

Uluslararası Düzenlemelerde ve Türkiye’de Kişisel Verilerin Korunması

Yasime Hoşnut, Yüksek Lisans Öğrencisi, Ankara Hacı Bayram Veli Üniversitesi Lisansüstü Eğitim Enstitüsü, yhosnut@gmail.com
ORCID ID: <https://orcid.org/0000-0002-9505-0136>, Geliş Tarihi: 06.08.2019, Kabul Tarihi: 29.08.2019

Öz Abstract

Kişisel verilerin korunması, geçmişte olduğu gibi günümüzde de önemli konulardan biridir. Bir yandan, günümüzde bilgi ve iletişim teknolojilerindeki gelişmelerle birlikte, kişisel verilerin toplanması, işlenmesi ve saklanmasına yönelik uygulamalar daha da önem kazanmaktadır. Diğer yandan, gelişmiş teknolojinin getirdiği işlem kolaylığı ve hız, kişisel verilerin korunmasıyla ilgili tartışmaları da gündeme getirmektedir. Çalışmada, kişisel verilerin korunması ve veri mahremiyetinin sağlanmasına ilişkin temel yasal düzenlemelerin ve uygulamaların incelenmesi

amaçlanmaktadır. Gelişen teknolojiler ile birlikte, ulusal ve uluslararası düzeyde, kişisel verileri korumak için görüşler bildirilmiş, kanun, yönetmelik ve sözleşmeler yapılmıştır. Çalışmada, Amerika Birleşik Devletleri, Avrupa Konseyi, Avrupa Birliği, Birleşmiş Milletler ile OECD Ülkeleri’nde kişisel verilerin düzenlenmesine ilişkin mevzuat, tarihçeleriyle birlikte ele alınmaktadır. Çalışmada, Türkiye’de 2016 yılı Nisan ayında kabul edilen Kişisel Verilerin Korunması Kanunu’ndaki düzenlemeler ile kişisel verileri korumak amacıyla yapılan çalışmalar da incelenerek sonuçlara ulaşılmaktadır.

Protection of Personal Data in Turkey and International Regulations

Protection of personal data is one of the important issues in the past and now. On the one hand, practices related with the collection, processing and storage of personal data become crucial alongside developments in information and communication technologies nowadays. On the other hand, easy and speedy processing of data which is provided by the high technology has sparked considerable public debate on the protection of personal data. This study aims to analyze the main legal regulations and practices related with the protection of personal data. In connection to the advancement of technologies, statements on

the protection of personal data were reported, and declarations, laws, regulations and conventions were issued at the national as well as international levels. In this study, legislations on the personal data protection in the United States of America, European Council, European Union, United Nations and OECD countries are examined by also considering their history. In the thesis, Personal Data Protection Act which was promulgated in April 2016 in Turkey is investigated along with the studies on protect personal data protection data in Turkey.

Anahtar Kelimeler

Keywords

Kişisel Verileri Koruma, Uluslararası Düzenlemeler, Türkiye’de Kişisel Verilerin Korunması Kanunu.

Protection of Personal Data, International Regulations, Personal Data Protection Act in Turkey.

Giriş

Kişisel veriler, bir kişinin tanınmasını sağlayan temel özellikleridir. “Kişisel veri kavramı isimden, tercihlere, duygu ve düşüncelere kadar çok geniş yelpazede ele alınan ve bene ait bir kavramdır” (İzgi, 2014: 29).

Adı, soyadı, doğum tarihi ve doğum yeri gibi bireyin sadece kimliğini ortaya koyan bilgiler değil; telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, genetik bilgiler, IP adresi, e-posta adresi, cihaz kimlikleri, hobiler, tercihler, etkileşimde bulunulan kişiler, grup üyelikleri, aile bilgileri gibi kişiyi doğrudan veya dolaylı olarak belirlenebilir kılan tüm veriler kişisel veri kapsamındadır (Devlet Denetleme Kurulu Raporu, 2013: 778).

Günümüzde gelişen bilgi ve iletişim teknolojileri, kişisel verileri kaydeden sistemleri artırmaktadır. Elektronik cihazlar, banka kartı kullanımları ve sosyal medya kullanım alanları her an nerede ve ne yapıldığına dair veriler içerir. Bütün elektronik sistemler anlamlı veya anlamsız birçok veriyi toplar ve daha sonra kullanmak için kaydeder. Bu noktada önemli olan, “elbette ki, kişilerin en doğal hakkı öz varlığını korumaktır. Bilgi teknolojileri aracılığıyla ve çeşitli nedenlerle kişisel bilgilerin bazen istemli, bazen istemsiz paylaşılması kişilik haklarının ihlâlini akla getirmektedir” (Aktaran: Türel ve diğerleri, 2015: 242). İnsanın kendi varlığını özgürce geliştirebilmesi için özel yaşamını başkasının denetiminden ve gözetiminden uzak bir biçimde sürdürmesi gerekmektedir. Bu bağlamda, gizlilik ve bağımsızlık özel yaşamın temel öğeleridir (Aktaran: M. Zengin ve İ. Zengin, 2015: 2) şeklinde belirtilir.

Bilgi ve iletişim teknolojilerinin yirminci yüzyıl sonlarında ivme kazanan gelişimi, yirmi birinci yüzyılda da devam etmektedir. Her geçen gün teknolojilerin daha fazla yaşantıya girmesi, işlem hızını arttırmakta, zaman açısından da kolaylıklar sağlamaktadır. Bu gelişmelerle, internet ağ ve sosyal medya kullanımı yaygınlaşmaktadır. Her geçen gün sistemlere kaydolma ve kişisel verileri paylaşma artan bir seyir göstermektedir. Bu gelişmeler aynı zamanda, kişisel verilerin toplanmasını ve yayılmasını da kolaylaştırıcı unsur olmaktadır. Bu noktada, gençlerin internette gönüllü olarak hayatlarına dair detayları paylaşmasını ebeveynlerin anlamakta zorlandığını belirtilirken, gençlerin görülme ve fark edilmek istemesi (Aktaran: Zengin ve diğerleri, 2013: 118) olarak ifade etmektedir.

Sistemler gelişmeden önceden dosyalarda kayıt yapma ve işleme hem uzun bir süreçti hem de masraflı bir işti. Oysa şu anda teknolojiyle birlikte, kişisel verilerin toplanması ve işlenmesinin kolaylaşmasıyla amaç dışı kullanımı da her geçen gün artmaktadır. Özellikle sosyal medyada görünme amaçlı yapılan gönüllü paylaşımlarla, kişisel veriler zahmetsizce elde edilmektedir. Bu durumda, kişisel verilerin yasa dışı yollarla toplanması ve satılması veri mahremiyeti ihlâllerini ortaya çıkarmaktadır. Örneğin; “Sağlık Bakanlığı’nın Sosyal Güvenlik Kurumu’nun bilgilerini satış (Birgün, 25 Ekim 2014) haberi ve “telefon operatörleri, bankalar ve anket şirketlerinden kişisel verileri elde eden aracılardan, bu bilgileri illegal çağrı merkezlerine sattığı ortaya çıktı” (Yeni Şafak, 3 Nisan 2018) haberi kişisel verilerin korunması öncesindeki durumla, Kanunu’nun çıkartılması sonraki durumu açıkça ortaya koymaktadır. Kişisel verilerin amaç dışında toplanması ve üçüncü şahıslara satılması sonucu birçok kişi veri mahremiyeti ihlâlüne uğramakla birlikte sonucunun bilinmeyeceği durumlarla karşı karşıya kalabilmektedir. Bu noktada kişisel verilerin işleme ve korunma süreçlerinin bilinmesi önemli olmaktadır. Elde edilen veri yığınları, sistemler aracılığıyla anlamlı bir veri haline dönüştürmeye çalışılır. Bu işlemler için genellikle veri madenciliği yöntemlerinden faydalanılır. Çünkü “bölük pörçük veri kopyaları, hikâyesini kendi ağzından anlatmayı tercih eden insandan daha güvenilir hâle gelir” (Bauman ve Lyon, 2013: 19). Veri madenciliği, çok büyük hacimdeki verilerden yeni trendler, biçimler, modeller bulma süreci

olarak, ham verinin tek başına sunamadığı bilgiyi, bilgisayar teknolojileri kullanılarak ortaya çıkaran keşif süreci (Aktaran: Esen, 2016: 96) olarak tanımlanır. Veri madenciliğinin, günümüzde bilgisayar algoritmaları ve sistematik kodlarla yapılması, büyük veri parçalarının kolaylıkla süzgeçten geçirilmesini sağlar. Anlamli hâle getirilen veri yığınları, veri tabanlarını oluşturur. Veri tabanları ise, istenildiği zaman tekrar tekrar kullanılma olanağı sunmaktadır. Veriyi elde etme ve veri madenciliği ile işleme, büyük kuruluşlar ve devletler için önemli bir hazine olan bilgiyi ortaya çıkarır. Yaşadığımız çağ bilgi toplumu çağı olarak da adlandırılmaktadır. Bu çağ, bilginin güç, gücün ekonomi olduğu anlamına da gelmektedir.

Teknolojilerin kullanımının yaygınlaşması, toplumları ve yaşayışları da birbirine yaklaştırmaktadır. Bu durum, kültürlerarası etkileşim köprüleri kurulmasını sağlarken, aynı zamanda toplumların farklılıklarını yok eden küreselleşme olgusunu da beraberinde getirir. Hem bilgi ve iletişim teknolojilerinin günden güne gelişmesiyle hem de küreselleşmeyle birlikte mekân ve sınırlar ortadan kalkmaktadır. Bu durum, kişisel verilerin de küreselleşerek, birçok yerde işlenmesine, depolanmasına ve aktarılmasına sebep olur. Kişilerin toplumdaki yeri, alışkanlıkları veya davranışları bu veriler aracılığıyla belirlenir. Kişisel verilerin, yeni teknolojiler ve küreselleşme süreçleriyle devletler ve özel kuruluşlar için yeni bir hammadde kaynağı olduğunu söylemek yanlış olmayacaktır. Buna istinaden özel kuruluşlar verileri, yeni pazarlar amaçlı kullanırken, devletler ise, güvenlik unsurlarını sağlama amaçlı kullanır. Kişisel veriler, doğru sonuçlara ulaşmadaki devletlere ve özel kuruluşlara sunduğu kolaylıklar sayesinde sıklıkla başvurulan bir konuma gelerek küresel güçler için önemli bir hammadde kaynağını oluşturmaktadır. Bu nedenle, kişisel verilerin korunması için gelişen teknolojiyle birlikte önlemler alınmalıdır. Aksi takdirde verilen örneklerin çoğalması veri mahremiyeti ihlalleri yaşanılması kaçınılmaz olacaktır. Tüm bu süreçler, kişisel verilerin korunması durumunu ortaya çıkarmaktadır. Hangi kurumların, hangi koşullarda verileri elde edeceği ne kadar süre saklayacağı ve ne için kullanacağını bilmek kişisel verilerin korunması için önemli olmaktadır. Ülkeler bazında kişisel verilerin toplanma, işleme, saklanma unsurlarının belirli ölçütlere dayandırılması öngörülmesi ve veri aktarımlarında sınırlayıcı önlemlerin alınması sağlanmıştır. Bu amaçla çalışmada, kişisel verilerin korunma durumu, uluslararası düzenlemelerde ve Türkiye’de oluşturulan mevzuatlar üzerinden incelenmektedir.

Uluslararası Düzenlemelerde Kişisel Verilerin Korunması

Sistemlerde kişisel verilerin korunma durumu aktarılmadan önce, ilk olarak hangi sözleşmelerde yer aldığını, kişisel veriler olarak ilk ne zaman tanımlandığını belirlemek yerinde olacaktır. Kişisel verilerin günümüz tanımını içeren hususlar, uluslararası alanda ilk defa 10 Aralık 1948 tarihli Birleşmiş Milletler İnsan Hakları Evrensel Beyannamesi’nde bulunmaktadır. Kişisel verilerin korunması hususunda içerikler barındıran bir diğer sözleşme ise, 4 Kasım 1950 tarihli Avrupa İnsan Hakları Sözleşmesi’dir. Temel özgürlüklerin korunmasının sağlanmaya çalışıldığı Sözleşme’nin sekizinci maddesinde konuyla ilişkili özel hayat ve aile hayatı, konut ve haberleşmesi koruma altına alındı. Kişisel verilerin korunması konularında hazırlanan bu sözleşmeler, hukuksal düzenlemelerin yapılmasının yolunu açtı.

1960’lardan itibaren bilgi ve iletişim teknolojilerinde artan gelişmeler, kişisel verilerin toplanıp işlenmesi sonucunu getirmiş ve bireylerin özel alanlarını korumaları önemli hâle gelmiştir. Kişisel verilerin, mahremiyet bağlamında değerlendirilmesi ve yasal olarak korunmasının gerekliliği üzerine tartışmalar da 1970’ler itibarıyla başlamaktadır. Tartışmalar Amerika Birleşik Devletleri’nde ortaya çıkmasına rağmen, ilk yasal düzenlemeyi, Avrupa Birliği üye ülkelerinden

Almanya yaptı. Ülkenin “Hessen Eyaleti 1970 yılında Veri Koruma Kanunu’nu” (Aktaran: Oğuz, 2013: 11) yürürlüğe koydu. Hessen Eyaleti, çıkardığı kanunla kişisel verilerin önemini ortaya koymaktadır. Dünyada kişisel verilerin korunmasına yönelik çalışmaların, Hessen Eyaleti kararı sonrasında hız kazandığı görülmektedir. İsveç, 1973 yılında ulusal yasasını çıkararak, ulusal alanda düzenlemeye sahip ilk ülke oldu. OECD ülkeleri ise, 1980 yılında, ilk uluslararası alanda çalışma yayınlayarak, dünya genelinde kapsayıcı özelliğine sahip oldu.

Avrupa Birliği Kişisel Verilerin Korunması

Avrupa Birliği’nin temelleri 1951 yılında, altı ülkenin bir araya gelmesiyle Avrupa Kömür ve Çelik Topluluğu olarak atıldı. 1993 yılında Avrupa Birliği Antlaşması görüşmeleri neticesinde Avrupa Birliği olarak kuruldu.

Avrupa Birliği, kişisel verilerle ilgili ilk düzenleme olarak 1995 yılında “Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Direktif” yayınlayarak Avrupa Birliği üye ülkelerindeki kişisel verilerin korunmasına ilişkin düzenlemelerin uyumlaştırılmasını amaçladı. Avrupa Birliği tarafından 1997 yılında, “Telekomünikasyon Alanında Kişisel Verilerin İşlenmesi ve Mahremiyetin Korunması Yönergesi” yürürlüğe girdi. Bu yönerge Avrupa Birliği’nin gelişen teknolojiler ışığında yenilikçi çalışmalara öncülük ettiğini göstermektedir. Avrupa Birliği, her geçen gün oluşan yeni durumlar ve teknolojiler karşısında kişisel verileri koruyucu çalışmalara yer vermektedir. 2000 yılında Avrupa Birliği Temel Haklar Şartı’nı ilan etti. Avrupa Birliği bu Şart ile üye ülkelerinin bütüncül ilişki içinde bulunmalarını, kişisel verilerin korunması konusunda destekleyici ve sürdürücü olmayı amaçlamaktadır. Avrupa Birliği yaptığı düzenlemeler ile toplanan ve işlenen kişisel verileri bilme hakkını ve yasaya yönelik işleme usullerini çok daha önceden belirlemiş oldu.

Avrupa Birliği, 2004 yılında “Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi’ne Ek Denetleyici Makamlar ve Sınıraşan Veri Akışına İlişkin Protokolü yürürlüğe koydu. Ek metin incelendiğinde, iki alanda kişisel verilerin korunmasının amaçlandığı görülmektedir. Birincisi, kişisel verilerin korunması hususunda kabul edilen yasa ve yönetmeliklere uyulmasının sağlanmasından sorumlu yetkili makamın kurulmasıdır. İkincisi ise, sınır ötesi veri akışında, yalnızca alıcı devlet veya uluslararası kuruluşun yeterli bir koruma seviyesinde olması durumunda aktarımın yapılmasıdır. Diğer düzenlemeler olarak Avrupa Birliği, “Özel Hayatın Korunması ve Elektronik İletişim Yönergesi” ile ileri teknolojik ortamlardaki ilişkileri de kapsayıcı düzenleme çıkardı. Sonrasında, “Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Özel Hayatın Gizliliğinin Korunmasına İlişkin Direktif” ile yenilikçi çalışmalarını sürdürdü.

Avrupa Birliği, her geçen yıl kişisel verilerin korunmasında aldığı kararları yenilemeye ve geliştirmeye devam etmektedir. Bu sayede teknolojinin ve toplumsal gelişimlerin getirdiği yenilikler karşısında bireyin kişisel verilerinin korunmasını sağlayabilmektedir. 2015 yılında veri güvenliğine ilişkin Avrupa Birliği vatandaşlarının algısını ölçen Eurobarometer anket çalışmasının en önemli bulguları, katılımcıların çoğunun verilerinin güvenliğinden endişeli olduğunu, bundan dolayı da verilerinin hâkimiyetini kendi ellerine almak istediklerini göstermiştir (Eurobarometer, 2015). Anket çalışmasından çıkan sonuç, Avrupa Birliği’nde yeniden düzenleme yapılmasında önemli bir faktördür. Buna istinaden, kişisel verilerin korunmasına yönelik en yeni ve en kapsamlı yasa içeriği hazırlayarak 2016 yılının Mayıs ayında General Data Protection Regulation - Genel Veri Koruma Tüzüğü çıkarttı. Avrupa Birliği’nin son düzenlemesi, kişisel verileri korumada özellikle üye ülkeler arasında ve sınır ötesi ticaret alanında artan veri akışları ile yeni teknoloji uygulamalarıyla gelen tehditlere karşı yenilikçi adımı oluşturdu. Ayrıca, yeni yasa ile Avrupa Birliği üye ülkeleri arasında kişisel verilerin korunması konusunda yasa bütünlüğü sağlandı.

Genel Veri Koruma Tüzüğü’nün getirdiği yeni koruma önlemlerini incelemek yerinde olacaktır. Öncelikle, Genel Veri Koruma Tüzüğü’nün kapsayıcı tüzük olmasından dolayı Avrupa Birliği ülkelerinde ve nerede olursa olsun tüm Avrupa Birliği vatandaşları için verilerinin işlenmesinde koruyucu özellik taşımaktadır. Bu nedenle Genel Veri Koruma Tüzüğü için yalnızca Avrupa Birliği sınırlarında değil, küresel ölçekte etkilere sahip bir tüzüktür. Tüzükte veri kontrolörü (data controller), veri işleyici (data processor) yer almaya devam ederken, ayrıca bir veri koruma görevlisi (data protection officer) tanımlaması ile karşılaşılmaktadır. Kontrolör veya veri işleyici verinin sorumlusudur ve veri sahibini hakları konusunda bilgilendirme ve bilinçlendirme yükümlülüğü bulunmaktadır. Veri koruma görevlisi ise, özellikle büyük çaplı veri izlenmeyi gerektiren durumlar ve hassas veri işleyen kurumlar için bir zorunluluktur.

Daha önceki düzenlemelerde yer aldığı gibi kişisel verinin işlenmesi açık rıza ile mümkündür. Tüzükte açık rıza, veri sahibinden, rıza talebi diğer hususlardan açıkça ayırt edilebilecek bir şekilde anlaşılır ve kolayca erişilebilir biçimde açık ve sade bir dil kullanılarak yazılı, elektronik ortam onayı olarak sunulması olarak tanımlanır. Tüzüğün getirdiği unutulma hakkıyla gerçek kişilere, kendisi ile ilgili toplanan kişisel verilerini istediği zaman silinmesini kontrolör veya veri sorumlusundan talep edebilir. Günümüzün dijital dünyasında sistemlerin topladığı çeşitli kişisel verilerle farklı yer ve zamanlarda tekrar karşılaşılmaktadır. Hak sayesinde kişiler, verisini sildirebilir, bir nevi unutulur. Diğer bir hak, kişisel veri ihlâlinin denetim makamına bildirilmesidir. Kişisel verilerin ihlâlinde veri işleyicinin haberdar olduktan sonra en geç yetmiş iki saat içerisinde denetim makamına bildirmesini ifade eder. Bu sorumluluk kişisel veri ihlâli yaşanmadan önlem alınmasını kolaylaştırıcı olmaktadır. Bir başka hak ise, yapılacak bir veri işlemenin gerçek kişilerin hak ve özgürlüklerini koruma açısından yüksek bir risk taşıması ihtimali durumunda, sorumlu kontrolör veya veri işleyici, işlenecek verinin mahiyeti, kapsamı, bağlamı ve amaçları bakımından bir etki değerlendirmesine tabi tutmasıdır. Ayrıca sınır ötesine veri aktarımları, üçüncü ülkeler veya uluslararası kuruluşlara veri işleyici tarafından belirli kistaslara göre yapılmaktadır. Tüzük, kişisel verilerin korunması ve veri ihlâli yaşanmasını önlemek amaçlı idari para cezalarının uygulanışını da düzenlemektedir. Avrupa Birliği kuruluş sürecinden itibaren kişisel veri korunması hakkına önem veren, ilerleyen teknolojiler karşısında en yenilikçi koruma haklarını yürürlüğe koyan ve de koymaya devam eden bir konumdadır.

Avrupa Konseyi Kişisel Verilerin Korunması

Avrupa Konseyi, 1949 yılında on Avrupa ülkesinin imzası ile kuruldu. Konsey, Avrupa ülkelerinde işbirliğinin artırılmasına yönelik oluştu. “Avrupa Konseyinin amacı, üyeleri arasında, müşterek malları olan ülkü ve prensipleri korumak ve yaymak ve siyasi, iktisadi ilerlemelerini sağlamak maksadıyla daha sıkı bir birlik meydana getirmektir” (Avrupa Konseyi Statü Metni, 1949: md.1) olarak açıklanır.

Avrupa Konseyi, kuruluşunun bir yıl sonrasında Avrupa İnsan Hakları Sözleşmesi’ni imzaladı. Bu sözleşme ile üye devletler arasında temel insan haklarını koruma hedeflendi. İnsan haklarına verilen önem ile alınan tedbir kararları, ilerleyen zamanlarda yerini daha özel alanlardaki kişisel verilere bıraktı. Kişisel verilerin korunması, Avrupa Konseyi’nin gündemine ilk girişi 1960’ların sonlarına doğru oldu. 1960’larda bilgi ve iletişim teknolojileri alanında yaşanan gelişmeler, kişisel verilerin gizliliğinin güvence altına alınması konusunda mevcut hukuki ve teknik önlemlerin yetersizliği konusunda artan bir endişenin oluşmasına neden olmuştu. “Dijital devrimin potansiyel etkisi güçlü bir şekilde görülmeye başlanmış ve kişisel verilerin kapsamlı bir şekilde işlenmesine karşı bireyleri korumak için önlemler alınması ihtiyacı net bir şekilde fark edilmeye başlanmıştır” (Aktaran: Atak, 2010: 91).

Kişisel verilerin korunmasının önemine istinaden Avrupa Konseyi, 1973'te "Özel Sektördeki Faaliyet Gösteren Elektronik Veri Bankaları Karşısında Bireylerin Mahremiyetinin Korunması Üzerine Alınan İlke Kararı" ve 1974'te "Kamu Sektöründeki Faaliyet Gösteren Elektronik Veri Bankaları Karşısında Bireylerin Mahremiyetinin Korunması Üzerine Alınan İlke Kararı" (Avrupa Konseyi Veri Koruma Hukuku El Kitabı, 2017: 10) yayınladı. Kabul ettiği iki kararla kişisel verilerin korunması için gerek kamu ve gerek özel sektör kuruluşlarında göz önünde bulundurulması gereken temel ilkeleri belirledi. Aynı zamanda Avrupa Konseyi, kapsayıcılığının geniş olması için uluslararası alanda iki anlaşma hazırladı. İlk olarak, İnsan Hakları Sözleşmesi'nde kişisel verilere yönelik özel bir madde bulunmaması nedeniyle 1981 yılında "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunmasına İlişkin 108 Sayılı Sözleşme" yürürlüğe girdi. Sözleşme'nin hükümleri, taraf ülkelerdeki özel sektörün ve kamu sektörünün tamamını kapsamaktadır. İkinci olarak, 1990 yılında ilk kez, ortaya konan ilkelerin uygulanmasını denetleyecek yetkili ve bağımsız veri koruma organı kurulması önerisini de içeren "Bilgisayara Geçirilmiş Kişisel Veri Dosyalarına İlişkin Rehber İlkeleri" kabul etti. 1995 yılına gelindiğinde ise, "Kişisel Verilerin İşlenmesi ve Bu Tür Verilerin Serbest Dolaşımına Dair Bireylerin Korunması" hakkında yönerge ile birlik dâhilinde verinin korunması alanında yüksek bir standart oluşturulmaya çalışılmıştır. Ayrıca, Avrupa Konseyi Kişisel Verilerin Korunması Yönergesinin elli yedinci maddesinde yer alan, "(...) yeterli ve elverişli koruma seviyesini sağlamayan üçüncü bir ülkeye, kişisel verilerin transferi yasaklanmalıdır" ifadesi, Avrupa Birliği'nde olduğu gibi önemli görüldü. Avrupa Konseyi, kuruluşundan itibaren kişisel verilerin korunmasını sağlamakta ve gerekli görülen alanlarda düzenlemeler getirmektedir.

Birleşmiş Milletler Kişisel Verilerin Korunması

Birleşmiş Milletler, ülkeler arasında ekonomik iş birlikleri yapma amacıyla beş ülkenin (ABD, İngiltere, Sovyet Rusya, Çin Halk Cumhuriyeti, Fransa) bir araya gelmesiyle oluşturuldu. Birleşmiş Milletler'in kuruluş anlaşması, 1945 yılında elli ülke tarafından imzalandı. BM'nin günümüz üye devlet sayısı üç katından fazlasına ulaşmış durumdadır.

Birleşmiş Milletler hukukunda, kişisel veriler, ilk defa 1948 yılında Birleşmiş Milletler İnsan Hakları Evrensel Bildirgesi tarafından güvence altına alındı. İnsan haklarını koruma güvencesi ve uluslararası alanda bağlayıcı hükümleri olmasıyla çıkarıldığı tarih veri koruma için önemli olmaktadır. Beyanname'nin on ikinci maddesine istinaden, bireylerin, kişisel verileri olarak kabul edilen özel hususlarına kimsenin karışamayacağı belirtilmektedir. Birleşmiş Milletler, 1990 yılında kişisel verilerin korunması konusunda, ortaya konan ilkelerin uygulanmasını denetleyecek yetkili ve bağımsız veri koruma organı kurulması önerisini de içeren "Bilgisayarla İşlenen Kişisel Veri Dosyaları Hakkında Yönlendirici İlkeler" adlı genel ilkeleri kabul etti. Bu ilkeler; "Yasallık ve Dürüstlük, Doğruluk, İlgili Kişilerin Erişme Hakkı, Ayrımcılıktan Kaçınma, İstisna Koyma Yetkisi, Güvenlik, Denetim ve Yaptırım ile Sınır Ötesi Veri Transferi" (Kılınç, 2011: 1111) olarak yer almaktadır.

Bilgi ve iletişim teknolojilerinin gelişmesi, kişisel verilerin korunmasına yönelik daha kapsamlı uluslararası düzenlemelere olan ihtiyacı artırdı. Bu noktada, Birleşmiş Milletler, kuruluşundan itibaren temel hakların koruyucusu oldu. Özellikle bilgisayarla işlenen kişisel verilerin korunmasına yönelik getirilen koruyucu ilkeler ile önemli adımlar atıldı. Diğer Avrupa sistemlerinde olduğu gibi Birleşmiş Milletler de kişisel veriler konusunda günün gereklerini yakalamaya çalışmaktadır.

Amerika Birleşik Devletleri Kişisel Verilerin Korunması

Amerika Birleşik Devletleri, kuruluşundan bugüne kadar ekonomik gücün en büyük simgelerinden biri olurken, sermaye ve hammaddeyi elinde bulundurarak küresel bir güç halini almakta, teknoloji ve bilginin de kilit taşlarından olmaktadır. Amerika Birleşik Devletleri’nde, kişisel verilerin korunması gerekliliği üzerinde tartışmalar 1970’li yıllardan itibaren başladığı görülmektedir. Yine de kişisel verilerin korunması konusunda Avrupa Birliği’ den sonra koruyucu çalışmalar yapıldı. 1974 yılında, Gizlilik Yasası çıkarıldı. Daha sonrasında bu yasayı “Mali bilgilerin korunmasına yönelik 1978 tarihli Mali Mahremiyet Kanunu, 1996 tarihli İletişim Ahlak Yasası, 1998 tarihli Çocukların Çevrimiçi Korunması Yasası (Aktaran: Boz, 2014: 76) takip etti.

Amerika’da çıkan bu yasa, bireyleri koruma ve diğer bireylerin kişisel verilere ulaşmasına karşı olarak değil, ülkenin yapısı itibariyle uluslararası kuruluş ve federal devletin topladığı kişisel verilerin işlenmesinin önlenmesine karşı olarak düzenlenmiştir. Solove ve Hoofnagle çalışmalarında “Amerika’da kişisel verilerin daha çok özel sektör alanında düzenlemelere ihtiyaç duyduğunu, fakat kamu sektörünün parlamentoya karşı sorumlu olması ve bu kurum tarafından denetleniyor olması nedeniyle daha az düzenleme yapılması gerektiği ileri sürülmektedir” (Aktaran: Kılınç, 2012: 1119). Kişisel verilerin korunması adına tek bir kanun yapmaktansa, birçok alana özgü kişisel veri düzenlemesinin yapılması kapsayıcı olmaktan çok, dağınık bir yapı (Boz, 2014:75) arz ettiği de belirtilmektedir.

OECD Ülkeleri Kişisel Verilerin Korunması

OECD (Organisation for Economic Co-Operation and Development-Ekonomik İş birliği ve Kalkınma Teşkilatı) 1960 yılında yirmi kurucu ülke ile oluştu. Kurucu ülkeler, Avrupa olarak ekonomik gelişme ve kalkınmaya destek amacıyla bir araya geldi. Kişisel verileri koruma konusunda Teşkilat, ilk uluslararası çalışmayı 1980 yılında yayınladı. Teşkilatın yayınladığı ilk düzenleme “Özel Yaşamın Korunması ve Kişisel Verilerin Sınırötesi Akışına İlişkin Rehber İlkeleri” oldu. Ekonomik İşbirliği ve Kalkınma Teşkilatı veri korunmasına ve veri akışının kontrol altına alınmasına yönelik olarak, 1980 yılında 8 yönlendirici ilke belirlemiştir. Sınırlandırma İlkesi, Veri Kalitesi İlkesi, Amacın Belirli Olması İlkesi, Kullanımın Sınırlandırılması İlkesi, Veri Güvenliği İlkesi, Açıklık İlkesi, Bireyin katılım İlkesi ve Hesap Verebilirlik İlkesi (Aktaran: Kılınç, 2012: 1109-1110) olarak sıralanmaktadır.

Günümüzde konuya ilişkin bütün ulusal ve uluslararası mevzuat, Teşkilatın yönlendirici ilkelerini dikkate almaktadır. Teşkilat ilerleyen zamanlarda gereklilikler üzerine yeni bildirgeler de yayınladı. Bunlar, “Sınırötesi Veri Transferi Hakkında Bildirge” ve “Global Ağ Gizliliğinin Korunması Hakkında Bakanlık Bildirgesi” şeklindedir. Avrupa Birliği bünyesinde kurulan bu sistemler ekonomik iş birlikleri amaçlarıyla kurulmalarına rağmen, bu iş birliklerinden oluşan, birbirlerine ve üçüncü şahıslara aktarılan kişisel veriler konusuna uzak kalmayarak, birlik içinde yürürlüğe sözleşmeler koymuşlardır. Bu sözleşmeleri günün koşullarına göre yeniden düzenlemiş ve daha kapsayıcı çalışmalara imza atmışlardır. Hatta birlik sınırları içerisinde kalmayacak şekilde uluslararası bağlayıcı hükümlerin olmasını sağlamışlardır.

Türkiye’de Kişisel Verilerin Korunması

Türkiye kişisel verilerin korunması konusunda kendi hukuk düzenlemesini oluşturmadan önce, uluslararası alanda yapılan anlaşmalarda taraf olarak yer aldı. Türkiye bu anlamda, Birleşmiş Milletlerin İnsan Hakları Evrensel Bildirgesi’ni imzalayan kurucu ülkelerden birisi olmuştur. Kişisel verilerin korunması çalışmalarında, Avrupa Konseyi’nin Avrupa İnsan Hakları Sözleşmesi 10 Mart 1954 tarihinde onaylandı. Avrupa Konseyi’nin 1981 yılında imzaladığı “Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunmasına ilişkin 108 sayılı Sözleşme” Türkiye tarafından da imzalamasına rağmen, onaylanması 2016 yılında yapıldı.

Türkiye’de kişisel verilerin korunması, koruyucu bir yasa çıkartılana kadar iç hukukta Anayasa’ya eklenen maddeler, kanun hükmünde kararname, sözleşmeler yoluyla ayrı ayrı güvence altına alınmaya çalışıldı. Anayasa incelendiğinde, kişisel veri korunması başlığı altında bütüncül ve bağlayıcı yasa bulunmamaktadır. Buna karşın Anayasa’da yönetmelikler ve buna bağlı maddeleri ile diğer kanun maddelerinde ve imzalanan sözleşmelerde, kişisel veri korunmasına ve haklarına değinilmektedir. Bu bağlamda Anayasa maddeleri incelendiğinde, özel hayatın gizliliği (md. 20), haberleşmenin gizliliği (md. 22), dini ve vicdani kanaatleri açıklamaya zorlanmama (md. 24), düşünce ve kanaatleri açıklamaya zorlanmama (md. 25) gibi temel hakların mevcut olduğu gözlenmektedir. Anayasa’da kişisel verilerin korunmasının bir başlık altında birleşmesi, “2010 yılında yapılan Anayasa değişikliği” (Kişisel Verileri Koruma Kurumu, 2018: 2) ile birlikte ilk kez Anayasa’da “Özel Hayatın Gizliliği ve Korunması” başlığı altında girmesi geç dönemlere rastlamaktadır.

Türkiye’de kişisel verilerin korunmasının yasal güvencelere dayandırılması uluslararası anlaşmalar dışında -ki 108 Sayılı Sözleşme’nin imzalanmasına rağmen yürürlüğe girmesi çok uzun sürdüğü göz önünde bulundurularak- Anayasa değişiklik teklifinin 2010 yılında yapılmasına kadar koruyucu tedbirler çok dağınık bir yapı göstermekteydi. Teknolojinin ilerlemesi ve getirdiği yenilikler karşısında kişisel verilerin korunması, Anayasa’da yer verilen kanunlar ile sağlanmaya çalışılmaktaydı. Bu durum ise, bütüncül çalışmanın oluşmasını geciktirdiği kadar, veri ihlali durumuyla karşılaşmadan önlem getirilmesini de engelleyici olmaktadır.

Türkiye’de Anayasa’ya bağlı olarak çıkartılan maddelerde ilk olarak, kişisel verilerin korunmasından Türk Medeni Kanunu’nun Kişiliğin Korunması kısmında söz edilir. İlgili kısma göre, Türk Medeni Kanunu’nun yirmi dördüncü maddesi tespit hükmünden kişinin, kişisel verisinin izinsiz kullanıldığı tespit edilebilir veya kişinin, kişisel verilerinin hukuka aykırı kullanılacağı konusunda bir endişesi söz konusuysa bu endişesini önleme davasıyla önleyebilir. Eğer ihlal başlamışsa bununla ilgili yine durdurma davası açılabilir (Altaş, 2015: 3). Medeni Kanunu’nda ayrıca kişiliğin tanımı yapılmakla birlikte getirdiği durumla ilgili de görüşler bulunmaktadır. Kanun’un yirmi sekizinci maddesinde “kişilik sağ ve tam doğmak şartıyla ceninin ana rahmine düştüğü andan itibaren başlar ibaresi bulunmaktadır. Kişilik yine ölümle sona erer. Bu durumda, ölümle kişilik sona ereceğinden, ölen kişinin kişisel verileri Kişisel Verilerin Korunması Kanunu kapsamında korunmayacaktır (Yücedağ, 2017: 766). Bu çerçevede “açıklığa kavuşturulması gereken mesele ise, doğmamış çocuklara ilişkin veriler ile ölmüş kişilere ilişkin verilerin, kişisel veri olarak değerlendirilip değerlendirilemeyeceği hususudur” (Zümbül, 2018: 2). Avrupa Birliği Veri Korumasına İlişkin Tüzük’de, küçüklerin kişisel verilerinin işlenmesine ilişkin detaylı düzenlemeler getirilmişken, Kişisel Verilerin Korunması Kanunu’nda küçüklerin kişisel verilerinin işlenmesine ilişkin herhangi bir özel düzenleme getirilmemiştir (Yücedağ, 2017: 767). Buradan hareketle aslında anne karnında henüz doğmamış bir bebeğin, ölçülen fiziki özellikleri, sağlık verileri gibi veriler de kişisel veri olmalıdır, kişinin ölümü gerçekleştiğinde geride bıraktığı veriler de yine kişisel veri statüsünde korunmaya devam edilmelidir. Yine, kişinin ölümü gerçekleştiğinde

geride bıraktığı verilerin korunmaya devam edilmesi hususunda tartışmalar bu şekildeyken, 21 Haziran 2019 tarihinde yürürlüğe konulan Kişisel Sağlık Verileri Yönetmeliğinde, ölen kişinin, kişisel verisi en az yirmi yıl saklanır hükmü getirildi. Böylece, ölen kişilerin de kişisel verileri ve kişisel sağlık verileri korunarak önemli bir konuda adım atıldı.

Türk Ceza Kanunu’nda, kişisel verilerin (kişinin görüşleri, üye kuruluşları ve sağlık durumları gibi) kişisel tercihlerinin hukuka aykırı olarak kaydedilmesi suç teşkil eden bir eylem olarak belirlenmektedir. Bir diğer kanun olan, Ceza Muhakemesi Kanunu’nda kişisel verilerin işlenmesi, ilgili maddelerine göre, kişisel kimlik belirleyici veriler suç işlediğinde elde edilebilir ancak üçüncü kişilere yayılamaz hükmünü içermektedir. İş Kanunu’na göre ise, işçilerin özlük dosyasının dürüstlük kuralları ve hukuka uygun olarak kullanılmasını zorunlu kılar. Bilgi Edinme Hakkı Kanunu’na göre de, kişinin kendisiyle alakalı tutulan bilgileri öğrenme hakkı verilmiştir. Kanun, verilere erişim sayesinde ilgili kişinin, başvurması halinde kendisi hakkında tutulan bilgilerin kopyasını elde etme, not alma veya dinleme imkanına sahip olabilmektedir. “Bilgi edinme hakkı, bir yandan düşünce ve düşünceyi açıklama özgürlüğüyle bağlantısı itibariyle, yeni olmayan bir haktır. Diğer yandan yurttaşın yönetimden hesap istemesi hakkıyla bağlantılıdır ve yeni haklar kuşağı olarak da anılan üçüncü kuşak hak ve özgürlükler arasında anılmaktadır” (Asrak Hasdemir, 2014: 115). Bilgi Edinme Hakkı Kanunu, henüz kişisel verilerin korunması konusunda bütüncül çalışmaları bulunmadığı, düzenlemelerin olması gerektiği yönünde görüşlerin geliştiği dönemde kabul edildi. 2003 yılında çıkarılan bu kanun ile şeffaflık adına bir eksiklik giderilmeye çalışılmış ve kamu kurum faaliyetlerinin topluma açılması sağlanmıştır. Ancak içerisinde barındırdığı sınırlılıklar nedeniyle eleştirildiği başlıklar olmuştur. Nitekim bu durum, yasanın uzmanlarca en çok eleştirilen yönlerinden biri de özel sektörün kapsama alınmamasıdır (Asrak Hasdemir, 2014: 122) şeklinde belirtilmektedir. Elektronik Haberleşme Kanunu’nda, sektörle ilgili kişisel verilerin işlenmesi ve gizliliğinin korunmasına yönelik usul ve esaslar belirlendi. Bankacılık Kanunu, banka çalışanlarının, müşterilere ait gizli bilgileri, kanunen açıkça yetkili kılınan mercilerden başkasına açıklanamayacağını düzenlemektedir.

Türkiye’de kişisel verileri koruma konusunda 2010 yasa değişikliğine kadar Avrupa Birliği’nin ilave kararlarına rağmen, somut bir adım atılmadı. Yasa değişikliğinde alınan karar neticesinde kişisel verileri koruma adına kanun çalışmalarına başlandı. Türkiye, Kişisel Verileri Koruma Kanun Tasarısı’nı 2011 yılında oluşturmaya başladığı halde, tasarı uzun bir bekleyişte kaldı. Bu arada Anayasa’ya bağlı olarak da kişisel verileri koruma kanunları eklenmeye devam etmiştir. Son olarak 2014 yılında Elektronik Ticaretin Düzenlenmesi Hakkında Kanun yayınlandı. Kişisel verilerin korunması konusunda kanun çalışması, gerek Avrupa Birliği üyelik müzakereleri için gerekse bütüncül, kapsayıcı bir koruma kanuna olan ihtiyaç nedeniyle beklenmekteydi. Ayrıca, Kanunu’nun çıkmasında Adalet Bakanlığı’nca hazırlanan rapor başlıklarında geçen, “Türkiye’nin veri güvenliği konusunda güvenilmez ülke” (Aktaran: Çelik, 2014) olarak nitelendirilmesi de etkili oldu. Sürecin ardından, Adalet Bakanlığı’na bağlı kurumlarca hazırlanan ve sorumluluk açısından Başbakanlığa bağlı olarak oluşturulan Kişisel Verilerin Korunması Kanunu 2016 yılı Nisan ayı itibariyle kabul edildi. Kişisel Verileri Koruma Kanunu çıkartılması ile birlikte Anayasa ve diğer düzenlemelerde alınan tedbirlerin ve tanımlamaların bir kanun çerçevesinde toplanması sağlandı. Kişisel verilerin korunması yönünde gerçekleştirilen en ilerici adımı bütüncül bir kanun ile sabitlenmesi oluşturdu.

2011 yılı itibariyle hazırlanan kanun tasarısı ve 2016 yılı itibariyle yürürlüğe giren kanunun maddeleri incelendiğinde, tasarıya eklenen ve çıkarılan bazı ifadeler dışında, büyük kısmının değiştirilmeden kabul edildiği görülmektedir. Diğer taraftan Türkiye için beklenen bir kanun olmakla birlikte, kanun maddelerinin bir kısmı olumlu karşılanırken, bir kısmı da eleştirilere konu

oldu. Öncelikle Kişisel Verilerin Korunması Kanunu ile kişisel veri ve hakların tanımlaması geniş bir çerçevede ele alınmıştır. Buna göre kişisel veri, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi olarak tanımlanır. Yine Kanun'da veri işleyici, veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişiyi; veri sorumlusu ise, kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi ifade eder. "Kanunun uygulaması bakımından kamu ve özel sektör ayrımı yapılmamış olup, düzenlenen usul ve esaslar her iki sektör bakımından da uygulama alanı bulmaktadır" (Korkmaz, 2016: 88).

Kanun'da açık rıza unsurları da düzenlenmiştir. Hiçbir kişisel verinin kişinin açık rızası olmadan işlenmesi mümkün olmamaktadır. Kanun'un altıncı maddesinde, özel nitelikteki ırk, etnik köken, siyasi düşünce, felsefi inanç, din, mezhep veya diğer inançlar, kılık ve kıyafet, dernek, vakıf ya da sendika üyeliği, sağlık, cinsel hayat, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verilerin işlenmesi yasaklandı. Ancak sağlık ve cinsel hayat dışındaki verilerin, kanunlarda gerekli görülen hâllerde işleneceği ve açık rızanın aranmayacağı belirtilir. Bir örnekle açıklamak gerekirse, Adli Sicil Kanunu'na göre siz bir yerde suç işlemişseniz, sizin sicilize bununla ilgili olarak birtakım işlemlerin yapılması diğer özel kanunlardan kaynaklandığı için bu kanun açısından istisnai bir durumdur (Sırataş, 2015: 5). Bir başka açıdan ise, özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınması şart koşulmuş olmasına rağmen yeterli önlemin ne olduğu bile yeterince açıklanmamıştır (İlkiz, 2016). Bu durum itirazlara konu olmuşsa da kanun maddesi aynı şekilde kabul edilmiştir (Habertürk, 26 Şubat 2016). İşlenen kişisel verilerin ilgili mevzuatta öngörülen ve işlendikleri amaç için öngörülen süre kadar muhafaza edilebileceği de belirtilir. Bu düzenleme süre olarak çok geniş ve yoruma açık bir süreyi kapsamaktadır. Hangi kurumun ne kadar süre ile kişisel verileri muhafaza edebileceğine bir sınırlama getirilmelidir. Aynı zamanda içerik, yani boyut ve miktar olarak da bir sınırlaması olmalıdır (Çayır, 2016).

Avrupa Birliği'nin hazırladığı Tüzükte yer verdiği unutulma hakkını, Kişisel Verileri Koruma Kanunu'nda kişisel verilerin silinmesi, yok edilmesi veya anonimleştirilmesi başlığı altında bulunan maddeler karşılamaktadır. İlgili düzenlemeye göre, "kişilerin şiddetin bir türüne maruz kaldıklarında veyahut bir işletmenin çalışanından ötürü yaşadığı bir kriz ve devamında uğradığı itibar kaybından dolayı oluşan durumun kullanılan kaynaklardan çıkartılmasını ve unutulmasını isteme hakkıdır" (Pehlivan, 2016). Kanun'da herhangi bir kişisel veri ihlâli veya şikâyet durumunda Kurul, şikâyetlerini karara bağlamak ve şikâyet üzerine veya ihlâl iddiasını öğrenmesi durumunda resen görev alanına giren konularda kişisel verilerin kanunlara uygun olarak işlenip işlenmediğini incelemek ve gerektiğinde bu konuda geçici önlemler almak ile sorumludur. Kurul yapılan incelemeler sonrası hukuka aykırılığın tespiti halinde veri sorumlusundan otuz gün içerisinde bu ihlalin giderilmesini istemektedir. Böylece kişisel verilerin ihlalinde yetkili merciler belirlenmiş olmaktadır.

Kanun'da dokuzuncu maddede düzenlenen yurt dışına kişisel verilerin aktarımı konusu yine açık rızaya bağlı olarak gerçekleşmektedir. Ancak bu rıza genel değil özel nitelikte olmalıdır. Yani, kişisel verilerin aktarılması için genel bir şekilde bir rıza tanınmış olması, kişisel verilerin yurt dışına da aktarılmasına rıza verildiği anlamına gelmemektedir (Melih hukuk, 2016). Ayrıca Kanun'da kişisel verilerin yasal dayanakları olmadan işlenmesi, aktarılması, anonim hale getirilmemesi veya silinmemesi durumlarında hakları korumak adına idari para cezaları da düzenlendi. Gerekli yükümlülüklerini yerine getirmeyen özel ve tüzel kişisel veri sorumlularına karşı farklı ölçütlerde bir milyon liraya kadar idari para cezaları kesilebilecektir.

Sonuç

Teknolojinin gelişmesi ve yaşantımıza yön vermeye başlaması, kişisel verilerin korunmasının önemini bir kat daha arttırdı. Teknolojik gelişmelerin uzantısı uygulamalar ve sosyal hesaplar kişilere ulaşmayı ve haklarında bilgi, görüntü, düşünce sahibi olmayı kolaylaştırdı. Kişilerarası konuşma ve paylaşımlara ulaşmak anlık olacak kadar hızlanmakla beraber geldiğimiz noktada, kişisel olarak yayılan verilerin güvenliğinin sağlanması meselesi öne çıkmaktadır. “Ancak burada husus teknoloji değil; söz konusu teknolojilerin sağladığı olanaklardan yararlanmaya çalışan şahısların, kamu görevlilerinin ve kamu kurumlarının insan hak ve özgürlüklerine ilişkin tutumları, bakış açıları, alışkanlıkları ve zihniyet dünyaları olmalıdır” (Yüksel, 2009: 276). Tüm yapılan araştırmaların ışığında kişisel verilerin korunmasının önemi fark edilmiş olup, verilerin güvenliğinin sağlanmasına yönelik dünyanın birçok ülke ve topluluklarında yasalar ve koruyucu sözleşmeler geçmişten günümüze düzenlenmektedir. Başta Avrupa ülke ve toplulukları ile Amerika olmak üzere Türkiye’de de çalışmalar yapılmış ve günün gereksinimlerine göre yapılmaya devam etmektedir. Her ülke kendi yapısına uygun olarak kişisel verileri hem devlet hem de özel kuruluşlar nazarında korumaya çalışmakta ve veri ihlalleri yaşanmaması için tedbirler almaktadır.

Avrupa Birliği’nde kişi öncelikli ve kişinin mahremiyetini başkalarına karşı korumaya yönelik kararlar alındı. Gelişen iletişim araçları ve teknoloji karşısında bireylerin kişisel verilerinin korunması konusunda alınan tedbirlere öncülük etmişlerdir. Birleşmiş Milletler, kişisel verilerin korunmasında uluslararası bağlayıcı ve üye ülke sayısı ile en çok sözleşmeye öncülük etmiş durumdadır. Avrupa Konseyi, kuruluş tarihinden itibaren kişisel hak ve özgürlüklere yönelik sadece örgüt içinde değil tüm dünyayı kapsayıcı koruyucu antlaşmalara öncülük etti. Amerika Birleşik Devletleri’nde alınan kararlar ise, kişilerin hassas verilerini üçüncü şahıslara karşı koruma amaçlı olmaktan ziyade, özel kuruluşların politikalarına paralel alınarak sektörler lehine sonuçlandı. Bu durum karşısında Avrupa Birliği, daha fazla veri koruma için Amerika Birleşik Devletleri ile Güvenli Liman Anlaşması’nı yeniledi. Avrupa Birliği kendi mevzuatına uygun olmayan bir ülkeyle transferler konusunda hassas davranmaktadır. OECD üye ülkelerinin kişisel verileri koruma sözleşmesini imzalaması uluslararası veri koruma ve transferlerine standartlar getirilmesini sağladı.

Türkiye’de bir çerçeve yasa bulunmadığı dönemlerde gerek Anayasa gerek Anayasa’ya bağlı olarak çıkartılan yönetmelikler ve de diğer hukuk maddelerinde ihtiyaç duyulan düzenlemelerle sağlanmaya çalışıldı. Kişisel Verilerin Korunması Kanunu ile birlikte, bütüncül ve kapsayıcı bir kanun elde edilmiş ve veri koruma ile alakalı yasal çerçeveler çizildi. Tüm incelenen süreçte Türkiye’nin geçirdiği aşamalarda en büyük olumlu yön, kişisel verilerin korunmasını sağlayacak bütüncül bir kanunun karşımızda olmasıdır. Kanunun getirdiği haklar olarak, açık rıza, aydınlatma yükümlülüğü, veri silinmesi, anonimleştirilmesi ve koruma kurulu ile ihlalin önlenir olması gibi haklar olumlu yönde sonuç ortaya koymaktadır. Yüksek miktarlardaki idari para cezaları, kişisel verilerin kanuna aykırı toplanmasını, işlenmesini ve saklanmasını önleyici görünmektedir. Diğer yandan Kanun’un geçirdiği üç yılda işleyiş süreci de önemli olmaktadır. Avrupa Birliği kişisel verilerin korunmasında son Tüzüğü’nün gerektirdiği iş birliklerini, veri işlemede güvenlik ve mahremiyet çabasında ilerleme kaydettiği (European Data Protection Supervisor, 2018: 19) yer almaktadır. Türkiye raporuna göre ise, kişisel verilerin korunmasına ilişkin mevzuat mevcut olmakla birlikte, henüz Avrupa standartlarıyla uyumlu değildir. Bu durum, özellikle Kişisel Verileri Koruma Kurumu’nun yetkilerine ve kişisel verilerin korunması ile ifade ve bilgi edinme özgürlüğü hakkı arasında bir denge kurulmasına ilişkin hususlar ile ilgilidir (Avrupa Komisyonu Türkiye Raporu, 2018: 33). Komisyonun Türkiye başlığında hazırladığı 2019 raporunda da aynı ifadeler yer almaktadır. Türkiye’de hazırlanan rapora göre ise, 2018 yılında kırk bir tanesi

ihlâl olmak üzere iki yüz altmış dokuz tane de şikâyet başvurusu vardır. İhlallerin çoğu kişisel verilerin işlenmesi veya paylaşılmasıyla ilgilidir. Başvurular en çok medya, kamu ve bankacılık sektörlerinde yoğunlaşmaktadır. İhlallerin tespitinde para cezaları uygulandığı belirtilmektedir (Kişisel Verileri Koruma Kurumu Faaliyet Raporu, 2018: 30).

Kişisel verilerin korunmasında, en büyük sorun hukukun statik olmasına karşılık, teknolojik alandaki gelişmelerin çok dinamik olmasıdır (Özen, 2015: 10). Bu noktada önemli olan dinamik teknolojik alana uyum sağlayacak koruma önlemlerinin var olması ve sürekliliğinin sağlanması ve de uygulanmasıdır. Ayrıca, hak ihlallerine karşı bireysel anlamda bilinç ve dikkat düzeyi de önemli olmaktadır. Kanun'un bireyi korumada ne haklar getirdiği, toplum bireyleri tarafından bilinirliğinin sağlanması ve özümsemesi gerekmektedir.

Sonuç olarak, çalışmada veri koruma konusunda ele alınan Avrupa Konseyi'nin 2007 yılından itibaren 108 Sayılı Sözleşme'nin kabulü olan 28 Ocak günü, Avrupa Veri Koruma Günü olarak kutlanmaktadır. Ülkemizde ise, kanunun yürürlüğe girdiği 2016 yılı itibariyle 28 Ocak günü Veri Koruma Günü olarak kutlanmaktadır. Bu özel günün, her geçen an gün ve yılda bilinirliğinin, öneminin artarak kutlanması ile birlikte kişisel verilerin korunması konusunda bir duyarlılık ve bilinç geliştirilmesine katkıda bulunması temenni edilmektedir.

Kaynaklar

Altaş, H. (2015). "Kişisel Verilerin Korunması ve Mahremiyet", *Gelişim Hukuk Topluluğu Konferansı*, s.1- 3.

Asrak Hasdemir, T. (2014). "Türkiye'de Kamusal İletişim ve Bilgi Edinme: 10 Yılın Ardından Panoramik Bir İnceleme", *Amme İdaresi Dergisi*, 47(3), s.111-144.

Atak, S. (2010). "Avrupa Konseyi'nin Kişisel Veriler Açısından Sağladığı Temel Güvenceler", *TBB Dergisi*, 87, s.90-120.

Avrupa Birliği Genel Veri Koruma Tüzüğü (2016). https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en. Erişim Tarihi: 2.11.2018.

Avrupa Komisyonu Türkiye Raporu (2018). <https://www.ab.gov.tr/siteimages/pub/komisyonulkeraporlari/2018turkiyeraporutr.pdf>. Erişim Tarihi: 01.08.2019

Avrupa Konseyi Statü Metni (1949). <https://insanhaklarimerkezi.bilgi.edu.tr/tr/content/29-avrupa-konseyi-genel-bilgi/>. Erişim Tarihi: 10.11.2018.

Avrupa Konseyi Veri Koruma Hukuku El Kitabı (2017) <https://kpveri.com/wp-content/uploads/2017/07/avrupaVeriKorumaHukukuElKitabi.pdf>. Erişim Tarihi: 15.11.2018.

Birgün, 25 Ekim 2014.

Bauman, Z. ve Lyon, D. (2013). *Akışkan Gözetim*, (Çev. Elçin Yılmaz), İstanbul: Ayrıntı Yayınları.

Boz, A. (2014). *Kişisel Verilerin Korunması: Türkiye, ABD ve AB Örnekleri*, (Yüksek Lisans Tezi), Ankara.

Çayır, Faruk, (2016). “Kişisel Verilerin Korunması Kanununa İlişkin Değerlendirme”, <https://yenimedya.wordpress.com/2016/04/27/kisisel-verilerin-korunmasi-kanuna-iliskin-degerlendirme/>. Erişim Tarihi: 1.06.2016.

Çelik, Halil, (2014). “Türkiye’nin Kişisel Verileri Koruma Serüveni”, http://www.academia.edu/5780340/T%C3%BCrkiye_nin_Ki%C5%9Fisel_Verileri_Koruma_Ser%C3%BCveni. Erişim Tarihi: 25.04.2016.

Devlet Denetleme Kurulu Raporu. (2013). *Kişisel Verilerin Korunmasına İlişkin Ulusal ve Uluslararası Durum Değerlendirmesi ile Bilgi Güvenliği ve Kişisel Verilerin Korunması Kapsamında Gerçekleştirilen Denetim Çalışmaları*, Ankara: Devlet Planlama Teşkilatı, 3, s.778 –817.

Esen, F. (2016). “Finansal Suçların Tespitinde Veri Madenciliği Yaklaşımı ve Literatüre Bakış”, *Eskişehir Osmangazi Üniversitesi İktisadi ve İdari Bilimler Dergisi*, 11(2), s.93-118.

Eurobarometer Veri Koruma Raporu. (2015). İKV Değerlendirme Notu, 2018.

European Data Protection Supervisor (2018), https://edps.europa.eu/data-protection/our-work/publications/annual-reports/2018-annual-report-new-era-data-protection_en. Erişim Tarihi: 20.08.2019.

Habertürk, 26 Şubat 2016.

İlkiz, Fikret, (2016). “Kişisel Verilerin Korunmaması Kanunu.” <http://bianet.org/bianet/bianet/174173-kisisel-verilerin-korunmaması-kanun>. Erişim Tarihi: 1.06.2016.

İzgi, M.C. (2014). “Mahremiyet Kavramı Bağlamında Kişisel Sağlık Verileri”, *Türkiye Biyoetik Dergisi*, 1(1), 25-37.

Kılınç, D. (2012). “Anayasal Bir Hak Olarak Kişisel Verilerin Korunması”, *Ankara Üniversitesi Hukuk Fakültesi Dergisi*, 61(3), s.1089-1169.

Kişisel Verilerin Korunması Kanunu, Kanun Numarası: 6698, Resmî Gazete Tarih: 7.4.2016, Sayı: 29677.

Kişisel Verilerin Korunması Kanun Tasarısı, (2014). www.adalet.gov.tr/Tasarilar/kisisel_verilerin_korunmasi.pdf. Erişim Tarihi: 20.04.2016.

Kişisel Verileri Koruma Kurumu, (2018). “Anayasal Bir Hak Olarak Kişisel Verilerin Korunmasını İsteme Hakkı”, <https://www.kvkk.gov.tr/Icerik/4184/Anayasal-Bir-Hak-Olarak-Kisisel-Verilerin-Korunmasini-Isteme-Hakki>. Erişim Tarihi: 17.06.2018.

Kişisel Verileri Koruma Kurumu Faaliyet Raporu, (2018). <https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/cef9699a-579d-4fbd-ab45-cade6f2bba3b.pdf>. Erişim Tarihi: 01.08.2019.

Korkmaz, İ. (2016). “Kişisel Verilerin Korunması Kanunu Hakkında Bir Değerlendirme”, *TBB Dergisi*, 124, 82-150.

Melih Hukuk, (2016). “Kişisel Verilerin Korunması Kanunu” (<http://www.melihhukuk.com/avukat/kisisel-verilerin-korunmasi-kanunu>). Erişim Tarihi:10.06.2018.

Oğuz, H. (2013). “Elektronik Ortamda Kişisel Verilerin Korunması, Bazı Ülke Uygulamaları ve Ülkemizdeki Durum”, *Çağ Üniversitesi Elektronik Ticaret Hukuku Sempozyumu*, s.2-37.

Özen, M. (2015). “Kişisel Verilerin Korunması ve Mahremiyet”, *Gelişim Hukuk Topluluğu Konferansı*, s.9-11.

Pehlivan, Oğuz Kaan, (2016). “Kişisel Verilerin Korunması Kanunu Ne Vaat Ediyor?”, *Aljazeera Türk*, 1 Mart.

Sırataş, B. (2015). “Kişisel Verilerin Korunması ve Mahremiyet”, *Gelişim Hukuk Topluluğu Konferansı*, s.5-8.

Türel, Ş. N., Davras, M. G. ve Dolmacı, N. (2015). “Turizm Sektöründe Bilgilerin Mahremiyeti”, *Uluslararası İnsan Bilimleri Dergisi*, 12(1), s.236-254.

Yeni Şafak, 3 Nisan 2018.

Yücedağ, N. (2017). “Medeni Hukuk Açısından Kişisel Verilerin Korunması Kanunu’nun Uygulama Alanı ve Genel Hukuka Uygunluk Sebepleri”, *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası* LXXV(2), s.765-790.

Yüksel, M. (2009). “Mahremiyet Hakkına ve Bireysel Özgürlüklere Felsefi Yaklaşımlar”, *Ankara Üniversitesi Siyasal Bilgiler Fakültesi Dergisi*, 64(1), s.275-298.

Zengin, M. ve Zengin, İ. (2015). “Facebook’ta Güvenlik Davranışı ve Mahremiyet Kaygısı: İstanbul’da Yaşayan Kullanıcılara İlişkin Bir Araştırma”, *Uluslararası Hakemli İletişim ve Edebiyat Araştırmaları Dergisi*, 6, s.2.

Zengin M., Zengin, G. ve Altunbaş H. (2013). “ Sosyal Medya ve Değişen Mahremiyet: Facebook Mahremiyeti”, *Medya ve Mahremiyetin Sınırları Ulusal Sempozyum Bildirisi*, s. 118.

Zümbül, H, (2018). “6698 Sayılı Kişisel Verilerin Korunması Kanunu Çerçevesinde Kişisel Veri Kavramı”, <http://www.mondaq.com/turkey/x/726714/Data+Protection+Privacy/6698+Sayili+Kiisel+Verilerin+Korunmasi+Kanunu+erevesinde+Kiisel+Veri+Kavrami>. Erişim Tarihi: 01.08.2019.