SİYASET, EKONOMİ ve YÖNETİM ARAŞTIRMALARI DERGİSİ

RESEARCH JOURNAL OF POLITICS, ECONOMICS AND MANAGEMENT

October 2017, Vol:5, Issue:4 Ekim 2017, Cilt:5, Sayı:4

P-ISSN: 2147-6071 E-ISSN: 2147-7035

Journal homepage: www.siyasetekonomiyonetim.org

Türkiye'de Kişisel Verilerin Korunması Politikasının Analizi

An Analysis of Personal Data Protection Policy in Turkey

Prof. Dr. Önder KUTLU
Necmettin Erbakan Üniversitesi, Siyasal Bilgiler Fakültesi, Siyaset Bilimi ve Kamu Yönetimi Bölümü, okutlu@konya.edu.tr
Araş. Gör. Selçuk KAHRAMAN
Necmettin Erbakan Üniversitesi, Siyasal Bilgiler Fakültesi, Siyaset Bilimi ve Kamu Yönetimi Bölümü, skahraman@konya.edu.tr

DOI: https://doi.org/10.25272/j.2147-7035.2017.5.4.03

MAKALE BİLGİSİ

Makale Geçmişi:
Geliş 03 Temmuz 2017
Düzeltme Geliş 11 Eylül 2017
Kabul 12 Eylül 2017

Anahtar Kelimeler:
Kişisel verilerin korunması, Kişisel Verilerin Korunması Kurulu, Özel hayat, İnsan hakları, Türkiye'de kişisel verilerin korunması

ÖZET

Türkiye'de belli dönemlerde gündeme gelen vatandaşların devlet tarafından muhafaza edilen mahrem bilgilerinin korunması sorunsalı ile vatandaşların özel hayatlarının ihlaline yönelik bazı gelişmeler ve muhtemel sorunlar özellikle teknolojinin ileri boyutlara ulaştığı günümüzde oldukça önem arz etmektedir. Bununla birlikte küresel ölçekteki bilişsel ve teknolojik propaganda yöntemleri dikkate alındığında kamu güvenlik bürokrasisi ile işbirliği de yapılarak bir takım güvenlik risklerinin analizinin yapılması gerekmektedir.

Diğer yandan Avrupa Konseyi tarafından hazırlanarak 1 Ekim 1985 tarihinde yürürlüğe giren 108 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi, Türkiye tarafından onaylanmasına rağmen 30 Ocak 2016 tarihine kadar yürürlüğe koymayan tek ülke pozisyonundaydı. Nitekim bu sözleşme 6669 sayılı Kanun olarak Türkiye'de 18 Şubat 2016 tarihinde Resmi Gazete'de yayımlanarak yürürlüğe konulmuştur. Buna bağlı olarak da Türkiye'de kişisel verilerin işlenmesinin disiplin altına alınmasını ve başta özel hayatın gizliliği olmak üzere kişi hak ve hürriyetlerinin kamusal aktörlerce korunmasını hedefleyen Kişisel Verilerin Korunması Kurulu ihdas edilmiştir.

Bu çalışma, oldukça hassas ve tartışmalı olan bu soruna 1985-2016 arasındaki dönemi gözden geçirerek ve böylece bilgi teknolojileri ve bireylerin kişisel haklarından kaynaklanan organizasyonel ve işlevsel eşitsizlikler üzerinde durarak katkı sağlamaktadır. Çalışma ayrıca Türkiye'de ve başka ülkelerde edinilmiş olan aynı dersleri ön plana çıkarmayı amaçlamaktadır.

ARTICLE INFO

Article History:
Received 03 July 2017
Received in revised form 11 September 2017
Accepted 12 September 2017

Keywords:
Personal data protection, Personal Data Protection Board, Privacy, human rights, personal data protection in Turkey

ABSTRACT

Keeping personal data of individuals by the state is always controversial as the issue tends to involve certain illegal attempts deploying the information for other and unrelated purposes. Turkey has experienced a number of examples in which the individuals responsible for obtaining and classifying personal data conducted some misdoings in keeping privacy of information.

In addition, though the agreement protecting personal data kept automatically by the article of the 108 of the European Council was ratified by Turkey in October 1985, it had not been implemented by January 2016. This shows the slow pace of developments in paying attention to the individual rights of citizens in due time. For this purpose, the Board for the Protection of Personal Data was launched in February 2016. Therefore there is a growing need to examine different aspects of the subject matter and evaluate further the establishment of the Board.

This study aims to contribute to this delicate and rather questionable issue by reviewing the time period from 1985 to 2016 and therefore elaborating on the organizational and functional discrepancies stemming from the information technologies and individual rights of the persons. The paper intends also to highlight same lessons learnt from the country and elsewhere.

GİRİŞ

Kamu kurum ve kuruluşlarınca çeşitli iş ve eylemlerin elektronik cihazlar ve ağlar üzerinden yürütülmesi bazı riskleri beraberinde getirmektedir. Zararlı yazılımlar ve kötü niyetli kişilerce yapılan elektronik saldırılar kişisel, kurumsal ve kamusal verilerin gizliliğini zafiyete uğratmakta, bilgi erişimine denetimi zorlaştırmakta ve çeşitli güvenlik risklerini ortaya çıkarmaktadır. Bununla birlikte çeşitli iletişim araçlarına elektronik ağlar üzerinden zararlı kodların ve virüslerin ulaştırılması ve tedbir amaçlı tekniklerinin bilgisayar yazılımcılarınca geliştirilmesi, devletlerin yazılım şirketleri ile daha fazla işbirliği yapmasına, farklı yöntemler ve mekanizmalar üzerinde çalışmasına ortam hazırlamaktadır.

Özellikle bilgi ve iletişim teknolojilerinin hızla yaygınlaşması, internet başta olmak üzere farklı iletişim kanallarının ve çeşitli elektronik cihazların gündelik yaşamda daha fazla yer bulması, bilgiye erişimin, kişisel verilere farklı yollardan erişimin de kolaylaştığı dikkate alındığında en temel insan hakları arasında sayılan kişisel verilerin korunmasının ulusal ve uluslararası birtakım standartlarla birlikte ele alınmasını gerekli kılmaktadır.

Farklı ülkelerde ortaya çıkan kişisel verilerin hukuka uygun olmayan biçimlerde ilgisiz, hatta kötü niyetli kişilerin eline geçmesi ve yine hukuka aykırı biçimde kullanılması aslında bu konuda toplumda çok ciddi bir hassasiyet meydana getirmiştir. Küresel düzeyde Wikileaks hadisesi, Türkiye'de ise Ergenekon davaları olarak bilinen hukuki süreçlerde hukuki olmayan yol ve yöntemlerle kişilik haklarının ihlali bu konudaki mevzuatın oluşmasında katkı sağlamıştır.

Çalışmamızda kişisel verilerin korunmasına yönelik temel ilke ve yasal düzenlemeler çerçevesinde başta Avrupa ülkeleri olmak üzere dünyadaki ilgili gelişmelere de vurgu yapılarak Türkiye'de kişisel verilerin korunmasına yönelik çalışmalara, politikalara, Kişisel Verilerin Korunması Kurumu'nun yönetsel ve yapısal rol ve işlevlerine değinilecektir.

6698 sayılı Kanun'da kişisel veriler özel ve kamu sektörü ayrımına tabi tutulmamakla birlikte her iki sektör açısından farklı anlamlar taşıdığı açıktır. Bununla birlikte Avrupa Birliği'nin Türkiye'ye vize muafiyeti getirmesinden, çeşitli müzakere fasılların açılmasına kadar geniş bir alanda bir baskı faktörü olarak kişisel verilerin korunmasına yönelik yasal ve yönetsel düzenleme talep etmesi Türkiye'nin bu alandaki politikalarının ve yasal mevzuatının geliştirilmesinde başat rol oynamıştır. Bu açıdan belli bir süre Türkiye için kişisel veri politikalarında en önemli itici gücü Avrupa Birliği olmuştur.

Çalışmada, kişisel verilen korunması hakkı ile ilgili yasal mevzuat da dikkate alınarak, bu hakkın sağlıklı bir şekilde işletilebilmesinde kamu kurum ve kuruluşlarının ne yönde hareket etmeleri gerektiği, sınırları ve işletilme aşamasında hangi faktörlerin dikkate alınması gerektiği gibi boyutlar üzerinde durulacaktır. Ayrıca yeni bir kurum olarak ihdas edilen Kişisel Verilerin Korunması Kurulu'nun fonksiyonel denetim rolü ile bu kurumdan ilgililerin beklentileri de analiz edilecektir. Böylece Türkiye'de kişisel verilerin korunması yönelik yasal, yapısal ve yönetsel bir çerçeve ortaya konulmaya çalışılacaktır.

Henüz çalışma döneminin başında olan Kurul'un sağlıklı biçimde dizayn edilmesi, kuruluş felsefe ve ilkelerinin ilerleyen dönemlerde daha belirgin olarak kendini göstereceği gerçeğinden hareketle geniş çerçeveli bir mevzuat ve yapı analizi ortaya konulacaktır.

1. Kişisel Veri Kavramı

Kişisel veri kavramı 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 3/1. maddesinde 'kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi' olarak tanımlanmaktadır. Avrupa İnsan Hakları Sözleşmesi ile Avrupa İnsan Hakları Mahkemesi kararları da benzer bir tanımlama yapmaktadırlar (Başalp, 2004: 22). Bu kapsamındaki bilgi içerisinde resmi kimlik bilgileri, eğitim ve sağlık verileri, güvenlik bürokrasine ait kayıtlar, kişisel harcamalar, soysal medya araçlarındaki bilgiler, resimler ve fotoğraflar ile genel olarak siyasi ve inançsal olmak üzere özel nitelikli veriler yer almaktadır. Bu tür verileri hassas olan ve olmayan veriler olarak sınıflandırmak mümkündür. Nitekim Avrupa Birliği Veri Koruma Direktifi 8. maddesinde hassas bilgilerin işlenmesinin kural olarak yasal olduğu belirtilerek etnik köken, sağlık durumu, cinsel hayat, inanç, kanaatler vb. unsurlar öne çıkarılmaktadır (Şimşek, 2008: 121; Sert, 2016: 276-278). Ayrıca, hassas veriler ülkeden ülkeye

çeşitlenebilmektedir. Bunlar arasında sendika üyeliği, genetik veriler (Polonya), ten rengi, cinsel davranışlar, alkol ve uyuşturucu kullanımı (İzlanda), cinsel tercihler ve sosyal refah yardımları (Finlandiya), mahkûmiyet kararlarına ilişkin veriler (İngiltere) yer alabilmektedir. Ayrıca hassas veriler arasında biometrik veriler de oldukça önemlidir. Örneğin 2004 tarihli Slovenya Kişisel Veri Koruma Kanunu'nda biometrik özellikler, bütün insanların sahip olduğu fiziksel, fizyolojik ve davranışsal özelliklerden oluşmakta ve özellikle, parmak izi kullanımı, parmağın çizgilerinin kaydedilmesi, iris taraması, retinal tarama, yüz ile ilgili özellikleri kaydetme, bir kulağı kaydetme, DNA taraması ve yürüme tipi özellikleri kullanılabilmektedir (m. 6/21) (Kaya, 2011: 319). Bütün bunlar dikkate alındığında kişisel veriyi, kişileri belirlenebilir kılan her türlü bilgi olarak tanımlamak mümkündür (Kılınç, 2012: 1095).

Kişisel verilerin elde edilmesinden kullanımına kadar geçen süreç genellikle dört önemli aşama üzerinden şekillenmektedir. İlki verilerin toplanması, ikincisi verilerin birleştirilmesi ve depolanması, üçüncüsü verilerin analiz edilmesi ve aktarılması, dördüncüsü ise derlenen, saklanan ve analiz edilen bilginin toplanmasıdır (Şahbaz, Alpaslan ve Sökmen, 2014: 4-5). Bununla birlikte kişisel verilerin korunmasına dair ilkeleri ise dört başlık altında değerlendirmek mümkündür. Bu başlıklar altında kişisel verilerin "işlenmesi" ile ilgili kriterler, "veri"lerin taşıması gereken özellikleri, verinin ilişkilendirildiği "özne" ile olan hususlar ve son olarak "veri güvenliği"ne dair konular yer almaktadır (Akdağ, 2015: 29). Kuşkusuz bu ilkeler ve yaklaşımlar politik ve yönetsel açılardan ülkeden ülkeye farklılık gösterebilmektedir. Örneğin Avrupa Birliği belgeleri açısında kişisel verilerde gizlilik temel bir insan hakkı olarak görülürken Amerika Birleşik Devletleri'nde (ABD) bankacılık sektörünün ve şirketlerin kendi düzenlemeleri çerçevesinde ele alınmaktadır (Cate, 1998: 61; Karlıdağ, 2013: 128).

2. Kişisel Verilerin Korunması İhtiyacı

Kişisel verilerin aktarımı ve depolanması günümüzde oldukça kolaylaşmıştır. Bu açıdan verilerin kayıt altına alınması, depolanması ve kullanımı hem devlet kurumlarını hem de özel sektör kuruluşlarını ilgilendirmektedir (Bainbridge, 1997: 17). Ayrıca, bilişim teknolojilerindeki gelişmeler kişisel verilerin kayıt altına alınmasına ve korunmasına yönelik politikaların geliştirilmesinde veri koruma yasalarının düzenlenmesini beraberinde getirmekte hatta İtalya gibi bazı ülkeler ayrıntılı kişisel verilerin korunması yasaları hazırlamaktadır (DDK, 2013: 150-154).

1990'lı yıllardan itibaren internet ağlarının ve kullanımının yaygınlaşması ile mobil teknolojilerin hızlı bir biçimde gelişmesi, kişisel verilerin toplanmasını, depolanmasını, paylaşılmasını ve analiz edilmesini kolaylaştırmakla birlikte birtakım güvenlik tedbirlerinin alınmasını da gerekli kılmaktadır. İnternet ağları üzerinden kullanılan cihazların artması, milyarlarca sensörün dünyadaki neredeyse her hareketi kayıt altına alması, derlenen verilerin hacmini artırmaktadır. İnternet üzerindeki kişisel veri yazılı materyaller, ses kayıtları, görsel dosyalar, videolar, animasyonlar ve diğer interaktif materyallerden elde edilmekte ve sosyal medya ağları üzerindeki her türlü bilgi kişisel veriler arasında yer almaktadır. İnternet kullanıcılarının sayısı üç milyar kişiyi ve internet ekonomisinin hacmi dört trilyon doları aşmış durumdadır (Şahbaz, Alpaslan ve Sökmen, 2014: 2-3). Bu sebeple böyle büyük bir sektörde kişisel verilerin korunmasını ve özel hayatın gizliliğini tehdit edecek ve kaygılandıracak pek çok gelişme ortaya çıkmaktadır.

2008 yılı Avrupa Birliği İlerleme Raporu'nda kişisel bilgilerin korunması hususunda Türkiye'de tam bağımsız bir veri koruma merciinin kurulması ve denetçi mekanizmaların ihdas edilmesi gerektiği belirtilmiştir (COM, 2008: 69). Örneğin Avrupa Veri Koruma Denetçisi (*European Data Protection Supervisor*-EDPS), AB kurum ve organlarında kişisel verilerin işlenmesini denetlemekten sorumludur. Bununla birlikte Birlik düzeyinde kişisel verilerin korunması politikalarının geliştirilmesinde önemli roller üstlenmekte, ticari amaçlı verilerin korunmasında ve çeşitli veri koruma ihlali davalarında müdahil olarak yer alabilmektedir (Doğan, 2015: 39).

Avrupa Birliği 2013 yılı İlerleme Raporu'nda ise Türkiye'de veri koruması ile ilgili bir çerçeve kanunun bulunmaması eleştirilerek çeşitli alanlarda Avrupa Birliği ile Türkiye arasındaki işbirliğinin zedelendiği savunulmaktadır. İlave olarak, Türkiye'de Siber Güvenlik Kurulu'nun kurulmasına ve Ulusal Siber Güvenlik Stratejisi ve Eylem Planı'nın hazırlanmasına karşın başta e-ticaret alanında olmak üzere

kişisel veri koruması alanındaki yasaların çıkartılmaması bir eksiklik olarak değerlendirilmektedir (Babahanoğlu ve Örselli, 2016: 555). Aynı biçimde Türkiye'nin "Şartlı Erişime Dayalı Hizmetlerin Yasal Olarak Korunmasına ilişkin Avrupa Sözleşmesi"ne taraf olmaması da eleştirilmiştir. Örgütlü suçlarla mücadele konusunda ise Türkiye'de kişisel verilerin korunmasına ilişkin mevzuatın olmamasının ve farklı terörizm tanımlamalarının bulunmasının Europol ile operasyonel işbirliği anlaşması imzalanamamasına yol açtığı belirtilmektedir (COM, 2013: 69; Keser, Alpaslan ve Sökmen, 2014: 42).

Türkiye'de kişisel verilerin korunmasına yönelik politikaların gerekçelerinden birisi de ekonomik sebeplerledir. Örneğin 95/46/EC sayılı Avrupa Yönergesi'nin ilgili maddelerinde yer alan veri transferine engel durumlar Avrupa ülkeleri ile olan ticareti aksatabileceğinden İlerleme Raporlarındaki tavsiye ve eleştiriler dikkate alınarak bir çerçeve yasa çıkartılması oldukça önemli bir gelişme olmuştur. Türkiye'de müstakil bir kişisel veri koruma yasasının çıkartılması Üyelik müzakereleri ile yakından ilişkilidir (Korkmaz, 2016: 85). Hatta Türk vatandaşlarına vizesiz Avrupa imkanını sunacak olan anlaşmanın hayata geçirilmesi için Birlik tarafından Türkiye'ye şart koşulan yetmiş iki kriterden birisi de veri güvenliğine ilişkin reformlardır.

Günümüzde bilişsel alanda, elektronik ağlar üzerinden gerçekleşen kişisel verilerin ihlaline yönelik suçlarda artış görülmektedir. Bu bağlamda bir kamu politikası olarak kişisel verilerin korunmasına yönelik politika ve stratejilerin geliştirilmesi bir zorunluluk halini almıştır. Buna karşın 5237 Sayılı Türk Ceza Kanunu ile taraf olunan uluslararası hukuk belgeleri kişisel verilerin elektronik ortamlar ve araçlar üzerinden ilgili kişilerinin rızası dışında elde edilmesine yönelik pek çok düzenlemeyi içermiştir. Örneğin 6698 sayılı Kanun'un Resmi Gazete'de yayımlanan 30. maddesinde yer alan 5327 sayılı Kanun'un 243. maddesinde; *"Bir bilişim sisteminin kendi içinde veya bilişim sistemleri arasında gerçekleşen veri nakillerini, sisteme girmeksizin teknik araçlarla hukuka aykırı olarak izleyen kişi, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır."* hükmü yer alırken, yasak cihaz ve programlar başlıklı 245. maddesinde ise; *"Bir cihazın, bilgisayar programının, şifrenin veya sair güvenlik kodunun; münhasıran bu Bölümde yer alan suçlar ile bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçların işlenmesi için yapılması veya oluşturulması durumunda, bunları imal eden, ithal eden, sevk eden, nakleden, depolayan, kabul eden, satan, satışa arz eden, satın alan, başkalarına veren veya bulunduran kişi, bir yıldan üç yıla kadar hapis ve beş bin güne kadar adli para cezası ile cezalandırılır"* hükmü yer almaktadır.

Kişisel verilerin korunması literatüründe öne çıkan kavramlardan bir diğeri de bazı hassas kişisel verilerin ilgili kişinin kendisinde ya da başka bir mecrada bulunması durumunda ortadan kaldırılmasına yönelik "unutulma hakkı" olarak karşımıza çıkmaktadır (Stuart, 2014: 479-482). Kuşkusuz günümüzde internet ağları üzerinden arama motoru adı verilen mekanizmalar bulunmakta ve bunlar aracılığıyla kişisel verilerin belli süreler zarfında ve kişinin gelecek yaşamına olumlu katkıda bulunamayacağı bir veri haline gelmesi durumunda bu verilerin ilgili arama motorlarının sahipleri aracılığıyla ya da ilgili işletmelerce otomatik olarak silinmesi bir hak olarak kabul edilmiştir. Nitekim Avrupa Adalet Divanı'nın bir İspanyol avukatın bir mülk satışına ilişkin verilerinin açık talebine rağmen Google adlı arama motorunun işletmecileri tarafından silinmemesine ilişkin davada alınan karar bir emsal niteliğindedir. İspanyol yargı makamlarının Google'dan on altı yıl öncesine ait ilgili verilerin silinmesi yönünden karar çıkması üzerine Google temyize gitmiş ve sonunda dava Adalet Divanı'nı gündemine gelmiştir. Adalet Divanı 13 Mayıs 2014 tarihinde 95/46/EC Direktifi'ndeki hükümlere dayanarak üye devletlerin sorumluluklarına dair 6. maddesini de dikkate alarak sonradan ilgisiz hale gelen bu tür bilgilerin silinmesi yönünde karar vermiştir (Akgül, 2015: 30-32, 34-35).

3. Çeşitli Alanlarında Kişisel Verilerin Korunması Politikaları

Ulusal literatürde kişisel verilerin korunmasına yönelik çalışmalar özel hayatın gizliliği, bankacılık hizmetleri ve internet ağları üzerinden alışveriş yapılmasında karşılaşılan sorunlar üzerinden ele alınmaktadır. Bu yazında yeterince değinilmeyen bir husus kamu kurum ve kuruluşlarınca elde edilen verilerin, çeşitli siber saldırılar ya da iç ve dış birtakım tehditler üzerinden yasadışı olarak elde edilmesine yönelik ihlalleridir. Bu açıdan özellikle aile birliğini ve toplum düzenini bozacak sorunlar ile e-alışveriş ya da e-ticaret kullanımından kaynaklı sorunlara ek olarak yalnızca vatandaşların değil devlet

güvenliğini ilgilendiren kişisel verilerin korunmasına yönelik yasal ve yapısal çalışmalara ve politikalara da gereksinim duyulmaktadır.

Veri güvenliğine ilişkin yazılım, güvenlik sistemi, kriptolama vb. teknik tedbirler kadar verilerin depolandığı işyerinin ya da kuruluşun yönetim anlayışı, kurumsal kültürü, personel kaynakları vs. hususlar da güvenlik bağlamında çok boyutlu olarak ele alınmalıdır (Ersoy, 2006). Örneğin Türkiye'de üniversite kütüphaneleri üzerinde kişisel verilerin korunmasına ilişkin yapılan bir araştırmada, üniversite kütüphanelerinde kişisel verilerin elde edilmesine ilişkin yeterli kriter, standart ve düzenleme bulunmamakta ve kütüphane yönetici ve personeli kişisel verilerle ilgili mevzuatı yeterince bilmemektedir (Henkoğlu ve Özenç-Uçak, 2015: 55).

3.1. Özel Hayatın Gizliliği ve Kişisel Verilerin Korunması

Hukuk doktrinde genel kabule göre bir kişinin özel hayatına dair verilerin korunmasında üç türlü hayat çevresi bulunmaktadır. Bunlardan ilki yalnızca kişilerin kendileri ve yakınları (akrabaları, dostları vs.) tarafından bilinen özel hayatları, ikincisi kişilerin gizlilik alanlarına ve sırlarına, üçüncüsü ise kişilerin umumi ve kamuya anlatılmasında hukuka aykırılık olmayan hayatlarına ilişkin bilgileri kapsamaktadır (İmre, 1974: 148-149). Özel hayatın gizliliği temel bir insan hakkı olarak değerlendirilerek çeşitli uluslararası metinlerde ve anayasalarda güvence altına alınmış (Kılınç, 2012: 1091) olmasına karşın bilgi teknolojilerindeki gelişmeler, suç örgütleri, istihbarat servisleri ve çeşitli tehdit mekanizmaları gizliliği ihlal eden kişisel verilerin elde edebilmesine olanak sağlamaktadır.

Türk Ceza Kanununda özel hayatın gizliliğini sağlayan kişisel verilerin korunmasına yönelik çeşitli düzenlemeler yer almıştır. Haberleşme gizliliğinin ihlali konusunda, kişiler-arası haberleşme içeriklerini hukuka aykırı olarak ifşa eden kişilerin bir yıldan üç yıla kadar hapis cezası ile; kendisiyle yapılan haberleşmelerin içeriğini diğer tarafın rızası olmaksızın ifşa eden kişilerin ise altı aydan iki yıla kadar hapis veya adlî para cezası ile cezalandırılacakları kayıt altına alınmıştır (m. 132/2-3). 133. maddede ise "kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması" başlığı altında şu hükümler yer almıştır:

(1) Kişiler arasındaki aleni olmayan konuşmaları, taraflardan herhangi birinin rızası olmaksızın bir aletle dinleyen veya bunları bir ses alma cihazı ile kaydeden kişi, iki aydan altı aya kadar hapis cezası ile cezalandırılır.

(2) Katıldığı aleni olmayan bir söyleşiyi, diğer konuşanların rızası olmadan ses alma cihazı ile kayda alan kişi, altı aya kadar hapis veya adlî para cezası ile cezalandırılır.

(3) Yukarıdaki fıkralarda yazılı fiillerden biri işlenerek elde edildiği bilinen bilgilerden yarar sağlayan veya bunları başkalarına veren veya diğer kişilerin bilgi edinmelerini temin eden kişi, altı aydan iki yıla kadar hapis ve bin güne kadar adlî para cezası ile cezalandırılır. Bu konuşmaların basın ve yayın yoluyla yayınlanması halinde de, aynı cezaya hükmolunur.

Özel hayatın gizliliğinin ihlal edilmesine yönelik nedenler oldukça çeşitlenmiştir. Bunlardan birisi, e-posta kayıtları üzerinden evlilik birliğinin bozulması yahut haberleşme hürriyetinin ihlali nedeniyle hukuka aykırılığın doğması vs. deliller üzerinden kişisel verilerin kullanımı kural olarak kabul edilmemektedir. İkincisi, ses kayıtları üzerinden özel hayata dair kişisel verilerin genel boşanma nedenleri arasında gösterilmesinde Yargıtay'ın bir kararı dikkate alındığında mekan mefhumu ve ortak alanlar dikkate alınmakta ve hukuka aykırı delillerin niteliğinin değişebileceği görülmektedir. Üçüncüsü ise, sosyal medya ağları üzerindeki kişisel verilerin boşanma davalarında delil gösterilmesi hususudur. Buna göre Yargıtay bir kararında *"elektronik ortamdaki fotoğraf, film, görüntü veya ses kaydı gibi veriler ve bunlara benzer bilgi taşıyıcılar, diğer delillerle desteklendikleri takdirde "delil" olarak hükme esas alınabilir"* demektedir (Sert, 2016: 287-289).

3.2. E-Ticarette Kişisel Verilerin Korunması

Kişisel verilerin güvenliğine ilişkin tehditlerden birisi e-ticaret, e-alışveriş adı verilen ve bankacılık sektörünü de ilgilendiren bilgilerin elektronik program ve yöntemler aracılığıyla yasa dışı biçimde elde edilerek kullanılmasına ilişkindir (Ersoy, 2006). E-ticaretin yaygınlaşmasının önündeki engellerin

başında hukuki düzenlemelerdeki yetersizlikler gelmektedir. Nitekim, Gümrük ve Ticaret Bakanlığı'nın da bu durumu kabul ettiği belirtilmekle birlikte 1 Mayıs 2015 tarihinde yürürlüğe giren 6563 sayılı Kanunla e-ticaret yapan şirketlerin gizlilik kurallarını ve alternatif çözüm mekanizmalarına dair bilgileri ilan etmeleri yükümlülüğü getirilmiş ve Gümrük ve Ticaret Bakanlığı tarafından e-alışveriş sitelerine yönelik "güven damgası" sistemi oluşturulması hedeflenmiştir (Karlıdağ ve Bulut, 2015: 205).

E-alışveriş sunan internet sitelerinin tüketicilerin kişisel bilgilerinin korunmasına yönelik hassasiyetleri, sorumlulukları ve gizlilik politikalarının niteliği oldukça önem arz etmektedir. Bununla birlikte çevrimiçi perakendeci sitelerin müşteri hareketlerini mobil cihazındaki GPS ya da başka bir elektronik cihazındaki bağlantılar üzerinden müşterinin konum bilgilerinin tespit edilerek ona göre promosyon teklifleri sunma imkanına kavuştuğu bilinmektedir (Şahbaz, Alpaslan ve Sökmen, 2014: 4). E-alışverişe imkan sağlayan bazı şirketlerin kişisel veriler üzerinden kişilerin istemi ve rızası dışında kazanç sağlayabildikleri bilinmekte ve tüketicilere ait olan gizlilik, piyasada alıp satılan bir ticari meta haline dönüştürülmektedir.

Türkiye'de internet üzerinden alışveriş imkânı sunan elli adet şirketin gizlilik politikalarına yönelik sözleşme metinleri üzerinden bir çalışma hazırlanmıştır. Çalışmada, şirketlerin tamamının kendilerine ait verilerin korunması konusunda her türlü tedbiri aldıkları, şirketlerden on birinin üyelik bilgilerinin doğruluğunu garanti altına alacak sözleşme hükümlerine yer verdikleri, on şirketin sayfalarında güvenlik bildirimine yer veren bildirimlerde bulunduğu, on bir şirketin güvenlik uyarısında bulunduğu ancak sorumluluk almadığı ve elektronik ödemelerin korunamamasına yönelik ise sadece üç şirketin sorumluluk aldığı ortaya konulmuştur (Karlıdağ ve Bulut, 2015: 211-214).

3.3. Devlet Belgelerinde Kişisel Verilerin Korunması

Türkiye'de kamu hizmetinin görülmesinde kullanılmakta olan gizlilik ile ilgili en eski temel düzenlemenin Bakanlar Kurulu kararıyla yürürlüğe konulan ancak "hizmete özel" gizlilik derecesi taşıması sebebiyle Resmi Gazete'de yayımlanmayan 1964 tarihli Gizlilik Dereceli Evrak ve Gerecin Güvenliği Hakkında Esaslar olduğu görülmektedir. Kuşkusuz gizlilik derecesi, kamu hizmeti yürütülürken bilgiye yetkisiz erişimi engellemek ve ilgili ülkeye veya ilgili kişiye olası zararları önlemek hedefiyle kullanılan bir terim olarak belirtilebilir (Diri ve Gülçiçek, 2012: 497, 499). Kuşkusuz bu tür verileri Türkiye'de, özellikle kamu kurum ve kuruluşlarında çalışanlara yönelik kamu güvenliğini de dikkate alan güvenlik soruşturmaları üzerinden ele almak mümkündür. Bu bağlamda güvenlik soruşturmalarında elde edilen verilerin işlenmesi, birleştirilmesi, analiz edilmesi ve korunması oldukça önemlidir. Bununla birlikte bilgi sistemlerinin güvenliği tasarım aşamasından itibaren ele alınması ve bu çerçevede işlevsellik ile güvenlik arasındaki dengenin sağlanması da gerekmektedir (DDK, 2013: 777).

Yakın dönemlerde küresel çapta etki uyandıran, eski bir CIA ajanı tarafından yayımlanan ve "Wikileaks" adı verilen belgelerle sayısız kişisel gizliliği ve veri mahremiyeti eden bir vaka kamuoyuna yansıdı. Bu olayın yankıları halen devam etmektedir.

ABD örneğinde mahrem nitelikli devlet belgelerindeki kişisel verilerin korunmasına yönelik politikadan kısaca bahsetmek gerekirse; öncelikli olarak ABD'de kişisel verileri de içeren devlet verilerindeki sınıflandırma düzeyleri üç şekilde ele alınmaktadır. İlki yetkisiz açıklanması halinde milli güvenliği bir zarar vermesi beklenen "özel" nitelikli bilgilerdir. İkincisi açıklanması halinde milli güvenliği ciddi zarar vermesi beklenen "gizli" ibareli bilgilerdir. Üçüncüsü ise milli güvenliği çok olumsuz etkide bulunması beklenen "çok gizli" ibareli bilgilerdir. Ancak doğrudan kişilerin veya vatandaşların mahrem verilerinin yetkisiz bir biçimde açıklanmasını doğuracak hassas nitelikli veriler "Yalnızca Resmi Kullanım İçin" (For Official Use Only) ibaresi ile resmi belgelere yansımaktadır (Diri ve Gülçiçek, 2012: 504-505). Bu bağlamda az ya da çok gizli ibareli olması fark etmeksizin kişisel verilerin korunması hakkı her daim devam etmekte ve devlet bu tür verilerin korunmasında birincil sorumlu aktör olarak gerekli tedbirleri almakla mükelleftir.

Türkiye'de 2009 yerel seçimlerinde seçime katılan siyasi partilerle paylaşılan, kayıtlı tüm seçmenlerin kişisel verilerinin bir internet sitesi üzerinden belli bir ücret karşılığı erişime açılması örneğinde olduğu

gibi devlet belgelerinde yer alan kişisel verilerin korunmasında yeni tedbirlerin alınması zaruri hale gelmektedir (Karlıdağ, 2013: 146). Türkiye'de kişisel verilerin korunmasına yönelik önemli politikalar ve yasal anlamda ilkler Ak Parti Hükümetleri döneminde gerçekleşmiştir. Örneğin 30 Eylül 2012 tarihinde yayımlanan "Ak Parti 2023 Siyasi Vizyonu" başlıklı belgede kişisel verilerin korunmasına yönelik yasal düzenlemenin tamamlanacağı vaat edilmiş (2012: 28) ve 2016 itibariyle bu vaat yerine getirilmiştir. Kişisel verilerin korunması politikalarında önemli adımların atılması politik iktidarların ya da adaylarının yaklaşımları ile yakından ilgilidir. Bununla birlikte kişisel verilerin korunmasında yalnızca teknolojik tedbirler yeterli olmayıp devlet, özel sektör, yerel, ulusal ve uluslararası sivil toplum kuruluşları başta olmak muhtemel politika aktörü tüm taraflar ile birlikte meselenin teknik, yönetsel ve ekonomik boyutlarının dikkate alındığı kapsamlı bir yaklaşıma ihtiyaç bulunmaktadır (DDK, 2013: 787). Kişisel verilerin korunması noktasında Wikileaks olayının da gösterdiği gibi, ortaya çıkan ihlal ve skandallar veri güvenliği konusunda hassasiyetin artması sonucunu doğurmuştur.

3.4. E-Devlet Kurumlarında Kişisel Verilerin Korunması

Günümüzde modern devletin en önemli göstergelerinden biri olarak devletin kamu hizmetlerini dijital ortamda sunabilmesi ve devlet kurumlarında işlerin elektronik ortamda yürütülerek bürokrasinin en aza indirgenmesi gösterilmektedir (Eren ve Durna, 2005: 139). Kuşkusuz e-devlet kurumları üzerinden hizmet alımında çeşitli kişisel veriler kullanılmaktadır. Vatandaşların kişisel bilgilerinin büyük bir kısmı Merkezi Nüfus İdare Sistemi (MERNİS), Adrese Dayalı Nüfus Kayıt Sistemi (ADNKS) ve Tapu ve Kadastro Bilgi Sistemi (TAKBİS) üzerinde kayıtlıdır. Önceleri fiziki arşivlerde ve dosyalarda yer alan kişisel veriler elektronik devlet uygulamalarında yer almaya başlamıştır. Ancak, dijital ortamlarda kayıtlı ve depolanan verilerin korunmasına yönelik önlemler diğer teknolojik gelişmelerin tehlikesi altında kalmakta ve eski kayıt sistemi ile mukayese edilemeyecek ölçüde elektronik veri tabanları çeşitli saldırılarla ve tehditlerle karşı karşıya kalabilmektedir (Tataroğlu, 2013: 264). E-devlet uygulamaları üzerinde karmaşık teknolojilerin artması ile uzman teknokratlar ve teknik birimler üzerindeki denetim de zayıflayabilmektedir (DDK, 2013: 787-788). Hatta bazı teknokratların ya da ilgili birim uzmanlarının kendi değerleri ve anlayışları çerçevesinde kişisel verilerin korunmasını ihlal edici özellikleri ilgili sisteme uygulayabilmeleri ve niyetlerini gizlemeleri mümkün görülmektedir (Tataroğlu, 2013: 286). Bu sebeple e-devlet uygulamalarında yalnızca sistemin teknik boyutunun muhafazası değil personel kaynakları, kurum kültürü ve muhtemel diğer etmenlerin de kişisel verilerin korunmasında dikkate alınması gerekmektedir.

4. Dünyada Kişisel Verilerin Korunmasında Temel Çerçeve Düzenlemeler

Amerika Birleşik Devletleri'nde 1966 tarihli Bilgi Edinme Hakkı Kanunu (The Freedom of Information Act) ile 1974 tarihli Özel Yaşamın Gizliliği Kanunu (The Privacy Act) kişisel nitelikli hassas verilere yönelik doğrudan bir koruma getirmiştir (Kaya, 2011: 321). Kişisel verilerin korunmasında önemli belgelerden birisini de Ekonomik İşbirliği ve Kalkınma Örgütü (OECD) tarafından hazırlanan ve 1981'de kabul edilen "Mahremiyetin Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber Ülkeler" oluşturmaktadır (Ünver ve Kim, 2016: 6). Bununla birlikte Birleşmiş Milletler Genel Kurulu tarafından 1990'da "Bilgisayarla İşlenen Kişisel Veri Dosyaları Hakkında Yönlendirici İlkeler" başlığında bir düzenleme kabul edilmiştir (Kılınç, 2012: 1097).

Avrupa İnsan Hakları Sözleşmesi'nin 8. maddesi çerçevesinde, Avrupa Konseyi 1960'lı yıllardan itibaren bilgi teknolojileri alanındaki gelişmelerin de etkisiyle kişisel verilerin korunmasına yönelik çeşitli metinleri kabul etmiştir (Warner, 2005: 79). Bu metinler arasında kişisel verilerin korunmasına yönelik çalışmalardan en önemlisi Avrupa Konseyi tarafından hazırlanan ve 1981 yılında kabul edilen 28 Ocak 1981 tarihinde imzaya açılıp 1 Ekim 1985 tarihinde yürürlüğe giren 108 sayılı Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Kişilerin Korunmasına Dair Sözleşme'dir. Sözleşmenin en önemli özelliği, kişisel verilerin korunmasında bağlayıcılığı olan ilk uluslararası hukuki düzenleme olmasıdır. Düzenleme çeşitli zamanlarda güncellenmiştir. Güncellemeler arasında telekomünikasyon hizmetlerinde kişisel verilerin korunması (4 sayılı Tavsiye Kararı – 1995), tıbbi verilerin korunması (5 sayılı Tavsiye Kararı – 1997), istatistik amaçlı kayıt altına alınan kişisel verilerin korunması (18 sayılı Tavsiye Kararı – 1997), internet ağlarında kişisel verilerin korunması (5 sayılı Tavsiye Kararı – 1999), arama motorları üzerinde insan haklarının ve kişisel

verilerin korunması (3 sayılı Tavsiye Kararı – 2012) ve sosyal ağ hizmetleri üzerinde insan haklarının ve kişisel verilerin korunması (4 sayılı Tavsiye Kararı – 2012) vb. kararlar yer almaktadır (Doğan, 2015: 9-10).

Diğer yandan Cumhurbaşkanlığı Devlet Denetleme Kurulu'nun 2013 tarihli "Kişisel Verilerin Korunmasına İlişkin Ulusal ve Uluslararası Durum Değerlendirmesi ile Bilgi Güvenliği ve Kişisel Verilerin Korunması Kapsamında Gerçekleştirilen Denetim Çalışmaları" başlıklı raporda da 108 sayılı düzenlemenin önemine değinilmektedir (Keser, Kaya ve Kınıkoğlu, 2014: 40).

5. Avrupa Birliği Açısından Kişisel Verilerin Korunması

Avrupa Birliği'nin kişisel verilerin korunmasına yönelik politikalar geliştirmesinde en önemli etmenlerden birisi tarihsel tecrübeler olmuştur. Özellikle otoriter yönetimler döneminde her türlü kişisel verinin kötüye kullanımı söz konusu olabilmiştir. Bu bağlamda kişisel verilerin kötüye kullanımının da temeli kabul edilebilecek düzenleme Avrupa Konseyi tarafından 3 Eylül 1953 tarihinde yürürlüğe konulan İnsan Hakları ve Özgürlüklerinin Korunmasına İlişkin Avrupa Sözleşmesi'dir. Avrupa İnsan Hakları Sözleşmesi'nin "Özel ve Aile Hayatına Saygı Hakkı" başlıklı 8. maddesine göre herkesin özel hayatına, konutuna ve yazışmalarına saygı gösterilmesi gerekmekte, bu hakların ifasına yönelik bir kamu otoritesinin müdahale etme hakkının ise yasayla öngörülmesi, ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, suç işlenmesinin önlenmesi ve başkalarının hak ve özgürlüklerinin korunmasına yönelik olması gerekmektedir.

Avrupa ülkelerindeki özel hayatın gizliliği ve kişisel verilerin korunmasına yönelik hukuksal gelişmelerin 1970 yılı öncesi dönemde ilk olarak Almanya, İsviçre ve Fransa'da olduğu belirtilmektedir (İmre, 1974: 150-151). Avrupa'daki kişisel verilerin korunmasına yönelik mevzuatta ilk veri koruma yasası 1970 yılında Almanya'nın Hesse Eyaletinde yürürlüğe konulmuştur (Tortop, 2000: 2-3). 1973'te ise İsveç ilk ulusal veri gizliliği yasasını yürürlüğe koyarken Fransa'da ise kişilerin özel hayatlarının korunması ilişkin olarak "Law Concerning Data Processing, Files, and Liberty" adı verilen bir kanun 1978 yılında çıkartılmıştır. Bu ilk kişisel verilerin saklanması ve korunmasına yönelik yasal düzenlemelerin 1960'lı yıllar ve 1970'li yıllarda Amerika Birleşik Devletleri'ndeki düzenlemelerle paralel bir süreç izlediği belirtilmekte ve ABD'den etkilenilerek kişisel verilerin korunması veya gizlenmesi fikrinin Avrupa tarafından benimsendiği ifade edilmektedir (Reidenberg, 1999: 771, 782; Assey ve Eleftheriou, 2001: 148; Schriver, 2002: 2782).

Öte yandan 108 numaralı Sözleşme hükümlerini yorumlamak ve geliştirmek üzere bir Danışma Komitesi oluşturulmuş, bu Komite de 181 sayılı Ek Protokolü kabul etmiştir. Bu Protokol ile kişisel verilerin işlenmesini denetleyecek ve şikâyetleri soruşturabilecek biçimde yetkilendirilmiş bağımsız bir organ öngörülmüştür. Böylece önemli bir eksikliğin giderilmesine yönelik adım atılmıştır. Bununla birlikte AB perspektifinde kişisel verilerin korunmasına yönelik en önemli düzenlemelerden birisi "Avrupa Birliği Veri Koruma Direktifi 95/46/EC" olarak karşımıza çıkmaktadır (Warner, 2005: 78). Bu direktif belirli güncellemelere ihtiyaç duymuş ve hızla gelişen teknoloji karşısında mevzuat yenilemesi ve yeni politikaların geliştirilmesinde birtakım zorluklar meydana gelmiştir (Robinson, vd., 2009: 4; Koops, 2014: 250). Örneğin bankalar tarafından kurulan güvenlik sistemleri ile dijital imzalar hakkında Direktif'te bir kriter ya da bilgi bulunmamaktadır (D'afflitto, 1996: 313-314). 1995 tarihli Direktif'ten sonra 1997 ve 2002'de güncellenmiş veri koruma direktifleri de yayımlanmıştır. Diğer yandan 181 sayılı Ek Protokol'de yer alan bağımsız organın niteliği, 95/46/EC sayılı Yönerge'deki niteliklerle benzerlik göstermiştir. 181 sayılı Ek Protokol, Avrupa Konseyi tarafından 1 Temmuz 2004 tarihinde yürürlüğe konulmuştur (Doğan, 2015: 11).

Avrupa Birliği ülkelerindeki kişisel verilerin korunmasına yönelik önemli düzenlemelerden birisi olan Kişisel Verilerin İşlenmesi ve Bu Türdeki Verilerin Serbest Dolaşımı Bağlamında Bireylerin Korunmasına İlişkin 24 Ekim 1995 tarihli ve 95/46/EC sayılı Avrupa Parlamentosu ve Konseyi Yönergesi'nin ilk maddesi önemlidir. Buna göre üye devletlerin gerçek kişilerin temel hak ve özgürlükleri ile özellikle kişisel verilerin işlenmesine yönelik özel yaşamın gizliliği hakkını korumaları hedeflenerek kişisel verilerin korunmasının temel bir insan hakkı olduğu kabul görmüştür. Bununla birlikte Yönerge'nin uygulanmasına yönelik kısıtlılıklar ve istisnalar da öngörülmüştür. Kamu

güvenliği, savunma, devlet güvenliği ve ceza hukukuna ilişkin faaliyetlerde kişisel verilerin korunması sınırlandırılmıştır (Oxman, 200: 194; Doğan, 2015: 18-19). Ayrıca veri korunmasında sıkı tedbirler almayı amaçlayan AB, üye ülkelerin 95/46/EC sayılı Direktifi'nden önce sahip oldukları veri koruma rejimi Direktif'ten daha yüksek bir düzeyde koruma sağlıyorsa, bu korumayı devem ettirme hakkını da ilgili ülkelere tanımaktadır (Keser, Kaya ve Kınıkoğlu, 2014: 40). Aksi takdirde Direktif'i kabul eden ülkelerin kişisel verilerin korunmasına yönelik yasalarında Direktif'teki hükümleri dikkate alarak yeniden düzenlenme yapmaları istenmektedir (Ilana, 1996: 680).

6. Türkiye'de Kişisel Verilerin Korunmasına Yönelik Düzenlemeler

Türkiye'de kişisel verilerin korunmasına yönelik politikaların geliştirilmesi her şeyden önce bir anayasal hak olması çerçevesinde temel hak ve özgürlükler ile ilgili evrensel ölçütleri dikkate alan bir bakışa ihtiyaç duymaktadır. Bununla birlikte Türkiye ile Avrupa Birliği entegrasyon ve katılım müzakereleri bu politikaların benimsenmesinde oldukça etkili olmuş (Pehlivan, 2016), küresel gereklilikler ve ekonomik sebeplerle süreç daha da hızlanmıştır. Bu bağlamda Türkiye'nin AB ile müzakerelerinde 23. ve 24. Fasıllarının tamamlanabilmesi ve vize serbestliğine ilişkin süreci kişisel verilerin korunmasına ilişkin politikaların geliştirilmesi şartına bağlanmıştır.

Türkiye'de kişisel verilerin korunmasına yönelik müstakil bir kanun yapımı ve bir kurul ihdası uzun yıllar ertelenmiştir. Türkiye'de kişisel verilerin korunması ile ilgili doğrudan bir yasa hazırlanması için ilk kez 1989 yılında bir komisyon kurulmuş ancak komisyon çalışmalarını tamamlayamamıştır (Nebil, 2016). İkinci komisyon girişimi ise 2000'de olmuş ve Kişisel Verilerin Korunmasına Dair Bir Kanun Taslağı hazırlanmıştır. Taslak Anayasanın 17. maddesinde yer alan kişi dokunulmazlığı ilkesi ile 95/46/EC Avrupa Birliği Veri Koruma Direktifi çerçevesinde hazırlanmıştır. 7 Eylül 2003 tarihinde açıklanan Tasarı, AB İlerleme Raporları ile çeşitli eylem planlarında yer almasına karşın 2008 yılında Adalet Bakanlığı'nın da birtakım ilaveler yapmasının ardından Başbakanlık tarafından 22 Nisan 2008 tarihinde Türkiye Büyük Millet Meclisi'ne (TBMM) gönderilmiş ancak politik gündem ve seçimlerle birlikte Tasarı yine kadük kalmıştır (Korkmaz, 2016: 87).

12 Eylül 2010 tarihli referandum sonrasında Anayasa'nın 20. maddesine getirilen ek hüküm ile kişisel verilerin koruma altına alınması kabul edilerek anayasal hüküm şeklini almıştır. 26 Aralık 2014 tarihinde tekrar TBMM'ye gönderilen Kişisel Verilerin Korunması Kanun Tasarısı yine yasalaşamamış ve 18 Ocak 2016'da yeniden başlatılan süreç, 6698 sayılı Kişisel Verilerin Korunması Kanunu olarak 24 Mart 2016 tarihinde TBMM'de kabul edilerek yasalaşmıştır. 108 numaralı Kişisel Verilerin Otomatik Olarak İşlenme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi, Türkiye tarafından Strazburg'da 28 Ocak 1981'de imzalanmasına karşın sözleşmenin yürürlüğe girmesi ancak 2016 yılında Kişisel Verilerin Korunması Kanunu'nun Resmi Gazete'de yayımlanması ile mümkün olmuştur (Sert, 2016: 277).

Türkiye'de kişisel verilerin korunmasına yönelik doğrudan bir çerçeve yasa hükmündeki 6698 sayılı Kanun'dan önce Türk Ceza Kanunu'nun (TCK) ilgili hükümleri kişisel verilerin ihlaline yönelik birer güvence olarak ele alınmıştır (Turan, 2015: 5). Nitekim Kanunun Dokuzuncu Bölümü "Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar" başlığı altında kişisel mahrem verilerin ihlali ile kişisel verilerin kaydedilmesi, hukuka aykırı verilmesi ya da ele geçirilmesi, yok edilmesi ve korunmasına yönelik güvenlik önlemleri hüküm altına alınmıştır.

Türkiye'de kişisel verilerin korunmasına yönelik yukarıda sayılan bütün birincil kaynaklara karşın ikincil derecede pek çok hukuki düzenleme de mevcuttur. Bunlar arasında İş Kanunu, Bankacılık Kanunu, Banka ve Kredi Kartları Kanunu, Tıbbi Deontoloji Sözlüğü, Elektronik Haberleşme Kanunu, Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğin Korunması Hakkında Yönetmelik, Elektronik İmza Kanunu, Türk Borçlar Kanunu, Türk Ticaret Kanunu, Nüfus Hizmetleri Kanunu, Resmi İstatistiklerde Veri Gizliliği ve Gizli Veri Güvenliğine İlişkin Usul ve Esaslar Hakkındaki Yönetmelik ile çeşitli Yargıtay kararları zikredilebilir. Bunlardan 24.07.2012 tarihli ve 28363 sayılı Resmi Gazete'de yayımlanan elektronik haberleşme ile ilgili yönetmelik, AB'nin ilgili düzenlemeleri ile uyumlu bir biçimde, veri işlemeye ilişkin temel ilkeleri belirlemiş ve işletmecilere şebekelerinin, abonelerine ya da kullanıcılarına ait kişisel verilerin ve sundukları

hizmetlerin güvenliğinin sağlanmasına yönelik birtakım önlemleri hedeflemiştir (Keser, Kaya ve Kınıkoğlu, 2014: 53-56).

6.1. 6698 Sayılı Kanun Çerçevesinde Kişisel Verilere Yönelik Düzenlemeler

Türkiye'de kişisel verilerin korunmasına yönelik bir çerçeve yasanın hazırlanması zorunluluk haline gelmiş ve 6698 sayılı Kanun bu çerçevede düzenlenmiştir (Küzeci, 2011: 149). Kanun özellikle kişisel verilerin korunmasına dair pek çok hak ihlalinin önlenmesine yönelik önemli bir adımdır. Bu bağlamda 1. maddesinde kanunun hedefinin, kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerinin korunması ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasların düzenlenmesi olduğu belirtilmektedir.

Aynı maddede "kişisel verilerin işlenmesi" kavramı, kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi ifade etmektedir. Örneğin Avrupa Adalet Divanı'nın Bodil Lindqvist kararı dikkate alındığında bir kişinin isim ve telefon numarası gibi o kişiyi belirlenebilir kılan bilgilerin bir internet sitesinde yayınlanmasının, kişisel verilerin kısmen veya tamamen otomatik yollarla işlenmesi olarak kabul edildiğini göstermektedir (Özer, 2017). Bununla birlikte kişisel verilerin işlenmesi, ilgili verilerin elde edilmesi ile başlayan kayıt, düzenlenme, uyarlama, değiştirme, düzeltme, inceleme, kullanma, açıklama, sıralama, birleştirme ve silme olmak üzere geniş bir süreç zincirinden oluşmaktadır (Kaya, 2011: 317).

Kişisel verilerin işlenmesinde uyulması gereken ilkeler Kanun'un 4/2. maddesinde şu şekilde sıralanmaktadır:

- *Hukuka ve dürüstlük kurallarına uygun olması,*
- *Doğru ve gerektiğinde güncel olması,*
- *Belirli, açık ve meşru amaçlar için işlenmesi,*
- *İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması,*
- *İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmesi.*

TCK'nın 135. maddesinde ise "Kişisel verilerin kaydedilmesi" konusunda şu hükümler bulunmaktadır:

(1) Hukuka aykırı olarak kişisel verileri kaydeden kimseye altı aydan üç yıla kadar hapis cezası verilir.

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

Kuşkusuz bu taahhütlerin yerine getirilmesinde özellikle hukuka uygunluk, şeffaflık ve dürüstlük ilkelerinin içselleştirilmesi gerekmektedir. Bununla birlikte kişisel verilerin bireylerin makul beklentileri dikkate alınarak işlenmesi ve meşru nedenlere dayanmaksızın kişisel verilerin aleyhte kullanılmaması gerekmektedir. Kişisel verilerin hangi amaçlar çerçevesinde toplanmakta olduğu açıkça belirtilmeli, veriler ilgili iş ya da eylemle ilişkili olmalı ve belirtilen amaçlar dışında işlenmesi halinde veri işleme görevlileri sorumlu tutulabilmelidir (EC, 2013: 15-19). Ayrıca çeşitli kurum ve kuruluşlarda kullanılan e-devlet uygulamaları ya da bilişim sistemlerinin yazılımları üzerinde ilgili kurum ve kuruluşlar denetim ve kontrol yapamamaktadır. Bilişim hizmetinin alındığı özel şirket yetkilileri ya da personeli ilgili sistem üzerinde asıl kontrol sahibi konumundadır. Bu açıdan Türkiye'de pek çok kurumun veri sistemlerinin yüklenici firma personelinin kontrolü altında olması veri güvenliğine ilişkin bazı kaygıları da doğurabilmektedir (DDK, 2013: 787-788).

Kanunun 5. maddesine göre kural olarak kişisel veriler bireylerin açık rızası olmaksızın işlenemez, ancak ilgili kişinin açık rızası alınmaksızın belirli durumlarda kişisel verilerin işlenmesi söz konusu olabilmektedir. Bunlardan ilki kanunda açıkça öngörülmesi durumlarıdır. Hukuk normları hiyerarşisi

çerçevesinde çeşitli düzenlemeler bulunmaktadır. En üstte bulunan birincil düzenlemeler arasında İnsan Hakları Avrupa Sözleşmesi, Anayasa, Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi ve 5 Mayıs 2016 tarihinde Resmi Gazete'de yayımlanan Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesine Ek Denetleyici Makamlar ve Sınıraşan Veri Akışına İlişkin Protokol yer almaktadır. Ancak, kanunda açıkça öngörülme halinin kapsamının geniş ve kötüye kullanıma müsait olduğu da savunulmaktadır. Örneğin 6532 sayılı Milli İstihbarat Teşkilatı Kanunu'na 17 Nisan 2014 tarihinde yapılan değişikliklerle milli savunma, terörle mücadele, dış istihbarat, uluslararası suçlar ve siber güvenlik ile ilgili konularda kamu kurum ve kuruluşları ile meslek kuruluşlarından her türlü veriyi elde etmesi hakkı MİT'e tanınmıştır. Bu durumun kanundaki istisnai haller kapsamına alınmasının fişlemeler vb. hedeflerle ulusal güvenlik ile kişi temel hak ve özgürlükler arasındaki dengenin ihlal edilmesi sonucunu doğurabileceği öne sürülmektedir (Şen, 2009: 1214; İKV, 2015: 30). Öte yandan, Türkiye'nin stratejik konumu ile iç ve dış politik gelişmeler dikkate alındığında istisnai hallerde birtakım kişisel verilerin ilgili kurum ve kuruluşlardan toplanması kamu düzeni ve toplum güvenliği açısından önem arz edebilmektedir.

İkinci olarak veri sorumlusunun hukuki sorumluluğunu yerine getirebilmesi için zorunlu verileri işleyebilmesidir. Bu veriler bir işyerinde çalışanlara yönelik iş sözleşmesindeki haklarını sunabilmesi için gerekli olan verileri işleyebilme hakkını içermektedir. Bir diğer açık rıza aranmaksızın veri işlenmesi imkanı kişisel verilerin ilgili kişi tarafından alenileştirilmesidir. Özellikle sosyal medya araçları üzerinden kamuya açık biçimde her türlü verinin sunulmuş olması o kişinin verilerinin korunmasına yönelik hukuki yararın korunması durumunu ortadan kaldırmaktadır. Bütün bunlara ek olarak bir hakkın tesisi, kullanılma ya da korunması için veri işlemenin zaruri olması halinde kişisel verilerin işlenebilmesi yasal olarak mümkündür.

Kişisel verilerin korunması ilişkin önemli hususlardan birisi de "özel nitelikli kişiler"in verilerinin işlenmesine yöneliktir. 6698 sayılı Kanun'un 6. maddesinde özel nitelikli kişisel verilerin kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biometrik ve genetik verilerinden oluştuğu belirtilmektedir. Kural olarak özel nitelikli kişisel verilerin işlenmesi bireylerin açık rızası olmaksızın yasal değildir. Bununla birlikte özel nitelikli kişisel verilerin işlenmesine dair bazı istisnalar yer almaktadır. Bu istisnalar çerçevesinde özel nitelikli kişisel verilerin işlenmesinde 6698 sayılı Kanun Kişisel Verileri Koruma Kurulu'nun gerekli ek tedbirleri almakla mükellef olduğunu hüküm altına almıştır. Ayrıca hassas verilerin sıradan verilerin işlenmesine göre daha sıkı bir denetime tabi tutulması gerekmektedir (Bygrave, 2002: 68). Bununla birlikte Kanun'da vefat etmiş kişilerin verilerinin korunmasına yönelik herhangi bir düzenleme yer almasa da Türk Medeni Kanunu'nun 25. maddesine göre vefat etmiş kişilerin kişisel verilerinin hukuka aykırı ihlal edilmesinde mirasçılara bu hakkın korunması ve savunması verilmektedir (Özdemir, 2009: 291).

6698 Sayılı Kanun ya da diğer hukuksal düzenlemeler çerçevesinde işlenen kişisel veriler, veri işlenmesini gerektiren şartların kalkması halinde resen ya da ilgili kişinin istemi üzerine veri sorumluları tarafından silinebilir (m. 7). Bu verilerin silinmesi kayıtlı oldukları evrak, dosya, CD, disket, hard disk gibi diğer araçlardan da geri dönüştürülemeyecek şekilde silinmesini ifade etmektedir. Böylece kişisel verilerin silinmesi ile ilgili verilerin tekrar hiçbir şekilde kullanılamaması ve geri getirilemeyecek bir biçimde imha edilmesi söz konusu olmaktadır. Ayrıca kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek şekilde anonim hale getirilmesi de mümkündür. Bununla birlikte TCK 138. maddesinde kişisel verilerin yok edilmemesi durumunda kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde altı aydan bir yıla kadar hapis cezası verileceği hüküm altına alınmıştır.

Kişisel verilerin korunması ilişkin önemli konu başlıklarından birisi de "kişisel verilerin yurt dışına aktarılması" hususudur. Buna göre kural olarak ilgili kişinin açık rızası olmaksızın verilerin aktarılması söz konusu olmasa da 6698 Sayılı Kanun ile diğer tüm hukuki bağlayıcı düzenlemeler çerçevesinde

açık rıza aranmaksızın da bazı kişisel verilerin yurtdışına aktarımı olanaklıdır. Bu çerçevede kişisel verinin aktarılacağı yabancı ülkede yeterli korumanın bulunması yahut yeterli korumanın bulunmaması durumunda Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri ve Kişisel Verileri Koruma Kurul izninin bulunması şartıyla ilgili kişinin açık rızası aranmaksızın yurt dışına aktarılması gerçekleşebilmektedir. Hangi ülkelerin yeterli korumayı sağladığının Koruma Kurulu tarafından belirlenerek ilan edilmesi hüküm altına alınmıştır (m. 9/3). Kurulun yabancı ülkede yeterli koruma bulunup bulunmadığını ve hangi durumlarda izin verilip verilmeyeceğini değerlendirmesi ve karar vermesi şu hususları dikkate almak şartıyla mümkündür:

- *Türkiye'nin taraf olduğu uluslararası sözleşmeler,*
- *Kişisel veri talep eden ülke ile Türkiye arasında veri aktarımına ilişkin karşılıklılık durumu,*
- *Her somut kişisel veri aktarımına ilişkin olarak, kişisel verinin niteliği ile işlenme amaç ve süresi,*
- *Kişisel verinin aktarılacağı ülkenin konuyla ilgili mevzuatı ve uygulaması,*
- *Kişisel verinin aktarılacağı ülkede bulunan veri sorumlusu tarafından taahhüt edilen önlemler.*

Kuşkusuz bütün bu hususlar dikkate alınmak kaydıyla ve uluslararası sözleşme hükümleri mahfuz olmak üzere Türkiye'nin veya ilgili kişinin menfaatinin ciddi bir şekilde zarar göreceği durumlarda ancak ilgili kamu kurum veya kuruluşunun görüşü alınarak ve Kurul'un izniyle kişisel verilerin yurtdışına aktarılması hüküm altına alınmıştır (m. 9/5). Bununla birlikte Avrupa Konseyi tarafından kabul edilen 108 sayılı Sözleşme'ye ek olan 181 sayılı Ek Protokol ile yeterli düzeylerde kişisel verilerin korunmasını sağlayamayan üçüncü ülkelere kişisel veri aktarımı yasaklanmaktadır. Yeterli düzeyde koruma şartı ise ilgili verilerin niteliği, kayıt altına alınan verilerin işlenme amacı, süresi ve transfer aktarımı ile ilgili veriye sahip olacak ülkenin genel, mesleki, sektörel ve güvenlik bazlı tedbirlerin ve kuralların işleyişi dikkate alınarak değerlendirilmektedir (Doğan, 2015: 12, 20).

Türkiye'de kişisel verilerin elektronik ortamlarda işlenmesine ilişkin esas ve usullerin düzenlenmesi, ilgili düzenlemelerin uluslararası veri değişimine uygun olması, gerekli cezai yaptırımların ve yasal güvencelerin sağlanması gerekmektedir (Ersoy, 2006). 6698 sayılı Kanunun Haklar ve Yükümlülükler başlıklı Üçüncü Bölümü'nde veri sorumluları ile ilgili veri sahibi kişilerin hakları ve görevleri düzenlenmiştir. Bu çerçevede herkes kendisi hakkındaki kişisel verilere yönelik veri sorumlularına başvurarak bilgi alma talebinde bulunabilir. Bu talepler ilgili hukuki mevzuattaki hükümler ve istisnalar çerçevesinde gerçekleşebilir. Bu açıdan ilgili kişilerin verilerine yönelik hakları şu şekilde sıralanmaktadır (m. 11/1):

- *Kişisel veri işlenip işlenmediğini öğrenme,*
- *Kişisel verileri işlenmişse buna ilişkin bilgi talep etme,*
- *Kişisel verilerin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme,*
- *Yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme,*
- *Kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme,*
- *Kişisel verilerin silinmesini veya yok edilmesini isteme,*
- *İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme,*
- *Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme.*

6698 sayılı Kanun'un 28. maddesi ile getirilen düzenlemelerin ise kamu kurum ve kuruluşları lehine ve 95/46/EC Direktifi'nin aksine geniş istisnalar getirerek veri güvenliğine ilişkin kişilerin daha çok özel sektör aktörlerinden korunmasına yönelik olduğu da savunulmaktadır (Pehlivan, 2016). Bu bağlamda 6698 sayılı Kanun hükümleri çeşitli hallerde uygulanamamakta ve bu istisnai hallerden bazıları şu şekilde sıralanmaktadır (m. 28/1):

- *Kişisel verilerin resmi istatistik ile anonim hâle getirilmesiyle araştırma, planlama ve istatistik gibi amaçlarla işlenmesi,*

- *Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini, ekonomik güvenliği, özel hayatın gizliliğini veya kişilik haklarını ihlal etmemek ya da suç teşkil etmemek kaydıyla, sanat, tarih, edebiyat veya bilimsel amaçlarla ya da ifade özgürlüğü kapsamında işlenmesi,*

- *Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi,*

- *Kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi.*

6698 sayılı Kanun'da yer alan ve bu çalışmanın da önemli vurguları arasında yer alan veri güvenliğine ilişkin yükümlülükler oldukça önem arz etmektedir. Nitekim Türkiye gibi stratejik ve küresel siyaset açısından önemli bir ülkenin çeşitli kamusal alanlarına yönelik pek çok kişisel verinin çeşitli amaçlar çerçevesinde yasal ve bazen de yasal olmayan yollardan elde edilmesine yönelik konular sık sık kamuoyunun gündemine gelebilmektedir. Bu açıdan kişisel verilerin korunmasında yasal düzenlemeler kadar kişisel veri sorumlularının da güvenirliğine ilişkin kaygıların giderilmesine yönelik tedbirlerin geliştirilmesi gerekmektedir. Buna karşın veri sorumluları, kişisel verilerin hukuka aykırı olarak işlenmesinin önlenmesi, kişisel verilerin hukuka aykırı olarak erişilmesinin engellenmesi ve kişisel verilerin korunmasını sağlamak üzere gerekli her türlü teknik ve idari tedbirleri almakla mükellef kılınmıştır (m. 12/1). Ayrıca Kişisel Verileri Koruma Kurumu Başkanlığı veri sorumlularının sicilini tutmakla görevlidir (m. 25/4). Bununla birlikte veri sorumluları ile veri işleyen kişiler, öğrendikleri kişisel verileri ilgili kanun hükümlerine aykırı olarak başkalarına açıklayamamakta, işlenme amacı dışında kullanamamakta ve bu yükümlülükleri görevden ayrılmalarından sonra da devam etmektedir. İşlenen kişisel verilerin yasal olmayan yollarla başkaları tarafından elde edilmesi durumunda ise, veri sorumlusu bu durumu en kısa sürede ilgili birime ve Kişisel Verileri Koruma Kurulu'na bildirmekle görevlidir. Kurul, gerekli görmesi hâlinde durumu kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilme hakkına sahiptir (m. 12/4-5).

6.2. Yapısal ve Yönetsel Açıdan Türkiye'de Kişisel Verileri Koruma Kurulu

Önceki bölümde de ortaya konulduğu gibi Türkiye'de kişisel verilerin korunmasına yönelik yasal düzenlemeler oldukça uzun bir zamanda tamamlanmıştır. Verilerin korunmasına dair hukuki mevzuat oldukça dağınık olsa da çerçeve bir yasanın çıkartılması ile durum daha net hale gelmiştir. 6698 Sayılı Kanun ile birlikte Türkiye'de kişisel verilerin korunmasına yönelik politikalar açısından ilk doğrudan kurumsal mekanizma hayata geçirilebilmiştir.

Kişisel verilerin korunmasında bağımsız bir veri koruma komitesinin kurulması Avrupa Birliği İlerleme Raporlarında önemle vurgulanan bir konu olmuştur (COM, 2013: 64). Bu bağlamda kurulan Kişisel Verileri Koruma Kurumu Başbakanlıkla ilişkili, kamu tüzel kişiliğine haiz, idari ve mali özerkliğe sahip bir kuruluştur.

Merkezi Ankara olan Kurum, Kurul ve Başkan'dan oluşmakta ve kurumun karar organı Kurul olarak hüküm altına alınmıştır (m. 19). Kurul, dokuz üyeden oluşmakta, beş üye Türkiye Büyük Millet Meclisi, iki üye Cumhurbaşkanı, iki üye ise Bakanlar Kurulu tarafından seçilmektedir. Kurul üyesi olabilmek için herhangi bir siyasi parti üyesi olmamak, en az dört yıllık lisans düzeyinde yükseköğrenim görmüş olmak, kamu kurum ve kuruluşlarında, uluslararası kuruluşlarda, sivil toplum kuruluşlarında veya kamu kurumu niteliğindeki meslek kuruluşlarında ya da özel sektörde toplamda en az on yıl çalışmış olmak gibi şartlar aranmaktadır (m. 20/3). TBMM'deki üyelik seçimleri için, siyasi parti gruplarının üye sayısı oranında belirlenecek üye sayısının ikişer katı aday gösterilmekte ve Kurul üyeleri bu adaylar arasından her siyasi parti grubuna düşen üye sayısı esas alınmak suretiyle TBMM Genel Kurulunca seçilmektedir (m. 21/5).

Üyelerin yeminleri, kurum içi ve dışı çalışma şartları, görev süreleri ve üyelik sürelerine yönelik ayrıntılı düzenlemeler yer almıştır. Buna göre kurul üyelerinin görev süresi dört yıl olup süresi biten üye

yeniden seçilebilmekte, görev süresi dolmadan herhangi bir sebeple görevi sona eren üyenin yerine seçilen kişi, yerine seçildiği üyenin kalan süresini tamamlayabilmektedir. Kurula seçilen üyeler Yargıtay Birinci Başkanlık Kurulu huzurunda *"Görevimi Anayasaya ve kanunlara uygun olarak, tam bir tarafsızlık, dürüstlük, hakkaniyet ve adalet anlayışı içinde yerine getireceğime, namusum ve şerefim üzerine yemin ederim."* şeklinde yemin ederek göreve başlamaktadır. Kurul üyeleri kuruldaki resmî görevlerinin yürütülmesi dışında resmî veya özel hiçbir görev alamayacakları belirtilmiş ancak asli görevlerini aksatmayacak biçimde bilimsel amaçlı yayın yapabilecekleri, ders ve konferans verebilecekleri ve bunlardan doğacak telif hakları ile ders ve konferans ücretlerini alabilecekleri hüküm altına alınmıştır (m. 21/8-10). Üyeler hakkındaki görevlerine dair soruşturma izni Başbakan tarafından verilmekte ve üyelikleri görev süreleri dolmadan sonlandırılmamakta ancak birtakım istisnaları bulunmaktadır. Örneğin seçilmek için yeterli şartları taşımadıklarının sonradan anlaşılması, haklarında verilen mahkumiyet kararı, izinsiz ve mazeretsiz kurul toplantılarına belirli süreler zarfında katılmamak, sağlık sorunları nedeniyle görevlerini yürütemeyeceklerinin anlaşılması üzerine görevleri sonlandırılabilir (m. 21/13).

Kurul, üyeleri arasından Başkan ve İkinci Başkanı seçmekte ve Kurulun Başkanı, Kurumun da başkanı olarak kabul edilmektedir (m. 21/7). Başkan, Kurul ve Kurumun başkanı sıfatıyla kurumun en üst amiri olup kurum hizmetlerinin mevzuata, stratejik planına, performans ölçütlerine ve hizmet kalite standartlarına uygun olarak düzenlenmesini yürütmekle ve hizmet birimleri arasında koordinasyonu sağlamakla görevlidir (m. 24/1). Kurulun toplantı günlerini ve gündemini Başkan belirlemekte, başkan gerekli durumlarda kurulu olağanüstü toplantıya çağırabilmektedir. Kurul, başkan dâhil en az altı üye ile toplanabilir, üye tam sayısının salt çoğunluğuyla karar alabilir ancak kurul üyeleri çekimser oy kullanamazlar (m. 23/1-2). Diğer yandan kurumda, Kişisel Verileri Koruma Uzmanı ve Kişisel Verileri Koruma Uzman Yardımcısı istihdam edilebilmektedir (m. 26/1).

6698 sayılı Kanun'da Kurumun görevleri; görev alanı itibariyle, uygulamaları ve mevzuattaki gelişmeleri takip etme, değerlendirme ve önerilerde bulunma, araştırma ve incelemeler yapma veya yaptırma, ihtiyaç hâlinde, görev alanına giren konularda kamu kurum ve kuruluşları, sivil toplum kuruluşları, meslek örgütleri veya üniversitelerle iş birliği yapma, kişisel verilerle ilgili uluslararası gelişmeleri izleme ve değerlendirme, görev alanına giren konularda uluslararası kuruluşlarla işbirliği yapma, toplantılara katılma, yıllık faaliyet raporunu Cumhurbaşkanlığına, Türkiye Büyük Millet Meclisi İnsan Haklarını İnceleme Komisyonuna ve Başbakanlığa sunma ve kanunlarla verilen diğer görevleri yerine getirme şeklinde sıralanmaktadır (m. 20/1). Bununla birlikte Kurul'un görev ve yetkilerinden bazıları ise şu şekilde sıralanmaktadır (m. 22/1):

- *Kişisel verilerin, temel hak ve özgürlüklere uygun şekilde işlenmesini sağlamak,*
- *Kişisel verilerle ilgili haklarının ihlal edildiğini ileri sürenlerin şikâyetlerini karara bağlamak,*
- *Özel nitelikli kişisel verilerin işlenmesi için aranan yeterli önlemleri belirlemek,*
- *Veri Sorumluları Sicilinin tutulmasını sağlamak,*
- *Veri sorumlusunun ve temsilcisinin görev, yetki ve sorumluluklarına ilişkin düzenleyici işlem yapmak,*
- *Bu Kanunda öngörülen idari yaptırımlara karar vermek,*
- *Diğer kurum ve kuruluşlarca hazırlanan ve kişisel verilere ilişkin hüküm içeren mevzuat taslakları hakkında görüş bildirmek.*

AB ve Avrupa Konseyi'nin ilgili düzenlemeleri dikkate alındığında ulusal ölçekteki kişisel verilerin korunması otoritesinin mali bütçesi dahil olmak üzere tam bağımsız bir niteliğe sahip olması arzulanmaktadır. Bununla birlikte Kurul'un daha etkin ve verimli bir biçimde işleyebilmesi için Kurul yapısının akademik çevreler, iş dünyası ve sivil toplum paydaşlarını içeren bir yaklaşımla oluşturulması ve mesleki uzmanlığı ve deneyimi öncelemesi vurgulanmaktadır (İKV, 2015: 31). 6698 sayılı Kanun ile mesleki yeterlilik, uzmanlık ve paydaş çeşitliliği dikkate alındığında bunun önemli ölçüde başarıldığını ifade etmek mümkündür. Buna karşın mevut Kurul yapısı önemli ölçüde politik ilişkiler üzerinden

şekillenmekle birlikte tek tip politik üye dağılımı üzerinden oluşmamaktadır. Bu açıdan bazı eksikliklerin bulunmasına karşın henüz oldukça yeni olan kurum ve kurulun önümüzdeki dönemdeki faaliyetleri ve işlevleri daha açık değerlendirmelerin yapılabilmesini kolaylaştıracaktır. Bununla birlikte kişisel veri ihlallerine yönelik şikâyetlerin tamamının Kurul'un inceleme yetkisi içerisine alınmasının ve sivil toplum kuruluşlarına da şikâyet edebilme hakkının verilmesinin yararlı olabileceği de belirtilmektedir (DDK, 2013: 793).

SONUÇ VE ÖNERİLER

Kişisel verilerin korunması konusunda ortaya çıkan yaygın ihlaller ve kötü niyetli uygulamalar kendileri hukuksuz olsa da hukuki birtakım adımların atılmasının önünü açmıştır. AB'nin talep ve hassasiyetleri ciddi bir çıkış kapısıdır. Ancak, tek ve en belirleyici etken de değildir. Ergenekon türü operasyonlar ve FETÖ/PDY terör örgütünün yaygın bir şekilde kullandığı bir yöntem olan kişisel verilere ulaşılması ve kötü niyetli kullanımı konuya karşı duyarlılığı artırmıştır. Bu açıdan Türkiye meseleyi daha fazla erteleyemeyeceğini anlamıştır.

Kişisel verilerin korunmasına yönelik kişisel veri mahremiyetine ilişkin 1951 tarihli Avrupa İnsan Hakları Sözleşmesi bir tarafa bırakılırsa Avrupa düzeyinde yasal mevzuat ilk olarak 1960'lı yıllarda oluşmaya başlamış ve 1970'li yıllarda yaygınlaşmıştır. Bununla birlikte kişisel verilerin korunmasında bağlayıcılığı olan ilk uluslararası hukuki düzenleme Avrupa Konseyi tarafından hazırlanarak 1 Ekim 1985 tarihinde yürürlüğe giren 108 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi Türkiye tarafından 1981'de imzalanmasına ve ilk yasal çalışma girişimleri 1985'de başlatılsa da 2016 yılında ancak nihayete erdirilebilmiştir. Kuşkusuz bu gecikmelerde birtakım politik gelişmeler ve öncelikler etkili olmuştur. Buna karşın kişisel verilerin korunmasına yönelik yasal ve kurumsal ihdas çalışmaları çeşitli hükümetlerce benimsenen bir politika olarak karşımıza çıkmıştır.

Avrupa Birliği perspektifinde kişisel verilerin korunmasına yönelik en önemli düzenlemelerden birisi olan "Avrupa Birliği Veri Koruma Direktifi 95/46/EC", Türkiye'de yasal mevzuat çalışmalarında oldukça esinlenilen bir düzenleme olarak ele alınmış ve e-ticaret ve e-devlet uygulamalarında oldukça önemsenmiştir. Açıkça belirtmek gerekir ki Türkiye'de kişisel veri politikalarında en önemli itici etken Birlik olmuştur. Nitekim AB tam üyelik çerçevesinde açılan pek çok fasıl veri güvenliğine ilişkin hak ve yükümlülükleri içermiştir. Bu açıdan Türkiye'nin kamu düzeni ve güvenliğine yönelik tedbirlerinde kişisel verilerin korunmasına yönelik güvenlik ve özgürlük dengesinin gözetilmesi önemlidir. Bununla birlikte Türkiye'de henüz çok yeni bir kurum olan Kişisel Verileri Koruma Kurulu'nun nasıl işleyeceği süreç içerisinde karar vericilerin ve uygulayıcıların yaklaşımları ile yakından ilişkili olacaktır. Ancak Türkiye'de iç ve dış politik tehditler ile hızla gelişen teknolojik gelişmeler, veri korunması politikalarının sağlam bir kontrol ve denetimden geçirilmesini eskisinden çok daha fazla ihtiyaç duymaktadır.

Türkiye'de ulusal veri güvenliğine yönelik strateji ve politikaların geliştirilmesi, veri güvenliğine ilişkin standartların belirlenmesi, gelişen şartlar çerçevesinde güncellemelere gidilmesi, veri sistemlerinin oluşturulmasından işletilmesine kadarki süreçte ilgili kurumlara teknik ve beşeri kaynak desteğinde bulunulması, kurumlar arası işbirliğinin geliştirilmesi ve yerli yazılım sistemlerinin oluşturulmasına yönelik çalışmaların yürütülmesi oldukça önem arz etmektedir. Bununla birlikte kurumsal ölçekte veri koruma yönetimi çerçevesinde yeni politikalar geliştirilmeli, kişisel verilerin işlenmesinden silinmesine kadar bütün aşama ve süreçlerindeki kriterler açık ve net olmalı, iç kontrol ve denetleme mekanizmaları oluşturulmalı, kurumsal cihazların yetkisiz kişilerce kullanılması önlenmeli ve kişisel verilerin korunmasına yönelik ulusal ve evrensel kaide ve kurallar kurum personellerince içselleştirilmelidir.

Sonuç olarak; Türkiye'de kişisel verilerin korunmasına yönelik mevzuatın kabul görmesi ve etkin bir denetim mekanizmasının oluşturulması Kurul'un etkinliğine bağlıdır. Kurul'un ise benzerlerine yakın bir başarı elde edeceği kolayca tahmin edilebilir. Kamu Denetçiliği Kurumu mesela ne kadar etkin olmuşsa Kişisel Verilerin Korunması Kurulu da aynı oranda etkili olacaktır. Ancak, bugünden yarına ve yüksek başarı oranında bir iyileşme ve mükemmel bir sistemin kurulmasını da kimse

beklememelidir. Belirli bir müddet zamana ihtiyaç duyulacak, mesele hakkında gerek akademik camiada gerekse uygulamada ortaya çıkacak ilke ve standartlar toplumca kabul gördükçe Kurul'un etkinliği artacaktır. Toplumsal duyarlık Kurul düzeyinde duyarlığa dönüşecektir. Böyle bir kurul gereklidir; mevzuat elzemdir. Başarı ve toplumsal kabul zamanla ortaya çıkacaktır.

KAYNAKÇA

Akdağ, Hale (2015). "Türk Ceza Hukukunda Kişisel Verilerin Korunması İlkeleri", Prof. Dr. Nevzat Toroslu'ya Armağan, Cilt. 1, No. 459, Ankara Üniversitesi Yayınları, ss. 27-48.

Akgül, Aydın (2015). "Kişisel Verilerin Korunmasında Yeni Bir Hak: "Unutulma Hakkı" ve AB Adalet Divanı'nın "Google Kararı", *TBB Dergisi*, Sayı. 116, ss. 11-38.

Assey, James M. and Eleftheriou, Demetrious A. (2001). "The EU-U.S. Privacy Safe Harbor: Smooth Sailing or Troubled Waters?", *Commlaw Conspectus*, Vol. 9, pp. 145-158.

Babahanoğlu, Veysel ve Örselli, Erhan (2016). "Türk Kamu Yönetiminde Kişisel Verilerin Korunması ve Güvenliğine İlişkin Kurumsal Yapılanma: Kişisel Verilerin Korunması Kurumu", *I. Uluslararası Sosyal Bilimler Sempozyumu ASOS Congress Bildiri Kitabı*, 13-15 Ekim 2016, Elazığ, ss. 550-556.

Bainbridge, David I. (1997). "Processing Personal Data and The Data Protection Directive", *Journal of Information & Communications Technology Law*, Vol. 6, No. 1, pp. 17-40.

Bygrave, Lee A. (2002). *Data Protection Law, Approaching its Rationale, Logic and Limits*, Wolters Kluwer.

Cate, Fred H. (1998). "The European Data Protection Directive and European-US Trade", *Current: International Trade Law*, Vol. 7, pp. 61-80.

Commission of the European Communities (COM) (2008). *Turkey 2008 Progress Report*, EN: Brussels.

Commission of the European Communities (COM) (2013). *Turkey 2013 Progress Report*, EN: Brussels.

Council of Europe (1981). *Committee of Ministers, Explanatory Report on the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, Texts Adopted, ETS No. 108, http://conventions.coe.int/Treaty/en/Reports/Html/108.htm, (Erişim Tarihi: 08.07.2017).

D'afflitto, Rosario Imperiali (1996). "European Union Directive on Personal Privacy Rights and Computerized Information", *Villanova Law Review*, Vol. 41, No. 1, pp. 305-323.

Devlet Denetleme Kurumu (DDK) (2013). *Kişisel Verilerin Korunmasına İlişkin Ulusal ve Uluslararası Durum Değerlendirmesi ile Bilgi Güvenliği ve Kişisel Verilerin Korunması Kapsamında Gerçekleştirilen Denetim Çalışmaları Raporu*, https://www.tccb.gov.tr/assets/dosya/ddk56.pdf, (Erişim Tarihi: 09.07.2017).

Diri, Mustafa ve Gülçiçek, Mirac (2012). "Türkiye'de Kamu Hizmetinin Görülmesinde Kullanılmakta Olan Gizlilik Derecesi Tanımları: Uygulamadaki Sorunlar ve Çözüm Önerileri", *Maliye Dergisi*, Sayı. 162, ss. 497-537.

Doğan, Adnan Çoşkun (2015). "Kişisel Verilerin Korunması, Muhafazası ve Paylaşımı", Ankara.

Eren, Veysel ve Durna, Ufuk (2005). "Kamu Hizmetlerinin Daha İyi Görülebilmesi İçin Alternatif Bir Yönetim Yaklaşımı: Elektronik Devlet", *İstanbul Üniversitesi Siyasal Bilgiler Fakültesi Dergisi*, Sayı. 32, ss. 139-166.

European Commission (EC) (2013). *Article 29 Data Protection Working Party*, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf, (Erişim Tarihi: 04.07.2017).

European Convention on Human Rights (ECHR) (1950). http://www.aihmbasvuru.com/avrupa-insan-haklari-sozlesmesi.html, (Erişim Tarihi: 05.07.2017).

Ersoy, Eren (2006). "Gizlilik, Bireysel Haklar, Kişisel Verilerin Korunması", 9-11 Şubat Telekomünikasyon Kurumu Akademik Bilişim 4. Bilgi Teknolojileri Kongresi, http://docslide.net/documents/gizlilik-bireysel-haklar-kisisel-verilerin-korunmasi-eren-ersoy-telekomuenikasyon.html, (Erişim Tarihi: 05.07.2017).

Henkoğlu, Türkay ve Özenç-Uçak, Nazan (2015). "Üniversite Kütüphanelerinde Kişisel Verilerin Korunması", *Bilgi Dünyası*, Cilt. 16, Sayı. 1, ss. 45-74.

Ilana, Saltzman (1996). "The Status of National Implementation of Directive 95/46/EC on the Processing and Free Movement of Personal Data, *European Intellectual Property Review*, Vol. 18, No. 6, pp. 680-683.

İktisadi Kalkınma Vakfı (İKV) (2015). *Türkiye'de ve AB'de Kişisel Verilerin Korunması*, İstanbul: Dünya Yayıncılık.

İmre, Zahit (1974). "Şahsiyet Haklarından Şahsın Özel Hayatının ve Gizliliklerinin Korunmasına İlişkin Meseleler", *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası*, Cilt. 39, Sayı. 1-4, ss. 146-168.

Karlıdağ, Serpil (2013). "Ekonomi Politik Açıdan Kişisel Verilerin Korunması", *Amme İdaresi Dergisi*, Cilt. 46, Sayı. 1, ss. 127-152.

Karlıdağ, Serpil ve Bulut, Selda (2015). "E-Ticarette Tüketici Gizliliğinin Korunması Üzerine Bir Araştırma", *İşletme Araştırmaları Dergisi*, Vol. 7, Issue. 4, ss. 200-224.

Kaya, Cemil (2011). "Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi", *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası*, Cilt. 69, Sayı. 1-2, ss. 317-334.

Keser, Leyla, Kaya, M. Bedii ve Kınıkoğlu, Batu (2014). "Hukuki Analiz", *Türkiye'de Kişisel Verilerin Korunmasının Hukuki ve Ekonomik Analizi*, İstanbul Bilgi Üniversitesi & TEPAV, ss. 39-74.

Kılınç, Doğan (2012). "Anayasal Bir Hak Olarak Kişisel Verilerin Korunması", *Ankara Üniversitesi Hukuk Fakültesi Dergisi*, Cilt. 61, Sayı. 3, ss. 1089-1169.

Koops, Bert-Jaap (2014). "The Trouble with European Data Protection Law", *International Data Privacy Law*, Vol. 4, No. 4, pp. 250-261.

Korkmaz, İbrahim (2016). "Kişisel Verilerin Korunması Kanunu Hakkında Bir Değerlendirme", *TBB Dergisi*, Sayı. 124, ss. 81-152.

Küzeci, Elif (2011). "Anayasal Bir Hak: Kişisel Verilerin Korunması", *Bilişim Kültürü Dergisi*, Ocak, ss. 142-149.

Nebil, Fusun S. (2016). "Kişisel Verilerin Korunması Kanununun Tarihçesi ve Analizi-II", http://www.turk-internet.com/portal/yazigoster.php?yaziid=52052, (Erişim Tarihi: 09.07.2017).

Oxman, Stephen A. (2000). "Exemptions to the European Union Personal Data Privacy Directive: Will They Swallow the Directive?", *Boston College International & Comparative Law Review*, Vol. 24, pp. 191-203.

Özdemir, Hayrunnisa (2009). "Haberleşmenin Gizliliği ve Kişisel Veriler", *Erzincan Üniversitesi Hukuk Fakültesi Dergisi*, Cilt. 13, Sayı. 1-2, ss. 285-303.

Pehlivan, Oğuz Kaan (2016). "Kişisel Verilerin Korunması Kanunu Ne Vadediyor?", http://www.aljazeera.com.tr/gorus/kisisel-verilerin-korunmasi-kanunu-ne-vadediyor, (Erişim Tarihi: 09.07.2017).

Reidenberg, Joel R. (1999). "Restoring Americans' Privacy in Electronic Commerce", *Berkeley Technology Law Journal*, Vol. 14, Issue. 2, pp. 771-792.

Robinson, N., Graux, H., Botterman, M. and Valeri, L. (2009). "Review of the European Data Protection Directive", Cambridge: Rand Europe, https://www.researchgate.net/publication/265450064_Review_of_the_European_Data_Protection_Directive, (Erişim Tarihi: 05.07.2017).

Schriver, Robert R. (2002). "You Cheated, You Lied: The Safe Harbor Agreement and its Enforcement by the Federal Trade Commission", *Fordham Law Review*, Vol. 70, Issue. 6, pp. 2777-2818.

Sert, Selin (2016). "İnternet Yoluyla Elde Edilen Kişisel Verilerin Genel Boşanma Sebepleri Arasında Değerlendirilmesi Meselesi", *TBB Dergisi*, Sayı. 116, ss. 275-292.

Stuart, Allyson Haynes (2014). "Google Search Results: Buried If Not Forgotten", *North Carolina of Law & Technology*, Vol. 15, Issue. 3, Spring, pp. 463-518.

Şahbaz, Ussal, Alpaslan, İdil Bilgiç ve Sökmen, Ali (2014). "Veriye Dayalı Ekonominin Getirdiği Fırsatlar ve Kişisel Verilerin Korunmasının Ekonomik Analizi", *Türkiye'de Kişisel Verilerin Korunmasının Hukuki ve Ekonomik Analizi*, İstanbul Bilgi Üniversitesi & TEPAV, ss. 2-38.

Şen, Ersan, (2009). "Kişisel Verilerin Korunması Kanunu Tasarısının Değerlendirilmesi", *İstanbul Barosu Dergisi*, Cilt. 83, Sayı. 3, ss. 1197-1214.

Şimşek, Oğuz (2008). *Anayasa Hukukunda Kişisel Verilerin Korunması*, Ankara: Beta Yayınevi.

Tataroğlu, Muhittin (2013). "Mahremiyet Sorunlarının Önlenmesinde Mahremiyet Etki Değerlendirmesi (MED)", *Yönetim ve Ekonomi*, Cilt. 20, Sayı. 1, ss. 263-289.

Tortop, Nuri (2000). "Çağımızın Önemli Sorunu: Kişisel Bilgilerin Güvenliği Sorunu", *Amme İdaresi Dergisi*, Cilt. 33, Sayı. 3, ss. 1-14.

Turan, Metin (2015). "Hukukumuzda Kişisel Verilerin Korunması", Türkiye Kalkınma Bankası Yayını, Sayı. 75, ss. 2-5.

Ünver, H. Akın ve Kim, Grace (2016). *Türkiye'de Veri Gizliliği ve Gözetimi: Kişisel Verilerin Korunması Kanunu Tasarısının Değerlendirilmesi*. İstanbul: Ekonomi ve Dış Politika Araştırmalar Merkezi.

Warner, Jeremy (2005). "The Right to Oblivion: Data Retention from Canada to Europe in Three Backward Steps", *University of Ottawa Law & Technology Journal*, 2 UOLTJ 75, pp. 75-104.

5237 Sayılı Türk Ceza Kanunu, http://www.resmigazete.gov.tr/eskiler/2004/10/20041012.htm, (Erişim Tarihi: 18.06.2017).

6698 Sayılı Kişisel Verilerin Korunması Kanunu, http://www.kisiselverilerinkorunmasi.org/, (21.06.2017).