



Avrupa Birliği Genel Veri Koruma Tüzüğü Işığında Türkiye’de Kişisel Verileri Koruma Kurumu ¹

Yurdanur URAL USLAN*, Samed DEĞİRMENCİ**

ÖZ

Günümüzde teknolojinin gelişmesi, verilerin dijital ortamda hızla dolaşmasını, depolanmasını ve ulaşılabilirliğini kolay kılmaktadır. Bu durum çok fazla veri trafiğine yol açmakta ve birçok hak ihlaline de neden olmaktadır. En önemlisi de kişinin mahrem alanı zarar görmektedir. Bu nedenle kişisel verilerin korunması konusu gerek ulusal gerekse uluslararası alanda yeni düzenlemelerin yapılmasını gerekli kılmıştır. İlgili düzenlemelerde, verinin işlenmesi sonucu oluşabilecek zararların önlenmesi açısından koruyucu mekanizmaların oluşturulması gerektiği vurgulanmıştır. Çalışmada Türkiye’de kişisel verilerin etkin bir şekilde korunmasını sağlamak için oluşturulan Kişisel Verileri Koruma Kurumu, yapısal ve işlevsel açıdan ele alınıp Avrupa Birliği’nce yapılan son düzenleme olan Genel Veri Koruma Tüzüğü ışığında değerlendirilmektedir. Tüzüğün değerlendirilmesi ile öngörülen idari para cezalarının artırılması ve veri sorumlusunun yanında veri işleyeninde veri ihlalden sorumlu olmasının sağlanması gerektiği sonuçlarına ulaşılmıştır.

Anahtar Sözcükler: Kişisel Veri, Veri Koruma, Kişisel Verileri Koruma Kurumu, Avrupa Birliği Genel Veri Koruma Tüzüğü.

JEL Sınıflandırması: K36, K38

Personal Data Protection Institution in Turkey within the Scope of European Union General Data Protection Regulation

ABSTRACT

Today, recent advancements in technology makes it easy to navigate, store and access data in digital environment. This leads to a complex and too much data traffic while it might also cause a great number of violations of rights. The personal confidentiality of people incurs to most of these violations. Thus, the protection of personal data has necessitated new regulations both in national and international dimensions. In these regulations, it is emphasized that protective mechanisms are to be established in order to prevent damages that may occur as a result of data processing. In this study, the Personal Data Protection Agency, established to ensure the effective protection of personal data in Turkey, has been explored in detail with regards to its structure and functions while the General Data Protection Regulation, the latest regulation published in the European Union has been comparatively analyzed. With the evaluation of the regulation, it has been concluded that the prescribed administrative fines should be increased and that the data controller should be responsible for the data breach, as well as the data controller.

Keywords: Personal Data, Data Protection, the Agency for the Protection of Personal Data, General Data Protection Regulation.

JEL Classification: K36, K38

Geliş Tarihi / Received: 21.04.2022 Kabul Tarihi / Accepted: 29.06.2022

¹ Bu makale yüksek lisans tezinden üretilmiştir.

* Dr Öğretim Üyesi, Uşak Üniversitesi, İİBF, Kamu Yönetimi Bölümü, yurdanur.ural@usak.edu.tr, ORCID: 0000-0002-1721-0712.

** sameddegirmenci92@gmail.com, ORCID: 0000-0002-9251-1937.

1. GİRİŞ

Teknolojideki ilerlemeler, akla gelebilecek birçok bilginin kolay bir şekilde verilere dönüştürülüp depolanmasını, aktarılmasını ve işlenmesini kolaylaştırmaktadır. Bu veriler arasında bizlerin bildiği ya da bilmediği fakat bizleri ilgilendiren bilgiler bulunmaktadır. Bu bilgiler literatürde kişisel veri olarak adlandırılmıştır. Kişisel verilerin çeşitli amaçlarla işlenmesi ve kullanılması bireyler açısından çeşitli hak ihlallerine ve mağduriyetlere neden olmaktadır. Hak ihlallerinin önüne geçebilmek için hem ulusal hem de uluslararası düzeyde çeşitli düzenlemeler yapılmıştır. Yapılan düzenlemelerde önceleri kişisel verilerin korunması konusu özel hayatın gizliliği kapsamında değerlendiriliyordu. Kişisel verilerin korunması zamanla bu kapsamdan sıyrılarak bir temel hak ve hürriyet olarak ayrı bir hak statüsüne kavuşmuştur. Yapılan düzenlemelerin uygulanması için bağımsız bir denetim mekanizmasının kurulması gerektiği vurgulanmaktadır.

Türkiye’de kişiler verilerin korunmasına ilişkin ilk yasal mevzuat 2016 yılında düzenlenerek, denetleyici makam olarak Kişisel Verileri Koruma Kurumu oluşturulmuştur. Mevzuat oluşturulurken Avrupa Birliğinde 1995 yılında kabul edilen Direktif (95/46/EC sayılı) esas alınmıştır. Avrupa Birliğinde daha etkili bir korumanın sağlanabilmesi için 2016 yılında yeni bir düzenlemeye gidilerek Genel Veri Koruma Tüzüğü (2016/679 sayılı) kabul edilmiştir. Kabul edilen Tüzük, kendinden önceki Direktifi yürürlükten kaldırmıştır. Kişisel verilerin korunmasında Avrupa Birliği müktesebatına uyum sağlanması ve en üst düzeyde verilerin korunması açısından, Tüzük’te öngörülen düzenlemeler ışığında Türkiye’deki mevzuat değişikliklerin yapılması ve kurumsal açıdan da iyileştirilme gereklilik arz etmektedir. Bu noktada çalışmanın konusunu, Türkiye’de kişisel verilerin korunmasını sağlamak amacıyla kabul edilen mevzuat ve kurulan Kişisel Verileri Koruma Kurumu oluşturmaktadır. Çalışmanın temel amacı, kişisel verilerin etkili bir şekilde korunmasını sağlamak üzere Türkiye ve Avrupa’da öngörülen denetim mekanizmalarının yapısını ve görevlerini inceleyerek, kurumsal benzerliklerini ve farklılıklarını ortaya çıkarmaktır. Çalışmada öncelikle kavramsal açıklamalara sonrasında kişisel verilerin korunmasına ilişkin ulusal ve uluslararası düzenlemelere yer verilmektedir. Çalışmanın nihayetinde ise Kişisel Verileri Koruma Kurumu ile Avrupa Birliği’ndeki denetim makamları (denetim otoriteleri) arasında bir karşılaştırma yapılmaktadır.

2. KİŞİSEL VERİ VE KİŞİSEL VERİLERİN KORUNMASININ ÖNEMİ

Kişisel veri, gerçek ve tüzel kişilerin belirlenebilir kılındığı her türlü bilgiyi kapsamaktadır (Kılınç, 2012: 1095). Bir verinin kişisel veri olup olmadığına karar verilirken, verinin kişiyle ilişkilendirilmesi veya kişinin belirli veya belirlenebiliyor olması gerekmektedir (Küzeci, 2020: 10). Kişisel verilerin unsurları genel olarak “veri”, “kimliği belirli veya belirlenebilir kişi” ve “bilginin kişiye ilişkin olması” şeklinde sayılmaktadır. Bir kişi hakkındaki öznel ya da nesnel her türlü bilgi kişisel verinin unsurudur ve bilginin doğruluğu veya yanlışlığı kişisel veri olması yönünde önemli değildir (Article 29 Data Protection Working Party, 2007: 6). Kişiyeye ilişkin bilginin ya kişiyi doğrudan tanımlaması ya da birtakım işlemler sonrasında kişiyi tanımlayacak hale gelmesi halinde, kişisel bilgi olarak kabul edilmektedir (Şimşek, 2008: 122). Veri ile kişi ilişkilendirilerek o kişiye ulaşılabilir olması ve verinin kişi hakkında olması gerekmektedir (Dülger, 2018: 73). Bilgi kişiyle ilişkilendirilirken içerik, amaç ve sonuç yönleri ele alınmaktadır. Sayılan bu yönlerden birinde veri ile kişinin ilişkisinden söz edilebiliyorsa, diğer yönlerden de ilişkili olmasına bakılmadan veri kişiyle ilişkili sayılmaktadır (Aksoy, 2010: 28).

Kişisel verilerin kaydedilmesi, aktarılması ve depolanmasının günümüzde kolaylaşması devlet kurumlarını ve özel sektör kuruluşlarını yakından ilgilendirmektedir (Bainbridge, 1997: 17). 1990’lı yılların sonlarına doğru internet kullanımının yaygınlaşması ve günümüzde mobil teknolojilerinde gelişmesiyle birlikte internet ekonomisinin de arttığı görülmektedir. Cihazların

internet üzerinden bağlantı kurması ve milyarlarca sensörün veri kaydetmesi kaydedilmiş verilerin hacminin artmasına sebep olmaktadır. İnternetteki verilerin ses dosyası, fotoğraf, animasyon, video, yazılı ve interaktif materyaller şeklinde kaydedilmesi, veri kaynaklarının bu denli çeşitli olması ve sürekli internet ortamına veri kaydedilmesi büyük bir veri havuzu oluşturmuştur (Şahbaz, Alpaslan ve Sökmen, 2014: 2-3).

Kişisel verilerin maruz kaldığı tehditlerin artmasıyla kişisel verilerin korunması ihtiyacı da artmıştır. Kişisel veriler korunurken hangi hukuki kapsamda değerlendirileceği hususu da önem kazanmıştır (Ayözger, 2016a: 13). Kişisel verilerin korunması hakkının “temel bir insan hakkı” olarak kabul edilmesi yönünde çalışmalar mevcuttur. Kişisel verilerin korunması hakkının, 1982 Anayasası’nda “kişinin hak ve ödevleri” başlığı altında düzenlenmesi, konuyla ilgili usul ve esasların kanunla düzenlenmesi gerektiği ve hakkın sınırlandırılmasının ancak Anayasanın “temel hak ve hürriyetlerin sınırlandırılması” başlıklı 13. maddesinde öngörülen usullere göre yapılabileceği göz önüne alındığında; kişisel verilerin korunması hakkının temel hak ve özgürlükler kapsamında değerlendirildiği görülmektedir (Dülger, 2018: 137).

3. ULUSLARARASI VE ULUSAL HUKUKTA KİŞİSEL VERİLERİN KORUNMASI

Özel hayatın gizliliği başta olmak üzere birçok temel insan hakkıyla doğrudan ilişkili olan kişisel verilerin korunması konusu teknolojik ilerlemeler ile birlikte tartışılır olmuştur. Bilgi ve iletişim teknolojilerindeki hızlı değişimler, bireylerin kişilik haklarının korunması için bir takım yasal düzenlemelerin yapılmasını zorunlu hale getirmiştir (Pearce ve Platten, 1998: 531).

Kişisel verilerin korunmasına yönelik ilk yasal düzenleme 1970 yılında Almanya’nın Hessen eyaletinde kabul edilmiştir.² Bu yasal düzenlemeden sonra 1973 yılında İsveç Veri Koruma Kanunu, 1974 yılında ABD Özel Yaşamın Gizliliği Kanunu, 1977 yılında Federal Almanya Veri Koruma Kanunu ve 1978 yılında Fransa Elektronik Veri İşlemesi, Veriler ve Özgürlük Haklarına İlişkin Kanun çıkarılmıştır (Şimşek, 2008: 10-11).

1980 yılında Ekonomik İşbirliği ve Kalkınma Örgütü (OECD), üye devletler açısından bağlayıcı olmayan “Özel Yaşamın Gizliliğinin ve Sınır Ötesi Kişisel Veri Dolaşımının Korunmasına İlişkin Rehber İlkeler”i kabul etmiştir. OECD bu ilkelerle özel hayatın gizliliği ve kişisel verilerin korunmasına yönelik olarak uluslararası düzeyde bazı güvenceler oluşturma çabasına girmiştir (Şimşek, 2008: 12-13; Küzeci, 2020: 130-131).

Birleşmiş Milletler³ ise kişisel verilerin korunmasına ilişkin olarak 1985 yılında aldığı kararlarla 1990 tarihinde “Bilgisayarda İşlenmiş Kişisel Veri Dosyalarına İlişkin Rehber İlkeler”i (Guidelines for the Regulation of Computerized Personal Data Files) düzenlemiştir. BM Rehber İlkeler düzenlemesi kişisel verilerin korunması ile ilgili bir mekanizma kurulmasını öngören ilk uluslararası belgedir (Aydın, 2015: 29; Küzeci, 2020: 137).

1981 yılında Avrupa Konseyi, kişisel verilerin korunması ile ilgili Avrupa İnsan Hakları Sözleşmesi’nde⁴ yer alan hak ve güvencelerin yeterli olmadığı kanaatiyle; 108 sayılı “Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi”ni kabul etmiştir. Avrupa Konseyi tarafından, 28 Ocak 1981 tarihinde kabul edilen 108 sayılı Sözleşme, 1 Ekim 1985 tarihinde yürürlüğe girmiştir. 108 sayılı Sözleşme, yalnızca üye ülkeler

² 1970 yılında Amerika Birleşik Devletleri Kongresi, Adil Kredi Raporlama Yasasını kabul etmiştir.

³ Birleşmiş Milletler İnsan Hakları Evrensel Bildirisi’nde kişisel verilerin korunması hakkıyla yakından ilişkisi bulunan özel hayatın gizliliği hakkı düzenlenmiştir. Ancak doğrudan kişisel verilerin korunmasına yönelik bir madde yer almamaktadır.

⁴ Avrupa İnsan Hakları Sözleşmesi’nin “özel ve aile hayatına saygı hakkı” başlıklı 8. maddesi kapsamında doğrudan olmasa da dolaylı olarak kişisel veriler korunmaktadır.

için değil, Sözleşme’ye taraf üçüncü ülkeler içinde çerçeve sunmaktadır. Ayrıca Sözleşme kişisel verilerin korunması alanında bağlayıcılığa sahip olan tek uluslararası metindir (Küzeci, 2020: 144).⁵

108 sayılı Sözleşme’ye Ek Protokol (181 sayılı) 2001’de imzalanmış ve bu Ek Protokol 2004 yılında yürürlüğe girmiştir. Ek Protokolde iki konu vurgulanmıştır. Bunlardan ilki kişisel verilerin korunması için ulusal düzenlemeler yapılarak gerekli denetim ve kontrolün sağlanmasıdır. İkinci konu ise bu denetim ve kontrol işlevleri için yapılan ulusal düzenlemelerin 108 sayılı Sözleşme hükümlerine uygun olmasıdır (Akgül, 2014: 193).⁶ Böylelikle 108 sayılı Sözleşme’ye taraf devletler, kişisel verilerin korunması hakkının güvence altına alınmasını ve bu güvencenin bağımsız kurum ve kuruluşlarca yerine getirilmesini ortak bir irade sergileyerek kabul etmişlerdir.

Avrupa Birliği (AB) üyesi devletlerin kişisel verilerin korunmasına ilişkin ulusal mevzuatlarında veri koruma düzeylerinin birbirinden farklı olması, AB’yi verilerin korunmasına yönelik olarak belirli standartlar oluşturmaya teşvik etmiştir. AB kişisel verileri korumaya yönelik olarak farklı tarihlerde yasal düzenlemeler yapmıştır. AB kişisel verilerin korunması ile ilgili attığı ilk yasal adım 24 Ekim 1995 tarihinde 95/46/EC sayılı “Kişisel Verilerin İşlenmesi ve Bu Tür Verilerin Serbest Dolaşımına Dair Bireylerin Korunması Direktifi”dir.⁷ Kişisel verilerin korunması yönünde AB üyesi devletlerarasındaki mevzuat farklılıklarının ortadan kaldırılması ve verilerin serbest dolaşımını sağlamayı amaçlayan Direktif’in ihtiyaçları karşılayamaması üzerine Avrupa Parlamentosu tarafından 14 Nisan 2016 tarihli ve 2016/679 sayılı “Avrupa Birliği Genel Veri Koruma Tüzüğü” kabul edilmiştir. “Genel Veri Koruma Tüzüğü” Direktif’i yürürlükten kaldırmıştır. Tüzük, AB üyesi tüm devletlerde bağlayıcılığa sahiptir (Akıncı, 2017: 5).

AB kişisel verilerin korunması alanında yaptığı çalışmalarla öne çıkmaktadır. AB bünyesinde bulunan devletler ve dışında kalan devletlere bakıldığında, kişisel verilerin korunmasında AB’nin çalışmalarıyla uyumlu olması söz konusu olmaktadır (Korkmaz, 2017: 84). Türkiye’deki veri ihlallerinin giderilmesi ve Türkiye ile AB arasında uyum sağlanması açısından ulusal mevzuatta çeşitli düzenlemeler yapılmıştır. Kişisel verilerin korunması, Türkiye Cumhuriyeti Anayasası’nda “özel hayatın gizliliği” başlığı altında 20. maddede düzenlenmiştir. 1982 Anayasası’nın ilk halindeki 20. maddede, kişisel verilere ilişkin hüküm bulunmazken, 2010 yılında 5982 sayılı kanunla yapılan anayasa değişikliği ile birlikte kişisel verilerin korunması hakkı 20. maddede anayasal güvence altına girmiştir.

Kişilik hakkı görüşü ile kişisel verilerin korunması düşünüldüğünde, 4721 sayılı Türk Medeni Kanunu’nun (TMK) kişiliği koruyan 23, 24 ve 25. maddelerinde yer alan hükümler ile kişisel verilerin korunmasının sağlanabileceği görülmektedir (Aksoy, 2010: 80). 5237 sayılı Türk Ceza Kanunu’nun (TCK) 134 ile 140. maddeler arasında “Özel Hayat ve Hayatın Gizli Alanına Karşı Suçlar” başlıklı bölümde kişisel verilerin korunmasına ilişkin çeşitli konular düzenlenmiştir.

⁵ Türkiye 108 Nolu Sözleşme’yi 28 Ocak 1981 tarihinde imzalayan ilk ülkelerden biri olmasına rağmen Kişisel Verileri Koruma Kanununun yasama sürecine kadar (2016) onaylamamıştır. 108 Nolu sözleşme 30 Ocak 2016 tarihinde 6669 sayılı kanun ile uygun bulunmuştur. 17 Mart 2016 tarihinde Resmi gazetede yayımlanarak yürürlüğe girmiş ve iç hukukumuza dâhil olmuştur. Kişisel Verileri Koruma Kanunu da Resmi Gazetede 7 Nisan 2016 tarihinde yayınlanarak yürürlüğe girmiştir (Özel, 2020: 243).

⁶ Sözleşmenin ek protokolü KVKK kanunu il birlikte Kişisel Verilerin Korunması Kurumunun kurulması ile 5 Mayıs 2016 tarihinde onaylanarak iç hukukumuza dâhil olmuştur.

⁷95/46/EC sayılı Direktifin tamamlamak amacıyla birçok düzenleme yapılmıştır. 1997 /66/EC sayılı Telekomünikasyon Veri Koruma Direktifi; 2002/58/EC sayılı Elektronik Veri Koruma Direktifi; 2006/24/EC Veri Saklama Direktifi; 2009/136/EC Vatandaşlık Hakkı Direktifi (Ayözger, 2016b: 79-80).

2016 yılında kişisel verilerin işlenebilmesi ile ilgili özel bir kanun ve etkin bir denetim mekanizmasının bulunmamasının toplumda olumsuz yönde bir algıya sebep olduğu, kişisel verilerin belli şartlar dâhilinde işlenmesi, muhafaza edilmesi ve kontrolüne ilişkin esasların belirlenmesi ile bu algının ortadan kaldırılabilmesi, Türkiye’de kişisel verilerin korunmasının farklı kanunlarla sağlandığı ve bütüncül düzenlemenin yapılması gerektiği, verilerin işlenmesi sürecinin güvenli şekilde sağlanması amacıyla oluşturulmuş bir kurumun bulunmadığı, kişisel verilerin yeterince korunamamasından dolayı hak ihlallerinin yaşandığı, AB’ye üyelik için kişisel verilerin korunmasının önemli rol oynadığı gerekçesiyle 6698 sayılı Kişisel Verilerin Korunması Kanunu düzenlenerek yürürlüğe girmiştir.

4. 6698 SAYILI KANUN’UN GENEL VERİ KORUMA TÜZÜĞÜ AÇISINDAN DEĞERLENDİRİLMESİ

6698 sayılı Kişisel Verilerin Korunması Hakkındaki Kanun’un, Avrupa Birliği Direktifi ile uyumlu olması gözetilerek hazırlanması ve Türkiye’de 6698 sayılı Kanun’un yayımlanması sonrasında AB’de kişisel verilerin korunması yönünde yapılan değişikliklerle Tüzük’ün kabul edilmesi, Kanun ile Tüzük arasında bazı farklılıkların ortaya çıkmasına neden olmuştur.

Tüzük ile birlikte kişisel verilerin korunması açısından AB üyesi devletler kendi aralarında üst düzey uyum sağlayarak, üye devletlerin kendi iç hukuklarından kaynaklanan farklılıklar giderilmiştir. Bu sayede AB üyesi devletlere kendi iç pazarı açısından küresel rekabet avantajı sağlanmıştır. Bu açıdan Türkiye’nin de Tüzük ile uyumlu bir mevzuata sahip olması önem teşkil etmektedir (Akıncı, 2017: 33). Tüzük’ün getirdiği başlıca değişiklikler ve farklılıklar şu şekilde gösterilebilir;

- Tüzük’te kişisel verinin hukuka uygun bir şekilde işlenmesinden sadece veri sorumlusu⁸ değil veri işleyeni⁹de sorumlu tutulmaktadır. Dolayısıyla veri işleme faaliyetinin tüm failleri, verilerin işlenmesinden kaynaklanan hukuki aykırılıklardan sorumludur. Bu kapsamda AB dışında işleme faaliyetlerini yürüten bulut hizmet sağlayıcılarına da Tüzük hükümlerine göre yaptırım uygulanabilmektedir. 6698 sayılı Kanun’da ise, Kanun’un 18. maddesinin ikinci fıkrası gereğince veri sorumluları veri işlemeden sorumlu tutularak idari cezaların uygulandığı fakat veri işleyen açısından bir yaptırım uygulanmasının söz konusu olmadığı görülmektedir. Bu durum veri işleyenlerin sorumlulukları açısından geniş bir sorumluluk alanına sahip olan Tüzük ile farklılık göstermektedir (Akıncı, 2017: 34).
- Bireylerin kendi kişisel verilerini kontrol edebilme ve gerektiğinde silebilme hakkı şeklinde ifade edilen ‘unutulma hakkı’ Tüzük’te ilk kez hukuki olarak düzenlenmiştir. 6698 sayılı Kanun’da ise unutulma hakkı yer almamaktadır (Akıncı, 2017: 35). Ancak Yargıtay ve Anayasa Mahkemesi kararlarında unutulma hakkına değinildiği görülmektedir.¹⁰
- Tüzük’te veri ihlallerine karşı 20 milyon Euro’ya kadar ulaşabilen ağır yaptırımların uygulanabileceği düzenlenmektedir. 6698 sayılı Kanun’da ise bu yaptırımlar en fazla 1 milyon Türk lirası olacak şekilde yer almaktadır. İdari para cezalarının her yıl yeniden

⁸ “Veri Sorumlusu” yalnız başına veya başkalarıyla birlikte kişisel verilerin işlenmesine ilişkin amaçlar ve yöntemleri belirleyen gerçek veya tüzel kişi, kamu kuruluşu, kurumu veya diğer herhangi bir organdır; söz konusu işleme amaçları ve yöntemlerinin Birlik ya da üye devlet hukukuna göre belirlenmesi durumunda, sorumlu veya sorumlunun belirlenmesine özgü kriterler Birlik ya da üye devlet hukukuna göre belirlenebilir (Tüzük, md. 4/7).

⁹ “Veri İşleyen” veri sorumlusu adına kişisel verileri işleyen bir gerçek ya da tüzel kişi, kamu kuruluşu, kurumu veya diğer herhangi bir organdır (Tüzük, md. 4/8).

¹⁰ T.C. Yargıtay Hukuk Genel Kurulu E. 2014/4-56 K. 2015/1679 T. 17.6.2015; Anayasa Mahkemesi B. No. 2013/5653, K. T. 03.03.2016, R.G. No. 29811 R.G. T. 24.08.2016.

değerleme oranları doğrultusunda artışı sözkonusu olmaktadır. Ancak oranlardaki artış ağır bir yaptırım niteliği taşımamaktadır.

- Tüzük'te ilk kez “veri taşınabilirliği hakkı” düzenlenerek, veri sahibine verisinin başka bir veri sorumlusuna taşıma hakkı verilmiştir. 6698 sayılı Kanun'da ise veri taşınabilirliği hakkı düzenlenmemiştir.
- Tüzük kişisel verilerin işlenmesi ile ilgili olarak yol gösterecek, denetim ile iş birliğini sağlayacak ve ilgili raporlamaları yapacak olan veri koruma görevlisinin atanmasını düzenlemiştir. 6698 sayılı Kanun böyle bir sorumluluk belirtmemiş olmakla birlikte uzman bir kişinin atanmasına da kanuni düzenlemede bir engel yoktur (Hizarci, 2020: 173).
- Veri işlemenin riskli olduğu durumlarda “veri koruma etki değerlendirmesi” yapılması Tüzük'te yer alan düzenlemeler arasındadır. Kişisel verilerin işlenmesinde meydana gelecek risklerin değerlendirilmesi ve yapılan değerlendirme sonrasında işleme faaliyetine ilişkin olarak bir denetim makamına başvurulması 6698 sayılı Kanun'da yer almamaktadır (Akıncı, 2017: 36; Hizarci, 2020: 174).
- Tüzük'te veri sahibinin rızası kavramına detaylı şekilde yer verildiği görülmektedir. Veri sahibinin rızasını istediği zaman çekebileceği Tüzük'te yer alırken 6698 sayılı Kanun metninde rızanın geri çekilmesine yer verilmemektedir. Ancak Kanun'da yer almasa da rıza kişiye sıkı sıkıya bağlı bir hak olduğu için kişi dilediği zaman rızasını geri alabilir. Ayrıca Tüzük'te işlenecek olan bütün veriler için ayrı ayrı rıza alınması öngörülmekte ve veri sorumlularına alınan bu rızaları ispatlama yükümlülüğü getirilmektedir. Tüzük, rıza kapsamında 16 yaş altındaki çocukların rızasının hukuka aykırı olduğunu ve çocuğun bilgi toplumu hizmetlerinden ebeveyn rızası ile faydalanabileceğini düzenlemiştir.
- Tüzük'te kişisel verilerin işlenmesi sırasında veri sahibi açısından bir zarar söz konusu ise veri sahibi veri sorumlusu veya veri işleyenden tazminat talebinde bulunabilmektedir. İşleme faaliyetine müdahil herhangi bir veri sorumlusu bu Tüzük'ü ihlal eden işleme faaliyetinin sebep olduğu zarardan sorumludur. Bir işleyici, ancak bu Tüzük'ün özellikle işleyicilere yönelik yükümlülüklerine uyum göstermediği veya kontrolörün hukuka uygun talimatları dışında veya bu talimatlara aykırı hareket ettiği hallerde, işleme faaliyetinin sebep olduğu zarardan sorumludur. 6698 sayılı Kanun'da da benzer şekilde veri sorumlusunun yükümlülükleri ve kişisel verileri işlenen kişinin hakları düzenlenmiştir. Kanunun 11. maddesine göre, kişisel verileri işlenen kişi kendisiyle ilgili kişisel veri işlenip işlenmediğini öğrenme, işlenmişse buna ilişkin bilgi talep etme, verilerin işlenme amacı ile verilerin 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 ve kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme haklarına sahiptir. İlgili kişi kişisel verilerin hatalı işlenmesinden dolayı zarara uğraması durumunda bu zararı tazmin etmek için talepte bulunabilir. Zararın tazmin edilebilmesi için haksız fiil sorumluluğu şartlarının oluşması gerekir. Buna göre, hukuka aykırı bir veri işleme faaliyeti olmalı, bu faaliyetten dolayı kişi zarar görmüş olmalı ve bunlar arasında illiyet bağı olmalıdır. 6698 sayılı Kanun kişisel verileri işlenen kişinin haklarını düzenlerken, Tüzük'ten farklı olarak, başvurulacak kişi ve yükümlü olarak sadece veri sorumlusundan bahsetmiş, veri işleyenden söz etmemiştir (Dülger, 2019: 164; İstanbul Bilgi Üniversitesi, 2018: 246-247).
- Bir veri ihlalinin olması durumunda veri sorumlusunun denetim makamına ve zarara uğrayabilecek veri sahibine en geç 72 saat içinde haber vermesi gerektiği Tüzük'te düzenlenmektedir. 6698 sayılı Kanun'da veri sorumlusuna veri ihlalinin “en kısa sürede”

ilgisine ve kurula bildirmesi sorumluluğu getirilmiştir. Ancak Kurul’un 2019/10 sayılı kararı¹¹ uyarınca, artık veri ihlal bildirimlerinin, veri sorumlusunun bu durumu öğrendiği tarihten itibaren gecikmeksizin ve en geç 72 saat içinde Kurula bildirmesine, veri sorumlusunca söz konusu veri ihlalinden etkilenen kişilerin belirlenmesini müteakip ilgili kişilere de makul olan en kısa süre içerisinde bildirilmesi gereklidir (Hizarci, 2020: 155-156). Kurul bu kararı alarak Kanun’da yer alan “en kısa sürede” ifadesini Tüzük ile uyumlu olarak en geç 72 saat olarak yorumlamış ve böylece konuya dair belirsizliği (ve muhtemel bir çelişkiyi) de ortadan kaldırmıştır.

Görüldüğü üzere, 6698 sayılı Kanun ile Tüzük arasında kişisel verilerin korunması yönünden bazı farklar mevcuttur. 6698 sayılı Kanun’da veri sorumlularının yükümlülüklerinin artırılması, idari para cezalarının artırılması, veri sahibine veri taşınabilirliği hakkı verilmesi ve veri koruma etki değerlendirmesinin yapılmasına yönelik düzenlemelerin yer alması kişisel verilerin etkin korunması ve Tüzük ile uyum açısından büyük önem taşımaktadır.

5. TÜRKİYE VE AVRUPA BİRLİĞİ’NDE KİŞİSEL VERİLERİN KORUNMASINDA KURUMSAL YAPILANMALAR

Bu başlık altında Türkiye’deki Kişisel Verileri Koruma Kurumu ile Avrupa Birliği’ndeki denetim makamları kurumsal açıdan ele alınmaktadır.

5.1. Türkiye’de Uygulanan Sistem

Türkiye’de kişisel verilerin korunması bağlamında “6698 sayılı Kişisel Verilerin Korunması Kanunu”nun yürürlüğe girmesi ve kanunun getirdiği bir yenilik olarak Kişisel Verileri Koruma Kurumu’nun kurulmasıyla teşkilatlanmaya gidilerek kurumsal anlamda ilk yapı oluşturulmuştur.

Kurul ve Başkanlık teşkilatından oluşan, denetleyici ve düzenleyici üst kuruluş olarak nitelendirilen Kişisel Verileri Koruma Kurumu Cumhurbaşkanının görevlendirdiği bir bakanlık ile ilişkilendirilmiştir (6698, md. 19). Adalet Bakanlığı ile ilişkili bir kamu kurumudur¹² İdari teşkilatı kurul, başkanlık ve başkanlığa bağlı daire başkanlıkları şeklinde oluşturulan Kurumun merkezi Ankara’dadır.¹³ Kurum görev alanı ile ilgili olarak hiçbir emir ve talimat almadan tarafsız, bağımsız, temel hak ve özgürlüklere saygılı, doğru, objektif, güvenilir, hukuka uygun ve şeffaflık ilkeleri öncelikli olmak üzere kişisel verilerin korunmasına ilişkin uluslararası alanda söz sahibi bir otorite olmayı hedeflemektedir¹⁴.

Kurumun görevleri: Görev alanı ile ilgili olan uygulamaları ve mevzuattaki gelişmeleri takip etmek, değerlendirme ve önerilerde bulunmak, araştırma ve incelemeler yapmak veya yaptırmak; ihtiyaç duyulması halinde, görev alanına giren konularda kamu kurum ve kuruluşları, sivil toplum kuruluşları, meslek örgütleri veya üniversitelerle iş birliği yapmak; kişisel veriler ile ilgili uluslararası gelişmeleri izlemek ve değerlendirmek, görev alanına giren konularda

¹¹ Kişisel Verileri Koruma Kurulunun 24.01.2019 tarih ve 2019/10 sayılı Kararı, <https://kvkk.gov.tr/Icerik/5362/Veri-Ihlali-Bildirimi> (Erişim Tarihi: 02.02.2022).

¹² İlişkili kuruluşların bakanlıklarla ilişkilendirilmesinin nedeni idarenin bütünlüğünü ve koordinasyonunu sağlamaktır. Yönetimsel bakımdan bir ilişkilendirme söz konusu değildir. Kurum idarenin bütünlüğü ilkesi gereği ilişkili kuruluş olarak nitelendirilmektedir (Yıldırım, vd. 2016: 31). İlişkili kuruluş ayrı bir tüzel kişiliğe sahip, bakanlıkla hiyerarşik bir bağlantısı bulunmayan, bakanlığın idari vesayet denetimine sınırlı şekilde tabi özerk kuruluşlar olarak tanımlanabilir (Gözler, 2009: 270).

¹³ Kişisel Verileri Koruma Kurumu Teşkilat Yönetmeliği madde 4/2-3.

¹⁴ Kişisel Verileri Koruma Kurumu, Misyon-Vizyon, <https://www.kvkk.gov.tr/Icerik/2074/Misyon---Vizyon>, (Erişim Tarihi: 30.01.2022)

uluslararası kuruluşlarla iş birliği yapmak, toplantılara katılmak; yıllık faaliyet raporunu Cumhurbaşkanlığına, Türkiye Büyük Millet Meclisi İnsan Haklarını İnceleme Komisyonuna sunmak ve Kanunla verilen diğer görevleri yerine getirmektir (6698, md. 20/1).

Kurumun idari ve mali özerkliği bulunmaktadır. Kurumun yıllık bütçesinin belirlenen stratejilere, yıllık amaç ve hedeflere uygun bir şekilde hazırlanması Başkanın¹⁵ görevleri arasında yer almaktadır (6698, md. 24/3-e). Hazırlanan bu bütçe teklifi Kurul tarafından görüşülüp karara bağlanmaktadır (6698, md. 22/1-i).

Kurumun karar organı olan Kurul, biri Başkan, biri İkinci Başkan olmak üzere dokuz üyeden oluşmaktadır. Kurum, kanun ile kendisine verilmiş görev ve yetkileri Kurul aracılığıyla yerine getirir. Kurulun beş üyesi Türkiye Büyük Millet Meclisi, geriye kalan dört üyesi de Cumhurbaşkanı tarafından seçilmektedir (6698, md. 21/2). Kurul üyelerinin görev süresi dört yıl olarak belirlenmiştir (6698, md. 21/8).

Kurul, Kanunla ve diğer mevzuatla verilen görev ve yetkilerini kendi sorumluluğu altında, bağımsız olarak yerine getirmektedir. Görev alanına giren konularla ilgili olarak hiçbir organ, makam, merci veya kişi, Kurula emir ve talimat veremez, tavsiye ve telkinde bulunamaz (6698, md. 21/1). Kurulun ve Kurumun en üst amiri olan Başkan, Kurumun genel yönetim ve temsili ile Kurul tarafından alınan kararların yürütülmesinden sorumludur. Başkanın izin, hastalık yurtdışı görev ve diğer nedenlerle yokluğunda İkinci Başkan, Başkana vekâlet eder (6698, md. 24).

Kurul, kişisel verilerin temel hak ve hürriyetlere uygun bir şekilde işlenmesini sağlamayı hedeflemektedir. Bu hususta hak kaybına uğrayanların şikâyetlerini karara bağlar (6698, md. 22/a-b). 13. madde uyarınca başvuru yolu tüketilmeden şikâyet yoluna başvurulamaz (6698, md. 14/2). İlgili kişi taleplerini yazılı olarak veri sorumlusuna iletir. Veri sorumlusu ya talebi kabul eder veya reddeder. Başvurunun reddedilmesi, verilen cevabın yetersiz bulunması veya süresinde başvuruya cevap verilmemesi hallerinde; ilgili kişi veri sorumlusunun cevabını öğrendiği tarihten itibaren otuz ve her halde başvuru tarihinden itibaren altmış gün içinde Kurula şikâyette bulunabilir (6698, md. 13-14/1).

Kurul ihlal iddiasını öğrenmesi üzerine resen de görev alanına giren konularda gerekli incelemeyi yapar. Şikâyet üzerine veya resen yapılan inceleme sonucunda, ihlal varlığının anlaşılması halinde Kurul, tespit ettiği hukuka aykırılıkların veri sorumlusu tarafından giderilmesine karar vererek ilgililere tebliğ eder. Kurul ayrıca inceleme sonucunda ihlalin yaygın olduğunun tespit etmesi halinde bu konuda ilke kararı alır. Kurul telafisi güç veya imkânsız zararların doğması ve açıkça hukuka aykırılık olması halinde veri işlenmesinin veya verinin yurt dışına aktarılmasının durdurulmasına karar verebilir. (6698, md. 10-15)

Kurulun görevlerinden biri de veri sorumlusunun sicilinin tutulmasını sağlamaktır (6698, md. 22/d). Kişisel verilerin yönetilmesinden sorumlu olan veri sorumlusu, Kurul'un gözetimindeki Başkanlık tarafından kamuya açık olarak tutulan Veri Sorumluları Siciline kayıt olmak zorundadır (6698, md. 16). Ayrıca veri sorumlularının ilgililere karşı aydınlatma yükümlülüğü, veri güvenliğine ilişkin yükümlülükleri, ilgili kişiler tarafından yapılan başvuruların cevaplanması yükümlülüğü ve kurul kararlarının yerine getirilmesi yükümlülüğü bulunmaktadır (6698, md. 10-15). Veri işleyenin ise işleme sebebiyle edindiği bilgiler açısından sır saklama yükümlülüğü mevcuttur.

Yükümlülüklerini yerine getirmeyen veri sorumluları hakkında 5.000 Türk lirasından 1.000.000 Türk lirasına kadar idari para cezası verilir. Öngörülen idari para cezaları veri

¹⁵ Başkan, Kurul ve Kurumun başkanı sıfatıyla kurumun en üst amiri olup Kurum hizmetlerini mevzuata, Kurumun amaç ve politikalarına, stratejik planına, performans ölçütlerine ve hizmet kalite standartlarına uygun olarak düzenler, yürütür ve hizmet birimleri arasında koordinasyonu sağlar (6698, md. 24/1).

sorumlusu olan gerçek kişiler ile özel hukuk kişileri hakkında uygulanır (6698, md.18/1-2). Kanunda öngörülen kabahatler gerçekleşmiş ise idari yaptırımların uygulanmasına karar verilmektedir. Eğer suç olarak belirlenen ve ceza uygulanacak olan durumlar söz konusu ise Türk Ceza Kanunu’nun kişisel verilerin kaydedilmesi başlığında düzenlenen 135 ve 140. maddeler arasındaki hükümler uygulanacaktır (6698, md. 17-18).

5.2. Avrupa Birliği’nde Uygulanan Sistem

AB Tüzüğü uyarınca her bir üye devlet bir veya birden fazla denetim makamı belirlemelidir (Tüzük, md.51). Üye devletlerde bir veya birden fazla denetim makamının varlığı halinde hangi denetim makamının ya da makamlarının AB Veri Koruma Kurulu¹⁶’nda söz konusu ülkeyi temsil edeceğini tayin etme hakkı o üye devlete aittir (Tüzük, md.51/3). Görevlendirilen makam veya makamlar Tüzüğün uygulanması konusunda gerek ulusal kurumlara gerek AB kurumlarıyla iş birliği halinde çalışmakla yükümlüdür (Tüzük, md.51/2).

Denetim makamları Tüzük uyarınca bağımsız bir statüye sahip olmalıdır. Bu kapsamda veri koruma makamlarının görevlerini tam bağımsızlık ile yerine getirmesi gerektiği gibi, doğrudan ve dolaylı dış etkilerden ve talimatlardan uzak olmalıdır. Ayrıca Tüzük uyarınca denetim makamları gerekli mali, teknik ve insan kaynaklarına sahip olmalıdır (Tüzük, md.52/1-4). Denetim makamı üyeleri, şeffaf bir seçim usulüne dayanılarak parlamento, hükümet, devlet başkanı veya üye devlet hukukunda belirtilen bağımsız bir kuruluş tarafından atanır. Her üyenin kişisel verilerin korunması alanında yeterli deneyime ve bilgiye sahip olması gerekmektedir (Tüzük, md.53/1-2). Tüzük’te üye devletlerin; denetim makamlarını, üyelerin seçilmesindeki nitelikleri ve uygunlukları, üye seçilmesindeki usul ve esasları, üyelerin çalışma sürelerinin en az dört yıl olmasını, üyelerin yeniden tayin edilebilme durumlarını, üyelerin ve personelin yükümlülükleri ile görevlerine son verilecek durumları belirlerken bu yükümlülüğünü kanunla yapması gerekmektedir (Tüzük md.54/1).

Denetim makamının görevlerinin başında kendi yetki alanında Tüzük’ün uygulanmasını izlemek ve sağlamak gelir. Bunun yanında denetim makamı, konuya ilişkin kamuoyunu bilinçlendirme yapar, hak ve özgürlüklerin korunması için tavsiye kararlarında bulunur, diğer denetim makamları ile işbirliği sağlar (Tüzük, md. 57). İlgili kişinin belirli koşullar altında denetim makamına şikâyette bulunma hakkı mevcuttur. Kişisel verilerinin hukuka aykırı olarak işlendiğini ileri süren kişi yaşadığı, çalıştığı veya ihlalin olduğu yerdeki üye devlette bulunan denetim makamına başvurabilir (Tüzük, md. 77/1)¹⁷. İlgili kişi denetim makamının kararından memnun kalmazsa ya denetim makamı üç ay içerisinde bir şikâyeti ele almazsa ya da şikâyetin seyri ve sonucu hakkında veri sahibi bilgilendirilmez ise konu yargıya taşınabilir (Tüzük, md. 78-79).

Tüzük uyarınca her bir veri sorumlusunun veri işleme etkinlikleri kayıtlarını muhafaza etmesi ve istenmesi halinde denetim makamına vermesi gerekmektedir (Tüzük, md. 30). Bir kişisel veri ihlalinin olması durumunda veri sorumlusunun gereksiz gecikmeye mahal vermeden ve eğer mümkünse sorunu fark etmesinden itibaren 72 saat içerisinde ilgili denetim makamına bildirmesi gerekmektedir (Tüzük, md. 33). Bunun yanında veri sorumlusu, işleme faaliyetinin yüksek bir riske sebebiyet vereceğinin görüldüğü hallerde, denetim makamına bir istişare

¹⁶ Avrupa Veri Koruma Kurulu Tüzük’le kurulan bir Birlik organıdır ve tüzel kişiliğe sahiptir. Avrupa Birliğine üye her devletin denetim makamlarının başkanları ile Avrupa Veri Koruma Denetmeni veya bunların ilgili temsilcilerinden oluşur (Tüzük, md. 68).

¹⁷Tüzük 56. Maddesi uyarınca veri sorumlusu veya veri işleyicinin ana işletmesinin veya tek işletmesinin denetim makamı, söz konusu veri sorumlusu veya veri işleyici tarafından gerçekleştirilen sınır ötesi işleme faaliyetlerine yönelik olarak baş denetim makamı şeklinde hareket etmeye yetkindir. Bu hükme göre başvuru sınır ötesi işleme faaliyetine yönelik bir başvuru olması durumunda baş denetim makamı tarafından denetlenebilir.

başvurusunda bulunabilir (Tüzük, md. 36). Ayrıca veri sorumlusunun ilgili kişiyi bilgilendirme¹⁸, veri koruma etki değerlendirilmesi¹⁹, işleme güvenliğini sağlama²⁰, kişisel verilerin üçüncü kişilere veya uluslararası kuruluşlara aktarımı²¹ ve veri koruma görevlisi belirleme²² yükümlülükleri bulunmaktadır. Veri işleyenin ise veri işleme faaliyetlerinin yapılması esnasında gerekli gizlilik tedbirlerini alma, veri sorumlusuna bilgi sağlama, işleme faaliyetinin sona ermesi ile verilerin silinmesi veya iade edilmesi, denetim için katkıda bulunması işlemin güvenliğini sağlamakla yükümlülükleri arasındadır (Tüzük, md. 28). Veri sorumlusu ve veri işleyenin, işleme faaliyetlerinin kayıtlarını tutma, denetim makamları ile işbirliği yapma, güvenliğini sağlama, veri koruma görevlisi belirleme ve veri koruma görevlisi belirleme ve gibi ortak yükümlülükleri mevcuttur (Tüzük, md. 30/2, 31, 32, 37).

Tüzük hukuka aykırı olarak verilerinin işlenmesinden dolayı zarara uğrayan kişinin veri sorumlusu yanında veri işleyene de başvurulmasının yolunu açmıştır. Veri sorumlusu ya da veri işleyen zarara neden olan olaydan sorumlu olmadıklarını kanıtlarsa bu sorumluluktan kurtulabilmektedir (Tüzük, md. 82). Tüzük uyarınca denetim makamlarının caydırıcı bir yaptırım mekanizması uygulaması gerekmektedir (Tüzük, md. 83). İdari para cezaları ağır ihlallerde 20 milyon Euro veya teşebbüsün bir önceki yıldaki mali yılda dünya çapındaki yıllık cirosunun %4'üne kadar belirlenebilmektedir (Tüzük, md. 83/5,6). Denetim makamları ihlal türlerini ve alınan tedbirleri içeren yıllık faaliyet raporunu ulusal parlamentoya, hükümete ve üye devlet hukuku çerçevesinde belirlenen diğer kuruluşlara iletilir. Raporlar kamuoyuna, Komisyon'a ve Kurul'a sağlanır (Tüzük md. 59).

Türkiye'de kişisel verilerin korunmasının sağlanması amacıyla oluşturulan Kişisel Verileri Koruma Kurumu ile Avrupa Birliği'nde uygulanan Tüzük'te belirtilen denetim makamlarının yapısal ve işlevsel açıdan karşılaştırılması Tablo 1'de verilmiştir.

Tablo 1: Türkiye ve Avrupa Birliği'ndeki Denetim Makamlarının Karşılaştırılması

	Avrupa Birliği'nde Denetim Makamı	Türkiye'de Denetim Makamı
Denetim makamlarının yasal dayanakları	- 2016/679 sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü	- 6698 sayılı Kişisel Verilerin Korunması Kanunu
Denetim makamlarının sayısı	Bir ve daha fazla denetim makamı	Kişisel Verileri Koruma Kurumu
Denetim makamı üyelerinin seçimi	- parlamento - hükümet - devlet başkanı - bağımsız kuruluş	- parlamento - cumhurbaşkanı
Denetim makamı üyelerinin görev süresi	En az 4 yıl	4 yıl
Denetim makamlarının mali özerkliği	Kendi yıllık kamusal bütçeye sahip	Kendi yıllık kamusal bütçeye sahip
Denetim makamlarının idari özerkliği	Görev ve yetkilerini kullanırken tam bağımsızdır	Görev ve yetkilerini kullanırken tam bağımsızdır
Denetim makamlarının vermiş	20.000.000 Euro	5.000 TL ile 1.000.000 TL arasında

¹⁸ Tüzük, md. 13-14.

¹⁹ Tüzük md. 35.

²⁰ Tüzük, md. 32.

²¹ Tüzük, md. 45-46.

²² Tüzük, md. 37.

oldukları idari cezalar		
Denetim makamlarının Faaliyet Raporu yayımlaması	Her yıl faaliyet raporu yayımlar	Her yıl faaliyet raporu yayımlar
Denetim makamları ihlal karşısında resen harekete geçmesi	İhlal karşısında resen harekete geçebilir	İhlal karşısında resen harekete geçebilir
Denetim makamlarının arasındaki yetki dağılımı	Denetim makamları diğer Üye Devletlerin denetim makamlarıyla işbirliği, tutarlılık ve ivedilik prosedürü uygulanmaktadır	Yalnızca Türkiye’de yetkili
Denetim makamlarının idari yaptırım uyguladığı gerçek ve tüzel kişiler	- veri sorumluları - veri işleyen	- veri sorumlusu

Kaynak: Yazarlar tarafından derlenmiştir.

Düzenleyici ve denetleyici bir kurum olan Kişisel Verileri Koruma Kurumu AB Direktifi temel alınarak oluşturulmuştur. Bu nedenle Kurum’un Tüzüğe uygunluğu konusunda birtakım farklılıklar bulunmaktadır. Kişisel Verileri Koruma Kurumu’nun kurumsal yapılanmasını Tüzüğe uygunluğu konusunda bir değerlendirme yapacak olursak;

- Kişisel Verileri Koruma Kurumu’nun idari yaptırım uyguladığı veri sorumlusudur. Veri sorumlusunun yanında veri işleyeni de veri ihlalden sorumlu olması sağlanarak Kuruma bu yönde idari işlem yapma yetkisi verilmelidir. Veri Koruma Tüzüğünde veri işleyene yönelik düzenlemeler ve müteselsil sorumlu olunan alanların sayısı fazladır.
- Kişisel Verileri Koruma Kurum’u tarafından verilen idari para cezalarının artırılması gerekmektedir. Veri Koruma Tüzüğü idari para cezalarının uygulanmasını oldukça yüksek miktardan belirlemiştir. Bu yüksek sınırlar içerisinde yapılan belirleme şirket ciroları üzerinden hesaplanmaktadır. 6698 sayılı Kanun ise işletmelerin ciro büyüklüklerini değil işleme faaliyetinin mahiyetini temel almıştır.
- Tüzük uyarınca veri sızıntısı olması durumunda veri sorumlusu gecikmeksizin ve eğer mümkünse sorunu fark etmesinden itibaren 72 saat içinde, ilgili denetim makamına bildirimde bulunur (Tüzük, md. 33). 6698 sayılı Kanun’da ise veri sorumlusuna veri ihlali olması durumunda “en kısa sürede” ilgisine ve Kurula bildirme yükümlülüğü getirilmiştir (6698, md. 12/5). Kurul 2019/10 sayılı kararı alarak Kanun’da yer alan “en kısa sürede” ifadesini Tüzük ile uyumlu olarak en geç 72 saat olarak yorumlamış ve böylece konuya dair belirsizliği ortadan kaldırmıştır. Kurulun verdiği kararlar kurulun sadece bir denetim organı olmadığını düzenleyici bir kurul olduğunu da göstermektedir.
- Tüzük denetim makamlarına şikâyet başvurularının yapılacağını öngörmektedir. Ancak 6698 sayılı Kanunun 13. maddesi uyarınca başvuru yolu tüketilmeden şikâyet yoluna başvurulamaz (6698, md. 14/2). Buna göre ilgili kişi, taleplerini önce veri sorumlusuna iletir. Veri sorumlusu yapılan başvuruyu kabul edebilir, reddedebilir ya da süresi içerisinde yanıt vermeyebilir. Başvurunun reddedilmesi, verilen cevabın yetersiz bulunması veya süresinde başvuruya cevap verilmemesi hallerinde; ilgili kişi veri sorumlusunun cevabını öğrendiği tarihten itibaren otuz ve her halde başvuru tarihinden itibaren altmış gün içinde Kurula şikâyetle bulunabilir (6698, md. 13-14/1).
- Veri sorumlusu bir işleme faaliyetine başlamadan önce veri işlemenin riskli olduğu kanaatine varırsa işleme faaliyeti için bir değerlendirme (veri koruma etki değerlendirilmesi)

yapabilir. Bu değerlendirme sonucunda veri sorumlusu yapılacak işlemin yüksek bir riske sebebiyet vereceğini ve Tüzüğü ihlal edeceği kanısına varırsa denetim makamına istişare başvurusunda bulunabilir (Tüzük md. 35). Kişisel verilerin işlenmesinde meydana gelecek risklerin değerlendirilmesi ve yapılan değerlendirme sonrasında işleme faaliyetine ilişkin olarak bir denetim makamına başvurulması 6698 sayılı Kanun'da yer almamaktadır.

- Kurul toplantılarındaki görüşmeler aksi kararlaştırılmadıkça görüşmeler gizlidir (Tüzük, md. 23/6). Kurulun aldığı kararların her durumda kamuoyu ile paylaşılması mümkün değildir. İlgili hüküm uyarınca Kurul “gerekli gördüğü kararları” kamuoyuna duyurur (Tüzük, 23/5-6). İstisnai durumlarda kararların yayınlanmamasına karar verilmesi şeffaflığın desteklenmesini sağlar.

Türkiye'nin kanundaki farklılıkları gidererek AB müktesebatıyla uyum sağlaması, kişisel verilerin etkin bir şekilde korunmasında katkı sağlayacaktır.

6. SONUÇ

Günümüzde teknolojik gelişmeler ve internetin kullanımının yaygınlaşması toplumsal ve ekonomik açıdan olumlu etkilere sahip olsa da kişisel verilerin işlenmesini kolay ve ulaşılabilir kılması özel hayat alanında tehdit oluşturmuştur. Kişilerin sır alanını oluşturan bilgilerin tehdit altına girmesiyle birlikte özel hayatın gizliliği kapsamında korunan kişisel veriler ayrı bir hak olarak ortaya çıkmıştır.

Kişisel verilerin korunması hakkı alanında ulusal ve uluslararası alanda çeşitli düzenlemelere gidilmiştir. Bu konuda uluslararası ilk düzenlemeler BM, OECD ve Avrupa Konseyi tarafından yapılmıştır. Avrupa'da 28 Ocak 1981 tarihli “Kişisel Verilerin Otomatik İşleme Tabi Tutulma Sürecinde Şahısların Korunmasına İlişkin Sözleşme” Avrupa Konseyi tarafından kabul edilmesinden sonra, 24 Ekim 1995 tarihli “Kişisel Verilerin İşlenmesi ve Bu Tür Verilerin Serbest Dolaşımına Dair Bireylerin Korunması Direktifi” onaylanmıştır. Kişisel verilerin korunması yönünde AB üyesi devletlerarasındaki mevzuat farklılıklarının ortadan kaldırılması ve verilerin serbest dolaşımını sağlamayı amaçlayan Direktifin ihtiyaçları karşılayamaması üzerine Avrupa Parlamentosu tarafından 14 Nisan 2016 tarihli ve 2016/679 sayılı “Avrupa Birliği Genel Veri Koruma Tüzüğü” kabul edilmiştir. Bu Tüzük kendinden önce uygulanmakta olan Direktif'i yürürlükten kaldırmıştır. Tüzük'ün tüm AB üyesi devletler için uyulma zorunluluğu olması sebebiyle kişisel verilerin korunmasında oluşan hukuki farklılıklar giderilerek uyum sağlanmıştır. Üst seviye uyumlaştırmanın yanında küresel alana hitap etmesi, veri aktarımında sıkı kural getirmesi ve unutulma hakkı kavramını ele alması, Tüzük'ün kişisel verilerin korunmasında devrimsel nitelikte olmasını sağlamıştır.

Kişisel verilerin korunmasında hukuksal olarak ilk bağlayıcı düzenleme olan 28 Ocak 1981 Tarih ve 108 Sayılı “Kişisel Verilerin Otomatik İşleme Tabi Tutulma Sürecinde Şahısların Korunmasına İlişkin Sözleşme”yi Türkiye hemen imzalamış fakat onaylanması 10 Şubat 2016 tarihinde gerçekleşmiştir. Bu durum AB ilerleme raporlarında sürekli gündeme getirilmiştir. AB müktesebatına uyum açısından kişisel verilerin korunmasının sağlanması için bir kanun çıkarılmasını ve bağımsız bir denetim organının kurulmasını istenmiştir. Nihayetinde Kişisel verilerin korunması hakkı 24 Mart 2016 tarihinde “6698 sayılı Kişisel Verilerin Korunması Kanunu” kabul edilmesiyle Türk hukukundan ayrı bir hak olarak yerini almıştır. Türkiye'de Kanun'un yürürlüğe girmesiyle birlikte kamu tüzel kişiliğine haiz idari ve mali açıdan özerk olan Kişisel Verileri Koruma Kurumu oluşturulmuştur. Kurum, hukuki nitelik bakımından düzenleyici ve denetleyici kurumlar arasında yerini almıştır.

Kişisel verilerin korunması bakımından Kanun'un çıkarılmış olması ve Kurumun kurulmuş olmasıyla müktesebata uyum sağlanmış görünse de 6698 sayılı Kanun'un AB

Direktifini referans alınarak oluşturulması ve Kanun’un kabulünden yaklaşık bir hafta sonra Avrupa’da kişisel verilerin korunmasında yeni düzenlemeye gidilip Tüzük’ün onaylanarak Direktif’in geçerliliğini yitirmesi müktesebata uyumda eksikliklere yol açmıştır. Bu durum Kanun’un AB müktesebatına uyumu açısından Tüzük dikkate alınarak güncellenmesi ihtiyacı ortaya çıkarmıştır. 2018 ve 2019 AB ilerleme raporlarında mevzuattaki uyumsuzluk “...bu durum, özellikle Kişisel Verileri Koruma Kurumunun yetkilerine ve kişisel verilerin korunması ile ifade ve bilgi edinme özgürlüğü hakkı arasında bir denge kurulmasına ilişkin hususlar ile ilgilidir.” ifadesiyle belirtilmiştir. Europol ve Eurojust ile Türkiye arasında verilerin paylaşılması yönündeki yapılacak olan uluslararası anlaşmanın sağlanabilmesi de Tüzük ile uyumun sağlanmış olmasıyla gerçekleştirileceği belirtilmiştir. Cumhurbaşkanlığınca yayımlanan Türkiye’nin 2019 ve 2023 yılları arasındaki hedeflerini içeren “On Birinci Kalkınma Planı”nda 6698 sayılı Kanun’un Tüzük ile uyumlu hale getirileceği yer almıştır.

Sonuç olarak müktesebata uyum için mevzuatta yapılması gereken değişiklikleri Kurum açısından değerlendirecek olursak; Kurum tarafından verilen idari cezaların artırılması gerektiği, Kurum’un AB üyesi devletlerdeki kurumlarla kişisel verilerin korunmasında uyum sağlayabilecek hale getirilmesi gerektiği, veri sorumlularına Tüzük’te belirtilen sorumlulukların getirilmesiyle Kurum’un yetkilerinin bu yönde artmasının sağlanması gerektiği, veri sorumlusunun yanında veri işleyeni de veri ihlalden sorumlu olması sağlanarak Kurum’a bu yönde idari işlem yapma yetkisi verilmesi gerektiği şeklinde sıralanabilir.

Tüzük’te kişisel verilerin korunmasına yönelik AB üyesi devletler açısından standartların belirlenmiş olması çok geniş bir etki oluşturmuştur. Üst düzey korumanın sağlanması, güncelliği ve ayrıntılı olarak kişisel verilerin korunmasını ele alması nedeniyle Türkiye’nin bu konuda uyum içinde olmasını gerekli kılmıştır. Kişisel Verileri Koruma Kurumu’nun Avrupa’ya başvuruda bulunduğu akreditasyon talebi 2019 yılı mayıs ayında kabul edilmiştir. Türkiye, kanundaki farklılıkları gidererek AB müktesebatıyla uyumu sağlamasıyla hem kişisel verilerin daha etkin korunmasını sağlayacak hem de AB’ye üyelik sürecinde büyük bir adım atmış olacaktır.

Araştırma ve Yayın Etiği Beyanı

Bu çalışma bilimsel araştırma ve yayın etiği kurallarına uygun olarak hazırlanmıştır.

Yazarların Makaleye Katkı Oranları

Yazar 1’in makaleye katkısı %50, Yazar 2’nin makaleye katkısı %50’dir.

Çıkar Beyanı

Yazarlar açısından ya da üçüncü taraflar açısından çalışmadan kaynaklı çıkar çatışması bulunmamaktadır.

KAYNAKÇA

Akgül, A. (2014). *Danıştay ve Avrupa insan hakları mahkemesi kararları ışığında kişisel verilerin korunması*. İstanbul: Beta Yayınları.

Akıncı, A. N. (2017). *Avrupa birliği genel veri koruma tüzüğü’nün getirdiği yenilikler ve türk hukuku bakımından değerlendirilmesi*. Ankara: T.C. Kalkınma Bakanlığı.

Aksoy, H. C. (2010). *Medeni hukuk ve özellikle kişilik hakkı yönünden kişisel verilerin korunması*. Ankara: Çakmak Yayınevi.

Article 29 Working dat a protection working party, opinion 4/2007 on the concept of personal data, 20.06.2007, 01248/07/EN, WP 136.

Aydın, S. E. (2015). *AİHM içtihatları bağlamında kişisel verilerin kaydedilmesi suçu*. İstanbul: Oniki Levha Yayınları.

AYM, Anayasa Mahkemesi B. No. 2013/5653, 03.03.2016 R.G. No: 29811 (24.08.2016). <https://www.resmigazete.gov.tr/eskiler/2016/08/20160824-14.pdf> (Erişim Tarihi: 02.02.2022).

Ayözger, A. Ç. (2016a). *Kişisel verilerin korunması*. İstanbul: Beta Yayıncılık.

Ayözger, A.Ç. (2016b). *Elektronik haberleşme sektöründe kişisel verilerin korunması*. Yayınlanmış Doktora Tezi, İstanbul Üniversitesi, 2016.

Bainbridge, D. I. (1997). Processing personal data and the data protection directive. *Journal of Information & Communications TechnologyLaw*, 6(1), 17-40.

Dülger, M. V. (2018). İnsan hakları ve temel hak ve özgürlükler bağlamında kişisel verilerin korunması. *İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi*, 5 (1), 71-144.

Dülger, M. V. (2019). Avrupa birliği genel veri koruma tüzüğü bağlamında kişisel verilerin korunması. *Yaşar Hukuk Dergisi*, 1(2), 71-174.

Gözler, K. (2009). *İdare hukuku (Cilt 1)*. Bursa: Ekin Yayınevi.

Hızarci, E. (2020). 6698 sayılı kişisel verilerin korunması kanununun ab veri koruma hukuku ışığında değerlendirilmesi. Ankara: Yetkin Yayıncılık.

İstanbul Bilgi Üniversitesi (2018) Avrupa Veri Koruma Mevzuatı El Kitabı. İstanbul Bilgi Üniversitesi Yayınları, https://itlaw.bilgi.edu.tr/media/2020/3/30/Bilgi_Avrupa_Veri_Koruma_Mevzuat%C4%B1_El_Kitab%C4%B1_2018_TR_v01_16022019.pdf (Erişim Tarihi: 02.02.2022).

Kılınç, D. (2012). Anayasal bir hak olarak kişisel verilerin korunması. *Ankara Üniversitesi Hukuk Fakültesi Dergisi*, 61 (3), 1089-1169.

Kişisel Verileri Koruma Kurumu, Misyon-Vizyon, <https://www.kvkk.gov.tr/Icerik/2074/Misyon---Vizyon> (Erişim Tarihi: 30.01.2022).

Kişisel Verileri Koruma Kurulunun K.2019/10 (24. Ocak.2019) <https://kvkk.gov.tr/Icerik/5362/Veri-Ihlali-Bildirim> (Erişim Tarihi: 02.02.2022).

Korkmaz, İ. (2017). *Kişisel verilerin ceza hukuku kapsamında korunması*. Ankara: Seçkin Yayıncılık.

Küzeci, E. (2020). *Kişisel verilerin korunması* (4.Basım). İstanbul: Onikilevha Yayıncılık.

Özel, K. C. (2020). Ana hatlarıyla kişisel verilerin korunmasının tarihsel süreci ile amacı ve kişisel verilerin korunması hakkı. *İstanbul Barosu Dergisi*, 94(2), 241-255.

Şahbaz, U. Alpaslan, İ. ve Sökmen, A. (2014). Türkiye’de kişisel verilerin korunmasının hukuki ve ekonomik analizi. İstanbul Bilgi Üniversitesi & TEPAV.

Şimşek, O. (2008). *Anayasa hukukunda kişisel verilerin korunması*. İstanbul: Beta Yayınları.

Yargıtay, Yargıtay Hukuk Genel Kurulu. E.2014/4-56 K.2015/1679 (17 Haziran 2015).

Yıldırım, T., Yasin, M., Kaman, N., Özdemir, H. E., Üstün, G., ve Okay Tekinsoy, Ö. (2016). *İdare hukuku*. İstanbul: On iki Levha Yayıncılık.

Extended Summary

Personal Data Protection Institution in Turkey within the Scope of European Union General Data Protection Regulation

Knowledge brings power. People's desire to be powerful has led them to use their knowledge in this direction. While the processing and using of personal data do not pose much of threaten times when access to information is difficult, the extent of the processing of personal data has constantly changed as a result of technological developments and the widespread use of the internet. Although these developments have a positive social and economic impact, making the processing of personal data easy and accessible has created a threat to the private sphere. Personal data protected within the scope of privacy has emerged as a separate right, with the boundaries of the private sphere gradually narrowing and the information that constitutes the people's confidential private life no one wants others to know is under threat. Various national and international regulations have been made for the right to personal data protection. The first international regulations on this issue were made by the UN, the OECD, and the Council of Europe. In these regulations, the procedures and principles to be followed in the processing of data, the rights and obligations arising as a result of this, and the duties and structure of the supervisory authorities to ensure the implementation of the regulations are specified in detail.

With the technological developments, the extent of protection has changed over the years and in order to provide adequate protection, the need for updating the regulations has emerged. For this purpose, the "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data" was adopted by the Council of Ministers, following the opening of the "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data" by the European Council on 28 January 1981. Aiming to eliminate the differences in legislation between EU member states to protect personal data and to ensure the free movement of data, this regulation could not meet the needs. Resultantly, the "European Union General Data Protection Regulation (No.2016/679)" was adopted by the European Parliament on April 14, 2016." This Regulation repeals the Convention that was in force before it. Due to the fact that the Regulation is obligatory for all EU member states, legal differences in the protection of personal data have been eliminated and harmonization has been achieved. In addition to its high level of harmonization, the Regulation revolutionized the protection of personal data due to addressing the global arena, imposing strict rules on data transfer, and addressing the concept of the right to be forgotten.

Dated 28 January 1981, the "The Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (ETS No.108) ", which is the first legally binding regulation in the protection of personal data, was signed by Turkey, however, its ratification was realized on 10 February 2016. This situation has been constantly brought to the agenda in EU progress reports. In terms of harmonization with the EU acquis, it was requested that a law be enacted and an independent inspection body established to ensure the protection of personal data. The protection of personal data in Turkey was firstly introduced under the Turkish Civil Code (TCC) within the framework of personal rights. Later, in the Turkish Penal Code (TPK), the crimes of recording, giving, capturing, disseminating, and not destroying personal data were regulated under the title of "crimes against private life and the confidential sphere of life", and then, with the amendment made in the Turkish Constitution in 2010, the "privacy of private sphere" is protected under Article 20. In these regulations, the protection of personal data is handled within the scope of privacy in Turkish law. The right to personal data protection was replaced as a separate right from Turkish law with the adoption of the "Law on Personal Data

Protection No. 6698” on March 24, 2016. In the Law, detailed regulations have been made on the general principles of processing personal data and its conditions, special category personal data and their processing, erasure, destruction or anonymization of personal data, transfer of personal data, and transfer of personal data abroad.

It has been emphasized in various documents that an independent and autonomous supervisory body should be created in order to ensure the effective protection of personal data. In this context, with the entry into force of the Law in Turkey, an administrative and financially autonomous Personal Data Protection Agency with a public legal entity has been established. The institution became part of the regulatory and supervisory institutions in terms of its legal nature. The institution was envisaged to be an independent authority. However, its lack of constitutional guarantee, ability to be established and abolished by law, and its association with a ministry have limited its independence, although it had full independence while performing its duties. While the establishment law of other regulatory and supervisory institutions in Turkey contains detailed content in terms of the autonomy and structuring of the institutions, Law No. 6698 did not include sufficient regulations on this issue. In terms of protection of personal data, it seems that compliance with the *acquis* has been achieved with the enactment of the Law and the establishment of the Institution since Law No. 6698 was created with reference to the Treaty. However, about a week after the adoption of the Law, a new regulation was made for the protection of personal data in Europe, the Regulation was approved and the Treaty lost its validity, leading to deficiencies in compliance with the *acquis*. This situation has revealed the need to update the Law in terms of harmonization with the EU *acquis* while taking the Regulation into account. In the 2018 and 2019 EU progress reports, the inconsistency in the legislation was stated as follows; “...this is especially related to the authorities of the Personal Data Protection Authority and issues about the balance between the right to privacy and right to freedom of expression.” It has been stated that the international agreement regarding data sharing to be made between Europol, Eurojust, and Turkey will be achieved by ensuring compliance with the Regulation. In the "Eleventh Development Plan" published by the Presidency, which includes Turkey's targets between 2019 and 2023, it was stated that Law No. 6698 would be harmonized with the Regulation.

As a result, for the changes to be made in the legislation for harmonization with the *acquis* are evaluated in terms of the Institution, the highlighting points are as follows; administrative penalties imposed by the Authority should be increased, the Institution should be able to adapt to institutions in EU member states in terms of the protection of personal data, the Institution's authorities should be increased in this direction by bringing the responsibilities specified in the Regulation to data controllers, the political influence in the election of the members of the Authority should be reduced to protect the independent status of the Institution, the data controller as well as the data processor to be responsible for the data breach, and the Authority should be given the authority to take administrative action in this direction. The fact that the standards for the protection of personal data in the Regulation have been determined based on the EU member states has had a wide impact. The provision of high-level protection has made it necessary for Turkey to comply with this issue due to its timeliness and detailed consideration of the protection of personal data. The accreditation request to Europe, which was made by the Personal Data Protection Authority, was accepted in May 2019. By eliminating the differences in the Law and ensuring harmonization with the EU *acquis*, Turkey will both ensure more effective protection of personal data and take a big step in the EU membership process.