site) aracılığıyla, kişilere ait kredi kartı bilgisi, şifre, diğer hesap bilgileri vb. çalmayı amaçlayan bir İnternet dolandırıcılığıdır. Oltalama saldırılarının 2007'de ABD'de tüketici ve işletmelere maliyetinin 2,1 milyar dolar olduğu tahmin edilmektedir.[77]

İnternet kullanıcılarının, bu sahte e-posta ya da kopyalanmış İnternet sitelerini gerçek zannederek söz konusu kişilerin istedikleri bilgileri onlara vermeleri halinde bilgileri çalınmış olur. Bu şekilde gönderilen e-postalara kesinlikle itibar edilmemelidir.

[76] Turhan, 2006:57
[77] Symantec, 2008:9

ii) İstenmeyen elektronik posta (spam):

Genellikle zararlı bir içeriğe sahip olan ve istenmeyen, alıcıya iradesi dışında gönderilen elektronik mesajlardır. Bu mesajlar, BİT'in gelişimine ve yayılımına paralel olarak tüm dünyada giderek büyüyen sorunların başında gelmektedir. İstenmeyen elektronik posta, yukarıda açıklanan kötü niyetli yazılım veya programlar aracılığıyla (malware) bilgi hırsızlığında ve oltalama faaliyetlerinde sıkça kullanılan bir araç haline gelmiştir. Amerika'nın önde gelen şirketlerinden olan World'ün Genel Müdürü Barry Shein, New York Times'a verdiği bir röportajında, istenmeyen elektronik posta için İnternet'in yarattığı organize suç nitelemesini kullanmaktadır.[78]

Rekabet Kurulu'nun 06.08.2009 tarihli ve 09-35/880-208 sayılı Kararına[79] esas Bilgi Teknolojileri ve İletişim Kurumu (BTK) görüşüne göre, yapılan araştırmalar Türkiye'nin en çok istenmeyen elektronik posta yayan ülkelerden biri olduğunu göstermektedir.

2.3.1.2.3. Sistem veya yazılımların açıklarından faydalanmak (hacking)

"Korsan saldırı" olarak da Türkçe'ye çevrilebilecek "hacking" kavramı, elektronik sistemler veya bilgisayar açıklarından yararlanmak suretiyle kişisel verileri çalmak için kullanılan en yaygın yöntemlerden biridir. İzinsiz ve hukuka aykırı bir şekilde kişisel verilerin çalınmasını sağlayan bir diğer yöntem de kırma (cracking)[80] yöntemidir. Kişisel veri elde etmenin yanısıra, sistemin ücretsiz kullanılmasını da sağlayan bu yöntemler, bilgisayar korsanlarını (hacker) bilgisayarla ilgili sahtecilik gibi daha tehlikeli suçlara teşvik edebilir.[81]

[78] The New York Times. "Tangled Up in Spam". February 9 2003. 11 Şubat 2010. <http://www.nytimes.com/2003/02/09/magazine/09SPAM.html?pagewanted=1>
[79] İlgili Karar için bkz. <http://www.rekabet.gov.tr/dosyalar/kararlar/karar3152.pdf>
[80] Cracking (kırma) suçu, hacking'den daha tehlikeli olup, kırıcılar teknik bilgi bakımından bilgisayar korsanlarına (hacker) göre daha ileri seviyededirler. Hacking'de, bir sistemin güvenlik duvarı aşılarak sisteme girilmekte, cracking'de ise güvenlik duvarı kırılmakta, bu suretle sisteme zarar verilmektedir. Kırmak suretiyle elde edilen verilere ciddi zararlar verilebilmekte, şifre kırma dahil olmak üzere elde edilen veriler dağıtılabilmektedir.
[81] Turhan, 2006:104

2.3.2. Kişisel verilerin suistimali

Ticari ya da meslek sırları, ya da diğer değerli kişisel bilgilerin kişinin kendisine veya bir başkasına menfaat sağlamak ya da zarar vermek amacıyla kullanılması, satılması ve dağıtılmasına *kişisel verilerin suistimali* denilmektedir. Banka, hastane, alışveriş merkezleri, devlet kurumları gibi kuruluşlarda tutulan büyük miktardaki kişisel bilgilerin ticari değeri ile ilgili suistimaller önemli siber suçların işlenmesinde basamak görevi görürler.

2.3.3. İletişimin gözetlenmesi ve denetlenmesi

Ulusal güvenliğin sağlanması, suçun önceden tespit edilebilmesi ve yargılama esnasında delil olarak kullanılabilmesi amacıyla kovuşturma organları tarafından genellikle gizli izleme sistemleri kullanılmaktadır. İletişimin bu şekilde gözetlenmesi ve denetlenmesi, ilgili hukuki usul ve esaslara ve zorunluluk unsuruna uygun olarak yapılmalı ve elde edilen veriler gerekirse anonimleştirilmelidir.

İletişimin gözetlenmesi ve denetlenmesi uluslararası alanda da başta istihbarat olmak üzere çeşitli nedenlerle yapılabilmektedir. Bütün dünya üzerindeki uydu tabanlı iletişimi izleyen beş devletin[82] gizli servislerinin ortaklaşa kurdukları ECHELON sistemi (Büyük Kulak) telefon görüşmeleri, faks, telsiz, İnternet, elektronik posta trafiği dahil olmak üzere tüm iletişim araçlarını dünya çapında dinleme ve kaydetme kapasitesine sahip bir sistemdir. Sistem sayesinde elde edilen ham veriler özel bir mekanizma sayesinde çözümlenmekte ve iletişimin içeriği bu şekilde öğrenilmektedir. Temel amacı ulusal güvenliği sağlamak olmasına rağmen ticari ve diğer sırların, sistem içinde yer alan devletler tarafından haksız olarak kullanıldığı ve diğer devletlere ait stratejik bilgilerin de elde edildiği bilinmektedir. ECHELON sisteminin dünya İnternet trafiğinin yüzde 90'ını kontrol ettiği de verilen istatistikler arasındadır. [83]

Günümüzde, istasyonlar, parklar, kamusal yollar, caddeler gibi herkesin ulaşabileceği kamusal alanlarda optik ve elektronik donanımlar vasıtasıyla gözetleme yapılabilmektedir. Bu alanların video ile gözetlenmesi bütün yurttaşların temel

[82] Bu beş devlet ABD, İngiltere, Kanada, Avustralya ve Yeni Zelanda'dır.
[83] Beceni, 2004:14

haklarını ilgilendirdiğinden sıkı hukuksal koşullara bağlanması gerekmektedir.[84] En azından vatandaşlar, ortamda görüntülerin kamera ile kayıt altına alındığı konusunda bilgilendirilmelidir. Lüksemburg'ta Avrupa Komisyonu'nun Jean Monnet binasında kişilerin görebileceği şekilde yapılan bilgilendirme buna örnek olarak verilebilir. Kolay görülebilen bir levha ile yapılan bilgilendirmede, binada bulunan kameraların kaydettiği kişisel verilerin yalnızca Avrupa Komisyonu'nun 2001/45 sayılı Tüzüğü uyarınca işlenebileceği ve bunun dışında kullanılmayacağı, bu verilerin sadece 30 günlük süre için saklanacağı ve gerekiyorsa suçların soruşturulması ve kovuşturulmasına ilişkin olarak adli mercilere iletilebileceği bilgisi verilmektedir. Böylece elde edilen verilerin bu amaçların dışında kullanılamayacağı güvencesi verilmektedir.

2.3.4. Veri madenciliği (data mining)

Veri madenciliği, veri yığınları arasından istatistik ve matematik teknikleri kullanılarak verilerdeki gizli örüntüleri çözmeye yarayan, fark edilmesi güç ilişkileri açığa çıkaran, ileriye yönelik tahminler yapılmasını sağlayan ve bu alanda kurallar üreten veri tabanı teknolojisi ve tekniklerinin uygulamasını ifade etmektedir.[85] Kısaca veri madenciliği, veri tabanlarından elde edilen bilgiyi yapılandırarak, bilgi keşfedilmesini sağlayan araçlar ve teknikler olarak nitelendirilebilir.

Günümüzde kurumlara ait veritabanlarında milyonlarca kişiye ait bilgi depolanmaktadır. Bu verilerle birtakım analizlerin otomatikleştirilmiş sistemler vasıtasıyla yapılması gerekliliği, veriye erişimi, en az verinin kendisi kadar önemli hale getirmiş ve veri madenciliği uygulamaları gündeme gelmiştir.

Veri madenciliği iyi niyetlerle kullanılabileceği gibi, kişisel verilerin elde edilerek çeşitli şekillerde kötüye kullanılmasına da sebep olabilmektedir.

2.3.5. Sahte kişilik oluşturma ve kişilik taklidi

Kişilik taklidi, gerçek kişilere ait bilgilerin kullanılarak suç işlenmesi ve o kişinin bu suçun faili durumuna düşmesi ile sonuçlanan eylemdir. Kredi kartı numara

[84] Şimşek, 2008:162,163'ten faydalanılmıştır.
[85] Bağcı, Hasan. "Yolsuzluklarla Mücadelede Veri Madenciliği". <http://www.alomaliye.com/2009/hasan_bagci_yolsuzlukla.htm>

oluşturucu programlar gibi araçlar kullanılarak elde edilecek gerçek bilgiler, bazen de hayali kişiler oluşturulmasında kullanılmakta, böylece haksız menfaat sağlanarak kişilere zarar verilmektedir.

Elektronik posta (e-posta) şifrelerinin elde edilmesiyle başka kişilerin hesaplarına girilebilmekte, girilen bu adreslerle istenmeyen e-posta (spam) gönderilebildiği gibi, kişinin iletişim listesindeki kişi adresleri de bu yetkisiz kişilerin yeni e-posta adreslerine erişebilmesine yardımcı olmaktadır. Söz konusu şifrelerin edinilmesiyle banka hesap verisi, okul bilgileri ve sağlık gibi hassas kişisel verilere de ulaşılabilir. Şöyle ki, kişinin e-posta hesabıyla üye olduğu sayfalardan şifre yenileme seçeneği kullanılarak e-postaya gönderilecek yeni şifre aracılığıyla tüm bu hesaplara erişmek mümkündür. Bir kişinin aynı şifreyle birden fazla hesabının olması, bu tehlikeyi artırmaktadır.

2.3.6. Sahte internet sitesi (Pharming)

Türkçe'de bilinen bir karşılığı olmayan pharming ifadesi "sahte İnternet sitesi" olarak kullanılabilir. Sanal dünyanın dolandırıcıları tarafından tasarlanan ve bir İnternet sitesinin çevrimiçi hesap ödeme sayfasıymış gibi görünen sahte İnternet sayfası ile kişilerin bilgilerinin çalınmasına "pharming" denilmektedir. Ödemeye ilişkin kısayolun tıklanması ile dolandırıcılar tarafından hazırlanan bu sahte sayfaya ulaşılmakta, daha sonra finansal bilgilerin sisteme girilmesi talep edilmektedir.

Sahte internet sitelerinin kurbanı olmamanın yolları arasında kapsamlı ve güncel bir İnternet güvenliği yazılımı kullanmak ve alışveriş yapılacak çevrimiçi mağazanın İnternet adresine kısayolları tıklayarak değil, bu adresleri İnternet tarayıcısına yazarak ulaşmak gösterilebilir.

2.3.7. Hesap ve aboneliklerin kötüye kullanılması

Veri hırsızları, kurbanlarının kredi kartı, çek, yatırım, telefon (sabit ve mobil), İnternet ödeme, e-posta ve diğer İnternet hesaplarını, sosyal sigorta numaralarıyla sağlık güvencelerini kullanmak suretiyle istismar edebilmektedirler. Bununla birlikte, elde edilen bilgiler telefon, kredi kartı, kredi, çek ve yatırım, İnternet ödeme, otomobil sigortası ile ilgili yeni hesapların açılmasında da kullanılabilmektedir.

Bir suça ilişkin soruşturma ve kovuşturma evrelerinde, tıbbi tedavi için, ev veya işyeri kiralarken, işe girerken vb. durumlarda da başkalarına ait kişisel veriler kullanılabilmektedir.[86]

2.4. Siber Suçlar ve Kişisel Verilerin Ticari Değeri

II. Dünya Savaşı'ndan itibaren ekonomilerin imalat odaklı olmaktan çıkarak hizmet merkezli yapıya bürünmesi BİT'in de gelişimini tetiklemiştir. Bu teknolojilerin gelişmesi ve yaygınlaşmasıyla "bilgi" değer kazanmıştır. Tüketiciden veya onunla ilişkili diğer kaynaklardan toplanarak analizlerde kullanılan bilgiler, üretimin de belirleyicileri olmuştur. Üretimde yaşanan bu "kişiselleştirme", işletmelerin tüketici taleplerine daha iyi karşılık verebilmek için tüketici hakkında daha fazla bilgiye sahip olmak ve saklamak istemesine neden olmuştur. Böylece, tüketici ihtiyaçlarına özel üretim artmıştır. Bununla birlikte, tüketiciler verdikleri veya onlar hakkında diğer yöntemlerle temin edilen bilgilerin güvenli ortamlarda muhafaza edildiğinden ve bu bilgilerin başka amaçlar için kullanılmayacağından emin olmak istemektedirler. Bu isteğin karşılanabilmesinin yolu ise, hukuki düzenlemelerin yapılmasıdır.

Sağlıklı bir veri işleme sistemi, işletmelere aşağıdaki faydaları sağlamaktadır:

- Birey ihtiyaçlarının tespit edilmesi ve bu ihtiyaçlara uygun hizmet ve üretim sağlanması,
- Fiyatların düşmesi ve alışverişin artması,
- Tüketiciye sağlanan rahatlık,
- Tüketicileri yeni fırsat ve ürünler hakkında bilgilendirme imkanı,
- Hizmet ve ürünlere erişimin kolaylaşması,
- Dolandırıcılık ve diğer suçların saptanması ve engellenmesi,
- Taleplere daha hızlı cevap verebilme yeteneği.

İşletmeler, BİT'in sunduğu imkanlardan yararlanarak doğrudan pazarlama faaliyetlerinde de bulunabilmekte ve prensip olarak kişisel veri koruma kurallarına uyulması kaydıyla bu hizmetler uluslararası bir pazar yaratılmasına katkı

[86] OECD, "Policy Guidance on Online Identity Theft". s.4. Haziran 2008.

sağlamaktadır.[87] Örneğin, Amerikan şirketlerinden Acxiom, bilgi teknolojilerini kullanarak tüketicilerin alışveriş alışkanlıkları ve kişisel verilerine dayalı olarak analiz yapmakta, bilgileri birleştirerek yorumlamakta ve böylece elde ettiği bilgileri diğer şirketlerin doğrudan pazarlama hizmetlerinde kullanılmak üzere sunan bir danışmanlık hizmeti vermektedir. Bu şirket, kişisel veri işleyerek dünyada doğrudan pazarlama hizmet sektörünün yüzde 12'sini elinde bulunduran, Amerikanın en iyi 100 şirketinden biridir.[88]

Bilgi transferleri ve veri işlemeleri tüketicilere ve finansal kurum ve işletmelere de bazı somut faydalar sağlayabilmektedir. Örneğin, kredi kurumlarının tüketicilerin kredi bilgilerini toplaması ile ödünç para verme işlemleri her zamankinden daha objektif ve güvenilir bir yapıya kavuşmuştur. Kişiler hakkında daha nitelikli ve gelişmiş bilgilere sahip olan kredi kurumlarının ellerindeki bu bilgiler, kredi dönüş riskini nispeten azalttığından faiz oranları da düşmektedir. ABD'de her yıl, kredi verenlerin kişisel verilerinin kullanılması ile faiz oranlarının yüzde iki düştüğü ve buna bağlı olarak tüketicilerin yıllık 130 milyar Dolar kar ettikleri tahmin edilmektedir.[89]

Yukarıda sayılan bazı faydalarla birlikte, kişisel veriler siber suçların en yaygın malzemelerinden biri olması ve suç işleyene sağladığı haksız menfaat ile arz ve talep tarafıyla kendine özgü pazarı olan bir ticari değer haline gelmiştir. Veri komisyoncuları (data brokers), veri ürünlerini geliştirmek ve pazarlama yapılmasında kullanılmak üzere satmak için kişilerin kredi kartı, sağlık, mali vb. bilgilerini toplayarak bu bilgileri analiz etmektedirler. Ancak bu veri toplama işlemleri çoğu kez hukuka aykırı yollardan yapılmaktadır. Günümüzde "İnternet ekonomisinin para birimi" tanımlamasıyla literatürde yerini almaya başlayan kişisel verilerin, pazarlanmasına yönelik reklam dahi verilmeye başlanmıştır. Dünyanın önde gelen İnternet güvenlik şirketlerinden Symantec'in 2008 tarihli Yeraltı Ekonomisi

[87] AB'nin 2002/58 sayılı Direktifinin 45. dibace paragrafında da, tacirlerin bu pazarlama faaliyetlerine ilişkin meşru menfaatleri olduğu, ancak eğer o ülkede opt-out kayıt sistemi benimsenmişse, bu tacirlerin 2000/31 sayılı e-ticaret Direktifinde doğrudan pazarlama amaçlı istenmeyen iletiler için belirtilen kurallara uyulması gerektiği ifade edilmektedir. Bu kurallardan en temel olanları, istenmeyen iletide göndericinin belirli olmasının sağlanması ve alıcıya iletiyi kolay bir şekilde reddetme imkanının sağlanmasıdır.
[88] Bkz. <http://en.wikipedia.org/wiki/Acxiom>
[89] International Chamber of Commerce (ICC), 2003:9

Raporu'nda, 1 Temmuz 2007-30 Haziran 2008 tarihleri arasında siber suç malzemeleri ve hizmetleri için 276 milyon Dolar değerinde reklam verildiği, reklamı verilen ürünlerden "çalıntı veri" ve "suç aletlerinin" geniş alıcı kitlesi bulduğu belirtilmektedir. Bu rakamın yüzde 59'unu oluşturan çalıntı kredi kartı bilgileri ve banka hesap bilgilerinin satılması ile elde edilecek kanun dışı gelirin 7 milyar dolara ulaşabileceği tahmin edilmektedir. Raporda 69.130 reklam veren olduğu, sunucuların yüzde 13'ünün ABD'de, ikinci büyük yüzdenin ise Romanya'da yer aldığı kaydedilmektedir. 225 Dolar değeriyle en pahalı saldırı aletinin Botnet[90] olduğu tespit edilmiştir. Şifre çalma programı ortalama 10, banka hesabı bilgileri ise 10 ila 1000 Dolar arasında satılmakta olup, fiyatlar, bahsi geçen banka hesabında ne kadar para olduğuna bağlı olarak değişmektedir.[91] Satılık mal ve hizmet sınıflarına bakıldığında siber suçların malzemesi olabilen kişisel verilerden yüzde 31'lik satış oranı ile birinci sırada "kredi kartı bilgileri" (kredi kartı numarası, doğrulama kodu[92], geçerlilik süresi, hesap numarası vb.) yer almaktadır. Satışı yapılan kredi kartı bilgilerini yüzde 20 satış oranıyla mali hesaplar (banka hesap numaraları, manyetik şerit okuma araçları, çevrimiçi ödeme hizmet ve hesapları) ve yüzde 19 ile istenmeyen e-posta ve oltalama ile elde edilen bilgi ve şifreler takip etmektedir. Çalıntı kimlik bilgileri de satışı yapılan diğer bilgilerdendir.[93] Kredi kartlarına ilişkin bilgileri elde etme yöntemleri çok çeşitli olduğundan yeraltı ekonomisinde bu bilgilerin arzının giderek artması beklenmektedir. Kredi kartlarının günlük hayatta sıklıkla kullanılıyor olması da arz yönündeki diğer bir tetikleyicidir. Örneğin ABD'de 2006 yılında kredi kartı ile yapılan işlem sayısı 22 milyar olup, bu sayı bir önceki yıla göre yüzde 8 artmıştır. Türkiye'de ise 2006 yılında kredi kartı sayısı 35 milyona ulaşmış olup, Türkiye bu rakam ile Avrupa'nın en büyük üçüncü pazarı

---

[90] Botnet (zombi ordu), kullancısının bilgisi dışında İnternet üzerinden diğer bilgisayarlara spam, virüs gibi iletiler göndermeye programlanmış bir dizi İnternete bağlı bilgisayardır. Bu bilgisayarlar, bir odağa aynı anda sürekli spam posta veya virüs göndererek sistemin kilitlenmesine neden olduklarından saldırı amacıyla kullanılmaktadırlar. Symantec firmasının "Internet Güvenliği Tehdit Raporu"na göre 2006'nın ilk altı ayında 4.696.903 aktif botnet bilgisayar tespit edilmiştir. Ayrıntılı bilgi için bkz. http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci1030284,00.html.

[91] İnterpromedya Haber Merkezi, Siber Suçtan Kazanılanlar. 1 Aralık 2008. BTnet. <http://www.btnet.com.tr/wps/portal/bilisim/hukuk/sayisal-suclar/detay?wcm.haberId=btnethaber_1227702054034>

[92] "Customer Card ID number" kısaca CID veya CVV2) kartın arka yüzündeki numaranın son üç hanesindeki koddur. Müşteri kart kimliği veya doğrulama kodu olarak ifade edilebilir.

[93] Symantec, 2008:17

durumuna geçmiştir.[94] Kredi kartı ile özellikle İnternette yapılan işlem hacminin giderek arttığı ülkemizde, kişisel veri avcıları karşısında tedbirler artırılmalıdır.

Tablo 2.1. Satış ve talep oranlarıyla mal ve hizmet sınıfları listesi

Satış sırası	Talep sırası	Mal ve hizmetler	Satış oranı (%)	Talep oranı (%)	Fiyat aralığı ($)
1	1	Banka hesap bilgileri	18	14	10-1000
2	2	CVV2 ve kredi kartı no	16	13	0,50-12
3	5	Kredi kartları	13	8	0,10-25
4	6	e-Posta adresleri	6	7	0,30-40
5	14	e-Posta şifreleri	6	2	4-30
6	3	Tam kimlik bilgileri	5	9	0,90-25
7	4	Ödeme bilgilerine ait hizmetler (Cash-out)	5	8	8-50
8	12	Aracı siteler (Proxies)	4	3	0,30-20
9	8	Dolandırıcılık için üretilen mal ve hizmetler (Scams)	3	6	2,50-1000/hafta barındırma için; 5-20 tasarım için
10	7	Toplu e-posta gönderimi hizmetleri (Mailers)	3	6	1-25

Kaynak: Symantec, 2008:20

Yukarıda Tablo 2.1'de ise satış ve talep oranlarıyla mal ve hizmet sınıfları yer almaktadır. Söz konusu mal ve hizmetler de yine kişisel verileri içermektedir. Bu bilgilerin satış fiyat aralığının da yer aldığı tabloya göre, banka hesap bilgileri talep ve satış oranıyla birinci sırada yer almaktadır. Bu bilgilerin 10-1000 Dolar fiyat aralığıyla en pahalı bilgiler olduğu dikkat çekmektedir. Söz konusu veriler, 15 dakikadan daha az bir sürede nakit transferleri ve alışverişte kullanılabilmesi, kredi başvusu yapılabilmesi gibi nedenlerle talep oranının artmasına sebep olmaktadır. Şirketlere ait hesaplar ve ABD hesaplarına göre daha nadir bulunan AB vatandaşlarına ait hesaplar, talebi ve fiyatı yükselten diğer faktörler olarak sayılabilir.

Aşağıdaki Tablo 2.2'de ise, kişileri tanımlanabilir kılan, tek örnek sayılabilecek ve genellikle yeraltı ekonomisi faaliyetlerinde kullanılan hassas veriler yer almaktadır. Bu veriler tek tek veya o veriyi bütünleyen diğer veri parçalarından oluşan veri setleri halinde kullanılmaktadır. Bu verilerin satışında, yüzde 23 talep oranıyla kredi kartı doğrulama kodu (CVV2 numarası) ilk sırada gelmektedir.

[94] Kara ve ark., 2008:2

Tablo 2.2. Tek örnek olarak bulunan hassas verilerin talep oranı

Hassas Veriler	Oran (%)
Doğrulama kodu (CVV2 numarası)	23
Kredi kartı numaraları	18
Kredi kartı geçerlilik süresi	15
Adresler	12
Telefon numaraları	11
e-posta adresleri	6
Şifreler	5
Sosyal güvenlik numarası	4
Ad-soyad	4
Doğum tarihleri	2

Kaynak: Symantec, 2008: 26

75 milyon genişbant kullanıcısının olması ve dünyadaki toplam sunucuların yüzde 41'ini barındırması nedeniyle ABD, kişisel verilerin satışı ile ilgili yeraltı ekonomik faaliyetlerinde ilk sırada bulunmaktadır. Buna paralel olarak, ABD siber suçların en fazla işlendiği ülkelerdendir. İkinci sırada yüzde 13'lük bir oranla Romanya gelmektedir. Romanya'da son yıllarda siber suçta oldukça büyük bir patlama yaşanmıştır. Ekonomide yaşanan sıkıntılar ve istihdam problemleri sonrasında bilgisayar konusunda yetkinlikleri yüksek olan insanlar yolsuzluk, dolandırıcılık ve siber suçların işlenme oranlarını artırmıştır.[95]

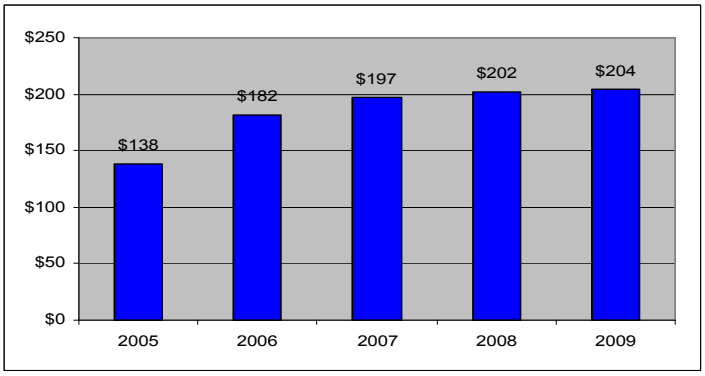
2.5. Siber Suçların Bazı Etkileri

Siber suç olgusu, BİT kullanımında sınırlandırıcı bir etki yaratmaktadır. Bu konuda, ITU'nun 2006 yılında yaptığı çevrimiçi araştırmaya göre, İnternet kullanıcılarının yüzde 40'ından fazlası, kişisel veri hırsızlığı endişesiyle elektronik ortamda işlem yapmaktan kaçındıklarını ifade etmişlerdir.[96] Yine Avrupa Komisyonu'nun bir çalışmasına göre, AB vatandaşlarının yüzde 64'ü kurum ve kuruluşların tuttukları kişisel bilgileri uygun bir biçimde sakladıkları ve doğru kullandıkları konusunda endişeli olduklarını dile getirmişlerdir.[97]

[95] Symantec, 2008:58
[96] OECD, "Policy Guidance on Online Identity Theft". Haziran 2008
[97] European Commission. Flash Eurobarometer, 2008:5 (Flash Eurobarometer, 1973 yılından bu yana, Avrupa Komisyonu adına bilgi ve iletişim politikalarının geliştirilmesine yardımcı olmak için üye ülkelerde kamuoyu görüşlerini araştırmakta ve düzenli olarak raporlamaktadır.)

Siber suç ve veri ihlalleri ile mücadele edilmesinin maliyet etkisi oldukça yüksektir. Amerikan Kimlik Hırsızlığı Araştırma Merkezi'nin (Identity Theft Resource Center)[98] yaptığı bir araştırmaya göre, 2008 yılı kişisel veri hırsızlığında zirve yıl olmuştur. 2007 yılı içinde toplam 35 milyon kişinin bilgisinin çalındığını ifade eden araştırma, veri güvenliği konusunun ne denli karmaşık olduğuna da işaret etmektedir. Ponemon Enstitüsü'nün veri ihlalleri ile ilgili 2010 tarihli yıllık raporu, ABD işletme ve kurumlarına vak'a başına maliyetin 2009 yılı için ortalama 6,75 milyon Dolar olduğunu, bu büyüklüğün her bir kayıt başına maliyetinin ise 204 Dolara denk geldiğini vurgulamaktadır. Önceki yılların verileri dikkate alındığında, bu rakamların, hizmetlerin elektronik ortama taşınması ve İnternetin artan kullanımı nedeniyle, gerekli tedbirler alınmazsa artacağı düşünülmektedir. Söz konusu çalışma, 2010 yılında kişisel verilerin kaybı ya da hırsızlığı ile sonuçlanan vak'aların yüzde 24'ünün kötü niyetli yazılımlar veya suç teşkil eden diğer araçlar ile ortaya çıktığını, bu araçların yarattığı ekonomik kaybın ise, ihmale dayalı kazalar sonrası ortaya çıkan kayıplardan çok daha yüksek olduğunu ortaya koymaktadır.[99]

Şekil 2.1. ABD'de kayıt başına ortalama veri ihlal maliyeti, 2005-2009



Kaynak: Ponemon Institute, 2010:12

[98] Bkz. <http://www.idtheftcenter.org/index.html>
[99] Ponemon Institute, 2010:12-16

2.6. Kişisel Verilerin Kötüye Kullanılmasında ve Siber Suçla Mücadelede Alınacak Tedbirler

Amerikan Kimlik Hırsızlığı Araştırma Merkezi'nin araştırmalarına göre, veri hırsızlığına maruz kalan kurumların büyük bir çoğunluğunun ortak zaafları gerekli şifrelemeleri yapmamış olmalarıdır. 2007 yılında ABD'de 446 ciddi veri hırsızlığı vak'ası tespit edilirken, bu sayı 2008'de yüzde 47 artarak 656'ya ulaşmıştır. Veri hırsızlıklarının yüzde 35'inin özel sektör faaliyetleri sırasında meydana geldiği; resmi ve askeri kurumlardaki hırsızlıkların sayısının ise 110 olarak tespit edilebildiği ifade edilmektedir. Araştırmada dikkate alınan veri hırsızlıklarının özel ya da kamu işletmeleri tarafından açıklanan veya basında yer alan olaylardan alındığı, dolayısıyla bu rakamın buzdağının sadece üst kısmını yansıttığı ve gerçek rakamın çok daha ciddi olduğu ifade edilmiştir. ABD'nin farklı eyaletlerinde veri koruma konusundaki farklı kanunlar, şirketleri veri hırsızlıklarını açıklayıp açıklamama konusunda karar vermeye yönlendirirken, basın ve kamunun baskısı bu tip olaylardan halkın haberdar olmasını sağlamaktadır.

Veri hırsızlıkları, fiziksel ve bilgi işlem güvenliğine yeterince önem verilmemesi, dizüstü bilgisayar hırsızlıkları, korsan faaliyetler, şirket çalışanlarının veri sızdırması gibi farklı şekillerde gerçekleşebilmektedir.

Siber suç ve veri hırsızlıklarında farkındalığı artırmaya yönelik olarak son yıllarda önleyici, caydırıcılığı artırıcı ve koruyucu birtakım önlemler alınmaktadır. Bu tedbirlerden *önleyici* nitelikte olanların başarısı, yalnızca bilgi teknolojileri okur-yazarlığının artırılması ile mümkün değildir. Bireyin farklı ortamlardaki davranışlarının mahremiyete yönelik etkilerinin farkında olabilmesi ve tehlikeleri öngörebilmesi oldukça önemlidir. Bu sebeple, kişilerin mağduriyete uğramadan önce neler yapmaları gerektiği konusunda bilgilendirilmeleri ve bilinçlendirilmeleri faaliyetleri önleyici niteliktedir.

Yasal yolların güçlendirilerek, siber suçların ve bu suçlar karşısında verilecek cezaların kanunda tanımlanması ise bu suçların işlenme oranlarının azaltılması bakımından *caydırıcı* tedbirlerindendir. Aynı zamanda bu tedbirler, bireye sağladığı kontrol ve erişim hakları nedeniyle siber suçlar karşısında bireylerin kullanmadan

kaçınma davranışlarını önlemekte, böylece teknolojinin sunduğu imkanların kullanımının önü açılmaktadır. Bu duruma örnek olarak, Kanada Mahremiyet Ofisi'nin 1999-2000 tarihli Yıllık Faaliyet Raporu'na göre, 1992 yılında Kanadalıların yüzde 60'ı "Günlük hayatımda 10 yıl öncesine göre şu anda daha az kişisel mahremiyetim olduğunu düşünüyorum." diyorken, bu oran 1999 yılında yüzde 47'ye düşmektedir. Bireye erişim hakkı tanıyan ve verileri üzerinde söz sahibi olmasını sağlayan yasalar ile sağlanan bu düşüş, benzer şekilde, 1992 yılında devletin kişiler hakkında istediği her şeyi öğrenebileceğini ve gerçekten mahremiyetin olmadığını düşünen yüzde 81'lik çoğunluğun, 1999'da % 63'lere düşmesine de sebep olmuştur. Nihayet, yüzde 54 oranındaki Kanadalılar, şirketlerin kendileri hakkında tuttukları kayıtlar hakkında bilgi sahibi iseler ve durdurma hakları varsa, bu durumu önemsemediklerini ve "kontrol" yetkisinin karşılığında bir kısım mahremiyetlerini de feda edebileceklerini ifade etmişlerdir.[100]

Mahremiyet artıcı teknolojiler, kimlik doğrulamada sağladığı avantaj nedeniyle mahremiyetin korunmasında *elektronik imza* ve güvenlik ve veri gizliliğinin sağlanmasında *akıllı kartlar* koruma ve özellikle maddi zararın azaltılmasında günümüzde yaygınlaşmaya başlayan tedbirlerdendir. Koruyucu nitelikteki bu tedbirler aşağıda incelenmektedir.

2.6.1. Mahremiyet artırıcı teknolojiler

Temel amacı; mahremiyet kanunlarının ya da ilkelerinin uygulanmasına yardımcı olmak, kişiyi belirlenebilir kılan verilerin toplanması veya bu verilerin daha ileri düzeylerde işlenmesini mümkün olduğunca aza indirgemek olan teknolojik çözüm araçlarına mahremiyet artırıcı teknolojiler[101] (MAT) denilmektedir. Bu teknolojiler, kullanıcıya verilerinin çevrimiçi ortamda ifşa edilmesi, yayılması ve kullanılması riskine karşı kontrol imkanı sağlamaktadır. Bu kontrol, herhangi bir ağ üzerindeki tarayıcılarda veya e-postalarda kişisel verilerin belirli durum ve şartlarda anonim hale getirilmesi, çerezlerin veya diğer izleme teknolojilerinin filtrelenmesi, verinin yayılması şartlarının belirlenmesi, verilerin şifrelenmesi vb. seçenekler ile gerçekleşmektedir.

[100] OECD, 2003:267
[101] Privacy Enhancing Technologies (PET)

"Güvenlik teknolojileri" ve "mahremiyet artırıcı teknolojiler" olarak ifade edilen araçlar arasında sıkı bir ilişki bulunmaktadır. Mahremiyetin korunabilmesi için güvenliğin de iyi sağlanması gerekmektedir. MAT'lar, kişisel verilerin küresel alanda çevrimiçi akışında (e-ticaret faaliyetleri gibi) kullanıcıların kişisel verilerini verirken duydukları endişeyi kısmen azaltmaktadır. Genellikle tüketiciler için tasarlanan MAT'ların bazı türleri ise, kurumlar ve işletmelerin mahremiyet politika ve uygulamalarına yardımcı olmak için tasarlanmaktadır.

MAT'lar fonksiyonları, teknik yapıları, kullanımları ve özellikleri ile çeşitlilik arz etmektedirler. Tüketicilerin ve işletmelerin işlemlerinde özel önem verdikleri MAT türünü seçmeleri gerekmektedir. Ulusal hukuklardaki farklılık da MAT'ların kullanıldığı amaçları etkileyen faktörlerdendir.

Avrupa Standardizasyon Komitesi (CEN)[102], AB Veri Koruma Direktifi'nin uygulanmasında teknolojik standartların kullanılabilirliği yönünde bir çalışma yürütmektedir. Bu çalışma kapsamında hangi teknolojilerin MAT sayılacağına ilişkin bir belirleme ile e-devlet uygulamalarında MAT kullanımı, bu teknolojilerde araştırma ve geliştirme faaliyetleri araştırılmaktadır.[103]

1997 yılında OECD'nin yayınladığı raporda[104] küresel düzeyde kişisel verilerin korunabilmesini sağlayacak teknolojilerin ve politikaların gelişimi desteklenmektedir. Yine 1998'de düzenlenen Ottawa Bakanlar Konferansında da OECD'nin "MAT'ların kullanımını desteklediği" açıkça kaydedilmiştir.

Bu teknolojilerin gelişimi konusunda çalışmalar devam etmektedir.[105] Bu çerçevede, ülkemizde yasal düzenlemelerin yapılmasının ardından, bireylerin, işletmelerin ve devletin mahremiyet ile ilgili iş ve işlemlerinde uygun MAT'lardan faydalanmaları gerektiği değerlendirilmektedir. MAT'lar bu yönüyle veri korumada

---

[102] Avrupa Standardizasyon Komitesi, 1961 yılında Avrupa'daki ulusal standart kuruluşları tarafından kurulmuştur (www.cenorm.be). Bu Komitenin standartlarına uymak ihtiyari olmakla birlikte, bunlara uygun olarak imal edilen ürünlerin otomatik olarak Topluluk mevzuatına da uygun oldukları kabul edilmektedir. (DPT, AB Sözlüğü, 2004).

[103] Bkz. CEN Workshop on Data Protection and Privacy (WS/DPP) <http://www.cen.eu/CEN/Sectors/Sectors/ISSS/Activity/Pages/wsdpp.aspx>

[104] OECD, 1997.

[105] OECD. "*Privacy Online (OECD Guidance on Policy and Practice)"* (2003) kitabının 245-268 sayfa aralığındaki "Chapter 12-Inventory of Privacy-Enhancing Technologies" bölümünden faydalanılmıştır.

ikincil kaynak olarak dikkate alınmalıdır. Aşağıda Tablo 2.3.te başlıca MAT'lar ve bunların kullanıldıkları alanlar verilmektedir.

Tablo 2.3. MAT'lar ve mahremiyet ilkeleri

MAT örnekleri	Temel politikalara etki örnekleri (OECD Mahremiyet Rehber İlkelerine dayalı olarak)
Anonimleştirme/ takma ad (*pseudonymity*) araçları	(Veri) Toplama sınırlaması (veya toplamadan kaçınma)
Kişisel veri yönetim araçları (bilgi satıcıları veya infomediaries[106])	Toplama sınırlaması; güvenlik
Bildirim/ seçim araçları (Mahremiyet Tercih Platformları gibi)	Açıklık/bildirim; toplama sınırlaması/izin ve seçenek
Pazarlama/ reklam kontrol araçları (çerezler, casus yazılım filtreleri, pazarlamada izin yönetim vb.)	Toplama sınırlaması; seçenek ve/veya izin; güvenlik
Güvenlik araçları	Güvenlik
e-Ticaret mahremiyeti/ güvenlik araçları	Toplama sınırlaması; güvenlik
Erişim kontrol araçları	Bildirim, güvenlik, kullanım sınırlaması, veri sahipleri aracılığıyla erişim
Çocuklar için mahremiyet araçları	Toplama sınırlaması / izin
Mahremiyet denetimi/ uygunluk araçları	Hesap verebilirlik

Kaynak: OECD, 2003:273

Birçok uluslararası çalışma ve özellikle OECD'nin üye ülkeleri üzerinde yaptığı bir araştırma, devletlerin kişisel verilerin korunmasında aldıkları yasal tedbirlerin, teknik ve kurumsal tedbirlerle desteklenmesi gerektiği noktasında buluşmaktadır. Sınır tanımayan mahremiyet ihlalleriyle mücadele de ulusaldan ziyade küresel bir perspektifle işbirliğine dayalı olarak ele alınmalıdır.

[106] *Infomediary:* Pazarlama ve reklam amacıyla tüketicilerle ilgili toplanan veriler üzerinde tüketiciler adına kontrol kurmaya yardımcı olan acenta gibi çalışan kişilerdir. Bu kişiler, kişisel veriyi toplayanın değil, tanımladığı kişinin mülkiyetinde olduğu prensibiyle hareket etmektedirler. Infomediary iş modelinde, kişisel verilerin ticari değerinden hareketle bu verilerin sahibi olan kişilerin bu değerleri paraya çevirmeleri ve kendi kişisel profilinden kar elde etmesini sağlayan güvenilir kişi olarak tanımlanan aracı kişilerdir. Ayrıntılı bilgi için bkz. <http://en.wikipedia.org/wiki/Infomediary>

2.6.2. Elektronik imza (e-İmza)

Kimlik doğrulama, neredeyse bütün hukuki işlemlerin gerçekleştirilmesinde ilk adımı oluşturmaktadır. Bu nedenle elektronik hizmet sunumunda kimlik doğrulama araçlarından sağlıklı olanlar tercih edilmelidir.

Bir kimlik doğrulayıcı olan elektronik imza ile MAT'ların farklı ihtiyaçlar ve farklı amaçlara özgü olduğunu söylemek mümkündür. Özellikle İnternet üzerinden yapılan sözleşmeler ve diğer hukuki işlemler "hazırlar arasında olmayan sözleşmeler"[107] olduklarından kişinin gerçekten o kişi olduğundan emin olmadan sözleşme yapılması zaman zaman sorunlar yaratabilmektedir. Bu çerçevede akıllı kimlik kartları ve elektronik imza kullanılmaktadır. Bu sayede, kişilerin kimlik bilgileri yetkisiz kişilerin ellerine geçmiş olsa bile, bu yetkisiz kişiler gerçek kişinin yerine işlem yapamayacaktır. Dolayısıyla bu araçlara günümüzde işlem yapabilmenin teknolojik ehliyeti de denilebilir.

Elektronik imza; bilginin, orijinalliği bozulmadan, tarafların kimliğini de belirleyebilecek şekilde elektronik ortamda karşı tarafa aktarılmasını garanti eden bir teknolojidir. Ülkemizde, 15 Ocak 2004 tarihli 5070 sayılı Elektronik İmza Kanunu, elektronik imzanın hukuki yapısını, elektronik sertifika hizmet sağlayıcılarının faaliyetlerini ve her alanda elektronik imzanın kullanımına ilişkin işlemleri düzenlemektedir. Bu Kanunun 3'üncü maddesinin (b) fıkrasına göre, elektronik imza; başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veriyi tanımlar.

Kimlik doğrulama araçlarından olan elektronik imza diğer birçok teknoloji gibi güvenliği desteklemektedir. Bu tür güvenlik araçları, bireylerin kimliklerini

[107] Akdedilen bir sözleşmenin hükümlerini doğurmaya başladığı zaman ile kurulduğu zamanın saptanması bakımından hukukumuzda, bir arada bulunan kişiler arasında yapılan sözleşmeler, yani hazırlar arasındaki sözleşmeler ile, bir arada bulunmayan kişiler arasındaki sözleşmeler, yani hazır olmayanlar arasındaki sözleşmeler birbirinden farklı hükümlere tabi kılınmıştır. Hazırlar arasında yapılan sözleşmelerde, icabın hemen kabul edilmesi gerekir ve kabul beyanı ile birlikte sözleşme aynı anda hükümlerini doğurmaya başlar ve kurulmuş olur. Hazır olmayanlar arasında yapılan sözleşmelerde ise, icap yapan taraf, makul bir süre boyunca yaptığı icap ile bağlı olacak ve karşı tarafın kabul haberini bekleyecektir. Sözleşme, kabul haberi gönderildiği anda hükümlerini doğurmaya başlar ve kabul haberi icapçıya vardığı anda da kurulmuş olur.

doğrulamak için tasarlandığından, mahremiyet kuralları gereği "anonim" olarak gerçekleştirilecek çevrimiçi faaliyetlerde kullanımı desteklememektedir.

Elektronik imzayı biraz daha yakından tanımak için aşağıda bu imzanın çeşitleri ve kullanımı, e-imza sertifikası ve 5070 sayılı Kanunda geçen güvenli elektronik imza kavramları açıklanmaktadır.

i) Elektronik imza çeşitleri ve kullanımı

Elektronik imza, biyometrik imza ve dijital (sayısal) imza olarak ikiye ayrılır. Biyometrik imza, kullanıcının parmak izi veya retina gibi kişiye has özellikler kullanılarak oluşturulan imzadır. Sayısal imza ise, imzalanan metne göre farklılık gösterir ve içeriğin matematiksel fonksiyonlardan geçirilerek eşsiz olduğu düşünülen bir değer bulunması sureti ile elde edilir. Bu imza, belge üzerinde değişiklik yapılıp yapılmadığının tespitini (verification) sağlamaktadır. Dünyada daha çok sayısal imza kullanılmaktadır. 5070 sayılı Elektronik İmza Kanunu'nda geçen "elektronik imza" kavramı da sayısal imzayı işaret etmektedir.

Elektronik imzada, elle atılan imzada olduğu şekilde kişinin tek imzası yoktur; bunun yerine imzalamada kullanılan anahtarları vardır. Anahtar, bir çift şifreden oluşmaktadır. Bu anahtarların birisi elektronik olarak haberleşen taraflardan göndericide, diğeri ise alıcıda bulunur. Bu anahtarlardan göndericide bulunan gizli anahtarla sayısal imza oluşturulur. Açık anahtar dediğimiz diğeri ise, alıcıya bildirilir ve sadece sayısal imzanın doğrulanmasında kullanılır.

İmzalama aşaması ise şöyle gerçekleşir; gönderilecek veri ya da ileti özgün bir şekilde kısaltılarak iletinin yeni bir versiyonu elde edilir, buna özdeğer (hash) adı verilir. Gizli anahtarla gönderici bu özdeğeri kodlar ve iletiyle birlikte alıcıya gönderir. Alıcının, göndericinin açık anahtarıyla çözdüğü özdeğer ile, orijinal belge için kendisinin hesapladığı özdeğer birbirini tutuyorsa, iletinin göndericinin orijinal belgesi olduğu ve iletinin değişmeden geldiği onaylanmış olur.[108]

[108] Erturgut, 2004'ten faydalanılmıştır.

ii) e-İmza Sertifikası

Sayısal imzadan beklenen bir başka özellik, imza sahibinin kimliğinin de güvenilir biçimde doğrulanmasıdır (identification). Bunu sağlamak için sertifikalara ihtiyaç duyulur. Sertifika, sertifika hizmet sağlayıcısı tarafından kişinin kimliğinin onaylanması, bu durumun belgelenmesidir. Bu sertifikalar, tarafsız bir üçüncü kişi tarafından sağlanıyor ise bu kişinin kimliğine güvenilebilir; fakat eğer imza sahipleri kendileri elektronik sertifika oluştururlarsa, herhangi bir isim altında bu imzayı oluşturabilme ihtimalleri vardır. Elektronik İmza Kanunumuzda elektronik sertifika hizmet sağlayıcısı, elektronik sertifika, zaman damgası ve elektronik imzalarla ilgili hizmetleri sağlayan kamu kurum ve kuruluşları ile gerçek veya özel hukuk tüzel kişileri şeklinde tanımlanmaktadır. Halen ülkemizde BTK tarafından yetkilendirilmiş olan Kamu Sertifikasyon Merkezi ve özel hukuk tüzelkişisi niteliğini haiz üç şirket bu işlevi yerine getirmektedir.

Elektronik sertifika, Elektronik İmza Kanunu'nun 3'üncü maddesinde "imza sahibinin imza doğrulama verisini ve kimlik bilgilerini birbirine bağlayan elektronik kayıt" olarak tanımlanmaktadır.

İmza anahtarı sahibi, sertifika hizmet sağlayıcısına başvurduktan sonra elde ettiği özel anahtarıyla elektronik belgeleri imzaladığında, sertifikası da imzalı elektronik belgelere eklenir. Yani elektronik olarak imzalanmış bir belge üç kısımdan oluşur; mesaj, mesaja bağlı olarak oluşturulmuş sayısal imza ve imza anahtarı sahibinin sertifikası.

Nitelikli elektronik sertifika: 5070 sayılı Kanunun 9'uncu maddesinde, nitelikli bir elektronik sertifikanın sahip olması gereken özellikler sayılmaktadır. Bu Kanuna göre nitelikli elektronik sertifikaya dayanmayan elektronik imzalar güvenli olarak nitelendirilmemektedir. Aşağıda güvenli elektronik imza ve unsurları ele alınmaktadır.

iii) Güvenli elektronik imza

AB'nin 1993/93/AT sayılı Elektronik İmza Direktifi ile gelişmiş (advanced) elektronik imzanın yargılamada delil olarak kullanılması temin edilmektedir. Gelişmiş elektronik imzanın nitelikli elektronik sertifikaya dayanması ve güvenli

imza oluşturma araçları ile oluşturulmuş olması gerekmektedir. Alman Elektronik İmza Kanunu AB mevzuatının karşılığını teşkil eden bu tür imzaya "nitelikli elektronik imza" adını vermektedir. Türk hukukunda ise "güvenli elektronik imza" kavramı tercih edilmiştir. 5070 sayılı Elektronik İmza Kanununun 4'üncü maddesine göre "güvenli elektronik imza"da bulunması gereken özellikler şunlardır:

1- Münhasıran imza sahibine bağlı olmak,

2- Sadece imza sahibinin tasarrufunda bulunan güvenli elektronik imza oluşturma aracı ile oluşturulmak,

3- Nitelikli elektronik sertifikaya dayanarak imza sahibinin kimliğinin tespitini sağlamak,

4- İmzalanmış elektronik veride sonradan herhangi bir değişiklik yapılıp yapılmadığının tespitini sağlamaktır.

Yukarıdaki dört şartın varlığı halinde o imza *güvenli* sayılmaktadır.

5070 sayılı Kanuna göre güvenli elektronik imza, elle atılan imza ile aynı hukuki etkiyi haizdir. Sadece kanunların resmi şekle veya özel bir merasime tabi tuttuğu hukuki işlemler ile teminat sözleşmeleri güvenli elektronik imza ile gerçekleştirilemez.

2.6.3. Akıllı kartlar

Akıllı kartlar, elektronik imza altyapılarında ve gizliliğinin korunması gereken bilgilerin taşınmasında sıklıkla kullanılan donanımlardır. Bu kartlar, gizli bilgilerin taşınması amacıyla kullanılabileceği gibi, şifreli yayınlara erişim gibi elektronik şifreleme vb. bazı özel fonksiyonları yerine getirmede veya GSM telefonları veya kredi kartlarında kullanılabilir.

Akıllı kartlar, gizli bilgilerin korunması ve bu bilgilerle işlem yapılması konusunda güvenli yapılardır. Bu nedenle söz konusu kartlar, elektronik imzanın gizliliğinin korunması gereken bazı uygulamalarında (örneğin, imza sahibi tarafından elektronik imza oluşturma amacıyla kullanılan ve bir eşi daha olmayan şifreler, kriptografik gizli anahtarlar gibi verilerin korunmasında) yaygın olarak

kullanılmaktadır. Bu kartlar, kimlik tespiti gerektiren hizmetlerin sunumunda da oldukça güvenli araçlar olarak kabul edilmektedir.

Akıllı kartlar esasında, gizli bilgilerin üzerinde bulunduğu ve şifreleme işlemlerini de yapan bir çip ve bu çipi çevreleyen bir plastikten oluşmaktadır. Bu haliyle bir kredi kartı büyüklüğünde olan bu kartlardaki çipin içerisinde bellek birimleri, işlemci, kripto işlemcisi vb. bileşenler bulunur.

Günümüzde üretilen akıllı kartlar sadece kriptografik işlemleri güvenilir şekilde yerine getirmenin yanı sıra, üzerlerindeki birden çok uygulamaya ait bilgiler ve program parçacıkları ile daha fazla alanda kullanılabilmektedir. Örneğin; kişisel sağlık bilgileri ve bu bilgileri kullanan program parçacıkları kart üzerindeki belleğin bir bölümünde, finansal bilgiler ise belleğin farklı bir bölümünde bulunabilir. Kart, sağlık hizmetleri için kullanılacaksa ilgili kurum (örneğin hastane) kartın sadece sağlık bilgileri ile ilgili kısmına erişebilir, finansal bilgilere ulaşamaz.

Akıllı kartlar, kimlik tanımlama ve kimlik tespiti işlemlerinde de önemli bir güvenlik teknolojisidir. Kartın işlem kontrolü, kimlik tespiti sonucunda sunulacak hizmetin niteliğine göre, PIN ya da biometrik verilerle yapılabilir. Örneğin, akıllı kart, malvarlığına ilişkin devredilebilir bir hak olarak, bankadan para çekme işlemi için kullanıldığında, PIN kontrollü tasarlanabilir. Böylece kişi kendi menfaati için, PIN numarasını kimseyle paylaşmama sorumluluğu ile birlikte, dilerse bu hizmeti bir yakını aracılığıyla da alabilir. Ancak, sağlık hizmetlerinden faydalanma veya yurt dışına çıkış gibi kişiye sıkı sıkıya bağlı olan ve devredilemeyen hakların kullanılmasında, sahteciliğin önlenmesi için akıllı kartın PIN kodu yerine, kişiden ayrılamayan biometrik veriyle aktive olması daha güvenli bir tercihtir.

Bu çalışmanın yapıldığı dönemde, birçok ülkede kullanıldığı gibi, Türkiye'de de kamu hizmetlerinin sunulmasında kimlik doğrulama için kimlik kartı olarak akıllı kart teknolojisi kullanılması yönünde başlatılan altyapı çalışmaları devam etmektedir.

3. ULUSLARARASI ALANDA VE KARŞILAŞTIRMALI HUKUKTA KİŞİSEL VERİLERİN KORUNMASI

3.1. Genel Çerçeve

Teknolojik gelişmelerin tetiklediği kişisel verilerle ilgili güvenlik sorunları yalnızca ulusal düzeydeki araçlarla çözümlenememektedir. Bu durumun birkaç sebebi vardır. Bunlardan ilki ve en önemlisi, bilgilerin serbest dolaşımı tartışmaları çerçevesinde, İnternetin gelişerek haberleşme maliyetlerinin düşmesi ve bu sebeple kişisel verilerin sınır ötesine iletiminin artmasıdır. Bu artışın paralelinde, ilk olarak 1983'te geliştirilen ve günümüzde veri işletim sistemleri olarak bilinen uluslararası veri bankalarının da sayısı ve kapasitesi artmaya başlamıştır. Veri bankalarında tutulan kişisel veriler, verinin uluslararası alanda korunması, toplanması, işlenmesi ve yayılmasına ilişkin kanunların uygulanmasında işbirliğini ve ülkelerin ortak hukuki zeminde buluşmasını gerektirmektedir.

Mahremiyetin ve kişisel verilerin korunmasına ilişkin kanunların uygulanmasında işbirliği gereksinimi OECD, Uluslararası Veri Koruma ve Mahremiyet Komiserleri Konferansı, Avrupa Konseyi, Asya Pasifik Ekonomik İşbirliği, Avrupa Birliği ve bünyesindeki ilgili Çalışma Grubu (Madde 29 Çalışma Grubu olarak anılmaktadır) nezdinde kabul edilmekte ve önemsenmektedir.[109]

Veri koruma konusunu uluslararası nitelikte kılan bir diğer sebep ise uluslararası veri iletiminde ülkelerin maliyetlerde ortak hareket ederek tasarrufa gitme kolaylığının mümkün olmasıdır. Yine ülkeler, veri işleme ile ilgili yasal düzenlemelerin dikkate alınmadığı bölgelerin yaratılmasının engellenmesi ve verinin aktığı alanlarda da en azından kendi düzenlemelerine yakın bir koruma düzeyinin sağlandığından emin olmak konusunda hemfikirdirler.

Bu nedenlerle, uluslararası birçok kuruluş, ülkelerin mahremiyet koruma alanında daha etkin politikalar belirleme ve düzenlemeler yapma konusunda teşvik edici çalışmalar yapmışlardır. Bu çalışmalar, genel olarak veri koruma alanında farklı ülkelerdeki kanunlar arasında doğacak ihtilafların çözümünde ortak hedef olan

[109] OECD, 2007:4

"bireyin korunması"nı esas almakta ve bunun bir hakka dönüştüğünü vurgulamaktadır[110]. Kişisel verilerin korunmasıyla ilgili olarak ciddi çalışmalar yapan uluslararası kuruluş ve birlikler; OECD, Avrupa Konseyi, Birleşmiş Milletler, Dünya Ticaret Örgütü, Avrupa Birliği ve diğer bazı platformlardır. Bu kuruluş ve birlikler, yapmış oldukları çalışmalarla kişisel verilerin korunması ve mahremiyetin gerekliliği konularında uluslararası bilincin oluşmasında önemli rol oynamışlardır. Bu bölümde, sırasıyla bu uluslararası kuruluş ve birliklerin mahremiyet ve kişisel verilerin korunması alanında yapmış oldukları çalışmalar incelenecek, daha sonra kişisel verilerin korunması konusu karşılaştırmalı hukuk bağlamında ülke incelemeleri ile ele alınacaktır.

3.2. Uluslararası Alanda Yürütülen Çalışmalar

3.2.1. OECD

BİT'in ekonomik ve sosyal yaşamın içine girmesi ve bilgisayarla veri işlemenin giderek önem kazanması neticesinde birçok OECD üyesi ülke mahremiyetin korunması alanında düzenlemeler yapmıştır. Bazı ülkelerde bu süreç halen devam etmektedir. Ancak, bilginin serbest dolaşımı ilkesi çerçevesinde, veri trafiğinin önem kazandığı ülkeler arasındaki mevzuat farklılıkları sorunlara neden olmuştur. Bu çerçevede OECD, 1978 yılında bir Uzman Grubu kurarak başlattığı çalışmalar neticesinde, 1980 yılında mahremiyetin korunması ve sınır ötesi kişisel veri korunmasını teşvik eden tavsiye niteliğindeki "Mahremiyetin Korunması ve Kişisel Verilerin Sınır Ötesine İletimi Hakkında Rehber İlkeler"i (kısa adıyla Mahremiyet Rehber İlkeleri) kabul etmiştir[111]. Söz konusu İlkelerin kabul edildiği yıllarda OECD üye ülkelerinin yaklaşık üçte biri mahremiyet kanunlarına sahip iken, günümüzde bu ülkelerin tamamına yakınında mahremiyet kanunları kabul edilmiş ve bu kanunların uygulanmasını sağlayacak sorumlu kurumlar kurulmuştur.[112]

Mahremiyet Rehber İlkeleri, bireylere ilişkin verilerin her türlü yerel bilgisayar ağlarından, karmaşık ulusal ve uluslararası ağlara kadar geniş bir alanda

[110] OECD, 2002:24
[111] OECD, 2002:28
[112] OECD, 2007:4

işlendiği durumlara yönelik bir içeriğe sahip olup, aynı zamanda küresel ağlarda mahremiyet korumaya ilişkin temel belge olarak görülmektedir. Kişisel verilerin toplanması ve yönetilmesi ile ilgili teknolojik gelişmelere ayak uydurabilecek esneklikte kaleme alınan bu ilkeler seti, mahremiyet standartları ve kişisel verilerin toplandığı her tür ortam için halen uluslararası uzlaşmayı temsil etmektedir. Mahremiyet Rehber İlkeleri'nde yer alan sekiz temel prensip şunlardır:

1-Sınırlı bilgi toplama: Kişisel verilerin toplanmasında belirli sınırlamalar olmalıdır. Hukuka uygun sebepler ve araçlarla veri toplanırken, veri sahibi (öznesi) toplama konusunda bilgilendirilmeli ve bilinçli rızası alınmalıdır.

2- Veri kalitesi: Kişisel veriler, kullanılacakları amaç ile ilgili olmak şartıyla mümkün olduğunca doğru, tam ve güncel olmalıdır.

3- Amaca özgülük: Kişisel verilerin toplanma amacı belirlenmeli ve bu veriler sadece belirlenen amaç için kullanılmalıdır. Kullanım amacı, verinin toplandığı zamandan sonraki bir tarihte değişiyorsa veya yeni amaca uygun olarak veri işleme faaliyetinin veri sahibine zarar verme ihtimali varsa, veri sahibi kişi bilgilendirilmelidir.

4- Kullanım sınırlaması: Toplanan veriler, "amaca özgülük" prensibi ile belirlenen amaçlar dışında yayılamaz, bulundurulamaz veya başka amaçlarla kullanılamaz. Kullanım sınırlamasının istisnaları; veri sahibinin bilinçli rızası ve kanuna dayalı yetkidir.

5- Güvenlik önlemleri: Toplanan veriler, potansiyel tehlikelere karşı (kayıp, yetkisiz erişim, zarar verme, değiştirme, kullanma, açıklama) makul güvenlik tedbirleri ile korunmalıdır.

6- Açıklık (aleniyet) ilkesi: Kişisel verilerle ilgili gelişmeler, uygulama ve politikalar hakkında genel bir açıklık ilkesi bulunmalı; kişilere kendileriyle ilgili veri barındıran kurum ve kuruluşların bu gizlilik politikalarına kolaylıkla erişebilme hakkı sağlanmalıdır.

7- Bireyin katılımı (rıza): Veri öznesinin rızası olmaksızın veriler erişilebilir hale getirilmemeli ve açıklanmamalıdır. Bununla birlikte veri sahibinin;

(a) veri kontrolörünün kendisi ile ilgili veriye sahip olup olmadığı hakkında bilgi alma hakkı,

(b) kendisiyle ilgili veri konusunda kontrolör ile

- Makul bir süre içinde,
- Ölçülü bir ücret mukabilinde,
- Makul bir şekilde,
- Açık ve anlaşılabilir araçlarla irtibata geçme hakkı sağlanmalıdır.

(c) Yukarıdaki (a) ve (b) bentlerinde yazılı gerekçelerle yapılan bir başvuru reddedilmişse buna karşı itiraz etme hakkı,

(d) İtiraz kabul edilirse verinin silinmesi, değiştirilmesi veya düzeltilmesini isteme hakkı temin edilmelidir.

8- Hesap verebilirlik: Veri öznelerinin veri toplayıcılarına karşı yukarıdaki ilkeler çerçevesinde hesap sorabilmeleri mümkün olmalıdır.

Mahremiyet Rehber İlkelerinin ardından, 1985 yılında, OECD üye ülke Bakanları tarafından "Sınır Ötesi Veri Akışları" ile ilgili bir bildiri kabul edilmiştir.[113] Bildiri, ticari, bilimsel ve teknolojik veri değişimi, şirket içi veri akışı (intracorporate flow) gibi sınır aşan kişisel veri trafiğine ilişkin politika alanlarına değinmektedir.

OECD, 1998'de Ottawa'daki Bakanlar Konferansında[114] ise bu kez global ağlarda mahremiyetin korunması taahhüdü ile bu alanda gelecekte yapılacak çalışmaları içeren bir bildiriyi kabul etmiştir.[115] Bu bildiri ile, global ağlarda güveni tesis etmek ve kişisel veri transferinde gerekli olmayan sınırlamaları kaldırmak amaçlanmaktadır. Bildiride, ayrıca, teknoloji yansız ilkeleri ile OECD Mahremiyet Rehber İlkelerin (1980) her tür ortamdaki kişisel verilerin toplanması ve tutulması konusunda uluslararası uzlaşıyı temsil etmesi ve mahremiyet koruma alanında bir referans olarak kabulüne devam edilmesi kararlaştırılmıştır.

3.2.2. Avrupa Konseyi

Mahremiyet hakkı, Avrupa Konseyi Parlamenterler Meclisinin 428 (1970) sayılı kararı ile "bireyin, hayatını minimum dış müdahaleyle yaşaması hakkı" olarak

[113] OECD, "Declaration on Transborder Data Flows". 2008.
[114] "A Borderless World: Realising the Potential of Global Electronic Commerce" konulu konferans.
[115] OECD, "Ministerial Declaration on the Protection of Privacy of Global Networks". 1998.

tanımlanmaktayken, Konseyin 1165 (1998) sayılı sonraki Kararında, bu tanıma "kişinin kendisiyle ilgili verileri kontrol hakkı" da eklenmiştir.

1973 ve 1974 yıllarında Avrupa Konseyi Bakanlar Komitesi özel sektörde ve kamu sektöründe elektronik veri bankaları karşısında kişilerin mahremiyetinin korunması hakkında iki karar (resolution) kabul etmiştir. Her iki karar da, Avrupa Konseyi üyesi ülkelerde verinin toplanmasında, veri kalitesinin sağlanmasında ve kişisel verilerin işlenmesinde kişinin bilgi edinme hakkının kabul edilmesini tavsiye etmektedir. Bu çerçevede, Konsey, bireyin "kontrol etme hakkını" bilgi edinme hakkı ile somut hale getiren bir başlangıç yapmıştır.

Türkiye'nin 1949 yılında katıldığı Avrupa Konseyi, 1980 yılında sınır ötesi veri işleme ile ilgili uluslararası alanda mahremiyetin korunmasına yönelik bir sözleşme kabul etmiştir. Avrupa Konseyi, 1981 yılında ise veri koruma alanında ilk uluslararası hukuk belgesi olan "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunması Hakkında Sözleşme"yi (108 no'lu Sözleşme) imzaya açmıştır. 2001 yılında bu Sözleşmeye ek olarak "Denetleyici Makamlar ve Sınırötesi Veri Akışına İlişkin Protokol" (181 no'lu Ek Protokol) kabul edilmiştir. Veri Koruma Hukukunda oldukça önemli bir yere sahip olan bu Sözleşmeler aşağıda incelenmektedir.

Avrupa Konseyi, veri korumanın çerçevesini çizen bu Sözleşmeler dışında, sonraki yıllarda veri koruma kurallarını sektörel bazda ele aldığı çeşitli tavsiye kararları da kabul etmiştir. Tıbbi veri bankaları (1981), bilimsel araştırma ve istatistik (1983), doğrudan pazarlama (1985), sosyal güvenlik (1986), elektronik ödeme ve diğer işlemler (1990), verilerin kamu kuruluşlarınca üçüncü kişilere açıklanması (1991), kişisel verilerin telekomünikasyon alanında korunması (1995), tıbbi verilerin korunması (1997), internette özel hayatın gizliliğinin korunması (1999) bunlardan birkaçıdır. Konseye üye gelişmiş devletlerden çoğu, bu tavsiye kararlarını takiben, özel olarak yasaları bulunduğu halde, konuları bu kez sektör bazında yeniden düzenlemişlerdir. Türkiye için hazırlanan KVKK Tasarısında ise, sektörel bazda bir yaklaşımın Tasarının hacmini çok fazla genişleteceği düşünülerek bu sektörel tavsiye kararlarında yer alan ilkelerin bir kısmı dikkate alınmış olmakla birlikte, esasında kişisel veri korumaya ilişkin çerçeve nitelikte genel hükümler tasarlanmıştır. Söz

konusu tavsiye kararlarında yer alan ilkelerin ise ilgili kurum, kuruluş ve meslek birlikleri tarafından Tasarının yasalaşmasından sonra düzenlenmesinin daha uygun olacağı değerlendirilmiştir.[116] Bu tercih, Kanunun uygulama alanının daha kapsamlı olmasını sağlaması ve sektörel düzenleme yapılmasını, sektör ihtiyaçlarına göre ilgili kurum ve kuruluşlara bırakması nedeniyle olumlu olarak değerlendirilmektedir.

3.2.2.1. 108 sayılı Sözleşme

Avrupa Konseyi'nin 28 Ocak 1981 tarihinde Strazburg'ta imzaya açmış olduğu "Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşme" (108 sayılı Sözleşme), veri koruma alanındaki ilk uluslararası hukuk belgesidir.[117] Bu Sözleşme, 1 Ekim 1985 yılında yürürlüğe girmiştir. Ülkemiz, anılan Sözleşmeyi 28 Ocak 1981 tarihinde imzalamış; ancak onaylayarak iç hukukta geçerli hale getirmemiştir. Zira, söz konusu Sözleşmenin 4'üncü maddesi gereğince, Sözleşmenin onaylanabilmesi için, imzalayan devletin, Sözleşmede öngörülen ilkeler çerçevesinde bir yasa kabul etmesi zorunludur. Bu nedenle KVKK Tasarısının yasalaşması, söz konusu Sözleşmenin onaylanabilmesi için gerekli ön şartın sağlanmasının da aracı durumundadır.

Sözleşme, genel olarak bilgi edinme hak ve özgürlüğünün sınırlardan bağımsız olması ve kişisel verilerin sınırlar ötesine iletilmesinin yoğunluk kazanması karşısında, özel hayatın ve mahremiyetin korunması gerektiği düşüncesiyle ortaya çıkmıştır. Bu çerçevede Sözleşme, kişisel verilerin tamamının veya bir kısmının otomatik yöntemlerle kaydı, bu verilere mantıksal veya aritmetik bazı işlemlerin uygulanması, verilerin değiştirilmesi, silinmesi gibi işlemeler karşısında bireyi korumaktadır.

Otomatik bilgi işleme durumlarında, bu korumanın gerçekleştirilebilmesi için Sözleşme'nin 5'inci maddesinde belirlenen temel ilkelere göre veriler:

- Meşru ve yasal yoldan elde edilmeli ve ancak bu şekilde işleme tabi tutulmalıdır;

[116] KVKK Tasarısı, Genel Gerekçe, s. 5.
[117] Sözleşmenin Türkçe metni için bkz. <http://www.avrupakonseyi.org.tr/antlasma/aas_108_p.htm>

- Belli ve meşru amaçlar için kaydedilmeli ve bu amaca aykırı şekilde kullanılmamalıdır;
- Kaydedildikleri amaca uygun ve bu amaçla ilgili bilgiler olmalıdır;
- Doğru ve güncellenebilir olmalıdır;
- İlgili kişilerin kimliklerinin tespit edilmesine izin verecek şekilde tutulmalı ve tutuldukları nihai amaç gerçekleşene kadar muhafaza edilmelidir.

Bu temel ilkelerin dışında, Sözleşme iç hukukta güvence sağlanmadıkça, hassas veri olarak kabul edilen ırk, siyasi düşünce, dini ve cinsel yaşamla ilgili bilgilerin otomatik işlemeye tabi tutulmaması gerektiğini, bu amaçla uygun güvenlik önlemlerinin alınması gerektiğini belirtmektedir. Öte yandan, Sözleşmede kişi bakımından da birtakım güvencelerin sağlanması gerektiği vurgulanmaktadır. Bu güvenceler; kişilerin kendileri hakkında tutulan bilgilere erişebilme, bunları güncelleyebilme, hukuka aykırı işleme halinde bu bilgilerin silinmesini isteme, söz konusu talepler yerine getirilmez ise kanun yoluna başvurabilme olarak ifade edilmektedir. Söz konusu hakların kullanılması, ancak devlet güvenliğinin korunması, kamu güvenliği, suçların önlenmesinin zorunluluk olduğu veya veri sahibinin ya da diğer kişilerin hak ve özgürlüklerini korumak için sınırlandırılabilir.

Sözleşme tarafları, bu Sözleşme ile karşılıklı işbirliği ve yardımda bulunmayı taahhüt etmekte olup, bu sebeple her ülkede tayin edilerek Avrupa Konseyine bildirilecek merciler, veri koruma ile ilgili olarak devlet güvenliği ve kamu düzenine ilişkin hususlar dışında, kendi iç hukukları ve idari uygulamaları ile ilgili talep üzerine diğer ülkelere bilgi verecektir.

Sözleşme ile, Avrupa Konseyi nezdinde bu Sözleşmeye taraf ülkelerde uygulamanın kolaylaştırılması ve işbirliği sağlamak üzere, bu ülkelerin tayin edeceği bir asıl ve bir yedek temsilciden oluşacak bir Danışma Komitesi kurulmaktadır. Avrupa Konseyi üyesi olduğu halde bu Sözleşmeye taraf olmayan ülke temsilcileri de bu Komiteye gözlemci sıfatıyla katılabilecektir. Ülkemizin de KVKK'nın yasalaşmasını müteakip, bu Sözleşmeyi bir an evvel onaylayarak iç hukukuna uyumlaştırması faydalı olacaktır.

3.2.2.2. 181 sayılı Sözleşme

Avrupa Konseyi'nin 2001 yılında kabul ettiği "Kişisel Verilerin Otomatik Yöntemlerle İşlenmesi, Denetleyici Otoriteler ve Sınır Ötesi Veri Akışları Hakkında Bireylerin Korunması Sözleşmesine Ek Protokol (181 sayılı Sözleşme)", bu Protokole taraf olan ülkelerde, kişisel veri koruma uygulamalarından sorumlu bağımsız ve özerk bir denetleyici otorite (kurum) oluşturulması ve yurtdışına veri transferinde standart belirlenmesi gerekliliğini öngörmektedir. Bu ek Protokolün üçüncü maddesinin birinci fıkrası uyarınca, bu Protokolün imzalanabilmesi ve iç hukukta uygun bulunması, 108 sayılı Sözleşmenin imzalanmış olması ve iç hukukta uygun bulunması şartına bağlıdır. Türkiye, bu ek Protokolü, tıpkı 108 sayılı Sözleşme gibi, 8 Kasım 2001 tarihinde imzalamış; ancak iç hukukunda onaylamamıştır.[118] Yukarıda ifade edilen madde gereği, 108 nolu Sözleşmenin iç hukukta onaylanması, bu Sözleşmenin de onaylanmasının ön şartıdır.

181 sayılı Ek Protokol, taraf ülkelerde kurulacak denetleyici otoritelerin özellikle araştırma ve soruşturma yapma, bununla birlikte kişisel veri mahremiyetinin ihlal edildiği bazı durumları yetkili yargı merciinin önüne getirme yetkileriyle donatılması gerektiğini vurgulamaktadır. Bu otoriteler ayrıca, kişisel verilerin işlenmesi ile ilgili iddia ve itirazlara bakacaktır. Bu mercilerin verdikleri kararlara karşı mahkemelere başvuru hakkı saklı olmalıdır.

Bu Sözleşmeye göre; Sözleşmeye taraf olmayan ülkelere kişisel veri transfer edilirken, o ülkede yeterli koruma düzeyinin olup olmadığına bakılmalıdır. Kişisel verinin sınır ötesine transferi, ancak veri sahibinin özel bir yararının olması, kamu yararı ya da meşru bir yararın bulunması halinde kolaylaştırılmalıdır.

Halihazırda 108 No'lu Avrupa Konseyi Sözleşmesi ve ek'i Protokolü imzalayarak, ülkemiz gibi iç hukukunda onay mekanizmasını harekete geçirmeyen 3

[118] 181 Sayılı Ek Protokolün imzalanması, onaylanması ve iç hukukta yürürlüğe girmesi hakkında ülke durumları için bkz.
<http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=181&CM=1&DF=&CL=ENG>

ülke (Ukrayna, Türkiye, Rusya); ve hem sözleşmeyi imzalayan hem de bunu iç hukukunda onaylayan 41 ülke bulunmaktadır.[119]

3.2.2.3. 185 sayılı Siber Suç Sözleşmesi

Milli yasalar ve özellikle ceza yasaları, genel olarak sadece ülke sınırları içinde uygulanabilmektedir. Buna yasaların ülkeselliği (territoriality) ilkesi denmektedir. Oysa siber uzayda işlenen bir suçun hangi ülkede işlendiğinin belirlenebilmesi için, bazı yeni hukuksal tanımların ve kabullerin yapılması ve üzerinde anlaşılması gerekmektedir. Bazen bir yasadışı eylemin meydana geldiği ülke ile sanığın vatandaşlık bağı ile bağlı olduğu ülke farklı olabilmekte, hatta yasadışı eylemi işleyen kişi üçüncü bir ülkede yaşayabilmektedir. Bu durumda söz konusu eylemin "suç" olup olmadığının hangi ülkenin yasasına göre belirleneceği ve yasadışı eylemle ilgili adli kovuşturma, yargılama ve cezalandırmanın hangi ülkede yapılacağı sorunları ortaya çıkmaktadır. Siber uzayda işlenen suçlarda, çoğu kez, suçun işlendiği, suçlunun yaşadığı ve vatandaşı olduğu ülkeler ayrı ayrı ülkeler olabilmektedir. Diğer taraftan yasadışı eylemin siber uzayda işlenmiş olması, bu fiilin kimin tarafından ve nerede yapıldığının *ve sonuçlarının nerelerde etkili olduğunu saptamak bugünkü teknolojinin sağladığı araçlarla zor da olsa büyük ölçüde mümkün bulunmakla beraber, bunun için ilgili ülke makamlarının işbirliği yapmaları ihtiyacı ortaya çıkmaktadır.*[120]

Siber suçlarla etkin bir şekilde mücadele söz konusu sorunları giderebilmek için, Avrupa Konseyi uluslararası geçerliliği olan bir sözleşme için çalışmalara başlamış ve bu çalışmaların sonucunda, 23 Kasım 2001 tarihinde 185 numaralı Siber Suç Sözleşmesi'ni[121] imzaya açmıştır. Bu Sözleşme, siber uzayda işlenen suçların kim tarafından, nerede işlendiğini ve sonuçlarının nerelerde etkili olduğunu saptamak üzere ABD'nin de katkı ve görüşleri alınarak hazırlanmıştır. Bu Sözleşmenin en önemli özelliği, uluslararası ortamda siber suçlara ilişkin müşterek bir yaklaşım

[119] 108 sayılı Sözleşmede Avrupa Konseyi üyesi ülkelerin imza durumlarını gösterir tablo için bkz. <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=108&CM=1&DF=4/28/2009&CL=ENG>

[120] Turhan, 2006:98

[121] Council of Europe, "Convention on Cybercrime". 2001. <http://conventions.coe.int/treaty/en/treaties/html/185.htm>

belirleyerek tarafların bu suçlara ilişkin benzer nitelikte düzenlemeler yapmasını gerektirmesi, bu yolla siber suçlara yönelik soruşturmalarda suça yönelik eylem ve suçun sahibini belirlemede bu Sözleşme hükümlerine dayalı olarak işbirliği yapılmasının kolaylaşmasıdır.

Türkiye, Siber Suç Sözleşme'sini 10 Kasım 2010 tarihinde imzalayarak taraf olmuştur. Bundan sonraki aşamada Türkiye'nin yapması gereken, ulusal düzenlemelerin bu Sözleşme hükümlerine uyumunun sağlanması ile siber suçlarla uluslararası mücadelede daha etkin işbirliği olanaklarının geliştirilmesi olmalıdır.

3.2.3. Birleşmiş Milletler

Veri koruma hukukuna ilişkin etkinliği olan bir diğer uluslararası merci de Birleşmiş Milletler (BM) dir. Bir üst hukuk normu olarak BM İnsan Hakları Evrensel Beyannamesinin 12'nci maddesinde, kişilerin mahremiyet, aile ve konut dokunulmazlığı güvence altına alınmış olup, bu haklara gelecek olası saldırılarda kişilerin hukuki korumadan yararlanma hakkı hükme bağlanmaktadır:

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

BM'nin 16 Aralık 1966 tarihli Sivil ve Siyasi Haklar Hakkında Uluslararası Sözleşmesi'nin 17'nci maddesinde de aynı koruma hükmü yer almaktadır.[122] 1990 yılında ise BM kişisel veri dosyalarının bilgisayar aracılığıyla işlenmesinde genel tavsiye ilkeleri yayımlamıştır.[123] BM Antlaşması'nın (BM Şartı-1945) 10'uncu maddesinin[124] BM Genel Kurulu'na, BM üyelerine tavsiyede bulunma yetkisi vermesi nedeniyle hazırlanan bu Rehber İlkeler, üye ülkelerin, bilgisayarla kişisel veri işleme konusunda yapacakları düzenlemelerde ortak olarak dikkate alınacak olup, bu ilkelerin uygulama usullerinin belirlenmesi üye ülkelerin inisiyatifindedir.

[122] International Covenant On Civil And Political Rights,1966.
[123] United Nations, "Guidelines Concerning Computerized Personal Data Files (Resolution 45/95)". 1990.
[124] BM Şartı, md. 10 "Genel Kurul, işbu Antlaşma kapsamına giren ya da işbu Antlaşma'da öngörülmüş organlardan herhangi birinin yetki ve görevlerine ilişkin bütün sorunları ya da işleri görüşebilir ve 12'nci madde hükümleri saklı kalmak koşuluyla, bu tür sorun ya da işler konusunda Birleşmiş Milletler üyelerine veya Güvenlik Konseyi'ne veya hem örgüt üyelerine hem de Güvenlik Konseyi'ne tavsiyelerde bulunabilir."

Türkiye'nin BM'ye üye olması nedeniyle (24 Ekim 1945) ülkemizde kişisel verilerle ilgili olarak çıkarılacak düzenlemelerin BM Rehber İlkelerine uyumlu olması gerektiği dikkate alınmalıdır.

BM İnsan Hakları Komisyonu'nun 1992 yılında kabul ettiği ve Paris İlkeleri olarak bilinen "İnsan Haklarının Korunması ile İlgili Ulusal Kurumların Statü ve Görevleri" hakkındaki ilkeleri ise, temel insan haklarından olan mahremiyet ve kişilik ile ilgili kurumsal yapı incelemesi bölümünde ele alınacaktır (bkz. Bölüm 4).

3.2.4. Dünya Ticaret Örgütü

Mahremiyet ve veri koruma alanının insan hakları ile ilgili bir konu olması nedeniyle Dünya Ticaret Örgütü'nün (DTÖ) bu alanda uluslararası bağlayıcılığı olan kapsamlı çalışmaları bulunmamaktadır. Bununla birlikte, DTÖ tarafından yönetilen ve hizmetlerde serbest ticareti teşvik eden çok taraflı bir antlaşma olarak Hizmet Ticareti Genel Antlaşması (GATS)'nın 14'üncü maddesinde[125] üye ülkelerin "kişisel verilerin işlenmesi ve yayılması karşısında kişilerin mahremiyetinin korunması ve kişisel bilgilerin tutulduğu dosya ve kişisel hesapların gizliliğinin korunması" için gerekli tedbirleri alabileceği hükme bağlanmaktadır.

AB'nin kişisel verilerin korunması alanındaki düzenlemelerinin, hizmet ticaretini etkileyebilecek nitelikte olması nedeniyle, bu düzenlemelerin DTÖ kapsamında özellikle gelecekteki e-ticaret faaliyetlerinde daha fazla rol oynayacağı düşünülmektedir.

3.2.5. Avrupa Birliği

Avrupa Birliği'nin (AB) temel amaçlarından olan malların, kişilerin, hizmetlerin ve sermayenin serbest dolaşımının sağlanabilmesinde kişisel verilerin toplanması ve işlenmesi bir zorunluluk arz etmektedir. Ancak, dünyanın öbür ucunda, hiç tanımadığınız birisi tarafından dolandırılmak ve bu eylemin nasıl yapıldığını bile bilememek, bu durum karşısında hukuken korunma şansının çok az olması, özellikle AB üyelerince tolere edilemeyecek nitelikte kabul edilmektedir. Bu

[125] WTO. "General Agreement on Trade in Services". 2009.

nedenle AB, yeni teknolojilerin gelişmesiyle geleceğin bilgi toplumunda da yeni politikaları ve düzenlemeleri ile lider rol üstlenmek istemektedir.[126]

Amsterdam Antlaşması'nın amacı da, bir taraftan AB vatandaşları ve üçüncü ülke uyruklu şahısların serbest dolaşımını sağlarken, diğer taraftan örgütlü suçlar ve terörizmin her türüyle mücadele etmek suretiyle kamu güvenliğini güvence altına almak, tedricen bir "özgürlük, güvenlik ve adalet" alanı yaratmaktır. AB Konsey ve Komisyonu'nun 3 Aralık 1998 tarihli Eylem Planı'nda "özgürlük" alanı, genel olarak kişilerin serbest dolaşımının güvence altına alınması, buna karşılık başta *özel hayata saygı ve özellikle kişisel verilerin korunması olmak üzere* temel hakların korunması ve her türlü ayırımcılıkla mücadele olarak tanımlanmaktadır. "Güvenlik" alanı ise başta terörizm, insan ticareti, çocuklara karşı işlenen suçlar, uyuşturucu kaçakçılığı, yolsuzluk ve sahtecilik olmak üzere suçla mücadeleyi kapsamaktadır.[127]

Hukuka uygun ve yeknesak veri dolaşımı ve işlenmesi AB'nin direktif, tüzük, anlaşma ve diğer normatif kuralları ile düzenlenmektedir. Veri koruma ile ilgili AB düzenlemeleri konu bazında kendi içinde sınıflandırılacak olursa;

- Genel olarak kişisel verilerin korunması (95/46/AT Direktifi, 2001/497 ve 2004/91 sayılı Kararlar),
- Kişisel verilerin telekomünikasyon alanında korunması (2002/58/AT ve 2006/24/AT Direktifleri),
- Topluluk kurum ve kuruluşlarınca veri korunması (45/2001 sayılı Tüzük)
- Bilgi güvenliği (Konsey Kararları[128])
- MAT aracılığıyla veri korumasını teşvik eden düzenlemeler

olmak üzere 5 bölüm altında incelenebilir. Bu alanda temel sayılabilecek düzenlemeler aşağıda Tablo 3.1'de özetlenmektedir:

[126] RISEPTIS, 2008:3
[127] AB Müktesebatının Üstlenilmesine İlişkin Türkiye Ulusal Programı. Cilt 1. 2001.
[128] 31 Mart 1992 tarihli ve 92/242/EEC sayılı bilgi güvenliğine ilişkin Konsey Kararı, 24 Şubat 2005 tarihli ve 2005/222/JHA sayılı bilgi sistemlerine karşı saldırılara ilişkin Konsey Çerçeve Kararı (AB Resmi Gazetesi L 69 16.03.2005), Avrupa Parlamentosu ve Konseyin 460/2004 sayılı ve 10 Mart 2004 tarihli Avrupa Ağ ve Bilgi Güvenliği Ajansının Kurulmasına İlişkin Tüzüğü (ENISA)

Tablo 3.1. AB'nin Veri Koruma Alanına İlişkin Temel Hukuki Belgeleri

Düzenlemenin Adı	İçeriği
Kişisel Verilerin İşlenmesi ve Bu Verilerin Serbest Dolaşımı Hakkında Bireylerin Korunması Hakkında Avrupa Parlamentosu ve Konseyin 95/46/AT Sayılı Direktifi (Veri Koruma Direktifi)	Kişisel verilerin korunması ile ilgili temel çerçeve düzenlemedir.
2001/497/AT sayılı Komisyon Kararı	15 Haziran 2001tarihli bu Karar, 95/46 sayılı Veri Koruma Direktifi altında üçüncü ülkelere kişisel veri transferi ile ilgili sözleşme hükümleri hakkındadır.
45/2001 Sayılı Kişisel Verilerin Topluluk Kurum ve Kuruluşları Tarafından İşlenmesi Bağlamında Bireylerin Korunması ve Bu Verilerin Serbest Dolaşımı Hakkında Tüzük	Birliğin kurum ve organlarının kişisel verileri korumak konusunda uyacakları esasları belirlemektedir. Birlik kurum ve kuruluşlarının tüm veri işleme operasyonlarının ve bu Tüzükle kurulan bağımsız "Avrupa Veri Koruma Denetçisi" vasıtasıyla izleneceği hüküm altına alınmıştır.
2004/915/AT sayılı ve 2001/497/AT sayılı kararları değiştiren Komisyon Kararı	Kişisel verilerin üçüncü ülkelere transferine ilişkin sözleşmelerde alternatif standart ifadelere ilişkin karardır.
97/66/AT Sayılı Telekomünikasyon Sektöründe Kişisel Verilerin İşlenmesi ve Mahremiyetin Korunması Hakkında Avrupa Parlamentosu ve Konsey Direktifi	Elektronik Haberleşme alanında kişisel veri korumasını düzenlemektedir.
Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Avrupa Parlamentosu ve Konseyin 2002/58/AT sayılı Direktifi (Elektronik Haberleşme ve Gizlilik Direktifi)	
2006/24/AT Sayılı Kamu Elektronik Haberleşme Hizmetlerinin Sağlanması veya Kamu Haberleşme Ağları Çerçevesinde Üretilen veya İşlenen Verilerin Saklanmasına İlişkin 2002/58 Sayılı Direktifi Değiştiren Direktif	2002/58/AT sayılı Direktifte bazı değişiklikler yapmakta ve veri saklanmasına ilişkin hükümler ihdas etmektedir.
92/242/AET sayılı Konsey Kararı	Bilgi güvenliği ile ilgilidir.
2005/222/JHA sayılı Konseyin Çerçeve Kararı	Bilgi Sistemlerine yönelik saldırılar hakkında çerçeve hükümler içermektedir.
Avrupa Parlamentosu ve Konseyin 460/2004 sayılı Tüzüğü	Avrupa Ağ ve Bilgi Güvenliği Ajansını (ENISA) kuran Tüzüktür.

Kaynak: European Commission, "Justice and Home Affairs, Data Protection" ait http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm İnternet sayfasından bu çalışma kapsamında derlenmiştir.

3.2.5.1. 95/46/AT sayılı Veri Koruma Direktifi (VKD)

3.2.5.1.1. Genel bilgiler

AB'nin kişisel verilerin korunmasında temel referans belgesi olan Veri Koruma Direktifi (VKD)[129], kişisel verilerin işlenmesi nedeniyle bireylerin korunması ve bilgilerin serbest dolaşımını düzenlemektedir. Bu Direktif, AB'nin daha önce kurum olarak çalışmalarına aktif katılım sağladığı, kişisel verilerin korunmasına ilişkin ilk uluslararası hukuk belgesi olan Avrupa Konseyi'nin 108 sayılı Sözleşmesinin devamında, AB üyesi ülkelerin veri koruma düzenlemeleri arasındaki farklılık ve çelişkileri gidererek uyumu sağlamak üzere açık ve kalıcı bir düzenleme yapmak istemesi ile kabul edilmiştir. Direktif, üye ülkelerde kişisel verilerin korunmasından sorumlu bir bağımsız ulusal otoritenin kurulmasını öngörmektedir. Ayrıca, bireylerin mahremiyetini yüksek koruma altına almak ile, bilginin serbest dolaşımı arasında bir denge sağlamaya çalışmaktadır.

Mevzuat isminin "Veri Koruma Direktifi" olarak geçmesi, kanunun yorumlanmasında bazı yanlış anlamaları beraberinde getirdiği, "koruma"dan kastın verinin başka kurumlarla hiçbir şekilde paylaşılmaması gibi anlaşıldığı görülmektedir. Bu nedenle veri koruma yasalarının anlaşılması en zor düzenlemelerden olduğu söylentisi de mevcuttur. AB Komisyonu, bu yanlış anlaşılmaların azaltılması için ve veri koruma alanında yeni çalışmalar yapmak üzere, VKD'nin 29'uncu maddesinde, kişisel verilerin işlenmesi ve bireylerin korunması konusunda özel çalışmalar yapan bir çalışma grubu kurmuştur. Grup, kısaca "Madde 29 Çalışma Grubu"[130] olarak anılmakta olup, AB'de ve diğer ülkelerde koruma düzeyi konusunda danışmanlık yapmaktadır. Bu grubun çalışmaları sonucunda sınır ötesine veri transferinde ülkeler arasındaki koruma düzeyleri arasında karşılaştırma yapmak mümkün hale gelmiştir. Grubun ABD ile müzakereleri sonucunda ise veri koruma alanında sıkça duyulan "Güvenli Liman İlkeleri" ortaya konulmuştur.

---

[129] Direktifin İngilizce tam metni için bkz.
<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML>

[130] İngilizcesi, *Article 29 Data Protection Working Party* olan bu grup hakkında ayrıntılı bilgi için bkz. <http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm>.

VKD'nin kapsamı, OECD Rehber İlkelerinin çerçevesinden daha geniş olarak düşünülmüştür. VKD'de, Rehber İlkelere ilave olarak, hassas veriler, verilerin açılması (açıklanması) halleri, kayıt hükümleri, ticari iletileri reddetmeye ilişkin opt-out (liste dışı) olma hakkı ve düzeltme hakkına ilişkin özel hükümler bulunmaktadır.

Avrupa Birliği Antlaşması olarak da bilinen Maastricht Antlaşması'nın (1993) (7a) maddesi uyarınca; malların, kişilerin, hizmetlerin ve sermayenin serbest dolaşımına imkan tanıyan bir iç pazarın oluşturulması ve işleyebilmesi, kişisel verilerin bir üye devletten diğerine serbestçe dolaşımının yanında, bireylerin temel haklarının korunmasını da gerektirmektedir. Bu çerçevede, VKD, bir taraftan kişisel verilerin gerekli durumlarda dolaşımını sağlarken, diğer taraftan bu verilerin toplanması, depolanması, kullanılması, paylaşılması, değiştirilmesi gibi verinin işlendiği her tür işlemin nasıl yapılması gerektiğine ilişkin esas ve usulleri belirleyen bir çerçeve direktiftir. Bu kapsamda, VKD ile gerçek kişilerin kişisel bilgilerinin işlenmesi neticesinde bu kişilerin zarara uğramalarının engellenmesi ve temel hak ve hürriyetleri ile mahremiyet haklarını koruyarak güvence altına alınması amaçlanmaktadır.

Bu çerçevede VKD, sistematik olarak yedi temel bölümden oluşmaktadır. Bu bölümler sırasıyla, genel hükümler, hukuka uygunluk sebepleri, hukuki tedbirler, sorumluluk ve yaptırımlar, kişisel verilerin üçüncü ülkelere transferi, davranış kuralları, denetleyici (teftiş) otorite ve topluluk düzeyinde uygulama tedbirleridir.

Kural olarak, bir AB Direktifi ile bireylere doğrudan bir hak ihdas ediliyorsa, Direktifin bir üye ülkede iç hukuka uygulanması beklenmeksizin, o ülkedeki AB vatandaşları direktife dayanarak mahkemeden bu hakkın korunmasını talep edebilmektedirler. VKD, bireye sağladığı "mahremiyet hakkı" nedeniyle hak ihdas edici niteliktedir. Bu sebeple, AB üyesi olan ancak henüz Direktifi uyumlaştırmamış olan bir ülkenin vatandaşları da, kendi ülkelerinde mahkemeden bu haklarına saygı gösterilmesini ve haklarının uygun araçlarla korunmasını isteyebilmektedirler. Direktifle kişilere tanınan veriye erişim, işlemeye itiraz ve mahkemelerde dava açma hakkı bu tür haklara örnek olarak gösterilebilir.

Mahremiyet hakkı, başta basın ve medyanın ifade özgürlüğü olmak üzere zaman zaman diğer bazı haklarla çelişki yaratabilir; bu nedenle üye ülkeler veri koruma kanunlarına bu farklı, fakat eşit düzeydeki temel haklar arasında nasıl bir denge kuracaklarına kendileri karar verirler.[131]

VKD, üye ülkelerce uyumlaştırılırken, ülkeler, Direktifle belirlenen temel ilkelerle tesis edilen koruma önlemlerinden daha düşük düzeyde koruma sağlayacak düzenleme yapamayacaklardır. Ancak, Direktifle belirlenmiş temel ilkeler çerçevesindeki koruma düzeyinin daha üstüne çıkmak ülkelerin inisiyatifine bırakılmıştır.

VKD ile oluşturulmak istenen koruma, kişisel verilerin işlenmesinin şartlarını düzenleyerek *önleyici* olmayı hedeflemektedir. Amaç, bir saldırının ortaya çıkması halinde sağlanacak korumadan ziyade, olası saldırılara karşı önleyici niteliğe sahip bir yapının oluşturulmasıdır.[132]

3.2.5.1.2. Veri Koruma Direktifinin kapsamı

VKD, kapsam olarak otomatik olan veya olmayan araçlarla, gerçek kişilere ait kişisel verilerin işlendiği durumlara uygulanmaktadır.[133] Bu Direktif, kamu güvenliği, savunma ve devletin güvenliğine ilişkin işlemelerde ve devletin ceza hukuku alanındaki faaliyetleri gibi Topluluk hukuku dışında kalan faaliyetlerinde uygulanmayacaktır. Benzer şekilde, gerçek bir kişinin tamamen kişisel olan veya evi ve ailesiyle ilgili olan veri işlemelerinde VKD hükümleri uygulanmayacaktır.[134] Örneğin Ceza Kanununda tanımlı bir suçtan bir kişinin kovuşturulması esnasında, o kişiye ait kişisel veriler mahkemece ilgili makamlardan istenebilecek, bu verilerin işaret ettiği maddi gerçeğe dayalı olarak hüküm tesis edilebilecektir. Bunun gibi, bir kişiye ait kişisel verileri içeren bir elektronik günlük veya kişinin ailesi ve arkadaşlarına ait bilgilerin yer aldığı resim, bilgi ve dosyalar veri işleme olarak bu

[131] Europe Direct, 2000.
[132] Başalp, 2004:31
[133] Verilerin otomatik araçlarla işlenmesi, kişisel verilerin otomasyon sistemleri kullanılmak suretiyle işlenmesidir.
[134] VKD, md. 3'te belirtilen bu istisnalar, kişilerin özel hayatlarında, kendileriyle veya aileleriyle ilgili olarak tuttukları veya çeşitli şekillerde işledikleri verilerle ilgili veri koruma kurallarına tabi olmalarının engellenmesi için Direktife eklenmiştir. Zira, veri koruma hukukunun felsefesinde mahremiyeti korumak vardır, mahremiyete müdahale ederek o alanı düzenlemek doğru değildir.

Direktif kapsamında değil, bu verilerin kişinin tasarrufu altında olması ve özel hayata ilişkin olması nedeniyle özel hukuk hükümlerine göre değerlendirilecektir.

VKD, teknoloji yansız bir direktiftir. Bu nedenle teknolojik araçlardan bağımsız olarak kişisel verinin işlendiği her tür durumda uygulanma imkanına sahiptir. Örneğin çevrimiçi ortamda kullanıcının İnternette gezinme alışkanlıklarını gizlice kontrol altına alan, kişisel verilerin edinilmesinde ve profil yaratılmasında kullanılabilen çerezler (cookies) gibi programlar için de VKD uygulanabilir niteliktedir.

3.2.5.1.3. Veri Koruma Direktifindeki temel kavramlar

VKD'de yer alan kavramlardan "kişisel veri" daha önce açıklanmıştı (bkz. 1.4. başlıklı bölüm). Bu kavramın dışında, VKD'nin tanımlar başlıklı ikinci maddesinde sırasıyla aşağıdaki kavramlar tanıtılmaktadır.

i) Kişisel verilerin işlenmesi (işleme): Kişisel verilerin otomatik ya da otomatik olmayan araçlar yoluyla toplanması, saklanması, elde edilmesi, değiştirilmesi, okunması, sorulması, kullanılması, başkalarına transfer edilmesi, yayılması ya da hazır bulundurulması için yapılan işlemlerle verilerin kombinasyonu, bloke edilmesi, silinmesi ya da yok edilmesi suretiyle gerçekleştirilen her türlü müdahale "işleme" olarak adlandırılır.

ii) Kişisel veri dosyalama sistemi (dosyalama sistemi): Merkezileşmiş, merkezileşmemiş veya fonksiyonel veya coğrafik esasa dayanarak dağılmış ve belirli kriterlere göre erişilebilir her tür yapılandırılmış kişisel veri dizisine dosyalama sistemi adı verilmektedir. Örneğin, ülkemizde sosyal yardımlardan faydalanacak kişilerin ad-soyad, T.C. kimlik ve sosyal sigorta numaralarının birlikte bulunduğu ortam, kişisel veri dosyası olarak adlandırılabilir. Bununla birlikte, kamuda veya özel sektörde ya da bir istatistik kurumunda bulunan herhangi bir çalışmaya özgü bir araya getirilmiş kişisel veri setleri, topluca veya tek tek birer kişisel veri dosyası olarak nitelendirilebilir.

iii) Veri kontrolörü: Kişisel veri işlemenin amaçlarını ve yöntemini birlikte veya tek başına belirleyen kişi, organ, ajans veya kamu kurumuna veri kontrolörü denilmektedir. Veri kontrolörü, verileri işlerken VKD'de belirlenmiş kurallara

uymakla yükümlüdür. Hukuka aykırı olarak yapılan iş ve işlemlerden veri kontrolörü sorumludur.

iv) Veri işleyicisi: Veri kontrolörü adına kişisel verileri işleyen gerçek veya tüzel kişilere "veri işleyicisi" denilmektedir.

v) Veri öznesinin rızası: Veri öznesinin, karşı tarafa, kendisine ilişkin kişisel verinin işlenmesini özgür iradesiyle kabul ettiğini onaylayan her tür belirlenmiş davranış, işaret veya ifade ile açıklanan irade beyanıdır.

3.2.5.1.4. Veri Koruma Direktifindeki temel ilkeler

VKD'nin benimsemiş olduğu temel ilkelere göre, üye devletler, kişisel verileri;

(a) Adil ve yasalara uygun şekilde işleyecektir.

(b) Bu veriler, belirlenmiş, kesin ve yasal amaçlara göre toplanmış olacak ve ilk toplandıkları amaca aykırı olarak sonraki işlemelere tabi olmayacaktır. Üye devletin gerekli önlemleri alması kaydıyla, söz konusu verilerin ilk toplandıkları amacın dışına çıkarak tarihsel, istatistiksel ve bilimsel amaçlarla sonraki işlenmeleri saklıdır.

(c) Veriler, toplama ve/veya müteakip olarak işleme amaçları için yeterli ve bu işlemlerle ilgili olacak, aşırı olmayacaktır.

(d) Veriler doğru ve güncel olarak tutulacaktır; böylece veri kalitesi sağlanacaktır. Toplanma amaçları veya müteakip işleme için yanlış veya eksik olan verinin silinmesi veya düzeltilmesi için bütün makul adımlar atılacaktır.

(e) Veriler, toplama amacının veya müteakip işlemenin gerektirdiğinden daha uzun süre saklanmayacaktır. Veriler, veriye konu olan kişilerin kimliğinin belirlenmesine müsaade edecek şekilde muhafaza edilecektir. Üye devletler tarihsel, istatistiksel veya bilimsel amaçlarla daha uzun sure muhafaza edilen kişisel veriler için uygun koruma önlemleri belirleyecektir.

3.2.5.2. 45/2001 sayılı Tüzük

AB'nin kurum ve organlarının kişisel verileri korumak konusunda münhasır olarak uyacakları usul ve esasları belirleyen 45/2001 sayılı Tüzük de OECD Rehber İlkeleri ile paralel olarak, kişisel verilerin sadece haklı sebeple ve hukuka uygun olarak işlenmesi; belirli, açık ve hukuka uygun sebeplerle toplanması ve bu sebeplerin gerektirdiği amaçlar dışında işlenememesini öngörmektedir. Tüzükte ayrıca, her bir AB kurum ve kuruluşunda bir veri koruma görevlisinin tayin edilmesi, bu görevlinin veri koruma uygulamalarının doğru olup olmadığını izlemesi ve AB kurumları düzeyinde veri korumadan sorumlu olan Avrupa Veri Koruma Kurumuna bildirmesi öngörülmektedir. Avrupa Veri Koruma Kurumu, yaklaşık 40 kişilik bir personeli olan ve Topluluk kurum ve kuruluşlarının uygulamalarını değerlendiren denetleyici bir oluşumdur. Kurum, özellikle kişisel verilerin kurallara aykırı biçimde kullanılması itirazları için şikayet mercii olarak düşünülmüştür. Bu yapı, ulusal düzeydeki veri ihlalleri ile değil, yalnızca AB kurum ve kuruluşlarının veri koruma uygulamaları ile ilgilenmektedir.[135]

3.2.5.3. 97/66/AT ve 2002/58/AT Direktifleri

VKD'nin elektronik haberleşme sektörüne ilişkin hususları düzenlemek üzere 1997 yılında Avrupa Parlamentosu ve Konseyi 97/66/AT sayılı Telekomünikasyon Sektöründe Kişisel Verilerin İşlenmesi ve Mahremiyetin Korunması Hakkında Avrupa Parlamentosu ve Konsey Direktifini kabul etmiştir. Bu Direktif; elektronik haberleşme alanında yeni çerçeve hükümler koyan ve bu sektördeki gelişmeleri[136] yansıtan 2002/58/AT sayılı Elektronik Haberleşme ve Gizlilik Direktifi ile yürürlükten kaldırılmıştır.

Ülkemizde telekomünikasyon alanında kişisel verilerin korunması ile ilgili ikincil düzenlemeler yapılmıştır. Ancak, çerçeve nitelikte bir veri koruma kanunu çıkmadan yönetmelik yapılması bazı çevrelerce eleştirilmektedir.

---

[135] Ayrıntılı bilgi için bkz. European Data Protection Supervisor.
<http://www.edps.europa.eu/EDPSWEB/edps/Home/EDPS> Erişim tarihi: 25 Kasım 2009.

[136] Spam, çerezler gibi unsurların kişilerin opt-in yani işlem öncesi açık ve belirlenebilir rızasına bağlı olması, VKD'de eksik kalan diğer hususları düzenlemek ve Telekom Paketi olarak adlandırılan genel çerçeve, erişim ve arabağlantı, yetkilendirme ve lisanslama ve evrensel hizmet olmak üzere dört direktif daha içeren Paket ile uyum amaçlı gelişmeler.

3.2.5.4. 2006/24/AT Direktifi

2006/24/AT sayılı Kamu Elektronik Haberleşme Hizmetlerinin Sağlanması veya Kamu Haberleşme Ağları Çerçevesinde Üretilen veya İşlenen Verilerin Saklanmasına İlişkin Direktif, telekomünikasyon sektöründe kişisel verilerin korunmasına yönelik 2002/58/AT Direktifini değiştirmektedir. 2006/24/AT sayılı Direktif, özellikle adli vakaların incelenmesi ve suçlu takibinde, elektronik haberleşme altyapı ve hizmetlerinin kullanımı ile ortaya çıkan özel ya da tüzel kişilere ait trafik ve konum bilgilerine ilişkin esasları düzenlemek amacıyla hazırlanmıştır. 2006/24/AT Direktifi, suçun takibi ve yargıya intikali sürecinde gerekli verilerin sağlanabilmesi amacıyla elektronik haberleşme hizmet sağlayıcılarına bazı yükümlülükler getirmesi, bu kapsamda, saklanacak veri kategorileri, saklama süresi, verileri saklama koşulları ve veri güvenliği kapsamında gözetilecek kuralları ele alması sebebiyle 2002/58/AT'den kapsam olarak daha geniştir. Ayrıca, mobil ve sabit hizmetler yanında İnternet hizmetleri de bu Direktifin kapsamına dahil edilmiştir.

Ülkemizde bu Direktifin uyumlaştırılmasına yönelik yönetmelik hazırlık çalışmaları devam etmektedir.

3.2.5.5. 92/242/AET sayılı Konsey Kararı

Topluluk düzeyinde bilgi sistemleri kullanımının güvenliğini tesis etmek ve bilginin serbest dolaşımı ile ilgili stratejilerin geliştirilmesi amacıyla 31 Mart 1992 tarihinde alınan 92/242/AET sayılı Konsey Kararı, bilgi güvenliği alanında Komisyona danışmanlık yapacak ve bir eylem planı tasarlayacak bir birim oluşturmaktadır.

24 Kasım 2005 tarihli ve 2005/222/JHA sayılı bilgi sistemlerine yönelik saldırılarla ilgili Konseyin Çerçeve Kararı, daha güvenli bilgi toplumu için bilgi altyapılarını geliştirmek ve bilgisayar bağlantılı suçlarla mücadele etmek ile ilgili (2000) 890 sayılı Komisyon Bildirisi ve ENISA'yı kuran 460/2004 sayılı Tüzük, 92/242/AET sayılı Konsey Kararı ile ilişkilidir.

3.2.5.6. (2007) 228 sayılı Komisyon Bildirisi

Avrupa Komisyonu'nun "(2007)228 sayılı Veri Korumanın Mahremiyet Artırıcı Teknolojilerle Desteklenmesi Hakkında Bildiri"sinde, MAT'ların daha geniş bir alanda kullanılmasıyla mahremiyeti korumanın kolaylaşacağı ifade edilmektedir. Elektronik kimlik yönetim sistemlerinde ve kimlik hırsızlığı ile mücadelede kullanılacak MAT'ların geliştirilmesi için özel sektöre de yatırım çağrısı yapan bildiri, bu teknolojilerin 7. Çerçeve Programı[137] kapsamındaki ar-ge projeleri içinde gelecekte daha çok destekleneceğini vurgulamaktadır.

3.2.6. Diğer uluslararası çalışmalar

Uluslararası konferans ve tartışma platformları, mahremiyetin ve kişisel verilerin korunması alanındaki literatüre önemli katkılar sağlamaktadır. 1979 yılından beri her yıl düzenli olarak yapılmakta olan Uluslararası Veri Koruma ve Mahremiyet Komiserleri Konferansları[138] ile AB düzeyinde yapılan Veri Koruma Komiserleri Konferansları[139] telekomünikasyon ve politika alanlarında bilgi paylaşımı ve tartışma alanları ile faydalı çıktılar sağlamaktadır. Telekomünikasyon ve medya alanında mahremiyetin gelişmesi ve veri korumanın sağlanması için bazı ülkelerce geliştirilen ve özellikle Berlin Veri Koruma Komiserinin liderliğinde başlatılan "Telekomünikasyon Sektöründe Uluslararası Veri Koruma Çalışma Grubu" İnternette de yaygın tartışma platformları ile önemli çalışmalar yapmaktadır.

Yine, Asya Pasifik Mahremiyet Otoriteleri (APPA-Asia Pacific Privacy Authorities), Asya Pasifik Bölgesinde mahremiyet alanında işbirliğini geliştirmek, yeni teknolojileri tartışmak üzere yılda iki kez bir araya gelen bir platformdur. Avustralya, Yeni Zelanda, Hong Kong, Güney Kore, Kanada Mahremiyet

---

[137] 7. Çerçeve Programı, AB'nin 2000 yılında Lizbon Stratejisinde belirlediği "**dünyanın en dinamik rekabetçi bilgi temelli ekonomisi**" olma hedefi kapsamında; bilgi temelli ekonomi ve toplumu oluşturmayı hedefleyen ve 2007-2013 yıllarını kapsayan, çok uluslu araştırma ve teknoloji geliştirme projelerinin desteklendiği bir Topluluk Programıdır. Proje teklif çağrılarında belirtilen şartlara sahip projeler, hakemler tarafından objektif bir şekilde değerlendirildikten sonra mali destek sağlanır. Daha fazla bilgi edinmek için bkz. TÜBİTAK, Avrupa Birliği 7. Çerçeve Programı, <http://www.fp7.org.tr/home.do;jsessionid=38544C30FE7E9848A37691DC39D1FF2F?ot=1&sid=3100>

[138] Bu Konferanslardan 30'uncusu için bkz. Protecting Privacy in a Borderless World, Strasbourg. <http://www.privacyconference2008.org/index.php?page_id=1>

[139] Konferansın detayları için bkz. Data Protection Conference, 2009, Brussels. <http://webcast.ec.europa.eu/eutv/portal/archive.html?viewConference=7334&catId=7256>

Komiserleri bu platformun üyesidirler. APPA daha önce PANZA ve PANZA+ (Privacy Agencies of New Zealand and Australia plus Hong Kong and Korea) olarak anılmaktaydı.[140]

Uluslararası Ticaret Odası (ICC), kişisel mahremiyetin korunması ve bilgi transferleri ile ilgili olarak dünya çapında çok sayıda rapor ve ticaret kodları hazırlamıştır. Bu dokümanlar, çoğunlukla İnternet reklamlarına ilişkin bir dizi rehber ilke ve pazarlama ilkeleri sunmaktadır. ICC, aynı zamanda uluslararası alanda kişisel veri transferlerine ilişkin bir sözleşme modeli de hazırlayarak Avrupa Komisyonuna sunmuştur.

3.3. Karşılaştırmalı Hukukta Kişisel Verilerin Korunması

Kişisel verilerin korunması alanında son yıllarda birçok ülkede düzenlemeler yapılmıştır ve artan bir hızla yapılmaya devam edilmektedir. Bu düzenlemelerden bir kısmı halihazırda günün koşullarına uygun olarak güncellenmektedir. Bir bölümü oldukça kapsamlı olarak, kamu ve özel sektör uygulamalarını da içerecek şekilde ele alınmıştır. Diğer bir grup düzenlemeler ise münhasıran bir sektöre odaklanmaktadır. Sadece kamu sektöründe veya sağlık alanında kişisel verileri korumaya yönelik düzenlemeler, sektöre özel düzenlemelere örnek olarak verilebilir (Bkz. Ek 1: Karşılaştırmalı Hukukta Kişisel Verilerin Korunması).

Aşağıda, veri koruma alanında ilk düzenlemeleri yapmış olan ülkelerden olmakla birlikte, şimdilerde AB ile uyumlu bir veri koruma anlayışını benimsemeye başlayan ABD, Kıta Avrupası hukukuna dahil olan ve dünyada ilk veri koruma düzenlemesini yapan Almanya ve son yıllarda önemli veri kayıplarının yaşandığı, Anglo-Sakson hukukun temsilcisi olmakla birlikte veri koruma alanında AB hukukuna yakınsayan İngiltere daha ayrıntılı olarak incelenmektedir.

3.3.1. Amerika Birleşik Devletleri

Amerika Birleşik Devletleri'nde (ABD), veri koruma ile ilgili endişeler, sosyal güvenlik numaralarının sıkça kullanılmaya başlanması ve veri bankalarının artması ile önem kazanmaya başlamıştır.

[140] APPA hakkında ayrıntılı bilgi için bkz. <http://www.privacy.gov.au/aboutus/international/appa>

ABD, veri koruma mevzuatında tek ve yeknesak bir yaklaşımdan ziyade, sektörel ve ilgili mevzuattan oluşan bir kombinasyonu tercih etmektedir. 1981 yılında OECD Rehber İlkelerini imzalayan taraflardan biri olmakla birlikte ABD, bu kuralları iç hukukuna yansıtmamıştır. Eski Başkan Clinton ve Yardımcısı Al Gore, "Küresel Elektronik Ticaret Çerçevesi"nde özel sektör ve şirketlerin İnternet teknolojisi karşısında kendi kurallarını koymalarını açıkça tavsiye etmektedirler. Bu durumun da bir yansıması olarak, bugüne kadar ABD'nin veri koruma alanında AB ile kıyaslanacak tek, kapsamlı ve çerçeve nitelikte bir veri koruma mevzuatı bulunmamaktadır. ABD'de mahremiyet kanunları "ihtiyaç duyuldukça" çıkartılmaktadır. Video Koruma Kanunu, Kablolu Televizyon, Tüketici Korunması ve Rekabet Kanunu bu tür kanunlara örnek olarak verilebilir. ABD'de çerçeve bir yasanın olmaması AB ve ABD arasında bir kutuplaşma yaratmıştır. AB, kişisel verilerin korunmasını temel bir hak meselesi olarak görürken, ABD bu konuya daha çok müşteri hakları gözüyle bakmıştır.

Bununla birlikte, ABD'nin California eyaletinde 1 Temmuz 2004 tarihinden itibaren yürürlükte bulunan "Çevrimiçi Mahremiyet Koruma Kanunu" (Online Privacy Protection Act, OPPA)[141] bu eyalette yaşayan kişilerin kişisel bilgilerini toplayan ticari İnternet sitesi işletmecilerinin, belirledikleri mahremiyet politikalarını açıkça ilan etmeleri ve diğer mahremiyet kurallarına riayet etmeleri gerekliliğini hükme bağlamaktadır.

ABD'nin veri koruma düzenlemelerinin AB düzenlemelerinden farklı unsurlar taşıması, iki kıta arasındaki birçok ticari iş ve işlemi sekteye uğratmaktadır. VKD'nin, veri transferine ilişkin ABD düzenlemelerine göre daha sıkı şartlar getiren kuralları bu durumun oluşmasında önemli bir paya sahiptir. VKD'nin 25'inci maddesine göre, bir AB üyesi devletin AB dışındaki bir ülkeye (üçüncü ülke) kişisel veri transferi yapabilmesi için, üçüncü ülkedeki mahremiyet kurallarının AB'nin veri koruma düzenlemeleri ile *uyumlu ve yeterli şartları* taşıması gerekmektedir. VKD'nin 26'ncı maddesinin birinci fıkrasında ise, yeterli koruma seviyesini sağlamayan üçüncü ülkelere transfer işlemi yapılırken sağlanması gereken koşullar

[141] The Online Privacy Protection Act of 2003 için bkz. <http://leginfo.ca.gov/cgi-bin/displaycode?section=bpc&group=22001-23000&file=22575-22579>

sayılmakta; aynı maddenin 2'nci fıkrasında, üçüncü ülkelere kişisel veri transfer edilirken, iki ülke arasında bir Sözleşme aktedileceği belirtilmektedir. Bu Sözleşme ile, üçüncü ülkelerdeki veri kontrolörleri, transfer edilen veriler üzerinde veri koruma kurallarına uyacaklarını garanti etmelidir.

11 Eylül saldırıları sonrası ABD'nin terörle mücadele kapsamında yürüttüğü çalışmalardan birisi de ülkeye giriş çıkışların daha kontrollü hale getirilmesidir. Bu kapsamda başlatılan tedbirlerden olan "Yolcu İsimleri Kaydı"na (Passenger Name Record) AB büyük bir tepki göstermişse de, AB vatandaşlarına ait yolcuların kayıtlarının tutulmasını sağlayacak mutabakat zaptı bazı AB üye devletleri ile ABD arasında 2007 yılının Temmuz ayında imzalanmıştır. Bu anlaşmayı imzalayan üye devlet vatandaşlarının yolcu olarak Avrupalı havayolu şirketleriyle ABD'ye seyahatlerinde, bu yolcuların kişisel verileri, terörle mücadele kapsamında ABD'nin bir dizi kurumlarına iletilmeye başlanmıştır. Bu veriler, ABD'de 15 yıl süreyle saklanacak olup, elde edilen veriler bazı kişilerin ABD'ye girişlerinin reddedilmesine de sebep olabilmektedir. ABD yetkilileri gerekiyorsa kişilere ait sağlık durumu, siyasi görüş veya etnik köken gibi hassas verileri de isteyebilmektedir.

ABD'nin 2007 yılının Temmuz ayında, Brüksel ile görüşme yapmaksızın, AB başkentlerine ikili işbirliğine dayalı mutabakat zaptını göndermesi birçok Avrupalı tarafından kabul edilemez görülmüşse de, bu gelişme bazı Avrupa devletlerince olumlu karşılanmıştır. Çoğu 2004'ten sonra AB'ye üye olan 11 AB ülkesi ABD'nin vize uygulamasına tabi olduklarından, ABD'ye girişlerde vize uygulamasının kaldırılması karşılığında, AB vatandaşlarının kişisel verilerini daha sıkı bir şekilde kayıt altına almayı öngören bu mutabakat zaptına sıcak bakmışlardır. Çek Cumhuriyeti de Avrupa Komisyonu'nun karşı telkinlerine rağmen, ABD ile arasında mutabakat zaptını imzalayan ülkelerdendir. Çek Cumhuriyeti İçişleri Bakanı Ivan Langer, Komisyonun karşı tutumuna karşı ülkesini bu Mutabakat Zaptı'nı imzalamaya teşvik eden nedeni açıklarken tam olarak "Tok açın halinden anlamaz." ifadesini kullanmış, AB'nin 15 eski üye ülkesinden farklı olarak kendilerinin ABD'nin vize muafiyetinden yararlanmadıklarını, AB'ye girerken üyeliğin ABD ile yapılacak müzakerelerde yardımcı olacağını düşündüklerini ancak hiçbir gelişme sağlanamaması üzerine yalnız hareket etmenin daha uygun olacağını, bu çerçevede

Prag'ın, vatandaşlarının ABD'ye daha kolay giriş yapabilmelerini sağlamak istediğini belirtmiştir.

Terörle mücadele kapsamında, vize uygulamasını daha sıkı şekil şartlarına bağlamak yerine, ABD'nin bu ülkeye yapılacak transatlantik uçuşlarda yolculara ilişkin kişisel verileri 15 yıllık bir süre ile barındıracak bir veritabanı tutması ve bunun karşılığında verileri sağlayan ülkelere vize muafiyeti getirmesi, vazgeçilen ve kazanılan değer bakımından kişisel verilerin güvenlik alanındaki rolünün önemini bir kez daha vurgulamaktadır. Bu olay, AB üye ülkeleri içinde ikili görüş ve tutum yaratmış olup, basına "Bölünmüş Avrupa, ABD'nin talep ettiği verilerini korumak istiyor"[142] başlıkları ile yansımıştır. Bu süreçte, başta Fransa olmak üzere bazı AB ülkeleri en azından mevcut durumu koruyarak daha fazla bilgi vermeme taraftarıdır.[143] ABD, elektronik yolcu yetkilendirme sistemi ile yolcular hakkında daha fazla bilgi edinme, böylece kayıp ve çalıntı pasaportların takibini daha kolay yapabilmeyi amaçlamaktadır.[144]

3.3.1.1. Amerika Birleşik Devletleri'nde yaşanan deneyimler

Artık dünyanın birçok ülkesinde sıkça gündeme geldiği gibi, ABD'de de veri hırsızlığı olaylarına rastlanmaktadır. Genellikle kredi kartı şirketlerinden, çevrimiçi perakende satış kuruluşlarından, devlet dairelerinden ve bankalardan çalındığı ortaya çıkan bu bilgiler, satışa konu olmakta, bu şekilde birçok suç işlenebilmektedir. 2005 yılında içinde 1 milyon devlet memuru ile ilgili bilgilerin bulunduğu teypler Amerikan Bankası'nda kaybolmuştur. Yine, 2006 yılında emekli askerler kurumunda çalışan bir kişinin evinden 26.5 milyon kişinin verileri çalınmıştır. 2009 yılı başlarında ise Iowa eyaletindeki bir veri merkezinde yaklaşık 3 milyon kişinin trafik sınavı kayıtları kaybolmuştur.

3.3.1.2. Güvenli Liman Kuralları

VKD'nin yukarıda ifade edilen "yeterlilik düzeyi" kısıtı karşısında, ABD Ticaret Bakanlığı, Avrupa Komisyonunun da görüşlerini alarak, VKD ile uyumlu

---

[142] Fahsi, 2008
[143] CNIL, 2007:1
[144] Goldirova, 2008

"Güvenli Liman Sistemi"ni geliştirmiştir. Bu sistemi Temmuz 2000'de tanıyan AB kurum ve kuruluşları ile ABD'nin bu ilkeleri benimseyen kuruluşları arasında kişisel veri paylaşımına dayalı ilişkiler devam etmektedir.[145]

Güvenli Liman Sistemi, yedi temel ilkeden oluşmaktadır. Bu ilkeler şunlardır:

i) Bildirim: Kuruluşlar; kişisel veri toplama amaçlarını, bu verileri nasıl kullandıklarını ve itiraz edilmesi durumunda gerekli irtibat bilgileri konusunda bireylere bilgi sunmak zorundadırlar.

ii) Seçim yapma ilkesi: Kuruluşlar, kişisel verileri üçüncü taraflarla paylaşmak ya da toplandığı amacın dışında kullanabilmek için veri sahibine opt-out (işlem sonrası reddetme hakkı) ve hassas veriler için ise opt-in (önceden izin) seçeneğini sağlamalıdır.

iii) Üçüncü taraflara iletim: Kişisel verilerin üçüncü taraflara iletilmesi durumunda, kuruluşlar bu tarafların veri koruma düzeyinin yeterli olup olmadığına bakacaktır. Bunun için üçüncü kişilerin de Güvenli Liman İlkelerine kaydı veya Direktife bağlı olup olmadığından emin olunacaktır. Alternatif olarak, bu taraflarla yazılı sözleşme de yapılabilecektir.

iv) Erişim: Veri sahiplerine, kuruluşların kendileri ile ilgili tuttukları verilerin doğru olup olmadığını görme, bu verileri düzeltme ve gerekiyorsa bunların silinmesini isteme hakkı tanınacaktır. Bu hakkın kullanılması için gereken erişim maliyetleri makul düzeyde olacaktır.

v) Güvenlik: Kuruluşlar, kişisel verilerin kayıp, kötüye kullanılma, yetkisiz erişim, değiştirme ve yok edilmesi risklerine karşı gerekli güvenlik önlemlerini alacaktır.

vi) Veri bütünlüğü: Elde edilen kişisel verilerin, kullanılacağı amaca uygun ve bu amaçla ilgili veriler olması gerekmektedir.

vii) Uygulama: Yürütülen faaliyetlerin Güvenli Liman İlkeleri ile uyumlu olmalarını sağlamak ve bireylerin şikayetlerini karara bağlamak için bağımsız karar organları kurulmalıdır.

---

[145] PRIVIREAL, 2005

Yukarıda belirtilen ilkelere ek olarak, uygun eleman istihdamı, bunların eğitimi ve uyuşmazlık çözüm mekanizmalarının belirlenmesi, Güvenli Liman Sistemi ile uyumlu olmanın diğer gerekliliklerindendir. Bu yedi ilkeyi ve diğer gereklilikleri kabul eden ABD şirketleri, ABD Ticaret Bakanlığına başvurarak kamuya ilan edilen[146] Güvenli Liman Sistemine kayıt olmaktadırlar. Sisteme kaydolan kurum veya kuruluşlar, ilkelere uyum konusunda her yıl bağımsız denetçiler aracılığıyla ya da kendi beyanlarına dayalı olarak değerlendirilirler.

3.3.2. Almanya

Tarihsel gelişim kısmında vurgulandığı gibi, dünyada ilk veri koruma yasası 1970 yılında Almanya'nın Hessen eyaletinde hazırlanmıştır. Ancak, her ne kadar VKD'den önceki dönemde Almanya'nın veri koruma alanında hassasiyetinden söz edilebilirse de, bu ülkede VKD'nin uyumlaştırılma çalışmaları uzun sürmüş ve 2001 yılında tamamlanmıştır.

Alman Fedaral Devleti'nde veri koruma mevzuatı farklı şekillerde uygulanmaktadır. Bu nedenle, her bir eyaletteki düzenleme ve uygulamanın incelenmesi yerine, Almanya'daki çerçeve nitelikteki Veri Koruma Yasası aşağıdaki Tablo 3.2.'de özetlenmektedir.

Federal Veri Koruma Komiseri dışında, Almanya'da veri koruma ile ilgili dört merci daha bulunmaktadır. Bunlar; Berlin Veri Koruma Komiseri, Ulusal Etik Konseyi, Alman Sağlık Birliği ve Bavyera Bioetik Komisyonu'dur. Almanya'da kişisel verilerin mahremiyetinin ihlali durumunda 30 bin Avro'ya kadar para cezası ve hapis cezası verilebilmektedir.

Bunların dışında, Alman Anayasa Mahkemesinin kişisel verilerin korunması konusunda çarpıcı kararları bulunmaktadır. Bu kararlar ile, kişisel verilerin korunması Anayasa Hukuku bakımından bir temele kavuşmuştur. Bu Mahkeme, genel olarak Anayasada bağımsız bir temel hak olarak düzenlenmeyen kişisel verilerin korunması hakkının anayasal temellerini kişiliğin serbest geliştirilmesi

[146]Kayıt listeleri için bkz.
<http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe%2Bharbor%2Blist>

hakkı ve insan onuru garantisinde bulan kişilik hakkından çıkartmış ve bu hakkı bireyin kişisel verileri üzerinde belirleme hakkı olarak nitelemiştir.[147]

Tablo 3.2. Alman Veri Koruma Yasası

Veri Koruma Mevzuatının adı	Federal Veri Koruma Kanunu (Bundesdatenschutzgesetz -BDSG) 2001
Denetleyici Kurumun Adı	Federal Veri Koruma Komiseri
Kurumun ve Komiserin Genel Yetkileri	Kamu kurumlarının bu Kanunu uygulamalarını sağlamak, bunun için uygulamaları izlemek, vergi gizliliği gibi özel alanlarda kişisel verileri korumak (bölüm 3, md. 24), bu Kanunun ihlal edilmesinin resen veya şikayet üzerine bildirilmesi halinde üst yargı yerlerinde dava açmak (md. 25), Fedaral Hükümete bu Kanunun uygulanması hakkında görüş ve tavsiyelerde bulunmak, bu konuda devletin diğer organlarına müşavirlik yapmak (md. 26).
İhlaller konusunda denetleyici kurumu bilgilendirmeye yetkili makam	Herkes
Veri kontrolörlerinin Kanunu ihlal etmeleri halinde verilecek ceza	Hapis ve para cezası (Bölüm 3-md. 43-44).
Kanunda ulusal kimlik numarası veya benzer bir numaranın işlenebilmesi şartlarına ilişkin herhangi bir hüküm var mı?[148]	Hayır – Federal Alman Cumhuriyetinde ulusal kimlik numaraları kullanılmamaktadır, bu nedenle Direktifin 8/7 maddesine karşılık olarak Kanunda bir hüküm bulunmamaktadır.
Kişisel verilerin işlenmesinden önce rıza alınması gerekmekte midir; yoksa, rıza almanın pratik veya uygun olmayacağı durumlar için alternatifler bulunmakta mıdır?	Rıza almanın uygun veya pratik olmadığı durumlarda rızaya alternatif uygulamalar bulunmaktadır.
Veri Koruma mevzuatı ölmüş kişileri kapsamakta mıdır?	Hayır, ancak her eyalette mevzuatın kapsamı genişletilebilir.

Kaynak: PRIVIREAL, *History of Data Protection in Germany*, 2005.

Otomatik veri işleyicilerin çoğalması karşısında bireyin kişisel verilerinin korunması bakımından Alman Anayasa Mahkemesinin Nüfus Sayımı Kararı (15 Aralık 1983) oldukça önemlidir. Alman Nüfus Sayımı Kanunu ile 1983 tarihli nüfus sayımında, istatistiki kullanıma da elverecek şekilde, kişilere ait daha ayrıntılı verilerin toplanması istenmiştir. Ancak bu Kanunun Anayasa'daki kişilik haklarına aykırı olduğu gerekçesiyle, Anayasa Mahkemesinde açılan davada, Mahkeme kişisel verilerin kullanılması ve devredilmesi konusunda esas olarak bireyin kendisinin karar

[147] Şimşek, 2008:119
[148] VKD'nin 8/7 maddesi uyarınca ulusal kimlik numarasının hangi koşullar altında işlenebileceğinin üye ülkelerde belirlenmesi gerekmektedir.

verme hakkına sahip olduğu gerekçesiyle sayımın yürütmesini durdurma kararı almıştır. Bu Karar, Alman kişisel veri koruma mevzuatı ve diğer uygulamalara da temel teşkil etmektedir. Zira, birey çoğunluktan ayrılan davranışlarının kamusal organlar tarafından kaydedildiği hususunda endişelenecek olursa, dikkat çekmemek için temel haklarını özgürce kullanmaktan vazgeçecektir. Kararda, ayrıca bireyin görünüşte önemsiz gibi görünen verilerinden hareketle onun davranış tarzının esas olarak belirlenebilmesinin mümkün olduğu, dolayısıyla önemsiz veri olmadığı vurgulanmıştır.[149]

Alman Anayasa Mahkemesinin verdiği kararla gündeme taşıdığı bir diğer konu ise kişisel veriler üzerindeki hakkın mülkiyet hakkı gibi kişiye mutlak ve sınırsız bir hak verip vermeyeceği konusu olmuştur. Baskın olan ve Mahkemenin verdiği kararla da paralel olan görüşe göre, kişisel verilere *kamu yararı* nedeniyle veya ancak *yasa* ve *kişinin rızası* ile müdahale edilebilir. Bu görüşe göre, yasa niteliğine sahip olan ve fakat; kamu yararı gerektirmediği halde kişisel veriler üzerinde hakimiyet sağlayan uygulamaların da kişi hakları ve hukukun genel ilkeleri çerçevesinde kişi lehine yorumlanması uygun olacaktır.

3.3.3. İngiltere

1981 yılında Avrupa Konseyi'nin kişisel mahremiyete halel getirmeksizin üye ülkeler arasında bilginin serbest dolaşımının sağlanmasına yönelik yayınladığı 108 sayılı Sözleşme'den üç yıl sonra, 1984'te İngiltere'de ilk veri koruma kanunu yürürlüğe girmiş ve 1998 yılına kadar geçerli olmuştur. Bu Kanun, bilgisayar ortamında kişisel veri tutan kamu kurum ve kuruluşları ile özel sektörün Veri Koruma Sicil'ine kayıt olmaları zorunluluğu getirmesine karşın, bireylerin mahremiyet hakkı ve bu hakkın nasıl kullanılacağına ilişkin açık hükümlere yer vermemiştir. Bu durum, İngiltere'de kişisel verilerle ilgili çeşitli sorunların yaşanmasına sebep olmuştur. Avrupa Komisyonuna danışmanlık hizmeti veren RISEPTIS[150], akademik bir raporun, İngiltere'de kamu kurumlarının tuttukları veritabanlarının (46 veritabanı içinde) dörtte birinin insan hakları ve veri koruma kanunlarına aykırı veri işlediğini tespit ettiğini kaydetmektedir.

[149] Şimşek, 2008:115,116
[150] RISEPTIS, 2008:2

1998 yılında VKD'nin uyumlaştırılması amacıyla İngiltere'de çıkarılan Veri Koruma Kanunu ile bu eğilim değişmiş, Kanunun asıl amacının kişilerin mahremiyet haklarının korunması olduğu hükme bağlanmıştır. Bu Kanun ile kişisel verilerin işlenebilme şartları belirlenmiş, hassas verilerin kullanımı konusunda daha sıkı koşullar getirilmiş ve kağıt ortamında tutulan bilgilerin de kapsanması için "veri" tanımı genişletilmiştir. Daha önceki dönemde, hem Kanunun uygulanmasından, hem de veri tutanların kaydını tutmaktan sorumlu olan Veri Koruma Sicil Ofisi yerine, kanunun uygulanmasından ve sicilin tutulmasından sorumlu iki ayrı yapı ihdas edilmiş, uygulamadan sorumlu olan Bilgi Komiserliğine geniş yetkiler verilmiştir.[151]

İngiltere'de yürürlükteki Veri Koruma Kanununun genel amacı bireylerin mahremiyet haklarının korunması, kendileri ile ilgili tutulan verilere erişim haklarının sağlanması ve bu bilgilerin düzeltilmesini isteme hakkından müteşekkildir. Kanun, verilerin haksız veya çok sayıda sebeple saklanması karşısında da bireyi korumaktadır. Bu çerçevede Kanun, veri kontrolörlerini, verileri aşağıdaki yedi temel ilkeye uygun bir şekilde tutmaya ve işlemeye zorlamaktadır:

- Adil ve hukuka uygun olarak işleme,
- Sadece belirlenmiş amaçlar için işleme,
- Kullanılacakları amaca uygun, orantılı ve ilgili verileri tutma,
- Gereğinden fazla süre saklamama,
- Kişi haklarıyla uyumlu ve bu haklara zarar vermeyecek şekilde kullanma,
- Güvenli ortamlarda tutma,
- Yeterli koruma düzeyinin olmadığı ülkelere transfer etmeme.

İngiltere'de Adalet Bakanlığı'nın himayesinde bağımsız idari yapıdaki Bilgi Komiseri Ofisi (ICO-Information Commissioner Office), verilerin korunmasını desteklerken, resmi bilgilere erişimi kolaylaştırma taraftarıdır.

İngiltere'de üç farklı yerdeki ofisiyle ICO, Veri Koruma Yasası, Bilgi Edinme Hakkı Kanunu, Çevre Verisi düzenlemeleri ile Mahremiyet ve Elektronik Haberleşme Düzenlemeleri'nin uygulanmasından ve izlenmesinden sorumlu olarak

[151] BBC News. Q&A: Data Protection Act. 23 Aralık 2003. Erişim tarihi: 12 Ekim 2009. <http://news.bbc.co.uk/2/hi/uk_news/3344075.stm>

görev yapmaktadır. Ofisin bu çerçevede temel fonksiyonları, kişisel veri koruma konusunda vatandaşları bilgilendirmek, eğitimler vermek, hakları ihlal edilenlerin şikayetlerine bakmak ve sorumluluklarını yerine getirmeyenlere yaptırım uygulamaktır.

3.3.3.1. İngiltere'de yaşanan deneyimler

Veri Koruma Kanununun uygulanmasında İngiltere'de bazı sorunlar yaşandığı bilinmektedir. Bunlardan önemli bir bölümü, kanunun muğlak ifadelere yer vermesi nedeniyle veri tutucuların nasıl hareket edeceklerini tam olarak bilememesinden kaynaklanmaktadır. Örneğin, Kanunda, kişisel verileri gerektiğinden daha uzun süre saklamama ilkesi bulunmaktadır. Kanuna uygun hareket etmek isteyen veri kontrolörleri, bu ilkedeki "gereklilik" ölçütü açık olmadığından veriyi uzun süre tutarak sorumluluk almak yerine, veriyi alelacele silme yoluna gidebilmektedirler. Bununla ilgili olarak 2003 yılında, Humberside'da, iki kişiyi öldürmekten zanlı bir kişinin polis tarafından daha önce hakkında cinsel istismar suçları nedeniyle tutulan kayıtları Kanunun uygulanmasını sağlamak üzere erken bir dönemde silinmiş olduğundan, bu kişi yakalanamamıştır. Bu durum, İngiliz Veri Koruma Kanununun acilen yeniden gözden geçirilmesi gerektiği yönünde tartışmaları gündeme getirmiştir.

Kanunun içeriği ve uygulanmasındaki sıkıntıların dışında, 2007 yılında İngiltere ciddi bir veri hırsızlığı ile karşı karşıya kalmıştır. Bu yılın Kasım ayında, İngiltere Maliye Bakanlığı 25 milyon İngiliz vatandaşının ve 7 milyon ailenin pek çoğunun banka hesapları, adresleri, sosyal sigorta numaraları ve aile bireylerinin isimleri ve doğum tarihlerini içeren iki bilgisayar diskinin kaybolduğunu açıklamıştır. Kasım ayında kaybolan disklerde çocuk sahibi ailelere devlet tarafından yapılan parasal yardım için kullanılan ve İngiltere'de 16 yaşından küçük hemen hemen her çocukla ilgili veriler bulunmaktaydı. İki kurum arasında disklerin posta yoluyla iletilmesi ile ortaya çıkan bu durum, Başbakan Gordon Brown'un halktan özür dilemesine sebep olmuştur. Vergi dairelerinde de 2005 yılından 2007 sonuna kadar sekiz kez veri kaybı olayına rastlandığı ortaya çıkmış, bazı resmi dairelerin bilgisayar sistemlerindeki teknik bir sorun nedeniyle bu kuruluşlarda iş arayan

doktorların ekranlarında aynı iş için başvuru yapan diğer doktorların kişisel bilgilerine ulaştığı görülmüştür.[152] Yine İngiltere'de 2007 yılının Eylül ayında 400 kişiye ait kişisel bilgilerin bulunduğu bir dizüstü bilgisayarın vergi ve gümrük dairesinde, Ekim ayında ise 15 bin kişinin emeklilik bilgilerini içeren bir diskin postada kaybolduğu anlaşılmıştır.

Bu olaylar neticesinde, İngiltere gelişmiş ülkeler içinde en gevşek veri güvenliği kurallarının uygulandığı ülke olarak görülmektedir. Söz konusu olayların mağduru olan vatandaşlar için sadece yeni banka hesaplarının düzenlenmesinin 600 milyon ABD Doları tutarında olacağı hesaplanmıştır. Başbakan Gordon Brown bu olaylar üzerine, hükümet olarak kişisel verilerin kullanımı ve korunması için yeni yöntemler uygulayacağını açıklamıştır. Bu yöntemlerin maliyetinin yüz milyonlarca doları bulacağı tahmin edilmektedir.

İngiltere'de, başta Bilgi Politikası Araştırma Vakfı olmak üzere bazı sivil toplum örgütleri, veri kayıplarının devletin kurduğu çok büyük veritabanlarının kötü yönetilmesinin bir sonucu olduğunu ve bürokratların vatandaşların özel bilgilerini paylaşma haklarının olmadığını ifade ederek tepki göstermişlerdir.

[152] BThaber. 11-17 Şubat 2008. s.46. Derleyen:Amil Kunt.

4. KURUMSAL YAPILANMA

4.1. Genel Çerçeve

1970'li yıllarda ilk modern mahremiyet yasalarını çıkarmış olan Almanya, İsveç ve ABD, kişisel verilerin ve mahremiyetin korunması ile ilgili dünyada yürütülen çalışmalarda birinci dalgada yer almaktadır. Aynı yıllarda Yeni Zelanda'da Bilgi Komiserliği ve New South Wales'de bir Mahremiyet Komitesi kurulduğu görülmektedir.

OECD ve Avrupa Konseyi'nin öncülüğünde yürütülen Rehber İlkeler'in yayımlanmasıyla sonuçlanan ikinci dalga ise 1980'li yıllara tekabül etmektedir. Bu dalgada, birçok batı Avrupa ülkesi ve Avustralya resmi veri koruma yasalarını kabul ederek uygulamaya başlamıştır.

1990'lı yılların başında harekete geçen ve "üçüncü ülkelere bilgi transferi" hassasiyetinin hakim olduğu üçüncü dalga ise etkisini hala sürdürmektedir. Özellikle Avrupa dışındaki ülkelere veri transferi yapılırken, üçüncü ülkenin "yeterli koruma" düzeyine sahip olmasının aranması, uluslararası standartlarda bir yapılanmanın gerekliliğini gündeme getirmiştir. Bilişim suçlarının işleniş biçimi ve ispatındaki zorluk nedeniyle bu suçlara bakacak yetkili mahkemelerin tespitinde yaşanan zorluk ve e-ticaret işlemlerinde tüketici güveninin kazanılması gerekliliği gibi sebeplerle giderek önem kazanan bilgi transferleri ve bu transferlere getirilen standartlar ve sınırlandırma, birçok ülkenin bu yapıya ayak uydurmasını gerektirmektedir. Uluslararası standartlarda düzenlemeler ile önem kazanan mahremiyet hakkı ve veri koruma yasaları, bu yasaların uygulanmasından sorumlu olacak otoriteleri de elzem kılmaktadır. Veri koruma kanunu olan ülkelerin büyük çoğunluğu bu kanunların uygulanmasını gözeten özel kurumlar kurmuşlardır. Bu konudaki en önemli istisna ise Japonya ve Amerikadır.[153] ABD'de yayımlanan "Mahremiyet Yasaları ve Gelişmeleri konusundaki Uluslararası Araştırma Raporunda"[154] kişisel verilerin kötüye kullanılma endişesi karşısında bireyin hak alanının genişletilmesi ve veri bankalarının belirli standartlarda çalışmasını sağlayacak, onların bu işlemlerine

[153] Bygrave, 2002:70
[154] Privacy International, 2007

başlaması için sicil tutarak yetki verecek bir merkezi (federal) düzenleyici ajansın kurulması önerilmektedir. Ancak, ABD'de federal düzeyde bir veri koruma kurumu kurma yönündeki pek çok girişim, bu ülkede devlet kurumlarının regülasyon yapmalarına karşı duyulan antipati nedeniyle sonuçlanmamıştır. Rapora göre bu ajans, özel sektör ve kamu alanındaki otomatik veri işleyiciler üzerinde denetleme ve gözetim yetkisine de sahip olmalıdır. AB'de de veri koruma alanında bazı yapılar kurulmaya başlanmıştır. Özellikle Avrupa Konseyi'nin 181 sayılı "Kişisel Verilerin Otomatik Yöntemlerle İşlenmesi, Denetleyici Otoriteler ve Sınır Ötesi Veri Akışları Hakkında Bireylerin Korunması Sözleşmesi" üye ülkelerde bu süreci tetiklemiştir. Nihayet OECD ülkeleri ve devamında uluslararası alanda otomatik sistemler kullanarak veri değişimi yapan, bilgi toplumuna geçmeyi hedefleyen ülkelerde de bu yapılar zorunluluk haline gelmiştir.

Uygulama araçlarına göre ayrım yapıldığında, birçok ülkede Veri Koruma Ofisleri veya Mahremiyet Komiserlikleri kurulduğu dikkat çekmektedir. Bu kurumsal yapıların genellikle danışmanlık, şikayetleri karara bağlama ve yaptırım uygulama yetkisini haiz oldukları görülmektedir.

Dokuzuncu Kalkınma Planı (2007-2013), Türkiye için; "İstikrar içinde büyüyen, gelirini daha adil paylaşan, küresel ölçekte rekabet gücüne sahip, *bilgi toplumuna dönüşen, AB'ye üyelik için uyum sürecini tamamlamış"* olma vizyonunu ortaya koymaktadır. Bilgi toplumuna dönüşüm sürecinde, tüm dünyada olduğu gibi Türkiye'de de e-devlet faaliyetleri ve diğer BT projelerinin hukuksal altyapısı, teknik altyapı kadar önem arz etmektedir. Bu çerçevede, kişisel verilerin korunması düzenlemeleri ve kişisel veri ihlalleri karşısında hızlı karar alma ve hayata geçirme yetisine sahip ve bu konuda uzmanlaşmış bir organizasyon yapısının varlığı bilgi toplumunun temel gereksinimlerindendir. Bu çalışmanın hazırlandığı sırada TBMM Adalet Komisyonunda bulunmakta olan KVKK Tasarısının 26'ncı maddesi de, bu gereksinime binaen "Kişisel Verileri Koruma Kurulu" kurulmasını öngörmektedir. Taslağın kurumsal yapılanma ile ilgili maddeleri ilerleyen bölümlerde incelenerek değerlendirilecektir.

Türkiye'de kurumsal yapılanma ile ilgili ihtiyacın ne düzeyde olduğu ve nasıl bir modelin gerekli olduğu konularında yeterli çalışma olmaması, ayrıca diğer ülke

uygulamalarının etkin bir şekilde takip edilememesi nedeniyle, kişisel verilerin önemi konusunda toplumda yeterli farkındalık oluşmamıştır. Bu durumun, kişisel verilerle ilgili düzenleme ihtiyacının sorgulanmasına ve özellikle kurumsal yapı alanında karar vermeyi erteleme eğilimine sebep olduğu gözlemlenmektedir.

4.2. Veri Koruma Otorite Modelleri ve Bunların Karşılaştırmalı İncelenmesi

Hemen hemen bütün başarılı veri koruma kanunları "bağımsız" bir veri koruma otoritesini tanımlamaktadır. VKD'nin "Düzenleyici ve Denetleyici Otorite" (Supervisory Authority) başlıklı 28'inci maddesi ve Avrupa Konseyi Sözleşmesine ek 181 sayılı Protokol de denetleyici bir üst kurum veya veri koruma biriminin temel rollerini tanımlamakta, bu kurumların mahremiyet düzenlemelerinin ulusal düzeyde uygulanmasının sağlanmasından sorumlu olacağını belirtmektedir. VKD, ayrıca bu kurumların tam bağımsız olarak hareket etmesi ve soruşturma alanında geniş yetkilerinin olması gerektiğini vurgulamaktadır, ancak yine de ulusal hukuklarda uygulama farklılıkları görülebilmektedir. VKD'nin 28'inci maddesi, kişisel verilerin sınır ötesine transferinde üst otoritelerin işbirliği içinde olmasını ve bu kurumlara hukuken geçerli karar verme yetkisi sağlanmasının da gerektiğini hükme bağlamaktadır.

Daha önce de ifade edildiği gibi, AB üye devletleri ve veri koruma yasalarına sahip ülkeler, üçüncü ülkelerle veri paylaşırken o ülkede "yeterli koruma" düzeyini aramakta; o ülkede bu yeterlilik ölçüsüne bakarken de *bağımsız* bir ulusal veri koruma otoritesinin var olup olmadığına göre karar vermektedirler.

Dünyada halihazırda mevcut veri koruma otoriteleri birbirinden farklı özellikler göstermektedir. Örneğin, Hong Kong, Kanada, Avustralya ve Yeni Zelanda'daki yapılar AB üye ülkelerindeki yapılardan çeşitli yönleriyle farklıdır. Bu otoritelerin kanunu uygulama yöntemi de değişebilmektedir. Bazı istisnalar haricinde çoğu AB üye ülkelerinde sadece tek ulusal veri koruma kanunu ve tek komiserlik kurumu bulunmakta iken[155] AB'ye üye üniter devletler ve federal devletler arasında farklı yapılanmalar bulunabilmektedir. Örneğin; Avustralya'da 5, Kanada'da 2,

[155] Kuner, 2007:13

Almanya'nın eyalet ve şehirlerinde 18, İsviçre'nin kantonları ve şehirlerinde 16 adet veri korumadan sorumlu komiser, ajans ya da otorite bulunmaktadır.

Dünyada veri koruma kurumlarına olan gereksinim ve bu kurumların sahip olmaları gereken temel ilkeler yalnızca veri korumaya ilişkin hukuki metinlerde düzenlenmekle kalmamakta, akreditasyon ilkeleri ile bu kurumların belli standartlara sahip olmalarını sağlayıcı tedbirler de alınmaktadır. Söz konusu standartlar sağlandıktan sonra, kurumsal yapının isimlendirmesi işi ise ülkelerin inisiyatifine bırakılmaktadır. Dolayısıyla bu konuda tek bir ölçü yoktur.

Veri koruma hukukunun uluslararası nitelikte olması ve uluslararası birtakım belgelerle koruma altına alınması, AB ile entegrasyon sürecinde bulunan; ancak, düzenlemeleri AB'den farklı olan ülkemizi de etkilemektedir. Bu sebeple, çalışmanın bu bölümünde AB düzenlemelerine uyum taahhütlerimiz de dikkate alınarak, AB üye ülkelerinde veri koruma hukukuna ilişkin kurumsal yapılar öncelikle incelenmiş, bununla birlikte OECD üye ülkelerinden Avustralya'daki kurumsal yapıya da değinilmiştir. Ancak münferit ülke incelemelerine geçilmeden önce, mevcut veri koruma otorite modelleri, bunların tipik ve ortak özellikleri, farklılıkları ile avantaj ve dezavantajları karşılaştırmalı olarak incelenmektedir.

Avrupa'daki veri koruma otoriteleri organizasyon yapıları ve görevleri nedeniyle pek çok benzerlik taşımaktadır. Bununla birlikte bazı konularda farklılıklara sahiptirler. Kuner, Avrupa veri koruma otoritelerini fonksiyonlarına göre *ombudsman* ve *düzenleyici* olmak üzere iki ana bölümde incelemektedir.[156] Bu ayrıma göre;

i) Ombudsman modeli: Üst (supervisory) kurum, kanunun ihlali halinde şikayet veya iddiada bulunan birey üzerinde odaklanmakta ve mağdur olan bireyin durumunu eski haline getirmek için bir karar vermektedir. Bu karar, birey hakkında tutulan bilgide değişiklik yapılması ya da bireye tazminat ödenmesi şeklinde olabilir. Bu modelin düzenleme modelinden temel farkı, kurumun veri kontrolörlerinin uygulamaları üzerinde çok fazla durmaması, daha ziyade vak'a bazlı hareket

[156] Kuner, 2007:13,14

etmesidir. Finlandiya, Macaristan, İsveç veri koruma otoriteleri işleyiş olarak ombudsman modelini benimsemişlerdir.

ii) Düzenleme (Regülasyon) modeli: Bu modelde ise üst kurum, kanuna uygunluk üzerinde yoğunlaşmaktadır. Kurum bir şikayet aldığında ve bu konuda kanunun ihlal edildiğine ilişkin bir sonuca vardığında, sadece şikayet edenin şartları ve tazmine ilişkin hususlarla değil, aynı zamanda geneli ilgilendiren ne tür önlemler alınması gerektiği ile de ilgilenmektedir. Düzenleme modelini benimseyen ülkelerde bireyin durumu yanında kanuna uygun hareket edilmesinin temini de oldukça önemlidir. Fransa, Polonya ve İspanya düzenleme modelinin örneklerindendir.

Kuner'in bu sınıflandırmasından başka, veri koruma otoritelerinin sınıflandırılmasında bir başka ayrım, o ülkenin bir kıta devleti, üniter devlet ya da eyaletlerden oluşmasına bakılmaksızın *yetkinin ait olduğu kişi veya gruba göre* yapılabilir. Buna göre veri koruma otoritelerinde yetki;

- Tek bir kişiye (Komiser),
- Atanmış birden fazla kişiye (Komisyon) veya
- Veri korumaya uygun görev ve bölümlere ayrılmış kuruma (Ajans) verilmiş olabilir.

Bu modeller, avantaj ve dezavantajlarıyla birlikte aşağıda incelenmektedir.

4.2.1. Komiser modeli

Veri koruma otoritesinin başında tek bir kişinin bulunduğu Komiser'lik (Commissioner), en yaygın kurumsal yapılanma modelidir. Yetkinin tek kişide olduğu "Veri Koruma Ombudsmanı" ve "Veri Koruma Kayıt İşleri Yetkilisi"[157] de Komiser modelinin altında değerlendirilmektedir.

Komiser ve mahiyetinde bulunan personel ile örgütlenen bu model bazı Avrupa ülkeleri, Kanada, Avustralya ve Hong Kong'ta görülmektedir.

Bu modelin o otoriteye sağladığı avantajlar şöyle sıralanabilir:

[157] Data Protection Registrar

- Esnek yapısı ve veri koruma ile ilgili sorunlarda tek kişinin yetkili olması nedeniyle azalan bürokrasi ve hızlı reaksiyon yeteneği,
- Veri korumanın bir kamusal figürle kişileştirilmesi nedeniyle veri korumaya olan önemin artması,
- Bu modelin bireysel ve kamusal alanın ihtiyaçlarına daha iyi cevap verebilmesi,
- Düzenli ya da birbirini izleyen resmi toplantılar ile bir araya gelen ve karar alması zaman alan yapıların hantallığından uzak olması.

Söz konusu modelin dezavantajları ise şöyle sıralanabilir:

- Kurumun, personelin ve hukuku uygulama kapasitesinin başarısı çoğunlukla Komiserin tercihlerine ve verdiği kararlara dayandığından hukuku yorumlamada genel eğilim tek yönlü, etkinlikten uzak ve subjektif olabilmekte, benzer nitelikteki vak'alarda farklı kararlar alınabilmektedir.
- Komiser, işlerin daha sağlıklı yürütülebilmesi için bu işleri yardımcı komiserlere veya diğer personele delege etmemeyi tercih edebilmektedir. Böyle bir durumda, her konuyla doğrudan ilgilenmek isteyen Komiserin bu tutumu nedeniyle kurum zamanında ve etkin bir biçimde çalışamamakta, dolayısıyla darboğaz yaratılmış olmaktadır.
- Kurumun tek bir yöneticiyle kişiselleştirildiği bu modelde, konuyla ilgili kurum dışındaki paydaşların ve kurum içi personelin, kurumsal prosedürleri aşarak Komiserle doğrudan temas kurma şans ve isteği azalmaktadır.

4.2.2. Komisyon (Kurul) modeli

Veri Koruma Yasalarının tüm yetkiyi bir grup kişiye verdiği yapıya Komisyon modeli denilmektedir. Bu yapıda yetkiler bir alt komiteye veya gruba devredilebilmektedir. Birden fazla kişinin olması nedeniyle, Komisyondaki üyelerin çalışma saatleri tam gün veya yarım gün olarak esnek tayin edilebilmektedir. Bazen bir dizi farklı komite de bu yapının içinde kurgulanabilmektedir.

Komisyon ifadesine alternatif olarak, ülkemizde ve İngilizce'de yaygın kabul gören "Kurul" (Board) kelimesi de yetkili bir grubu işaret etmekte olup, bu çalışmada Komisyonla eş anlamda kullanılmaktadır.

Komisyon Modelinin avantajları:

- Tek bir Komiserde bulunması mümkün olmayan; farklı disiplinlerden bir araya getirilmiş kişilerin konuyu algılama ve kavrayış farklılığı ile korumanın daha geniş bir perspektifle ele alınabilmesi,
- Veri işleme ile ilgili farklı gruplara mensup kişilerin –tüketiciler, bireyler, veri sahipleri, devlet, akademisyenler, iş dünyası- komisyonda temsil edilmesi ile katılımcılık unsurunun sağlanması,
- Uzlaşmacı karar alma unsurunun sağlanması,
- Üyelerin görevlerinin sona ermesi veya üyeliğin boşalması gibi unsurlardan bağımsız olarak, kurumsal bilgi ve kültürün gelişerek birikim yaratma imkanı,
- Üyelerin belli aralıklarla değişiminin sağlanarak hukuka uygun ve belirlenmiş üye seçim kriterinin varlığı olarak sayılabilir.

Komisyon modelinin dezavantajları ise şöyle sıralanabilir:

- Tek bir Komisere kıyasla karar alma sürecinde birden fazla kişiyi bir araya getirmek için katlanılan maliyet daha yüksektir.
- Karar alma sistemi etkinlikten uzaklaşmakta ve bürokrasi yaratılmaktadır.
- Çekişmeli konularda ihtilaf doğabilmekte ve karar alma sürecinde gecikme, zaman zaman kilitlenme yaşanabilmektedir.
- Üye sayısının fazlalığı nedeniyle, veri korumada "kamusal figür" olarak tanınacak bir kişinin bulunmayışı, konunun ilgi görme ihtimalini azaltmakta; nihayet bu durum kamuoyunun veri koruma konusundaki bilgi düzeyinde olumsuz etki yaratabilmektedir.[158]

Fransa *(CNIL - Commission nationale de l'informatique et des libertés)*, Belçika *(the Commission de la protection de la vie privée)*, Lüksemburg *(CNPD-Commission nationale pour la protection des données)*, Malta *(Data Protection Commission)*, ABD'de bazı yapılar ve Güney Kore (*Bilgi Güvenliği Ajansına bağlı*

[158] Bu dezavantaj çoğu kez bir Komisyon Başkanı ile giderilmektedir.

"Kişisel Veriler ile ilgili Uzlaşı Komitesi[159]*)*'deki veri koruma ile ilgili yapılar komisyon modeline örnek gösterilebilir.

4.2.3. Çok amaçlı ajanslar

Bazı ülkelerde veri koruma ile ilgili yapılanmalar birbiriyle ilişkili birden fazla fonksiyonu bir arada yürütmektedir. Çok amaçlı ajanslar, mevcut yapılara veri koruma ile ilgili görevler tayin etmek şeklinde oluşabileceği gibi, kurulan veri koruma kurumlarına benzer nitelikte başka görevler vermek suretiyle de yapılandırılabilir. Bu şekilde, farklı kurumlar kurulmasının önüne geçilmekte ve ilişkili konuların genişlemesiyle bir sinerji elde edilmektedir.

Bu modelde, bilgi edinme hakkı ile veri koruma fonksiyonlarını birleştirmek şeklinde tezahür eden yapı en bilinen örnektir. Kanada'nın birçok eyaleti, Macaristan, Almanya'nın bazı eyaletleri ve İngiltere'de mahremiyet ve bilgi edinme hakkının sağlanması görevleri tek bir Komiserde birleşmiş durumdadır.

Bazı ülkelerde ise veri koruma kurumları mevcut ombudsman'larla[160] birleştirilmiştir. Benzer şekilde, sektörel veri koruma kanunları çıkararak her bir kanunu ilgili sektörün düzenleyici veya şikayet merciine tabi kılan yapılar da dikkat çekmektedir. Bununla birlikte bir veri koruma kurumu kuran ve fakat bağlayıcı karar alma ve davalara bakma işini özel bir mahkemeye (tribunal) veren ülkeler de bulunmaktadır.

Çok amaçlı kurumların avantajları:

- Yeni kurum kurulmasının yaratacağı maliyetlerden tasarruf etmek, mevcut yapılarla işin yapılmasını sağlamak,
- Daha geniş bir uzmanlık ile konuya yaklaşarak ilgili kurumlarla daha rahat koordinasyon sağlayabilmek,

---

[159] Ayrıntılı bilgi için bkz. Privacynet. The Personal Information Dispute Mediation Committee (PIDMC). <http://www.kisa.or.kr/kisae/privacy/jsp/privacy_02_01.jsp>

[160] Ombudsman kelimesi İsveç dilinde "aracı" anlamına gelen "ombuds" ve "kişi" anlamına gelen "man" kelimelerinden oluşmuştur. Kurumsal olarak Ombudsman terimi, Parlamento tarafından halkın şikayetlerini dinleyip, çözümlere ulaştırmak üzere seçilmiş kimse veya kimseleri simgelemektedir. Türk Dil Kurumuna göre bu kavram hukukta *"Parlamento tarafından görevlendirilen, vatandaşları resmî makamların keyfî ve yasa dışı davranışlarına karşı korumakla görevli kişi veya kurum."* anlamında kullanılmaktadır. TDK, bu söz için "kamu denetçisi" karşılığını önermektedir.

- Ayrı bir kurum kurulmasını gerçek anlamda gerektirmeyen küçük ülkelerde veya eyaletlerde mevcut yapıların kullanılması ya da aynı kuruma birden fazla görev verilmesi ile maliyet avantajı ve etkinlik sağlamak.

Çok amaçlı kurumların dezavantajları ise şöyle sıralanabilir:

- Odaklanmış ve uzmanlaşmış bir veri koruma altyapısı mümkün olamamaktadır.
- Bu tür kurumlarda çalışan personel çoğu kez benzer yapıda birçok konuyla ilgilendiğinden veri koruma alanında etkin ve derinleşmiş bir uzmanlık elde edilememekte ve kalifiye personel konusunda sorunlar yaşanmaktadır.

4.2.4. Karma modeller

Veri koruma kurumları, zaman zaman komiser veya komisyon modellerinden esinlenilerek karma yapıda tasarlanmaktadır. Örneğin; komiserle birlikte bir danışman komitenin yer aldığı karma model de görülmektedir. Bu yapılarda farklı yapıların avantajları ve uzmanlık bilgisinin bir araya getirilerek etkinliğin artırılması hedeflenmektedir. Avustralya Mahremiyet Kanunu (1988)[161] ile kurulan yapı da bir karma modeldir. Bu Kanuna göre kurulan Danışma Komitesi en fazla altı üyeden oluşmakta olup, bir Komiser bu Komiteye başkanlık etmektedir.

4.3. Veri Koruma Otoritelerinin Özellikleri

4.3.1. Bağımsızlık ve özerklik

Veri koruma otoritelerinin sahip olmaları gereken en önemli iki özellik özerklik ve bağımsızlıktır. *Özerklik,* bir kurumun görevlerini yerine getirirken hiçbir organ, makam, merci veya kişiden emir, talimat veya izin almamasıdır. *Bağımsızlık* ise bir yandan hükümete, düzenlenen ve denetlenen sektöre, medyaya, diğer kamu idarelerine ve gerçek ve tüzel kişilere karşı özerkliğin; öte yandan kurul üyelerinin düşünce ve kanaatlerini serbestçe dile getirip oylarını özgürce kullanabilmelerinin sağlanmasıdır. Birinci manada bağımsızlık genellikle "dışsal bağımsızlık", ikinci manada bağımsızlık ise "içsel bağımsızlık" olarak nitelendirilmektedir. Dışsal

[161] Bu Kanunun yedinci bölümünde model varyasyonunu örneklendiren yapı yer almaktadır. Avustralya Mahremiyet Kanunu (1988) için bkz. <http://www.privacy.gov.au/law> .

bağımsızlık, başta kurul üyelerinin seçimi, atanması ve görev sürelerinin yasa koyucu tarafından düzenlenmesi, diğer kamu görevlilerine nazaran bu kurulda çalışan üyelerin daha güvenceli konuma getirilmesi ve kurul işlemlerinin klasik idari denetim mekanizmalarından (hiyerarşi, idari vesayet) arındırılmasıyla sağlanır. İçsel bağımsızlık ise, kurul üyelerinin alınan kararlara muhalif kalabilme, aksi yönde düşündüklerinde alınan karara şerh düşebilme ve kararların alınması aşamasında görüş ve düşüncelerini özgürce savunabilme imkanının yaratılmasıyla sağlanır.[162] Özerklik ve bağımsızlık kavramları birlikte değerlendirildiğinde, söz konusu otoritenin konuyla ilgili olan veya olmayan hiçbir kurumdan veya kişiden baskı görmemesi, siyasi etkilerden uzak olması anlaşılmalıdır.

Veri koruma otoriteleri görevlerini yerine getirirken bu kurumların fonksiyonel olarak onları kuran yürütme ve yasama erklerinden bağımsız olmaları gerekmektedir. Bu bağımsızlık kriteri, bir veri koruma kurumunun somut bir olayda başka bir organ tarafından talimat almaksızın kendi kararını almayı sağlamayı hedefler.[163]

VKD'nin 28'inci maddesi de veri koruma otoritelerinin "tam bağımsız" olmaları gerektiğini vurgular. Bygrave'e göre bu bağımsızlık, idari ve yasal düzenlemeler ile bu kurumlara diğer kurum veya kişilerden talimat verilmesine kapı açan küçük bir izne bile yer verilmemesi gerektiğini ifade eder.[164] Düzenleyici kurumun bağımsızlığını sağlayacak birkaç husus bulunmaktadır. Bunlardan en önemlileri; ilgili kanunun veri koruma otoritesinin bağımsız olduğunu vurgulaması, o otoritenin yeterli mali ve insan kaynaklarına sahip olması ile işlerini doğru ve kesintisiz yerine getirebilmesi ve bu suretle de siyasi etkilere maruz kalmamasının sağlanmasıdır. Pek çok veri koruma otoritesi hukuken bağımsız olsa da, bunların bir kısmı diğer kamu kurumları veya yargı makamları içinde konumlanmaktadır. Böylece bu kurumlar doğrudan siyasi etkiye maruz kalabilmektedir. Özellikle, 2004 yılında AB'ye üye olan bazı Baltık ülkeleri gibi ülkelerde veri koruma kurumları bağımsız kurumlar olarak değil, diğer kamu kurumlarına bağlı olarak kurulmuşlardır. Bazı eski üye ülkelerin veri koruma otoritelerinde de benzer bir şekilde siyasi

[162] Altundiş, 2006
[163] Bygrave, 2002:70
[164] Bygrave, 2002:71

etkilerden bağımsız olmak tam olarak sağlanamamıştır, özellikle de Almanya'da. Almanya'da federal veri koruma kanunu müstakil bir kanun ise de, bazı eyaletlerde veri koruma otoriteleri İçişleri Bakanlığına bağlıdır. 2005 yılında Avrupa Komisyonu Alman Federal Devletine bir mektup iletmiş, bu mektupta 16 eyaletteki yerel veri koruma otoritelerinin yeterli bağımsızlığa sahip olmadıkları, şayet bu durum giderilmez ise Almanya'nın Avrupa Adalet Divanında yargılanacağı belirtilmiştir. Komisyonun VKD'nin uygulanmasına ilişkin ilk uygulama raporunda da[165] belirtildiği gibi, pek çok otorite yeterli mali ve insan kaynağına sahip değildir. Ancak İspanya gibi bazı ülkelerde yeterli kaynaklar bulunmaktadır.[166] Yine Kurul üyelerinin atanması, görevden alınması ve özlük haklarının kanunla düzenlenmesi Kurulun bağımsızlığını sağlamada önemli etkenlerdendir.

BM İnsan Hakları Komisyonu'nun 1992/54 ve BM Genel Kurulu'nun 1993 yılında 48/134 sayılı kararıyla kabul ettiği Paris İlkeleri[167] de, insan hakları ile ilgili ulusal kurum ve kuruluşlarda bulunması gereken özellikleri sıralarken, bu kurum ve kuruluşların bağımsızlığına özel bir vurgu yapmaktadır. Bunun için Komiser veya Kurul üyelerinin atanma ve görev süresinin kanunla açık ve net bir biçimde hükme bağlanması gerektiğinin altını çizmektedir. İnsan hakları ile ilgili ulusal kurumların yükümlülükleri Paris İlkelerinde şöyle ele alınmaktadır:

- Bu kurumlar görev alanlarıyla ilgili insan hakları ihlallerini izleyeceklerdir. Önemli insan hakkı ihlalleri, ilgili bir yasa çıkarılması veya uluslararası insan hakları ile ilgili konularda hükümeti, meclisi ve yetkili makamları bilgilendirecek ve danışmanlık yapacaktır.
- Bu kurumlar, ilgili ulusal ve uluslararası organizasyonlarla temas içinde olacaktır.
- İnsan hakları ile ilgili konularda vatandaşları bilgilendirecek ve eğitim vereceklerdir.

[165] Bkz. "Analysis and impact study on the implementation of Directive EC 95/46 in Member States", 2003, <http://ec.europa.eu/justice_home/fsj/privacy/docs/lawreport/consultation/technical-annex_en.pdf>
[166] Kuner, 2007:17
[167] "The Paris Principles" için bkz. http://www2.ohchr.org/english/law/parisprinciples.htm

- Bu kurumlar, yargı benzeri karar alma ehliyeti ile donatılacaklardır (quasi-judicial competence).

25 Eylül 2001 tarihinde Paris'te 23'üncüsü gerçekleştirilen Uluslararası Veri Koruma ve Mahremiyet Komiserleri Konferansında kabul edilen *Veri Koruma Otoritelerinin Akreditasyon İlkelerine İlişkin Karar*[168] (bundan böyle *Akreditasyon İlkeleri Kararı* olarak anılacaktır) da veri koruma otoritelerinde bulunması gereken özellikleri belirlemekte; ulusal, eyalet veya il bazında örgütlenmiş veri koruma otoriteleri ya da sadece belli bir alana özgü çalışan veri koruma otoritelerine – örneğin, sağlık kayıtlarının mahremiyeti ile ilgili bir kurum- ilişkin ilkeler öngörmektedir. Söz konusu Karar, veri koruma otoritelerinin bağımsızlık ve özerkliğini garanti etmek üzere, aşağıdaki akreditasyon ilkelerini öngörmektedir:

Kurum başkanı veya Komiser;

- *Belirli* bir dönem için atanacaktır.
- Görevi ihmal veya meslekten çıkarılmayı gerektiren bir suçtan dolayı hüküm giymek veya sağlık bakımından görevini yerine getiremeyecek durumda olmak dışındaki gerekçelerle görevden alınamayacaktır.
- Doğrudan hükümet başkanına veya yasama organına raporlama ve kurumun görevleriyle ilgili resmi açıklama yapabilecektir.
- Görevi dolayısıyla yürüttüğü faaliyetler nedeniyle dokunulmazlık hakkı olacaktır.
- Soruşturma başlatma yetkisini haiz olacaktır.

Akreditasyon, uluslararası veri alışverişlerinde muhatap ülkedeki veri koruma otoritesinin güvenilirliği bakımından önem arz etmektedir. Uluslararası akreditasyon için, her yıl düzenlenen Uluslararası Mahremiyet ve Kişisel Verilerin Korunması Konferansından en az 3 ay önce, Konferansın ilgili Komitesine başvuru yapılması gerekmektedir. 2005 yılında Montrö'de 27'ncisi gerçekleştirilen Uluslararası Mahremiyet ve Kişisel Verilerin Korunması Konferansında, bu Konferansın ilgili

[168] International Conference of Data Protection Commissioners, "Criteria and Rules for Credentials Committee and the Accreditation Principles" as amended on 9-11 September 2002. 9 Şubat 2010. <http://www.privacyconference2003.org/pdf/Criteria_and_Rules.pdf>

Komitesi tarafından Lüksemburg (National Data Protection Commission), Kanada (Saskatchewan, Information and Privacy Commissioner), İsviçre (Canton of Basel-Landschaft, Data Protection Commissioner) ve İspanya (Basque Country, Data Protection Commissioner) veri koruma otoriteleri akredite edilmiştir.

4.3.2. Özerk bütçe

Veri koruma otoritelerinin bağımsızlığını sağlayacak unsurlardan biri de uygun nitelikte finansman yapısıdır. Yargı benzeri karar verme yetkisi bulunması gereken bir veri koruma otoritesinin bütçesinin herhangi bir kurum veya kuruluşun bütçesine bağlı olması, o otoritenin kararlarının da bağımsızlığına gölge düşürecek niteliktedir. Örneğin, bir bakanlık içinde kurulmuş veri koruma kurumu, ayrı bütçesinin olmaması nedeniyle bağımsız olarak hareket edemeyebilecektir.

4.3.3. Veri koruma otoritelerinde bulunması gereken diğer özellikler

Yukarıda, VKD'nin *28'inci maddesi*, BM'in kabul ettiği *Paris İlkeleri* ve Veri Koruma ve Mahremiyet Komiserleri Konferansında kabul edilen *Akreditasyon İlkeleri Kararı* uyarınca, veri koruma otoritelerinde bulunması gereken özelliklerden "bağımsızlık" hususu incelenmiştir.

Bağımsız olması gereken her tür kurumsal yapıda aranacak özelliklerden ilki, o kurumu *kanunla kurmak* ve kurumda çalışacakların atanma ve görevden alınma esas ve usullerini de kanunla hükme bağlamaktır. Keyfiliğin ve kayırmacılığın önlenmesini sağlayacak bu hususun dışında, görev yapma süreleri, kurumun yasama veya yürütmenin başındaki kişiye doğrudan raporlama yapması ve yargı benzeri karar verme yetkisiyle donatılmış olması, kurumun başındaki kişinin (komiser, başkan vs.) görevi süresince diğer bir iş veya meslekle iştigal etmemesi, Kurul üyelerinin görevden alınamaması da yine kanunla düzenlenmelidir. Ayrıca, veri koruma otoritelerini siyasi etki, kontrol ve imtiyazlara karşı koruyacak, kurumun görev alanıyla ilgili konularda basına demeç verme yetkisi ile bağımsız hareket edilmesini temin edecek açık ve anlaşılır kanun hükmünün tesisi de gerekebilmektedir.

4.4. Veri Koruma Otoritelerinin Görevleri

Veri koruma otoritelerinin en tipik görevi, vatandaşların kişisel verilerinin işlenmesi konusundaki şikayetlerini ele almak ve çözüm üretmektir. Bu kurumlar aynı zamanda, şikayetlerden bağımsız olarak veri işleme operasyonlarının hukuka uygunluğunu da denetlemekte; hükümete, meclise, özel ve kamu kurum ve kuruluşlarına veri koruma konularında danışmanlık hizmeti vermektedirler. Bununla birlikte, bir veri koruma kurumu genellikle kamu tarafından erişilebilir olan ve farklı veri işleme operasyonlarının ayrıntılarını içeren sicili tutmakla ve hükümete ve meclise yıllık olarak faaliyetlerini raporlamakla da görevlidir.[169]

Akreditasyon İlkeleri Kararı'na (2001) göre, bir veri koruma otoritesi yasaya uygunluk denetimi, soruşturma, durumun düzeltilmesi/iadesi (tazminat-redress), rehberlik, danışmanlık ve kamunun bu konuda eğitilmesi görevleri ile sorumlu olmalı ve idari uygulamada bu görevleri yerine getirecek kapasitede yapılandırılmalıdır.

Uluslararası alanda veri koruma otoritelerinin yetki ve görevlerini en ayrıntılı olarak ortaya koyan düzenleme AB Veri Koruma Direktifidir. VKD'nin 28'inci maddesi, her üye ülkenin bir veya birden fazla veri koruma otoritesi (supervisory-üst kurul) kurmasını ve bu kurumların kendilerine verilen görevleri yerine getirirken tam bağımsız bir şekilde hareket etmelerinin temin edilmesini ortaya koyar. VKD'ye göre söz konusu kurumsal yapıların aşağıdaki görevleri yerine getirmek üzere yapılandırılması ve devletlerin bu koşulları temin etmeleri beklenmektedir:

- Bireylerin kişisel verileriyle ilgili hak ve özgürlüklerini ilgilendiren her tür idari düzenleme ve tedbir için bu kurumlardan görüş alınacaktır.
- Otoriteye, denetim (supervisory) görevini yerine getirmesinde her tür veriye erişim hakkı ile araştırma yapma yetkisi (investigation) sağlanacaktır.
- Veri işlemenin kişi hak ve özgürlükleri ile ilgili belli riskleri taşıdığı durumlarda, veri kontrolörünün veya denetim görevlisinin bildirimi üzerine kurum, veri işleme süreçlerini ve yöntemlerini belirleyecektir. Belirlenen yöntem veya süreçleri ilgili kişilerin istifade etmesi için ilan edebilecektir.

[169] Bygrave, 2002:70

- Kurum, gerekiyorsa veriyi işleyeceklere verileri silme veya bloke etme talimatını verebilecek, işleme ile ilgili belirli veya geçici bir yasak koyabilecek, veri kontrolörünü uyarabilecek, önemli konuları ulusal meclis veya diğer siyasi alanlara taşıyabilecektir.
- VKD çerçevesinde o ülkede çıkarılmış kanunların ihlali durumlarında, kendi görev alanındaki durumlara müdahale edecek, konuyu yargı mercilerine taşıyabilecektir. Kendisi yaptırım uygulayabileceği gibi, mahremiyet kanunlarının uygulanmasında polis, mahkemeler ve diğer hukuk uygulayıcı mercilerle işbirliği yapacaktır. Veri Koruma Kurumlarının verdikleri kararlara karşı yargı yolu açık olacaktır.
- Kişiler veya bir kişiyi temsil eden birlik ya da kuruluşlar tarafından kişisel veri işlenmesi ile ilgili hak ve özgürlükler hakkındaki iddiaları inceleyecektir.
- Düzenli aralıklarla kurumun faaliyetlerini raporlayacaktır. Bu rapor, herkesin erişebileceği şekilde kamuoyuna ilan edilecektir.
- AB üyesi ülkelerdeki veri koruma kurumları ile gerekli işbirliğini yerine getirecek ve ihtiyaç halinde ilgili verileri paylaşacaktır.[170]
- Kurumun üyeleri ve diğer personeli görev süreleri sona erdikten sonra dahi görev nedeniyle öğrendikleri mesleki gizli bilgileri saklamakla yükümlü olacaklardır.

Söz konusu görevler, özel uzmanlık gerektiren işlerden olup, bu görevlerin yerine getirilmesi ancak veri koruma alanında ihtisaslaşmış Kurumların varlığı çerçevesinde, vatandaşların mahremiyet ve verilerinin korunmasını talep etme haklarının garanti altına alınması ile mümkündür.

4.5. Atanma Usulü

Ülkeler veri koruma otoritelerine atama yaparken genel olarak aşağıda anlatılan iki yöntemden birini kullanmaktadırlar.

[170] OECD üyesi ülkelerde de Mahremiyet Koruma Kurumlarının işbirliği yapmalarını tavsiye eden OECD Tavsiye Kararı (Recommendation on Cross-border Co-operation in the Enforcement opf Laws Protecting Privacy, 2007) için bkz. <http://www.oecd.org/dataoecd/43/28/38770483.pdf>

4.5.1. Yasama organı tarafından atanma

Yasama organı doğrudan atama yapabileceği gibi, bu süreçteki rolü yalnızca kuruma aday gösterme veya atamayı onaylama da olabilmektedir. Yasama organınca yapılan atamanın temel avantajları şöyle sıralanabilir:

- Kurumun statüsü ve prestijine olumlu bir katkı sağlar.
- Atanan kişi Parlamentonun, dolayısıyla kamunun ve vatandaşların potansiyel olarak güvenini kazanmaktadır.
- Yasama organı ile kurum arasında ilişkilerin gelişmesine vesile olur. Bu da Parlamentodaki temsilcilerin, kişi haklarının korunmasında görev yapacak kişilerle işbirliği içinde hareket etmelerine zemin hazırlar.

Yasama tarafından yapılan atamanın dezavantajları ise şunlardır:

- Atama siyasi etkiye maruz kalabilir.
- Herhangi bir siyasi sorun veya kriz nedeniyle atama gecikebilir.

4.5.2. Hükümet başkanı tarafından atanma

Veri Koruma Otorite yetkilisinin, ilgili ülkedeki devlet yapısı ve örgütlenmesine göre; hükümet veya devlet başkanı ya da başka bir devlet temsilcisi tarafından atamasının yapıldığı örnekler de bulunmaktadır. İngiltere'de Veri Koruma Komiserinin ataması Kraliçe tarafından yapılmaktadır. Aynı şekilde Yeni Zelanda ve Avustralya'nın bazı bölgelerinde Veri Koruma Komiseri valiler tarafından atanmaktadır. Devlet Başkanı ve hükümet gibi, merkezi yapının başındaki kişilerce yapılan atamalar, veri koruma otoritelerinin saygınlık ve etkinliğini artıran faktörlerdendir.

4.6. Görevden Alma

Bağımsız idari yapılarda kurum temsilcisi ancak görevi yerine getiremeyeceğine dair genel kanaatin oluştuğu belirli durumlarda görevden alınabilmektedir. Görevi yerine getiremeyecek bir suç ile hüküm giymiş olmak, fiziki veya psikolojik bir rahatsızlık sebebiyle görevin gereğini ifa edememek, meslekte kalmanın uygun olmadığına dair bir yargı kararı veya uygunsuz davranış ya da

hareketler göreve son verilmesi için kanunla hükme bağlanması uygun olacak sebeplerdir.

Hukuki bakımdan geçerli bir görevden alma işlemi, "usulde paralellik" ilkesi gereği, atamayı yapan makam veya merciin işlemi ile gerçekleştirilebilir. Bununla birlikte, bağımsızlığın güçlendirilmesi adına atama işleminin iptalinden önce, görevden alma işlemi, atamayı yapıp yapmadığına bakılmaksızın Yasama organının da iznine tabi tutulabilmektedir.

4.7. Görev Süresi

Veri koruma kurumlarında genel olarak görev süresi bağımsızlığın sağlanabilmesi için uzun bir süre olarak belirlenmektedir. Bu süre, birçok ülkede 5 ve 7 yıl arasında değişmektedir.

4.8. Ülke Örnekleri

Tablo 4.1. Ulusal Mahremiyet ve Veri Koruma Otoriteleri

Ülke	Mahremiyet ve Veri Koruma Birimleri	Kurum Modeli
Almanya	Federal Veri Koruma Komiserliği (Bundesbeauftragter für den Datenschutz und die Informationsfreiheit) (Ayrıca 18 adet eyalet veri koruma otoritesi bulunmaktadır)	Komiser Modeli
Avustralya	Federal Mahremiyet Komiseri (Australian Federal Privacy Commissioner) (Ayrıca 4 adet eyalet veri koruma otoritesi bulunmaktadır.)	
İrlanda	Veri Koruma Komiseri (Data Protection Commissioner)	
Kanada	Federal Mahremiyet Komiseri (Privacy Commissioner) (Yerel düzeyde mahremiyet kanunları ile ilgili ayrı bir ofis de var.)	
Norveç	Veri Denetçisi (Datatilsynet- Data Inspectorate)	
Belçika	Veri Koruma Ajansı (Data Protection Agency- the Commission de la protection de la vie privée)	Ajans Modeli
Danimarka	Veri Koruma Ajansı (Data Protection Agency-Datatilsynet)	
İtalya	Veri Koruma Ajansı (Regulatory Authority for the Protection of Personal Data - Garante per la protezione dei dati personali)	
Finlandiya	Veri Koruma Ombudsmanı (Office of the Data Protection Ombudsman)	
Avusturya	Veri Koruma Komisyonu (Datenschutzkommission)	Komisyon (Kurul) Modeli
Fransa	Enformatik ve Özgürlükler Milli Komisyonu (CNIL–Commission nationale de l'informatique et des libertés)	
Lüksemburg	Veri Koruma Ulusal Komisyonu (Commission nationale pour la protection des données)	
Portekiz	Veri Koruma Komisyonu (Comissão Nacional de Protecção de Dados)	
Güney Kore	Bilgi Güvenliği Ajansına bağlı Kişisel Veriler ile İlgili Uzlaşı Komitesi (The Personal Information Dispute Mediation Committee (PIDMC))	
Yunanistan	Veri Koruma Otoritesi (Hellenic Data Protection Authority)	

Kaynak: Austrian Data Protection Commission, Hyperlinks of Data Protection Authorities, (http://www.dsk.gv.at/site/6280/default.aspx) sayfasından bu çalışma kapsamında derlenmiştir.

Veri koruma otoriteleri farklı ülkelerde farklı isimler altında örgütlenebilmektedir. Yukarıdaki Tablo 4.1'de veri koruma alanında uluslararası alanda öne çıkan bazı ulusal mahremiyet ve veri koruma otoriteleri verilmektedir.

4.8.1. Fransa Enformatik ve Özgürlükler Milli Komisyonu

Fransa'nın veri korumadan sorumlu otoritesi olan Enformatik ve Özgürlükler Milli Komisyonu (CNIL)[171], 6 Ocak 1978 tarihli Veri Koruma Kanunu ile kurulmuş bağımsız bir Komisyondur. Kanun, kamu ve özel kurum ve kuruluşların tuttukları verileri kapsamakta olup, kişisel veri işleyen herkesin daha önceden bu Komisyona başvurarak kayıt olması ve izin alması gerekmektedir. Veri toplayanlar, bireylere veri toplama sebeplerini bildirmek zorundadır. 17 kişiden oluşan Komisyonda Parlamentodan 4 (2 milletvekili ve 2 senator olmak üzere), Ekonomik ve Sosyal Konsey'den 2 ve yüksek yargı organlarından 6 kişi (2 kişi Danıştay "Conseil d'Etat", 2 kişi Yargıtay "Cour de Cassation" ve 2 kişi Hesap Mahkemesi "Cour des Comptes") bulunmaktadır. Kalan 5 kişiden üçü Bakanlar Kurulu, 1 kişi Meclis Başkanı ve 1 kişi de Senato Başkanı tarafından atanmakta olup, Komisyonun çalışma usul ve esasları bir iç tüzükle belirlenir. Görevini yerine getiremeyeceği anlaşılan üyenin (suç, hastalık gibi sebeplerle) yerine kalan süreyi tamamlamak üzere, o kişinin atanmasındaki usule paralel olarak yeni üye atanır. Komisyon'un görev süresi, parlamento üyelerinin seçim dönemine paralel olarak 5 yıldır. Üyeler bir kez daha seçilebilirler ancak toplam görev süresi 10 yılı aşamaz. Bağımsız bir otorite olması nedeniyle, Komisyon Başkanı, ilgili Kanunun 13'üncü maddesi gereği hiçbir Bakan, kamu otoritesi, kamu veya özel şirket yöneticisi veya diğer otoritelerden emir veya talimat almaksızın Komisyon üyeleri arasından seçilir. Ayrıca biri vekaleten olmak üzere iki Başkan yardımcısı seçilir. Başkan ve yardımcıları Yönetim Kurulunu (bureau) oluştururlar. Üyelerin başka bir işle iştigal etmeleri yasaktır.

Bağımsızlık unsuru gereği, Komisyon üyelerine görevlerini yerine getirirken ve yetkilerini kullanırken hiçbir kurum emir ve talimat veremez. Komisyon her yıl Başbakana ve Parlamentoya raporlama yapar ve Başkan çalışma arkadaşlarını özgür ve bağımsız olarak kendisi seçer.

[171] CNIL (Commission nationale de l'informatique et des libertés)

4.8.1.1. Görevleri

CNIL'in kuruluş Kanununun 11'inci maddesinde, Komisyonun temel görevlerinin veri özneleri ve veri kontrolörlerine hak ve görevleri konusunda bilgi vermek ile kişisel verilerin işlenmesinde bu Kanunun uygulanmasını temin etmek olduğu belirtilmektedir. Bu temel görevleri yerine getirebilmek için Komisyonun kanunla belirlenmiş diğer görevleri şöyle sıralanmaktadır:

a- Siyasi, felsefi, tıbbi, cinsel hayat, genetik veriler, mahkumiyete ilişkin bilgiler ile sosyal güvenlik numarası, biyometrik veriler, devletin güvenliği, vatandaşlık hizmetleri ve çevrimiçi kamu hizmetleri ile ilgili alanlarda veri işlenmesine ilişkin *görüş vermek* ve diğer veri işlemelerine ilişkin kamu kesiminden ve özel sektörden bildirimleri almak,

b- Gerektiğinde sistem güvenliğine ilişkin standart düzenlemeler yayımlamak,

c- Devam eden kişisel veri işlemeleri ile ilgili iddia, şikayet ve dilekçeleri kabul etmek, bu kişileri kendileri ile ilgili alınmış kararlar hakkında bilgilendirmek,

d- Kamu kurumları veya mahkemelerden, gerçek veya tüzel kişilerin otomatik veri işleme sistemi kurmaya yönelik girişimlerinde soruları cevaplamak, bu kişilere görüş vermek ve tavsiyede bulunmak,

e- Veri mahremiyeti veya kişisel verilerle ilgili diğer suç hallerinde savcıya görüşleriyle birlikte bilgi vermek,

f- Kanuna aykırı hareket eden veri kontrolörleri için uyarma ve para cezası ya da "işlemenin durdurulması"; veri işlemenin temel hak ve özgürlükleri ihlal ettiği ve gecikmesinde sakınca bulunan hallerde, işlemenin 3 ay durdurulması ya da işlenen kişisel verilerin 3 ay süresince bloke edilmesi cezalarını vermek, özellikle devletin güvenliğine yönelik olan veya hassas verilerin işlendiğinin tespit edildiği durumlarda, Başbakana ihlalin durdurulması için bildirimde bulunmak,

g- Veri işleme ile ilgili çıkarılacak düzenlemelere görüş vermek,

h- Uluslararası müzakerelerde, Başbakanın talebi ile Fransa'nın kişisel veri koruma ile ilgili pozisyonunun belirlenmesine katkıda bulunmak,

i- Kanunla verilmiş görevlerini yerine getirebilmek için tavsiye niteliğinde veya düzenleyici nitelikte kararlar almak.

4.8.1.2. Bütçesinin denetimi

Fransız Veri Koruma Kanununun 12'nci maddesine göre, bu Komisyonun mali denetimini Hesap Mahkemesi (Sayıştay-Cour des Comptes) yapmaktadır. Bu madde, Fransa'nın mali yönetimine ilişkin 1992 tarihli genel Kanunun uygulanmasını dışlamaktadır. Böylece, bağımsız düzenleyici ve denetleyici bir otorite olarak CNIL'in bütçe yapısı, bağımsızlığı zedelemeyecek şekilde yapılandırılmış olmaktadır.

4.8.1.3. Faaliyetleri

2007 yılında 2006 yılına göre yüzde 25 artışla CNIL'e 4.455 adet şikayette bulunulmuş olup, CNIL bu şikayetler hakkında, 2006 yılına göre yüzde 30 artışla 393 adet cezai karar almıştır. Şikayetlerin büyük çoğunluğu telekomünikasyon, bankacılık, istihdam gibi sektörlerin veri işlemelerine ilişkin olup, bu şikayetler çoğunlukla veri işlemelerine itiraz niteliğindedir. Aynı yıl, CNIL, Fransa'da 56.404 hukuka aykırı kişisel veri dosyasının işlendiğini tespit etmiştir. Bunların dışında CNIL yine 2007 yılında;

- Denetim: 164 tahkikat, 140 kurum ve kuruluş denetimi yapmış,
- Yetkilendirme: 214 yetkilendirme ve 26 yetki reddi kararı almış, hassas veya yüksek riskli veri işleme konusunda 22 görüş vermiş,
- Yaptırım: 5.000-50.000 Avro arasında değişen 9 adet mali ceza ve 5 uyarı cezası vermiş; muhatabını uymakla yükümlü kılan 101 resmi bildirimde bulunmuştur. [172]

CNIL'in 2004 yılından 2007'ye kadar olan sürede verdiği kararların yüzde 70'i özel sektöre yönelik kararlardır. Asıl görevleri, danışmanlık, delil doğrulama ve

[172] CNIL, 2007

denetleme olmasına rağmen, Danıştay'ın CNIL'i son zamanlarda tam ehliyetli bir yargı mercii olarak nitelendirmesiyle, Komisyon, görüş veren bir Kurumdan ziyade, başta özel sektöre yönelik olmak üzere tam ve gerçek bir *regülasyon* otoritesi haline gelmiştir. Zira Fransa'da 30 yılını doldurmuş olan bu kurum, bağımsızlığına karşı müdahalelere oldukça sert yanıtlar vermektedir. 2007 yılı raporunda CNIL Başkanı, 30 yıllık tecrübenin sonucunda, bağımsızlığı korumanın önemli bir değer olduğunu ifade etmektedir.

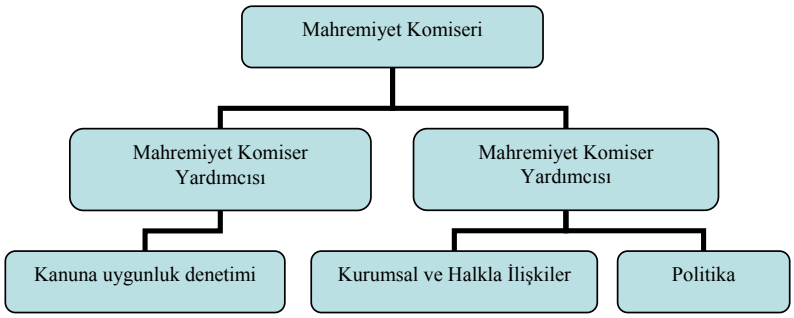
4.8.2. Avustralya, Mahremiyet Komiseri Ofisi

Avustralya'da veri koruma ile ilgili çalışmalarını sürdüren Mahremiyet Komiseri Ofisi (Office of the Privacy Commissioner), uluslararası alanda Asya Pasifik Mahremiyet Otoriteleri'nin sekreterya görevini de yerine getirmekle adını sıkça duyurmaya başlamıştır. Avustralya Mahremiyet Komiseri Ofisini ihdas eden Mahremiyet Kanunu, 1988 yılında yürürlüğe girmiştir.

4.8.2.1. Kurumsal yapısı

Ofisin organizasyon şeması şu şekildedir:

Şekil 4.1. Avustralya Mahremiyet Koruma Ofisi Organizasyon Şeması



Kaynak: Australian Government, Office of the Privacy Commissioner, *The Operation of the Privacy Act Annual Report,* 2008, s.5.

Avustralya Mahremiyet Koruma Ofisinin politikadan sorumlu birimi de Komisere mahremiyet konusunda danışmanlık yapmaktadır. Bu birim ayrıca, Kanunun yorumlanmasında ve mahremiyetle ilgili düzenlemelerin yapılmasında, bu düzenlemelerin Kanuna aykırı olup olmadığı konusunda Komisere görüş

vermektedir. Kurumsal ve halkla ilişkiler birimi ise Ofisin İnternet sitesinin geliştirilmesi, basın müşavirliği, sekreterya gibi destek hizmetlerini yürütmektedir.

Avustralya'da bunların dışında, yukarıda karma model alanında da örnek verildiği üzere bir Danışma Komitesi bulunmaktadır. Mahremiyet Kanununun 82'nci bölümünde bahsi geçen bu Komitenin üyeleri merkezi hükümet tarafından atanmaktadır. Komitenin temel görevi, Komisere özel sektör, kamu ve vatandaşların mahremiyetlerinin korunmasına ilişkin görüş ve önerilerde bulunmaktır.[173] Komiser dışında Komitenin üye sayısı altıdır.

4.8.2.2. Görevleri

Mahremiyet Komiser Ofisi'nin temel görevi mahremiyetin korunması ve bu korumanın teşvik edilmesini sağlamaktır. Bu amaçla Ofis, bağımsız, tarafsız ve bütünlük içinde, Kanunun ihlal edilmesi ile ilgili araştırma ve ihlal durumunda soruşturma yapmak, kurum ve kuruluşların Mahremiyet Kanunu ile uyumlu çalışıp çalışmadığını denetlemek, mahremiyet ile ilgili vatandaşlara ve kamu kurum ve kuruluşlarına danışmanlık yapmak ve ülkedeki mahremiyet standartlarını belirlemek ile görevlidir. Ofis, bunların yanında mahremiyetle ilgili eğitici faaliyetlerde bulunmakta ve şikayetleri incelemektedir. Şikayet başvurusu Mahremiyet Kanunun belirlediği sınırlar dahilinde makul ise Komiser tarafından gerekli araştırma yapıldıktan sonra idari bir karar verilmektedir. Bu kararlar, mahremiyeti ihlal edenlerin özür dilemesi, iş prosedürlerini değiştirmesi ve 500 ile 20.000 ABD Doları arasında değişen tazminat ödemesine ilişkin olabilmektedir. Hakkında fazla sayıda şikayet olan kurum ve kuruluşlara Ofis tarafından eğitimler de verilmektedir. 2001 yılından itibaren Ofise telefonla ve yazılı olarak yapılan şikayetlerdeki artış sebebiyle Ofis personel sayısı da artırılmıştır.[174]

Avustralya Mahremiyet Kanunu (1988) çerçevesinde Ofisin önemli görevlerinden birisi, kamu kurumlarını ve talebi halinde özel sektör kuruluşları ile

---

[173] Australian Government, Office of the Privacy Commissioner, "The Operation of the Privacy Act Annual Report", 2008:36.

[174] Avustralya Mahremiyet Komiser Ofisi'ne yapılan şikayetlerin yıllara göre istatistiklerini veren grafikler için bkz. Complaints received by the Office of the Privacy Commissioner. <http://www.privacy.gov.au/complaints/statistics>

diğer kurum ve kuruluşları denetlemektir. Ofis, denetimlerde en iyi mahremiyet uygulamalarını da teşvik etmektedir.

4.8.3. Avusturya, Veri Koruma Komisyonu

Bir Avrupa Konseyi üyesi olarak Konseyin 108 sayılı Sözleşmesini imzalamış ve iç hukukunda da onaylamış olan, ayrıca, OECD'nin veri koruma alanındaki Rehber İlkelerini de benimseyen[175] Avusturya'da VKD'yi uyumlaştırmak için 2000 yılında çıkarılan ve 1978 tarihli eski Kanunu değiştiren Veri Koruma Kanunu (Datenschutzgesetz) ile bu Kanunun uygulanmasını sağlayacak bağımsız bir Veri Koruma Komisyonu[176] ve Veri Koruma Konseyi kurulmuştur. Komisyon, 6 daimi üye, 6 yardımcı üye ve 10 tam zamanlı personelden oluşmaktadır.[177] Komisyon ve Konsey hiçbir merci veya makamdan emir almaksızın faaliyet göstermektedir. Kişisel veri işleyen herkesin bu Komisyona bildirimde bulunması veya kayıt olması gerekmektedir. Komisyon, kanunu uygulamak, kamu sektör kontrolörleri hakkında yapılan şikayetleri incelemek, kayıt sistemini yönetmek ve sınır ötesi veri transferleri için yetki vermek, veri işlemeye ilişkin şikayetleri almakla sorumludur. Komisyonun verdiği kararlara karşı idare mahkemeleri veya anayasa mahkemesine temyiz başvurusunda bulunulabilir. Komisyonun, veri korumaya ilişkin çıkarılacak her tür mevzuatta görüşleri alınmaktadır. Bu yönüyle de Komisyon danışma organı niteliğindedir.[178]

Veri Koruma Konseyi (Datenschutzrat), Komisyondan farklı olarak, Kanunun uygulanmasına değil, veri koruma konusunda önemli ve temel alanlarda görüş vermek ve karar almakla görevli bir organdır. Başbakanlık (Federal Chancellery) bünyesinde kurulmuş olan Konsey, veri korumaya ilişkin politikalar konusunda Federal Hükümete ve eyalet hükümetlerine, talep üzerine önerilerde bulunmakta, bakanlıkların veri korumaya ilişkin taslak düzenlemelerine görüş bildirmekte, kamu alanında faaliyet gösteren kontrolörlerin veri korumaya ilişkin projelerini değerlendirmekte ve bu süreçte kamu kurum ve kuruluşlarından her tür bilgi ve

[175] Pan American Health Organization, 2001:72
[176] Avusturya Veri Koruma Komisyonu için bkz. <http://www.dsk.gv.at/DesktopDefault.aspx?alias=dsken>
[177] EPIC, 2003:153
[178] A.g.e. s. 154

belgeyi isteyebilmektedir. Konsey ayrıca, veri korumaya ilişkin olarak eyalet ve federal hükümetler ile yasama organına görüş, düşünce ve eleştirilerini iletmektedir.

4.8.3.1. Komisyon ve Konseyin oluşumu

Avusturya Veri Koruma Komisyonu, Federal Hükümetin *(Bundesregierung)*[179] 5 yıllığına teklif ettiği ve Federal Başbakan (*Bundespräsident)* tarafından atanan 6 üyeden oluşmaktadır. Tüm üyelerin hukuk alanında veri koruma ile ilgili uzmanlıklarının olması ve en az bir üyenin de hakim olması gerekmektedir. Ayrıca her üye için bir de yedek üye atanmaktadır. Komisyonun karar alabilmesi için 6 üyenin de hazır olması gerekmekte olup, üyelerden birinin olmaması durumunda onun yerine yedek üye geçmektedir. Kararlar oyçokluğu ile alınmaktadır ve oyların eşitliği halinde Başkanın oyu yönünde karar alınmaktadır. Komisyonun kararlarına karşı Yüksek İdare Mahkemesinde temyiz hakkı bulunmaktadır. Komisyon, yıllık faaliyet raporu hazırlamakta ve bunu halka uygun araçlarla yayımlamaktadır.[180]

Tablo 4.2. Avusturya Veri Koruma Komisyonu üyelerinin seçimi

Teklifi yapan organ	Teklif ettiği aday sayısı	Seçilen aday
Yüksek Yargı Makamı (Yargıtay) Başkanı	3	1
Eyaletler	2	2
İş Kurumu	3	1
Avusturya Ekonomi Odası	3	1
Kamu kurumları (Circle of federal officials)	1	1

Kaynak: Federal Act Concerning the Protection of Personal Data (Datenschutzgesetz 2000-DSG 2000) md. 36'dan bu çalışma kapsamında derlenmiştir. <http://www.dsk.gv.at/site/6230/default.aspx>

Veri Koruma Konseyi, iktidar partisinin 4, ana muhalefet partisinin 3 - koalisyon durumunda her parti 3 aday- ve Mecliste temsilcisi bulunan diğer siyasi partilerden birer, eyaletler birliğinden 2 ve belediyeler birliğinden gösterilecek 1 kişiden oluşmaktadır. Bu kişilerin bilgisayar bilimleri ve veri koruma alanında profesyonel tecrübelerinin olması gerekmektedir. Konsey hükümete, yasama organına ve devletin diğer birimlerine veri koruma ile ilgili politikalarda görüş ve

[179] Federal Hükümet hakkında ayrıntılı bilgi için bkz. The Austrian Federal Government. <http://www.bundeskanzleramt.at/site/3539/default.aspx>

[180] Federal Act concerning the Protection of Personal Data. Sect.36, Composition of the Data Protection Commission. Erişim tarihi: 08 Ocak 2010. <http://www.dsk.gv.at/site/6230/default.aspx#E37>

tavsiyelerde bulunmaktadır. Bununla ilgili olarak özellikle veri korunma ile ilgili kanunlara, kamu kurum ve kuruluşlarının veri koruma ile ilgili projelerine de görüşler vermektedir.

4.8.3.2. Görevin sona ermesi

Üyelerin ve yedek üyelerin görev süreleri 5 yıldır. Ancak bu sürenin bitmesinden önce üyenin kendi isteğiyle istifa dilekçesi vermesi, geçerli bir mazereti bulunmaksızın ardı ardına üç toplantıya katılmaması üzerine en az 3 üyenin kararı veya ölüm ile görevin kendiliğinden sona ermesi hallerinde, görevi sona eren üyenin kalan süresinde görev yapmak üzere yedek üye görevlendirilir. Yedek üyenin görevinden önce üyelikten ayrılması halinde ise yerine gecikmeksizin yeni bir yedek üye seçilir. Bu durumların dışında üyelik görevi, ancak ciddi sebeplerle ve en az üç üyenin kararıyla sonlandırılabilir.

4.8.3.3. Komisyonun bağımsızlığı

Avusturya Veri Koruma Komisyonunun bağımsızlığı Federal Mahremiyet Yasasının 37'nci maddesi ile hükme bağlanmıştır. Hükme göre, Veri Koruma Komisyonu, görevlerini yerine getirirken hiçbir surette emir ve talimat alamaz ve kararlarında tam bağımsız olarak hareket eder.

4.8.3.4. Organizasyon yapısı ve işleyiş

Komisyon, çalışmalarında kendi iç tüzüğünü hazırlar ve uygular. Yıllık faaliyetlerine ilişkin her yıl hazırlanan rapor ise Başbakana (The Federal Chancellor) sunulur. Başbakan, Komisyon için bir ofis kurar ve iş ve işlemlerini destekleyecek nitelik ve sayıda personel ve teçhizat ile destekler.

Altı kişiden oluşan Komisyonun toplantı yeter sayısı altıdır. Toplantılar, üyeler arasından seçilecek Başkanın nezaretinde gerçekleştirilir. Oyların eşitliği halinde Başkanın oyu yönünde karar alınır. Alınan bu kararlardan tüm toplumu etkileyecek veya genel önemde olanları, kurumsal gizlilik gerekleri de dikkate alınarak uygun araçlarla yayımlanır.

4.8.4. Finlandiya, Veri Koruma Ombudsmanı

Finlandiya'da Kişisel Veri Koruma Kanunu'na göre Danıştay (Council of State) tarafından 5 yıllığına seçilen Ombudsman kişisel verilerin korunmasından sorumludur. Ombudsman Ofisi, Adalet Bakanlığı ile ilişkili olup, bağımsız olarak görev yapmaktadır. Ofisin toplam personel sayısı 20'dir.

4.8.4.1. Ombudsmanın Görevleri

Finlandiya Anayasası, kişilerin özel hayat, mahremiyet ve konut dokunulmazlıklarını garanti altına almakta olup, münhasır olarak kişisel verilerin korunması ise Kişisel Verilerin Korunması Kanununda[181] düzenlenmektedir. Bu Kanun, bireyin kişisel verileri üzerinde kontrol imkanının kapsamını genişletmekte, bireye kişisel verilerinin neden ve nasıl işlendiğini öğrenme hakkı ile kanunla aksi belirtilmedikçe bu konuda belirleme yetkisi vermektedir. Kanun ayrıca özel hukuk alanında ceza hukukuna ilişkin bir yıla kadar hapis cezası öngörmektedir. Bu süreçlerde Ombudsmanın genel olarak görevi, Kanunun uygulanmasını sağlamak ve şikayetleri incelemektir. Ombudsman, kurum ve kuruluşların kişisel kayıt ve sicil dosyaları tutmalarından önce incelemelerde bulunur ve Veri Koruma Yasasının uygulanması ile ilgili veri işleyiciler olan veri kontrolörlerine görüş ve önerilerde bulunur. Diğer kurum ve kuruluşlara seminer ve konferanslar verir, veri sistemleri ile ilgili projelere rehberlik ve danışmanlık yapar, veri kontrolör ve veri öznelerine telefonla ve elektronik ortamda görüş verir. Yine, kayıt ve sicil tutulmasında personelin kendi kendisini izlemesini (self-steering) geliştirmek ve iyi veri işleme örneklerinin teşvik edilmesini sağlamak üzere davranış kuralları geliştirilmesine katkıda bulunur. Kişisel verilerin doğrulanması ve düzeltilmesi hakkının kullanılmasında yetki kullanır; kullandığı bu yetki ile aldığı kararlar bağlayıcı olup, belirli süre içinde mahkemede itiraza konu olabilir. Ombudsman, ayrıca kişisel verilerin işlenmesinin geliştirilmesi ile ilgili inisiyatif kullanır ve VKD çerçevesinde oluşturulan çalışma grubuna iştirak eder. Diğer uluslararası işbirlikleri ile birlikte Europol (Avrupa Polis Ofisi) ve Schengen anlaşmaları çerçevesinde denetleyici organların da üyesidir. Kişisel hak ve özgürlükleri ilgilendiren yasal veya idari

[181] Personal Data Protection Act (523/99), Amendment of the Personal Data Act (986/2000).

düzenlemelerin hazırlıklarında görüş verir, Kişisel Veriler Yasasının ihlali durumunda verilecek cezalarda savcı, Ombudsmanın görüşünü alır. Ombudsmanın denetim yetkisi re'sen veya veri kontrolörlerinin talebi çerçevesinde yerine getirilir. Veri Koruma Ombudsman Ofisi, Telekomünikasyon Düzenleyici Otoritesi ve Veri Koruma Kurulu ile ortaklaşa, veri koruma ve veri güvenliği ile ilgili yılda dört kez düzenli yayın çıkarır. Bu yayın ile veri koruma kuralları ve uygulamaları ile elektronik haberleşme güvenliği hakkında halkın bilgilendirilmesi amaçlanmaktadır. Ombudsman Ofisi'nin sürekli güncellenen İnternet sitesi aracılığıyla da veri koruma konusunda bilgiler verilmektedir.

4.8.4.2. Veri Koruma Kurulu

Finlandiya'da Ombudsmanın dışında, yine Danıştay'ın 3 yıllığına görev yapmak üzere 5 üyeden oluşturduğu bir Kurul bulunmaktadır. Kurul, Ombudsmanın verdiği kararların temyiz edildiği makamdır. Bu Kurul, bir Başkan, Başkan Yardımcısı ve beş üyeden oluşmaktadır.[182] Kişisel veri işlenmesi hakkında mevzuat ihtiyaçlarını izleyen ve tespit eden bu Kurul yapılacak düzenlemelere görüş vermektedir.[183]

4.8.4.3. Veri öznesi ve veri kontrolörünün hakları

Finlandiya'da birey, kendisiyle ilgili ne tür kayıtların tutulduğunu öğrenme, kimlerin kişisel verileri tuttuğunu ve neden tuttuğunu bilme, bu konuda kendisine bildirimde bulunulmasını ve yanlış bilginin düzeltilmesini isteme haklarına sahiptir. e-Posta veya cep telefonuna gönderilen doğrudan pazarlama amaçlı iletiler de ancak bireyin iznine tabi olduğundan reddetme hakkı kullanılabilmektedir. Bireyler, Veri Koruma Ombudsman ofisine doğrudan danışma amacıyla da başvurarak haklarını nasıl kullanacaklarını öğrenebilmektedirler.

Veri kontrolörü ise veri öznesinin karşısında, veri işleme sürecini dikkatli bir şekilde planlamak ve gerekli olmayan bilgiyi barındırmamakla yükümlüdür. Kontrolör, sistem güvenliğini sağlamak, gerekli olmayan bilgileri tutmamak, veri öznesinin haklarına saygı göstermek, verileri kayıt amacı dışında kullanmamak,

[182] EPIC, 2003:232
[183] Data Protection Board. 18 Mayıs 2010. <http://www.tietosuoja.fi/27311.htm>

kişisel verileri dosyalamak için veri sahibinin izni gerektiğinde o kişiye yeteri derecede bilgi vermekten sorumludur. Veri kontrolörü de veri sahibi gibi veri işlemeleri konusunda Ombudsman ofisine görüş sorabilir.[184]

4.8.5. Polonya, Kişisel Verileri Koruma Genel Müfettişliği

Kişisel hakların artan önemi nedeniyle Polonya'da veri koruma alanında çıkarılmış olan ilk düzenleme 29 Ağustos 1997 tarihinde kabul edilen ve 1998 yılında yürürlüğe giren Polonya Kişisel Verileri Koruma Kanunu[185] olup, bu Kanun aynı zamanda 95/46/AT sayılı VKD'yi uyumlaştırmayı hedeflemektedir. Bu çerçevede VKD ile uyumlu olarak, bu Kanun, kişilerin kimlik bilgilerinin ancak bireyin rızası ile işlenebileceğini belirtmekte ve hassas verilerin işlenmesinde ise birtakım özel hükümler getirmektedir. Polonya'da her vatandaşın kamu ve özel kurumların kendileriyle ilgili tutuğu verileri ve bu verilerin tutulduğu veritabanı yöneticilerini öğrenme hakları bulunmakta olup, bu yöndeki taleplerine en geç bir ay içinde cevap verilmektedir. Polonya dışına kişisel veri transferlerinde, transferin yapılacağı ülkede Polonya'daki koruma ölçüsünde veri koruma kurallarının bulunması şartı bulunmaktadır.[186]

Kişisel verilerin korunması hususu, Polonya Cumhuriyeti Anayasasının 47 ve 51'inci maddelerinde yer almaktadır. Anayasanın 47'inci maddesi vatandaşların aile ve özel hayatlarının hukuken korunmasını teminat altına alırken, 51'inci madde ise devletin kişisel verileri toplamasına sınırlandırma getirmekte ve vatandaşların verilerine erişimi sağlama gibi bazı temel hakları garanti etmektedir. Bu maddeye göre, kanunun zorunlu kıldığı durumlar haricinde hiç kimse kişisel verilerini açıklamaya zorlanamaz.

Polonya'da Kişisel Verileri Koruma Kanunu ile kurulan Kişisel Verilerin Korunması Müfettişliği üst kurum olarak görev yapmaktadır. Bu kurumun başındaki Müfettiş, Parlamentonun teklifi üzerine Devlet Başkanı tarafından atanmakta ve aynı usulle görevden alınmaktadır. Bu kurumsal yapının dört temel görevi şunlardır:

---

[184] Finland, Office of The Data Protection. "Privacy is Your Personal Right*"* Erişim tarihi: 11 Şubat 2010. <http://www.tietosuoja.fi/uploads/qz41ii.pdf>
[185] Act of August 29, 1997 on the Protection of Personal Data (original text - Journal of Laws of October 29, 1997, No. 133, item 883) http://www.giodo.gov.pl/data/filemanager_en/61.doc
[186] EPIC, 2003:401

a) Kişisel verilerin mevzuata uyumlu işlenmesini denetlemek,

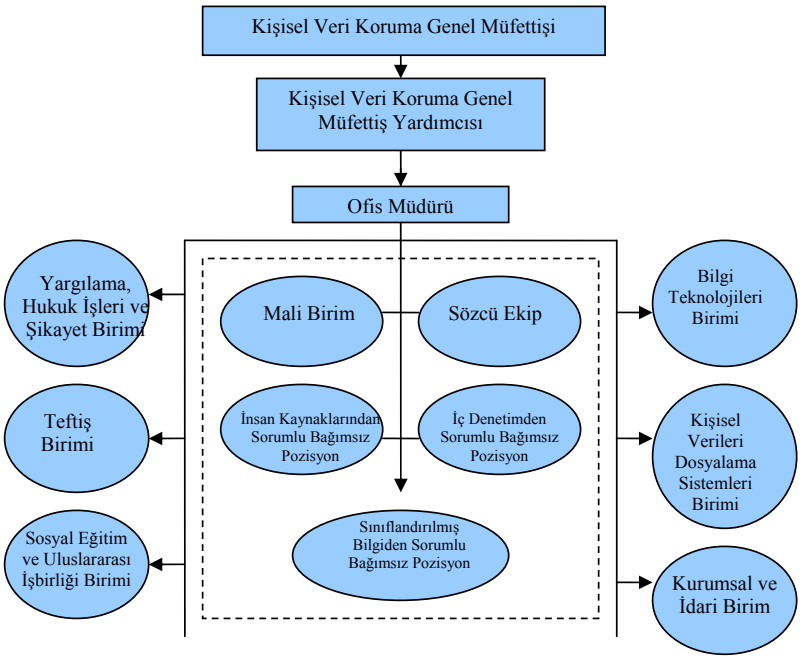
b) Kişisel verilerin korunması düzenlemelerinin uygulanması bağlamında idari kararlar almak ve şikayetleri incelemek,

c) Veri dosyalama sistemleri sicilini tutmak ve kayıtlı veri dosyalama sistemleri hakkında bilgi vermek,

d) Kişisel verilerin korunması alanındaki düzenleme taslaklarına görüş vermek.

Bu Müfettişlik, sicili tutarken, veri kontrolörünün adı, adresi, veri işlemenin amacı ve kapsamı, veri toplamanın araçları ve verileri kullanma yöntemleri ile güvenlik tedbirlerine ilişkin bilgiler verirler. Bir müfettişin ise, verilere erişme, veri transferlerini kontrol etme, veri toplamanın amaca uygun olup olmadığını kontrol etme hakkı vardır.

Şekil 4.2. Polonya, Kişisel Veri Koruma Genel Müfettişliği, Organizasyon Şeması



Kaynak: GIODO (Generalny Inspektor Ochrony Danych Osobowych), http://www.giodo.gov.pl/430/j/en/

4.8.6. Romanya, Ombudsman Ofisi ve Kişisel Verilerin İşlenmesi Ulusal Düzenleyici Otoritesi

Romanya'da veri koruma düzenlemeleri ve uygulayıcı kurumda AB uyum sürecinde bazı değişiklikler yaşanmıştır. Türkiye için de özel bir örnek teşkil edecek bu ülkedeki aşamalı kurumsal dönemler aşağıda sırasıyla incelenmektedir.

4.8.6.1. Ombudsman (Kamu Denetçisi)

Romanya'da Kişisel Verilerin Korunması Kanunu, bu ülkenin İnsan Hakları Evrensel Beyannamesi'ni imzalamasından uzun yıllar sonra ihdas edilmiş olup, kişisel verilerin korunması konusu bu ülkede diğer üye ülkelere nazaran yenidir. Romanya'da Ombudsman Ofisi (Anayasal adıyla Kamu Denetçisi Kurumu)[187] 1991 tarihli Anayasa ile, gerçek kişilerin hak ve özgürlüklerini savunmak, bu konuda Parlamentoya raporlama yaparak vatandaşların haklarını koruyucu tavsiyelerde bulunmak ve düzenleme yapılmasını talep etmek üzere kurulmuştur. Aynı anayasada "mahremiyet hakkı" da ilk kez düzenlenmişse de, Ombudsman fiilen 1997 yılına kadar mahremiyet ve kişisel verilerin korunması ile ilgilenmemiş, ancak bu tarihten sonra birkaç olayla ilgilenmiştir.

AB'ye entegrasyon süreci nedeniyle Romanya'da 2001 yılında AB düzenlemeleriyle uyumlu olarak *Telekomünikasyon Sektöründe Kişisel Verilerin Korunması* (676/2001)[188] ve VKD'yi uyumlaştırmak üzere *Kişisel Verilerin İşlenmesi ve Bu Verilerin Serbest Dolaşımı Hakkında* (677/2001) iki kanun kabul edilmiştir. Romanya, bu dönemde veri koruma konusunu sadece AB'ye üyelik yolunda bir şart olarak algıladığından, bu konuyu mevcut bir yapı ile geçiştirme eğilimine girmiştir. Bu nedenle, 677 no'lu Kanunun uygulanmasında Ombudsmana

[187] People's Advocate Institution

[188] Bu Kanunun uygulanması için Haberleşme ve Bilgi Teknolojileri Bakanlığına yetki verilmiş; ancak Bakanlık bünyesinde bu Kanunun uygulanmasını sağlayacak özel birim kurulamadığından 2004'te bu Kanunda değişiklik yapılarak yetkiler Haberleşmeden sorumlu Ulusal Düzenleyici Otorite (NRAC) ve Kamu Denetçisi arasında paylaştırılmıştır. Ancak, NRAC, 676 nolu kanundan kaynaklanan yetkilerini hiçbir zaman tam olarak yerine getirmemiştir.

yeni görevler verilerek bu Kurum içinde "Mahrem Bilgileri Koruma Birimi (PIPO)"[189] kurulmuştur.

Ancak bu birime tahsis edilen personel sayısı 15 ile sınırlı kalmış olup, bu durum Ombudsmanın mahremiyet hakkı ve veri koruma alanındaki aktif faaliyetinin sınırlı düzeyde kalmasına sebep olmuştur. Örneğin, Romanya'da elektronik kimlik kartlarının içerdiği bilgilerin kişisel veya hassas bilgi olması konusunda dört yıl süren tartışmalarda Ombudsman resmi bir görüş ortaya koyamamış, bu konuda sivil inisiyatif daha etkili olmuştur. Ayrıca, Ombudsmanın veri koruma alanında kamusal bilinirliği çok sınırlı düzeyde kalmıştır. Yine, veri koruma ve teknolojik araçlardaki gelişmeler nedeniyle veri koruma otoriteleri arasında artan işbirliği çalışmalarında ve veri işleyenlerin sicillerini tutma konularında bu Ofis yetersiz kalmıştır. Kısacası, genel amaçlarla kurulan Ombudsman Ofisi veri koruma alanında başarılı olamamıştır.[190]

Romanya'nın veri koruma alanında var olan Ombudsmana özel yetkiler vermesi bu alanda tam bağımsız kurumlar kuran diğer AB üye ülke uygulamalarından sapmış, bu durum Romanya'yı orta ve doğu Avrupa ülkeleri arasında tam bağımsız ve özerk veri koruma kurumu olmayan tek ülke haline getirmiştir.[191] Bu durumun nedeni başlangıçta kanunun yeni olması ve anlaşılamamış olmasına bağlanmışsa da sonradan, Ombudsman Ofisi kaynaklarının bu alanda yeterli olmadığı ve Ombudsmanın genel yetkileri ile veri koruma alanında gerekli olan uzmanlığın örtüşmediği kanaatine varılarak kurumsal yapıda değişiklik tartışmaları gündeme gelmiştir.

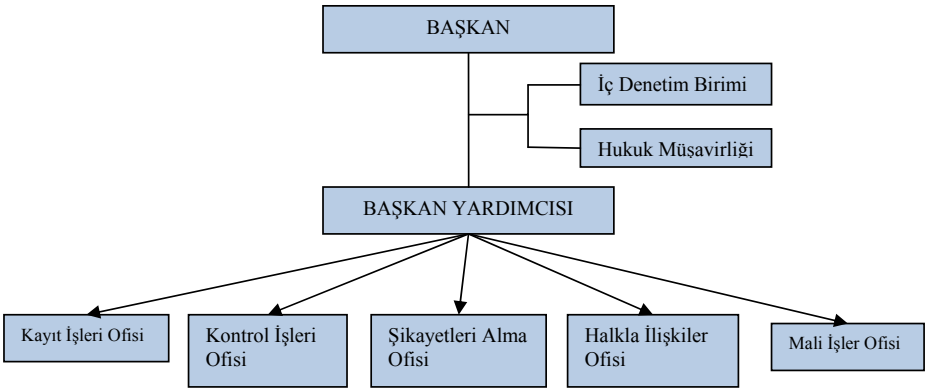
4.8.6.1. Kişisel Verilerin Korunması Ulusal Denetleyici Otoritesi

Ombudsman Ofisinin etkinliğinin bu şekilde sınırlı kalması üzerine Ombudsman Ioan Muraru, bu Ofisin kişisel verilerin işlenmesi üzerinde izleme ve denetleme fonksiyonlarını yerine getirmesinin uygun olmayacağını belirterek özel uzmanlık gerektiren söz konusu yetkilerinin başka bir kuruma devredilmesi ya da kişisel verilerin işlenmesi konusunda özel bir Kurum kurulmasını Parlamentoya

[189] Private Information Protection Office
[190] Bogdan, 2007:9
[191] Bogdan, 2007:10

teklif etmiştir.[192] Romanya'da veri koruma alanında bağımsız bir yapının gerekliliği Avrupa Komisyonu tarafından, özellikle 2004 Romanya İlerleme Raporunda da dile getirilmiştir. Bu gelişmeler üzerine 2005 yılında Romanya'da 102/2005 sayılı Kanunla[193] "Kişisel Verilerin İşlenmesinin Denetimi konusunda Ulusal Otorite"[194] kurulmuştur. Bundan iki yıl sonra, 1 Ocak 2007 tarihinde ise Romanya AB'ye üye olmuştur. Söz konusu Kurumun organizasyon şeması aşağıdaki gibidir.

Şekil 4. 3. Romanya, Kişisel Verilerin Korunması Ulusal Denetleyici Otoritesi, Organizasyon Şeması



Kaynak: The National Supervisory Authority For Personal Data Processing, Organizational Chart, http://www.dataprotection.ro/index.jsp?page=organigrama&lang=en

Halihazırda Romanya Ulusal Otoritesinin lojistik, uzman personel, idari kapasite ve mali alanda kendi kaynakları bulunmaktadır.

Romanya veri koruma kurumunu kuran Kanunun 17'nci maddesine göre bu otoritenin bütçesi devlet bütçesinden ayrılan bir kalemden oluşmaktadır. Bu süreçte, öncelikle Kurum tarafından gerekli bütçe hazırlandıktan sonra, bu bütçe taslak bütçeye alınmak üzere ilgili birimlere gönderilir. Kurum başkanının, hükümet tarafından koordine edilen ve bazı değişiklikler yapılan taslak bütçeye itirazları çözümlenmek üzere Parlamentoya yapılır.

[192] Bogdan, 2007:12
[193]Law no.102/2005 regarding the setting up, organisation and functioning of the National Supervisory Authority for Personal Data Processing http://www.dataprotection.ro/servlet/ViewDocument?id=172
[194] National Supervisory Authority for Personal Data Processing, http://www.dataprotection.ro/

5. TÜRKİYE'DE VE TÜRK HUKUKUNDA KİŞİSEL VERİLERİN KORUNMASI

5.1. Kişisel Verilerin Korunması ile İlgili Ulusal Politikalar

5.1.1. Kalkınma Planları ve Yıllık Programlar

Türkiye'de veri koruma hukuku, BİT politikalarının gelişmesiyle gündeme gelmiştir. İlk kez Sekizinci Beş Yıllık Kalkınma Planında (2001-2005) kişilik haklarının korunmasına ilişkin olarak bir hedef belirlenmiştir. Bilgi ve iletişim teknolojilerindeki gelişmeler nedeniyle ortaya çıkan, kişilik haklarının ihlal edilmesi gibi sorunların, hukukun temel ilkelerine uygun olarak çözüme kavuşturulacağının belirtildiği bu hedef[195] dışında Planda ayrıca, bilgi güvenliğinin sağlanması için uluslararası kural ve standartlar çerçevesinde çalışmaların tamamlanacağı, özellikle e-ticareti kolaylaştıracak önlemlerin alınacağı da ifade edilmektedir.[196]

Bilgi toplumuna dönüşüm vizyonuna sahip olan Dokuzuncu Kalkınma Planı (2007-2013), kişisel verilerin korunmasına ilişkin politika özelinde e-devlet hizmetlerinin gerektirdiği kurumlararası bilgi paylaşımında, kişisel bilgilerin mahremiyeti ilkesinin gözetilmesi esasını benimsemektedir. Anılan Plan dönemine ait programlardan 2008 Yılı Programının "e-Devlet Uygulamalarının Yaygınlaştırılması ve Etkinleştirilmesi" bölümünde ise, kişisel verilerin korunmasını temin edecek yasal düzenlemenin 2008 yılı içinde yapılması öngörülmüşse de Tasarının yasalaşma süreci tamamlanmamıştır. 2010 Yılı Programında ise Avrupa Konseyi'nin 185 sayılı Siber Suç Sözleşmesine taraf olunması[197] ve kişisel verilerin korunmasına ilişkin 108 ve 181 sayılı Sözleşmelerin onaylanması çalışmalarının başlatılacağına yer verilmektedir.[198]

---

[195] DPT, Sekizinci Beş Yıllık Kalkınma Planı (2001-2005). Adalet Hizmetlerinde Etkinlik. 1872'inci paragraf.
[196] DPT, Sekizinci Beş Yıllık Kalkınma Planı (2001-2005). Bilgi ve İletişim Teknolojileri. 1256'ncı paragraf.
[197] 10 Kasım 2010 tarihinde Türkiye bu Sözleşmeyi imzalayarak taraf olmuştur.
[198] DPT, 2010 Yılı Programı. E-Devlet Uygulamalarının Yaygınlaştırılması ve Etkinleştirilmesi. Tedbir 260.

5.1.2. e-Dönüşüm Türkiye Projesi

Türkiye'nin bilgi toplumuna geçiş çalışmalarının hızlandırılması, başta BİT politikaları olmak üzere bilgi toplumu strateji ve politikalarının belirlenerek bu alandaki tüm faaliyetlerin bir bütünlük içerisinde yürütülmesi ve küresel rekabet koşullarına uyum sağlamak üzere ekonomik ve sosyal dönüşümün gerçekleştirilmesi amacıyla yeni bir proje başlatılması kararlaştırılmış, bu bağlamda, 58'inci Hükümet tarafından hazırlanan Acil Eylem Planı'nda e-Dönüşüm Türkiye (e-DTr) Projesi'ne yer verilmiştir. Söz konusu projenin koordinasyonu, izlenmesi, değerlendirilmesi ve yönlendirilmesi ile ilgili olarak DPT Müsteşarlığı görevlendirilmiş, bu görevin yerine getirilmesi amacıyla da DPT Müsteşarlığı bünyesinde Bilgi Toplumu Dairesi Başkanlığı kurulmuştur. 27 Şubat 2003 tarihli ve 2003/12 sayılı Genelge ile e-DTr Projesi'nin amaçları, kurumsal yapısı ve uygulama esasları belirlenmiştir.[199]

e-DTr Projesi kapsamında, Türkiye'de bilgi toplumu olma yolundaki çalışmaların somut hedeflere dayalı olarak, katılımcı bir yaklaşımla ve daha bütüncül olarak ele alınması, kişisel verilerin korunması ile ilgili yasal düzenleme ihtiyacını daha belirgin bir hale getirmiştir. Bu kapsamda hazırlanan projeler içinde önemli bir yere sahip olan e-Devlet projelerinin temel hedefi, devlet tarafından vatandaşa sunulan hizmetlerin tek noktadan vatandaşın kullanımına açılması, bu sayede bürokrasinin azaltılması, mükerrer iş ve işlemlerden kaçınarak zaman ve masraflardan tasarruf edilmesidir. e-Devlet çalışmaları çerçevesinde kamu kurumlarının topladığı, işlediği ve sakladığı bilgilerin, gerekli olduğu ölçüde ve toplandığı amaçla bağlı kalarak diğer kamu kurumları ve kuruluşlar tarafından da kullanılması gerekmektedir.

e-DTr Projesi kapsamında DPT Bilgi Toplumu Dairesi tarafından koordine edilerek ikisi YPK Kararı, birisi ise Başbakanlık Genelgesi ek'i olarak Resmi Gazete'de yayımlanarak yürürlüğe giren üç eylem planında da kişisel verilerin korunmasına ilişkin yasal düzenleme gereksinimi belirtilmektedir. Türkiye'nin bilgi toplumuna dönüşümü için somut ve üzerinde uzlaşı sağlanan hedefler belirleyen bu

[199] DPT, Bilgi Toplumu Dairesi. E-Dönüşüm Türkiye Projesi. Erişim tarihi: 23 Aralık 2009. <http://www.bilgitoplumu.gov.tr/Portal.aspx?value=UE9SVEFMSUQ9MSZQQUdFSUQ9MiZQQUdFVkVSU0lPTj0tMSZNT0RFPVBVQkxJU0hFRF9WRVJTSU9O>

eylem planlarına ve Türkiye'nin ilk bilgi toplumu stratejisine aşağıda kısaca değinilmektedir.

i) 2003-2004 Kısa Dönem Eylem Planı

e-DTr Projesi kapsamında 4 Aralık 2003 tarihli ve 2003/48 sayılı Başbakanlık Genelgesinin eki olarak yürürlüğe giren ve 2003 ve 2004 yıllarında yapılacak iş adımlarının yer aldığı Kısa Dönem Eylem Planındaki (KDEP) 73 eylemden münhasır olarak iki eylem kişisel veri koruma ile ilgilidir. Bu kapsamda 17 numaralı eylem ile Adalet Bakanlığı'na Kişisel Verilerin Korunması Hakkında Kanun'un çıkarılması ve elektronik hasta kayıtları sistemi için çalışma yapması sorumluluğu verilmiştir. 64 numaralı eylem ise kişisel sağlık kayıtlarının erişim denetimi (e-imza) ve gizlilik ihtiyaçlarının belirlenmesi ile ilgilidir. Bu Eylem Planının uygulandığı dönemde, KVKK Tasarısı Taslağı 2 Haziran 2004 tarihinde Başbakanlığa sevk edilmiş ve Başbakanlık tarafından görüşleri alınmak üzere kamu kurum ve kuruluşlarına gönderilmiştir.[200]

ii) 2005 Eylem Planı

e-DTr Projesi kapsamında, 24 Mart 2005 tarihli ve 2005/5 sayılı YPK Kararı eki olarak yürürlüğe giren 2005 Eylem Planında veri koruma ve mahremiyetle ilgili olarak sağlık kayıtlarının mahremiyetinin korunması konulu 44 numaralı eylem dışında bir eylem bulunmamaktadır. 2005 Eylem Planı döneminde, daha önce kurum ve kuruluşların görüşlerine sunulan KVKK Tasarısı Taslağı, yeniden değerlendirilmek üzere Başbakanlık tarafından Adalet Bakanlığına geri gönderilmiştir. Ayrıca, 44 numaralı eylemle ilgili olarak veri ve bilgi güvenliği açısından Sağlık Bakanlığına bağlı tüm kurum ve kuruluşlar ile merkezdeki bilgi sistemi uygulamalarının yaygınlaşması sürecinde uyulması gerekli usul ve esaslara ilişkin bir Başbakanlık Genelgesi (7 Ekim 2005 tarihli ve 153 sayılı) yayımlanmıştır.[201]

---

[200] DPT, e-Dönüşüm Türkiye Projesi Kısa Dönem Eylem Planı, Sonuç Raporu. Mayıs 2005. 14 Kasım 2009. <http://www.bilgitoplumu.gov.tr/kdep/rapor/KDEP-Sonu%E7Raporu.pdf >

[201] DPT, e-Dönüşüm Türkiye Projesi 2005 Eylem Planı, Sonuç Raporu. Mayıs 2006. 14 Kasım 2009. <http://www.bilgitoplumu.gov.tr/2005EP/Rapor/2005EylemPlani_Sonuc_Raporu.pdf>

iii) Bilgi Toplumu Stratejisi ve ek'i Eylem Planı (2006-2010)

Eylem planları çerçevesinde yürütülen kısa vadeli hedeflerin gerçekleştirilmesine yönelik çalışmaların yanı sıra, 2005 yılında ayrıca, Türkiye'nin BİT'ten etkin olarak yararlanması ve bilgi toplumuna dönüşümün gerçekleştirilmesine yönelik orta ve uzun vadeli strateji ve hedefleri belirlemek üzere, 2006-2010 dönemini kapsayacak olan Bilgi Toplumu Stratejisi (BTS) hazırlık süreci başlatılmıştır.[202]

28 Temmuz 2006 tarihinde 2006/38 sayılı YPK Kararı eki olarak RG'de yayımlanarak yürürlüğe giren BTS ve ek'i Eylem Planında[203] toplumun temel öğelerini oluşturan vatandaşlar, kamu sektörü ve işletmeler ile BİT sektörünün mevcut durumları ve Türkiye'nin 2010 yılında bilgi toplumuna dönüşüm potansiyeli değerlendirilmiş, belirlenen stratejik öncelikler çerçevesinde 2010 yılı için hedefler ve bu hedeflere ulaşmak için atılması gereken adımlar tespit edilmiştir. 2005 Eylem Planı döneminde KVKK Tasarısı Taslağı yasalaşamadığından, BTS'nin eki eylem planında bu hususa yeniden yer verilmiş ve 87 numaralı eylem kapsamında bir KVKK ve ayrıca korunması kritik önemi haiz ulusal bilgilerin korunması ile ilgili bir Bilgi Güvenliği Kanunu çıkarılması planlanmıştır. Başbakanlık tarafından geri gönderilen taslağı Adalet Bakanlığı, 9 Kasım 2005 tarihinde Başbakanlığa yenileyerek sunmuş, Başbakanlık Taslağa ilişkin bazı değişiklikler yaptıktan sonra TBMM'ye iletmiştir.

Tasarı, halihazırda TBMM Adalet Komisyonunda 1/576 esas numarası ile görüşülmeyi beklemektedir.

5.2. AB'ye Uyum Sürecinde Kişisel Verilerin Korunması

i) Ulusal Programlar

AB Müktesebatının Üstlenilmesine İlişkin Türkiye Ulusal Programları, Türkiye'nin AB'ye tam üyelik süreci içinde kısa ve orta vadede gerçekleştirilmesi

[202] DPT, Bilgi Toplumu Stratejisi (2006-2010). s.2. 28 Temmuz 2006. 23 Aralık 2009. <http://rega.basbakanlik.gov.tr/main.aspx?home=http://rega.basbakanlik.gov.tr/eskiler/2006/07/20060728.htm&main=http://rega.basbakanlik.gov.tr/eskiler/2006/07/20060728-7.htm>

[203] DPT, Bilgi Toplumu Dairesi. Bilgi Toplumu Stratejisi ve Eylem Planı. 28 Temmuz 2006. 23 Aralık 2009.
<http://www.bilgitoplumu.gov.tr/Portal.aspx?value=UEFHRUlEPTE0Jk1PREU9MQ==>

öngörülen çalışmaları kapsayan ve yapılacak çalışmaların genel çerçevesini çizen yönlendirici nitelik taşımaktadır. Ulusal Program, Bakanlar Kurulu Kararı ek'i olarak yayımlanmaktadır.

Veri koruma ve kişisel veri ile ilgili düzenleme taahhütleri, ülkemizin Katılım Ortaklığı Belgelerine cevaben hazırladığı 2001 ve 2003 Yılları Ulusal Programlarında da yer alan yükümlülüklerdendir. 2008 Yılı Ulusal Programında[204] ise bu konuya AB'nin Katılım Ortaklığı Belgesinde doğrudan atıf yapmaması sebebiyle değinilmemiştir. Bu durumun, AB gözünden, Türkiye'de çalışmalarının 2008 yılından önce bitirilmiş olması gereken bir konunun aynı nitelikteki bir belgede tekrar yer verilmesine gerek görmemesi olarak bakılması mümkün olup, bu durum konunun aciliyet taşıması gerektiği yönünde değerlendirilmelidir.

2001 Yılı Ulusal Programında, telekomünikasyon konu başlığı altında veri koruma mevzuatı, uyumu öngörülen mevzuat olarak yer almaktadır. 2003 Ulusal Programının mevzuat uyum takviminde ise veri koruma ile ilgili 97/66, 2002/58 gibi telekomünikasyon alanında kişisel veri korumasına ilişkin düzenlemelere uyum amacıyla bir takvim belirlemesi yapılmıştır.

ii) İlerleme Raporları

AB'nin Türkiye hakkındaki 2005 Yılı İlerleme Raporunda[205] AB Komisyonu, Türkiye'de veri koruma alanında TCK'nın ilgili hükümlerine atıf yapmaktadır. Daha sonra ise, Türkiye'nin Avrupa Konseyi'nin "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Kişilerin Korunması Sözleşmesi"ni imzaladığı ancak henüz onaylamadığı hatırlatılarak Türkiye'de kişisel verilerin korunmasına ilişkin kuralların uygulanması ve kişisel veri muhafazasını denetleyecek bağımsız bir kurum oluşturulmasına ihtiyaç bulunduğu belirtilmektedir.

AB Komisyonunun COM(2006)649 sayılı Bildirimi ile yayımlanan 2006 Türkiye İlerleme Raporunda kişisel verilerin korunması tekrar gündeme gelmiş olup, bu alanda herhangi bir gelişme olmadığı kaydedilmiştir.

---

[204] "Avrupa Birliği Müktesebatının Üstlenilmesine İlişkin Türkiye Ulusal Programı ile Avrupa Birliği Müktesebatının Üstlenilmesine İlişkin Türkiye Ulusal Programının Uygulanması, Koordinasyonu ve İzlenmesine Dair Karar" 10/11/2008 tarihinde Bakanlar Kurulunca alınmıştır.
[205] COM(2005) 561 sayılı Komisyon Bildirisi.

Bir yıl sonra yayımlanan 2007 Türkiye İlerleme Raporunda ise, Yargı ve Temel Haklar (23'üncü fasıl) ile Adalet, Özgürlük ve Güvenlik (24'üncü fasıl) fasıllarında Türkiye'de veri koruma ile ilgili eksiklikler gündeme getirilmektedir. Bu Raporda, 23'üncü fasıl altında, Türkiye'de Haziran 2007 tarihinde Polis Vazife ve Salahiyat Kanununa sürücü belgesi, pasaport veya silah ruhsatı gibi başvurularda vatandaşların parmak izleri ve resimlerinin alınacağı ve 80 yıl süreyle saklanacağı hükmünün eklendiği belirtilmekte; ardından Türkiye'nin VKD'yi uyumlaştırarak bir veri koruma denetleyici otorite ihdas etmesi gerektiği ifade edilmektedir. Söz konusu Raporda 24'üncü fasıl başlığı altında ise veri koruma alanındaki yasal boşluğun, Türkiye'nin Europol (Avrupa Polis Ofisi) ile uluslararası düzeyde operasyonel anlaşma yapmasında yarattığı sıkıntılar ile Türkiye'de bağımsız bir denetleyici kurum kurmak gerekliliğine değinilmektedir. Aynı raporda, Gümrük Müsteşarlığının risk yönetimi ile ilgili bir strateji belgesi hazırladığı, ancak özellikle suçla mücadelede, gümrüklerin işbirliği yapabilmelerinde de veri korumasına ilişkin belirli bir mevzuatın bulunmamasının sorun yarattığı ifade edilmektedir.

2008 Türkiye İlerleme Raporu'nun yargı ve temel haklar (23'üncü fasıl) bölümünde konuya şu ifadelerle tekrar dikkat çekilmektedir: *"Özel hayat ve aile hayatına saygı, özellikle kişisel verilerin korunması hakkı kapsamında Türkiye'nin mevzuatını veri koruma müktesebatından özellikle 95/46/AT sayılı Direktifle uyumlaştırması ve bu çerçevede tam bağımsız bir veri koruma denetleyici kurumu kurması gerekmektedir. Türkiye'nin ayrıca, kişisel verilerin otomatik yollarla işlenmesi hakkındaki Avrupa Konseyi Sözleşmesini (108 sayılı) ve bu sözleşmenin eki niteliğindeki üst kurullar ve sınır ötesi veri akışı ile ilgili protokolü (181 sayılı) onaylaması gerekmektedir."*

Son olarak, 2009 Türkiye İlerleme Raporunun 23. fasıl başlığı altında bu ihtiyaç aynı şekilde ifade edilmektedir.

Türkiye'de veri koruma alanında düzenleme yapılması ihtiyacı, hem ulusal hem de uluslararası etkenlerle etkisini hissettirmektedir. Bu ihtiyaçlar, e-Dönüşüm faaliyetleri çerçevesinde *ulusal,* AB Komisyonu'nun İlerleme Raporları aracılığıyla sıklıkla dile getirmesi ve ülkemizin AB'ye uyum kararlılığı doğrultusunda *uluslararası* politikada önceliği olan konulardan biridir.

iii) Türkiye'nin AB Müktesebatına Uyum Programı

10 Ocak 2007 tarihinde, Dışişleri Bakanı ve Başbakan Yardımcısı başkanlığında, Devlet Bakanı ve Başmüzakereci, İzleme ve Yönlendirme Komitesi üyeleri ve ilgili tüm kurumların üst düzey yetkilileriyle düzenlenen toplantıda, Türkiye'nin AB'ye tam üyelik perspektifi ile 2007-2013 döneminde AB müktesebatına uyumun tamamlanmasını hedefleyen bütüncül bir program hazırlanması kararı alınmıştır.[206]

Bu karar üzerine, katılımcı bir yaklaşımla ve yedi yıllık dönem için hazırlanan AB Müktesebatına Uyum Programında (2007-2013) takvimlendirme yapılırken, Türkiye'nin ihtiyaçları ve öncelikleri esas alınmıştır. KVKK, bu Programda 10.0708.1.04 referans numarası ile çıkarılması planlanan kanunlar arasında yer almaktadır. KVKK ile 95/46 sayılı VKD, 2006/24 ile değişik 2002/58 sayılı Direktif, Kişisel Verilerin Elektronik Ortamda İşlenmesi Bağlamında Bireylerin Korunmasına Dair 108 numaralı Avrupa Konseyi Sözleşmesi ve Kişisel Verilerin Üçüncü Ülkelere Transferi için Standart Akdi Kurallara İlişkin 2001/497/AT sayılı Komisyon Kararına uyum öngörülmektedir. Son olarak, Türkiye'nin Katılım Süreci için AB Stratejisi çerçevesinde hazırlanan 2010-2011 Eylem Planında da KVKK çıkarılmasına ilişkin bir tedbir yer almaktadır.[207]

5.3. Türkiye'de Yasal Boşluk Nedeniyle Yaşanan Sorunlar ve Mevcut Tehdit Alanları

Türkiye'de bazı e-devlet hizmetleri ve özel şirketlerin çevrimiçi hizmetleri nedeniyle kişisel veri setlerinin sayısı artmış durumdadır. Değişik kurumların İnternet sitelerinden anonim olarak ulaşılabilen parça parça bilgilerin biraraya getirilerek bireylerin rızası ve menfaati hilafına kullanılması bir yana, bu durum kişisel bilgilerin mahremiyeti ilkesi açısından da potansiyel sorun ve riskler taşımaktadır. Türkiye'de veri paylaşım ihtiyaçları da artmakla birlikte, bilginin kurum içi ve kurumlararası paylaşımında yasal boşluklar nedeniyle belirsizlikler

[206] Türkiye'nin AB Müktesebatına Uyum Programı (2007-2013). Giriş bölümü. 8 Ocak 2010. <http://www.abgs.gov.tr/files/Muktesebat_Uyum_Programi/Giris.pdf>
[207] Bkz. 2010-2011 Eylem Planı. Ankara 15 Mart 2010. s.52. <http://www.abgs.gov.tr/files/strateji/2010_2011_eylem_plani.pdf>

bulunmaktadır. Paylaşım esas ve usulleri ve paylaşımın sınırlarını net olarak belirleyen çerçeve nitelikte bir kanunun bulunmaması nedeniyle uygulayıcılar;

- Genel hukuk kurallarına göre hareket etmekte,
- Paylaşımdan tamamen kaçınmakta,
- Kendilerine göre mantıklı olan kararlar almakta ya da
- Hata yapma korkusuyla karar almamaktadırlar.

Kanunun bulunmamasının yarattığı belirsizlik, özellikle e-devlet projelerinde kendisini göstermektedir. OECD'nin 2007 yılında Türkiye'deki e-Devlet çalışmalarını inceleyen raporunda[208] da, diğer OECD ülkeleri deneyimlerinin gösterdiği gibi e-devlet girişimlerinin ve süreçlerinin başarısının devletin bu alanda yeterli hukuki çerçeve sağlamasına bağlı olduğu, Türkiye'nin elektronik işlemlere ilişkin hukuki çerçevesinin kapsamlı bir kişisel verilerin korunması kanunu haricinde tamamlandığı belirtilmektedir. Raporda bu konuda Türkiye'de e-imza, e-sözleşme, fikri mülkiyet, bilgi edinme hakkı, evrensel hizmet, tüketicilerin korunması, e-Dönüşüm ve e-devlet çalışmalarının yoğunluk kazandığı bir dönemde, Türkiye'de bir "Kişisel Verilerin Koruması Kanunu"nun bulunmaması nedeniyle, özellikle kamu kurumlarının karşılaştıkları sorunlar aşağıda incelenmektedir.

5.3.1. İçişleri ve kolluk alanında

1973 tarihli Kimlik Bildirme Kanununa göre askeri konaklama, dinlenme ve kamp tesisleri ile ordu evleri hariç, özel veya resmi, her tür konaklama, dinlenme bakım ve tedavi tesisleri ve işyerleri ile konutlarda geçici veya sürekli olarak kalanlar, oturanlar, çalışanlar ve ayrılanların kimliklerinin tespit edilerek kolluk kuvvetlerinin incelemelerine hazır bulundurulması ile talebi halinde Türkiye İstatistik Kurumuna verilmesi zorunludur. Bu Kanunda 1996 ve 2008 yıllarında yapılan değişikliklerle genel kolluk kuvvetlerine ait karakollara, il merkezlerinden de sorgulanabilen bilgisayar terminalleri konulması zorunluluğu getirilmiştir. Bununla birlikte, özel veya resmi her türlü konaklama tesislerinden Bakanlar Kurulunca belirlenecek olanlara, tespit ve ilan tarihinden itibaren üç yıl içerisinde tüm

[208] OECD, 2007:35

kayıtlarını bilgisayarda tutmak ve bilgisayar terminallerini genel kolluk kuvvetlerinin bilgisayar terminallerine bağlamak zorunluluğu getirilmiştir.

Günümüzde bazı muhtarların, mahallerinde ikamet eden kişilere ait bilgileri, hızla bilgisayar ortamına aktarmaya başladıkları gözlenmektedir. Ancak, bu verilerin nasıl ve ne şekilde korunduğu ve kimlere açık olduğu konularında birçok açık nokta bulunmaktadır.[209]

Suç ve suçla mücadele olgusundaki hızlı değişimlere paralel olarak suçlular arasında mevcut olan uluslararası örgütlenmelere cevap olarak, ülkemiz polis teşkilatları da yabancı ülke polis teşkilatları ve kanun uygulama birimleri ile işbirliği mekanizmaları tesis etme gayreti içerisinde diğer ülkelerle Güvenlik İşbirliği Anlaşmaları imzalamaktadır. Ülkemizde bir veri koruma kanununun bulunmaması nedeniyle, İçişleri Bakanlığı ve Emniyet Genel Müdürlüğü'nün uluslararası çalışmalarında karşılaştıkları bazı sorunlar aşağıda özetlenmektedir.

5.3.1.1. Europol (Avrupa Polis Ofisi) ile ilişkiler

Europol, en az iki AB Üyesi Devletin etkilendiği terör, uyuşturucu ticareti ve diğer uluslararası organize suçlarla mücadelede kolluk birimleri arasındaki etkinliği ve işbirliğini geliştirmeye yönelik görev yapan bir birimdir. Bu birim, 1995 yılında kabul edilen "Europol Sözleşmesi"[210] ile kurulmuş olup, sınır aşan organize suç örgütleriyle mücadele etmek üzere, bünyesindeki "Europol Bilgi Sistemi" ve "Analiz Çalışma Dosyaları" aracılığıyla gerekli bilgileri toplamakta, analiz etmekte ve bunları üye devletlerin Europol Ulusal Birimlerine iletmektedir.

Europol, sözleşme maddeleri kapsamında görev ve sorumluluklarını yerine getirmek üzere bilgi sistemlerinde kişisel verileri kaydetmekte, işlemekte ve kullanmaktadır. Europol Sözleşmesi'nin 8'inci maddesine göre, kişilerin adları, soyadları, kızlık soyadları, doğum yeri ve doğum tarihleri, milliyeti, cinsiyeti, fiziksel görünümünü ve o kişiyi tanımlayacak diğer özellikleri ile değişmeyecek nitelikteki parmak izi gibi biyometrik veriler ve hatta hassas veriler bu sisteme işlenebilmektedir. Uluslararası nitelikte suçlarla mücadelede bu verilerin, üçüncü

[209] Dinç, 2006:8
[210] Europol Sözleşmesi için bkz.
<http://www.europol.europa.eu/index.asp?page=legalconv#TITLE%20I>

ülke ve kuruluşlarla da paylaşılması gerekebilmektedir (md. 18). Ancak bu üçüncü ülkelerin Europol ile kişisel verilerin iletimine esas "operasyonel düzey işbirliği anlaşması" imzalamış olmaları şartı aranmaktadır. Europol ile operasyonel düzey işbirliği anlaşması imzalayacak ülke ve kuruluşların ise Europol Sözleşmesi'nin 18'inci maddesinde ifade edilen *yeterli veri koruma standartlarına sahip olmaları* gerekmektedir. VKD'de de aranan bu şart, veri koruma alanında uygulanan hükümlerin 1981 sayılı Avrupa Konseyi Sözleşmesindeki standartlara ve Avrupa Konseyi Bakanlar Komitesinin 1987 yılı, (87)15 nolu Tavsiye Kararı[211]na (md. 14) uygun mevzuatın varlığı şartıdır.

Türkiye, Europol ile 2004 yılında kişisel verilerin paylaşılmasına *imkan tanımayan* Teknik ve Stratejik Düzey İşbirliği Anlaşması imzalamıştır. Ulusal düzeyde bir kişisel veri koruma kanununun bulunmamasından dolayı, mezkur anlaşmayı ileriye taşıyacak ve kişisel veri paylaşımını da sağlayacak Operasyonel İşbirliği Anlaşması imzalanamamaktadır. Aynı sebep, Europol ile ülkemiz arasında güvenli ve hızlı bir iletişim hattının tesis edilmesinin önünde de engel teşkil etmektedir. Europol ile ülkemiz arasında paylaşılan bilgi ve belgeler kişisel veri içermese dahi çoğunlukla "posta" yoluyla yapılmakta, bu da suçla etkin bir şekilde mücadele edilmesini engellemektedir. KVKK Tasarısının yasalaşması halinde, Europol ile aramızda *güvenli bir elektronik iletişim hattı* tesis edilebilecek, bilgi ve belge paylaşımı hızlı ve güvenli bir şekilde gerçekleştirilebilecektir.

5.3.1.2. Schengen Bilgi Sistemi

Avrupa Tek İç Pazarına hazırlık olmak üzere, 14 Haziran 1985'te Lüksemburg'un Schengen kentinde üç Benelüks ülkesi (Belçika, Hollanda, Lüksemburg), Fransa ve Almanya arasında imzalanan Schengen Antlaşması; taraf devletler arasında bulunan sınır kontrollerinin aşamalı olarak kaldırılması ile silah, mermi ve uyuşturucu madde kaçakçılığı ile mücadelede ülkeler arasındaki işbirliğini geliştirmeyi amaçlamaktadır. Antlaşma; sınır ötesi takip ve izleme konularında

[211] Recommendation No. R (87) 15 of the Committee of Ministers to Member States Regulating the Use of Personal Data in the Police Sector : Avrupa Birliği Bakanlar Komitesinin bu tavsiye kararı, polis sektöründe gerekli olan verilerin otomatik araçlarla işlenmesine ilişkin genel toplama, depolama, kullanma ve iletimine ilişkin tavsiye ilkelerden oluşmaktadır. Tavsiye Kararı için bkz. <http://www.coe.int/T/DG1/LegalCooperation/Economiccrime/organisedcrime/Rec_1987_15.pdf>

ülkelerarası işbirliği ve polis teşkilatları arasında haberleşmeyi sağlayacak Schengen Bilgi Sistemi (SBS) olarak adlandırılan bir bilgi ağının kurulması olanağını getirmiştir.

SBS, bu sisteme üye devletlerce oluşturulan ve Schengen alanında güvenlik ve adaletin sağlanabilmesi için kişi ve olaylara ait gerekli bilgilerin (uyarılar) bulunduğu ortak bir veritabanı sistemidir. Sistemde, tutukluluk nedeniyle arananlar, üçüncü ülkelerden Schengen alanına girişi yasaklananlar, kayıp kişiler ve ceza davalarında tanıklığı gerekenler ile kayıp veya çalınmış motorlu araç, sahte banknot vb. bilgiler yer almaktadır.[212]

Ülkemizde bir veri koruma kanununun bulunmaması, SBS'ye dahil olmaya engel teşkil etmektedir. Ayrıca, Türkiye, Sirene Ofisleri olarak adlandırılan ve suç ve suçlulukla mücadelede kullandığı SBS ile en az Interpol ve Europol kadar önemli bir işbirliği kanalı olan Ofislerden de SBS'ye dahil olmadığı için faydalanamamaktadır. Bu Ofislere üye olan devletler, çalıntı oto, pasaport, Avrupa Tutuklama Müzekkeresi, aranan şahıslar, istenmeyen yabancılar vb. bilgileri otomatik olarak sorgulayabilmektedir.

Avrupa Konseyi'nin 14 Nisan 2003 tarihli "Türkiye İçin Katılım Ortaklığı Belgesi"nin[213] (KOB) üyelikten kaynaklanan yükümlülükleri üstlenebilme yeteneği bölümünde, verilerin korunması ve mevzuatın uygulanması için kişisel verilerin değişimi alanındaki AB müktesebatının kabul edilmesi ve Schengen Bilgi Sistemi ve Europol'e tam katılım sağlanabilmesi amacıyla bağımsız bir denetleyici otoritenin oluşturulması da dahil olmak üzere, müktesebatın uygulanması için idari kapasitenin oluşturulması gerektiği ifade edilmektedir.

Söz konusu KOB'a karşılık olmak üzere, Türkiye'nin yayımladığı 24 Temmuz 2003 tarihli Ulusal Programda, *Kişisel Verilerin Korunması Hakkında Kanununun yürürlüğe girmesini takiben,* Schengen Bilgi Sistemi ile ilgili gerekli idari düzenleme çalışmalarına başlanarak, bu alanda AB mevzuatına uyum sağlanması çalışmalarının sürdürüleceği; ülkemizin Schengen Müktesebatını

[212] Ayrıntılı bilgi için bkz. "General Information on the Schengen Information System". <http://www.mzv.cz/public/ef/b6/ac/187211_14916_infoSIS_anglicky.pdf>
[213] DPT, Türkiye İçin Katılım Ortaklığı Belgesi, 2003:21

kabulünden sonra, İçişleri Bakanlığı Emniyet Genel Müdürlüğü iletişim alt yapısının da Schengen Bilgi Sistemleri Ağına (SISNET) bağlanmasına yönelik çalışmalara başlanabileceği ifade edilmektedir.

Kişisel Verilerin Korunması Hakkında Kanunun yasalaşamamış olması nedeniyle, organize suçla mücadelede yukarıda bahsi geçen uluslararası işbirliği kanalları ülkemiz tarafından etkin bir şekilde kullanılamamakta veya hiç kullanılamamaktadır.

5.3.1.3. Güvenlik işbirliği anlaşmaları

Ülkemizin diğer ülkelerle imzalamayı öngördüğü bazı güvenlik işbirliği anlaşmaları belirli bir aşamaya kadar getirilmekte ve müzakereler yapılmakta; ancak, müzakereler kişisel verilerin korunmasına ilişkin yasal düzenleme bulunmaması sebebiyle askıda beklemektedir. Bu çerçevede, Fransa ve Belçika müzakerelerin askıya alındığı ülkelerdendir.

5.3.2. Sağlık

Sağlık sektöründe büyüyen arz ve hizmet kapasitesi sebebiyle, hasta kayıtlarının ve hastane iş ve işlemlerinin klasik yöntemlerle kağıt üzerinde tutulması hizmette büyük yavaşlamalara sebep olmaya başlamış; bunun üzerine, günümüzün teknolojik gelişimi de göz önünde bulundurulmak suretiyle, Yataklı Tedavi Kurumları İşletme Yönetmeliğinde 2005 yılında değişiklik yapılarak, tüm hastane kayıtlarının bilgisayar ortamında tutulabilmesine imkan tanınmıştır.[214] Bu değişikliğin yapıldığı yılı takip eden 2006 yılında ülkemizde Sağlık Bakanlığına bağlı hastanelerde yapılan poliklinik muayene sayısı 190 milyondur.

Avrupa Konseyinin 108 sayılı Sözleşmesinin 6'ncı maddesine göre, kişisel sağlık verisi, özel niteliği olan kişisel verilerdendir. VKD uyarınca, nitelikli kişisel veri sayılan sağlık verilerinin sağlık kurum ve kuruluşlarınca toplanması ve kaydedilmesi "kişisel veri işleme" sayılmaktadır. Diğer taraftan, AİHM "Ferdin özel hayatı kapsamındaki bilgilere ilişkin kamu müdahaleleri, ferdi koruyucu uygun ve

[214] Yataklı Tedavi Kurumları İşletme Yönetmeliği, md. 32: "Merkezî tıbbî arşivin çalışma şekli ile hastanede tutulan tüm kayıtların bilgisayar ortamında tutulabilmesine ilişkin usul ve esaslar Yönerge ile belirlenir."

etkili garantiler içeren kanuni düzenlemeler bulunmadığı sürece, Sözleşmenin 8/1 maddesinde belirtilen hakların bir ihlali olarak değerlendirilir." (Klass Kararı)[215] kararını vermiştir. [216]

Alman Anayasa Mahkemesi ise "Hasta Dosyaları Kararı"nda, hastanın izni olmaksızın bir doktorun bu bilgileri açıklama, yayma ve paylaşmasının hem doktorların sır saklama yükümlülüğüne aykırı olduğunu belirtmiş, hem de hastanın bu bilgilerin sadece doktorla kendisi arasında kalacağı beklentisine aykırı olması nedeniyle durumun, kişilik alanı kapsamındaki gizli bilgilerin ihlali olduğu yönünde karar vermiştir.

Türkiye'nin "insan hakları ihlali" iddiasına muhatap olmaması bakımından, veri korumada genel hukuki çerçeveyi çizecek KVKK Tasarısı yasalaştıktan sonra, kişisel sağlık verilerinin korunması yönünde spesifik bir düzenleme yapılması gerektiği değerlendirilmektedir.

5.3.3. Dışişleri Bakanlığının görev alanı ile ilgili hususlar

Yabancı ülke makamlarınca ülkemiz Dışişleri Bakanlığı ve temsilciliklerinden zaman zaman T.C. vatandaşlarının, kimlik, vatandaşlık, askerlik vb. bilgileri talep edilmektedir. Ancak, bu verilerin veya türevlerinin kişisel veri olup olmadığı konusunda hukuki boşluk nedeniyle tereddütler oluşmakta, bu tür taleplerde yeknesak uygulama sağlanamayabilmektedir.

Bununla birlikte, dış temsilciliklerimiz yurtdışındaki konsolosluk hizmetlerini Türkiye'deki resmi kurumlarımız adına yürütmektedir. Bu itibarla, depolanan pasaport, nüfus, askerlik vb. bilgiler esasen İçişleri Bakanlığı, Milli Savunma Bakanlığı vb. kurumlarımız adına toplanmaktadır. Bu durumda, söz konusu kişisel bilginin asıl sahibi, depolayıcısı ve paylaşmaya yetkili makamın tespit edilmesi gerekmektedir.

---

[215] Case of Klass and others v. Germany. Application no. 5029/71. 6 September 1978. <http://cmiskp.echr.coe.int/tkp197/view.asp?item=1&portal=hbkm&action=html&highlight=klass&sessionid=41003495&skin=hudoc-en>

[216] Adalet Bakanlığı, Kanunlar Genel Müdürlüğü. "*Kişisel Verilerin Korunması"* konulu bilgi notu. s. 11.

5.3.4. Adli yardımlaşma

Türkiye'de yasal düzenleme bulunmamasının sonuçlarının uygulamaya yansıdığı bir diğer alan da, adli yardımlaşma anlaşmalarının uygulanmasıdır. Bu konuda, başta Almanya olmak üzere, Konseye üye diğer devletler, Türk mahkemelerince yapılan kişiler hakkındaki adres tespiti, istinabe[217] gibi istemleri, Türkiye'nin konuya ilişkin eşdeğer koruma mevzuatı bulunmadığı için geri çevirmektedirler.[218] Türkiye'deki adli makamların, yabancı ülkelere ait vatandaşların nüfus ve sabıka kayıtlarını temin edebilmesi için düzenlenerek Interpol[219], Europol, üye devlet emniyet güçleri veya adli makamlarına iletilen cezai istinabe talepleri üzerine elde edilen AB ve diğer ülke vatandaşlarına ait kişisel verilerin, Türkiye'de hangi usul ve esaslara göre kullanılacağını belirleyen veya bu kişisel verilerin başka bir suçun kovuşturulmasında kullanılmasını yasaklayan bir mevzuatımız bulunmadığından, AB üyesi ülkeler, verdikleri kişisel bilgilerin başka bir suçun kovuşturulmasında kullanılmaması konusunda teminat istediklerinde, ülkemizde bu konuya ilişkin mevzuat bulunmaması sorun yaratmaktadır. Nitekim, Hollanda; adli makamlarımızın İçişleri Bakanlığı Emniyet Genel Müdürlüğü aracı kılınarak nüfus ve sabıka kaydının temini taleplerinde, ülkemizde kişisel verilere ilişkin kanun bulunmadığı gerekçesiyle kendi vatandaşlarının nüfus ve sabıka kaydı bilgilerini vermemektedir.[220] Oysa, kişisel verilerin korunmasına ilişkin mevzuat bulunan ülkelerde, temin edilen kişisel verinin başka bir suçta veya başka bir işlem için kullanılması zaten müeyyideye bağlı olduğundan, veriyi ileten ülke vatandaşının mahremiyeti de korunuyor olmaktadır. Bu durum, ülkemiz için bir sorun olmaya devam etmektedir.

---

[217] Görülmekte olan bir davada tebliğ, şahit, ehli vukuf dinlenmesi, keşif, isticvap, yemin gibi muameleleri yapması için bir mahkeme tarafından diğer bir mahkemeye veya kendi üyelerinden birisine yetki verilmesine istinabe denilmektedir. Kendisine yetki verilen mahkemeye "istinabe olunan mahkeme"; üyeye, hakime veya memura ise "naip" denilmektedir.

[218] KVKK Tasarısı, Genel Gerekçe, s. 4.

[219] Uluslararası Polis Teşkilatı (International Criminal Police Organization - Interpol), 1923 yılında uluslararası polis işbirliği sağlamak amacıyla kurulmuştur. BM'den sonra, dünyanın ikinci büyük uluslararası örgütüdür. Şu anda 184 üye ülkeye sahiptir.

[220] Adalet Bakanlığı, Kanunlar Genel Müdürlüğü. "*Kişisel Verilerin Korunması"* konulu bilgi notu. s. 13

5.3.5. Türkiye'de yaşanan diğer sorunlar ve mevcut tehditler

Yukarıda adli yardımlaşma ve Dışişleri Bakanlığının görev alanı ile ilgili hususlarda ifade edilen, Türkiye'nin ihtiyaç duyduğu bazı kişisel verilerin iletimine diğer ülkelerin izin vermemesine bir başka örnek de gümrüklerdir. Türkiye ile AB arasında gerçekleştirilen gümrük birliği çerçevesinde, Türkiye ile AB üyesi devletlerin gümrük idareleri arasında bilgi akışında Türkiye yine olumsuz yönde etkilenmektedir.

Dış ilişkilere mahsus sorunların yanı sıra, Türkiye, kendi içinde de bir veri koruma kanununun olmamasının yarattığı ve yaratacağı sorunlarla karşı karşıyadır. Türkiye'de kamu kurum ve kuruluşlarının bazı hizmetlerini elektronik ortama taşımasıyla, T.C. kimlik numarası, sınav sonuçları, vergi borcu, sosyal güvenlik numarası ve prim borcu gibi kişisel verilere yetkisiz erişimlerin teknik olarak mümkün olduğu dönemler yaşanmıştır. Zaman zaman çeşitli bilgiler sorgulama seçeneği yerine, listeler halinde yayımlanmıştır. Yine, farklı internet sitelerinden basit bilgilerle yapılabilen sorgulamalar sonucunda elde edilen kişinin telefon numarasından, aldığı maaşın miktarına, maaşına ne oranda zam yapıldığına, kaç yıldır çalıştığına, maaşını hangi banka şubesinden çektiğine, diploma notuna, su, elektrik ve telefon faturalarına, sınavlardan aldığı puana kadar pek çok bilgi bir araya getirilerek kişiler hakkında anlamlı veri setleri oluşturulabilmiştir. Bürokratik yöntemlerle bazı kamu kurumlarındaki bu tür sorgulamaların yapılmasının önüne geçecek tedbirler alınmıştır. Söz konusu uygulamaların bir bölümü kısmen giderilmişse de, Türkiye'de verilerin paylaşılmasına ilişkin genel nitelikte belirleyici kural, ölçü veya norm halen bulunmamaktadır. Ayrıca, geçmişe dönük bilgilerin de İnternet ortamında tamamen kaybolmayacağı düşünüldüğünde, bu bilgilerin potansiyel kötüye kullanılması tehlikesinin devam ettiğini söylemek yanlış olmayacaktır.

Türkiye'de 5664 sayılı Kanun uyarınca Konut Edindirme Yardımı (KEY) hak sahiplerine yapılacak geri ödemelerde hak sahiplerinin adı, soyadı, T.C. kimlik numarası ve sosyal güvenlik numaralarının birlikte yer aldığı listelerin İnternette yayımlanması bu konuda yaşanan sorunlardan biridir. Söz konusu listeler 27 Temmuz 2008 tarihli ve 26949 sayılı Resmi Gazete'de yayımlanmıştır. Bu olay,

ülkemizde bu olayın önem ve hassasiyetinin farkında olunmadığı, bu yayımın bir hizmet olarak faydalı algılandığını göstermektedir. Oysa, İngiltere'de yaşanan veri kaybı kazası sonucu, Başbakan halktan özür dilemiş ve oldukça büyük bir bütçeyle numaraların değiştirilmesi gündeme gelmiştir. Türkiye'de KEY listesinde yer alan kişilerin halihazırda önemli devlet görevlerinde bulunması veya bulunacak olması nedeniyle bu kişilere ait verilerin ifşası ayrıca ciddi bir ulusal güvenlik zaafiyeti olarak da değerlendirilmektedir. Söz konusu listeler üzerinde bürokratik düzeyde yapılan çalışmalar neticesinde, ilgili Kanun çıkarılana kadar alternatif tedbirler alınarak sonraki listelerin sorgulama yapılmasına imkan verecek şekilde yayımlanması ile, listelerin İnternetten ve uluslararası bazı dosya paylaşım sitelerinden kaldırılması sağlanabilmiştir.

Kısa bir süre için yayımlanmış olsa bile, BİT'in sunduğu olanaklarla birçok veritabanına alınabilen bu bilgiler ile, zincirleme şekilde başkaca kişisel bilgilere ulaşılabilmektedir. Bir başka örnek olarak, MEB tarafından kurulan e-okul sistemine aktarmak üzere okulların anne-baba ve velilerden talep ettiği bilgilerin gündeme getirdiği "fişlenme" kaygısı gösterilebilir. Sistemin "e-okul için öğrenci bilgileri" başlıklı bölümünde öğrencinin anne-babasının kimlik bilgileri yanında bu kişilerin sağlık bilgileri, öğrencinin dinine ilişkin bilgiler, anne-babanın medeni durumu ve üye oldukları sosyal ve kültürel dernekler, sivil toplum örgütlerine ilişkin bilgiler istenmiştir. Bu bilgiler kullanılarak ilgili öğrenci ve aile bireylerine ilişkin profil çıkartılması mümkündür. Bilgi toplama işlemleri konusunda hassasiyet gösterilmemesi, bu bilgilerin yetkisiz kişilerin eline geçmesine ve mahremiyetin ihlal edilerek hukuka aykırı uygulamaların doğmasına sebep olabilecek niteliktedir.

Türkiye'de 2007 genel seçimlerinde ve devamında 2008 yerel seçimlerinde, adrese dayalı kayıt sistemiyle kayıt altına alınan ve Yüksek Seçim Kurulu tarafından askıya çıkartılan 18 yaşından büyük yaklaşık 50 milyon kişiye ait kişisel verilerin ele geçirilerek İnternet üzerinden satışının yapılması kişisel verilerin korunması konusunda ülkedeki en ciddi olay olarak kabul edilebilir. İnternet üzerinden Adres Rehberi adıyla satılan programda, ad soyad, T.C. kimlik no, anne baba adı, doğum yeri, bulunduğu il v.b. farklı kriterlerle arama yapılarak kişilerin adres bilgileri öğrenilebilmektedir. Bedelsiz olarak on sorgulama yapılabilen program 1.500 TL'ye

satılmaktadır. Hatta bu konuda birden fazla program olduğu da söylentiler arasındadır. Türkiye'de yaşanan bu vak'aların sebepleri, bu verilerin nasıl ele geçirildiğinin araştırılması ve sistemdeki açıkların bir an önce kapatılması gerekmektedir.[221]

Genel bir prensip olarak; herhangi bir alanda, kimlik tanımlayıcıların kullanılmasıyla hak sahipliğinin belirlendiği işlemlerde kişisel veriler, o işlemin gerektirdiği miktarla sınırlı olarak ve hak sahipleri arasında iltibasa mahal vermeyecek kadar kullanılmalıdır. Zira, ayrıntılı olarak verilecek bilgiler, anlamlı veri setlerinin oluşturulması suretiyle suç işlenmesinde ve verilerin hukuka aykırı şekillerde analiz edilerek doğrudan pazarlama alanında kullanılmasına sebep olacaktır.

Halihazırda ülkemizde sık rastlanan bir sorun da veri koruma alanında karar verici bir birimin bulunmamasıdır. Günlük hayatta sıkça karşılaştığımız pek çok durumda kimlik kartlarımızın fotokopileri ya da TC kimlik numaralarımız talep edilmektedir. Bu alanlardan birisi de kargo alanında hizmet veren özel sektör firmalarıdır. Bu firmalar, çoğu kez gerekçe göstermeden, bazen de en fazla sözel olarak güvenlik gerekçesi ile yaptıklarını söyledikleri kişisel veri toplama işlemlerinde vatandaşı zor durumda bırakmakta, bu konuda hassasiyet gösteren kişilerin ise verilerini vermezlerse gönderilerini iletmeyeceklerini ifade etmektedirler. Yani ücreti karşılığında alınan bir hizmet için, ücretle orantısı tartışmalı derecede kişisel veri talep edilmektedir. Hatta bu konuda, ülkemizde otobüs firmalarının bazılarının verdikleri kargo hizmetinin, yalnızca göndericinin kimlik kartının fotokopisini doğrudan kolinin üzerine yapıştırılması şartıyla gönderilebileceği ile de karşılaşılmıştır. Oysa ülkemizde bir veri koruma kurumunun varlığı halinde vatandaşlar, bu talepleri kuruma şikayet edebilecek ve hukuka aykırı bu tür uygulamalar karşısında ilgili gerçek/tüzel kişiye para ya da idari cezalarla birlikte, işlemin durdurulması, doğan zararların tazmini, aydınlatma yükümlülüğünün yazılı olarak yerine getirilmesi ya da durumun özelliklerine göre belirlenecek başkaca bir tedbirin alınması gibi karar verilebilecektir.

[221] Turkey Social News. "70 milyon kişinin vatandaşlık bilgisi sadece bin 500 TL." 11 Aralık 2009. Erişim tarihi: 31 Aralık 2009. <http://www.socialnewsturkey.com/2009/12/11/70-milyon-kisinin-vatandaslik-bilgisi-sadece-bin-500-tl/>

Yukarıda, gelişen teknoloji ve İnternet karşısında mevcut sorunlar ve doğabilecek riskler örneklendirilmiş olup, bunlar sınırlı sayıda değildir. Her geçen gün bu tehditlere yenileri eklenmekte olup, kişisel verilerin korunması konusunda gerekli tedbirlerin ivedilikle alınması gerekmektedir.

Kişisel verilerin paylaşılması ve işlenmesi konusunda ortaya çıkan tehlikeler konusunda Türkiye'de yeterli bilinç ve duyarlılığın oluştuğunu söylemek pek de mümkün değildir. TBD'nin Kişisel Verilerin Korunması ile ilgili raporunda bu duyarlılık "…günümüz bilinçli insanı pasaport, sürücü belgesi alırken parmak izi vermekten fişlendiğini bilerek rahatsız olmaktadır, ya da olmalıdır ya da en azından sorgulamalıdır." ifadesiyle vurgulanmaktadır. Gerçekten de, otomatik araçların kullanılmadığı veya nispeten daha az kullanıldığı geçmişe göre, günümüz insanının kendine göre bazı tedbirleri alması gerekmekte, bireylerin kendileriyle ilgili veriler üzerinde tasarruf ederken bilinçli ve bilgili olmaları büyük önem taşımaktadır. Zira, ülkemizde pek çok insan, kimlik numarası, ses kayıtları, ad, soyadı, e-posta adresi, pasaport numarası, çalışılan işyeri, özgeçmiş, banka hesap numarası, resim gibi unsurların kişisel veri olduğunun farkında değildir. Vatandaşların bu konuda bilgilendirilmesi ve bilinçlendirilmesi de yasa çıkarılması kadar büyük önem taşımaktadır.

5.4. Türkiye'de Veri Koruma ile İlgili Mevcut Hukuki Dayanak

Türkiye'de kişisel verileri koruma ile ilgili yapılan düzenlemeler, Anayasa Hukuku, Ceza Hukuku ve Medeni Hukuk'ta etkilerini göstermektedir. KVKK'nın kabul edilmesi ile bu düzenlemelerin daha sistematik, uluslararası gereksinim ve güncel gelişmelere uygun olarak ele alınması sağlanmış olacaktır. Türkiye'de kişisel verilerin korunması ile ilgili mevcut mevzuat Anayasa Hukuku, Ceza Hukuku ve Özel Hukuk alanlarında aşağıda irdelenmektedir.

5.4.1. Anayasa'da kişisel verilerin korunması

Kişisel verilerin korunması konusunun tartışıldığı 1970'li yıllardan bu yana mahremiyet hakkı, kişi hak ve onurunun korunması ve dolayısıyla kişisel verilerin korunması kavramları, anayasalar ile güvence altına alınan *kişilerin özel hayatının korunması* hakkının uzantıları olarak değerlendirilmektedir. Ülkemizde normlar

hiyerarşisi dikkate alındığında en üst sırada yer alan Anayasal hükümler, diğer her tür Kanun ve düzenlemenin uygun ve uyumlu olması gereken hükümler niteliğindedir.

Nitekim Anayasa Mahkemesi'nin 6.1.1999 tarihli, 1996/68 Esas ve 1991/1 numaralı Kararında[222] *kişisel verilerin* Anayasanın 20'nci maddesinde[223] düzenlenen özel hayatın gizliliği ile doğrudan ilişkili olduğu teyit edilmiştir.[224] Bu karar doğrultusunda, kişisel verilerin işlenmesine ilişkin düzenlemelerin, Anayasada yer alan özel hayatın gizliliğinin sınırlandırılmasına ilişkin usul ve esaslara uyması gerekmektedir. Anayasanın 20'nci maddesinin ikinci fıkrasında bu sınırlandırma sebepleri; *milli güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlakın korunması veya başkalarının hak ve özgürlüklerinin korunması* olarak sayılmaktadır. Söz konusu sınırlandırma sebepleri, Anayasa'nın 13'üncü maddesinde temel hak ve hürriyetlerin, özlerine dokunulmaksızın yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabileceği hükmüyle birlikte değerlendirilmelidir. Kişisel verilerin özel hayatın gizliliğinin bir parçası olması nedeniyle, bu veriler üzerindeki haklar da, özüne dokunulmaksızın ancak kanunla sınırlandırılabilecektir.

Anayasanın 22'nci maddesinde kapsam itibarıyla kişisel veri niteliğindeki bilgilerin özel hayat kapsamında değerlendirilmesini sağlayan *haberleşme hürriyeti* ve *aile ve özel hayatın gizliliği* güvence altına alınmaktadır.[225] Anayasanın 13'üncü maddesinde öngörülen temel hak ve hürriyetlerin özlerine dokunulmaksızın ancak

---

[222] Karar için bkz. <http://www.anayasa.gov.tr/eskisite/KARARLAR/IPTALITIRAZ/K1999/K1999-01.htm>

[223] 1982 Anayasasının 20'nci maddesinin birinci fıkrasında: *"Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz."* hükmü yer almaktadır.

[224] Türkiye Bilişim Derneği, 2008:29

[225] AY, Haberleşme Hürriyeti, Madde 22 - (Değişik madde: 03/10/2001 - 4709 S.K./7. md.)
"Herkes, haberleşme hürriyetine sahiptir. Haberleşmenin gizliliği esastır.
Milli güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlakın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak usulüne göre verilmiş hakim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; haberleşme engellenemez ve gizliliğine dokunulamaz. Yetkili merciin kararı yirmidört saat içinde görevli hakimin onayına sunulur. Hakim, kararını kırksekiz saat içinde açıklar; aksi halde, karar kendiliğinden kalkar.
İstisnaların uygulanacağı kamu kurum ve kuruluşları kanunda belirtilir."

kanunla sınırlandırılabileceği hükmü gereği haberleşme hürriyeti, kanun dışındaki sebeplerle sınırlandırılamaz ve haberleşmenin gizliliği ihlal edilemez. Anayasal hükümler, kişisel verilerin korunmasının sınırlandırılmasında dikkate alınması gereken ve hakkın özünü koruyan hükümler olarak değerlendirilmelidir.

Ayrıca, bu çalışmanın hazırlandığı dönemde, ülkemizde, 5982 sayılı "Türkiye Cumhuriyeti Anayasasının Bazı Maddelerinde Değişiklik Yapılması Hakkında Kanun"[226] Anayasa'nın 175'inci maddesinin dördüncü fıkrası uyarınca, halkoyuna sunulmak üzere 13 Mayıs 2010 tarihli ve 27580 sayılı Resmi Gazete'de yayımlanmıştır. 5982 sayılı bu Kanunun 2'nci maddesi ile, Türkiye Cumhuriyeti Anayasasının 20. maddesine aşağıdaki fıkranın eklenmesi öngörülmektedir:

"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."

Söz konusu Kanun, 12 Eylül 2010 tarihinde halkoyuna sunulmuş ve çoğunluğun oyuyla kabul edilmiştir. Bu gelişme ile Türkiye'de de öncelik ve önem kazanan kişisel verilerin korunması hakkının yasa ile de sınırlarının netleşmesi ile, pek çok Avrupa üyesi ülkede olduğu gibi, kişisel verilerin korunması konusu Türkiye'de de yasal temellerine kavuşmuş olacaktır.

Halkoyuna sunularak kabul edilen yukarıdaki madde, kişisel verilerin korunması ile ilgili olarak kişiye temel bir hak ihdas etmektedir. Bu temel hak, beraberinde, kişiye kişisel verileri hakkında bilgilendirilme, bu verilere erişme, verilerin düzeltilmesi veya silinmesini talep etme ve verilerin amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de getirmektedir. Yine kişisel verilerin ancak kişinin açık rızası veya kanunda öngörülen hallerde işlenebileceği ifade edilmiş olup, bu konulardaki usul ve esaslar kanuna bırakılmaktadır. Halkoyuna sunulan söz konusu düzenleme, AB'nin reform çalışmaları kapsamında başlatmış olduğu Avrupa

[226] http://rega.basbakanlik.gov.tr/eskiler/2010/05/20100513-1.htm

Anayasası ile benzerlik göstermektedir. Zira, 29 Ekim 2004'te, 25 üye devletin devlet ya da hükümet başkanları ile Türkiye ve o dönem aday statüsünda bulunan Romanya ve Bulgaristan tarafından da imzalanan Taslak AB Anayasasında da benzer hükümler görülmektedir. Bu Anayasanın kabul edilebilmesi için tüm üye ülkelerce onaylanması gerekmekte olup, 2005 yılında Fransa ve Hollanda'da yapılan referandumlarda siyasi olduğu belirtilen bazı sebeplerle hayır oyu çıkması üzerine Anayasa kabul edilmemiştir. Söz konusu Taslak AB Anayasasının I-51'inci maddesinde kişisel verilerin korunması şöyle ele alınmaktaydı:

"Herkesin kendisiyle ilgili kişisel verilerinin korunmasını isteme hakkı vardır. Avrupa kanunları veya çerçeve kanunları, kişisel verilerin Birliğin kurum, kuruluş, ofis ve ajanslarınca, üye ülkelerin Birlik hukuku kapsamında yürüttükleri faaliyetler sırasında ve bu verilerin serbest dolaşımı ile ilgili kurallarda işlenmesi ile ilgili koruyucu kurallar ihdas edecektir. Bu kurallara uyum, bağımsız kurumlar tarafından sağlanacaktır."

Söz konusu Anayasanın Avrupa'da kabulüne ilişkin sürecin tamamlanıp tamamlanmayacağı ile referandumun yenilenmesi konusu tartışılan konular arasında yer almaktadır.

5.4.2. Ceza Hukukunda kişisel verilerin korunması

5327 sayılı Türk Ceza Kanunu'nda (TCK) kişisel verilerin korunması ile doğrudan ilişkili kimi suçlara yer verilmiştir. Bu suçlar, "Özel Hayat ve Hayatın Gizli Alanına Karşı Suçlar" (md.132-140) başlıklı dokuzuncu bölümde yer almaktadır. Bu bölümde kişisel verilerle ilgili suçlar; haberleşmenin gizliliğini ihlal (md.132), kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması (md.133), özel hayatın gizliliğini ihlal (md.134), kişisel verilerin kaydedilmesi (md.135), verileri hukuka aykırı olarak verme veya ele geçirme (md.136), verileri yok etmeme (md.138) suçları olarak karşımıza çıkmaktadır. Söz konusu suçlar ile bu suçların unsurları ve uygulanmasına ilişkin şartlar aşağıda Tablo 5.1'de özetlenmektedir.

Tablo 5.1. Kişisel Verilerin Korunmasına İlişkin Türk Ceza Kanununda Düzenlenen Suçlar

5237 s. Türk Ceza Kanunu md. 135, 136, 138	Kişisel verilerin hukuka aykırı olarak kaydedilmesi (135. md.)	Kişisel verileri hukuka aykırı olarak verme veya ele geçirme (md.136)	Verileri yok etmeme (md.138.)
Maddi Unsur	Kişisel verilerin kaydedilmesi	Başkasına verme, Yayma, Ele geçirme	Sistem içinde veriyi yok etmeme
Manevi Unsur	Kasıt	Kasıt	Kasıt
İşleme Sekli	Otomatik / Elle	Otomatik / Elle	Otomatik/ Elle işleme sistemin yorumuna bağlı
Uygulama alanı	Kamu / Özel	Kamu / Özel	Kamu / Özel
Şikayet şartı	Yok (md. 139)	Yok (md. 139)	Yok (md. 139)
137. maddede yer alan ağırlatıcı nedenlerin uygulanma sebebi (cezada yarı oranında artırım getiren)	-kamu görevlisi tarafından görevin verdiği yetkinin kötüye kullanılması -belli meslek/sanatın sağladığı yetkinin kötüye kullanılması	-kamu görevlisi tarafından görevin verdiği yetkinin kötüye kullanılması -belli meslek/sanatın sağladığı yetkinin kötüye kullanılması	-
Ceza	6 aydan 3 yıla kadar hapis cezası (137. maddede sayılan ağırlatıcı nedenlerin varlığı halinde yarı oranında artırılır)	1 yıldan 4 yıla kadar hapis cezası (137. maddede sayılan ağırlatıcı nedenlerin varlığı halinde yarı oranında artırılır)	6 aydan 1 yıla kadar hapis cezası (137. maddede sayılan ağırlaştırıcı nedenlerin varlığı halinde yarı oranında artırılır)
Tüzel kişilere özgü güvenlik tedbirleri (140. md. dolayısıyla 60. md.)	Evet	Evet	Evet

Kaynak: TBD, 2008:34

Henüz kişisel verilerin korunmasına ilişkin bir kanun çıkarılmadan TCK'daki md. 135 vd. niteliğindeki hükümler, hukuka aykırılığın hangi hallerde oluştuğuna ilişkin başvurulabilecek kapsayıcı bir kaynak ya da norm olmaması nedeniyle eksik norm sayılabilir. KVKK'nın çıkarılması ile kişisel verilerin korunması alanında çerçeve düzenleme tamamlanmış olacaktır. Bu söylenenlere karşın söz konusu hükümler yürürlüktedir. Bu hükümlerin yürürlükte olması kurum ve kuruluşların gerekli tedbirleri almasını zorunlu kılmaktadır. Bu nedenle de kurum ve kuruluşların hangi hallerde hangi tür kişisel verileri işlemekle yetkili oldukları konusunda kendi mevzuatı ve ilgili diğer mevzuat hakkında bilgi sahibi olması zorunludur. Uygulamada ortaya çıkan kişisel veri işleme halleri söz konusu hükümler karşısında hukuka aykırı olabilecektir. [227]

[227] TBD, 2008:35

Anayasal bir hak olan haberleşmenin gizliliği ilkesi bazı durumlarda kanunla sınırlandırılmaktadır. Suçların kovuşturulmasına ilişkin olarak, 5271 sayılı Ceza Muhakemesi Kanunu'nun (CMK) 135'inci maddesine göre, bir suç dolayısıyla yapılan soruşturma ve kovuşturmada, suç işlendiğine ilişkin *kuvvetli şüphe* sebeplerinin varlığı ve *başka suretle delil elde edilmesi imkanının bulunmaması* durumunda, hakim veya gecikmesinde sakınca bulunan hallerde Cumhuriyet Savcısının kararıyla, şüpheli veya sanığın telekomünikasyon yoluyla iletişimi tespit edilebilir, dinlenebilir, kayda alınabilir ve sinyal bilgileri değerlendirilebilir. Bu kararda tedbirin türü, kapsamı ve süresi belirtilmelidir.

2559 sayılı Polis Vazife ve Salahiyet Kanunu ve 2803 sayılı Jandarma Teşkilat, Görev ve Yetkileri Hakkında Kanunlar da telekomünikasyon yoluyla yapılan iletişimin tespitine ilişkin yetki verici diğer Kanunlardır. 2559 sayılı Kanunun Ek 7'nci maddesinde belirtildiği üzere, 5271 sayılı Ceza Muhakemesi Kanununun, casusluk suçları hariç, 250'nci maddesinin birinci fıkrasının (a), (b) ve (c) bentlerinde yazılı suçların işlenmesinin önlenmesi amacıyla, hakim kararı veya gecikmesinde sakınca bulunan hallerde Emniyet Genel Müdürü veya İstihbarat Dairesi Başkanının yazılı emriyle, telekomünikasyon yoluyla yapılan iletişim tespit edilebilir, dinlenebilir, sinyal bilgileri değerlendirilebilir, kayda alınabilir. Uygulanan tedbirin sona ermesi halinde, dinlemenin içeriğine ilişkin kayıtlar en geç on gün içinde yok edilir. Aynı şekilde, 2803 sayılı Kanunun ek 5'inci maddesinde hakim kararı ile veya gecikmesinde sakınca bulunan hallerde Jandarma Genel Komutanı veya istihbarat başkanının yazılı emriyle, jandarma da telekomünikasyon yoluyla yapılan iletişimi tespit edebilme, dinleyebilme, sinyal bilgilerini değerlendirebilme ve kayda alabilme yetkilerini haizdir. 2937 sayılı Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanununun 6'ıncı maddesine göre ise, belirlenmiş durumlarda MİT Müsteşarı veya yardımcısının yazılı emriyle telekomünikasyon yoluyla yapılan iletişim tespit edilebilir, dinlenebilir, sinyal bilgileri değerlendirilebilir ve kayda alınabilir. Gecikmesinde sakınca bulunan hallerde verilen yazılı emir, yirmi dört saat içinde yetkili ve görevli hakimin onayına sunulur, hakim kararını en geç yirmi dört saat içinde verir, sürenin dolması ya da hakim

tarafından aksine karar verilmesi halinde tedbir derhal kaldırılır ve kayıtlar en geç on gün içinde yok edilir.

Yukarıda ifade edilen tüm 5271, 2559, 2803 ve 2937 sayılı Kanunlar uyarınca usulüne uygun olarak alınmış telekomünikasyon yoluyla yapılan iletişimin tespit edilmesi kararları ve yazılı emirler, gereğinin icrası için Bilgi Teknolojileri ve İletişim Kurumu bünyesinde, Kurum başkanına doğrudan bağlı "Telekomünikasyon İletişim Başkanlığı" (TİB) adıyla kurulan merkeze havale edilir. Söz konusu kararlar ve yazılı emirler, "Ceza Muhakemesi Kanununda Öngörülen Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi, Gizli Soruşturmacı ve Teknik Araçlarla İzleme Tedbirlerinin Uygulanmasına İlişkin Yönetmelik"in 14'üncü maddesi gereğince ilgili kurum görevlileri ve TİB tarafından yerine getirilir. Suç soruşturma veya kovuşturmasında kullanılabilen bir diğer yöntem de teknik araçlarla izlemedir. "Ceza Muhakemesi Kanununda Öngörülen Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi, Gizli Soruşturmacı ve Teknik Araçlarla İzleme Tedbirlerinin Uygulanmasına İlişkin Yönetmelik"in 15'inci maddesine göre, bu Yönetmelikte belirtilen suçlardan biri dolayısıyla yapılan soruşturmalarda, suçun işlendiğine ilişkin kuvvetli şüphe sebeplerinin bulunması ve başka suretle delil elde edilememesi halinde, şüpheli veya sanığın kamuya açık yerlerdeki faaliyetleri ve işyeri hakim kararı alınmak koşuluyla teknik araçlarla (video gibi) izlenebilir, ses veya görüntü kaydı alınabilir. Teknik araçlarla izleme konusunda 2559 sayılı Polis Vazife ve Salahiyet Kanunu, 2803 sayılı Jandarma Teşkilat, Görev ve Yetkileri Hakkında Kanun ve istihbarata ilişkin mevzuatta da benzer hükümler bulunmaktadır. Teknik araçlarla izlemenin kişilere zarar vermemesi ve veri koruma çerçevesine uygun olabilmesi için bu tedbir ile ulaşılmak istenen amacın da yasal olması, kamu yararının bulunması, gözetlemenin zorunlu olması ve amaç ile araç arasında bir ölçünün olmasına dikkat edilmelidir.

5.4.3. Özel hukukta kişisel verilerin korunması

1982 Anayasası'nın "Kişinin dokunulmazlığı, maddi ve manevi varlığı" başlıklı 17'nci maddesi herkesin, yaşama, maddi ve manevi varlığını koruma ve geliştirme hakkı olduğunu ifade etmektedir. Bu hak, kişilik hakkını oluşturmaktadır.

Özel hukukta kişisel verilerin korunmasına ilişkin düzenlemelerin çerçevesini oluşturan bu Anayasal hükmün kişisel verilerin korunması ile ilişkili olarak TMK'daki yansıması; kişiliğin korunması ile ilgili 24-27'nci maddeleri ile Borçlar Kanunu'nun şahsi menfaatlerin haleldar olmasına ilişkin 49'uncu maddesidir.

Kişisel veriler, kişilik hakkına dahil değerler olduğundan, bu değeri konu edinen hukuki işlemlerde, hak ve fiil ehliyetinin kısıtlanması hallerinde TMK'nin 23'üncü maddesi uygulama alanı bulur. Zira bu hüküm, kişilik hakkına hukuki işlem yoluyla yapılan saldırılardan korumayı amaç edinir. Kişilik hakkına giren maddi ya da manevi bir varlığın saldırıya uğraması durumunda TMK'nin 24'üncü maddesi saldırıya karşı korunmayı isteme yetkisi verirken, 25'inci madde ise kişilik hakkına saldırı karşısında açılacak davaları konu edinir. Kişisel veriler, kişilik hakkı kapsamında değerlendirildiğinden, bu verilere yönelik saldırı tehlikesinin önlenmesi, sürmekte olan saldırıya son verilmesi, sona ermiş olsa bile etkisinin devam etmesi nedeniyle saldırının hukuka aykırılığının tespiti davaları bu çerçevede koruma bulacaktır.[228] TMK md. 25'te sayılan söz konusu davalar savunma davaları olarak adlandırılır. Bu madde çerçevesinde kişisel verileri ihlal edilenlerin tazminat hakkı da saklıdır. Kişiliğin korunmasına ilişkin tazminat davaları, maddi tazminat davası, manevi tazminat davası ve saldırıdan elde edilen kazancın verilmesi davasıdır. TMK md. 25/II'e göre, savunma davalarından herhangi birini açan davacı, maddi ve manevi tazminat istemleri ile hukuka aykırı saldırı dolayısıyla elde edilmiş kazancın, vekaletsiz iş görme hükümlerine göre kendisine verilmesine ilişkin istemde bulunabilecektir. Özel hukuk alanında kişisel verilerin korunmasına ilişkin diğer bazı düzenlemeler de mevcuttur. Bunlardan biri de, sektör itibarıyla kişisel verilerle

[228] **TMK, Madde 23** - Kimse, hak ve fiil ehliyetlerinden kısmen de olsa vazgeçemez.
Kimse özgürlüklerinden vazgeçemez veya onları hukuka ya da ahlaka aykırı olarak sınırlayamaz. Yazılı rıza üzerine insan kökenli biyolojik maddelerin alınması, aşılanması ve nakli mümkündür. Ancak, biyolojik madde verme borcu altına girmiş olandan edimini yerine getirmesi istenemez; maddi ve manevi tazminat isteminde bulunulamaz.
Madde 24 - Hukuka aykırı olarak kişilik hakkına saldırılan kimse, hakimden, saldırıda bulunanlara karşı korunmasını isteyebilir.
Kişilik hakkı zedelenen kimsenin rızası, daha üstün nitelikte özel veya kamusal yarar ya da kanunun verdiği yetkinin kullanılması sebeplerinden biriyle haklı kılınmadıkça, kişilik haklarına yapılan her saldırı hukuka aykırıdır.
Madde 25 - Davacı, hakimden saldırı tehlikesinin önlenmesini, sürmekte olan saldırıya son verilmesini, sona ermiş olsa bile etkileri devam eden saldırının hukuka aykırılığının tespitini isteyebilir.

yakından ilgili olan istatistiklerdir. Veri gizliliğinin önem arz ettiği konulardan olan istatistiki verilerin hangi usul ve esaslarda toplanacağı ve paylaşılacağına ilişkin 5429 sayılı Türkiye İstatistik Kanunu'nda da kişisel verilerin toplanması, işlenmesi, kaydedilmesi ve devredilmesine ilişkin çeşitli tedbirler yer almaktadır. Bu Kanunda, gizli verinin[229] kişiyle ilişkilendirilebilir olması hususu VKD'deki kişisel veri tanımının kişiyi belirleyebilir olması ile örtüşmektedir. Yine *istatistiki amaçlı kullanım sınırlaması*[230] ise, OECD Rehber İlkelerinde yer alan *amaca uygunluk* prensibi ile benzeşmektedir. Kanunun gizli verilere ilişkin 13'üncü maddesinde, resmi istatistik üretiminde görev alanlara, gizli verilere sadece görevlerini yerine getirebilmek için ihtiyaç duydukları ölçüde erişebilecekleri ile resmi istatistiklerin üretilmesi için toplanan, işlenen ve saklanan verilerden gizli olanların, idari, adli ve askeri hiçbir organ, makam, merci veya kişiye verilemeyeceği, istatistik amacı dışında kullanılamayacağı ve ispat aracı olamayacağı hükme bağlanmaktadır. Bilgileri derleyen ve değerlendiren memurlar ve diğer görevliler de bu yasağa uymak zorundadır. Bu yükümlülük, görevlilerin görevlerinden ayrılmalarından sonra da devam eder.

Hakkında istatistiki bilgi tutulan kişi veya kurum, kendisine ait gizli verilerin açıklanmasına "yazılı onay" verirse, veri gizliliği de ortadan kalkar. Bunun dışında, veriler anonimleştirilerek, kişiyi doğrudan ya da dolaylı tanımlamaya yol açmayacak şekilde diğer bilgilerle birleştirilmesi suretiyle yayımlanabilirler. Bu hükümler, Türkiye İstatistik Kanununda "istatistiki birim" olarak kabul edilen bireyi korumaya yöneliktir.

---

[229] **Gizli veri:** İstatistiki birimin doğrudan veya dolaylı bir şekilde özellikleri ile birlikte tanınabilmesine ve bu şekilde bireysel bilgilerin açığa çıkarılmasına imkân sağlayan bireysel veya tablo halinde saklı tutulan veriyi ifade eder (5429 sayılı Kanun, md. 2/s).
Md. 13/2: "Bireysel verinin toplulaştırılması ile oluşturulan veri tablosunun herhangi bir hücresindeki istatistikî birim sayısının üçten az olması veya birim sayısı üç ve daha fazla olduğu hâlde bir veya iki istatistikî birimin hakim durumda olması hâlinde ilgili hücredeki veri gizli kabul edilir."
Md. 13/5: "Herkese açık kaynaklardan elde edilen veri veya bilgiler gizli kabul edilmez."

[230] İstatistik amaçlı kullanım: İstatistiki birimlerden toplanan verilerin sadece istatistikî tabloların oluşturulması ve istatistikî analizlerin yapılması için kullanımını ifade eder. (5429 sayılı Kanun, md. 2/t)

Türkiye'deki bilgi toplumu çalışmaları kapsamında, Nisan 2004'te yürürlüğe giren Bilgi Edinme Hakkı Kanunu,[231] iş ve işlemlerde demokratik ve şeffaf yönetimin gereği ve açık erişim rejiminin yansıması olarak atılmış önemli adımlardan biridir. Bilgi Edinme Hakkı Kanunu, kamu kurumlarına karşı, kişiye kendisi ile ilgili verilerin doğruluğu ve güncelliği hakkında bilgi vermesi bakımından veri koruma hukuku için bir destek enstrüman olarak kabul edilebilir. Bu Kanun, daha önce OECD Rehber İlkeleri'nde yer verilen bireyin katılımı şartının ülkemizdeki önemli adımlarından biri olarak değerlendirilmelidir. Bu Kanuna göre bilgi, *kurum ve kuruluşların sahip oldukları kayıtlarda yer alan bu Kanun kapsamındaki her türlü veriyi* (md. 3/c) ifade etmektedir. Söz konusu Kanunda, kişisel veriler üzerindeki temel haklar veya veri korumaya ilişkin ilkeler yer almamaktadır. Ancak bu Kanun, bilgi edinme hakkını (freedom of information) düzenlemesi nedeniyle tüm dünyada olduğu gibi ülkemizde de bilgi toplumunun yasal altyapısının şekillenmesinde kişisel verilerin korunması hukuku ile birlikte değerlendirilmektedir.

Türkiye'de kişisel verilerin korunması bağlamında özel hayatı ilgilendiren diğer bazı düzenlemeler şunlardır:

- Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Korunması Hakkında Yönetmelik (6 Şubat 2004)
- Bazı özel Kanunlar (4857 sayılı İş Kanunu, 5490 sayılı Nüfus Hizmetleri Kanunu)
- Resmi İstatistiklerde Veri Gizliliği ve Gizli Veri Güvenliğine İlişkin Usul ve Esaslar Hakkında Yönetmelik

5.5. Kişisel Verilerin Korunması Kanunu Tasarısının İncelenmesi

Bu çalışmanın hazırlanması sırasında TBMM Adalet Komisyonunda bulunmakta olan KVKK Tasarısı, genel nitelikte hükümler içermekte ve veri korumaya ilişkin sektörel nitelikteki düzenleme ihtiyaçlarını ise bu çerçeveye bağlı

[231] Kanun ile, belirli istisnalar dışında, kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarına bilgi verme yükümlülüğü getirilmektedir.

kalacak şekilde, ilgili kurum, kuruluş ve meslek birliklerine bırakmayı tercih etmektedir.

Tasarı, kişisel verileri işleme tabi tutulan kişiler ile bu verileri işleme tabi tutan kamu kurum ve kuruluşları ile gerçek ve özel hukuk tüzel kişilerini kapsamaktadır. Söz konusu kişisel veriler, geleneksel dosyalama yöntemiyle işlemede olduğu gibi, otomatik işlemeye tabi tutulduklarında da bu Kanun çerçevesindeki ilke ve kurallara tabi olacaklar; verileri işlenenler ise bu Kanun çerçevesinde çeşitli haklarını kullanabileceklerdir. Kişisel verilerin, kamu kuruluşlarınca, gerçek veya özel hukuk tüzel kişileri tarafından işlenmesi dolayısıyla kişilik hakları ihlal edilenlerin şikayetleri konusunda Kişisel Verileri Koruma Kurulu (Kurul) karar verecektir. Kişilik hakları ihlal edilen bireyin tazminat hakları ise saklı tutulmuştur.

Avrupa Konseyi'nin 108 sayılı Sözleşmesi'nin 10'uncu maddesi ve AB'nin 95/46/AT sayılı Direktifinin (VKD) 11'inci bölümünde devletlerin kişisel veri işleme ilkelerinin ihlali halinde yaptırım uygulamaya davet edilmesi de dikkate alınarak, Tasarıda, ihlalin ağırlık derecesine göre idari para cezaları ile ayrıca hapis ve para cezaları öngörülmektedir.

KVKK Tasarısı beş kısımdan oluşmaktadır.

Birinci Kısımda *(md. 1- md. 10)*; Tasarının amaç ve kapsamı belirlenmiş ve Tasarıda kullanılan terimlerin tanımları yapılmıştır. Buna göre, bu Kanunun amacı kişisel verilerin işlenmesinde kişinin dokunulmazlığı, maddi ve manevi varlığı ve temel hak ve özgürlüklerini korumak ve veri işlemelerinde uyulması gereken usul ve esasları düzenlemektir. Bu çerçevede hakları korunacak kişiler, kişisel verileri işlenen gerçek ve tüzel kişiler olup; bu korumanın talep edileceği muhataplar ise otomatik olan veya olmayan yollarla veri işleyen gerçek ve tüzel kişilerdir. Gerçek kişilerin sadece kişisel veya birlikte oturduğu kişiler veya ailesi ile ilgili faaliyetleri bu kanun kapsamı dışında tutulmaktadır. Bu Kısımda, kişisel verilerin ancak bu Kanunda ve diğer kanunlarda öngörülen hallerde işlenebileceğine dair "kanunilik" ilkesine yer verilmektedir. İlgili uluslararası belgelere paralel olarak, ceza hukukunda olduğu gibi, bu Kanun kapsamında da kanunilik ilkesinin benimsenmesi, keyfi

uygulamaların önlenmesinde bir teminat niteliğinde kabul edilebilir. Ancak uygulamada bu ilkenin, salt *şekli* anlamda yasama organı tarafından kanun koyma usulüne göre çıkarılan metinleri mi, yoksa *maddi* anlamda mevzuata karşılık gelen ve hukuk kaidesi olarak mecburilik ve genellik vasfını yasama organından değil, yürütme (icra) organından alan tüzük ve yönetmelikleri de mi kapsayıp kapsamayacağı tartışma yaratabilecektir.

Birinci Kısmın devam eden maddelerinde, VKD, OECD'nin Mahremiyet Rehber İlkeleri ve Avrupa Konseyi'nin 108 numaralı Sözleşmesi ile uyumlu olarak, kişisel verilerin işlenmesine ilişkin ilkeler ile kişisel verilerin kural olarak ilgili kişinin açık rızasıyla işlenebileceği ve hukuka uygunluk sebepleri belirlenmekte; özel niteliği olan ırk, siyasi düşünce, felsefi inanç, din, mezhep veya diğer inançlar ile dernek, vakıf, sendika üyeliği, sağlık ve özel yaşam ve her tür mahkumiyet ile ilgili kişisel verilerin işlenemeyeceği kuralı getirilmektedir. Bununla birlikte, Tasarıda, vatandaşlık kimlik numarasının ve benzeri karakteristik işaretlerin işlenme usul ve esaslarının belirlenmesinde Kurulun görüşünün alınacağı ifade edilmektedir. Yine bu bölümde, milli güvenliğin sağlanması, suçun önlenmesi, istihbari faaliyetlerle ilgili devam eden bir soruşturmada kanundan kaynaklanan bir görevin yerine getirilmesi hallerinde de kişisel verilerin ilgili kamu kurum veya kuruluşuna aktarılabileceği; ihtiyaç duyulmayan kişisel verilerin anonim hale getirilmesi veya yok edilmesine ilişkin usul ve esasların ilgili kurum ve kuruluşlarca yönetmelikle belirleneceği ve planlama, istatistik ve araştırma amacıyla veri işlemelerinde, bu verilerin yalnızca anonim hale getirildikten sonra işlenebileceği hükme bağlanmaktadır. KVKK Tasarısının İkinci Kısmında *(md. 11- md. 15)*; veri işleyenlere (veri kütüğü sahibi) verisi işlenen gerçek veya tüzel kişileri aydınlatma yükümlülüğü yüklenmekte ve verisi işlenen gerçek ve tüzel kişilerin hakları ile yurtdışına veri aktarımına ilişkin hususlar belirlenmektedir. Aydınlatma yükümlülüğü kapsamında, verisi işleneceklere veri kütüğü sahibinin veya varsa temsilcisinin kimliği, verilerin hangi amaçla işleneceği, kimlere aktarılacağı, veri toplamanın yöntemi, hukuki sebebi, muhtemel sonuçları ile ilgili kişinin kişisel verilerini öğrenme ve düzeltme hakları konusunda bilgi verilmesi gerekmektedir. Eğer veriler, kişinin dışındaki bir kaynaktan temin ediliyorsa, bu konuda da ilgili kişinin bilgilendirilmesi gerekmektedir. Bunun

karşılığında verisi işlenen kişilere, veri kütüğü sahibine başvurarak kendisiyle ilgili kişisel veri kaydedilip kaydedilmediğini öğrenme, kaydedilmişse bunları talep etme, verilerin düzeltilmesini isteme, işlemin hukuka aykırı olması durumunda verilerin silinmesini, aktarımının engellenmesini isteme gibi haklar tanınmaktadır. Söz konusu taleplere karşılık veri kütüğü sahibi 15 iş günü içinde cevap vermek zorunda olup, bu süre içerisinde cevap alamayan veya olumsuz cevap alan kişiler, 20 gün içinde Kurula itiraz edebilirler. İlgili kişiye tanınan bu haklar, yalnızca milli güvenliğin korunması, milli savunmanın gerçekleştirilmesi, suçun önlenmesi veya istihbarat amacıyla kanundan kaynaklanan bir görevin yerine getirilmesi ile ceza soruşturma veya kovuşturmasına zarar verilmesinin engellenmesi nedenleriyle sınırlandırılabilir. Yine Tasarının İkinci Kısmında (md. 14) verinin yurt dışına hangi koşullarda aktarımının yapılabileceği ile verinin aktarılacağı ülkede eşdeğer ve etkin bir koruma olmaması durumunda Kurul görüşünün alınacağı düzenlenmektedir.

Tasarının AB ve uluslararası düzenlemelere uyumlu olarak düzenlenen üçüncü Kısmında ise (md. 16-md. 25); Sicil ve Kurula bildirim ve ön inceleme konuları ile özel denetim kuruluşları, istisna getiren hükümler, mesleki davranış kuralları, kişisel verilerin silinmesi ve yok edilmesi konuları düzenlenmektedir. Tasarıya göre, Kurul, kişisel verileri işleyen gerçek ve tüzel kişilerin, veri kütüğü kurmadan önce kaydolmak zorunda oldukları bir Sicil tutacaktır. Kamuya açık olarak tutulacak bu Sicile kayıt için, veri kütüğü sahibi, kendisine ilişkin kimlik ve adres bilgileri, veri işlemenin amacı, varsa üçüncü ülkelere veri aktarımına ilişkin bilgilerle başvuru yapacak ve bu bilgilerin değişmesi halinde Kurula yeni bildirimde bulunacaktır. Ancak Tasarıda, Kurulun, kayıt başvurusu üzerine bir aylık süre içinde yapacağı ön incelemede, kişilerin temel hak ve özgürlüklerine yönelik riskli veya genel olarak bu Kanun kapsamına aykırılık teşkil edecek veri işlemeleri için ne tür kararlar alacağına yönelik bir belirleme bulunmamaktadır.

Tasarının dördüncü Kısmında *(md.26- md.33)*; "Kişisel Verileri Koruma Kurulu"nun oluşumu ile Kurulun yetki ve görevlerine, son ve beşinci Kısmında *(md. 34-md. 39)* ise; kişisel verilerin hukuka aykırı olarak işlenmesi durumunda izlenecek soruşturma ve kovuşturma esasları ile uygulanacak idari para cezaları ile hapis ve para cezasına yer verilmektedir.

5.5.1. Tasarı ile öngörülen kurumsal yapının incelenmesi

Tasarının 26'ncı maddesinin birinci fıkrasında bu Kanunla verilen görevleri yapmak üzere, Kişisel Verileri Koruma Kurulu oluşturulmaktadır. Tasarının genel gerekçesi ve aynı maddesinin ikinci fıkrasına göre Kurul yetkilerini *bağımsız* olarak kullanacak, hiçbir organ, makam, merci veya kişi Kurulun kararını etkilemek amacıyla emir ve talimat veremeyecektir. Ayrıca, Kurul görevlerini yerine getirirken tüm kamu kurum ve kuruluşları ile gerçek ve tüzel kişilerden her türlü bilgi ve belgeyi isteyebilecek, bu kurum, kuruluş ve kişiler söz konusu isteğe cevap verecek ve gereken kolaylığı sağlayacaktır.

Kurulun oluşumu ve görev süreleri:

Tasarıya göre (md. 27) yedi üyeden oluşacak ve altı yıl görev yapacak olan Kurul üyelerini ve Kurul Başkanını Bakanlar Kurulu seçecektir. Görev süreleri dolan üyeler yeniden seçilemeyecek olup, Başkanlık ve üyelikler, görev süresi dolmadan herhangi bir sebeple boşaldığı takdirde, boşalan yerlere bir ay içinde ilk seçim usulüne uygun olarak yine Bakanlar Kurulu tarafından yeni üye seçilecektir. Bu şekilde seçilen üye, yerine atandıkları kişinin 6 yıla kalan süresini tamamlayacaktır. Bu şekilde seçilenlerden iki yıl veya daha az süreyle görev yapanlar bir defalığına tekrar seçilebileceklerdir. Başkan ve üyelerin güvence içinde görev yapmalarını sağlamak üzere, görev süreleri dolmadan görevlerine son verilemeyecek olup; seçilmeleri için gerekli şartları taşımadıkları anlaşılan, görevleri ile ilgili olarak işledikleri suçlardan dolayı haklarında mahkumiyet kararları kesinleşen Başkan veya üyelerin ise Başbakanın onayıyla görevden alınabileceği hükme bağlanmaktadır.

Kurulun çalışma esasları:

Tasarının 30'uncu maddesine göre, Kurul ayda iki defa olmak üzere en az beş üye ile toplanır ve üye tamsayısının salt çoğunluğuyla karar alır. Kurul üyeleri, çalışmaları ve denetlemeleri sırasında öğrendikleri sırları kanunen yetkili merciler dışında, görev süreleri sona erdikten sonra dahi açıklayamazlar. Kurul üyelerine, daha önce kamu görevi yapıp yapmadığına bakılmaksızın 3000 gösterge rakamının memur aylık katsayısı ile çarpımı sonucunda elde edilecek miktar, görev yaptıkları

her gün için huzur hakkı olarak ödenir. Bir ay içinde dörtten fazla huzur hakkı ödenmez.

Tasarıda Kurulun sekreterya hizmetlerinin Başbakanlık tarafından yerine getirileceği de hükme bağlanmaktadır.

Kurulun görev ve yetkileri:

Kurulun görev ve yetkileri (md. 31) başlıca; kişisel verileri işlenerek kişilik hakları ihlal edilenlerin şikayetleri konusunda karar vermek, bu kişiler bakımından telafisi güç veya imkansız zararların doğması ihtimali halinde geçici önlemler almak, veri işlenmesine ilişkin düzenleyici işlemleri hazırlamak, sicilin tutulmasını sağlamak, yurt dışına veri aktarımına ilişkin tereddütlü durumlarda karar vermek ve ulusal ve uluslararası makamlarla işbirliği içinde bulunmak, gerekirse araştırma ve teknik yardım projeleri hazırlamak ve yürütmek olarak belirlenmiştir. Kişilik hakları ihlal edilen bireylerin özel hukuk hükümlerine tabi olan tazminat hakları ise saklı tutulmuştur.

Kurula ayrıca, kişisel verileri işleyen kamu kurum ve kuruluşları ile gerçek ve özel hukuk tüzel kişilerinin kamuya açık Sicilleri ile bu Kanunun uygulanmasını sağlamak üzere görevlendirilen ve herhangi bir talimat almaksızın denetim yapacak olan "veri koruma denetim kuruluşları" için "bağımsız denetim kuruluşu sicili" tutma görevleri verilmektedir. Kurulun diğer ülkelerde de olduğu gibi her yıl bir önceki yıla ait kararları, yaptığı düzenlemeleri ile bunların ekonomik ve sosyal etkilerini analiz eden bir faaliyet raporu hazırlayarak yayımlaması da gerekmektedir (md. 38/2). Tasarıya göre Kurulun bir diğer görevi de kişisel verilerle ilgili düzenlemeler hazırlamak veya hazırlanan düzenlemelere görüşler vermektir.

Tasarının 32'nci maddesine göre, bu Kanunun uygulanmasından kaynaklanan şikayetler, şikayet konusu işlemin yapıldığı veya öğrenildiği tarihten itibaren 60 gün içinde Kurula yapılabilecektir. Kurulun şikayetleri inceleme süresi üç aydır. Bu süre içinde, inceleme hukuki veya fiili sebeplerle sonuçlandırılmaz ise, süre bir defaya mahsus üç ay daha uzatılabilir.

Kurul, yaptığı inceleme üzerine, bu Kanun hükümlerinin ihlal edildiğine karar verirse, verdiği Kararı veri kütüğü sahibine iletir ve verilerin bu Kanun

hükümlerine uygun olarak işlenmesini ister. Veri kütüğü sahibi, bu kararı derhal yerine getirir. Veri kütüğü sahibinin kamu tüzel kişisi olması durumunda ise, Kurul aynı şekilde, ilgili kamu tüzel kişisinden verilerin hukuka uygun işlenmesini ister. İlgili kamu tüzel kişisinin bu isteği en geç bir ay içinde yerine getirmesi gerekmektedir.

Telafisi güç veya imkansız zararların doğması ihtimali veya açıkça hukuka aykırılık halinde Kurul, ilgili kişi hakkında veri işlenmesinin veya yurt dışına aktarımının durdurulmasına da karar verebilir (md. 33/6).

6. TÜRKİYE İÇİN HUKUKİ DÜZENLEME VE KURUMSAL YAPILANMA ÖNERİLERİ

Kişisel verilerin ticari bir değer haline geldiği günümüzde, bu verilerin gelişigüzel kullanılması karşısında kişi haklarının ihlali nedeniyle birtakım kurallar seti oluşturulması zorunlu hale gelmiştir. Buna karşın, Türkiye'nin politikalarına da yansıtmış olduğu bilgi toplumu olma vizyonu çerçevesinde, e-dönüşüm ve e-devlet alanında yürütülen çalışmalar kapsamında halen kişisel verilerin hukuki korumasının sağlanmamış olması, bu girişimlerin güvenilirliğine zarar vermektedir. Bu durum, Türkiye'nin BİT kullanarak gelişmesi yolundaki engellerden biri olmanın yanı sıra, yürütülen e-devlet projelerinde belli bir aşamadan sonra, verilerin yönetimi konusunda boşluklar nedeniyle inisiyatife dayalı farklı uygulamaların doğmasına sebep olabilmekte; böylece ekonomik ve sosyal kayıpların yaşanması kaçınılmaz hale gelmektedir.

Türkiye'de kişisel verilerin korunması konusunda farkındalığın düşük olması, bu konu hakkında çeşitli çekinceleri de beraberinde getirmekte; bazı kesimler içeriğinin tam aksine bir veri koruma kanunu çıkarılmasına endişe ile bakmaktadırlar. Bu endişenin temelinde ise kişilerin fişlenecekleri iddiaları yer almaktadır. Kişisel verilerin korunması yaklaşımının son yıllarda daha etkin bir şekilde ortaya çıkışına rağmen söz konusu yanlış anlamanın sebebinin, bu konunun hukuk için yeni bir çalışma alanı olmasının kişilerde yarattığı kaygı olduğu değerlendirilmektedir. Dolayısıyla yaşanan çekinceler esasında konunun ülkemizde gerektiği şekilde anlaşılamamış olmasından kaynaklanmakta; böylece bir veri koruma kanunu çıkarılması ve uygulamadan sorumlu olacak bir kurum kurulması fikri sağlıklı bir tartışma ortamında gündeme gelememektedir.

Oysa pek çok ülkede uzun yıllardan beri veri koruma düzenlemeleri ve uygulama birimleri bulunmaktadır. Hatta kişisel veri koruma konusunun anavatanı sayılan Avrupa'da, VKD ve bununla uyumlu ulusal kanunlar çıkarıldıktan sonra dahi, bu hususun peşi bırakılmamış, yaygınlaşan elektronik araçların vatandaşlarda yarattığı huzursuzluk ve "acaba kişisel verilerimi paylaşmalı mıyım?" endişesini ortadan kaldırmak üzere AB, yeni politika ve stratejilerinde vatandaşa kişisel veriler

konusunda daha fazla hak tanıyan, etkin ve koruyucu düzenlemeleri yapma niyetini beyan etmiştir. Son olarak, Avrupa Konseyi'nin küresel ekonomik krizin etkilerin azaltmak, akılcı, sürdürülebilir ve kapsayıcı büyüme dinamiklerini harekete geçirmek üzere 17 Haziran 2010 tarihinde resmi olarak kabul ettiği "Avrupa 2020: Akılcı, Sürdürülebilir ve Kapsayıcı Büyüme Stratejisi"[232]nin (kısaca Avrupa 2020) yedi temel ekseninden birisi de "Avrupa için Sayısal Gündem" olmuştur. Avrupa Komisyonu'nun 19 Mayıs 2010 tarih ve COM(2010) 245 sayılı Bildirisi[233] ile ortaya koyduğu söz konusu Sayısal Gündem, Avrupa'nın ekonomik büyümesinde sayısal ortamdaki "Güven ve Güvenlik" konusuna özel bir önem vermektedir. Bu çerçevede geliştirilen eylemler ile AB, 2020 yılına kadar, özellikle elektronik ortamda gerçekleştirilen iş ve işlemlerde kötü niyetli yazılımlar, siber saldırılar ve diğer tehlikeler karşısında kişisel verilerinin çalınması ve kötüye kullanılmasının önlenmesi konusunda veri koruma düzenlemelerini kişiler lehine güçlendirmeyi hedeflemektedir.[234] Avrupa, vatandaşların sisteme güvenlerinin tesis edilmemesi halinde, ekonomik büyümeye büyük katkı sağlayan BİT ve BİT'in sunduğu imkanlardan yararlanma oranının düşük kalacağının; ayrıca bu alanda yapılan yatırımların etkinlikten uzak olacağının bilinciyle veri koruma düzenlemelerini oldukça önemsemektedir.

Türkiye'nin veri koruma alanında bir düzenlemeye duyduğu gereksinim, AB entegrasyon süreci ve bilgi toplumu olma yolunda demokratik bir hak alanının teminine olan ihtiyaç ile daha belirgin bir hal almaktadır. Bu çerçevede, veri korumada ulusal ve özellikle uluslararası itibarın artırılması için Türkiye'nin kişisel verilerin korunması konusuna hızlıca eğilerek geç kalmış birtakım uygulamaları hayata geçirmesi büyük önemi haizdir.

Yukarıdaki bölümlerde, kişisel verilerin korunması ile ilgili olarak AB'nin ve diğer bazı uluslararası kurum ve kuruluşların yaklaşımları; ABD ve AB üyesi olan ve olmayan bazı ülkelerin uygulamaları ile Türkiye'deki mevcut durum ve çalışmalar

---

[232] Bkz. European Council. EUCO 13/10. Conclusions.17 June 2010. 15 Ağustos 2010. <http://ec.europa.eu/eu2020/pdf/115346.pdf>

[233] Bkz. <http://ec.europa.eu/information_society/digital-agenda/documents/digital-agenda-communication-en.pdf>

[234] Ayrıntılı bilgi için bkz. "Digital Agenda For Europe". <http://ec.europa.eu/information_society/digital-agenda/index_en.htm>

incelenmiştir. Çalışmanın bu son bölümünde ise, Türkiye'de kişisel verilerin korunması kanununa olan ihtiyaçtan hareketle bu kanunda yer alması gerektiği düşünülen temel özellikler ile Türkiye'de oluşturulacak kurumsal yapı için öneriler geliştirilmektedir.

6.1. Türkiye'de Kişisel Verilerin Korunmasına İlişkin Hukuki Düzenleme Önerileri

Veri koruma hukuku yatay bir düzenleme alanı olup, bu alandaki düzenlemelerin etkileri başta sağlık, sosyal güvenlik, bilişim, haberleşme ve araştırma ve geliştirme sektörlerinde hissedilmektedir. Karşılaştırmalı hukuk ile de yoğun bağlantıları olan bu alanın yeni gelişmelere ve dolayısıyla bu gelişmeleri karşılayacak düzenlemelere açık olması için Türkiye'deki veri koruma düzenlemelerinin diğer hukuk sistemleriyle çatışmayacak ve kendi içinde birbiriyle çelişmeyecek bir şekilde ele alınması gerekmektedir.

Bu çerçevede, bu çalışmanın "Uluslararası Alanda ve Karşılaştırmalı Hukukta Kişisel Verilerin Korunması" başlıklı üçüncü bölümünde öne çıkan bulgular ile bir örnek kanun olarak Polonya'da 29 Ağustos 1997 tarihinde çıkarılmış olan Kişisel Verilerin Korunması Kanunu birlikte değerlendirilerek; Türkiye'de çıkarılması beklenen KVKK'da aşağıda belirlenen hususların dikkate alınması önerilmektedir:

- Türkiye'de çıkarılacak KVKK Kanununda öncelikle kişilerin "kişisel verilerini koruma hakkı" olduğunun belirtilmesi önerilmektedir. Bu belirlemeden sonra ise başta "kişisel veri" olmak üzere, bu verilerin "işlenme"si "anonim hale getirilme"si, "veri öznesi", "veri kontrolörü" gibi kavramların karışıklığa mahal vermeyecek şekilde tanımlanması gerekmektedir.

- Kişisel verilerin ancak kanunla belirlenmiş sınırlar çerçevesinde ve kamu yararı, veri sahibinin yararı veya herhangi üçüncü bir şahsın yararına işlenebileceği vurgulanmalıdır.

- Kişisel verilerin korunması hakkı, herkese karşı ileri sürülebilecek bir hak olduğundan, koruma taleplerinin kamu kurum ve kuruluşları, meslek örgütleri, özel hukuk kişileri, tüzel kişiliği olmayan kuruluşlara karşı ileri sürülebileceği belirtilmelidir.

- Bu Kanun ile uygulamanın sağlanmasından ve bu kapsamda kişisel verilerin korunması ve vatandaşların haklarını korumada başta Kanuna uygunluk denetimi yapmak, kanunun ihlali halinde şikayetleri almak ve karara bağlamak, kamuya açık olarak veri dosyalama sistemleri sicili tutmak, ülkede kişisel veri koruma konusunda düzenlemeler yapmak ve bu konuda düzenlenen taslaklara görüş vermek, uluslararası alanda gerekli işbirliği ve koordinasyon çalışmalarını yürütmek üzere bağımsız ve özerk bir Kurum kurulması ile bu Kurumun, bağımsız statüsü, üyelerinin seçilme ve görevden alınma ile görev süreleri, kurumsal birimleri, personeli gibi unsurların Kanunda net bir şekilde belirlenmesi gerekmektedir.

- Kanunda veri işleme ilkeleri açıkça belirtilmelidir. Bu ilkeler genel hatlarıyla şöyle sıralanmalıdır:

i) Kişisel verinin silinmesi hali dışındaki işlemelerde veri öznesinin rızası alınmış olmalıdır. Ancak veri öznesinin hayati çıkarları söz konusu ise veriler kişinin rızası alınmaksızın da işlenebilir, bu durumda ilerleyen aşamalarda rıza tekrar alınmalıdır.

ii) İşleme, kanundan kaynaklanan bir hakkın kullanılması veya görevin yerine getirilmesi; ya da veri öznesinin taraf olduğu bir sözleşmenin ifası için; veya veri öznesinin bir sözleşmenin kurulmasından önce talebi halinde bazı işlemlerin yapılabilmesi için zorunlu olmalıdır.

iii) Veri işleme, veri öznesinin hak ve özgürlüklerine halel getirmeksizin, verilerin iletildiği alıcıların veya kişisel veri işlemenin amaçlarını ve yöntemini birlikte veya tek başına belirleyen kişi, organ, ajans veya kamu kurumu şeklindeki veri kontrolörlerinin meşru faaliyetlerinin ifası sırasında zorunlu olmalıdır. Böylece keyfi işlemelerin önüne geçilmelidir.

- Veri kontrolörünün doğrudan veri öznesinden kişisel veri topladığı durumlarda, özel bir kanun ile aksi belirtilmemişse, veri öznesini bu toplamayla ilgili aydınlatma yükümlülüğü bulunmalıdır. Bu yükümlülük çerçevesinde, veri kontrolörünün veri öznesine şu bilgileri vermesi gerekmektedir:

i) Kontrolörün kendisine ait yerleşim yeri adresi, şirket ise tam adı ve unvanı, gerçek kişi ise yine tam adı ve yerleşim yeri bilgileri,

ii) Veri toplamanın amacı, veri alıcıları toplama anında belirli ise alıcılar hakkındaki bilgileri,

iii) Veri öznesinin talebi halinde verilerine ulaşabilme hakkı ile bu verileri gerektiğinde güncelleme veya düzeltme haklarının bulunduğuna ilişkin bilgiyi.

- Kişisel verilerin doğrudan veri öznesinden alınmadığı durumlarda da veri kontrolörü, kişisel verilerin kaydedilmesinden itibaren derhal veri öznesini bilgilendirmek zorunda olmalıdır. Bu durumda da kontrolör, veri öznesine, verinin elde edildiği kaynak, kendisine ait yerleşim yeri bilgisi, tüzel kişiyse şirket adı ve unvanı, gerçek kişiyse tam adı ve adresi, veri işlemenin amacı ve kapsamı, veri öznesinin haklarının tamamını bildirmelidir. Bu zorunluluğun istisnası ancak kanunlarla düzenlenebilir. Ayrıca, kişisel verilere bilimsel, tarihi, akademik, istatistik veya kamu araştırması gibi sebeplerle ihtiyaç duyuluyorsa kişisel veri işlemenin kişi hak ve özgürlüklerini ihlal etmediği varsayımıyla söz konusu bilgilendirmenin yapılmasına gerek olmayabilecektir.

- Kanunda veri kontrolörünün diğer yükümlülükleri de yer almalıdır. Bu yükümlülükler başlıca; verilerin hukuka uygun olarak işlendiğini, bu verilerin belirlenmiş ve hukuka uygun amaçlarla toplandığını, bu verilerin toplandıkları amacın dışında kullanılmadığını, verilerin işleme amacıyla uygun ve yeterli olduğunu, verilerin işlendikleri amaç sona erdikten sonra kişilerin kimliklerini tespite izin vermeyecek şekilde tutulduğunu temin etmektir.

- Kanunda ayrıca birçoğu hassas veri niteliğinde olan ırk, etnik köken, siyasi düşünce, dini ve felsefi inanç, ticaret birliği üyeliği, sağlık, genetik kod, cinsel hayat, kişi hakkında verilen mahkeme kararları gibi verilerin işlenmesi belirli istisnalar dışında yasaklanmalıdır. Kişinin yazılı rıza verdiği, veri öznesinin veya üçüncü kişinin hayati çıkarlarının söz konusu olduğu veya o kişinin fiziksel olarak ya da hukuken rızasını belirtebilecek durumda olmadığı durumlarda kişinin veli ya da vasisinin izni alınıncaya kadar bu verilerin işlenmesi hali istisna olarak Kanunda sayılmalıdır.

- Kanuna istisna olarak eklenebilecek bir diğer husus ise kişisel veriler üzerinde devlet sırrı, milli savunma ve güvenlik, kişinin sağlığı veya hayati çıkarları, kamu düzeni, devletin temel ekonomik ve finansal faaliyetleri nedeniyle tasarrufta bulunulabileceğidir.

- Kanunda bulunması gereken en temel hususlardan biri de veri öznelerine ait hakların düzenlenmesi gereğidir. Kişisel verilerin korunması kapsamında bu kişilerin kanunla düzenlenmesi gereken belli başlı hakları şunlardır:

i) Veri öznesine bir dosyalama sisteminde bulunan kişisel verileri üzerinde kontrol hakkı ile gerçek/ tüzel kişi veri kontrolörünün tam adı, adresi, unvanı konusunda geniş bilgi alma hakkı,

ii) Kendisine ait kişisel verinin bulunduğu sistemde verilerin ne amaçla, hangi kapsamda ve hangi araçlarla, ne kadar süredir işlendiğine ilişkin bilgi alma hakkı,

iii) İşleme faaliyeti devlet sırrı, ticari veya mesleki sır kapsamında değilse veri kontrolöründen verilerin kaynağını öğrenme hakkı,

v) Verilerin hukuka aykırı olarak toplanmış olması, bu verilerin eksik, yanlış veya güncel olmaması durumlarında verilerin düzeltilmesi, güncellenmesi, geçici veya sürekli olarak silinmesini isteme hakları tanınmalıdır.

Söz konusu talepler karşısında veri öznesi ile veri kontrolörünün anlaşamamaları halinde veri koruma kurumuna başvurularak bu konuda uygun bir karar alınması beklenmelidir.

- Veri öznesinin talebi üzerine, yukarıda belirlenen haklar çerçevesindeki bilgilerin yazılı olarak belirlenecek süre içinde veri öznesine bildirilmesi gerekmektedir.

- Kanunda kişisel verilerin korunmasına ilişkin hükümler de bulunmalıdır. Buna göre, kişisel verilerin yetkisiz olarak açıklanması, kanuna aykırı olarak işlenmesi, kaybolması, tahrif edilmesi vb. risklere karşı veri kontrolörünün gerekli teknik ve kurumsal tedbirleri alması zorunlu olmalıdır. Yine veri kontrolörünün hangi verilerin ne zaman ve kim tarafından sisteme girildiğini, bu verilerin kimlere

transfer edildiğini, üzerinde ne tür işlemler yapıldığına ilişkin bilgileri sağlayacak teknik tedbirleri temin etmesi gerekmektedir. Bu amaçla, kontrolörün işlemeyi yapan yetkililere ait isim, yetkilendirme tarihinin başlangıcı ve sonu, verilerin bir bilgisayar aracılığıyla işlenmesi durumunda kimlik tespitine yarayan araçları belirleyen tam listeyi tutması gerekir.

- Kanunda belirtilmesi gereken bir diğer konu, veri kontrolörünün alacağı teknik tedbirlerin dışında, kişisel veri işleyen gerçek ve tüzel kişilerin hangi amaçla, ne tür verileri, ne yöntemle topladıkları ve ne şekilde işleyeceklerini, bu verileri kimlerle paylaşacaklarını belirtecekleri ve yetkili Kurumun tutacağı bir sicile kayıt olmaları gerekliliğidir. Şayet sicile kayıtlı olan bilgilerde bir değişiklik olursa, bunların sicile yeniden bildirilmesi kaydın değiştirilmesi/ yenilenmesi gerekecektir. Pek çok ülkede bu sicil, veri koruma otoritelerince ulusal düzeyde ve kamuya açık bir şekilde tutulmaktadır. Bu sicillerde, devlet savunması ve güvenliği, kamu düzeni, kişilerin hayatı ile ilgili olan dosyalama sistemlerinin kaydedilmesine gerek yoktur. Sicile kayıt için gerekli olan temel teknik ve kurumsal şartlar sağlanmıyorsa ya da veri işleme Kanuna aykırılık taşıyorsa Kurum kayıt talebini reddedebilir, bazı verilerin işlenmesini sınırlandırabilir veya halin icabına göre güncelliğini yitirmiş, hukuka aykırı olarak toplanmış, hukuka aykırı bir şekilde yurt dışına iletilmesi öngörülen veriler için diğer idari tedbirleri de alabilir.

- Çeşitli ekonomik, sosyal ve diğer uluslararası yükümlülükler çerçevesinde Türkiye'den üçüncü ülkelere kişisel veri iletilirken, VKD ile uyumlu olarak, iletilen ülkede de kişisel verileri koruyucu düzenlemelerin varlığı şartının aranması Kanuna dercedilmelidir. Uluslararası antlaşmalardan kaynaklanan yükümlülükler ile kanuni zorunluluk halleri ve ayrıca kanunda sayılacak olan hukuka uygunluk sebepleri (kişinin rızası, veri öznesinin hayati çıkarları vb.) gibi istisnalar dışında bu şart Kanunda öncelikle yer almalıdır.

- Kanunda yer alması gereken bir diğer önemli konu ise müeyyidelerdir. Bu müeyyideler, kişisel verilerin hukuka aykırı kullanımının etkisinin büyüklüğüne göre, idari para cezası ve hapis cezasını da mümkün kılan yargı müdahalesini harekete geçirecek araçlarla birlikte ele alınmalıdır. Bu çerçevede Türk Ceza Kanununun ilgili maddelerine atıflar yapılarak bütünlük sağlanmalıdır. Cezaların

miktarının tayininde ise kişi hak ve özgürlüğüne olan müdahale sonucunda elde edilen haksız menfaat ve hukuka aykırılığın niteliği dikkate alınarak caydırıcı nitelikte cezalara hükmedilmesi önem arz etmektedir. Bu Kanun kapsamında işlenen suçların başlıcaları; amacın gerçekleşmesine hizmet etmenin üstünde bir oranda kişisel veri depolama, verileri yetkisiz kişi veya kişilerle paylaşma veya erişime açık hale getirme, kasıtlı olarak veya ihmal ile verilerin güvenliğini tehlikeye atma, verilere zarar verme, Kurum nezdinde tutulan sicile kayıt yaptırmamış olma, aydınlatma yükümlülüğünü ihlal olarak sayılabilir. Her bir durumda suçun yarattığı ekonomik değer ve ihlalin büyüklüğüne, bu suçların işlenmesinde işleyenin teknik bilgi ve birikimine, yetki ve suçun manevi unsuru olarak kastın var olup olmadığına göre uygun cezalar verilmelidir.

- Akustik veya optik araçlarla, bireyin özel hayatını sürdürdüğü ev, ofis, taşıt gibi alanlar dışındaki kamuya veya belli bir gruba açık alanlarda değişik amaçlarla yapılan izleme işlemleri bilgilendirici uyaranlarla belirtilmelidir. Bu itibarla, Tasarıya kamuya açık alanların video ile gözetlemesinin ne tür hallerde yapılacağı, kayıtların hangi amaçla ve ne sürede tutulacağı ve hangi araçlarla kişilere bilgi verileceğine ilişkin olarak ek yapılması uygun olacaktır.[235]

6.2. Türkiye İçin Kurumsal Yapılanma Önerisi

Bu çalışmanın uluslararası alanda yapılan çalışmalar ve karşılaştırmalı hukukta kişisel verilerin korunması ile ilgili otoritelerin incelenmesi bahsinde görüldüğü gibi, veri koruma otoritelerinin düzenleme yapma, yargı benzeri faaliyet

---

[235] Alman Federal Kişisel Verilerin Korunması Kanunu'nun 6(b) maddesinde elektronik araçlarla izleme yapılmasına ilişkin aşağıdaki hükümler yer almaktadır:
"(1) Kamuya açık alanların izlenmesinin optik elektronik araçlarla (Video Gözetleme ile) yapılması ancak:
i) Kamusal kurumların görevlerini yerine getirmesi, ii)Konut dokunulmazlığının sağlanması için, iii)Somut olarak ortaya konulan amaçlar doğrultusunda ilgili kişinin hukuken korunan, daha ağır basan bir hakkı yok ise ve hukuken geçerli faydaları elde etmek için gerekli ise mümkündür.
(2) İzleme durumu ve sorumlu kuruluş uygun tedbirlerle fark edilir şekilde bildirilir.
(3) Birinci fıkraya göre alınan veriler ancak; güdülen amaç gerektiriyor ve ilgili kişilerin hukuken daha fazla korumaya değer bir hakkı olduğuna dair herhangi bir emare bulunmuyorsa işlenebilir veya kullanılabilir. Başka bir amaç için bu veriler ancak; devleti veya kamu güvenliğini bir tehlikeden korumak veya bir suç soruşturması veya kovuşturması gerektiriyorsa, işlenebilir veya kullanılabilir.
(4) Video izleme ile kaydedilmiş olan verinin belirli bir kişiye ait olduğu anlaşılabiliyorsa, bu verilerin yeniden işlenmesi veya kullanılması halinde Verilerin Korunması Kanununun 19(a) ve 33'üncü maddeleri gereğince bu kişiye haber verilir.
(5)Ulaşılmak istenen amaç artık gerektirmiyorsa veya ilgilinin korumaya değer daha üstün başka bir menfaati yoksa bu veriler derhal silinir." (TBD, 2008:78-79)

gösterme ve diğer görevlerini yerine getirmede bağımsız ve özerk olmaları gerekmektedir. Ülkemizde düzenleyici ve denetleyici otoriteleri bağımsız ve özerk olarak faaliyet gösteren kurumlar olarak göstermek mümkündür.

Türkiye'de kişisel verilerin korunması konusunda bağımsız bir otorite bulunmadığı hususu, 2005'ten itibaren 2009 yılına kadar geçen tüm Türkiye İlerleme Raporlarında AB tarafından eksiklik olarak gündeme getirilmiş olup, bu raporlar çalışmamızın beşinci bölümde ayrıntılı olarak incelenmiştir. Diğer yandan, Türkiye'nin ulusal politikaları da vatandaşların kişisel verileri üzerindeki kontrol ve hakimiyet alanını genişletici tedbirler ile bir kurumsal yapıyı gerektirmekteyse de bu konuda ülkemizde sonuca ilişkin bir gelişme olmamıştır. Bu çalışmada da, ülkemizde bir veri koruma kanununun bulunmamasının doğurduğu diğer sorunların yanı sıra, özellikle faili yurt dışında bulunan siber suçlarla mücadelede Türkiye'nin uluslararası işbirliği olanaklarının yetersiz kalışı ve vatandaşların teknolojik gelişmeler karşısındaki demokratik haklarının giderek daha fazla sınırlandırıldığına dikkat çekilmektedir.

Anılan gerekçeler ve diğer ülke örneklerinin incelenmesi sonucunda, bu çalışma ile Türkiye'de *bağımsız ve düzenleyici (regülatör) bir Kişisel Verileri Koruma Kurumu* oluşturulması önerilmektedir.

Bu doğrultuda, aşağıda yetkinin verildiği kişi ya da gruba göre, Türkiye için neden Ajans ya da Komiserlik değil de Kurum[236] modelinin önerildiği ve bu modelin neden düzenleme (regülasyon) yaklaşımı üzerine inşa edilmesi gerektiği hususunda bir değerlendirme yapılmaktadır.

6.2.1. Neden "Düzenleyici (Regülatör) Kurul" Olmalı

4.2. numaralı bölümde de belirtildiği gibi, Kuner kişisel verilerin korunması ile ilgili mevcut otoriteleri fonksiyonlarına göre ombudsman ve düzenleme (regülasyon) olmak üzere iki ana alanda incelemekteydi. Bu çalışma kapsamında

[236] Kurumsal yapılanma bölümü için Kurul ve Komisyon kelimeleri aynı anlamda kullanılmakta olup, bu kavramlar ile yetkinin birden fazla kişiye ait olduğu yapı anlaşılmalıdır. Kurum ise, Kurulun sekreterya dahil diğer alt birimlerinin de kapsandığı teşkilatın tamamı olarak algılanmalıdır.

Türkiye'de düzenleme yaklaşımının daha etkin olacağı değerlendirilmektedir. Türkiye'de bu yaklaşımı ön plana çıkaran sebepler şöyle sıralanabilir:

i) Düzenleme yaklaşımını benimsemiş olan ülkelerde, ilgili alanı düzenleyen kanunun ihlaline yönelik bir şikayetle karşılaşıldığında, ilgili düzenleyici merci sadece şikayet edenin durumunun düzeltilmesi yoluna gitmemekte, aynı zamanda geneli ilgilendiren önlemler almaktadır. Böylece hem benzer vak'alarda farklı nitelikte karar verilmesinin önüne geçilmekte, hem de uygulayıcılar ihlalin gerçekleşmesinden önce bu kararları dikkate almaktadırlar. Düzenleme modelinin ombudsmandan ayrılan bu yönü, Türk hukuk sistemindeki benzer vak'alarda içtihatların emsal oluşturmasına benzetilebilir.

ii) Yine düzenleme yaklaşımında, düzenleyici kurum kanuna uygun hareket edilmesini sağlayıcı önlemler almakla da görevlidir. Bu önlemler, uzun ve masraflı mahkeme süreçlerine nazaran oldukça kısa ve hızlı bir şekilde alınabilmektedir. Bu özelliğiyle de düzenleme yaklaşımının Türkiye'de henüz çok bilinmeyen veri koruma hukuku alanındaki uygulamaların netliğe kavuşturulmasında faydalı olacağı değerlendirilmektedir.

iii) Türk hukukunda ombudsmanlık sistemi zaman zaman tartışılmışsa da, bugüne kadar bu konuda bir tecrübe yaşanmamıştır. Bu nedenle özel uzmanlık gerektiren veri koruma alanında Türkiye'de ombudsmanlık tercihinin yapılmasının uygun olmayacağı değerlendirilmektedir. Ayrıca ombudsman modelini kabul etmiş olan ülkelerden Finlandiya ve Macaristan Türk hukuk sistemi bakımından farklı uygulamaları haiz, uzak ülkelerdir.

iv) Türkiye'de düzenleme modelinin benimsenmesinin uygun olacağına dair bir diğer gerekçe ise, diğer ülke incelemelerinden çıkan sonuçtur. Fransa ve Polonya'da düzenleyici veri koruma yaklaşımı benimsenmiştir. Fransa'nın kamu hukuku alanındaki pek çok düzenlemesinin Türk hukuk sisteminde mehaz nitelikte olması ve Türkiye'nin de Fransa gibi Kıta Avrupası Hukuk Sistemi içinde konumlanması nedeniyle, bu iki ülkenin hukuk sistemleri ve uygulamaları birbirine yakınsamaktadır. Ayrıca veri koruma alanında nispeten yeni bir sisteme sahip olması, AB'ye yeni üye ülkelerden biri olması ve gelişmişlik düzeyi yanında nüfus

ve nüfus yoğunluğu bakımından da Türkiye'ye benzemesi gibi sebeplerle Polonya ölçüt kabul edilebilecek diğer bir ülkedir.

v) Düzenleme yaklaşımını öne çıkaran bir diğer faktör ise bu yaklaşımın Türkiye'de telekomünikasyon, rekabet, radyo ve televizyon ve bankacılık gibi alanlarda yerleşik ve kabul edilmiş olmasıdır. Veri koruma alanında gerekli olan bağımsızlığın sağlanmasında benzeri bir yapının tesisi, gerek bu yapılara Türkiye'nin yabancı olmayışı, gerekse diğer ülke uygulamalarındaki standartların sağlanması bakımından uygun olacaktır.

Kurulacak olan yapının düzenleyici olması önerisinin değerlendirilmesinden sonra, yetkinin verildiği kişi ya da gruba göre, bu yapı için neden "Kurul" yapısının önerildiği konusunda değerlendirmelere geçilmesinde yarar görülmektedir.

Bu çalışmanın, 4.8. nolu başlığı altında incelenen ülke örneklerinde görüldüğü gibi, veri koruma kurumları yetkinin verildiği kişi ya da gruba göre Komiserlik, çok amaçlı Ajans ya da Komisyon (Kurul) şeklinde yapılandırılmaktadır. Kurul yapısında katılımcılık, uzlaşmacı karar alma, üyelerin görevlerinin sona ermesi veya üyeliğin boşalmasından bağımsız olarak kurumsal bilgi ve birikimin gelişmesi gibi bazı avantajlar bulunmaktadır. Türkiye'de mevcut kamu örgütlenmesi dikkate alındığında da Komisyon (Kurul) yapısının ön plana çıktığı görülür. İncelenen ülkelerden, kamu örgütlenmesi Türkiye'ye en çok benzeyen ülkenin Fransa olduğu ve bu ülkenin de düzenlemeden sorumlu bağımsız *Kurul* yapısını 1978 yılından bu yana başarılı bir şekilde yürütmekte olduğu dikkat çekmektedir. Yine Türkiye'de bağımsız olarak faaliyet gösteren otoritelere bakıldığında, bunların tamamında, karar alma yetkisinin birden fazla kişiye verildiği Kurul yapısı ile karşılaşılmaktadır. Yarı-yargısal mekanizma içindeki bu yapıların birden fazla disiplin veya altyapıdan gelen üyelerce desteklenmesinin, veri koruma gibi teknik ve hukuki konuları bünyesinde barındıran bir alan için uygun bir yapılanma modeli olacağı değerlendirilmektedir.

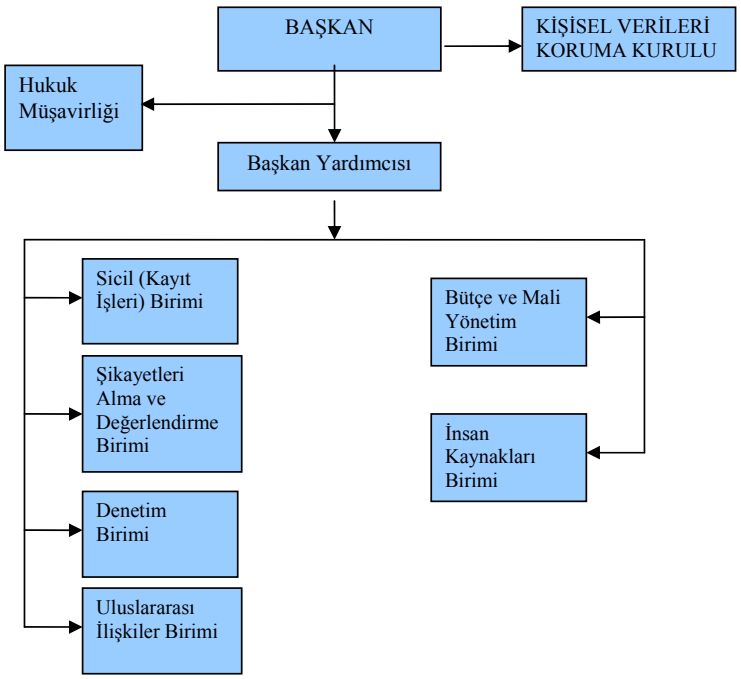
Bu sebeplerle, Türkiye'de düzenleyici Kurula sahip bir Kurum kurulmasının uygun olacağı düşünülmektedir.

6.2.2. Kurum İçin Önerilen Organizasyon Şeması ve Kurumun Görevleri

Kişisel Verileri Koruma Kurumu'nun, Türkiye'de yasanın uygulanmasında etkin olacak nitelikte yapılandırılması; ancak ihtiyacın ötesinde büyüklükte tasarlanmaması önerilmektedir. Bu çerçevede, aşağıda Kurum için önerilen organizasyon yapısının, Kurumun temel görevlerini yerine getirmede ve Türkiye'de veri koruma uygulamalarının etkinliğini gerçekleştirmede mümkün olduğunca yalın olmasına dikkat edilmiştir. Gelişen teknolojiler, uluslararası yeni yaklaşımlar ve diğer ihtiyaçlar karşısında kurumsal yapının geliştirilmesi mümkündür.

Kurumun, Kişisel Verileri Koruma Kurulu ile Kişisel Verileri Koruma Kurumu Başkanlığından oluşması ve Avusturya örneğindeki Veri Koruma Konseyi (Datenschutzrat) gibi Başbakanlıkla ilişkilendirilmesi uygun olacaktır.

Şekil 6.1. Türkiye için Önerilen Kişisel Verilerin Korunması Kurumu, Organizasyon Şeması



T.C. Anayasasının "İdare" başlıklı 123'üncü maddesinin 3'üncü fıkrasına göre, kamu tüzel kişiliğinin ancak kanunla veya kanunun açıkça verdiği yetkiye dayanılarak kurulması gerektiğinden, söz konusu Kurumun da kanunla kurulması, görev ve yetkilerinin kanunla belirlenmesi gerekmektedir. Kanunla kurulması önerilen Kurumun temel görevleri ise aşağıdaki gibi olmalıdır:

a) Vatandaşların kişisel verilerin ihlali konusundaki şikayetlerini almak ve karar vermek (idari para cezası vermek, durumun düzeltilmesi/iadesi, veriyi işleyeceklere verileri silme veya bloke etme talimatını vermek, veri işleme ile ilgili belirli veya geçici yasaklar koymak, veri kontrolörünü uyarmak),

b) Veri işleme operasyonlarının yasaya uygunluğunu re'sen denetlemek,

c) Veri işlemenin kişi hak ve özgürlükleri ile ilgili risk taşıdığı durumlarda veri kontrolörünün veya denetim görevlisinin bildirimi üzerine veri işleme süreç ve yöntemlerini belirlemek,

ç) Hükümete, meclise, özel ve kamu kurum ve kuruluşlarına veri koruma konularında danışmanlık hizmeti vermek,

d) Veri koruma alanında düzenleme yapmak ve ilgili kurumlarca yapılacak düzenlemelere görüş vermek,

e) Verilerin iletildiği alıcıların veya kişisel veri işlemenin amaçlarını ve yöntemini birlikte veya tek başına belirleyen kişi, organ, ajans veya kamu kurumu şeklindeki veri kontrolörlerine ve bu belirleme kapsamında doğrudan veri işlemeden sorumlu kişilere Kanun ve ilgili düzenlemeler konusunda eğitim vermek,

f) Veri işleyenler, adresleri, isimleri ve unvan bilgileri ile bu kişilerin topladıkları ve işledikleri kişisel verilerin niteliği, kapsamı, amacı ve işleme süresini belirten ve kamu tarafından erişilebilir olan sicili (kaydı) tutmak,

g) Her yıl kurum faaliyet raporunu kamuoyuna ilan etmek,

h) Veri koruma konusunda vatandaşları bilinçlendirici tedbirler almak,

ı) Veri koruma düzenlemelerinin uygulanmasında polis, mahkemeler ve diğer hukuk uygulayıcı mercilerle, aynı zamanda ilgili uluslararası kurum ve kuruluşlarla işbirliği yapmak.

6.2.3. Kurulun Yapısı ve Görevleri

Kurumun karar organlarını oluşturan üyelerin belirlenmesinde izlenecek yöntemin mümkün olduğunca siyasi etkiye kapalı olması gerekmektedir.[237] Ülkemizde de pek çok bağımsız düzenleyici Kurumun Kurul üyeleri, her boş üyelik için farklı kurum ve kuruluşların kendi içlerinden veya dışarıdan göstereceği ve kanunda belirlenen niteliklere uygun birden fazla aday arasından Bakanlar Kurulu veya Parlamento tarafından seçilir ve atanır.[238] Bu seçim usulunün katılımcılık ve bağımsızlık unsurunun gerçekleşmesinde güçlü bir yol olduğu düşünülmektedir.

Söz konusu gerekçeler ve diğer ülke incelemelerinden çıkan sonuca paralel olarak, Kurul üyelerinin görev ve yetkileri farklı olan çevrelerce aday gösterildikten sonra Bakanlar Kurulunca seçilmesi ve atanmasının uygun olacağı düşünülmektedir. Şekil şartları kanunla tanımlanacak olan bu hususun dışında önemli olan bir diğer konu, uygulamada da gerçekten bağımsızlığın sağlanabilmiş olmasıdır. Bu Kurum, siyasal güçlerin, farklı ekonomik çıkar gruplarının ve uluslararası kuruluşların baskı ve taleplerine karşı ne kadar dirençli olursa bağımsızlığı o kadar güçlü olacaktır. Aksi takdirde hukuki bağımsızlık ne kadar yüksek olursa olsun, gerçek bağımsızlıktan bahsetmek mümkün olmayacaktır.[239] Bu nedenle de, kişisel verilerin ve dolayısıyla kişi haklarının korunması ile bu verilerin kullanılmasının yaratacağı fayda arasında uygun dengenin gözetilmesi oldukça önemlidir.

Kurulun üye sayısının, diğer ülke örneklerinde de beş ile yedi kişi arasında değiştiği ve Türkiye'deki diğer kurullardaki üye sayısı da dikkate alındığında; nispeten farklı görüş sayısının daha fazla olduğu, ancak, oyların eşitliği durumunun söz konusu olmayacağı yedi üye olarak belirlenmesi önerilmektedir. Avusturya örneğinde olduğu gibi bu üyeliklere aday gösterme usulünün tek bir makam veya organ tarafından yapılmaması, üyelerin hukuk veya mühendislik alanlarında veri koruma ile ilgili uzmanlıklarının aranması ve en az bir üyenin de hakim olmasının takdir yetkisinin olaya uyarlanmasında pratik fayda sağlayacağı düşünülmektedir. Uzmanlık konusunda; ülkemizde bağımsız ve özerk Kurul üyelerinin seçim

[237] Şanlısoy ve Özcan, 2006:106
[238] Bu düzenleyici otoritelere Sermaye Piyasası Kurulu, Rekabet Kurulu ve Radyo ve Televizyon Üst Kurulu örnek gösterilebilir.
[239] Şanlısoy ve Özcan, 2006:129

kriterlerini belirleyen emsal Kanunlarda konuyla ilgili ayrıntılı niteliklerin belirlenmesi nedeniyle,[240] Tasarının üye seçimine ilişkin kriterlerinde de özel niteliklerin belirtilmesinde fayda görülmektedir. Bu konu ile ilgili olarak, sosyal bilimler alanında hukuk, siyasal bilgiler (bilimler), iktisadi ve idari bilimler, iktisat, işletme fakülteleri veya bölümlerinden; mühendislik alanında elektronik, elektrik-elektronik, elektronik ve haberleşme, endüstri, bilgisayar, telekomünikasyon ve işletme mühendisliği fakültelerinden veya bölümlerinden mezun olmak ya da belirtilen bölümlerden mezun olmamakla birlikte sayılan alanlarda yüksek lisans veya doktora yapmış olmak, öğretim kurumlarında en az on yıl öğretim üyeliği yapmış veya kamu hizmetinde en az on yıl fiilen çalışmış olmak, veri koruma hukuku ve/veya bilgi güvenliği alanlarında yeterli bilgi ve deneyime sahip olmak gibi hususlar Kanunda sayılmalıdır.

Kurul üyelerinin seçilmesinde şu alternatif önerilmektedir:

Kurulun, Bakanlar Kurulunca re'sen gösterilecek bir aday ile kalan üyelerin Danıştay ve Yargıtay üyeleri arasından gösterilecek ikişer adaydan birer, Türkiye Barolar Birliğinin göstereceği iki adaydan bir, Adalet Bakanlığının idari görevlerde çalışan birinci sınıfa ayrılmış hakim ve savcıları arasından göstereceği iki adaydan bir, Türkiye Bilimsel ve Teknolojik Araştırma Kurumunun Bilim Kurulu üyeleri arasından göstereceği iki adaydan bir ve Yükseköğretim Kurulunun kendi üyesi olmayan ve mühendislik alanlarında profesör veya doçent unvanına sahip öğretim üyeleri arasından göstereceği iki adaydan birinin Bakanlar Kurulu tarafından seçilmesi ve atanmasında fayda görülmektedir.

---

[240] 5809 sayılı Elektronik Haberleşme Kanunu'nun 67'inci maddesinin ilgili fıkrası: "Kurul üyeliklerine atanacakların; mühendislik alanında elektronik, elektrik-elektronik, elektronik ve haberleşme, endüstri, fizik, matematik, bilgisayar, telekomünikasyon ve işletme mühendisliği fakültelerinden veya bölümlerinden, sosyal bilimler alanında siyasal bilgiler (bilimler), iktisadi ve idarî bilimler, iktisat, hukuk, işletme fakülteleri veya bölümlerinden ya da fakültelerden fizikçi veya matematikçi unvanıyla veya sayılan fakülte ve bölümlere denkliği yetkili makamlarca kabul edilmiş yurt dışındaki yüksek öğretim kurumlarından mezun olmaları ya da belirtilen bölümlerden mezun olmamakla birlikte sayılan alanlarda yüksek lisans veya doktora yapmış olmaları, mesleki ve elektronik haberleşme alanında yeterli bilgi ve deneyime sahip, kamu veya özel sektörde en az on yıl çalışmış olmaları, 657 sayılı Kanunun 48 inci maddesinin (A) bendinin (1), (4), (5), (6) ve (7) numaralı alt bentlerinde belirtilen şartları taşımaları ve herhangi bir siyasi partinin yönetim ve denetim organlarında görev almamış veya bu görevlerinden ayrılmış olmaları gerekir."

Fransa'daki CNIL örneğinde olduğu gibi, Kurum Başkanı, hiçbir Bakan, kamu otoritesi, kamu veya özel şirket yöneticisi veya diğer otoritelerden emir veya talimat almaksızın Kurul üyeleri arasından seçilmelidir. Komisyon'un görev süresi ise parlamento üyelerinin seçim dönemine paralel olarak 5 yıl olarak düzenlenebilir. Üyelerin bir kez daha seçilmesi de yine CNIL örneğinde olduğu gibi mümkün olmalı ancak toplam görev süresi 10 yılı aşmamalıdır. Kurum Başkanı aynı zamanda Kurula da Başkanlık etmelidir. Kurum Başkanının önerisiyle Kurulun üyeleri arasından Kurum İkinci Başkanı da seçilerek izin, hastalık, yurt içi ve yurt dışı görevlendirme, görevden alınma ve görevde bulunmadığı diğer hallerde Başkan'a vekalet etmelidir.

Yukarıda ifade edilen yapıda tasarlanması önerilen Kurulun görevleri ise aşağıdaki gibi olmalıdır:

a) Kişisel Veri Koruma Kanununun uygulanması açısından veri işleme operasyonlarının hukuka uygun olarak gerçekleştirilmesi şartlarını düzenlemek ve denetlemek,

b) Kişilik hakları ihlal edilenlerin şikayetleri hakkında karar vermek,

c) İlgili kişi bakımından telafisi güç veya imkansız bir zararın doğması ihtimalinin bulunması halinde geçici önlemler almak,

d) Kişisel verilerin işlenmesine ilişkin konularda düzenleyici işlemler tesis etmek, bu konuda hazırlanan düzenleme taslaklarına görüş vermek,

e) Kişisel veriler ve bu verilerin korunması konusunda vatandaşları bilinçlendirici faaliyetler yürütmek,

f) Yabancı ülkelere veri aktarımı konusunda tereddüt bulunması halinde karar vermek,

g) Başkanın sunduğu önerileri karara bağlamak,

h) TBMM Başkanlığına Kurul faaliyetleri hakkında yıllık rapor sunmak,

ı) Kurumun yıllık çalışma raporu ve programı ile denetim raporunu onaylamak,

i) Kurumun yıllık hesapları ile yıllık bütçe teklifini onaylamak,

j) Kanunlarda verilen diğer görevleri yerine getirmek.

6.2.4. Kurumun Hizmet Birimleri İçin Önerilen Görevler

Kurum Birimleri kendi içinde ana ve yardımcı hizmet birimleri olmak üzere iki gruba ayrılabilir. Ana hizmet birimleri ve bu birimlerin genel olarak üstleneceği görevlerin aşağıdaki şekilde olması önerilmektedir:

Sicil (Kayıt İşleri) Birimi: Kişisel veri işleyen gerçek ve tüzel kişilerin bu verileri hangi kapsamda ve ne tür yöntemlerle işlediklerine ilişkin ayrıntıları içeren ve kamuya açık olarak tutulacak olan Sicile kayıt başvurularını incelemek ve kayıtları tutmak.

Denetim Birimi: Sicile kayıtlı olmayan veya Kanuna aykırı veri işleyenleri şikayet üzerine veya re'sen yapılacak denetim üzerine tespit etmek, Kanunun uygulanması ile ilgili hukuka aykırılıkları tespit etmek ve Kurula raporlamak.

Şikayetleri Alma ve Değerlendirme Birimi: Kanunun uygulanmasına ilişkin şikayetleri almak, bunları değerlendirmek ve hazırlayacağı raporu karar verilmek üzere Kurula sunmak.

Uluslararası İlişkiler Birimi: Kişisel verilerin korunması ile ilgili uluslararası girişim ve inisiyatiflere katılmak, yurt dışına aktarılacak verilerle ilgili rapor hazırlayarak karar verilmek üzere Kurula sunmak ve uluslararası kurum ve kuruluşlarla işbirliği içinde araştırma ve teknik yardım projeleri hazırlamak.

Hukuk Müşavirliği (Danışma Birimi): Kurum birimleri ve bakanlıklar tarafından gönderilen kanun, tüzük ve yönetmelik tasarıları ile diğer hukuki konular hakkında görüş bildirmek, Başkanlığın menfaatlerini koruyucu, anlaşmazlıkları önleyici hukuki tedbirleri almak, anlaşma ve sözleşmelerin bu esaslara uygun olarak yapılmasına yardımcı olmak, Başkanlığı taraf olduğu davalarda temsil etmek.

Yardımcı hizmet birimleri: Kurumun bütçesinin hazırlanması, ihtiyaç duyulan her türlü yapım, satın alma, kiralama, bakım ve onarım, arşiv, sağlık ve benzeri idari ve mali hizmetler ile Başkanlığın insan gücü politikası ve planlaması, personelin atama, nakil, emeklilik vb. özlük işlemlerini yürütmek, eğitim planını

hazırlamak, uygulamak ve değerlendirmek gibi yardımcı hizmetlerinin "Bütçe ve Mali İşler" ve "İnsan Kaynakları" Birimlerince yerine getirilmesi önerilmektedir.

6.2.5. Kurumun bağımsızlığı

Gerçek anlamda bir kurumsal yapının bağımsızlığı, bağımsızlığı sağlayacak unsurların[241] kanun ile garanti altına alınması ile mümkündür. Bu unsurlardan, özellikle idari ve mali özerkliğin bulunduğunun kanunda ifade edilmesi, o otoritenin bağımsızlığının sağlanmasında önemli bir husustur. Uluslararası alanda veri koruma otoritelerinin bağımsız olması gerektiğine ilişkin yaklaşımlar ve diğer ülke örneklerinin incelenmesinden çıkan sonuç da bu yöndedir. Bu otoritelerin kamu kurum ve kuruluşlarının veri koruma uygulamalarını incelemeleri, yargı benzeri karar vermeleri nedeniyle bağımsız olmaları gerekmektedir. Bu itibarla, Kanuna, *Kurumun kamu tüzel kişiliğine, idari ve mali özerkliğe sahip olduğu ile, Kurumun görevlerini yerine getirirken bağımsız olduğu ve hiçbir organ, makam, merci veya kişinin Kuruma emir ve talimat veremeyeceği* hususlarının dercedilmesi gerektiği değerlendirilmektedir.

Bir veri koruma otoritesinin bağımsızlığı sorun çözümünde tek başına yeterli olmayacaktır. Söz konusu otoritenin doğru çalışabilmesi için yeterli ve uygun nitelikte insan kaynağı ile beslenmesi ve aynı zamanda Kanunun ne şekilde uygulanacağı konusunda stratejisinin olması gerekmektedir.

6.2.6. Kurum personeli

Kanunlarla Kuruma verilen görevlerin gerektirdiği asli ve sürekli görev ve hizmetlerin, uzman ve uzman yardımcılarından oluşan meslek personeli ve diğer personelden oluşan kişilerce yerine getirilmesi ve Kurumun gerektiğinde sözleşmeli

---

[241] Kurumsal bağımsızlığı sağlayacak unsurlar, 4.3.1 numaralı "Bağımsızlık ve özerklik" bahsinde incelenmiştir. Burada; ö*zerklik,* bir kurumun görevlerini yerine getirirken hiçbir organ, makam, merci veya kişiden emir, talimat veya izin almaması iken; *bağımsızlık* ise hükümete, düzenlenen ve denetlenen sektöre, medyaya, diğer kamu idarelerine ve diğer gerçek ve tüzel kişilere karşı özerkliği; diğer yandan kurul üyelerinin düşünce ve kanaatlerini serbestçe dile getirip oylarını özgürce kullanabilmeleri anlamına gelmektedir. Bu özerkliğin sağlanarak bağımsızlığın elde edilebilmesinin en önemli şartı, diğer kurum ve kişilerden her tür emir-talimat gibi etkileri bertaraf edecek bağımsız bir bütçesinin olması gerekliliğidir.

uzman personel çalıştırabilecek şekilde yapılandırılması önerilmektedir. Kurulun memurlarının ve sözleşme ile çalıştırılacak personelinin kadro ve ücretlerine ilişkin esasları, Kurulun önerisi üzerine Bakanlar Kurulunca tespit edilebilir.

Kişisel verilerin korunması kanunu ve ilgili düzenleme hükümlerinin uygulanmasının ve her türlü kişisel veri işleme faaliyetlerinin denetimi Kurum uzman ve uzman yardımcıları tarafından yapılmalıdır. Denetimlerde Kurumca görevlendirilen uzman ve uzman yardımcıları, veri işleyen gerçek ve tüzel kişilerden veri işlemeye ilişkin yöntem, amaç, kullanım usulleri, verilerin tutulduğu ortam, saklama süresi gibi konularda bilgi istemeye, bunların tüm defter, kayıt ve belgelerini ve diğer bilgi ihtiva eden vasıtalarını incelemeye ve bunların örneklerini almaya, işleme şekillerini denetlemeye, ilgililerden yazılı ve sözlü bilgi almaya, gerekli tutanakları düzenlemeye yetkili olmalı, incelemeye giderken yanlarında incelemenin konusunu, amacını ve yanlış bilgi verilmesi halinde idari para cezası uygulanacağını gösteren bir yetki belgesi bulundurmalıdır. Bunun karşısında ilgililer de istenilen bilgi, belge, defter ve diğer vasıtaların örneklerini vermek, yazılı ve sözlü bilgi vermek ve tutanakları imzalamakla yükümlü olmalıdır. Yerinde incelemenin engellenmesi veya engellenme olasılığının bulunması durumunda, sulh ceza hakimi kararı ile yerinde inceleme yapılması sağlanmalıdır.

Kurum Başkan ve personeli ile Kurul üyeleri çalışmaları ve denetlemeleri sırasında ilgililere ve üçüncü kişilere ait öğrendikleri sırları, bu konuda kanunen yetkili kılınan mercilerden başkasına açıklayamamalı ve bu bilgileri kendi yararlarına kullanamamalıdır. Bu yükümlülük görevin sona ermesi halinde de devam etmelidir.

Kurumda uzman yardımcılığına atanabilme şartları Türkiye'de bilinen diğer bağımsız kurumlardaki atanma usul ve esaslarına göre yapılmalıdır. Uzmanlığa atanma koşulları da, paralel bir şekilde, Kurum içinde belirlenecek sözlü ve/veya yazılı mesleki yeterlilik şartlarına bağlı olarak çıkarılacak mevzuat hükümlerine göre yapılmalıdır.

Kurum personel sayısının ilk etapta düşük tutulması ve Avustralya örneğinde olduğu gibi ihtiyaca binaen çoğaltılmasına imkan sağlanmalıdır.

6.2.7. Kurumun bütçesi

Türkiye'de mali özerkliği haiz bağımsız düzenleyici kurum bütçeleri genel ve özel bütçeden farklı olarak, 5018 sayılı Kamu Mali Yönetimi ve Kontrol Kanununun belirli maddeleri ile bağlıdırlar. 5018 sayılı Kanunun 17'nci maddesine göre bu bütçeler, üç yıllık bütçeleme anlayışı ile, stratejik plan ve performans hedefleri ile kurumsal, işlevsel ve ekonomik sınıflandırma sistemine göre hazırlandıktan sonra doğrudan TBMM'ye sunulmaktadır. Bu sürece genel ve özel, mahalli idareler ve sosyal güvenlik kurumları bütçelerinden farklı olarak Bakanlar Kurulu dahil olmamaktadır. Bağımsız düzenleyici kurum bütçeleri, "Merkezi Yönetim Bütçe Kanunu"nda yer almakta olup, bunların uygulama sonuçları "Kesin Hesap Kanunu" ile yine TBMM tarafından onaylanmaktadır. Bununla birlikte, bu kurumlarda iç denetim birimleri bulunmamakta olup, dış denetimleri ise Sayıştay tarafından yerine getirilmekte ve her üç ayda bir belirlenen gelir fazlaları ise genel bütçeye aktarılmaktadır.

Bir örneği, Fransız Veri Koruma Otoritesi olan CNIL'de görüldüğü gibi, Türkiye'deki Veri Korumu Kurumunun da yukarıda ifade edilen mali özerklik esaslarına bağlanması gerektiği düşünülmektedir. Kurulacak olan Kurumun hesapları bu çerçevede Sayıştay tarafından denetlenmeli ve mali özerklik esasına bağlı olarak Kurumun bütün giderleri kendi gelirlerinden karşılanmalıdır.

6.2.8. Kurumun gelirleri

Kurumun gelirlerinin şu kalemlerden oluşması önerilmektedir: Kurum tarafından uygulanacak idari para cezaları, yayın gelirleri, Kuruma ait taşınır ve taşınmaz mallardan elde edilen gelirler, müşavirlik hizmetlerinden elde edilecek gelirler, kurs, toplantı, seminer ve eğitim faaliyetlerinden sağlanacak gelirler, genel bütçeden gerektiğinde yapılacak yardımlar, her türlü bağış, yardım ve diğer gelirler ile bu gelirlerin nemalandırılması suretiyle elde edilecek gelirler.

Kurum gelirleri 5018 sayılı Kamu Mali Yönetimi ve Kontrol Kanununun üçüncü maddesinin birinci fıkrasının (c) bendinde belirtilen cetvel için öngörülen usul ve esaslara göre hazırlanmalı ve kabul edilmelidir.

6.2.9. Kurum kararları ve cezalar

Kanunun ihlali halinde, re'sen veya şikayet üzerine Kurum; i) idari para cezası ii) kişisel verilerin tamamlanması, güncellenmesi, düzeltilmesi, açıklanması veya açıklanmaması, iii) toplanan bu verilerin iletimi veya korunması için ek tedbirler alınmasını isteme, iv) verinin üçüncü ülkeye transferini bekletme, durdurma veya erteleme, v) kişisel verileri silme kararları alabilmelidir.

Kurumun vereceği idari para cezalarının miktarı belirlenirken bu cezaların hakları koruma özelliğinin yanı sıra caydırıcı nitelikte olmasına özen gösterilmelidir. Hukuka aykırı veri işleme operasyonlarının, önemli ve geri döndürülemez nitelikte zararlar doğurma potansiyeli dikkate alınarak bu hususa özellikle dikkat edilmelidir. Bu çerçevede, bir örnek olarak, tüzel kişilere verilecek para cezalarında, bu tüzel kişilerin karardan bir önceki mali yıl sonunda oluşan veya bunun hesaplanması mümkün olmazsa karar tarihine en yakın mali yıl sonunda oluşan ve Kurul tarafından saptanacak olan yıllık gayri safi gelirinin binde biri ile beşi arasında değişen oranda idari para cezası verilmesi; ancak bu esasa göre tespit edilecek cezaların her halde belirli bir miktardan (örneğin onbin Türk Lirasından) az olmaması hükme bağlanabilir. Ayrıca, tespit edilecek ceza miktarı ne olursa olsun, Kurumun vereceği idari para cezalarında 30/3/2005 tarihli ve 5326 sayılı Kabahatler Kanununun 17'nci maddesinin ikinci fıkrası bağlamında, işlenen kabahatin haksızlık içeriği ile failin kusuru ve ekonomik durumu ile ihlalin tekerrürü, süresi, işletmenin piyasadaki gücü, ihlalin gerçekleşmesindeki belirleyici etkisi, verilen taahhütlere uyup uymaması, incelemeye yardımcı olup olmaması, gerçekleşen veya gerçekleşmesi muhtemel zararın ağırlığı gibi hususlar dikkate alınmalıdır.

Kişisel Verilerin Korunması Kanunu ve 5326 sayılı Kabahatler Kanunu kapsamında Kurumun vereceği idari para cezalarının yanı sıra, 5237 sayılı Türk Ceza Kanununun "Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar"ı düzenleyen bölümündeki kişisel verilerin kaydedilmesi (md. 135), verileri hukuka aykırı olarak verme veya ele geçirme (md. 136), bunların nitelikli halleri (md. 137) ve verileri yok etmeme suçlarının (md.138) işlenmesi üzerine savcılık ve ceza mahkemeleri aracılığıyla suçun soruşturma ve kovuşturma hükümlerinin saklı olduğu Kanunda da belirtilmeli, böylece iki Kanun arasındaki ilişki sağlanmalıdır. Söz konusu maddelere

dayalı olarak yürütülecek soruşturma ve kovuşturma evrelerinden sonra suçun sabit olması durumunda, suçun nitelikli hallerinde cezanın yarı oranında artırılması da mümkün olmak üzere, altı aydan dört yıla kadar hapis cezası verilebilecektir.[242] Bu çerçevede, 5326 sayılı Kanunun 23'üncü maddesi uyarınca, bir suç dolayısıyla başlatılan soruşturma kapsamında bir kabahatin işlendiğini öğrenmesi halinde Cumhuriyet savcısı, durumu ilgili kamu kurum ve kuruluşuna (Kuruma) bildirebileceği gibi, kendisi de idari yaptırım kararı verebilir. Ancak, bunun için ilgili kamu kurum ve kuruluşu tarafından idari yaptırım kararı verilmemiş olması gerekmektedir. Herhangi bir olayda, suç işlendiğine ilişkin Kurumun bir kanaati hasıl olduğunda ise, Kurum adli ve idari kolluk makamları ile işbirliği içinde hareket edecektir.

Kurumun Kanunun uygulanmasına ilişkin vereceği kararlar Anayasa'nın 125'inci maddesi gereğince yargısal denetime tabi olmalıdır. Bu konuda Danıştay'a ilk derece mahkemesi olarak görev verilmelidir.

6.3. Tasarının Kurumsal Yapısı Hakkında Bazı Değerlendirmeler

Yukarıda, kişisel verilerin korunması ile ilgili Türkiye için hukuki düzenleme ve kurumsal yapılanma konuları ayrıntılı olarak ele alınmış, bu konularda çeşitli öneriler geliştirilmiştir. Söz konusu inceleme ve öneriler saklı kalmak üzere, aşağıda Tasarı ile ilgili önemli olduğu düşünülen çeşitli alanlarda bazı değerlendirmeler yapılmaktadır.

Türkiye'de mevcut KVKK Tasarısı ile oluşturulması öngörülen Kişisel Verileri Koruma Kurulu'nun üyelerinin Bakanlar Kurulunca seçilmesi ve bu Kurulun Başbakanlık bünyesinde bağımsız olarak faaliyetlerini gerçekleştirmesi planlanmaktadır. Kurulun sekreterya hizmetlerini de Başbakanlık yürütecektir.

Sözü edilen yapı çerçevesinde, Tasarının 26'ncı maddesinde Kurulun yetkilerini bağımsız olarak kullanacağı, hiçbir organ, makam, merci ve kişiden Kurul kararlarını etkileyecek emir ve talimat alamayacağı ifade edilmektedir. Ancak bu

[242] Bu çalışmanın yapıldığı dönemde Türk Ceza Kanunun söz konusu maddeleri yürürlükte olmasına rağmen, uygulamada kişisel veri kavramının çerçevesinin belirli olmaması sebebiyle, etkin kararlar alınamamaktadır. Kişisel Verilerin Korunması Kanununun yasalaşması halinde bu sorun çözülmüş olacaktır.

madde lafzi ile vurgu yapılan bağımsızlık, sadece ilgili kanunda o otoritenin yetkilerini bağımsız olarak kullanacağının belirtilmesi ile sağlanamayacak, idari ve mali özerklik ile desteklendiğinde anlam kazanacak bir özelliktir. Başka bir kamu kurum veya kuruluşunun bütçesinden pay alan ve sekreteryası o kurum veya kuruluş tarafından yapılacak olan bir Kurumun, *Kanununda bağımsız olduğu açıkça belirtilse dahi,* uygulamada bağımsız hareket edip etmediğinin tartışma yaratacağı düşünülmektedir. Zira, konuyla ilgili VKD ve 181 sayılı Avrupa Konseyi Sözleşmesinde vurgulandığı üzere, veri koruma otoritelerinin tam bağımsız olmaları gerekmektedir. Bu nedenle, Kurul üyelerinin tamamının Bakanlar Kurulunca seçimi Kurulun idareye karşı bağımsızlığını zedeleyecek bir yaklaşım olup, bunun yerine, ilgili kurum ve kuruluşların katılımını sağlayacak, daha katılımcı ve çoğulcu bir seçim usulünün belirlenmesi gerektiği değerlendirilmektedir. Benzer bir örnekle, Türkiye'de 2001 yılından bu yana Başbakanlık bünyesinde faaliyet gösteren ve kişisel verilerin korunması ile ilgili kurumlarda olduğu gibi Paris İlkelerine[243] uyumu gözetmek durumunda olan Başbakanlık İnsan Hakları Başkanlığı'nın mevcut haliyle bağımsız olmadığı her fırsatta AB tarafından dile getirilmektedir.[244]

Yine Tasarının 27 ve 28'inci maddelerine göre Bakanlar Kurulu Veri Koruma Kurulunun üyelerini seçecektir. Yürütmenin başındaki Başbakanın altında bulunan ve yürütme fonksiyonunun yerine getirilmesini sağlamakla görevli olan *Bakanlar Kurulu'nun Kurul'un Başkanını ve tüm üyelerini seçecek olması,* bu yapının bağımsızlık ve özerkliğini tartışmalı hale getiren diğer bir unsurdur. Tasarı ile yapılan bu tercih, yürütme lehine ağırlık oluşturduğundan, Kurulun insan hak ve özgürlükleri ile insan onurunun korunması noktasında devlet menfaatlerini vatandaşın menfaatinin önünde görecek bir yapının oluşmasına zemin hazırlayabilir.

---

[243] İnsan hakları ile ilgili ulusal kurumların yükümlülüklerinin beş başlık altında ele alındığı Paris İlkeler'i kısaca hatırlanacak olursa, bu kurumların görev alanlarıyla ilgili insan hakları ihlallerini izlemeleri, konuyla ilgili düzenleme yapıldığında veya uluslararası insan hakları ile ilgili konularda Hükümeti, meclisi ve yetkili makamları bilgilendirme ve danışmanlık yapmaları, ilgili ulusal ve uluslararası organizasyonlarla temas içinde olmaları, vatandaşları bilgilendirme ve eğitim vermeleri ve yargı benzeri karar alma ehliyeti (quasi-judicial competence) ile donatılmaları gerekmektedir.

[244] Bu konuda AB'nin 2009 yılı Türkiye İlerleme Raporu'nun "2.2 İnsan Hakları ve Azınlıkların Korunması" bölümünde Türkiye'de kaynakların, bağımsızlığın ve kamu bilincinin eksikliğinin insan hakları kurumlarının düzgün işleyişini engellediği ve kurumsal çerçeve bağlamında bağımsız bir insan hakları kurumunun güçlendirilmesi için çaba gösterilmesine ihtiyaç bulunduğu ifade edilmektedir.

Tasarının 30'uncu maddesinde Kurulun çalışma esasları, 31'inci maddesinde ise Kurulun görev ve yetkileri düzenlenmektedir. 30'uncu maddede, Kurulun sekreteryasını Başbakanlığın yapacağı ifade edilirken, 31'inci maddede Kurula genellikle uluslararası yaklaşımlara uygun geniş yelpazede görevler verilmektedir. Bu iki madde birlikte değerlendirildiğinde öncelikle, bu Kurulun şikayetleri incelemek, sicil tutmak, yurtiçi ve yurtdışında verileri koruma makamları ile işbirliği yapmak, düzenleyici ve uluslararası örneklerdeki yapılara uygun olarak eğitici faaliyetlerin de eklenmesi halinde, bu görevlerin özel uzmanlık gerektirdiği açıktır. Bu türlü özel görevleri olan bir Kurulun sekreterya hizmetinin başka bir kamu kurumu tarafından verilmesinin etkin olmayacağı ve bu yaklaşımın kısa vadeli olacağı, kurumsal bilgi ve birikim sağlama açısından yetersiz kalacağı, hatta veri koruma faaliyetinin yanlış anlamalara sebep olarak özel sektörde ve kamu kurumlarında yanlış uygulamalara meydan verebileceği düşünülmektedir. Ayrıca, bu çalışmada da ele alındığı üzere, mevcut bir kuruma veri korumaya ilişkin görevler veren ancak özel uzmanlık gerektiren veri korumada başarısız olan Romanya'yı sonradan yeni bir veri koruma kurumu ihdasına götüren süreç de örnek alınarak bir karar verilmelidir. Sonradan telafisi mümkün olmayan zararlara ve zaman kaybına uğramamak için bu kurumsal yapının en başından uluslararası norm ve standartlara uygun olarak tasarlanmasında fayda görülmektedir.

Özetle, sekreteryası başka bir kamu kurum veya kuruluşu tarafından yürütülen bir Kurulun bağımsızlığından söz etmek mümkün olmayacağı gibi böyle bir yapının insan kaynağı ve lojistik anlamda da yetersiz olacağı değerlendirilmektedir. Bu nedenlerle, yargı benzeri fonksiyonları olan, şikayetleri karara bağlayan, özel sektörün de içinde bulunduğu bir alanda, yerinde denetim yapması da beklenen bir Kurulun (Tasarı md. 33/5) başka bir kuruma bağımlı olarak konumlandırılması uygun olarak değerlendirilmemektedir. Söz konusu görevlerin ifası özel uzmanlık gerektirmektedir. Tek başına, veri işleyenlerin hangi çerçevede veri işlediklerine ilişkin kayıtların (Sicil) tutulması ve yönetimi özel zaman ve emek gerektirdiğinden bu görevlerin Başbakanlığın sekreteryası ile yürütülmesi mümkün olmayacaktır.

Kurul üyeliğine seçileceklerin nitelikleri için Tasarının 27'nci maddesinin ikinci fıkrasında belirtilen, üyelerin yükseköğrenim görmüş ve öğretim kurumlarında en az on yıl öğretim üyeliği yapmış veya özel veya kamu hizmetinde en az on yıl fiilen çalışmış olmaları şartları, bu Kurulun etkin olarak çalışmasında asgari şartları yerine getirme bakımından yeterli bulunmamakta; üyelerde, bu çalışmanın 6.2. başlıklı Türkiye İçin Kurumsal Yapılanma Önerisi bölümünde örneklendirilen niteliklerin aranması gerektiği değerlendirilmektedir.

SONUÇ

Günlük hayatta karşılaştığımız özel hukuka tabi bir çok iş ve işlem ile çevrimiçi hizmetlerin görüldüğü e-devlet uygulamalarıyla gündeme gelen kişisel veri ve mahremiyet kavramları, bazı *idari*, *yasal* ve *teknik* tedbirler ile korunmayı gerektirmektedir. Bu tedbirlerin, çevrimiçi hizmetlerin sunulmasından önce tasarlanması ve uygulanması, e-devlet hizmetlerinin sunumunda en ideal ve yerinde olanıdır.[245]

Kişisel verilerin korunması konusu dünyada 70'li yıllardan bu yana ciddi önlemlerin alındığı bir konu olmasına rağmen, ülkemizde bu konudaki tedbir ve çalışmalar oldukça sınırlı düzeyde kalmış, gelişen teknoloji ve uygulamalarla paralel bir gelişim gösterememiştir. Bu verileri koruyucu tedbirlerin alınması, içinde bulunduğumuz AB üyelik sürecinde de oldukça kritik önemi haiz olmakla birlikte, bu konuda atılması gereken adımlar salt AB'ye giriş için teknik bir şart olarak değil, ülkenin diğer uluslararası ilişkileri ile vatandaşların demokratik hakları bağlamında ihtiyaç olarak algılanmalıdır. Ancak bu şekilde gerçek bir veri koruma felsefesi ve uygulaması geliştirilebilecektir. Yalnız bırakılma hakkı olarak da ifade edilen mahremiyet hakkı ve bu hak kapsamındaki özel hayatın gizliliği kavramlarının çerçevesi, artık tüm dünyada kişinin kendisi ile ilgili bilgileri *kontrol etme* ve bu bilgilerin kullanılmasına *katılma hakkını* içerecek şekilde genişlemiştir. AİHS (md. 8), OECD'nin Rehber İlkeleri, Avrupa Konseyinin 108 sayılı Sözleşmesi ve 181 sayılı ek Protokolü ile VKD çerçevesinde şekillenen kişisel verilerin korunması kavramı, Türkiye'de henüz net bir hukuksal çerçeveye kavuşmamıştır. Çevrimiçi ortamda sınır ötesi veri transferlerinin de yaygınlaşması nedeniyle bu çerçeve, ülkemizde de tüm ilke ve kurumlarıyla uluslararası ölçütlere uygun şekilde kurgulanarak geliştirilmesi gereken bir hukuk disiplinidir.

Mahremiyet kavramının ülkemizde bir "hak" olarak yerleşik olmamasının ve bu doğrultuda kişinin kendisine ait verileri üzerinde tasarruf taleplerinin amaç ve kapsamının doğru anlaşılamamasının, bu çalışmanın hazırlandığı dönemde TBMM Adalet Komisyonunda bulunan KVKK Tasarısının da doğru yorumlanmasını ve

[245] OECD. "The e-Government Imperative: Main Findings". 2003.

yasalaşmasını engellediği değerlendirilmektedir. Genel olarak gelişen teknolojiler ve bu kapsamda otomatik veri işleme tekniklerinin kazandığı ivme karşısında, hukukun aynı sürat ile cevap veremeyişi doğal karşılanabilirse de, ülkemizdeki uygulamalar bu dengesizliği oldukça artırmıştır. Kamusal alanda, özellikle maliyeti yüksek e-devlet projeleri, kişisel verilerin korunması mevzuatının bulunmaması nedeniyle sadece teknolojik çerçevede geliştirilmektedir. Ancak bu hizmetlerin güvenilirliğine olan inanç ve beklentilerin bir mevzuatla sağlanamaması, bu hizmetlere olan talebin sınırlı düzeyde kalmasına neden olmakta, bu da söz konusu projelerin etkinliğini azaltmaktadır. Ya da pek çok proje, anılan nedenle ilerleyememektedir. Mahremiyetin "hak ve özgürlük" olarak ele alınması, bu veriler üzerindeki her tür aktif veya pasif müdahalenin, kaynağının açıkça kanuna dayanan yetki, zorunluluk veya gereklilik ile mümkün olabilmesini gerektirir. Bir kanun ile çerçevesi belirlenecek mahremiyet hakkı ile kişisel verilerin gelişigüzel toplanarak denetimsiz bir şekilde açıklanması ve yetkisiz kişilerce kötüye kullanılması karşısında kişilere söz hakkı tanınması; böylece kişinin dokunulmazlığı, maddi-manevi varlığı ve temel hak ve özgürlüklerinin korunması sağlanmalıdır. Kanunda, başta kişinin açık rızası olmak üzere diğer hukuka uygunluk sebeplerinin ve bu sebeplerin nasıl kullanılacağının belirtilmesi ile veri işlemelerin hukuka uygun ve meşru bir şekilde yapılması da sağlanmış olacaktır.

Bu çerçevede, Türkiye'de kişilerin hak ve özgürlüklerini güvence altına alacak, bu alanda çalışan kişi ve kurumların yetki ve sorumluluklarının genel çerçevesini çizecek, uluslararası veri transferlerinde ilkeler belirleyecek olan KVKK Tasarısının, bu çalışmada önerilen yapısal düzenlemeler de dikkate alınarak bir an evvel yasalaşması gerektiği değerlendirilmektedir.

Bu çalışmanın içeriğini teşkil eden unsurların belli başlı sonuçları aşağıda yer almaktadır.

Yasal ve kurumsal alanda:

1- BİT'in hızla yaygınlaşması, bilgi toplumuna dönüşüm sürecinin ivme kazanarak kişisel verilerin dolaşımının giderek artması ve bu durum karşısında mahremiyet hakkının korunması gereği; ayrıca, Türk mevzuatının AB müktesebatı

ile uyumlaştırılması süreci; ülkemizde kişisel verilerin korunması mevzuatının çıkarılması ve uygulamadan sorumlu olacak bağımsız bir yapının ivedilikle tesis edilmesini gerekli kılmaktadır. Böylece kişisel verilerin kötüye kullanılması ile mücadelede *caydırıcı önlem* unsuru sağlanmış olacaktır.

2- KVKK Tasarısının kabul edilerek yasalaşması ile hukukumuzda "kişisel veri"nin tanımı, hangi bilgilerin bu kapsama girdiği, hangi eylemlerin bu verilerin işlenmesi anlamına geleceği hususlarında yasal unsurlar belirlenmiş olacaktır. Ayrıca, uluslararası hukuk belgelerinde hükme bağlanan kişilerin bilgi alma, kendilerine ait verilerinin silinmesini veya düzeltilmesini talep etme gibi çok önemli, somut ve pratik haklar vatandaşlarımıza da tanınmış ve bu hakları kullanabilmeleri için etkin mekanizmalar oluşturulmuş olacaktır. Bu mekanizmalar içinde, özellikle hem kamu kurum ve kuruluşları, hem de birçok kişisel veriyi kaydeden, depolayan ve türlü şekillerde işleyen özel sektör karşısında kişinin kendisiyle ilgili verinin silinmesi, yanlış ise düzeltilmesi gibi taleplerini yerine getirmeye zorlayacak, karşı tarafı yetkisiz ve hukuka aykırı işlemelerden sorumlu tutacak, kimin haklı olduğu konusunda uzun ve masraflı bir süreç gerektiren yargı yoluna başvurmaksızın karar verecek bir merciye olan ihtiyaç da karşılanmış olacaktır. Tüm bu haklar, konusunda uzman ve uluslararası uygulamalarla eşgüdüm sağlayacak bir Kurum bünyesinde, hızlı ve bağımsız karar alınması sağlanarak gerçekleştiğinde, bir özgürlük konusu olarak kişisel veriler korunmuş olacaktır.

Kişisel veriler kullanılarak işlenen siber suçlarla mücadelede, uluslararası kurum ve kuruluşlarla Türk makamları arasındaki işbirliği imkanlarının artırılması, bu makamlar arasında bilgi ve belge paylaşımının hızlı ve güvenli bir şekilde gerçekleşebilmesi gereklilikleri de Türkiye'de bir Veri Koruma Kanunu çıkarılmasını gerektirmektedir.

3- AB'ye üyelik sürecinde uyumlaştırılması gereken konulardan biri olarak KVKK Tasarısının yasalaşması hususuna 2008 yılı KOB'da ve 5 Kasım 2008 tarihli İlerleme Raporunun Yargı ve Temel Haklar faslı başlığı altında, ayrıca bu faslın Tarama Sonu Raporunda yer verilmektedir. Bunun yanında, başta 24 nolu faslın "Polis İşbirliği" altında ve 10 nolu "Bilgi Toplumu ve Medya" fasıllarında olmak

üzere, kişisel bilgilerin iletilmesi, işlenmesi saklanması ile ilgili olan fasıllara[246] ait çalışmalarda KVKK Tasarısının önemine dikkat çekilmektedir.

4- Dünyada veri koruma ile ilgili önde gelen ülkelerde bile her gün bir yenisiyle karşılaşılan veri koruma ihlal ve kazaları sonucunda çok sayıda kişinin verileri çalınmakta veya anonim olarak ele geçirilmekte; böylece hem haksız bir ticari kazanç elde edilmekte, hem de önemli mağduriyetler yaratan birçok suç işlenmektedir. Sınır ötesini ilgilendiren mahremiyet ihlalleriyle mücadele, daha ziyade küresel çözümler gerektirdiğinden Türkiye de uluslararası düzeydeki çabalar içinde yerini almalı ve özellikle uluslararası kuruluşlarla işbirliği yapmalıdır.

5- Yeni ihlaller karşısında ülkemizin tek başına alternatif yollar üretmesi ve uygulaması oldukça zor, hatta imkansızdır. Yaşanmakta olan ve muhtemel sorunlara karşı uluslararası literatürde birikmiş bilgi ve deneyimlerden faydalanmak, bu alandaki gelişmeleri takip edecek ve uluslararası faaliyetlerde aktif olacak kurumsal bir yapıyı gerekli kılmaktadır.

6- Tasarı, kurumsal yapı alanında mevcut ihtiyacı karşılayacak niteliği haiz değildir. Tasarı ile, Başbakanlık bünyesinde, sekreterya hizmetlerini de Başbakanlığın yapacağı bir Veri Koruma Kurulu kurulması öngörülmektedir. Oysa, ilgili tüm uluslararası uygulama ve politika dokümanlarının incelenmesinden, veri koruma talep ve şikayetlerini inceleyecek ve karar verecek bir kurumun başka bir kamu kurum ve kuruluşu içinde konumlanması o kurumun bağımsızlık ve özerkliği açısından uygun değildir. Örneğin şikayet edilenin İçişleri Bakanlığı olduğu bir dosyada, kararın Başbakanlık bünyesindeki bir Kurul tarafından verilecek olması, hukuki tarafsızlık ilkesini zedeleyecek olup, karar verme işinin tarafsızlık gerektiren doğasına aykırı bulunmaktadır. Aynı şekilde, Kurumun ayrı bir bütçeye sahip olmaması, Kurumun bağımsız karar verme yetki ve yeteneğine gölge düşürmektedir. Yeterli düzeyde yetki ve kaynaklarla donatılmış ve yaptırım gücünü haiz bir düzenleyici otoritenin kurulması ile kişisel verilerin korunmasında denetim fonksiyonu da sağlanmış olacaktır.

[246] 2007 yılında müzakerelere açılan Tüketicinin ve Sağlığın Korunması Faslının bulaşıcı hastalıklar, kan ve kan bileşenleri ile doku-hücre alanındaki mevzuat uyumu da kişisel verilerle ilgili içerik taşımaktadır.

Bu çalışmanın ülke örnekleri incelemesinden hareketle, ülkemizde de gecikmeksizin bağımsız ve özerk bir Veri Koruma Kurumu kurulması, bu kurumun başta 181 sayılı Sözleşme, 95/46/AT sayılı Direktif ve diğer hukuki belgelerde yer alan yetkilere paralel yetkilerle donatılması önerilmektedir. Kurum, kişisel verileri otomatik olan veya olmayan yollarla verisi işlenen ve bu yolla zarara uğrayan veya zarara uğrama tehlikesi bulunan kişilerin kişilik haklarını güvence altına alacak şikayetleri inceleme ve bağlayıcı; ancak temyiz edilebilir karar verme yetkisi ile veri işleme iş ve işlemlerini en başından bir kayıt sistemine bağlayarak gelişigüzel veri işlemelerinin önüne geçecek şekilde tasarlanmalıdır.

7- TCK'nın dokuzuncu bölümünde (md. 132 – 140) "Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar" düzenlenmektedir. Bu suçlardan md. 135'de düzenlenen "kişisel verilerin kayda alınması" suçu, çağımızda kişilerle ilgili kayıtları bilgisayar ortamında veya kağıt üzerinde muhafaza eden hastane, sigorta şirketi, bankalar, kredili alışveriş yapan mağazaların bu bilgileri amacı dışında kullanmasının önlenmesi amacıyla hükme bağlanmıştır. Ancak TCK'daki hukuka aykırı "kayıt", kişisel veri işleme türlerinden yalnızca bir tanesi olup, diğer hukuka aykırı veri işlemelerine ilişkin genel bir tedbir değildir. Ayrıca, TCK'da "kişisel veri" tanımının olmaması bu maddelerin uygulanmasında bir boşluk yaratmaktadır. TCK'nın dokuzuncu bölümünde yer alan söz konusu suçların (kişisel verileri hukuka aykırı olarak verme veya ele geçirme, verileri yok etmeme) uygulamaya ilişkin boşluğunu gidermede de KVKK önemli bir yer tutacaktır.

8- Veri korumada genel hukuki çerçeveyi çizecek KVKK Tasarısı yasalaştıktan sonra, ihtiyaç duyulan bazı sektörlerde de veri koruma düzenlemeleri yapılmalıdır. Doğrudan pazarlama, sosyal güvenlik, elektronik ödeme ve diğer işlemler, telekomünikasyon, güvenlik, istatistik vb. alanlar kişisel verilerin korunmasına ilişkin özel düzenleme gerektirir niteliktedir. Avrupa Konseyinin 108 sayılı Sözleşmesinin 6'ncı maddesi ve VKD, kişisel sağlık verilerini özel ve nitelikli kabul etmektedir. Bu çerçevede sağlık kurum ve kuruluşlarınca toplanan ve kaydedilen kişisel verileri koruyucu düzenleme yapılması, ülkemizin ulusal ve uluslararası alanda "insan hakları ihlali" iddiasına muhatap olmaması bakımından önem arz etmektedir.

Bununla birlikte, KVKK Tasarısında da yer alan, kişisel verilerin ancak bu Kanunda ve diğer kanunlarda öngörülen hallerde işlenebileceğine ilişkin "kanunilik" ilkesi uyarınca, keyfi uygulamalara mahal verilmemesinde kişisel verilerin korunması ile ilgili özel düzenlemelerin de *kanun* ile yapılması, en azından ikincil düzenlemelerin ilgili kanunundan açıkça yetki alması önem arz etmektedir. Mevcut ikincil düzenlemelerin bu çerçevede gözden geçirilmesi gerektiği düşünülmektedir.

9- Veri koruma alanında atılması gereken en önemli adımlardan biri de, kişilerin mağduriyete uğramadan önce neler yapmaları gerektiği konusunda bilgilendirilmeleri ve bilinçlendirilmelerine ilişkin *önleyici tedbirlerin* alınmasıdır. Bu çerçevede, konuya ilişkin yasa çalışmasının ardından, vatandaşların kişisel verilerini koruma konusundaki haklarını içeren bir rehberin yayımlanması oldukça etkili olacaktır. Kurulması önerilen Veri Koruma Kurumu'nun böyle bir Rehberi hazırlaması ve zaman zaman güncellemesi, halkın erişebileceği uygun araçlarla ilan etmesi uygun olacaktır. Bu tür rehberler halihazırda Avusturya, Belçika, Danimarka, Finlandiya, Fransa, Almanya, Yunanistan, İrlanda, İtalya, Lüksemburg, Hollanda, Portekiz, İspanya, İsveç ve İngiltere'de bulunmaktadır.[247]

Teknik alanda;

10- Kişisel verilerin kötüye kullanılması ile mücadelede ve kişilerin korunmasında *koruyucu tedbirlerden* de faydalanılmalıdır. Bu tedbirlerin birçoğu teknik nitelikte olup, çoğu kez de kimlik doğrulama amacıyla kullanılırlar. Bilgi toplumunda neredeyse bütün hukuki işlemlerin gerçekleştirilmesinde ilk adımı oluşturan kimlik doğrulama araçlarından sağlıklı olanlar tercih edilmelidir. Özellikle İnternet üzerinden yapılan sözleşmeler ve diğer hukuki işlemler hazırlar arasında olmayan sözleşmeler olduklarından, kişinin gerçekten o kişi olduğundan emin olmadan sözleşme yapılması zaman zaman sorunlar yaratabilmektedir. Bu çerçevede, akıllı kimlik kartları ve elektronik imza kullanılmalıdır. Bu sayede, kişilerin kimlik bilgileri yetkisiz kişilerin ellerine geçmiş olsa dahi bu yetkisiz kişiler gerçek kişinin yerine işlem yapamayacaktır. Dolayısıyla bu araçlara günümüzde işlem yapabilmenin teknolojik ehliyeti de denilebilir.

[247] Örnek için bkz. http://ec.europa.eu/justice_home/fsj/privacy/guide/index_en.htm

Ayrıca, kişisel mahremiyetin korunmasında politikalar ve yasalar kadar önemli olan MAT'lar (mahremiyet artırıcı teknolojiler), bireylerin, işletmelerin ve devletin mahremiyet ile ilgili yürütülen iş ve işlemlerinde kullanılmalı ve kullanılması teşvik edilmelidir. Ülkemizde yasal düzenlemelerin yapılmasının ardından, bireylerin, işletmelerin ve devletin mahremiyet ile ilgili yürütülen iş ve işlemlerin niteliğine uygun olacak MAT'lardan veri korumada ikincil kaynak olarak faydalanılması gerektiği değerlendirilmektedir.

11- Türkiye'de ticari faaliyetlere konu olmaya başlayan kişisel verilerin korunmasında kurum ve kuruluşlara da rol düşmektedir. Bu konuda, verilerin nasıl ele geçirildiğinin araştırılması ve sistem açıklarının kapatılması ile potansiyel bilgi güvenliği ihlallerine karşı bünyelerindeki ağ bağlantılı bilgisayarlar izlenmeli, dağıtık olarak hizmet çökertme saldırılarından (DDoS) etkilenen bilgisayarlar ağdan derhal kaldırılarak tehlikenin tüm ağa sirayet etmesinin önüne geçilmelidir. Böylelikle bu tür zararlı ataklar karşısında ağdaki kullanıcıların kişisel verilerinin toplanmasının önüne geçilmelidir. Yine idareler anti-virus programlarını düzenli olarak güncellemeli ve tüm masaüstü, dizüstü ve sunucu bilgisayarların işletim sistemlerinde gerekli güvenlik güncellemeleri yapılmalıdır.

12- Kimlik hırsızlığını nispeten azaltmak amacıyla kişisel veri depolayan kurum ve kuruluşlar İnternet üzerinden aktarılan veriler için gerekli tedbirleri almalıdır. Özellikle hassas veriler güçlü kripto araçlarıyla şifrelenmelidir. Böylece veritabanlarında depolanan hassas verilerin görülmesi veya kullanılması sınırlandırılmış olacaktır. Hassas veri içeren bilgisayarlar güvenli fiziki ortamlarda korunmalı ve sadece yetkili kişilerin erişim sağlayabileceklerinden emin olunmalıdır. Hassas veriler taşınabilir araçlarda (cep telefonu ve diğer mobil cihazlar) tutulmamalıdır.

13- Kişisel verilerin izleme araçları ile elde edildiği yerlerde kişileri bilgilendirici notlar açık ve anlaşılır bir şekilde ilgili kurum veya kuruluş tarafından ilan edilmelidir.

14- Yapılacak tüm teknik ve yasal düzenlemelerin yanısıra, kişisel verilerin korunması konusunda kamu kesimi başta olmak üzere, veri kontrolörleri, kişisel

verilerin yönetilmesi ve paylaşılmasında yetkili gerçek ve özel hukuk tüzel kişilerinin bu konunun önemi konusunda bilinç düzeyleri artırılmalıdır. Bu sebeple, farkındalık düzeyini artıracak eğitimler verilmelidir. Ayrıca, kişisel verilerin yönetilmesine ilişkin kişisel ve kurumsal kültürün geliştirilmesinde; kişisel verilerin tanımlayıcı olarak kullanılması ve böylece hak sahiplerinin tespit edildiği işlemlerde, bu verilerin o işlemin gerektirdiği miktarla sınırlı ve hak sahipleri arasında iltibasa mahal vermeyecek ölçüde kullanılmasının genel bir prensip olarak benimsenmesinde yarar görülmektedir. Böylece, çok daha fazla bilginin bir araya getirilmesi suretiyle anlamlı veri setlerinin oluşturulmasının; bu yolla verilerin anonim olarak erişilerek suç işlenmesi, verilerin analiz edilmesi ve doğrudan pazarlama amaçlarıyla kullanılmasının önüne geçilmesine katkı sağlanmış olacaktır.

15- Tüketicilerin BİT'i kullanırken dikkat etmeleri gereken noktalar konusunda bilinç ve farkındalık düzeyleri artırılmalıdır. Bu çerçevede, özellikle e-ticaret işlemlerinde tüketicilerin potansiyel güvenlik ve mahremiyet konularında bilinçlendirilmelerini sağlayacak tedbirler Sanayi ve Ticaret Bakanlığı ile diğer ilgili kurum ve kuruluşlar tarafından alınmalıdır.

EK 1: Karşılaştırmalı Hukukta Kişisel Verilerin Korunması[248]

I- Avrupa Konseyi Üyesi Ülkeler

Devlet	108 Sayılı Sözleşme		İlgili Anayasa Hükümleri	İlgili Ulusal Mevzuat	Yürürlük tarihi	Kapsamı			Kayıt veya bildirim	Verinin ihracında (dışarı iletiminde) özel yetki	Veri Koruma Otoritesi
	İmza tarihi	Onay tarihi				Elle işleme	Tüzel kişiler	Kamu veya özel sektör			
Arnavutluk	14/02/2004	09/06/2004	1998 AY, md. 35	9887 sayılı Kişisel Verilerin Korunması Hakkında Kanun, 2008	10/03/2008	Var	Yok	Her ikisi	Yok	Yok	Veri Koruma Komiseri
Ermenistan			1995 AY, md. 20								
Avusturya**	28/01/81	30/03/88	Veri Koruma Kanunu 2000, md.1 Bölüm 1-3'teki anayasal koşul	Kişisel Verilerin Korunmasına İlişkin Kanun (Federal Act concerning the Protection of Personal Data –Implementation of Directive 95/46/EC9)	17/08/99	Var	Var	Her ikisi	Tüm veriler (önemli istisnalar)	Bazı veriler	Veri Koruma Komisyonu
Azerbaycan			1995 AY, md.32	Veri, Veri işleme ve Veri Koruma Hakkında Azerbaycan Cumhuriyeti Kanunu	07.12.99						
Belçika**	07/05/82	28/05/93	1970 AY, md. 22	-Kişisel Verilerin Korunması Kanunu -95/46 sayılı VKD'nin uygulanmasına ilişkin Kanun -Kişisel Verilerin Korunması Kararnamesi	08/12/92 11/12/98 13/02/2001	Var	Var	Her ikisi	Tüm veriler	Bazı verileri	Mahremiyet Koruma Komisyonu

[248] Council of Europe. Human Rights and Legal Affairs, National Laws'a ait verilerden faydalanılmıştır.
* AB üyesi ülkelerden 95/46/AT sayılı VKD'yi uyumlaştıran ülkeler.
** AB üyesi ülkelerden 95/46/AT sayılı VKD'yi uyumlaştırma sürecinde olan ülkeler.

(I- Avrupa Konseyi Üyesi Ülkeler, devamı)

Devlet	108 Sayılı Sözleşme		İlgili Anayasa Hükümleri	İlgili Ulusal Mevzuat	Yürürlük tarihi	Kapsamı			Kayıt veya bildirim	Verinin ihracında (dışarı iletiminde) özel yetki	Veri Koruma Otoritesi
	İmza tarihi	Onay tarihi				Elle işleme	Tüzel kişiler	Kamu veya özel sektör			
Bosna Hersek	02/03/2004		Bosna Hersek'in 1995 tarihli AY, md. II, paragraf 3f	Kişisel Verilerin Korunması Kanunu	20/12/2001	-	-	Her ikisi	-	Yok	Veri Koruma Komisyonu
Bulgaristan	02/06/98	18/09/02	1991 AY, md. 32	Kişisel Verilerin Korunması Kanunu	21/12/2001	Var	Var	Her ikisi	Tüm veriler	Evet	Kişisel Verilerin Korunması Komisyonu
Hırvatistan	05/06/2003	21/06/2005	1990 AY, md. 37 (1997 ve 2000'de değişen)	Kişisel Verilerin Korunması Kanunu	01/10/2005	Var	Yok	Her ikisi	Tüm veriler (önemli istisnalar)	Yok	Kişisel Verileri Koruma Ajansı
Güney Kıbrıs Rum Yönetimi	25/07/86	21/02/02	1960 AY, md.15	Kişisel Verilerin İşlenmesi (Bireylerin Korunması) Kanunu, 2001	2001	Var	Yok	Her ikisi	Bazı verileri	Evet	Kişisel Verileri Koruma Komiseri
Almanya**	28/01/81	19/06/85	1943 AY, md.10	Federal Veri Koruma Kanunu (95/46 sayılı VKD'nin uygulanmasına yönelik)	01/01/2002	Var	Yok	Her ikisi	Bazı veriler	Yok	Federal Veri Koruma Komiseri
Yunanistan**	17/02/83	11/08/95		1997 tarihli ve 2472 sayılı kişisel verilerin işlenmesi ile ilgili bireyin korunması hakkında kanun Kişisel verilerin ve mahremiyetin elektronik haberleşme sektöründe korunması ve 2472/1997 sayılı kanunu değiştiren kanun (2006)	26/03/1997	Var	Yok	Her ikisi	Tüm veriler	Bazı veriler	Kişisel Veri Koruma Kurumu
Macaristan	13/05/93	08/10/97	149 AY, md. 59	LXIII sayılı kişisel verilerin korunması ve kamuyu ilgilendiren bilgilerin açıklanması hakkında kanun	17/11/92 Bölüm III Bölüm IV	Var	Yok	Her ikisi	Tüm veriler	Yok	Veri Koruma Ombudsmanı

(I- Avrupa Konseyi Üyesi Ülkeler, devamı)

Devlet	108 Sayılı Sözleşme		İlgili Anayasa Hükümleri	İlgili Ulusal Mevzuat	Yürürlük tarihi	Kapsamı			Kayıt veya bildirim	Verinin ihracında (dışarı iletimind e) özel yetki	Veri Koruma Otoritesi
	İmza tarihi	Onay tarihi				Elle işleme	Tüzel kişiler	Kamu veya özel sektör			
İzlanda	27/09/82	25/03/91		Kişisel verilerin işlenmesi karşısında bireylerin korunmasına ilişkin kanun	01/01/2000	Var	Var	Her ikisi	Tüm veriler	Tüm veriler	Kişisel Veri Koruma Kurumu
İrlanda*	18/12/86	25/04/90		1988 tarihli Veri Koruma Kanunu (2003'te değişti) Elektronik Mahremiyet Kanunu, 2003 (2008'de değiştirildi)	13/07/88 19/12/01	Yok	Yok	Her ikisi	Bazı veriler	Yok	Veri Koruma Komiseri
İtalya**	02/02/83	29/03/97		196/2003 sayılı Kişisel Veri Koruma Kanunu	01/01/2004	Var	Var	Her ikisi	Bazı veriler	Bazı veriler	Kişisel Verileri Koruma Kurumu
Letonya	31/10/00	30/05/01	1922 AY, m 96	Kişisel Veri Koruma Kanunu	23/03/00	Var	Yok	Her ikisi	Bazı veriler	Bazı veriler	Devlet Veri Denetim Otoritesi (Data State Inspectorate)
Lihtenştayn	02/03/2004	11/05/2004	-	Veri Koruma Kanunu, 2002 Veri Koruma üzerine 9 Temmuz 2002 tarihli Yönetmelik	14/03/02 09/07/02	Var	Var	Evet	Evet Bazı veriler	Evet	Veri Koruma Komiseri
Litvanya	11/02/00	01/06/01	1992 AY, md. 22	Kişisel Verilerin Yasal olarak Korunması Hakkında Kanun	17/07/00	Var	Yok	Her ikisi	Bazı veriler	Bazı veriler	Devlet Veri Denetim Otoritesi (State Data Protection Inspectorate)
Lüksemburg*	28/01/81	10/02/88	1868 AY, md. 28	Kişisel Verilerin İşlenmesi Halinde Bireyin Korunması Hakkında Kanun Telekomünikasyon Kanunu	02/08/2002	Var	Var	Her ikisi	Tüm veriler (istisnaları var)	Bazı veriler	Veri Koruma Ulusal Komisyonu

(I- Avrupa Konseyi Üyesi Ülkeler, devamı)

Devlet	108 Sayılı Sözleşme		İlgili Anayasa Hükümleri	İlgili Ulusal Mevzuat	Yürürlük tarihi	Kapsamı			Kayıt veya bildirim	Verinin ihracında (dışarı iletiminde) özel yetki	Veri Koruma Otoritesi
	İmza tarihi	Onay tarihi				Elle işleme	Tüzel kişiler	Kamu veya özel sektör			
Malta	15/01/2003	28/02/2003	1964 AY, bölüm 32	Veri Koruma Kanunu, 2001	14/12/2001	Var	Yok	Her ikisi	Tüm veriler	Bazı veriler	Veri Koruma Komiseri
Moldova	04/05/1998	28/02/2008	1994 AY, md. 28			Yok	Yok	Her ikisi			
Monako	01/10/2008	24/12/2008	1962 AY, md.22	İsimsel bilginin işlenmesi hakkında Kanun İsimsel verinin işlenmesi hakkında kanunun uygulanmasıona ilişkin Yönetmelik	23/12/1993	Var	-		Tüm veriler	Yok	Kişisel Verilerin Denetlenmesi Hakkında Kanun
Karadağ	06/09/2005	06/09/2005									
Hollanda**	21/01/88	24/08/93	1989 AY, m.10	Kişisel Veri Koruma Kanunu	06/07/00	Var	Yok		Her ikisi	Bazı veriler	Veri Koruma Komisyonu
Norveç	13/03/81	20/02/84		Kişisel Veri Kanunu	14/04/00	Var	-	Her ikisi	Tüm veriler	Tüm veriler	Veri Müfettişliği
Polonya	21/04/99	23/05/02	1997 AY, m. 51	Kişisel Verilerin Korunması Hakkında Kanun	29/08/97	Var	Var	Her ikisi	Bazı veriler	Evet	Kişisel Veri Koruma Genel Müfettişi
Portekiz**	14/05/81	02/09/93	1976 AY, m. 35	Kişisel Verilerin Korunması Kanunu (95/46 sayılı VKD'nin uygulanmasına ilişkin)	28/10/1998	Var	Yok	Her ikisi	Bazı veriler	Bazı veriler	Ulusal Veri Koruma Komisyonu
Romanya	18/03/97	27/02/02	1991 AY, m.26	Kişisel Verilerin İşlenmesi Karşısında Bireylerin Korunması ve Bu Verilerin Serbest Dolaşımı Hakkında 677/2001 sayılı Kanun 102/2005 ve 506/2004 sayılı Kanunlar	12/12/2001	Var	Var	Her ikisi	Evet	Evet	Kişisel Verilerin İşlenmesinin Denetlenmesi Hakkında Ulusal Otorite
Rusya	07/11/01		1993 AY, m.24								

(I- Avrupa Konseyi Üyesi Ülkeler, devamı)

Devlet	108 Sayılı Sözleşme		İlgili Anayasa Hükümleri	İlgili Ulusal Mevzuat	Yürürlük tarihi	Kapsamı			Kayıt veya bildirim	Verinin ihracında (dışarı iletiminde) özel yetki	Veri Koruma Otoritesi
	İmza tarihi	Onay tarihi				Elle işleme	Tüzel kişiler	Kamu veya özel sektör			
San Marino				Sayısallaştırılmış kişisel verilerin toplanması, işlenmesi ve kullanılması hakkında kanun	01/03/83	Yok	Var	Her ikisi	Tüm veriler	Bazı veriler	Gizli ve Kişisel Verilerin Korunmasından Sorumlu Garantör (Guarantor)
Sırbistan	06/09/2005	06/09/2005		Kişisel Veri Koruma Kanunu	/10/2008						
Slovakya	14/04/00	13/09/00	1992 AY, m. 19 ve 22	Kişisel Veri Koruma Kanunu	03/02/2005	Var	Yok	Her ikisi	Bazı veriler	Yok	Slovak Cumhuriyetini ve Kişisel Verileri Koruma Ofisi
Slovenya	23/11/93	27/05/94	1991 AY, m. 38	Kişisel Veri Koruma Kanunu	08/07/99	Var	Yok	Her ikisi	Tüm veriler	Bazı veriler	Bilgi Komiserliği
İspanya**	28/01/82	31/04/84	1978 AY, m. 18	Kişisel Verilerin Korunması Hakkında 15/99 sayılı Kanun	13/12/99	Var	Yok	Her ikisi	Tüm veriler	Bazı veriler	Veri Koruma Ajansı
İsveç**	28/01/81	29/09/82	1989 AY, Bölüm 2, m. 3	Kişisel Veri Kanunu	29/04/1998	Var	Yok	Her ikisi			Veri Teftiş Kurulu
İsviçre	02/10/97	02/10/97	1999 AY, m. 13	Federal Veri Koruma Kanunu Yönetmelikler:OLPD, OALSP	19/06/92 Yönetmelikler 14/06/93'te kabul edildi.	Var	Var	Her ikisi	Bazı veriler	Bazı veriler	Federal Veri Koruma ve Bilgi Komiseri
Makedonya	24/03/2006	24/03/2006	1992 AY, m.18	Kişisel Veri Koruma Kanunu	25/01/2005	Var	Var	Her ikisi	Yok	Evet	Kişisel Veri Koruma Müdürlüğü (İdari organ)
Türkiye	28/01/81		1982 AY (2001 değ.) m. 20								

(I- Avrupa Konseyi Üyesi Ülkeler, devamı)

Devlet	108 Sayılı Sözleşme		İlgili Anayasa Hükümleri	İlgili Ulusal Mevzuat	Yürürlük tarihi	Kapsamı			Kayıt veya bildirim	Verinin ihracında (dışarı iletiminde) özel yetki	Veri Koruma Otoritesi
	İmza tarihi	Onay tarihi				Elle işleme	Tüzel kişiler	Kamu veya özel sektör			
Ukrayna	29/08/2005		1996 AY, m.32	Bilgi ve telekomünikasyon sistemlerinde Ukrayna veri koruma kanunu, 2006 Kişisel Verilerin Korunması Hakkında Taslak Kanun, 09.01.2007							
İngiltere**	02/10/97	02/10/97		Veri Koruma Kanunu	Bölge kanunları: Jersey Kanunu, Guernsey Kanunu, Isle of Man Kanunu	16/07/98	Var	Yok	Her ikisi	Tüm veriler	Evet

II- Avrupa Konseyi Üyesi Olmayan Bazı Ülkeler

Devlet	108 Sayılı Sözleşme		İlgili Anayasa Hükümleri	İlgili Ulusal Mevzuat	Yürürlük tarihi	Kapsamı			Kayıt veya bildirim	Verinin ihracında (dışarı iletiminde) özel yetki	Veri Koruma Otoritesi
	İmza tarihi	Onay tarihi				Elle işleme	Tüzel kişiler	Kamu veya özel sektör			
Vatikan											
ABD				1-Mahremiyet Kanunu 2-Kişisel verilerin korunmasında farklı sektörlere ait kanunlar[249] 3- Güvenli Liman Kuralları	1- 1974 3-2000						
Kanada			1982 AY, Bölüm 8	1- Mahremiyet Kanunu 2- Kişisel Verilerin Korunması ve Elektronik Belgelere İlişkin Kanun	01/07/83 13/04/00	Var		Kamu			Mahremiyet Komiseri Federal Kurumlar
Japonya				1-Kamu sektörü: Kamu kurumlarında sayısal ortamda tutulan kişisel verilerin korunması hakkında kanun 2-Kamu kurumlarında sayısal ortamda tutulan kişisel verilerin korunması hakkında kanunun uygulanmasına ilişkin yönetmelik	16/12/88 01/10/89	Yok	Yok	Kamu	Bazı veriler		İdari Yönetim Ofisi, İçişleri, Posta ve Telekomünikasyon
Meksika			1917 AY, m.16	Federal Şeffaflık ve kamu kurumlarındaki bilgilere erişim kanunu Federal Kanunlar	05/2002						Kamu Bilgilerine Erişim Enstitüsü
Arjantin			1853 AY, m.43	Kişisel Verilerin Korunması Kanunu	04/10/2000	Var		Her ikisi			
Avustralya				Federal Mahremiyet Kanunu	18/10/88 21/12/2002	Var	Yok	Kamu ve özel sektör			Mahremiyet Komiseri
Brezilya			1988 AY, m.5.X,	Habeas Veri Kanunu	1997						

[249] Cable Privacy Protection Act (1984), Family Educational Right to Privacy Act (FERPA) (2008), Electronic Communications Privacy Act

(II- Avrupa Konseyi Üyesi Olmayan Bazı Ülkeler, devamı)

Devlet	108 Sayılı Sözleşme		İlgili Anayasa Hükümleri	İlgili Ulusal Mevzuat	Yürürlük tarihi	Kapsamı			Kayıt veya bildirim	Verinin ihracında (dışarı iletiminde) özel yetki	Veri Koruma Otoritesi
	İmza tarihi	Onay tarihi				Elle işleme	Tüzel kişiler	Kamu veya özel sektör			
Şili			1980 AY, m.19	Kişisel Verilerin Korunması Kanunu	28/08/99	Var	Evet	Her ikisi	Yok	-	
İsrail			1992, Bölüm 7, Temel Kanunlar; İnsan Onuru ve Özgürlüğü	5741 sayılı Mahremiyeti Koruma Kanunu 5746 sayılı İdari Verileri Koruma Kanunu	02/1981 1986	Yok	Yok				
Güney Kore			1948 AY, M.17	Kamu Kurumlarınca Yönetilen Kişisel Verilerin Korunması Kanunu	07/01/94	Yok	Yok	Kamu			
Tayland	06/09/2005	06/09/2005	1997 AY, Bölüm 34	Bilgi Kanunu no: B.E 2540	1997		-	Evet			Resmi Bilgi Komisyonu Ofisi
Yeni Zelanda			1990 Yeni Zelanda Haklar Kanunu, m.28	Mahremiyet Kanunu	17/05/93					Yok	Mahremiyet Komiseri

EK 2: KİŞİSEL VERİLERİN KORUNMASI KANUNU TASARISI

BİRİNCİ KISIM
Genel Hükümler
BİRİNCİ BÖLÜM
Amaç, Kapsam ve Tanımlar

Amaç

MADDE 1- (1) Bu Kanunun amacı; kişisel verilerin işlenmesinde kişinin dokunulmazlığı, maddi ve manevi varlığı ile temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin uyacakları esas ve usulleri düzenlemektir.

Kapsam

MADDE 2- (1) Bu Kanun hükümleri, kişisel verileri işlenen gerçek ve tüzel kişiler ile bu verileri tamamen veya kısmen, otomatik olan veya olmayan yollarla herhangi bir veri kütüğüne dahil olacak şekilde işleyen gerçek ve tüzel kişiler hakkında uygulanır.

(2) Bu Kanun hükümleri, kişisel verilerin gerçek kişiler tarafından sadece kişisel veya birlikte oturanlarla ilgili faaliyetlerine ilişkin olarak işlenmesi halinde uygulanmaz.

Tanımlar

MADDE 3- (1) Bu Kanunda geçen;

a) Alıcı: Kişisel verileri belirli bir soruşturma çerçevesinde alan makamlar hariç olmak üzere, üçüncü kişi olsun veya olmasın verinin açıklandığı herhangi bir gerçek veya tüzel kişi ile kişi topluluğunu, kamu kurum veya kuruluşunu,

b) Anonim hale getirme: Kişisel verilerin, belirli veya kimliği belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek veya kaynağı belirlenemeyecek hale getirilmek suretiyle işlenmesini,

c) İlgili kişi: Hakkında kişisel veri işlenen gerçek ve tüzel kişileri,

ç) Kişisel veri: Belirli veya kimliği belirlenebilir gerçek ve tüzel kişilere ilişkin bütün bilgileri,

d) Kişisel verileri işleyen: Veri kütüğü sahibi adına, bu verileri işleyen gerçek ve tüzel kişileri,

e) 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 veya tasniflenmesi veya kullanılmasının engellenmesi gibi bu veriler üzerinde gerçekleştirilen bir işlem ya da işlemler bütününü,

f) Kurul: Kişisel Verileri Koruma Kurulunu,

g) Sicil: Veri Kütüğü Sicilini,

ğ) Üçüncü kişi: Veri kütüğü sahibi ile kişisel verileri işleyen ve bunların doğrudan talimatı altında bulunan kişilerin dışında kalan ve kişisel veri işleyen gerçek ve tüzel kişi ile kişi topluluğunu, kamu kurum veya kuruluşunu,

h) Veri kütüğü: Gerçek ve tüzel kişilere ilişkin belirli bir kritere göre kişisel verilere ulaşımı kolaylaştıracak şekilde yapılandırılmış herhangi bir kişisel veri grubunu,

ı) Veri kütüğü sahibi: Kişisel verilerin işlenmesinin amaç ve metodlarını tek başına veya başkaları ile birlikte belirleyen gerçek ve tüzel kişileri,

ifade eder.

İKİNCİ BÖLÜM
Kişisel Verilerin İşlenmesi

Kanunîlik ilkesi

MADDE 4- (1) Kişisel veriler, ancak, bu Kanunda ve diğer kanunlarda öngörülen hâllerde işlenebilir.

Kişisel verilerin işlenmesine ilişkin ilkeler

MADDE 5- (1) Kişisel verilerin;

a) Hukuka ve dürüstlük kurallarına uygun olarak işlenmesi,

b) Belirli, açık ve meşru amaçlar için toplanması ve bu amaçlara 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,

zorunludur.

(2) Kişisel veriler, ilgili mevzuatta yeniden işlenme amacına yönelik yeterli koruma tedbirleri getiren düzenlemenin bulunması veya kişisel verileri kontrol eden tarafından bu yönde gerekli tedbirlerin alınması şartıyla tarihî, istatistikî veya bilimsel amaçlarla yeniden işlenebilir veya birinci fıkranın (d) bendinde öngörülenden daha uzun bir süre saklanabilir.

Hukuka uygunluk sebepleri

MADDE 6- (1) Kişisel veriler ancak ilgili kişinin açık rızasıyla işlenebilir.

(2) Kanunlarda öngörülen yükümlülüklerin yerine getirilmesi dışında, ilgili kişinin bir itirazda bulunması hâlinde veri işlenemez.

(3) Aşağıdaki hâllerde de hukuka uygunluk sebeplerinin bulunduğu kabul edilir:

a) Kanunun öngördüğü bir zorunluluk dolayısıyla, kamu yararına veya resmi olarak verilmiş bir görevin yerine getirilmesi amacıyla veri işlenmesi,

b) Kişisel verilerin, ilgili kişinin rızasını açıklayamayacak durumda olması hâlinde kendisinin veya başkasının hayatını veya beden bütünlüğünü korumak amacıyla işlenmesi,

c) Bir sözleşmenin kurulması ve ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesi,

ç) İlgili kişiler tarafından açıklanmış olması veya açık sicillerde mevcut bilgiler olması sebebiyle herkesçe bilinen kişisel verilerin işlenmesi,

d) Veri kütüğü sahibinin kendi haklı çıkarları için, ilgili kişinin temel hak ve özgürlükleri ile meşru çıkarlarına zarar vermediği sürece, veri işlemesinin zorunlu olması.

Özel niteliği olan kişisel veriler

MADDE 7- (1) Kişilerin ırk, siyasî düşünce, felsefî inanç, din, mezhep veya diğer inançları, dernek, vakıf ve sendika üyeliği, sağlık ve özel yaşamları ve her türlü mahkûmiyetleri ile ilgili kişisel veriler işlenemez.

(2) Birinci fıkrada belirtilen kişisel verilerin, özel hayatın ve aile hayatının gizliliğinin korunmasını sağlayacak yeterli önlemlerin alınması şartıyla, aşağıda sayılan hallerde işlenmesi mümkündür:

a) Kanunla yasaklanmayan hallerde kişinin yazılı rızasının alınması,

b) Hukukî veya fiilî nedenlerle rızasını açıklayamayacak durumda bulunan bir kişinin kendisinin veya bir başkasının hayatı veya beden bütünlüğünün idamesi için veri işlemenin zorunlu olması,

c) İlgili kişiye yeterli koruma imkânının sağlanması şartıyla, veri kütüğü sahibinin, bu Kanunla veya diğer kanunlarla tanınan hak ve yetkileri kullanabilmesi veya yükümlülükleri yerine getirebilmesi için veri işlemenin zorunlu olması,

ç) Vakıf, dernek, sendika ve siyasi partilerce, kuruluş amaçlarına ve tâbi oldukları mevzuata uygun ve faaliyet alanlarıyla sınırlı olmak şartıyla, üye ve mensuplarına yönelik ve ilgili kişinin rızası olmadan üçüncü kişilere açıklanmamak kaydıyla veri işlenmesi,

d) İlgili kişi tarafından alenen açıklanmış olan veriler hakkında olması,

e) Hukuken bir hakkı tesis, kullanma veya korunması için veri işlemenin zorunlu olması,

f) Koruyucu hekimlik, tıbbî teşhis, tedavi, bakım veya sağlık hizmetlerinin yürütülmesi amacıyla kişisel verilerin;

1) Sağlık kurumları,

2) Sigorta şirketleri,

3) Sosyal güvenlik kurumları,

4) İşyeri sağlık birimi oluşturmakla yükümlü işverenler,

5) Sağlıkla ilgili okul ve üniversiteler,

tarafından ilgili kanunlara uygun olarak, hukuken veya meslek kurallarına göre sır saklama yükümlülüğü altında bulunan sağlık personeli veya eşdeğer seviyede sır saklama yükümlülüğü altındaki bir başka kişinin gözetimi altında işlenmesi.

(3) Özel hayatın ve aile hayatının gizliliğine dokunmamak şartıyla, temel kamu yararlarının gerektirmesi hâlinde, ilgili mevzuatta yeterli koruma tedbiri bulunması kaydıyla, Kurul, özel niteliği olan kişisel verilerin işlenmesine karar verebilir.

(4) Suçun soruşturulmasına, koruma ve kontrol tedbirlerine ve ceza mahkûmiyetlerine ilişkin özel nitelikteki kişisel veriler, ilgili kanunlarda yeterli koruma tedbiri bulunması kaydıyla, yetkili mercilerin kontrolü altında işlenebilir.

Ancak, ceza mahkûmiyetlerine ilişkin sicil sadece Adalet Bakanlığının kontrolü altında tutulabilir.

(5) İdarî nitelikteki yaptırımlar ve özel hukuk alanındaki mahkeme kararlarına ilişkin veriler de resmî mercilerin kontrolü altında işlenebilir.

(6) Vatandaşlık kimlik numarası veya benzeri karakteristik işaretlerin işlenme usul ve esaslarını belirlemek amacıyla yapılacak yönetmeliklerde Kurulun görüşü alınır.

Kişisel verilerin üçüncü kişilere aktarılması

MADDE 8- (1) Aşağıda sayılan haller dışında kişisel veriler üçüncü kişilere aktarılamaz:

a) Aktarmayı isteyen gerçek ve tüzel kişilerin belirli bir olayda kanundan doğan bir görevini yerine getirmesi için bu bilgiye ihtiyaç duyması,

b)Bu Kanunun 6 ncı maddesinin üçüncü fıkrasında sayılan hâllerin gerçekleşmesi.

(2) Millî güvenliğin ve millî savunmanın sağlanması, suçun önlenmesi veya soruşturulması amacıyla yapılan istihbarî faaliyetlerle ilgili olarak kanundan doğan bir görevin yerine getirilmesi için gerekli olması hâlinde de kamu kurum ve kuruluşlarınca kişisel veriler ilgili kamu kurum ve kuruluşuna aktarılabilir.

(3) Kamu kurum veya kuruluşları; kamu yararı, sır saklama yükümlülüğü, ilgili kişinin meşru menfaati veya kişisel verilere ilişkin özel koruma kurallarının varlığından bahisle kişisel verilerin üçüncü kişilere aktarılmasını reddedebilir, sınırlandırabilir veya şarta bağlayabilir.

(4) Kamu kurum veya kuruluşlarının görev alanlarıyla ilgili konularda yapacakları talep üzerine, gizlilik esaslarına göre görev yapan personelin bilgileri hariç olmak üzere, kişilerin nüfus kayıt örnekleri ve adresleri bildirilir.

Kişisel verilerin anonim hale getirilmesi veya yok edilmesi

MADDE 9- (1) İhtiyaç duyulmayan kişisel veriler, koruma tedbiri veya ispat amacıyla muhafazasının gerekli olmadığı durumlarda, anonim hâle getirilir veya yok edilir.

(2) Verilerin anonim hale getirilmesi veya yok edilmesine ilişkin usul ve esaslar Kurulca, ilgili kamu kurum ve kuruluşları ile diğer özel hukuk tüzel kişilerinin görüşleri alınarak hazırlanan yönetmelikte gösterilir.

(3) Diğer kanun hükümleri saklıdır.

Verilerin araştırma, plânlama ve istatistik amacıyla kullanılması

MADDE 10- (1) Kişisel veriler, araştırma, plânlama ve istatistik gibi amaçlarla anonim hale getirilmesi kaydıyla işlenebilir. Bu suretle elde edilen veriler ve sonuçlar üçüncü kişilere aktarılabilir veya yayımlanabilir.

İKİNCİ KISIM
İlgili Kişinin Hakları ve Yurtdışına Veri Aktarımı
BİRİNCİ BÖLÜM
Aydınlatma Yükümlülüğü ve İlgili Kişinin Hakları

Aydınlatma yükümlülüğü

MADDE 11- (1) Kişisel verilerin elde edilmesi sırasında veri kütüğü sahibi, ilgili kişilere;

a) Veri kütüğü sahibi ve varsa temsilcisinin kimliği,

b) Kişisel verilerin hangi amaçla işleneceği,

c) Kişisel verilerin kimlere aktarılabileceği,

ç) Veri toplamanın yöntemi, hukukî sebebi ve muhtemel sonuçları,

d) Kişisel verileri öğrenme hakkı,

e) Düzeltme hakkı,

konusunda bilgi vermekle yükümlüdür.

(2) Kişisel verilerin, ilgili kişi dışındaki kaynaklardan edinilmesi hâlinde de ilgili kişiye yukarıdaki bilgilerle birlikte işleme konu olan veri kategorileri hakkında bilgi verilir.

İlgili kişinin hakları

MADDE 12- (1) Herkes, veri kütüğü sahibine başvurarak; kendisiyle ilgili kişisel veri kaydedilip kaydedilmediğini öğrenmek, kaydedilmişse bunları talep etmek, verinin muhtevasının eksik veya gerçeğe aykırı olması hâlinde bunların düzeltilmesini, hukuka aykırı olması hâlinde ise silinmesini, yok edilmesini veya aktarımının engellenmesini ve buna göre yapılacak işlemlerin verilerin açıklandığı üçüncü kişilere bildirilmesini istemek hakkına sahiptir.

(2) Bu talep karşısında veri kütüğü sahibi;

a) Veri kütüğündeki ilgili kişiye ait bilgilerin ve işlenen bilgi türlerinin tamamını bildirmekle,

b) Veri işlemenin hukukî dayanağını ve amacını bildirmekle,

c) Hangi tür kişisel verilerin üçüncü kişilere aktarılabileceği ve aktarılacak kişilerin kimliklerini bildirmekle,

ç) Verinin muhtevasının eksik veya gerçeğe aykırı olması hâlinde düzeltmekle,

d) Hukuka aykırı olması hâlinde silmek, yok etmek ve üçüncü kişilere aktarımını engellemekle,

e) Uygulanması imkansız olmamak veya büyük güçlükler yaratmamak kaydıyla bu fıkranın (a) ve (b) bentlerine göre yapılan işlemleri, verilerin açıklandığı üçüncü kişilere bildirmekle,

yükümlüdür.

(3) Bu maddede sayılan haklar, aşağıda sayılan hallerde sınırlandırılabilir:

a) Milli güvenliğin korunması, milli savunmanın gerçekleştirilmesi, suçun önlenmesi veya istihbarat amacıyla yapılan faaliyetlerle ilgili olarak kanundan doğan bir görevin yerine getirilmesi,

b) Ceza soruşturması veya kovuşturmasına zarar verilmesinin engellenmesi.

Başvuru usulü

MADDE 13- (1) 12 nci maddeye göre başvurular, yazılı olarak yapılır. Veri kütüğü sahibi talep hakkında başvuru tarihinden itibaren onbeş iş günü içinde cevap vermek zorundadır.

(2) İlgili kişi talebine cevap verilmediği, cevabın olumsuz olduğu veya yeterli olmadığı iddiasıyla yirmi gün içinde Kurula itiraz edebilir. Kurul, 33 üncü madde çerçevesinde başvuru hakkında üç ay içerisinde karar verir.

(3) Başvurunun yapıldığı veri kütüğü sahibi, erişimine olanak sağladığı bilgi veya belgeler için başvuru sahibinden erişimin gerektirdiği maliyet tutarı kadar, Kurul tarafından her yıl Ocak ayında belirlenecek miktarda bir ücret talep edebilir.

İKİNCİ BÖLÜM

Yurtdışına Veri Aktarımı ve Tedbirler

Yurtdışına bilgi aktarımı

MADDE 14- (1) Kişisel veriler, ancak kişilik haklarının korunması açısından verinin istendiği yabancı ülkede eşdeğer ve etkin koruma bulunuyorsa yurtdışına aktarılabilir.

(2) Verinin istendiği ülkede eşdeğer ve etkin bir koruma olmasa dahi;

a) İlgili kişinin açık rızasının bulunması,

b) İlgili kişi ile veri kütüğü sahibi arasında bir sözleşmenin yapılması, sözleşme öncesi ilişkinin yürütülmesi veya sözleşmenin ifası için aktarımın gerekli olması,

c) Suçun önlenmesi veya bir hakkın tespiti, icrası veya korunması için aktarımın gerekli veya kanun gereği zorunlu olması,

ç) Veri konusu kişinin hayatı veya beden bütünlüğünün idamesi için aktarımın zorunlu olması,

d) Veri aktarımının, ilgili mevzuatın aradığı şartları yerine getirmek koşuluyla kamunun veya ilgisini ispat eden herkesin erişimine açık bulunan sicillerden yapılması,

hallerinde kişisel veriler yurtdışına aktarılabilir.

(3) Yabancı ülkede bulunan veri kütüğü sahibinin, eşdeğer ve uygun bir korumayı yazılı olarak taahhüt etmesi ve Kurulun izninin bulunması halinde de kişisel veriler yurtdışına aktarılabilir. Ancak, gecikmesinde sakınca bulunan veya telafisi güç veya imkansız zararların doğması ihtimali bulunan hallerde, veri kütüğü sahibi kişisel verileri yurtdışına aktarabilir. Bu halde veri kütüğü sahibi, durumu yirmidört saat içerisinde Kurula bildirir. Kurul, veri aktarımının bu Kanun hükümlerine uygun olup olmadığı hususunda inceleme yaparak bir karar verir.

(4) Kurul, yurtdışına bilgi aktarımında;

a) Taraf olduğumuz uluslararası anlaşmaları,

b) Veri talep eden ülkeyle ülkemiz arasında veri aktarımına ilişkin fiili karşılıklılık durumunu,

c) Her somut veri transferine ilişkin olarak, verinin niteliği, işlenme amaç ve süresini,

ç) Verinin transfer edileceği ülke ve bu ülkede uygulanan konuyla ilgili kanunları,

d) Koruma tedbirleri ve verinin transfer edileceği ülkede bulunan veri kütüğü sahibi tarafından yeterli önlemlerin alınıp alınmadığını,

değerlendirmek suretiyle karar verir.

Kişisel verilerin işlenmesine ilişkin tedbirler

MADDE 15- (1) Veri kütüğü sahibi, kişisel verilerin, tedbirsizlikle veya hukuka aykırı amaçlarla yok edilmesini, kaybolmasını, değiştirilmesini, yetkisiz olarak açıklanmasını veya aktarılmasını ve başka şekillerdeki tüm hukuka aykırı işlenmelerini önlemek için, korunacak verinin niteliği, teknolojik imkânlar ve uygulama maliyetine göre uygun teknik ve idarî tedbirleri almak zorundadır.

(2) Verilerin, veri kütüğü sahibi adına başka bir işleyen tarafından işlenmesi halinde, veri kütüğü sahibinin, işleyenin yeterli teknik ve idarî tedbirleri temin etmesini bir sözleşme veya hukukî tasarrufla yazılı olarak yükümlü tutması zorunludur.

(3) Veri kütüğü sahibi, işleyenin veya onun kontrolü altında olup da verilere ulaşma imkanı olan kişilerin; kanunla öngörülen haller dışında, yalnızca veri kütüğü sahibinin talimatları doğrultusunda veri işlemesini ve birinci fıkrada belirtilen yükümlülükleri yerine getirmesini, ikinci fıkrada belirtilen şekilde sağlar.

ÜÇÜNCÜ KISIM
Sicil
BİRİNCİ BÖLÜM
Sicil, Sicile Kayıt ve Ön İnceleme

Veri Kütüğü Sicili

MADDE 16- (1) Kurul tarafından bir Veri Kütüğü Sicili tutulur.

(2) Kişisel verileri işleyen gerçek ve tüzel kişiler, veri kütüğü kurmadan önce Sicile kaydolmak zorundadır.

(3) Sicil kamuya açık olarak tutulur.

Sicile kayıt başvurusu

MADDE 17- (1) Sicile kayıt başvurusu aşağıdaki hususları içeren bir bildirimle yapılır:

a) Veri kütüğü sahibi veya varsa temsilcisinin kimlik ve adres bilgileri,

b) Kişisel veri işlemenin amaçları,

c) Veri konusu kişi grubu ve grupları ile bu kişilere ait veri kategorileri hakkındaki açıklamalar,

ç) Verilerin açıklanabileceği alıcılar veya alıcı grupları,

d) Üçüncü ülkelere aktarımı öngörülen veriler,

e) 15 inci madde uyarınca alınan tedbirlere ilişkin genel açıklama.

(2) Yukarıda sayılan bilgilerde yapılan değişiklikler yıl sonunda toplu olarak yeniden Kurula bildirilir.

Bildirimin istisnaları

MADDE 18- (1) Aşağıdaki hallerde Sicile bildirim zorunluluğu yoktur:

a) Kişilerin temel hak ve özgürlüklerini olumsuz yönde etkilemeyecek nitelikte veri işlenmesi,

b) Veri işlemenin kamuya bilgi verilmesi amacıyla tutulan ve yasal çıkarı bulunan herkesin incelemesine açık bir sicil için yapılması,

c) Veri işlemenin 6 ncı maddenin üçüncü fıkrasının (ç) bendinde belirtilen amaçlarla yapılması,

ç) Veri koruma denetim kuruluşunun görevlendirilmiş olması.

(2) Birinci fıkranın (a) bendinde belirtilen veriler veya veri kategorileri, veri işlemenin amaçları, ilgili kişilerin dahil olduğu kategoriler, alıcılar veya alıcı kategorileri ile verilerin saklama süreleri Kurul tarafından belirlenir.

Ön inceleme

MADDE 19- (1) Kurul, veri konusu kişilerin, kişiliklerine, temel hak ve özgürlüklerine yönelik risk taşıma ihtimali olan ve bu Kanunun 5 inci maddesinde belirtilen niteliklere uygun olmayan ve 6 ncı ve 7 nci maddelerinde belirtilen koşulları taşımayan veri işlemelerini belirlemek üzere, ilgili veri işlemeleri başlamadan önce bir ön inceleme yapar.

(2) Ön inceleme, Kurul tarafından, veri kütüğü sahibi veya varsa temsilcisi tarafından Sicile kayıt başvurusundan itibaren en geç bir ay içinde yapılır. Ön inceleme sonuçlanmadan veri işlemesi yapılamaz.

İKİNCİ BÖLÜM
Veri Koruma Denetim Kuruluşu ve Bildirim

Veri koruma denetim kuruluşu

MADDE 20- (1) Veri kütüğü sahipleri, bu Kanun hükümlerinin uygulanmasını sağlamak üzere bağımsız denetim kuruluşu görevlendirebilir. Bu kuruluşlar, kendilerini atayan veri kütüğü sahibi tarafından bu Kanunun uygulanmasını, herhangi bir talimat almaksızın denetlerler ve bu amaçla, 16 ncı maddede belirtilen Sicili tutarlar.

(2) Denetleme kuruluşları, ilgili kişilerin şikayet ve talepleri nedeniyle öğrendikleri bilgileri, o kişilerin rızası olmadıkça, gizli tutmakla yükümlüdür. Kuruluşlar, çalışmaları hakkında hazırladıkları yıllık raporları her yıl Ekim ayı sonuna kadar Kurula sunarlar.

(3) Veri kütüğü sahibi, kuruluşun görevini yapabilmesi için gerekli imkanları sağlamakla yükümlüdür. Bağımsız denetleme kuruluşlarının kuruluş ve çalışma esasları ile niteliği Bakanlar Kurulu kararı ile yürürlüğe konulan yönetmelikle düzenlenir.

Kurula bildirim

MADDE 21- (1) Bağımsız denetim kuruluşunun göreve başlayabilmesi için veri kütüğü sahibi tarafından Kurula bildirimde bulunulması zorunludur. Kurul ayrı bir bağımsız denetim kuruluşu sicili tutar. Kurulun bu Kanundan doğan görev ve yetkileri saklıdır.

ÜÇÜNCÜ BÖLÜM
İstisnalar ve Meslek Kuralları

İstisnalar

MADDE 22- (1) Bu Kanunun 6 ncı, 11 inci, 16 ncı, 17 nci ve 19 uncu maddeleri aşağıda sayılan haller bakımından uygulanmaz:

a) Milli güvenliğin korunması, milli savunmanın gerçekleştirilmesi veya bu amaçla yapılan istihbarî faaliyetlerin yürütülmesi,

b) Kamu düzeninin korunması,

c) Suçun önlenmesi için gerekli olması, suç veya meslek ahlak kurallarını ihlâl eden eylemlerin soruşturulması veya kovuşturulması,

ç) Bütçe, vergi ve mâli konulara ilişkin olarak Devletin önemli ekonomik veya malî çıkarlarının gerektirmesi,

d) Bu fıkranın (b), (c) ve (ç) bentlerinde belirtilen konularda, resmî mercilerin izleme, denetleme veya düzenleme görevlerinin gerektirmesi.

(2) Bu Kanunun 12 nci maddesinde belirtilen haklar, kişisel verilerin özellikle belli bir kişiye ilişkin tedbir veya karar alınmasına yönelik kullanılmadığı ve ilgili kişinin özel yaşamının gizliliğinin ihlal edilmesi riskinin bulunmadığı hallerde, ilgili mevzuatta yeterli koruma tedbiri bulunması kaydıyla, bilimsel araştırma veya istatistik oluşturma amaçları ile sınırlanabilir.

Gazetecilik amacıyla kişisel verilerin işlenmesi

MADDE 23- (1) Yayın sahipleri veya temsilcileri ile bunların çalışanları tarafından sadece gazetecilik amacıyla veri işlenmesi halinde bu Kanunun 5 inci, 15 inci ve 24 üncü maddeleri uygulanır.

(2) Birinci fıkrada belirtilen kişisel verilerin işlenmesi fiilleri, ancak düşünceyi açıklama ve yayma hürriyeti sınırları çerçevesinde, yayın sahipleri veya temsilcileri ve bunların çalışanlarının enformasyon ihtiyaçlarının karşılanması için gerekli olması halinde hukuka uygun sayılır.

Kişisel verilerin işlenmesi bakımından meslekî davranış kuralları

MADDE 24- (1) Veri kütüğü sahiplerinin bağlı oldukları meslek birlikleri tarafından, değişik sektörlerin özellikleri dikkate alınarak, kişisel verilerin işlenmesiyle ilgili kuralların yerinde uygulanabilmesini temin etme amacıyla hazırlanan mesleki davranış kuralları, bu Kanuna uygunluğunun denetimi için, Kurula sunularak görüşü alınır. Kurul yapacağı denetimde ilgili kişiler veya temsilcilerinin de görüşlerine başvurur.

Kişisel verilerin silinmesi veya yok edilmesi

MADDE 25- (1) 22 nci maddenin birinci fıkrasında sayılan haller saklı kalmak üzere, bu Kanunda yer alan genel ilkeleri taşımayan kişisel veriler silinir veya yok edilir.

(2) Kişisel verilerin silinmesi veya yok edilmesinin esas ve usulleri Kurul tarafından hazırlanan yönetmelikle belirlenir.

DÖRDÜNCÜ KISIM
Kişisel Verileri Koruma Kurulu
BİRİNCİ BÖLÜM
Kurulun Oluşumu ve Görevleri

Kurul

MADDE 26- (1) Bu Kanunla verilen görevleri yapmak üzere, Kişisel Verileri Koruma Kurulu oluşturulmuştur.

(2) Kurul, yetkilerini bağımsız olarak kullanır. Hiçbir organ, makam, merci ve kişi Kurulun kararını etkilemek amacıyla emir ve talimat veremez.

(3) Kurul, görevleri ile ilgili konularda tüm kamu kurum ve kuruluşları ile gerçek ve tüzel kişilerden her türlü bilgi ve belgeyi isteyebilir. Kamu kurum ve kuruluşları ile gerçek ve tüzel kişiler, söz konusu isteğe cevap vermek ve gereken kolaylığı göstermekle yükümlüdür.

Kurulun oluşumu

MADDE 27- (1) Kurul, Bakanlar Kurulunca seçilen yedi üyeden oluşur.

(2) Üyelerin yükseköğrenim görmüş ve öğretim kurumlarında en az on yıl öğretim üyeliği yapmış veya özel veya kamu hizmetinde en az on yıl fiilen çalışmış olmaları şarttır.

(3) Kurul üyeliğine önerilen adayların muvafakatleri aranır.

(4) Kurul Başkanını Bakanlar Kurulu seçer. Başkan vekili, Kurul tarafından yapılacak bir seçimle kendi üyeleri arasından üye tamsayısının salt çoğunluğuyla seçilir.

Görev süreleri

MADDE 28- (1) Kurul üyelerinin görev süresi altı yıldır. Görev süresi bitenler yeniden seçilemez.

(2) Başkanlık ve üyelikler görev süreleri dolmadan herhangi bir sebeple boşaldığı takdirde, boşalan yerlere bir ay içinde 27 nci madde hükümlerine göre, seçim yapılır. Bu şekilde seçilen kişiler yerine atandıklarının süresini tamamlar ve bu şekilde seçilenlerden iki yıl veya daha az süreyle görev yapanlar bir defalığına tekrar seçilebilir.

(3) Kurul Başkan ve üyelerinin görev süreleri dolmadan görevlerine son verilemez. Ancak seçilmeleri için gerekli şartları taşımadığı anlaşılan, görevleri ile ilgili olarak işledikleri suçlardan dolayı haklarında verilen mahkûmiyet kararı kesinleşen Kurul Başkan ve üyeleri süreleri dolmadan Başbakanın onayı ile görevden alınır. Bu durumda en geç bir ay içinde başkan veya üye seçimi yapılır.

Yemin

MADDE 29- (1) Kurul üyeleri, Yargıtay Birinci Başkanlık Kurulu huzurunda, "Üstlendiğim görevi Anayasa ve kanunlar gereğince tam bir dikkat,

dürüstlük ve tarafsızlıkla yürüteceğime namusum ve şerefim üzerine yemin ederim." şeklinde yemin ederler. Yemin için yapılan başvuru Yargıtayca acele işlerden sayılır. Kurul üyeleri, yemin etmedikçe göreve başlayamaz.

Kurulun çalışma esasları

MADDE 30- (1) Kurul ayda en az iki defa olmak üzere, gerekli hallerde Başkanın veya Başkanın bulunmadığı durumlarda Başkan vekilinin çağrısı üzerine, Başkan dahil en az beş üye ile toplanır ve üye tam sayısının salt çoğunluğuyla karar alır. Kurul üyeleri çekimser oy kullanamaz.

(2) Başkan ve üyeler kendilerini, üçüncü dereceye kadar kan ve ikinci dereceye kadar kayın hısımlarını, evlatlıklarını ve aralarındaki evlilik bağı kalkmış olsa bile eşlerini ilgilendiren kararlarla ilgili toplantı ve oylamaya katılamaz.

(3) Kurul üyeleri çalışmaları ve denetlemeleri sırasında ilgililere ve üçüncü kişilere ait öğrendikleri sırları bu konuda kanunen yetkili kılınan mercilerden başkasına açıklayamazlar ve kendi yararlarına kullanamazlar. Bu yükümlülük görevden ayrılmalarından sonra da devam eder.

(4) Bu maddede belirtilen haller dışında bir nedenle bir takvim yılında üç toplantıya katılmayan üyeler üyelikten çekilmiş sayılır.

(5) Kurul üyelerine 10/02/1954 tarihli ve 6245 sayılı Harcırah Kanunu hükümleri saklı kalmak kaydıyla fiilen görev yaptıkları her gün için uhdesinde kamu görevi bulunup bulunmadığına bakılmaksızın (3000) gösterge rakamının memur aylık katsayısı ile çarpımı sonucu bulunacak miktarda huzur hakkı ödenir. Bu ödemelerde damga vergisi hariç herhangi bir kesinti yapılmaz. Bir ayda fiilen görev yapılan gün sayısının dördü aşması halinde, aşan günler için huzur hakkı ödenmez.

(6) Kurul tarafından alınan kararların yürütülmesi Başkana, yokluğunda vekiline aittir.

(7) Kurulun sekretarya hizmetleri Başbakanlık tarafından yerine getirilir.

(8) Kurulun görev ve çalışmalarına ilişkin esas ve usuller yönetmelik ile düzenlenir.

Kurulun görev ve yetkileri

MADDE 31- (1) Kurulun görev ve yetkileri şunlardır:

a) Kişilik hakları ihlâl edilenlerin başvuruları hakkında karar vermek,

b) İlgili kişi bakımından telâfisi güç veya imkânsız bir zararın doğması ihtimalinin bulunması halinde geçici önlemler almak,

c) Kişisel verilerin işlenmesine ilişkin konularda düzenleyici işlemleri hazırlamak,

ç) Yabancı ülkelere veri aktarımı konusunda tereddüt bulunması hâlinde karar vermek,

d) Başkanın sunduğu önerileri karara bağlamak,

e) Kurul faaliyetleri hakkında yıllık rapor hazırlamak,

f) Sicilin tutulmasını sağlamak,

g) Yurtiçi ve yurtdışında verilerin korunması makamları ile işbirliği yapmak,

ğ) Veri koruma hukuku alanındaki gelişmeleri takip etmek ve bunların uygulanması için gerekli önlemleri almak,

h) İhtiyaç duyulan alanlarda ulusal ve uluslararası kurum ve kuruluşlarla işbirliği içinde araştırma ve teknik yardım projeleri hazırlamak, geliştirmek ve yürütmek,

ı) Kanunlarda verilen diğer görevleri yerine getirmek.

ÜÇÜNCÜ BÖLÜM
Şikâyet ve inceleme usulü

Şikâyet başvurusu

MADDE 32- (1) Bu Kanunun uygulanmasından kaynaklanan şikâyetler dilekçeyle şikâyet konusu işlemin yapıldığı veya öğrenildiği tarihten itibaren altmış gün içinde Kurula yapılır. Kurul şikâyeti üç ay içinde inceler. Ancak hukukî veya fiili sebeplerle bu süre içerisinde incelemenin sonuçlandırılamaması hâlinde süre, bir defaya mahsus olmak üzere üç ay daha uzatabilir. Şikâyetin 12 nci maddenin üçüncü fıkrasına veya 22 nci maddenin birinci fıkrasının (a) bendinde sayılan hallere ilişkin olmadığı ya da (c) bendinde belirtilen görevlerin yerine getirilmesini engellemediği sürece, işlem sonucunu ilgililere tebliğ eder.

(2) Şikâyet başvurusunda bulunanlar, şikâyet konusunda Kurulca verilen kararın kendilerine tebliğinden itibaren altmış gün içinde idare mahkemelerinde dava açabilirler. Kişilik hakları ihlal edilenlerin, genel hükümlere göre zararını tazmin hakkı saklıdır.

İnceleme usul ve esasları

MADDE 33- (1) Kurul, re'sen veya ilgili tarafların başvurusu üzerine bu Kanunun uygulanması ile ilgili konuları inceler.

(2) Veri kütüğü sahibi, Kurulun istemi üzerine, inceleme konusuyla ilgili bilgi ve belgeleri onbeş gün içinde göndermek ve yerinde inceleme yapılmasına imkan sağlamakla yükümlüdür.

(3) İnceleme sonucunda bu Kanun hükümlerinin ihlâl edildiğinin anlaşılması hâlinde, Kurul, veri kütüğü sahibinden bu Kanun hükümlerine uygun olarak kişisel verilerin işlenmesini ister. Bu istem, derhal yerine getirilir.

(4) Veri kütüğü sahibi kamu tüzel kişisi ise, Kurul, ilgili kamu tüzel kişisinden verilerin bu Kanun hükümlerine uygun olarak işlenmesini ister. Bu istem, en geç otuz gün içinde yerine getirilir.

(5) 22 nci maddenin birinci fıkrasının (a) ve (c) bentlerinde sayılan hallerde Kurul, üyelerinden birini ilgili kurumda incelemelerde bulunmak üzere görevlendirir. Görevlendirilen üye, inceleme sonucunda Kurula sözlü olarak bilgi verir.

(6) Kurul, telafisi güç veya imkansız zararların doğması ihtimali ve açıkça hukuka aykırılık halinde ilgili kişi hakkında veri işlenmesinin veya yurtdışına aktarımının durdurulmasına karar verebilir.

BEŞİNCİ KISIM
Çeşitli Hükümler
BİRİNCİ BÖLÜM
Soruşturma ve Kovuşturma Hükümleri

Kişisel verilerin hukuka aykırı olarak işlenmesi

MADDE 34- (1) Hukuka aykırı olarak üçüncü fıkrada belirtilenler dışında kişisel verileri işleyen kişi, Türk Ceza Kanununun 135 inci maddesinin birinci fıkrasına göre cezalandırılır.

(2) Birinci fıkrada yazılı fiilin, bu Kanunun 7 nci maddesinde düzenlenen özel niteliği olan kişisel veriler hakkında işlenmesi hâlinde de birinci fıkrada belirtilen cezaya hükmolunur.

(3) Hukuka aykırı olarak kişisel verileri açıklayan, yayan, bir başkasına veren, aktaran veya ele geçiren kişi Türk Ceza Kanununun 136 ncı maddesine göre cezalandırılır.

(4) Yukarıdaki fıkralarda belirtilen fiillerin Türk Ceza Kanunun 137 nci maddesinde belirtilen şekilde işlenmesi halinde ceza, aynı maddeye göre tayin edilir.

(5) 25 inci maddeye aykırı hareket edenler Türk Ceza Kanununun 138 inci maddesine göre cezalandırılır.

Verilerin korunması ve yok edilmesi görevinin ihmali

MADDE 35- (1) Kanuna uygun olarak veri kütüğüne işlenmekle beraber bunların muhafazalarında veya kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmek yükümlülüğünde ihmalleri görülenler, Türk Ceza Kanununun 138 inci maddesine göre cezalandırılır.

Tüzel kişiler hakkında güvenlik tedbiri uygulanması

MADDE 36- (1) Bu Kanunda tanımlanan suçların bir tüzel kişinin faaliyeti çerçevesinde işlenmesi halinde, ilgili tüzel kişi hakkında Türk Ceza Kanununun tüzel kişilere özgü güvenlik tedbirlerine hükmolunur.

İdarî para cezaları

MADDE 37- (1) Bu Kanunun;

a) 11 inci, 12 nci, 15 inci, 19 uncu ve 33 üncü maddeleri ile 26 ncı maddesinin üçüncü fıkrasında öngörülen yükümlülüklere aykırı hareket edenlere beşbin Türk Lirası,

b) 16 ncı, 21 inci ve 24 üncü maddelerinde öngörülen yükümlülüklere aykırı hareket edenlere onbin Türk Lirası,

idarî para cezası verilir.

(2) Bu Kanuna göre idarî para cezaları Kurul tarafından verilir.

(3) Bu maddedeki fiillerden özel hukuk tüzel kişileri de sorumludur.

İKİNCİ BÖLÜM
Son Hükümler

Yıllık faaliyet raporu

MADDE 38- (1) Kurul, faaliyetlerine ilişkin olarak her yılın Mart ayı sonuna kadar bir önceki yıla ait kararları, yaptığı düzenlemeleri ile bunların ekonomik ve sosyal etkilerini analiz eden bir faaliyet raporu hazırlar. Faaliyet raporu, ayrıca, Kurulun performans hedefleri ile uygulama sonuçlarının karşılaştırılmasını ve değerlendirilmesini de içerir.

(2) Yıllık faaliyet raporu ve Kurul kararları elektronik ortamda erişime açılır.

Yönetmelik

MADDE 39- (1) Bu Kanunun uygulanmasına ilişkin yönetmelikler, ilgili kurum ve kuruluşların görüşleri alınarak Kurul tarafından hazırlanır ve Başbakanlık tarafından yürürlüğe konulur.

GEÇİCİ MADDE 1- (1) Kişisel verileri işleyen kamu kurum veya kuruluşları ile gerçek ve özel hukuk tüzel kişileri, ilgili yönetmeliğin yürürlüğe girmesinden sonra üç ay içinde Sicile kayıt başvurusunda bulunmak zorundadırlar. Yönetmeliğin yürürlüğe girdiği tarihten itibaren bir yıl süreyle 19 uncu maddenin ikinci fıkrası uygulanmaz.

Yürürlük

MADDE 40- (1) Bu Kanun yayımı tarihinde yürürlüğe girer.

Yürütme

MADDE 41- (1) Bu Kanun hükümlerini Bakanlar Kurulu yürütür.

KAYNAKLAR

AICHHOLZER, Georg, H. BURKERT, *Public Sector Information in the Digital Age*, Edward Elgar Publishing Ltd., 28 February 2005'ten Charles D. RAAB, "Privacy Issues as Limits to Access", pp. 23-48.

AB Müktesebatının Üstlenilmesine İlişkin Türkiye Ulusal Programı, Cilt 1, 2001, (çevrimiçi) http://www.abgs.gov.tr/index.php?p=195&l=1, 26 Ocak 2009.

AKİPEK ÖCAL, Şebnem, "Elektronik Ticarette Sözleşme-Mesafeli Sözleşmelere İlişkin AB Direktifleri Çerçevesinde", Bilişim Teknolojileri ve Hukuk Semineri, 16 Mart 2001, (çevrimiçi) http://enoter_hukuk.tripod.com/tubitak_sozlesme.htm, 11 Eylül 2009.

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

ALTUNDİŞ, Mehmet, "Bağımsız İdari Otoritelerin Türk Hukuku'nda Ortaya Çıkardığı Sorunlar ve Türk Hukuku'na Etkileri", 2006, (çevrimiçi) http://www.danistay.gov.tr/makale_mehmet_altundis113.htm, 27 Ağustos 2009.ARİFOĞLU, Ali, *e-Dönüşüm Yol Haritası, Dünya, Türkiye*, 1. Baskı, sas Bilişim, Ankara, 2004.

Australian Government, Office of the Privacy Commissioner, *The Operation of the Privacy Act Annual Report*, 1 July 2007-30 June 2008, Sydney, 2008.

Austrian Data Protection Commission, Hyperlinks of Data Protection Authorities, (çevrimiçi) http://www.dsk.gv.at/site/6280/default.aspx, 11 Şubat 2010.

BAĞCI, Hasan, "Yolsuzluklarla Mücadelede Veri Madenciliği", Nisan 2009, (çevrimiçi) http://www.alomaliye.com/2009/hasan_bagci_yolsuzlukla.htm, 18 Kasım 2009.

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

BECENİ, Yasin, "Siber Uzayda Mahremiyet", II. Türkiye Bilişim Şurası Hukuk Çalışma Grubu, Mart 2004, (çevrimiçi) http://www.bilisimsurasi.org.tr/hukuk/docs/siber_uzayda_mahremiyet.pdf, 22 Ocak 2009.

Birleşmiş Milletler, *İnsan Hakları Evrensel Beyannamesi*, 10/12/1948, Office of the High Commissioner for Human Rights, (çevrimiçi) http://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/trk.pdf, 10 Şubat 2010.

BYGRAVE, Lee A., *Data Protection Law Approaching Its Rationale, Logic and Limits,* Kluwer Law International, 2002, The Hague, London, New York.

Caprioli, E., Y. SAADOUN, I. CANTERO, "The Right To Digital Privacy: A European Survey", *Rutgers Journal of Law & Urban Policy*, Vol. 3:2, 2006, pp. 211-218, (çevrimiçi)

http://www.rutgerspolicyjournal.org/journal/vol3no2/Caprioli_Saadoun_Cantero_European_Overview.pdf, 18 Aralık 2009.

CNIL, (Commission nationale de l'informatique et des libertés), *2007 Annual Activity Report,* (çevrimiçi) http://www.cnil.fr/fileadmin/documents/en/CNIL-AnnualReport-2008.pdf, 9 Şubat 2010.

Commission of the European Communities, *COM (2001) 298 final, Network and Information Security: Proposal for A European Policy Approach*, Brussels, 06/06/2001, (çevrimiçi)

http://www.justice.gov/criminal/cybercrime/intl/netsec_comm.pdf, 9 Şubat 2010.

Commission of the European Communities, *COM (2007)228 final, Communication from the Commission to the European Parliament and the Council on Promoting Data Protection by Privacy Enhancing Technologies (PETs),* Brussels, 2/05/2007, (çevrimiçi) http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0228:FIN:EN:PDF 7 Ocak 2010.

Council of Europe, *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, (ETS 108), Strasbourg, 28 January 1981, (çevrimiçi)

http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm, 23 Kasım 2008.

Council of Europe, *Convention on Cybercrime*, 23.11.2001, (çevrimiçi) http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm, 9 Şubat 2010. (Bu metnin Türkçe çevirisi İnternet ve Hukuk Platformu (İvHP) tarafından yapılmıştır. Çeviri için bkz. http://www.ivhp.org.tr)

Council of Europe, Human Rights and Legal Affairs, National Laws, (çevrimiçi) http://www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/documents/national%20laws/1NATIONAlLAWS_en.asp#TopOfPage, 10 Şubat 2010.

Council of Europe, *Recommendation Rec(2006)4 of the Committee of Ministers to member states on research on biological materials of human origin*, 15 March 2006, (çevrimiçi) https://wcd.coe.int/ViewDoc.jsp?id=977859, 9 Şubat 2010.

Council of Europe, *Resolution 1165 (1998) of the Parliamentary Assembly on Right to Privacy*, 26 June 1998, (çevrimiçi) http://assembly.coe.int/main.asp?Link=/documents/adoptedtext/ta98/eres1165.htm#_ftn1, 9 Şubat 2010.

Council of Europe, *Resolution 428 (1970) of the Parliamentary Assembly containing a declaration on mass communication media and human rights*, 23 January 1970, (çevrimiçi)

http://assembly.coe.int//main.asp?link=http://assembly.coe.int/Documents/AdoptedText/TA70/ERES428.htm#1, 9 Şubat 2010.

Devlet Planlama Teşkilatı, *AB Sözlüğü*, (Avrupa Birliği ile İlişkiler Genel Müdürlüğü çalışanlarının katkılarıyla K. Ecevit, Ö. Kavalalı ve S. Özdemir tarafından hazırlanmıştır), Ekim 2004, (çevrimiçi) http://ekutup.dpt.gov.tr/ab/sozluk.pdf, 9 Şubat 2010.

Devlet Planlama Teşkilatı, *Bilgi Toplumu Stratejisi (2006-2010) ve Eylem Planı*, 28 Temmuz 2006, (çevrimiçi) http://www.bilgitoplumu.gov.tr/, 9 Şubat 2010.

Devlet Planlama Teşkilatı, *Dokuzuncu Kalkınma Planı (2007-2013)*, Ankara, 2007, (çevrimiçi) http://ekutup.dpt.gov.tr/plan/plan9.pdf, 9 Şubat 2010.

Devlet Planlama Teşkilatı, *e-Dönüşüm Türkiye Projesi Kısa Dönem Eylem Planı (2003-2004)*, Ankara, Eylül 2004, (çevrimiçi) http://www.bilgitoplumu.gov.tr/Documents/1/KDEP/050000_E-DonusunTurkiyeKDEP.doc, 9 Şubat 2010.

Devlet Planlama Teşkilatı, *Sekizinci Beş Yıllık Kalkınma Planı (2001-2005),* Ankara, 2000, (çevrimiçi) http://www.dpt.gov.tr/DPT.portal, 9 Şubat 2010.

Devlet Planlama Teşkilatı, *Türkiye İçin Katılım Ortaklığı Belgesi,* Ankara, Nisan 2003, (çevrimiçi) www.dpt.gov.tr/DocObjects/.../987/KatlmOrtaklıBelgeleri2003.pdf, 15 Ekim 2009.

DİNÇ, Engin, "Kişisel Verilerin Korunmasında Uluslararası Düzenlemeler ve Türkiye'nin Durumu", (Dicle Üniversitesi Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi), Diyarbakır, 2006.

DRUCKER, Peter F., *Değişim Çağının Yönetimi,* çev. Zülfü Dicleli, Türk Henkel Dergisi Yayınları, İstanbul, 1995.

DRUCKER, Peter F., *Kapitalist Ötesi Toplum*, çev. Belkıs Çorakçı, İnkılap Kitabevi, İstanbul, 1993.

EPIC, *Privacy and Human Rights 2003, An International Survey of Privacy Laws and Developments,* USA, 2003.

EPIC (Electronic Privacy Information Center), *Records, Computers and the Rights of Citizens, Secretary's Advisory Comittee on Automated Personal Data Systems,* July 1973, DHEW Publication No (OS) 73-94, Washington, D.C., (çevrimiçi) http://epic.org/privacy/hew1973report/, 9 Şubat 2010.

ERTURGUT, Mine, *Medeni Usul Hukukunda Elektronik İmzalı Belgelerin Delil Olarak Değerlendirilmesi*, Yetkin Yayınları, Ankara, 2004.

European Commission, Flash Eurobarometer, *Data Protection in the European Union-Citizens' Perceptions*, February 2008, (çevrimiçi) http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf, 9 Şubat 2010.

European Commission, *(COM(2007)663) Turkey 2007 Progress Report*, 6.11.2007, (çevrimiçi)

http://ec.europa.eu/enlargement/pdf/key_documents/2007/nov/turkey_progress_reports_en.pdf, 9 Şubat 2010.

European Commission, *COM(2006)649 Turkey 2006 Progress Report*, 8.11.2006. (çevrimiçi) http://ec.europa.eu/enlargement/pdf/key_documents/2006/nov/tr_sec_1390_en.pdf, 9 Şubat 2010.

European Commission, "Justice and Home Affairs, Data Protection" (çevrimiçi) http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm, 11 Şubat 2010.

European Commission, "Analysis and impact study on the implementation of Directive EC 95/46 in Member States", (çevrimiçi) http://ec.europa.eu/justice_home/fsj/privacy/docs/lawreport/consultation/technical-annex_en.pdf, 2003.

European Court of Human Rights, *Case of Klass and others v. Germany*, Strasbourg, 6 September 1978, (çevrimiçi) http://cmiskp.echr.coe.int/tkp197/view.asp?item=1&portal=hbkm&action=html&highlight=klass&sessionid=41003495&skin=hudoc-en, 23 Aralık 2009.

Europe Direct, *Data protection in the European Union, Dialogue with citizens and business, EN/IRL*, 2000, (çevrimiçi) http://ec.europa.eu/justice_home/fsj/privacy/docs/guide/guide-ireland%20%20_en.pdf, 9 Şubat 2010.

European Parliament and of the Council, *Directive 95/46/EC on the Protection of individuals with regard to the processing of personal data and on the free movement of such data*, 24.10.1995, (çevrimiçi) http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf, 15/08/2008.

FAHSI, Par Magda, *A divided Europe wants to protect its personal data wanted by the US*, Rue 89, 04.03.2008, (çevrimiçi) http://www.rue89.com/2008/03/04/a-divided-europe-wants-to-protect-its-personal-data-wanted-by-the-us, 4 Aralık 2008.

Finland, Office of The Data Protection. "Privacy is Your Personal Right", (çevrimiçi) http://www.tietosuoja.fi/uploads/qz41ii.pdf, 11 Şubat 2010.

FRIEDMAN, Thomas L., *Dünya Düzdür*, çev. Levent Cinemre, I. Basım, Boyner Yayınları, İstanbul, Şubat 2006.

GOLDIROVA, Renata, "Brussels attacks new US security demands", 14.02.2008, http://euobserver.com/9/25657, 10 Şubat 2010.

GÜR, İkbal, *Kişisel Verilerin Korunması Hususunda AB ile ABD Arasında Çıkan Uyuşmazlıklar ve Çözüm Yolları*, Turhan Kitabevi, Ankara, Şubat 2010.

International Chamber of Commerce, *Privacy Toolkit*, Paris, November 2003, (çevrimiçi)http://www.iccwbo.org/home/e_business/word_documents/TOOLKIT-rev.pdf, 9 Şubat 2010.

International Conference of Data Protection Commissioners, "Criteria and Rules for Credentials Committee and the Accreditation Principles", 9-11 September

2002, (çevrimiçi) http://www.privacyconference2003.org/pdf/Criteria_and_Rules.pdf, 9 Şubat 2010.

International Covenant On Civil And Political Rights, 16 Aralık 1966, (çevrimiçi) http://ec.europa.eu/justice_home/fsj/privacy/docs/16-12-1996_en.pdf, 9 Şubat 2010.

KARA, G., A.F. AYSAN, L. YILDIRAN, A.N. MÜSLİM, U. DUR, "Türkiye'de Kredi Kartı Sektöründe Yasal Düzenlemeler ve Rekabet", *İktisat İşletme ve Finans,* Cilt: 23, Sayı: 265, Nisan 2008, ss. 34-49. (İngilizce, "Regulations and Competition in Credit Card Market in Turkey", (çevrimiçi) http://www.unc.edu/~gkara/regulations%20price%20competition.pdf, 9 Şubat 2010.

KELLECİ, Mehmet Ali, *Bilgi Ekonomisi, İşgücü Piyasasının Temel Aktörleri ve Eşitsizlik: Eğilimler, Roller, Fırsatlar ve Riskler,* DPT Yayın No: 2674, Temmuz 2003.

KETİZMEN, Muammer, Türk Ceza Hukukunda Bilişim Suçları, 1. Baskı, Ankara, 2008.

KUNER, Christopher, *European Data Protection Law: Corporate Compliance and Regulation*, Oxford University Press, second edition, 2007.MILLER, Arthur R., The Assault on Privacy, University of Michigan Pres, Ann Arbor, 1971.

NAGPAL, Rohas, "What is a Trojan?", December 2005, (çevrimiçi) http://www.webmasterdigest.com/print/366.html, 9 Şubat 2010.

OECD, *Declaration on Transborder Data Flows*, 11 April 1985, (çevrimiçi) http://www.oecd.org/document/25/0,3343,en_2649_34255_1888153_1_1_1_1,00.html, 9 Şubat 2010.

OECD, *e-Devlet Çalışmaları TÜRKİYE*, Türkçe basım, Ankara, 2007.

OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,* Paris, 2002, (çevrimiçi) http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_119820_1_1_1,00.html, 9 Şubat 2010.

OECD, *Implementing the OECD Privacy Guidelines in the Electronic Environment*, *Focus on the Internet*, 1997.

OECD, *Ministerial Declaration on the Protection of Privacy of Global Networks*, 1998, (çevrimiçi) http://www.oecd.org/dataoecd/39/13/1840065.pdf, 9 Şubat 2010.

OECD, *Policy Guidance on Online Identity Theft*, June 2008.

OECD, *Privacy Online*, OECD Guidance on Policy and Practice, 2003.

OECD, *Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy*, 12 June 2007, (çevrimiçi) http://www.oecd.org/dataoecd/43/28/38770483.pdf, 9 Şubat 2010.

OECD, *Shaping Policies for the Future of the Internet Economy*, Ministerial Meeting Seoul, Korea, 17-18 Haziran 2008, (çevrimiçi) http://www.oecd.org/dataoecd/1/29/40821707.pdf, 9 Şubat 2010.

OECD, *The e-Government Imperative: Main Findings*, 2003.

ÖZDEMİR, Hayrünnisa, *Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması,* 1. Baskı, Seçkin Yayıncılık, Ankara, 2009.

ÖZTAN, Bilge, *Medeni Hukuk'un Temel Kavramları*, 18. Baskı, Ankara, 2005.

Pan American Health Organization, *The Regulation of Privacy and Data Protection in the Use of Electronic Health Information*, Washington, DC, 2001.

Ponemon Institute, "Fourth Annual US Cost of Data Breach Study", January 2009, (çevrimiçi) http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/2008-2009%20US%20Cost%20of%20Data%20Breach%20Report%20Final.pdf, 9 Şubat 2010.

Ponemon Institute, "2009 Annual Study: Cost of a Data Breach, Understanding Financial Impact, Customer Turnover, and Preventive Solutions", January 2010, (çevrimiçi) http://www.encryptionreports.com/download/Ponemon_COB_2009_US.pdf, 27 Ağustos 2010.

Privacy International, "Privacy and Human Rights 2005: An International Survey of Privacy Laws and Developments", 17/12/2007, (çevrimiçi) http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559063&als[theme]=Privacy and Human Rights 2004, 10 Şubat 2010.

PRIVIREAL, "History of Data Protection in the United States", 3 June 2005, (çevrimiçi) http://www.privireal.org/content/dp/usa.php, 9 Şubat 2010.

PRIVIREAL, "History of Data Protection in Germany", 31 October 2005, (çevrimiçi) http://www.privireal.org/content/dp/germany.php, 10 Şubat 2010.

Rand Europe, "Review of the European Data Protection Directive", 2009, (çevrimiçi) http://www.rand.org/pubs/technical_reports/2009/RAND_TR710.pdf, 9 Şubat 2010.

RISEPTIS (Advisory Board for Research & Innovation On Security, Privacy And Trustworthiness in the Information Society), "Trust in the Information Society", 2008 (çevrimiçi) https://trustworthyict.inteco.es/ , 9 Şubat 2010.

ROTENBERG, Marc, *The Privacy Law Sourcebook 2002: United States Law, International Law, and Recent Developments,* EPIC Publications, Washington DC, 2002.

SARIHAN, Tan Deniz, *Herkes İçin İnternet*, Sistem Yayıncılık, İstanbul, 1995. STEWART, Blair, "A Comparative Survey of Data Protection Authorities-Part 1: Form and Structure", *Australasian Legal Information Institute,* Vol. 11, No: 2, 2004, (çevrimiçi)

http://www.austlii.edu.au/au/journals/PLPR/2004/30.html#Footnote10, 9 Şubat 2010.

Symantec, *Report on the Underground Economy, July 07-June 08*, November 2008, (çevrimiçi) http://www.symantec.com/content/en/us/about/media/pdfs/Underground_Econ_Report.pdf, 9 Şubat 2010.

ŞANLISOY, S., ÖZCAN, A., "Türkiye'de Bağımsız Düzenleyici Kurumların Bağımsızlığı", *ESİAD Siyasa,* Yıl:2, Sayı:3-4, 2006, ss. 99-132, (çevrimiçi) http://www.econturk.org/sanlisoy2.pdf, 19 Temmuz 2010.

ŞİMŞEK, Oğuz, *Anayasa Hukukunda Kişisel Verilerin Korunması*, 1. Baskı, Beta Yayınları, İstanbul, Şubat 2008.

The Online Privacy Protection Act of 2003, California, (Code Section 22575-22579) (çevrimiçi) http://entrepreneurs.about.com/od/internetmarketing/i/caprivacyact.htm, 9 Şubat 2010.

The New York Times, "Tangled Up in Spam", February 9 2003, http://www.nytimes.com/2003/02/09/magazine/09SPAM.html?pagewanted=1, 11 Şubat 2010.

The Paris Principles, adopted by UN General Assembly Resolution 48/134 of 20 December 1993, (çevrimiçi) http://www2.ohchr.org/english/law/parisprinciples.htm, 10 Şubat 2010.

The World Bank, *Turkey Knowledge Economy Assessment Study,* March 2004, Washington, D.C.

THOMAS, Richard, M. Walport, "Data Sharing Review Report", 11 July 2008, (çevrimiçi) http://www.justice.gov.uk/docs/data-sharing-review-report.pdf, 9 Şubat 2010.

TOFFLER, Alvin ve Heidi, *Yeni Bir Uygarlık Yaratmak*, çev. Zülfü Dicleli, İnkılap Kitabevi, İstanbul, 1996.

TOPALOĞLU, Mustafa, *Bilişim Hukuku*, Adana, 2005.

TURHAN, Oğuz, "Bilgisayar Ağları ile İlgili Suçlar", (DPT Uzmanlık Tezi), Ankara, 2006.

Turkey Social News, "70 milyon kişinin vatandaşlık bilgisi sadece bin 500 TL", 11 Aralık 2009, (çevrimiçi) http://www.socialnewsturkey.com/2009/12/11/70-milyon-kisinin-vatandaslik-bilgisi-sadece-bin-500-tl/, 31 Aralık 2009.

TÜBİTAK, Avrupa Birliği 7. Çerçeve Programı, 10 Aralık 2009, (çevrimiçi) http://www.fp7.org.tr/home.do;jsessionid=38544C30FE7E9848A37691DC39D1FF2F?ot=1&sid=3100.

Türkiye'nin AB Müktesebatına Uyum Programı (2007-2013), (çevrimiçi) http://www.abgs.gov.tr/index.php?p=6&l=1, 9 Şubat 2010.

Türkiye Bilişim Derneği (TBD), Kamu Bilişim Platformu, *Kişisel Verilerin Korunması*, 2. Çalışma Grubu, Nisan 2008.

United Nations, *Guidelines for the Regulation of Computerized Personal Data Files Resolution no: A/RES/45/95*, 14 December 1990, (çevrimiçi) http://www.un.org/documents/ga/res/45/a45r095.htm, 9 Şubat 2010.

US Department of Commerce, *Safe Harbor Workbook*, 03/02/2005, (çevrimiçi) http://www.export.gov/safeharbor/sh_workbook.html, 28 Kasım 2008.

VERE, Angeline, "Legal and Regulatory Frameworks for the Knowledge Economy, Concept Paper" *United Nations Economic and Social Council*, 26 March 2009.

WESTIN, Alan F., *Privacy and Freedom*, New York, 1967.WTO, *General Agreement on Trade in Services,* Art. XIV(c)(ii), Part II. 24 June 2009, (çevrimiçi) http://www.wto.org/english/docs_e/legal_e/26-gats_01_e.htm.

YILDIRIM, Süreyya, "Bilgi Ekonomisi ve Bilgi Ekonomisinin Türkiye Açısından Değerlendirilmesi", *Sosyal Bilimler Dergisi*, ss. 106-124, (çevrimiçi) http://sbe.balikesir.edu.tr/dergi/edergi/c7s12/makale/c7s12m6.pdf, 31 Mayıs 2010.

YILMAZ, Davut, *HACKING Bilişim Korsanlığı ve Korunma Yöntemleri*, Hayat Yayıncılık, İstanbul, 2004.

ZEVKLİLER, A. ACABEY, M. B. GÖKYAYLA, *Medeni Hukuk*, Seçkin Yayınevi, Ankara, 1999.

DİZİN